Author:
Price, Alasdair

Title:
Pragmatic Quantum Cryptography in Next-Generation Photonic Networks

Pragmatic Quantum Cryptography in Next-Generation Photonic Networks

Alasdair B. Price

School of Physics
University of Bristol

A dissertation submitted to the University of Bristol in accordance with the requirements of the degree of Doctor of Philosophy in the Faculty of Science.

March 2019

Word count: 49,000 (approx.)

> *Saying that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about freedom of speech because you have nothing to say. It's a deeply anti-social principle because rights are not just individual, they're collective, and what may not have value to you today may have value to an entire population, an entire people, an entire way of life tomorrow. And if you don't stand up for it, then who will?*

– Edward Snowden

Abstract

Humanity's understanding of quantum physics has finally reached the level where it can be harnessed to revolutionise society. Radical new technologies will transform a wide range of fields that rely on sensing, imaging, information processing and communications. In particular, quantum computers will be able to run algorithms that offer a substantial advantage over their classical counterparts in trying to solve some of the world's hardest problems. However, there is an equally significant cost, as this allows attackers to break the public-key cryptography that underpins both our daily lives and our critical infrastructure.

Quantum key distribution is one possible defence. It uses single photons to transmit cryptographic keys, with security reliant on the principles of quantum mechanics. Here, we will endeavour to overcome some of the challenges that manifest when trying to deploy such a technology in everyday networks. We present the first demonstration of quantum key distribution as part of a software-defined architecture, ensuring compatibility with future infrastructure, and incorporating time-division multiple access to reduce implementation costs. In addition, the development of a hybrid quantum/post-quantum network acts as a first step towards ensuring quantum key distribution does not remain an isolated technology.

We also counteract a particularly devastating denial of service attack through the invention of a new protocol, established on the basis that information-theoretically secure encryption remains impractical even when the keys are supplied by a quantum device. A wide range of theoretical and experimental evidence is used to support this hypothesis. Finally, we advance the state-of-the-art in chip-to-chip quantum key distribution, using wavelength-division multiplexing to introduce additional flexibility and maximise the secret key rates.

Acknowledgements

For giving me the opportunity to develop the skills and mindset required to fix a catastrophic hardware failure in my laptop two weeks before being due to hand in, thanks must first go to my supervisors Dr. Chris Erven and Prof. John Rarity FRS.

Also appreciated are the efforts of those who proofread parts of this thesis without obligation or personal reward: Euan Allen, Henry Semenenko, Alexandra Moylett and Dr. Djeylan Aktas.

When a research group reaches the size of a small department, it becomes impossible to list each person by name who has made some kind of impact on everyday and not-so-everyday life. Instead, I will simply say thank you to all those who have helped me in what is now known as the Quantum Engineering Technology Labs (although vive la Centre for Quantum Photonics). A special mention should go to Dr. Philip Sibson, known to remain remarkably calm when new PhD students destroy several-thousand-pounds-worth of optical chip, along with an £8 fan. Also to Dr. David "that's in my thesis" Lowndes, whose thumb will continue to haunt me on flyers and billboards long after I've left Bristol.

I am grateful to Prof. Kenny Paterson for useful conversations, the workshop staff for all of their assistance, and Dr. Graham Marshall, whose chip-packaging knowledge was invaluable.

For providing an avenue to instant gratification, thanks must also go the outreach team, and especially to Rebecca McCutcheon, in the absence of whom we would never have had such a huge impact.

It would not be an acknowledgements section without a shout-out to the rest of Cohort 1 from the Quantum Engineering Centre for Doctoral Training: Jeremy Adcock, Euan Allen, Matt Day, Stefan Frick, Janna Hinchliff, Mack Johnson, Sam Morley-Short, Sam Pallister and Stasja Stanisic. Along with Dr. Peter Turner, Dr. Chris Erven, Andrea Watkins and Lin Burden, they are responsible for some of the best memories of my PhD.

Finally, to those who have made city life bearable: Florence, Jim, Tim, George, Rebekah, Tash, Gareth, Sam, Merk and Eben. And to my family: Mum, Dad and Chantal. It is a long road from fundamental research to a technology that can positively impact everyday life, and the list of people who have contributed is even longer. But the most influential names are often forgotten: those for whom the scientists and engineers want to make the world a better place.

Author's declaration

I declare that the work in this dissertation was carried out in accordance with the requirements of the university's *Regulations and Code of Practice for Research Degree Programmes* and that it has not been submitted for any other academic award. Except where indicated by specific reference in the text, the work is the candidate's own work. Work done in collaboration with, or with the assistance of others is indicated as such. Any views expressed in the dissertation are those of the author.

SIGNED: ..... DATE: .....

Table of Contents

Page

List of Tables **xi**

List of Figures **xiii**

List of Acronyms and Abbreviations **xix**

List of Symbols **xxiii**

List of Publications **xxix**

1 Introduction **1**
- 1.1 Foreword . . . 1
- 1.2 Thesis Outline . . . 2

2 Background **5**
- 2.1 Modern Cryptography . . . 6
  - 2.1.1 Symmetric-Key Encryption . . . 6
  - 2.1.2 Symmetric-Key Authentication . . . 10
  - 2.1.3 Public-Key Cryptography for Symmetric-Key Distribution . . . 12
- 2.2 Quantum Information . . . 14
  - 2.2.1 Quantum Mechanics . . . 15
  - 2.2.2 Quantum Computing . . . 19
  - 2.2.3 Photonic Quantum Bits . . . 22
- 2.3 Quantum Cryptography . . . 31
  - 2.3.1 Quantum Key Distribution Protocols . . . 31
  - 2.3.2 Attacks on Quantum Key Distribution . . . 34
- 2.4 Summary . . . 39

3 Time-Shared Quantum Cryptography on Software-Defined Networks **41**
- 3.1 State-of-the-Art in Telecommunications Networks . . . 42
  - 3.1.1 Quantum Key Distribution Networks . . . 42

3.1.2 Software-Defined Networks . . . 45
3.1.3 Next-Generation Quantum Networks . . . 48
3.2 A First-Generation Testbed for Quantum Key Distribution on Software-Defined Networks 50
3.2.1 The Clavis^2 Quantum Key Distribution System . . . 50
3.2.2 The Polatis Optical Switch . . . 53
3.2.3 SFP+ and QSFP+ Transceivers . . . 56
3.2.4 Equipment that is Detrimental to Quantum Key Distribution . . . 56
3.3 Time-Division Multiple Access Quantum Key Distribution . . . 59
3.3.1 A Time-Sharing Model for Cost-Effective Quantum Key Distribution . . . 60
3.3.2 Bristol is Open Emulator . . . 62
3.3.3 Results . . . 65
3.4 Outlook . . . 68
3.4.1 Construction of the Second-Generation Testbed and Bristol Quantum Network 70

4 The Impracticality of the One-Time Pad for Everyday Quantum-Secured Communications 75
4.1 The Effect of the Classical Channel on Key Generation . . . 76
4.2 The Effect of the Quantum Channel on Key Generation . . . 85
4.3 State of the One-Time Pad . . . 89
4.4 Outlook . . . 90
4.4.1 An Attempt to Circumvent the Restrictions on the Quantum and Classical Channels . . . 91

5 Quantum Key Distribution for Imperfect Encryption Schemes 93
5.1 A New Denial of Service Attack on Quantum Key Distribution . . . 94
5.2 BB84-AES: A Quantum Key Distribution Protocol for Rapid Denial of Service Detection 95
5.3 Initial Security Analysis of BB84-AES . . . 97
5.3.1 Rapid Denial of Service Detection . . . 97
5.3.2 100% Sifting Efficiency . . . 99
5.3.3 Authentication Tag Confidentiality . . . 100
5.3.4 Resistance to Photon Number Splitting Attacks on Two-Photon Pulses . . . 101
5.3.5 Perfect Forward Secrecy when Combining BB84-AES with Encryption Based on the Advanced Encryption Standard Block Cipher. . . . 102
5.3.6 Everlasting Security when Combining BB84-AES with the One-Time Pad Encryption Scheme . . . 102
5.3.7 The Role of Randomness in BB84-AES . . . 103
5.4 Optimising BB84-AES for Resource-Limited Applications . . . 104
5.4.1 Reduced Processing Variant . . . 104
5.4.2 Reduced Bandwidth Variant . . . 104

5.4.3 Dense Information Transfer Variant 106
5.5 Comparing BB84-AES with Other Photon-Number-Splitting-Resistant and Highly-Efficient Quantum Key Distribution Protocols 109
5.6 Outlook 110
5.6.1 On the Cryptographic Choices for Communicating the Bases 112
5.6.2 Beyond Basis Announcements and BB84 114

6 Implementing Hybrid Quantum/Post-Quantum Security to Defend Against Shor's Algorithm 117
6.1 Consequences of Computationally-Secure Encryption in Quantum-Safe Networks . 118
6.2 Post-Quantum Cryptography 121
6.2.1 The Post-Quantum Landscape 121
6.2.2 The McEliece Cryptosystem 122
6.2.3 The Niederreiter Cryptosystem 126
6.3 Scenario I: Symmetric-Key Conversion for Long-Term Quantum Security in a Post-Quantum Ecosystem 126
6.4 Scenario II: Quantum Key Distribution as an Entropy Source for Efficient and Automated Private-Key Backups 128
6.5 Scenario III: Lesser-Trusted Nodes for Long-Distance Quantum Key Distribution & Scenario IV: Introducing Compatibility with Legacy Networks 133
6.6 Outlook 137

7 Integrated Photonics for High-Speed, Reconfigurable Quantum Key Distribution 139
7.1 Integrated Photonics 141
7.1.1 Platforms for Integrated Photonics 141
7.1.2 Sources and Detectors 142
7.1.3 Photonic Circuit Components 144
7.2 Device Characterisation for On-Chip Wavelength-Division Multiplexed Quantum Key Distribution 152
7.2.1 Characterising the Wavelength-Division Multiplexers 154
7.2.2 Characterising the Integrated Laser 155
7.2.3 Modulating the Asymmetricity of a Mach-Zehnder Interferometer 156
7.3 Monolithic Wavelength-Division Multiplexed Quantum Key Distribution 159
7.4 Next-Generation Silicon Photonic Chip Design 164
7.4.1 A Reference-Frame-Independent Quantum Key Distribution Transmitter . . 165
7.4.2 A Transmitter and Receiver for Chip-to-Chip Quantum Key Distribution at 1310 nm 167
7.4.3 A Polarisation-Compensating Receiver for Time-Bin-Encoded Quantum Key Distribution 170

7.5 Outlook 171

8 Conclusion **177**

Bibliography **181**

A Appendix to Chapter 2: Quantum Logic Gates **213**

B Appendix to Chapter 2: The Exponents of the Coherent-State Beam-Splitter Output Commute **215**

C Appendix to Chapter 6: Summarising Ciphertext Indistinguishability **217**

D Appendix to Chapter 7: A Description of the Gluing Process for the Four-Channel Integrated Receiver **219**

E Appendix to Chapter 7: Consequences of Tesselating Multiple Silicon Chips on a Single Wafer **221**

List of Tables

Table		Page
2.1	Truth table for the XOR function	7
2.2	S-box used in the Advanced Encryption Standard to perform byte-wise substitutions	8
2.3	Quantum resource estimates for attacking modern cryptography	23
3.1	A history of quantum networks throughout the world	43
3.2	Wavelength bands for optical communications	54
4.1	Average number of classical bits transmitted by the ID Quantique Clavis^2 per secret bit for both the minimum and maximum attenuations at which key is reliably generated	81
5.1	Showing the probability of a bit-flip error occurring between Alice and Bob for BB84-AES with reduced processing in the presence of an eavesdropper	105
5.2	Comparing the original forms of BB84-AES, BB84 with biased bases, SARG04 and BB84 with decoy states	111

List of Figures

Figure **Page**

2.1 Demonstrating the effect of directly encrypting the Centre for Quantum Photonics logo with the Advanced Encryption Standard . . . 8
2.2 Illustrating (a) the encryption process and (b) the decryption process for a block cipher running in Counter Mode . . . 9
2.3 Illustrating the mechanisms used for encryption and authentication in Galois/Counter Mode . . . 10
2.4 Hypothesised relationship between the polynomial time, bounded-error quantum polynomial time, non-deterministic polynomial time and polynomial space complexity classes . . . 21
2.5 The four polarisation states $|H\rangle$, $|V\rangle$, $|D\rangle$ and $|A\rangle$ . . . 24
2.6 The four dual-rail states used to represent the logical qubits $|\overline{0}\rangle$, $|\overline{1}\rangle$, $|+\rangle$ and $|-\rangle$ . . . 25
2.7 An example setup used for encoding quantum information onto the time-of-arrival of a single photon . . . 26
2.8 Labelling convention for the input and output modes of (a) a single beam splitter, and (b) two beam splitters connected in series . . . 27

3.1 The Micius quantum satellite as seen from the Shanghai ground station . . . 44
3.2 Showing the distribution of publicly-known quantum networks throughout the world, along with the types of technology that have been implemented on each continent . . . 46
3.3 Illustrating the separation between the control plane and the data plane in software-defined networks, with higher-level applications sitting over the top . . . 47
3.4 The internal structure of a single node in a software-defined network . . . 47
3.5 Physical topology of the Bristol Quantum Network . . . 49
3.6 Physical topology of the UK Quantum Network . . . 49
3.7 Part of the first-generation testbed, capable of emulating any configuration of the Bristol Quantum Network . . . 51
3.8 Optical schematic for the ID Quantique Clavis^2 . . . 52
3.9 Showing how (a) the secret key rate and (b) the quantum bit error rate changes with loss for the ID Quantique Clavis^2 . . . 54

3.10 The internal structure of a Polatis optical switch 55
3.11 Showing how (a) the secret key rate and (b) the quantum bit error rate of an ID Quantique Clavis^2 changes depending on whether or not the quantum channel passes through a Polatis switch 55
3.12 Illustrating the amplification process for Er^{3+} 57
3.13 Noise profile for a Nortel Networks erbium-doped fibre amplifier, acting on a 1550 nm signal 58
3.14 The internal structure of a Waveshaper programmable optical processor 59
3.15 Showing how (a) the secret key rate and (b) the quantum bit error rate of an ID Quantique Clavis^2 changes depending on whether or not the quantum channel passes through a Waveshaper programmable optical processor 60
3.16 A logical diagram of the time-sharing setup 61
3.17 A network topology for which the initial configuration of quantum devices may be sub-optimal due to future ambiguity 62
3.18 A physical diagram of the emulator, based on a Bristol is Open node 63
3.19 Workflow for the software layer of time-division multiple access quantum key distribution 64
3.20 Showing how the time taken to complete the first round of quantum key distribution changes with loss for the ID Quantique Clavis^2 66
3.21 Showing the maximum number of senders per receiver in a time-division multiple access quantum key distribution network 69
3.22 Illustrating the setup used for the first transmission over the Bristol Quantum Network . 71
3.23 Showing (a) the secret key rate and (b) the quantum bit error rate for an ID Quantique Clavis^2 installed on the first link of the Bristol Quantum Network 71
3.24 Showing the crosstalk from a single classical channel into a single quantum channel when their light paths cross inside the Polatis switch 72
3.25 The second-generation testbed, capable of emulating any configuration of the Bristol Quantum Network and acting as a fully-fledged fifth node 73

4.1 A graphical representation of the relationships between the number of classical bits per pulse, the number of secret bits per pulse and the number of classical bits per usable secret bit 77
4.2 A graphical representation of the relationships between the channel variables used in this chapter, considering cases when the on-peak channel (a) does not, and (b) does take advantage of any unused off-peak capacity 79
4.3 The encapsulation structure for an Ethernet II frame containing an Internet Protocol version 4 packet, which in turn contains a Transmission Control Protocol packet 81

4.4 Showing the amount of off-peak time required per second of on-peak time in order to encrypt all data with a quantum key distribution (QKD)-keyed one-time pad, and considering only limitations imposed by the classical QKD channel for the ID Quantique Clavis^2 83

4.5 Showing the amount of off-peak time required per second of on-peak time in order to encrypt all data with the Advanced Encryption Standard running in Galois/Counter Mode, keyed using quantum key distribution (QKD) and considering only limitations imposed by the classical QKD channel for the ID Quantique Clavis^2 84

4.6 Comparing world-record quantum secret key rates with average end-user connection speeds, classical data rates from the IEEE Ethernet standards, and world-record classical data rates using experimental technology 87

4.7 Showing the amount of off-peak time required per second of on-peak time in order to encrypt all data with a quantum-key-distribution-keyed one-time pad, and considering only limitations imposed by the quantum channel 89

5.1 Block diagram showing the transmission of a single bit of key from Alice to Bob for BB84-AES with reduced processing 106

5.2 Illustrating how changing the number of bases represented by a single authentication tag affects both classical communication and computational resource requirements for BB84-AES with dense information transfer 108

5.3 Showing the amount of off-peak time required per second of on-peak time in order to encrypt all data with the Advanced Encryption Standard running in Galois/Counter Mode, keyed using BB84-AES and considering only limitations imposed by the classical quantum-key-distribution channel, modelled for the ID Quantique Clavis^2 113

6.1 Decision tree for generating quantum-safe symmetric encryption keys in networks of fixed capacity 120

6.2 An example of a Privacy-Enhanced-Mail-formatted McEliece public key 127

6.3 Workflow for generating symmetric keys using a McEliece key encapsulation mechanism and performing a quantum-secure conversion, the result of which is supplied to an authenticated encryption scheme 129

6.4 Illustrating the generation of public/private key pairs when quantum key distribution is used as an entropy source to enable fast, automated backups 130

6.5 Illustrating how, for a range of attenuations on the quantum channel, the fastest approach to sequential entropy backups depends on the number of corresponding private keys . 130

6.6 Showing how, experimentally, the time taken to sequentially perform entropy backups depends on the number of corresponding private keys 131

6.7 Simulating how the fastest approach to sequential entropy backups will depend on the number of corresponding private keys when the size of the quantum secret key is fixed at the lowest value observed across all attenuations . . . 132
6.8 Simulating how the secret key size of the ID Quantique Clavis^2 affects the minimum number of backups above which quantum key distribution is a faster solution than McEliece . . . 132
6.9 Rate at which the post-quantum key-encapsulation-mechanism-distributed keys can be refreshed from scratch, relative to each ID Quantique Clavis^2 quantum-key-distribution key . . . 136
6.10 Illustrating the topology considered for interfacing optical quantum networks with legacy devices . . . 137

7.1 Circuit symbol for a Fabry-Perot laser . . . 142
7.2 Circuit symbol for an avalanche photodiode . . . 143
7.3 Circuit symbol for a superconducting-nanowire single-photon detector . . . 143
7.4 Circuit symbol for a delay line . . . 144
7.5 Circuit symbol for a waveguide crosser . . . 144
7.6 Circuit symbol for a one-dimensional grating coupler . . . 145
7.7 Circuit symbol for a two-dimensional grating coupler . . . 145
7.8 Circuit symbol for a directional coupler . . . 145
7.9 Illustrating the optical intensity on each output of a directional coupler, for an arbitrary coupling constant . . . 146
7.10 Circuit symbol for a multi-mode interferometer . . . 146
7.11 Illustrating periodic self-imaging of the input signal in a multi-mode interferometer . . . 147
7.12 Circuit symbol for a thermo-optic phase modulator . . . 147
7.13 Circuit symbol for an electro-optic phase modulator . . . 148
7.14 Circuit symbol for a carrier-depletion modulator . . . 148
7.15 Circuit diagram for a Mach-Zehnder interferometer constructed from directional couplers and a thermo-optic phase modulator . . . 149
7.16 Circuit symbol for a switch constructed from a Mach-Zehnder interferometer . . . 149
7.17 Circuit diagram for a de-multiplexing asymmetric Mach-Zehnder interferometer . . . 151
7.18 Illustrating how a wavelength-division multiplexer is used to combine the outputs from two Alice chips down a single channel. A de-multiplexer is used at the end to split the signals and divert them to different Bobs . . . 152
7.19 A schematic of the two-channel Bob chip with wavelength-division de-multiplexing capabilities . . . 153
7.20 A schematic of the single-channel Alice chip . . . 154
7.21 Wavelength-division de-multiplexing white light using the bulk arrayed waveguide grating . . . 155

7.22 Wavelength-division de-multiplexing white light using the asymmetric Mach-Zehnder interferometer on the Bob chip 156
7.23 Temperature-tuning the asymmetric Mach-Zehnder interferometer on the Bob chip . . . 157
7.24 (a) Optical spectra for the integrated laser on the Alice chip over a range of different temperatures. (b) Plotting the peak wavelength of the integrated laser against the temperature at which the chip is stabilised 158
7.25 Fine-tuning the peak wavelength for the integrated laser on the Alice chip by applying a range of different voltages to the tunable distributed Bragg reflectors 158
7.26 Showing the physical setup of the Alice chip, with an external probe on a temporary mount 159
7.27 Showing how the absolute phase shift across a Mach-Zehnder interferometer varies according to the voltage applied by an external probe 160
7.28 The test transmitter for monolithic wavelength-division multiplexed quantum key distribution 161
7.29 A simplified schematic of the four-channel Bob chip with wavelength-division de-multiplexing capabilities 162
7.30 The fully packaged receiver chip for monolithic wavelength-division multiplexed quantum key distribution 163
7.31 Plotting the absolute loss for different lengths of component-free waveguide on the four-channel Bob chip 164
7.32 Plotting (a) the current-voltage relationship for a thermo-optic phase modulator on the Bob chip, and (b) the voltage-dependent relative phase shift of the Mach-Zehnder interferometer in which it is embedded 165
7.33 A schematic for Anubis, the 1550 nm reference-frame-independent quantum key distribution transmitter chip 166
7.34 The mask for Anubis, compiled from source code written in Python 168
7.35 Raman noise for a single classical signal emulated by a 1550 nm continuous-wave laser with a -4.8 dBm launch power 169
7.36 A schematic for Big Ear, the 1310 nm quantum key distribution receiver chip 170
7.37 The mask for Big Ear, compiled from source code written in Python 170
7.38 A schematic for Cher Ami, the 1310 nm quantum key distribution transmitter chip that can be used to implement a range of protocols 171
7.39 The mask for Cher Ami, compiled from source code written in Python 172
7.40 A schematic for Dzakar, the 1550 nm quantum key distribution chip with clock de-multiplexing or polarisation-compensating capabilities 173
7.41 The mask for Dzakar, compiled from source code written in Python 174

E.1 Showing the complete mask for the silicon quantum key distribution devices Anubis, Big Ear, Cher Ami and Dzakar 222

List of Acronyms and Abbreviations

Expansion	Acronym/Abbreviation
Advanced Encryption Standard	AES
Asymmetric Mach-Zehnder interferometer	AMZI
Avalanche photodiode	APD
Arrayed waveguide grating	AWG
Bennett-Brassard 1984	BB84
Bristol is Open	BiO
Carrier-depletion modulator	CDM
100 Gbit/s C form-factor pluggable	CFP4
Complementary metal–oxide–semiconductor	CMOS
Central processing unit	CPU
Counter Mode	CTR
Continuous-variable quantum key distribution	CV-QKD
Distributed denial of service	DDoS
Denial of service	DoS
Discrete-variable quantum key distribution	DV-QKD
Dense wavelength-division multiplexing	DWDM
Ekert 1991	E91
Erbium-doped fibre amplifier	EDFA
Electro-optic phase modulator	EOPM
Floodlight quantum key distribution	FL-QKD
Galois/Counter Mode	GCM
Gottesman-Lo-Lütkenhaus-Preskill	GLLP
Hash-Based Message Authentication Code Deterministic Random Bit Generator	HMAC_DRBG
Institute of Electrical and Electronics Engineers	IEEE
Indistinguishability under non-adaptive chosen ciphertext attack	IND-CCA1
Indistinguishability under adaptive chosen ciphertext attack	IND-CCA2
Indistinguishability under chosen plaintext attack	IND-CPA

Indium phosphide . . . . . InP
Internet Protocol version 4 . . . . . IPv4
Internet Protocol version 6 . . . . . IPv6
Key derivation function . . . . . KDF
Key Derivation Function 1 . . . . . KDF1
Key Derivation Function 2 . . . . . KDF2
Key encapsulation mechanism . . . . . KEM
Learning With Errors . . . . . LWE
Message authentication code . . . . . MAC
Measurement-device-independent . . . . . MDI
Microelectromechanical system . . . . . MEMS
Multi-mode interferometer . . . . . MMI
Mach-Zehnder interferometer . . . . . MZI
National Institute of Standards and Technology . . . . . NIST
One-time pad . . . . . OTP
Printed circuit board . . . . . PCB
Privacy Enhanced Mail . . . . . PEM
Pretty Good Privacy . . . . . PGP
Photon number splitting . . . . . PNS
Pseudorandom function . . . . . PRF
Programming interface . . . . . PI
Pseudorandom permutation . . . . . PRP
Pound-force per square inch . . . . . psi
Quantum bit error rate . . . . . QBER
Quantum key distribution . . . . . QKD
Quantum random number generator . . . . . QRNG
100 Gbit/s quad small form-factor pluggable QSFP28
Enhanced quad small form-factor pluggable . . . . . QSFP+
Random-access memory . . . . . RAM
Reference-frame-independent . . . . . RFI
Random number generator . . . . . RNG
Rivest–Shamir–Adleman . . . . . RSA
Scarani-Acín-Ribordy-Gisin 2004 . . . . . SARG04
Software-defined network . . . . . SDN
Enhanced small form-factor pluggable . . . . . SFP+
Secure Hash Algorithm 2 . . . . . SHA-2
Secure Hash Algorithm 256 . . . . . SHA-256
Secure Hash Algorithm 512 . . . . . SHA-512

Supersingular Isogeny Diffie-Hellman . . . . . SIDH
Silicon . . . . . Si
Silicon nitride . . . . . Si_3N_4
Silicon dioxide . . . . . SiO_2
Single-mode fibre . . . . . SMF
Superconducting nanowire single-photon detector . . . . . SNSPD
Semiconductor optical amplifier . . . . . SOA
Silicon-on-insulator . . . . . SoI
Silicon oxynitride . . . . . SiO_xN_y
Transmission Control Protocol . . . . . TCP
Tunable distributed Bragg reflector . . . . . TDBR
Time-division multiple access . . . . . TDMA
Transport Layer Security . . . . . TLS
Thermo-optic phase modulator . . . . . TOPM
Transverse electric . . . . . TE
Transverse magnetic . . . . . TM
Ultraviolet . . . . . UV
V-Groove array . . . . . VGA
Wavelength-division multiplexing . . . . . WDM
Exclusive-OR . . . . . XOR

List of Symbols

Name	Symbol
Zero-photon number state	$\|0\rangle$
Qubit in the logical zero state	$\|\overline{0}\rangle$
Identity operator	$\hat{\mathbb{1}}$
Identity matrix	$\mathbb{1}$
One-photon number state	$\|1\rangle$
Qubit in the logical one state	$\|\overline{1}\rangle$
Primitive element of $\mathbb{Z}_V^*$	a
Annihilation operator	$\hat{a}$
Creation operator	$\hat{a}^\dagger$
Scrambler matrix	$\mathbf{A}$
Qubit in the anti-diagonal polarisation state	$\|A\rangle$
Arbitrary bit	b
Arbitrary basis	B
Bounded-error quantum polynomial time complexity class	BQP
Ciphertext	c
Cloning operator	$\hat{C}$
Set of complex numbers	$\mathbb{C}$
Set of ciphertexts	$\mathcal{C}$
Toffoli gate	CCNOT
Controlled-NOT gate	CNOT
Number of communication nodes	d
Number of multiplexed devices	D_{mux}
Number of time-shared devices	D_{t}
Displacement operator	$\hat{D}(\alpha)$
Qubit in the diagonal polarisation state	$\|D\rangle$
Arbitrary decryption function	$\text{Dec}(\cdot)$
Euler's number	e
Quantum bit error rate	E
Electric field	$\vec{E}$

Arbitrary encryption function . . . . . $\mathrm{Enc}(\cdot)$
Fractional part of a number . . . . . $\{\cdot\}_f$
Random integer . . . . . F
Goppa code generator matrix . . . . . $\mathbf{G}$
Public generator matrix . . . . . $\mathbf{G}'$
Greatest common divisor . . . . . $\gcd(\cdot,\cdot)$
Arbitrary hash function . . . . . h
Binary entropy function . . . . . $H_2(\cdot)$
Hadamard operator . . . . . $\hat{H}$
Set of hash function outputs . . . . . $\mathcal{H}_m$
Qubit in the horizontal polarisation state . . . . . $|H\rangle$
Arbitrary iterator i
Unit imaginary number . . . . . $\mathbb{i}$
Qubit in the logical $+\mathbb{i}$ state . . . . . $|\mathbb{i}\rangle$
Qubit in the logical $-\mathbb{i}$ state . . . . . $|-\mathbb{i}\rangle$
$L = 6$ energy level I
Set of basis announcements . . . . . $\mathcal{I}$
Arbitrary iterator . . . . . j
Total angular momentum . . . . . J
Arbitrary cryptographic key . . . . . k
Cipher key . . . . . k_{C}
Hash function key . . . . . k_{H}
Initial secret key . . . . . k_{init}
One-time key for a message authentication code . . . . . k_{M}
Number of encryption keys generated per key exchange . . . . . K_{max}
Set of one-time keys for message authentication codes . . . . . $\mathcal{K}_{\mathrm{M}}$
Goppa code length l
Total orbital angular momentum L
Binary logarithm . . . . . $\log_2(\cdot)$
Plaintext . . . . . m
Measurement operator for outcome i . . . . . $\hat{M}_i$
Set of measurement operators . . . . . $\mathcal{M}$
Machine epsilon . . . . . $\mathbb{M}$
Effective refractive index . . . . . n_{eff}
Number of transmitted qubits . . . . . N
Non-deterministic polynomial time complexity class . . . . . NP
Arbitrary operator . . . . . $\hat{O}$
Length of the output from a pseudo-random function . . . . . $|p|$

Permutation matrix . . . . . $\mathbf{P}$
Polynomial time complexity class . . . . . P
Polynomial space complexity class . . . . . PSPACE
Probability . . . . . $\mathrm{Prob}(\cdot)$
Γ-photon gain . . . . . Q_Γ
Qudit dimensionality . . . . . r
Algebraic dimension . . . . . r_a
Classical bits per weak coherent pulse . . . . . $R_{\mathrm{c/p}}$
Classical bits per secret bit . . . . . $R_{\mathrm{c/s}}$
Quantum clock rate . . . . . $R_{\mathrm{p/t}}$
Number of secret bits per weak coherent pulse . . . . . $R_{\mathrm{s/p}}$
Secret key rate . . . . . $R_{\mathrm{s/t}}$
Phase-shift gate . . . . . $\hat{R}_\theta$
One-time number (nonce) . . . . . s
Total spin . . . . . S
Phase gate . . . . . $\hat{S}$
Time . . . . . t
Characterisation time . . . . . t_{char}
Time taken to exhaust distributed key . . . . . t_{exhaust}
Initialisation time . . . . . t_{init}
Average time taken to generate a single secret bit . . . . . t_{ssb}
Qubit in the ith time-bin state . . . . . $|t_i\rangle$
Temperature . . . . . T
T gate . . . . . $\hat{T}$
Set of authentication tags . . . . . $\mathcal{T}$
Unused classical channel capacity . . . . . u
Unitary operator . . . . . $\hat{U}$
Directional coupler operator . . . . . $\hat{U}_{\mathrm{DC}}$
Initialisation vector v
Prime number V
Qubit in the vertical polarisation state . . . . . $|V\rangle$
Optical field amplitude . . . . . W
Arbitrary number x
Pauli-X operator . . . . . $\hat{X}$
Arbitrary number . . . . . y
Pauli-Y operator . . . . . $\hat{Y}$
Γ-photon yield . . . . . Y_Γ
Distance . . . . . z

Length of a physical object . . . . . $|z|$
Pauli-Z operator . . . . . $\hat{Z}$
Set of integers . . . . . $\mathbb{Z}$
Set of positive integers . . . . . $\mathbb{Z}^{+}$
Multiplicative group of integers modulo V . . . . . $\mathbb{Z}_{V}^{*}$
Eigenvalue of the annihilation operator . . . . . α
Coherent state . . . . . $|\alpha\rangle$
Size of the lookup table in BB84-AES (dense information transfer) . . . . . β
Number operator . . . . . $\hat{\gamma}$
Arbitrary number state . . . . . $|\gamma\rangle$
Γ-photon number state . . . . . $|\Gamma\rangle$
Probability of distinguishing AES from a truly random function . . . . . δ
Difference . . . . . Δ
Free spectral range . . . . . $\Delta\lambda_{\mathrm{FSR}}$
Statistical deviation from an ideal model . . . . . ε
Error vector . . . . . $\vec{\epsilon}$
Sifting efficiency . . . . . ζ
Variable offset used in BB84-AES (dense information transfer) . . . . . η
Phase . . . . . θ
Absorption co-efficient . . . . . Θ
Coupling constant . . . . . κ
Wavelength . . . . . λ
Angle of separation . . . . . Λ
Mean photon number . . . . . μ
Number of basis announcements per authentication tag . . . . . ξ
Iterator used in BB84-AES (dense information transfer) . . . . . Ξ
Archimedes' constant . . . . . π
Propagation constant . . . . . ρ
Speed of light . . . . . σ
Adjusted channel capacity per unit time . . . . . ς
Off-peak data rate . . . . . $\varsigma_{\vee}$
On-peak data rate . . . . . $\varsigma_{\wedge}$
Authentication tag . . . . . τ
Number of bits communicated during error correction . . . . . $|\Upsilon|$
Number of correctable errors . . . . . υ
Arbitrary quantum state . . . . . $|\phi\rangle$
Product of two numbers, each equal to a prime minus one . . . . . Φ_{1}
Product of two primes . . . . . Φ_{2}

Second-order non-linear electric susceptibility . . . . . $\chi^{(2)}$
Arbitrary quantum state . . . . . $|\chi\rangle$
Arbitrary quantum state . . . . . $|\psi\rangle$
Orthogonal state to $|\psi\rangle$ . . . . . $|\psi^{\perp}\rangle$
Angular frequency . . . . . ω
Number of bits communicated during sifting . . . . . $|\Omega|$
Qubit in the logical + state . . . . . $|+\rangle$
Qubit in the logical − state . . . . . $|-\rangle$
Unknown quantum state . . . . . $|?\rangle$
Number of bits associated with extraneous communications . . . . . $|\boldsymbol{\times}|$
Cardinality of $\mathcal{A}$, an arbitrary set . . . . . $\#\mathcal{A}$
Concatenation of the arbitrary bit strings x and y . . . . . $x||y$
Length of an arbitrary bit string, x . . . . . $|x|$

List of Publications

$*$ = Corresponding Author(s)

N.B: Quantum technology research is highly interdisciplinary and, as such, the conventions for author lists differ depending on the place of publication. Here, most follow the physics standard; non-alphabetical and in order of contribution. Two follow the engineering standard, where the list is split by research group and the sub-lists are ordered by contribution. These are highlighted by [Eng], and the lead authors for each group are the corresponding authors. One paper is ordered alphabetically as all authors were considered to have contributed equally. This is highlighted by [Alph], and the corresponding author was assigned randomly.

Articles and Conference Proceedings

[Alph] J. C. Adcock, E. Allen, M. Day*, S. Frick, J. Hinchliff, M. Johnson, S. Morley-Short, S. Pallister, A. B. Price & S. Stanisic. "Advances in Quantum Machine Learning", arXiv:1512.02900, 2015.

[Eng] A. Aguado*, E. Hugues-Salas, P. A. Haigh, J. Marhuenda, A. B. Price*, P. Sibson, J. E. Kennard, C. Erven, J. G. Rarity, M. G. Thompson, A. Lord, R. Nejabati & D. Simeonidou. "First Experimental Demonstration of Secure NFV Orchestration over an SDN-Controlled Optical Network with Time-Shared Quantum Key Distribution Resources", Proceedings of the 42nd European Conference and Exhibition on Optical Communication (ECOC), 2016.

[Eng] A. Aguado*, E. Hugues-Salas, P. A. Haigh, J. Marhuenda, A. B. Price*, P. Sibson, J. E. Kennard, C. Erven, J. G. Rarity, M. G. Thompson, A. Lord, R. Nejabati & D. Simeonidou. "Secure NFV Orchestration Over an SDN-Controlled Optical Network With Time-Shared Quantum Key Distribution Resources", IEEE Journal of Lightwave Technology, 2017.

A. B. Price*, J. G. Rarity & C. Erven. "A Quantum Key Distribution Protocol for Rapid Denial of Service Detection", arXiv:1707.03331, 2017.

A. B. Price*, P. Sibson, C. Erven, J. G. Rarity & M. G. Thompson. "High-Speed Quantum Key Distribution with Wavelength-Division Multiplexing on Integrated Photonic Devices", Conference on Lasers and Electro-Optics (CLEO), OSA Technical Digest, 2018.

P. Sibson, C. Erven, J. Kennard, A. B. Price, D. Llewellyn, J. Wang, M. G. Thompson*. "Chip-Based Quantum Communications", Proceedings of the 44th European Conference and Exhibition on Optical Communication (ECOC), 2018.

R. Santagati, A. B. Price, J. G. Rarity & M. Leonetti. “Localisation-Based Two-Photon Wavefunction Information Encoding”. *Submitted.*

Conference and Workshop Presentations

P. Sibson*, A. B. Price, S. Stanisic, J. Kennard, C. Erven, J. L. O’Brien & M. G. Thompson. “Integrated Photonics for Quantum Key Distribution”, Contributed Talk, 6th International Conference in Quantum Cryptography (QCRYPT), Washington DC, USA, 2016.

A. B. Price*, A. Aguado*, E. Hugues-Salas, P. A. Haigh, P. Sibson, J. Marhuenda, J. Kennard, J. G. Rarity, M. G. Thompson, R. Nejabati, D. Simeonidou & C. Erven. “Towards the Deployment of Quantum Key Distribution Systems in a Software Defined Networking Environment”, Poster Presentation, 6th International Conference in Quantum Cryptography (QCRYPT), Washington DC, USA, 2016.

A. B. Price*, A. Aguado*, E. Hugues-Salas, P. A. Haigh, P. Sibson, J. Marhuenda, J. Kennard, J. G. Rarity, M. G. Thompson, R. Nejabati, D. Simeonidou & C. Erven. “Practical Integration of Quantum Key Distribution with Next-Generation Networks”, Contributed Talk, 2nd International Conference for Young Quantum Information Scientists (YQIS), Barcelona, Spain, 2016.

A. B. Price*, A. Aguado, E. Hugues-Salas, P. A. Haigh, P. Sibson, J. Marhuenda, J. Kennard, J. G. Rarity, M. G. Thompson, R. Nejabati, D. Simeonidou & C. Erven. “Scalable Quantum Key Distribution on Software Defined Networks”, Poster Presentation, 4th Bristol Quantum Information Technologies Workshop (BQIT), Bristol, UK, 2017.

P. Sibson*, D. Lowndes, S. Frick, A. B. Price, H. Semenenko, F. Raffaelli, D. Llewellyn, J. Kennard, Y. Ou, F. Ntavou, E. Hugues-Salas, A. Hart, R. Collins, A. Laing, C. Erven, R. Nejabati, D. Simeonidou, M. G. Thompson & J. G. Rarity. “Networked Quantum-Secured Communications with Hand-held and Integrated Devices: Bristol’s Activities in the UK Quantum Communications Hub”, Contributed Talk, 7th International Conference in Quantum Cryptography (QCRYPT), Cambridge, UK, 2017.

A. B. Price*, J. G. Rarity & C. Erven, “Quantum Key Distribution Without Sifting”, Poster Presentation, 7th International Conference in Quantum Cryptography (QCRYPT), Cambridge, UK, 2017.

A. B. Price*, J. G. Rarity & C. Erven. “A Quantum Key Distribution Protocol for Rapid Denial of Service Detection”, Poster Presentation, 5th Bristol Quantum Information Technologies Workshop (BQIT), Bristol, UK, 2018.

A. B. Price*, J. G. Rarity & C. Erven, “Implementing Hybrid Quantum-Postquantum Security in a Prototype Network”, Poster Presentation, 8th International Conference in Quantum Cryptography (QCRYPT), Shanghai, China, 2018.

D. Aktas*, P. Sibson, D. Lowndes, S. Frick, A. B. Price, H. Semenenko, F. Raffaelli, D. Llewellyn, J. Kennard, Y. Ou, F. Ntavou, E. Hugues-Salas, A. Hart, R. Collins, A. Laing, C. Erven, R. Nejabati, D. Simeonidou, M. G. Thompson & J. G. Rarity. “A Metropolitan Quantum Network with Hand-Held and Integrated Devices”, Poster Presentation, GDR IFQA - 9th Colloquium, Montpellier, France, 2018.

CHAPTER 1

INTRODUCTION

1.1 Foreword

Quantum computers will have far-reaching effects on society, through efficient simulation of complex molecules [1, 2], and by providing new insights into machine learning [3–5]. Applications such as environmental technology and drug design are expected to benefit enormously, however a quantum computer can also solve the mathematical problems that we use for securing our electronic data. This will enable cyber attacks to be mounted both on individuals and critical pieces of infrastructure.

To illustrate the scale of the problem, we note that the systems used for controlling our water supply, sewage, gas pipelines and power grid [6] could all be infiltrated if we do not employ any kind of countermeasure. Attackers could target the networks on which our medical records are stored, or to which life-saving equipment is connected, either by stealing login credentials, or through compromising the distribution of software updates. Additional opportunities will arise for those in the business of seeding misinformation (colloquially known as fake news), because connections to legitimate websites will no longer be properly authenticated. Finally, one can only speculate on what would happen to the world economy if the majority of internet transactions were modified, such that each payee received a sum of money that was radically different to the amount sent. Individually, these avenues of attack could cause disruption, economic damage and loss of life. Together, they could lead to total societal collapse.

In this thesis, we contribute to the development of a new cryptographic ecosystem that will prevent such a catastrophe from taking place. In particular, we focus on quantum key distribution (QKD), with a pragmatic view towards how it will be used in the real world. While the main body of work is centred around techniques for resisting quantum attacks, there are also elements that will be of wider application within general quantum networks.

1.2 Thesis Outline

This thesis is structured as follows:

- **Chapter 2** contains general background information, beginning with modern cryptography, summarising symmetric protocols that remain secure in the presence of quantum computers and asymmetric protocols that do not. We then move to cover some of the main principles of quantum mechanics that underlie the security of the work described herein. Finally, we introduce the QKD protocols around which this thesis is primarily focused, and discuss a number of possible attack vectors.

- **Chapter 3** presents work done both in building the Bristol Quantum Network, and as part of implementing the first demonstration of time-division multiple access QKD. We describe the construction and characterisation of the first quantum-enabled software-defined network testbed, and quantify the advantages of a time-shared architecture by evaluating the number of links that each node can support. Finally, we present the first quantum-secured communication over the Bristol Quantum Network and discuss the second-generation testbed that is distributed across the city.

- **Chapter 4** justifies the previous chapter's choice to use a computationally-secure cipher as a basis for encrypting data. It explores the resource requirements for the classical QKD channel when a one-time pad is implemented, and contrasts this with the case where QKD is used to key computationally-secure encryption modes. The results are supported by a review of both classical and quantum bit rates in a range of scenarios.

- **Chapter 5** explores what happens if we accept the conclusion of chapter 4 (in everyday networks, contemporary ciphers will continue to dominate indefinitely) and relax the security of QKD in line with the encryption scheme being used. We develop a protocol that acts as a countermeasure to a new denial of service attack on QKD (identified from the results of chapter 3) and provide an initial exploration of how well it can withstand an eavesdropper.

- **Chapter 6** considers the wider impact of computationally-secure QKD, highlighting the circumstances in which it is preferable to alternatives. We build the first hybrid quantum/post-quantum network prototype, designed around these instances. We also demonstrate scenarios that reduce the trust placed in QKD intermediaries while introducing compatibility with legacy networks, and explore speed advantages that can be acquired when using QKD instead of post-quantum cryptography.

- **Chapter 7** closes this thesis with a summary of the work done as part of an initial demonstration of wavelength-division multiplexed QKD using integrated devices, which can augment the work of chapter 3 or increase secret key rates. Steps towards a monolithic experiment are also detailed, and early successes have included compressing the receiver chip and electronics

into a router-sized package that does not need to be mounted on an optical table. Finally, we present a series of designs for next-generation chip masks, all of which have now been fabricated by an external foundry.

CHAPTER 2

BACKGROUND

Declaration of Work

Parts of this chapter have previously appeared as background material in [7–9]. Where appropriate, some text has been reused, as it was originally written by me.

Here, we present the general background that is necessary to understand both the content of this thesis, and the motivations behind it. We focus on numerous aspects of modern cryptography, including the encryption and authentication schemes that will be used throughout, as well as the public-key cryptosystems that are widely utilised for distributing symmetric keys, but will be compromised by quantum computers.

Next, we outline the principles of quantum mechanics on which new forms of key distribution can be based, before segueing into quantum computing and reviewing the size of device required to break the cryptography described in the previous section. This can be used to inform estimates on the length of time available before replacement systems need to be fully adopted. We also include a general discussion of the different ways photonic quantum bits (qubits) can be realised, all of which will be used at various points in later chapters.

An introduction to quantum key distribution follows, along with a summary of the most relevant protocols. Finally, we explore a selection of physical vulnerabilities, as these will be a primary focus of the research presented herein.

2.1 Modern Cryptography

In this section, we will examine a range of constructs that are used to secure communications across public and private networks around the globe. When speaking with quantum scientists, these are often referred to as being part of "classical cryptography", because they sit firmly in the domain of classical physics. However, computer scientists consider classical cryptography to be comprised of algorithms such as the Caesar cipher [10], which are insecure and have fallen into disuse. Thus, to avoid confusion, we will adhere to their convention and refer to the algorithms of this section as being part of "modern cryptography". Elsewhere, we continue to identify technology according the type of physics by which it is governed (for example, "classical networks" and "classical computers"), with the exception of "post-quantum cryptography" in chapter 6. Once again, this is a name introduced by modern cryptographers, referring to public-key cryptosystems that continue to be secure in a world where quantum computers are a reality. Such terminology is slightly unfortunate in that it could be interpreted as referring to a successor to quantum cryptography, developed using post-quantum physics. Yet, because alternative names were not proposed before the term became widespread, we must abide by this convention also.

2.1.1 Symmetric-Key Encryption

Encryption is the oldest and most well-known form of cryptography. Here, we will cover the mathematically-unbreakable cipher that is often considered to be a leading application of the quantum key distribution (QKD) protocols in section 2.3.1. We will also give a high-level overview of the much-more-practical block cipher that is used in real life, along with the cryptosystems in which it can be implemented.

The Vernam Cipher and One-Time Pad

The one-time pad (OTP) was first invented by Frank Miller in 1882 [11]. Despite this, it was not until the turn of the 20th Century that it became possible to use his system for the automated encryption of electronic communications, when Vernam patented a method for implementing the exclusive-OR (XOR) operation [12]. In a cryptographic context, this is known as the Vernam cipher. Alice takes her message, m, and represents it as a sequence of bits, which can then be encrypted such that

$$c = m \oplus k \tag{2.1}$$

Here, c is the ciphertext, k is a random secret key and $\oplus$ stands for addition modulo 2 (see table 2.1). If Bob is also in possession of the key, then he can decrypt this using a second XOR, because

$$m = c \oplus k \tag{2.2}$$

If k is single-use, the Vernam cipher becomes an OTP, which has been proven secure even against adversaries with unlimited computational power [13]. Such a property is often referred to as

TABLE 2.1: Truth table for the XOR ($\oplus$) function, which is equivalent to performing addition modulo two with no carry. When this is implemented as part of a one-time pad, x and y correspond either to a single bit of plaintext and a single bit of key, or to a single bit of ciphertext and a single bit of key.

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

"unconditional" or "information-theoretic" security, which simply means there is no mathematical attack under which the system can be broken. However, it says nothing about physical vulnerabilities that may arise from a specific implementation, and any technique related to the exploitation of these is referred to as a side-channel attack.

The Advanced Encryption Standard

Unfortunately, even though the OTP provides the holy grail of security guarantees, it has only ever found use in niche applications [10]. This is because the length of the key must equal the length of the plaintext and, as current techniques for key distribution deliver data deterministically, it would be more efficient and no less secure if they were to directly transmit the message instead. Yet, as we will discover in section 2.1.3, these methods are still very slow, and so it would be preferable to use them alongside an encryption scheme that consumes less than one bit of key per bit of message.

Thus, for many years, we have relied on the use of block ciphers, the most prominent of which is the Advanced Encryption Standard (AES) [14]. This divides the plaintext up into a series of 128-bit blocks, treated hereafter like separate messages. Each block is encoded as a 4x4 byte-array, and a symmetric key of length 128, 192 or 256 bits is used to derive a set of so-called "round keys". The number derived is dependent on the size of the symmetric key, and this affects how many times each subsequent operation is invoked (i.e. how many rounds there are). The remainder of the algorithm is a combination of XORs between one of the round keys and the byte array, as well as S-box substitutions on each byte (see table 2.2), cyclic shifts of the last three rows of the array, and multiplications of each column by a pre-defined matrix.

However, using AES to directly encrypt a message is not secure. A perfect encryption scheme should have an output that appears random, as will be the case for the OTP when used with a maximally random key. Figure 2.1 shows AES generates ciphertexts that retain the structure of the plaintext so, to get around this, we must implement block ciphers using special modes of operation, which we now go on to discuss.

TABLE 2.2: S-box used in the Advanced Encryption Standard to perform byte-wise substitutions. In the example highlighted, the byte c9 maps to dd, both of which are expressed in hexidecimal. Based on figure 7 in [14].

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

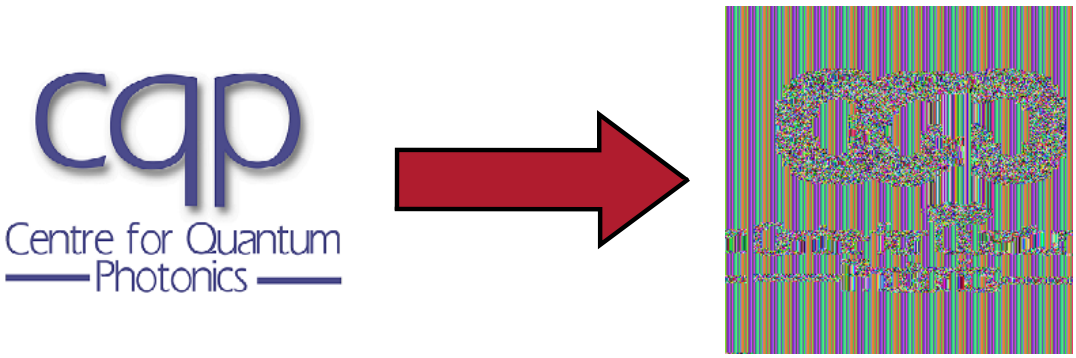


FIGURE 2.1: Demonstrating the effect of directly encrypting the Centre for Quantum Photonics logo with the Advanced Encryption Standard.

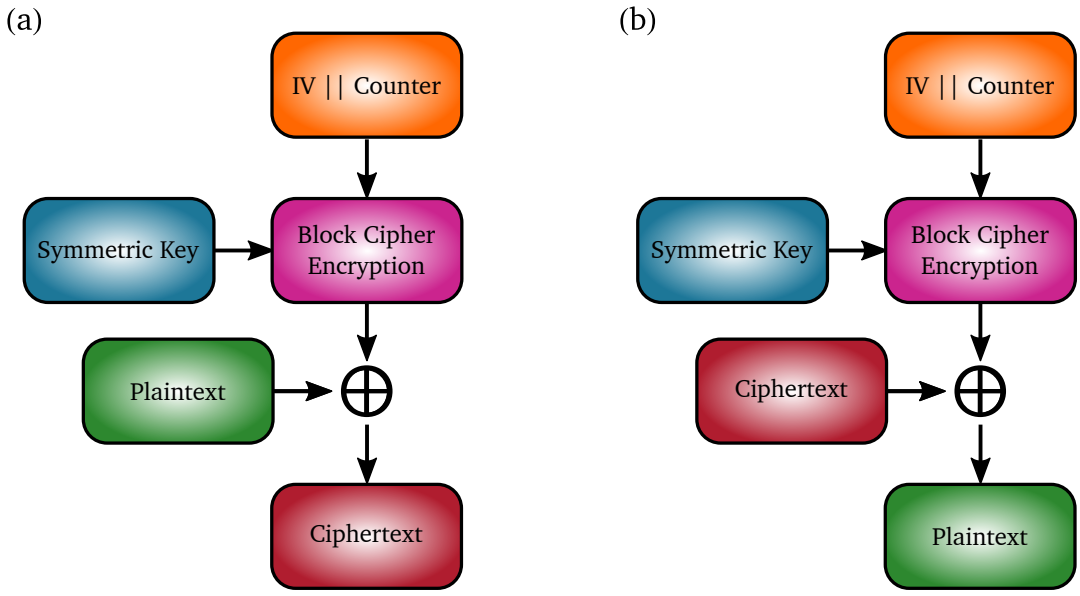


FIGURE 2.2: Illustrating (a) the encryption process and (b) the decryption process for a block cipher running in Counter Mode. IV||Counter represents the concatenation of a random initialisation vector with a counter that increments sequentially for each call to the block cipher.

Counter Mode (CTR)

Block ciphers running in Counter Mode [15] can be viewed as a computationally-secure approximation of the OTP. As depicted in figure 2.2, AES effectively expands a symmetric key, and the output is used to encrypt a message with the Vernam cipher. That is,

$$c = m \oplus \mathrm{AES}_k(\mathrm{IV}||\mathrm{Counter}) \tag{2.3}$$

and

$$m = c \oplus \mathrm{AES}_k(\mathrm{IV}||\mathrm{Counter}) \tag{2.4}$$

Such an approach is allowed under the condition that the input to the block cipher cannot be distinguished from random, as then there is no underlying structure capable of being exploited. The length of the counter affects the maximum number of times the Advanced Encryption Standard running in Counter Mode (AES-CTR) can be invoked with the same key. When this wraps around, the system becomes a two-time pad, and is therefore insecure. However, the counter length must be balanced off against the size of the initialisation vector, which is responsible for introducing the required randomness. In the case of AES, it is standard to define both as being 64 bits long [16].

Galois/Counter Mode (GCM)

The Advanced Encryption Standard running in Galois/Counter Mode (AES-GCM) [17] is an authenticated version of AES-CTR. As shown in figure 2.3, the encryption process remains unchanged,

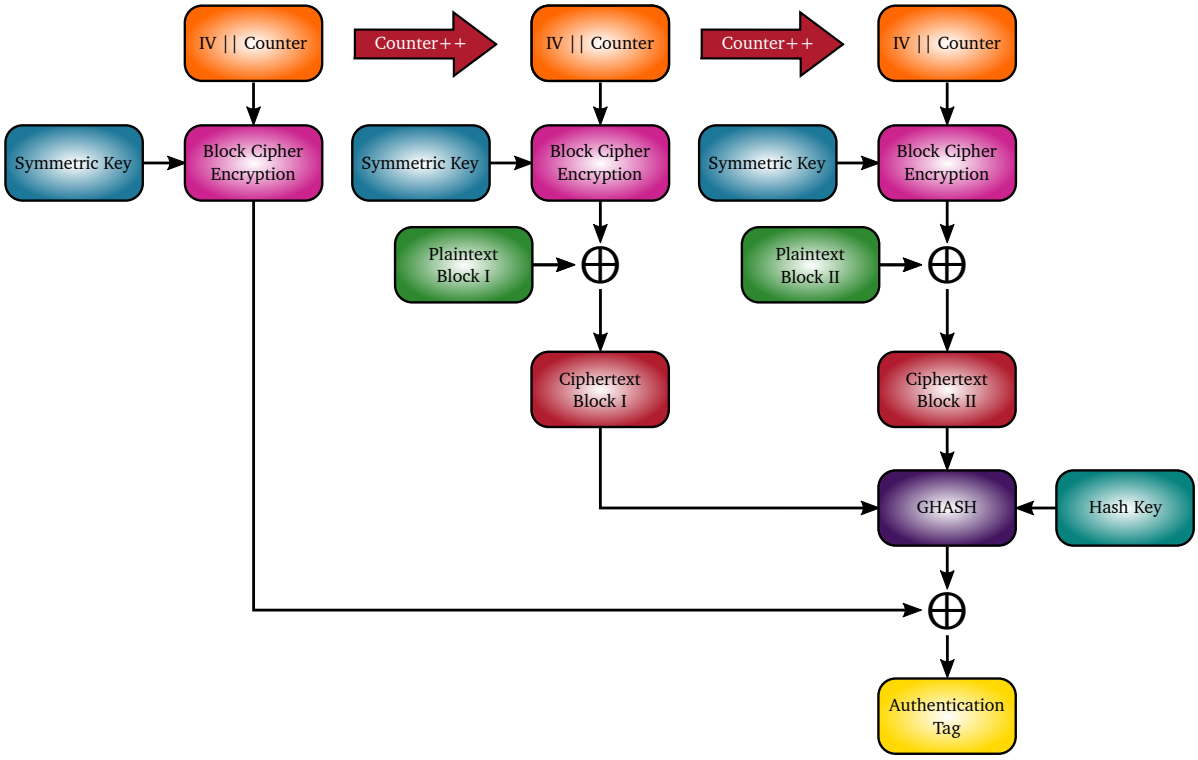


FIGURE 2.3: Illustrating the mechanisms used for encryption and authentication in Galois/Counter Mode. Here, we consider only two blocks of plaintext, however the protocol can be extended to encrypt messages of no more than $2^{39} - 256$ bits [18]. GHASH is a hash function that can also be used to authenticate any unencrypted data to which the ciphertext may be appended. IV||Counter represents the concatenation of a random initialisation vector with a counter, as in figure 2.2. Based on figure 1 in [17].

outputting ciphertexts based on the XOR of the plaintext with an enciphered initialisation vector, and using a counter to prevent repetition.

The authentication tag is based on a hash function known as GHASH, using a key that is derived by enciphering 128 zeroes with the block cipher and symmetric key from elsewhere in the protocol. This produces an output that is encrypted in the same way as the message, before being concatenated with the ciphertext and sent to Bob. On receipt, he can confirm authenticity by calculating an equivalent tag for the ciphertext in his possession. Decryption is then the same as in figure 2.2.

2.1.2 Symmetric-Key Authentication

Another way of symmetrically authenticating messages is to use a Wegman-Carter message authentication code (MAC) [19]. This has the advantage of being information-theoretically secure, and

takes the form

$$\tau = h_{k_{\mathrm{H}}}(m) \oplus k_{\mathrm{M}} \tag{2.5}$$

Here, h is a universal hash function keyed with k_{H}, m is the message to be authenticated and k_{M} is a one-time key used to mask the output of the hash. The authentication procedure goes as follows. Alice calculates a tag τ that corresponds to a message, and concatenates the two. She sends the result to Bob. who is also in possession of k_{H}, so can compute an equivalent τ for the message he received. So long as this matches the tag constructed by Alice, Bob can be confident that the information has not come from or been modified by a third party.

A set of hash functions is defined to be universal if the upper bound on the collision probability is equal to that for the case where authentication tags are randomly assigned. More specifically, if $\#\mathcal{H}_m$ is the cardinality of the set of hash function outputs then, for $m_1 \neq m_2$, [20]

$$\mathrm{Prob}\Big[h_{k_{\mathrm{H}}}(m_1) = h_{k_{\mathrm{H}}}(m_2)\Big] \leq \frac{1}{\#\mathcal{H}_m} \tag{2.6}$$

Many universal hash functions also have small differential probabilities. That is,

$$\mathrm{Prob}\Big[h_{k_{\mathrm{H}}}(m_1) = h_{k_{\mathrm{H}}}(m_2) + x\Big] \approx 0 \tag{2.7}$$

where x is an arbitrary bit string. We note that this is a slightly stronger condition than simply requiring there to be no collisions, which would correspond to the case where $x = 0$. To give an idea of exactly what we consider to be a small probability, we can consider the hash function used in Poly1305, for which [21]

$$\mathrm{Prob}\Big[h_{k_{\mathrm{H}}}(m_1) = h_{k_{\mathrm{H}}}(m_2) + x\Big] \leq \frac{8}{2^{106}}\left\lceil \frac{|m|_{\max}}{16} \right\rceil \tag{2.8}$$

assuming m_1 and m_2 are each no more than $|m|_{\max}$ bytes long.

Naturally, an attacker in possession of m and τ should not be able to obtain any information on $h_{k_{\mathrm{H}}}$. However, in the case where multiple messages are authenticated using the same hash function, then we have an additional condition: m_i, τ_i and m_{i+1} must reveal no information about τ_{i+1}. In order to fulfil such a requirement, we must mask the output of $h_{k_{\mathrm{H}}}$, and this is the reason for using k_{M} to encrypt $h_{k_{\mathrm{H}}}(m)$ in equation 2.5. Care must be taken to ensure that the raw output of the hash function is never transmitted in the clear, despite it sometimes being recommended for the initial round [22]. Failure to encrypt the first $h_{k_{\mathrm{H}}}(m)$ is equivalent to deterministically selecting a one-time key of all zeros, and it has been shown that this can be exploited to generate successful forgeries [23].

Finally, just as AES-CTR is a computationally-secure alternative to the OTP, there are also computationally-secure Wegman-Carter MACs, further details on which can be found in chapter 5.

2.1.3 Public-Key Cryptography for Symmetric-Key Distribution

There is, of course, still a missing part of the jigsaw. The above methods assume that, prior to running the encryption or authentication algorithm, Alice and Bob somehow managed to share a symmetric key, using an approach that was free from compromise. While such a task is trivial if the two parties can meet in person, it is more complex when they cannot.

The most popular solution is to protect the distribution of keys using mathematical problems that are presumed hard. This, known as public-key cryptography, was first invented by Ellis in 1970 [24], though as he was an employee of GCHQ, it remained classified, and key distribution over public channels was separately conceived by Merkle a few years later [25].

In this section, we will briefly summarise simplified versions of the most widely-used public-key cryptosystems. We note that while some of these are capable of encrypting data directly, it is more efficient to use them as a means for distributing symmetric keys that will then be used in encryption schemes like AES-GCM.

Diffie-Hellman Key Exchange

Diffie-Hellman key exchange was first published by its namesakes in 1976 [26], though this post-dated the work of Williamson [27], who invented it independently as part of a body of research that followed on from the initial work of Ellis, and remained classified for many years.

Protocol 2.1 presents Diffie-Hellman in its original form, the security of which relies on the assumption that, given V, a prime, and a, a primitive element of $\mathbb{Z}_V^*$, it is computationally hard to find k from $a^k \bmod V$. This is known as the discrete logarithm problem, where $\mathbb{Z}_V^*$ is the group of integers taken from the set $\{0, 1, \ldots, V-1\}$, and for which the greatest common divisor with V is 1. In practice, because we choose V to be prime, this makes $\mathbb{Z}_V^*$ the set of non-negative integers modulo V. If x is an arbitrary integer, a primitive element of $\mathbb{Z}_V^*$ is one from which any other element can be generated by calculating $a^x \bmod V$.

There are a number of Diffie-Hellman variants, including one based on elliptic curves [28]. This offers smaller key sizes than the original version, for the same classical security level, and so is the preferred option in everyday networks. However, if used exactly as presented here, all forms of Diffie-Hellman are vulnerable to attack. Since Alice and Bob do not authenticate one another, they have no way of knowing if their messages have been tampered with, and so naturally this can be exploited. We could get around the problem by using a Wegman-Carter MAC (see section 2.1.2), but this would require an initial shared secret to have previously been distributed. Therefore, it is more common to use the public-key equivalent, known as a digital signature. Although we will not go into full details here, such a scheme can be based on Rivest–Shamir–Adleman (RSA), an alternative method of key distribution that we explore next.

Protocol 2.1: Diffie-Hellman Key Exchange [26, 27, 29]

SUMMARY: Alice and Bob each select a bit string and transmit it to the other party, using the discrete logarithm problem to ensure secrecy against eavesdroppers. The bit strings are then combined to produce a single, symmetric key.

1. *One-Time Setup.*
   (a) Alice and Bob agree on a prime V.
   (b) Alice and Bob agree on a primitive element a of $\mathbb{Z}_V^*$. Here, $1 < a < V-1$ and $\mathbb{Z}_V^*$ is the multiplicative group of integers modulo V.
2. *Secret Generation.*
   a) Alice generates a random integer $1 \leq k_1 < V-1$.
   b) Bob generates a random integer $1 \leq k_2 < V-1$.
3. *Symmetric-Key Generation.*
   (a) Alice transmits $a^{k_1} \bmod V$.
   (b) Bob transmits $a^{k_2} \bmod V$.
   (c) The symmetric key is defined to be $a^{k_1 k_2} \bmod V$, which Alice can generate by computing $\left(a^{k_2}\right)^{k_1} \bmod V$, and Bob can generate by computing $\left(a^{k_1}\right)^{k_2} \bmod V$.

RSA

Like in the case of Diffie-Hellman, it was classified research that lead to the original discovery of RSA, this time by Cocks in 1973 [30]. Five years later, Rivest, Shamir and Adleman publicly described the same idea [31], summarised in protocols 2.2, 2.3 and 2.4. More explicitly, protocol 2.2 details the generation of an RSA public/private key pair, while protocols 2.3 and 2.4 give an example of how these can be used to ensure message confidentiality. The public key is made up of two numbers, one of which is a product of two primes. An eavesdropper with knowledge of said primes would be able to reconstruct the private key, so we must assume that it is computationally hard to decompose a large integer into two prime factors. Technically, the security of the scheme relies on the RSA problem [29], which is slightly more general than this, however integer factorisation is the most efficient attack that we know of, and is the way in which we will use quantum computers to break RSA.

As prime numbers are easy to check but hard to find, the quickest approach to key generation involves selecting a random number (constrained to exclude obvious non-primes), before applying a primality test, such as the example given in [32]. When using RSA for symmetric-key distribution, a transport algorithm known as a key encapsulation mechanism (KEM) [33] can offer advantages over the encryption presented here, as it avoids the need for padding. This will be explored further as part of chapter 6.

Once again, we have omitted the authentication steps, despite these being essential for security. Loosely speaking, an RSA digital signature can be implemented by hashing the information that we

Protocol 2.2: RSA Public/Private-Key Generation [30, 31]

SUMMARY: Alice creates a public/private key pair for use in protocols 2.3 and 2.4.

1. *Private Key.*
   (a) Alice generates two prime numbers V_1 and V_2, which should be distinct from one another and differ in length by no more than a few bits.
   (b) Alice computes $\Phi_1 = (V_1 - 1)(V_2 - 1)$.
   (c) Alice generates a random integer F_1, where $1 < F_1 < \Phi_1$ and $\gcd(F_1, \Phi_1) = 1$. Here, $\gcd(x, y)$ is used to indicate the greatest common divisor of x and y.
   (d) Alice computes F_2, where $1 < F_2 < \Phi_1$ and $F_1 F_2 \equiv 1 \bmod \Phi_1$.
   (e) The private key is defined to be F_2.
2. *Public Key.*
   (a) Alice computes $\Phi_2 = V_1 V_2$.
   (b) The public key is defined to be (Φ_2, F_1).

Protocol 2.3: RSA Encryption [30, 31]

SUMMARY: Bob uses Alice's public key from protocol 2.2 to encrypt a message. Secrecy against eavesdroppers is assured if the non-trivial factors of the public key cannot be found.

1. *Message Conversion.* Bob pads his message using a publicly-known scheme such as Optimal Asymmetric Encryption Padding [35]. The result is represented as an integer $0 \leq m < \Phi_2$.
2. *Message Encryption.* Bob transmits the ciphertext $c = m^{F_1} \bmod \Phi_2$.

Protocol 2.4: RSA Decryption [30, 31]

SUMMARY: Alice uses the private key from protocol 2.2 to decrypt Bob's message.

1. *Message Decryption.* Alice recovers the plaintext by computing $m = c^{F_2} \bmod \Phi_2$.
2. *Message Conversion.* Alice reverses the padding scheme to recover the original message.

wish to authenticate, before encrypting the output with a private key. The result can be decrypted by anyone in possession of the corresponding public key, meaning they can compare the hash of a message they received with one that is known to have been computed by Alice [29]. However, in practice, digital signatures cannot be generated simply by reversing the protocols given here, as a different padding scheme is required [34].

2.2 Quantum Information

We now move to cover the principles of quantum mechanics that underlie the work of this thesis, and discuss the effect of quantum computers on modern cryptography. We also provide a summary

of the most popular approaches for encoding information on quantum states of light.

2.2.1 Quantum Mechanics

Except where otherwise referenced, the following is based on information that can be found in [36] and [37], both of which provide a comprehensive summary for the less-experienced reader.

Quantum States

Any state of a quantum system can be described by a complex vector of appropriate dimension. A qubit is a two-level system used for information processing and, in this context, we can define $|\bar{0}\rangle$ (logical zero) and $|\bar{1}\rangle$ (logical one) using two-dimensional vectors, such that

$$|\bar{0}\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad , \quad |\bar{1}\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{2.9}$$

Together, these form a basis which, for our purposes, simply means that we can express any vector in $\mathbb{C}^2$ as a linear sum of $|\bar{0}\rangle$ and $|\bar{1}\rangle$. That is, any arbitrary qubit can be defined as

$$|\psi\rangle = x_0 |\bar{0}\rangle + x_1 |\bar{1}\rangle = \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} \tag{2.10}$$

where x_0 and x_1 are complex numbers. Similarly,

$$\langle\psi| = \langle\bar{0}| x_0^* + \langle\bar{1}| x_1^* = \begin{bmatrix} x_0^* & x_1^* \end{bmatrix} \tag{2.11}$$

and we refer to $\{|\bar{0}\rangle, |\bar{1}\rangle\}$ as the Z basis. Throughout this thesis, the X basis will also be used, defined by $\{|+\rangle, |-\rangle\}$. The $|+\rangle$ and $|-\rangle$ states are superpositions of $|\bar{0}\rangle$ and $|\bar{1}\rangle$, which we express mathematically as follows:

$$|+\rangle = \frac{|\bar{0}\rangle + |\bar{1}\rangle}{\sqrt{2}} \quad , \quad |-\rangle = \frac{|\bar{0}\rangle - |\bar{1}\rangle}{\sqrt{2}} \tag{2.12}$$

We can take the inner product $\langle\psi|\phi\rangle$ of two arbitrary, normalised states, where

$$\langle\psi|\phi\rangle = \langle\phi|\psi\rangle^* = \begin{cases} 0, & \text{for } |\phi\rangle \equiv |\psi^\perp\rangle \\ 1, & \text{for } |\phi\rangle \equiv |\psi\rangle \end{cases} \tag{2.13}$$

$|\psi^\perp\rangle$ is the state that is orthogonal to $|\psi\rangle$, so it can be seen that $|\bar{0}\rangle$ and $|\bar{1}\rangle$ are orthogonal to one another, as are $|+\rangle$ and $|-\rangle$. However, neither $|\bar{0}\rangle$ nor $|\bar{1}\rangle$ are orthogonal to $|+\rangle$ or $|-\rangle$, the significance of which will become apparent as we progress through this chapter.

It is possible to evolve a quantum state through application of an operator, $\hat{O}$, meaning

$$\begin{aligned} |\psi\rangle &= \hat{O}\,|\phi\rangle \\ \langle\psi| &= \langle\phi|\,\hat{O}^\dagger \end{aligned} \tag{2.14}$$

For qubits,

$$\begin{aligned}\hat{O} &= x_{0,0}\left|\overline{0}\right\rangle\left\langle\overline{0}\right| + x_{0,1}\left|\overline{0}\right\rangle\left\langle\overline{1}\right| + x_{1,0}\left|\overline{1}\right\rangle\left\langle\overline{0}\right| + x_{1,1}\left|\overline{1}\right\rangle\left\langle\overline{1}\right| &&= \begin{bmatrix} x_{0,0} & x_{0,1} \\ x_{1,0} & x_{1,1} \end{bmatrix} \\ \hat{O}^{\dagger} &= x^{*}_{0,0}\left|\overline{0}\right\rangle\left\langle\overline{0}\right| + x^{*}_{0,1}\left|\overline{1}\right\rangle\left\langle\overline{0}\right| + x^{*}_{1,0}\left|\overline{0}\right\rangle\left\langle\overline{1}\right| + x^{*}_{1,1}\left|\overline{1}\right\rangle\left\langle\overline{1}\right| &&= \begin{bmatrix} x^{*}_{0,0} & x^{*}_{1,0} \\ x^{*}_{0,1} & x^{*}_{1,1} \end{bmatrix}\end{aligned} \tag{2.15}$$

taking care to note that $|\psi\rangle\langle\phi|$ represents the outer product of $|\psi\rangle$ and $\langle\phi|$. A particularly significant set of operators is that defined by the Pauli matrices

$$\hat{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad , \quad \hat{Y} = \begin{bmatrix} 0 & -\mathbb{i} \\ \mathbb{i} & 0 \end{bmatrix} \quad , \quad \hat{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{2.16}$$

from which the etymology of the X and Z bases becomes clear, as they are the eigenbases of $\hat{X}$ and $\hat{Z}$ respectively. Finally, an operator $\hat{U}$ is referred to as being unitary if

$$\hat{U}^{\dagger}\hat{U} = \hat{\mathbb{1}} \tag{2.17}$$

where $\hat{\mathbb{1}}$ is the identity operator, i.e.

$$\hat{\mathbb{1}} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{2.18}$$

Together with the Pauli matrices, equation 2.18 can be used to create a basis into which all $\mathbb{C}^2$ operators can be decomposed.

Measurement

Two quantum states can only be reliably distinguished by measurement if they are orthogonal to one another. We show this using similar techniques to the proof by contradiction in [37], though to different effect. For each possible measurement outcome i, we can define an operator

$$\hat{M}_i = |\psi_i\rangle\langle\psi_i| \tag{2.19}$$

If the system is initially in the state $|\phi\rangle$,

$$\text{Prob}\,(\text{Outcome } i) = \langle\phi|\hat{M}_i^{\dagger}\hat{M}_i|\phi\rangle \tag{2.20}$$

and, naturally,

$$\sum_i \text{Prob}\,(\text{Outcome } i) = 1 \tag{2.21}$$

If we are to deterministically distinguish between $|\phi_1\rangle$ and $|\phi_2\rangle$ then, based on equation 2.20, we require

$$\begin{aligned}\langle\phi_1|\hat{M}_1^{\dagger}\hat{M}_1|\phi_1\rangle = 1 \\ \langle\phi_2|\hat{M}_2^{\dagger}\hat{M}_2|\phi_2\rangle = 1\end{aligned} \tag{2.22}$$

In order to fulfil equation 2.21, this means

$$\langle\phi_1|\hat{M}_2^\dagger\hat{M}_2|\phi_1\rangle = 0 \tag{2.23}$$

Now,

$$\hat{M}_i^\dagger\hat{M}_i = |\psi_i\rangle\langle\psi_i|\psi_i\rangle\langle\psi_i| = |\psi_i\rangle\langle\psi_i| \tag{2.24}$$

and so equation 2.23 becomes

$$\langle\phi_1|\psi_2\rangle\langle\psi_2|\phi_1\rangle = 0 \tag{2.25}$$

Thus,

$$\langle\phi_1|\psi_2\rangle = \langle\psi_2|\phi_1\rangle = 0 \tag{2.26}$$

Next, $|\phi_2\rangle$ can be expressed using the basis $\left\{|\phi_1\rangle, |\phi_1^\perp\rangle\right\}$ such that

$$|\phi_2\rangle = x|\phi_1\rangle + y|\phi_1^\perp\rangle \tag{2.27}$$

where $|x|^2 + |y|^2 = 1$ and $\langle\phi_1|\phi_1^\perp\rangle = 0$. This means that, given equation 2.22,

$$\begin{aligned} 1 &= \left(\langle\phi_1|x^* + \langle\phi_1^\perp|y^*\right)|\psi_2\rangle\langle\psi_2|\left(x|\phi_1\rangle + y|\phi_1^\perp\rangle\right) \\ &= |x|^2\langle\phi_1|\psi_2\rangle\langle\psi_2|\phi_1\rangle + xy^*\langle\phi_1^\perp|\psi_2\rangle\langle\psi_2|\phi_1\rangle \\ &\quad + x^*y\langle\phi_1|\psi_2\rangle\langle\psi_2|\phi_1^\perp\rangle + |y|^2\langle\phi_1^\perp|\psi_2\rangle\langle\psi_2|\phi_1^\perp\rangle \end{aligned} \tag{2.28}$$

From equation 2.26, we know that the first three terms are 0, and that $|\psi_2\rangle = |\phi_1^\perp\rangle$. Therefore,

$$|y|^2 = 1 \tag{2.29}$$

If equation 2.22 is true then, as a consequence of the fact that $|x|^2$ and $|y|^2$ must sum to 1, $|\phi_2\rangle = |\phi_1^\perp\rangle$. In other words, two states can only be reliably distinguished if they are orthogonal to one another. This does not mean that we are unable to distinguish non-orthogonal states, just that we cannot do so with certainty. For example, if $|\phi_1\rangle = |\overline{0}\rangle$ and $|\phi_2\rangle = |+\rangle$, then we can take advantage of the fact that measuring an X-basis state in the Z basis, and vice versa, will return a random result. As we show in section 2.3.2, measuring $|+\rangle$ with the set of operators

$$\mathcal{M}_Z = \left\{|\overline{0}\rangle\langle\overline{0}|, |\overline{1}\rangle\langle\overline{1}|\right\} \tag{2.30}$$

will produce an outcome corresponding to either $|\overline{0}\rangle$ or $|\overline{1}\rangle$, each with probability $\frac{1}{2}$. The latter of these measurement results would be impossible had we been given $|\phi_1\rangle$ so, assuming there is an equal chance of the system being in either state, this allows us to distinguish $|\phi_2\rangle$ from $|\phi_1\rangle$ with 25% probability.

No-Cloning Theorem

In addition to the restrictions on quantum measurement that are described above, the work of this thesis will rely on the fact that it is physically impossible to construct a general machine for producing perfect copies of two or more distinct, non-orthogonal quantum states. This non-orthogonality condition is made clearest by the proof in [38], so it is that which we will present here. Alternatively, one could consider the approach from [39, 40], as it has the benefit of being generalisable to any arbitrary quantum operation through introduction of an ancilla [41].

Suppose we have two arbitrary quantum states, $|\psi\rangle$ and $|\phi\rangle$, plus a unitary cloning operator $\hat{C}$ that converts a "blank" state $|\chi\rangle$ into a copy of $|\psi\rangle$ or $|\phi\rangle$. That is,

$$\begin{aligned} \hat{C}\,|\psi\rangle\,|\chi\rangle &= |\psi\rangle\,|\psi\rangle \\ \hat{C}\,|\phi\rangle\,|\chi\rangle &= |\phi\rangle\,|\phi\rangle \end{aligned} \tag{2.31}$$

where $|\psi\rangle \neq |\phi\rangle$. From the above, we can construct the following expression:

$$\langle\chi|\,\langle\psi|\,\hat{C}^{\dagger}\hat{C}\,|\phi\rangle\,|\chi\rangle = \langle\psi|\,\langle\psi|\phi\rangle\,|\phi\rangle \tag{2.32}$$

Recall that evaluating the inner product of two states returns a number, and so, by taking advantage of the unitary property described in equation 2.17, we can simplify equation 2.32 to find

$$\langle\psi|\phi\rangle = (\langle\psi|\phi\rangle)^2 \tag{2.33}$$

Since $\langle\psi|\phi\rangle = 1$ requires that $|\psi\rangle = |\phi\rangle$, then the only valid solution is $\langle\psi|\phi\rangle = 0$, which means the states must be orthogonal (see equation 2.13). Hence, it is impossible to construct a general device capable of perfectly and deterministically cloning any quantum state.

Unambiguous State Discrimination

Finally, while we cannot obtain full information on a system by cloning or measuring unknown states from a non-orthogonal set, a third approach still remains. Under certain conditions, it is possible to perform unambiguous state discrimination, with a chance that the result will be inconclusive. As indicated, "unambiguous" is not used to mean that none of the measurement outcomes have ambiguity. Instead, from the measurement outcome we receive, there is no ambiguity as to whether or not we can work out which state the system was originally in. The example we give here is taken from [42] and applies to two non-orthogonal quantum states of the kind that may be realised using single photons. This has been chosen because it nicely illustrates a way in which unambiguous state discrimination can be performed, without becoming overly complex. Other approaches are set out in [43] and [44]; these will be of relevance in chapters 5 and 7 respectively.

Consider the situation where we have in our possession a single copy of an unknown quantum state, defined to be either $|\psi\rangle$ or $|\phi\rangle$, which can be expressed in the $\{|\chi_1\rangle, |\chi_2\rangle\}$ basis such that

$$
\begin{aligned}
|\psi\rangle &= \frac{1}{\sqrt{2}}\left(\cos\frac{\Lambda}{2}+\sin\frac{\Lambda}{2}\right)|\chi_1\rangle+\frac{1}{\sqrt{2}}\left(\cos\frac{\Lambda}{2}-\sin\frac{\Lambda}{2}\right)|\chi_2\rangle \\
|\phi\rangle &= \frac{1}{\sqrt{2}}\left(\cos\frac{\Lambda}{2}-\sin\frac{\Lambda}{2}\right)|\chi_1\rangle+\frac{1}{\sqrt{2}}\left(\cos\frac{\Lambda}{2}+\sin\frac{\Lambda}{2}\right)|\chi_2\rangle
\end{aligned}
\tag{2.34}
$$

It is important to note that these may be viewed as qutrits with an unoccupied third level, $|\chi_3\rangle$, where $\langle\chi_1|\chi_3\rangle = \langle\chi_2|\chi_3\rangle = 0$. From the output states in [42], we can derive the unitary

$$
\hat{U} = \begin{bmatrix}
\frac{1}{2}(\cos\theta+1) & \frac{1}{2}(\cos\theta-1) & -\frac{1}{\sqrt{2}}\sin\theta \\
\frac{1}{2}(\cos\theta-1) & \frac{1}{2}(\cos\theta+1) & \frac{1}{\sqrt{2}}\sin\theta \\
\frac{1}{\sqrt{2}}\sin\theta & \frac{1}{\sqrt{2}}\sin\theta & \cos\theta
\end{bmatrix}
\tag{2.35}
$$

which is written in the $\{|\chi_1\rangle, |\chi_2\rangle, |\chi_3\rangle\}$ basis, meaning that it can be used to populate the third level of the "qutrit", rotating $|\psi\rangle$ and $|\phi\rangle$ out of a two-dimensional Hilbert space and into a three-dimensional one. As a result, if we set $\cos\theta = \tan\frac{\Lambda}{2}$, then implementing $\hat{U}$ on $|\psi\rangle$ and $|\phi\rangle$ leaves us with

$$
\begin{aligned}
|\psi\rangle' &= \sqrt{2}\sin\frac{\Lambda}{2}|\chi_1\rangle+\sqrt{\cos\Lambda}\,|\chi_3\rangle \\
|\phi\rangle' &= \sqrt{2}\sin\frac{\Lambda}{2}|\chi_2\rangle+\sqrt{\cos\Lambda}\,|\chi_3\rangle
\end{aligned}
\tag{2.36}
$$

The $|\chi_1\rangle$ and $|\chi_2\rangle$ terms are unique to $|\psi\rangle'$ and $|\phi\rangle'$ respectively. Therefore, we can try to establish whether the initial state was $|\psi\rangle$ or $|\phi\rangle$ by applying the set of measurement operators

$$
\mathcal{M}_\chi = \left\{|\chi_1\rangle\langle\chi_1|, |\chi_2\rangle\langle\chi_2|, |\chi_3\rangle\langle\chi_3|\right\}
\tag{2.37}
$$

The success probabilities are

$$
\begin{aligned}
\text{Prob}\big(|?\rangle \to |\psi\rangle\big) &= 2\sin^2\frac{\Lambda}{2} \\
\text{Prob}\big(|?\rangle \to |\phi\rangle\big) &= 2\sin^2\frac{\Lambda}{2}
\end{aligned}
\tag{2.38}
$$

where one should be careful to observe that $2\sin^2\frac{\Lambda}{2} = 1-\cos\Lambda$. As a $|\chi_3\rangle$ term is present in both $|\psi\rangle'$ and $|\phi\rangle'$, there is a chance we will be unable to identify the original state, given by

$$
\text{Prob}\big(|?\rangle \to |?\rangle\big) = \cos\Lambda
\tag{2.39}
$$

Thus, it is clear that discriminating between non-orthogonal states is possible, and it will be evident from the measurement outcome if the procedure fails.

2.2.2 Quantum Computing

Quantum computers are famed for their ability to efficiently solve mathematical problems that are intractable on normal computers, made possible by their ability to implement algorithms that take

advantage of the superposition states already discussed. In this context, quantum operations are often referred to as logic gates (see appendix A), and only a specific few of these must be directly, physically implementable, because this subset can then be used to approximate all others.

While we do not wish to delve into all the intricacies of complexity classes here, a rudimentary understanding will be helpful in chapter 6. With respect to figure 2.4, P is the set of decision problems (i.e. questions with a yes/no answer) that are solvable in polynomial time with a deterministic Turing machine (an abstraction of a classical computer that can be used to simulate any algorithm). Similarly, PSPACE is the set of decision problems that are solvable in polynomial space. NP is the set of decision problems solvable in polynomial time with a non-deterministic Turing machine, although its deterministic counterpart can verify any solution in polynomial time also [45]. The factoring decision problem on which RSA relies is widely believed to be in NP [37], however the fact that this can be solved using a quantum algorithm does not necessarily mean a quantum computer can be represented as a non-determistic Turing machine. An algorithm capable of solving an NP-complete problem in polynomial time can be repurposed to solve any NP problem in polynomial time, and it is known that there are no general approaches by which a quantum computer can efficiently solve problems that are NP-complete [46]. Such a statement does not rule out algorithms that require specific knowledge of the problem, however it is nonetheless speculated that BQP, the set of decision problems solvable by a quantum Turing machine in polynomial time with a bounded probability of error, does not contain all of NP [37].

To summarise, it is known that $\mathsf{P} \subseteq \mathsf{BQP} \subseteq \mathsf{PSPACE}$ and $\mathsf{P} \subseteq \mathsf{NP} \subseteq \mathsf{PSPACE}$ [37]. It is not known that $\mathsf{P} \neq \mathsf{NP}$ and $\mathsf{NP} \not\subseteq \mathsf{BQP}$, though these relations are assumed.

Quantum Attacks on Modern Cryptography

As we have already indicated, there are a number of ways in which quantum computers can be used to attack both the public- and symmetric-key cryptography outlined in section 2.1. Our current methods of key distribution (RSA, Diffie-Hellman and techniques based on elliptic curves) will all be fatally compromised by Shor's algorithm, which can perform integer factorisation or evaluate discrete logarithms in polynomial time [47]. Systems that rely on symmetric keys will not be fundamentally broken, however their security parameters need to be adjusted, because Grover's algorithm can speed up brute-force attacks. Given a key space of size $\#\mathcal{K}$, the number of steps required to identify the correct key is only $\mathcal{O}\left(\sqrt{\#\mathcal{K}}\right)$ [48], compared to $\mathcal{O}\left(\#\mathcal{K}\right)$ classically.

Table 2.3 summarises the above, quantifying the impact that quantum computing will have on some of the most widely-used pieces of cryptography, and gives quantum resource estimates in each case. These values should be taken only as a rough indicator, because trade-offs can often be made between spatial and temporal resources [49].

To estimate the classical security of RSA, we use the complexity of the General Number Field Sieve [50], as this is the fastest known algorithm for factoring large integers on a conventional computer. The National Institute of Standards and Technology (NIST) appears to round the resulting

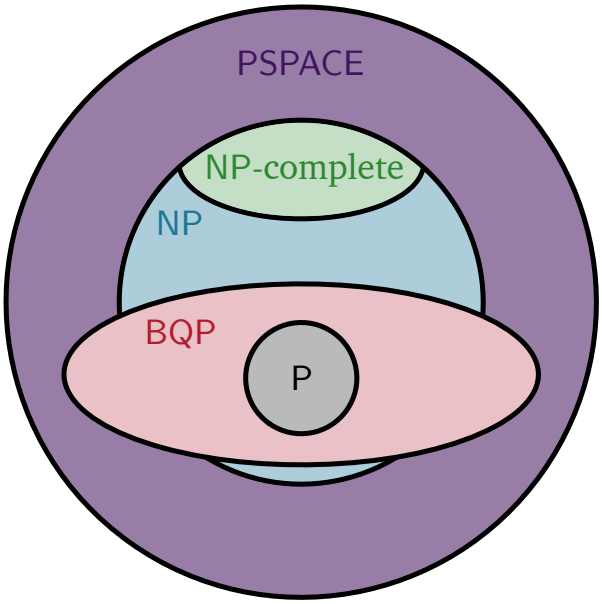


FIGURE 2.4: Hypothesised relationship between the polynomial time (P), bounded-error quantum polynomial time (BQP), non-deterministic polynomial time (NP) and polynomial space (PSPACE) complexity classes. Based on figure 1.21 in [37].

values down to the nearest symmetric-key security strength in their key management recommendations [51], for ease of comparison between disparate elements of larger systems.

We also consider the effect that quantum computers will have on elliptic curves. With regards to notation, ECC (P-256) is used to mean elliptic-curve cryptography with the NIST-approved 256-bit curve P-256 [28]. It is said that an x-bit curve has $\frac{x}{2}$ bits of classical security, based on the complexity of Pollard's rho algorithm [52], which is the joint-fastest approach to calculating discrete logarithms.

Finally, classical security for symmetric-key cryptography comes directly from the size of the key, as a brute-force search is the most effective attack if the system is otherwise considered secure. We note that while Secure Hash Algorithm 256 (SHA-256) has a 128-bit quantum security level, and so is still considered safe, we use Secure Hash Algorithm 512 (SHA-512) herein. This is because it has been shown that pre-processing can improve the effectiveness of a quantum search in certain situations [53], meaning it pays to be conservative with parameter choices in case there are any unforeseen techniques that could accelerate the attacks in our table.

While all the quantum resource estimates come from the references cited by this thesis, directly comparing them allows us to highlight some interesting points. First, as noted in [54], we can see that, for a pre-defined security level, it is easier to break elliptic-curve cryptosystems with a quantum computer than it is to break RSA. However, less intuitively, fewer qubits are required to brute force AES with 128-bit keys than are needed to break RSA-2048 and above. Therefore, while quantum security research quite rightly tends to focus on making key distribution capable of resisting quantum attacks, it is important that the urgency of upgrading to 256-bit keys is not

overlooked. RSA-1024 is now considered obsolete [55] so, with regard to the number of qubits required to compromise encrypted data, AES-128 is currently the weakest link in many modern systems.

2.2.3 Photonic Quantum Bits

There are a number of platforms on which qubits can be physically implemented, including but not limited to trapped ions, superconducting circuits and nitrogen-vacancy centres. Given this thesis focuses on quantum communications, we are fundamentally restricted to choosing some form of flying qubit. Of the options available, photons interact the least with their surrounding environment and so offer the easiest approach to building maximally-isolated quantum systems, as we require. Although typical wavelengths vary depending on the application, our work primarily targets networks constructed from optical fibres, meaning it is important to occupy an area of the spectrum that corresponds to a local minimum in the silica loss profile [60]. As a result, we will use 1310 nm and 1550 nm qubits in the chapters that follow, a choice which is supported by the availability of low-noise single-photon detectors at those wavelengths.

Mathematically, we can represent a γ-photon number state as $|\gamma\rangle$. Here, the following relations apply [61]

$$\begin{aligned} \hat{a}\,|\gamma\rangle &= \sqrt{\gamma}\,|\gamma-1\rangle \\ \hat{a}^\dagger\,|\gamma\rangle &= \sqrt{\gamma+1}\,|\gamma+1\rangle \end{aligned} \tag{2.40}$$

where $\hat{a}^\dagger$ and $\hat{a}$ are the creation and annihilation operators respectively, a pair of which exists for each mode of the field. When considering only a single mode, these obey the commutation relation

$$\left[\hat{a},\hat{a}^\dagger\right] = \hat{a}\hat{a}^\dagger - \hat{a}^\dagger\hat{a} = \hat{\mathbb{1}} \tag{2.41}$$

Therefore, given equation 2.40, we can define the zero-photon number state, $|0\rangle$, and one-photon number state, $|1\rangle$, as

$$|0\rangle = \hat{a}\,|1\rangle \quad , \quad |1\rangle = \hat{a}^\dagger\,|0\rangle \tag{2.42}$$

This section will explore the different degrees of freedom that can be used to encode logical qubits onto single photons. Some use the value of γ at different points in space or time to represent $|\overline{0}\rangle$ and $|\overline{1}\rangle$, while others simply require that $\gamma \equiv 1$. However, experimentally, a deterministic single-photon source is difficult to achieve and so, with this in mind, we close with a discussion on coherent states, which can be used when perfect number states are not available.

Polarisation-Encoded Single Photons

Just like classical light, single photons can be vertically or horizontally polarised. However, if we introduce a diagonal filter to the light path, immediately followed by a detector, there cannot simply be a halving of the intensity, as we would observe if the single-photon source were to be replaced

TABLE 2.3: Quantum resource estimates for attacking modern cryptography.

Cryptosystem	Quantum Algorithm	Number of Logical Qubits	Number of Gates	Circuit Depth	Classical/Quantum Security (bits)	Reference
RSA-1024	Shor's	2050	1.06×2^{39} (∗)	1.25×2^{37} (∗)	86/☠	[54, 56, 57]
RSA-2048	Shor's	4098	1.18×2^{42} (∗)	1.25×2^{40} (∗)	116/☠	[54, 56, 57]
RSA-3072	Shor's	6146	1.06×2^{44} (∗)	1.05×2^{42} (∗)	138/☠	[54, 56, 57]
RSA-4096	Shor's	8194	1.31×2^{45} (∗)	1.25×2^{43} (∗)	156/☠	[54, 56, 57]
ECC (P-224)	Shor's	2042	1.23×2^{36} (∗)	1.12×2^{36} (∗)	112/☠	[54]
ECC (P-256)	Shor's	2330	1.83×2^{36} (∗)	1.69×2^{36} (∗)	128/☠	[54]
ECC (P-384)	Shor's	3484	1.64×2^{38} (∗)	1.51×2^{38} (∗)	192/☠	[54]
ECC (P-521)	Shor's	4719	1.04×2^{40} (∗)	1.91×2^{39} (∗)	256/☠	[54]
AES-128	Grover's	2953	1.19×2^{86} (†) 1.55×2^{86} (‡)	1.06×2^{80} (†) 1.26×2^{80} (‡)	128/64	[58]
AES-192	Grover's	4449	1.81×2^{118} (†) 1.17×2^{119} (‡)	1.21×2^{112} (†) 1.45×2^{112} (‡)	192/96	[58]
AES-256	Grover's	6681	1.41×2^{151} (†) 1.83×2^{151} (‡)	1.44×2^{144} (†) 1.70×2^{144} (‡)	256/128	[58]
SHA-256	Grover's	2402	1.42×2^{146} (†) 1.64×2^{150} (‡)	1.69×2^{144} (†) Not Given (‡)	256/128	[59]
SHA3-256	Grover's	3200	1.52×2^{147} (†) 1.61×2^{153} (‡)	1.33×2^{137} (†) Not Given (‡)	256/128	[59]

Key: (∗) = CCNOT gates; (†) = T gates; (‡) = Clifford gates; ☠ = Broken.

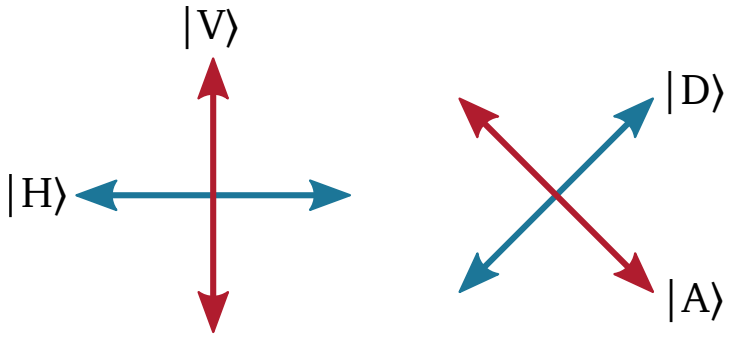


FIGURE 2.5: The four polarisation states $|H\rangle$, $|V\rangle$, $|D\rangle$ and $|A\rangle$. These can be used to represent the logical qubits $|\bar{0}\rangle$, $|\bar{1}\rangle$, $|+\rangle$ and $|-\rangle$.

with a laser. What we find instead is that this measurement process obeys the rules of quantum mechanics where, as illustrated in figure 2.5, the horizontal, vertical, diagonal and anti-diagonal polarisations are represented by the quantum states $|H\rangle$, $|V\rangle$, $|D\rangle$ and $|A\rangle$. Mathematically,

$$|D\rangle = \frac{|H\rangle + |V\rangle}{\sqrt{2}} \quad , \quad |A\rangle = \frac{|H\rangle - |V\rangle}{\sqrt{2}} \tag{2.43}$$

with $\{|H\rangle, |V\rangle\}$ and $\{|D\rangle, |A\rangle\}$ defined to be the rectilinear and diagonal bases respectively. Quantum operations can be implemented using waveplates, which introduce an arbitrary phase, thereby rotating the polarisation. Hence, it is easy to see that we can encode logical qubits such that

$$|\bar{0}\rangle \doteq |H\rangle \quad , \quad |\bar{1}\rangle \doteq |V\rangle \quad , \quad |+\rangle \doteq |D\rangle \quad , \quad |-\rangle \doteq |A\rangle \tag{2.44}$$

Mode-Encoded Single Photons

An alternate approach is to use the spatial modes of the photon in a scheme known as dual-rail encoding. Here, we consider two light paths, commonly implemented using on-chip waveguides (see chapter 7), as these provide high levels of control over the relative path length. As shown in figure 2.6, a photon in the lower rail is said to be in the number state $|0\rangle_{\text{upper}}|1\rangle_{\text{lower}} = |01\rangle$, and a photon in the upper rail is in $|1\rangle_{\text{upper}}|0\rangle_{\text{lower}} = |10\rangle$.

A beam splitter can be used to put the photon into the superposition $\frac{|01\rangle+|10\rangle}{\sqrt{2}}$ and, if we introduce a phase modulator, we can also generate $\frac{|01\rangle-|10\rangle}{\sqrt{2}}$. More generally, a Mach-Zehnder interferometer (see section 7.1.3) can be used to implement arbitrary qubit rotations. Therefore, it is once again easy to see that we can use dual-rail devices to implement logical qubits, where

$$|\bar{0}\rangle \doteq |01\rangle \quad , \quad |\bar{1}\rangle \doteq |10\rangle \quad , \quad |+\rangle \doteq \frac{|01\rangle + |10\rangle}{\sqrt{2}} \quad , \quad |-\rangle \doteq \frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{2.45}$$

We note that the photon-number representations of $|+\rangle$ and $|-\rangle$ are inseparable (or Bell states, to be even more precise), meaning superposition of a single photon over two modes is mathematically equivalent to the modes becoming entangled with one another.

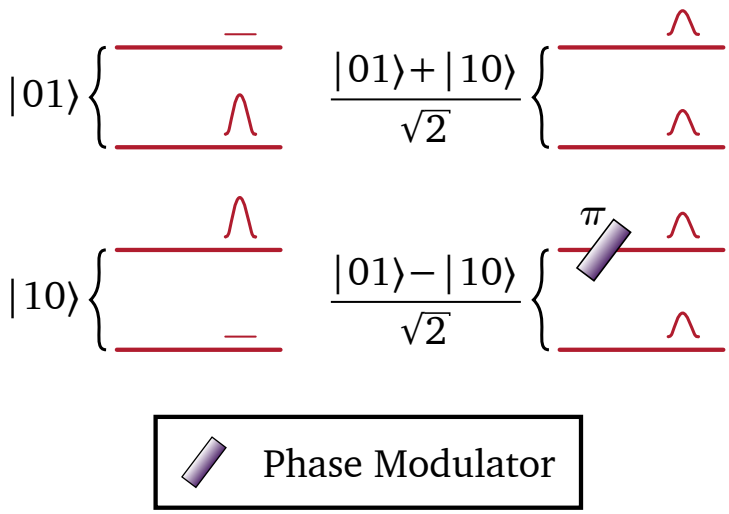


FIGURE 2.6: The four dual-rail states used to represent the logical qubits $|\bar{0}\rangle$, $|\bar{1}\rangle$, $|+\rangle$ and $|-\rangle$.

Time-Bin-Encoded Single Photons

A third method of encoding was originally proposed in [62], where each logical qubit is defined over a pair of time bins. In this work, we will use a scheme that also includes an empty bin at the end, meaning $|t_1\rangle = |1\rangle_{\text{early}} |0\rangle_{\text{late}} |0\rangle_{\text{empty}}$ and $|t_2\rangle = |0\rangle_{\text{early}} |1\rangle_{\text{late}} |0\rangle_{\text{empty}}$. If the final time bin were to contain a photon, we could expand our notation such that $|t_3\rangle = |0\rangle_{\text{early}} |0\rangle_{\text{late}} |1\rangle_{\text{empty}}$, although this is not used in the formation of logical qubits, which can be expressed as

$$|\bar{0}\rangle \doteq |t_1\rangle \quad , \quad |\bar{1}\rangle \doteq |t_2\rangle \quad , \quad |+\rangle \doteq \frac{|t_1\rangle + |t_2\rangle}{\sqrt{2}} \quad , \quad |-\rangle \doteq \frac{|t_1\rangle - |t_2\rangle}{\sqrt{2}} \tag{2.46}$$

The states in equation 2.46 may be prepared using the setup shown in figure 2.7. Assuming the photons are path-encoded when they enter Alice, the asymmetry between the two rails means that the $|10\rangle$ component will reach Alice's beam splitter after $|01\rangle$. More precisely, if both components begin in the early time bin, and the delay line is of the correct length, then for the upper arm (mode 1),

$$\hat{a}_{t_1,1} \xrightarrow{\text{Delay}} \hat{a}_{t_2,1} \tag{2.47}$$

while for the lower arm (mode 2),

$$\hat{a}_{t_1,2} \xrightarrow{\text{Delay}} \hat{a}_{t_1,2} \tag{2.48}$$

Consequently, if we have a superposition in space, it can be converted to a superposition in time, where

$$\frac{|01\rangle + e^{\mathrm{i}\theta} |10\rangle}{\sqrt{2}} \rightarrow \frac{|t_1\rangle + e^{\mathrm{i}\theta} |t_2\rangle}{\sqrt{2}} \tag{2.49}$$

To rotate the logical qubit, we can modulate the relative phase between the first two time bins; a method which bears strong similarities to that used in dual-rail encoding. Alice's beam splitter

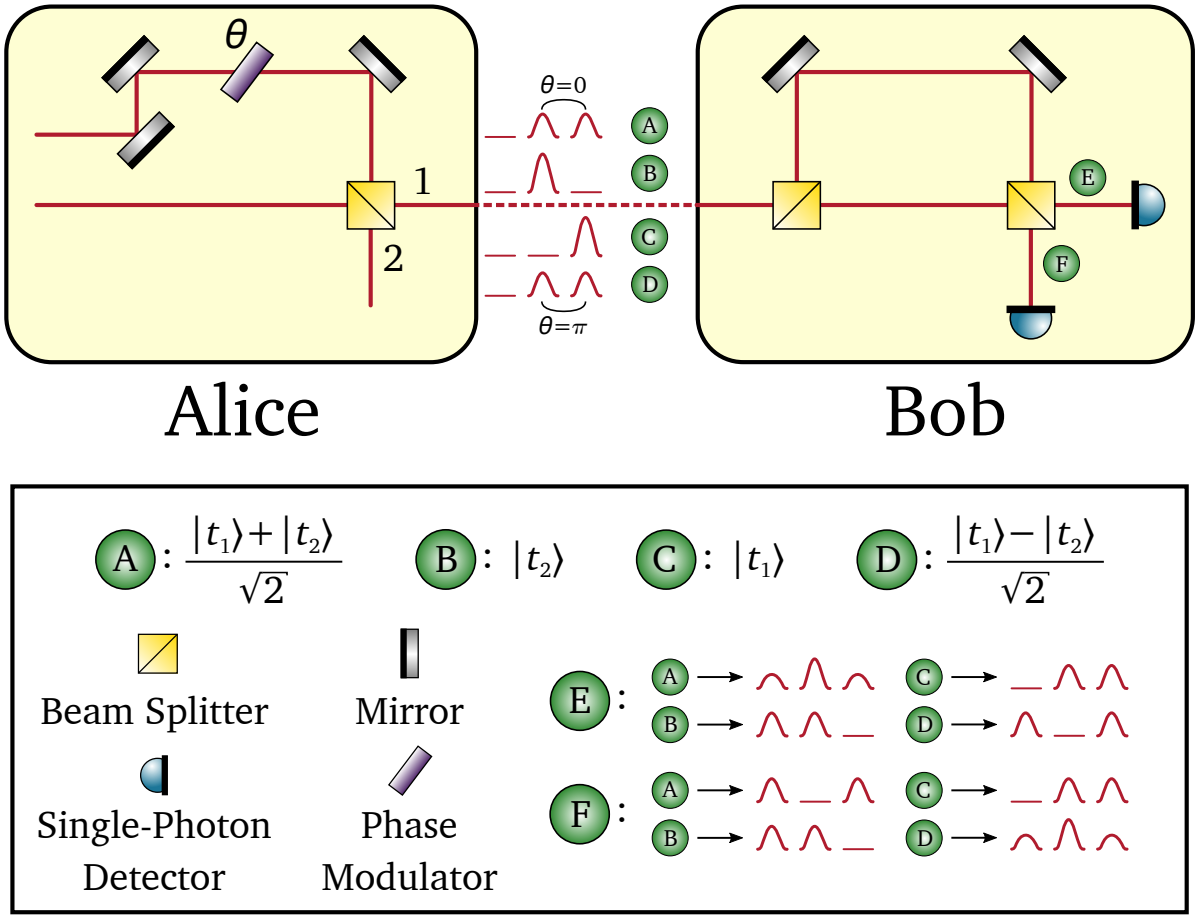


FIGURE 2.7: An example setup used for encoding quantum information onto the time-of-arrival of a single photon.

removes the spatial separation between temporal states, and while a combiner could be implemented as a way of merging outputs 1 and 2 (defined in figure 2.8a as beam splitter modes 3 and 4), it is not a cause for concern if this is omitted in practice. As will be described in the next part of this section, experimental setups use weak coherent pulses rather than true single photons, meaning a beam splitter with only a single connected output is equivalent to introducing 3 dB of loss.

With regards to the measurement process, a detector with a high enough temporal resolution would be able to distinguish between time-bins t_1 and t_2 directly. However, this is only of use if the qubits were prepared in the Z basis and, to measure in the X basis also, we must implement a detection scheme like in figure 2.7. The state is divided between two paths that differ in length so, for the component directed into the longer arm, and using the mode labels in figure 2.8b,

$$\begin{aligned} \hat{a}_{t_1,3} &\xrightarrow{\text{Delay}} \hat{a}_{t_2,3} \\ \hat{a}_{t_2,3} &\xrightarrow{\text{Delay}} \hat{a}_{t_3,3} \end{aligned} \tag{2.50}$$

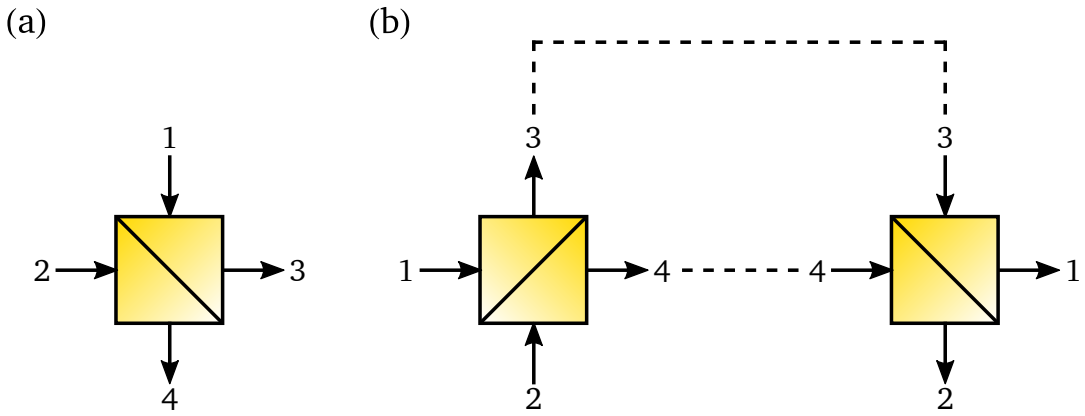


FIGURE 2.8: Labelling convention for the input and output modes of (a) a single beam splitter, and (b) two beam splitters connected in series.

Once again, the component that passes through the shorter arm remains unchanged.

Based on the above, it is simple to see that the receiver will transform non-superposition Z-basis states such that

$$\begin{aligned} |t_1\rangle &\rightarrow \frac{|t_1\rangle + |t_2\rangle}{\sqrt{2}} \\ |t_2\rangle &\rightarrow \frac{|t_2\rangle + |t_3\rangle}{\sqrt{2}} \end{aligned} \tag{2.51}$$

However, states of the form $\frac{1}{\sqrt{2}}\left(|t_1\rangle + e^{\mathrm{i}\theta}|t_2\rangle\right)$ are a little more complex. With reference to the port numbers in figure 2.8, the creation and annihilation beam splitter relations are

$$\begin{bmatrix} \hat{a}_1^{(\dagger)} \\ \hat{a}_2^{(\dagger)} \end{bmatrix} = \hat{H} \begin{bmatrix} \hat{a}_3^{(\dagger)} \\ \hat{a}_4^{(\dagger)} \end{bmatrix} \tag{2.52}$$

where $\hat{H}$ is defined in appendix A, and $\hat{H} = \hat{H}^{-1}$. On Bob's first beam splitter, we can represent port 1 as being connected to the upper arm of a dual-rail scheme (though this is not used to form a qubit), and port 2 as being connected to an unused lower arm, meaning

$$\begin{aligned} \frac{|t_1\rangle + e^{\mathrm{i}\theta}|t_2\rangle}{\sqrt{2}} &= \frac{1}{\sqrt{2}}\left(\hat{a}_{t_1}^\dagger + e^{\mathrm{i}\theta}\hat{a}_{t_2}^\dagger\right)|1\rangle_{\text{upper}}|0\rangle_{\text{lower}} \\ &= \frac{1}{\sqrt{2}}\left(\hat{a}_{t_1,1}^\dagger + e^{\mathrm{i}\theta}\hat{a}_{t_2,1}^\dagger\right)|00\rangle \\ &\xrightarrow{\text{BS}} \frac{1}{2}\left(\hat{a}_{t_1,3}^\dagger + \hat{a}_{t_1,4}^\dagger + e^{\mathrm{i}\theta}\hat{a}_{t_2,3}^\dagger + e^{\mathrm{i}\theta}\hat{a}_{t_2,4}^\dagger\right)|00\rangle \\ &\xrightarrow{\text{Delay}} \frac{1}{2}\left(\hat{a}_{t_2,3}^\dagger + \hat{a}_{t_1,4}^\dagger + e^{\mathrm{i}\theta}\hat{a}_{t_3,3}^\dagger + e^{\mathrm{i}\theta}\hat{a}_{t_2,4}^\dagger\right)|00\rangle \\ &\xrightarrow{\text{BS}} \frac{1}{2\sqrt{2}}\left[\hat{a}_{t_1,1}^\dagger - \hat{a}_{t_1,2}^\dagger + \left(1+e^{\mathrm{i}\theta}\right)\hat{a}_{t_2,1}^\dagger + \left(1-e^{\mathrm{i}\theta}\right)\hat{a}_{t_2,2}^\dagger + e^{\mathrm{i}\theta}\hat{a}_{t_3,1}^\dagger + \hat{a}_{t_3,2}^\dagger\right]|00\rangle \end{aligned} \tag{2.53}$$

Given equations 2.51 and 2.53, we can see that, for an unknown state in the Z basis, a click at time t_1 will signify that the initial state was $|\overline{0}\rangle$, while a click at time t_3 will indicate a $|\overline{1}\rangle$, regardless

of which detector we consider. Similarly, under the condition that Alice transmitted in the X basis, the detector on arm E will only click at time t_2 if the initial state was $|+\rangle$. If there is a click in the same time bin, but on arm F instead, this will correspond to Alice having sent a $|-\rangle$.

Of course, it is still possible to obtain a click in t_2 if Alice generated a qubit in the Z basis. This means that, in cases where Bob does not know how the state was prepared, he will be forced to incorrectly conclude that she transmitted either a $|+\rangle$ or a $|-\rangle$, depending on the arm in which the t_2 detection occurred. In other words, if the state sent by Alice was a $|\overline{0}\rangle$ or a $|\overline{1}\rangle$, then a click in the middle time bin will correspond to Bob measuring in the wrong basis. Likewise, if Alice transmitted a qubit in the X basis, and Bob observed a detection event in either t_1 or t_3, then he has to attribute it to a state in the Z basis. As before, this is just another way of saying that he has measured incorrectly and, if Alice later announces her bases, he can discard any erroneous results.

We note that because the detection scheme is passive in nature, its security may be brought into question if the beam splitters demonstrate wavelength-dependent behaviour [63]. However, the devices that rely on time-bin encoding herein, have too low a bandwidth to be compromised in this manner.

Coherent States

Unfortunately, the performance and practicality of single-photon sources is still not yet at a stage where they can be incorporated with application-oriented quantum technologies. This means that, for the time being, we must rely on weak coherent pulses instead. Coherent states are eigenstates of the annihilation operator, meaning [61]

$$\begin{aligned} \hat{a}\,|\alpha\rangle &= \alpha\,|\alpha\rangle \\ \langle\alpha|\,\hat{a}^\dagger &= \langle\alpha|\,\alpha^* \end{aligned} \tag{2.54}$$

They can be implemented using lasers attenuated down to the single-photon level and, as a coherent state is the most classical-like of the quantum states, it is sometimes mistakenly referred to as being non-quantum. However, they can still become entangled [64] which, in certain cases [65], leads to stronger violations of Bell-type inequalities when compared to states that take the form

$$\frac{|\gamma\rangle\,|0\rangle + e^{i\theta}\,|0\rangle\,|\gamma\rangle}{\sqrt{2}} \quad \text{for} \quad \gamma > 0 \tag{2.55}$$

There are also practical advantages to using entangled coherent states over those in equation 2.55, for example in quantum metrology [66].

We can illustrate the relation between coherent and number states using the derivation from [61]. This begins with the observation that a coherent state is a displacement of the quantum vacuum:

$$|\alpha\rangle = \hat{D}(\alpha)\,|0\rangle \tag{2.56}$$

$\hat{D}(\alpha)$, the displacement operator, is defined to be

$$\hat{D}(\alpha) = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}} \tag{2.57}$$

and the Baker-Campbell-Hausdorff formula states that

$$e^{\hat{O}_x+\hat{O}_y} = e^{\hat{O}_x} e^{\hat{O}_y} e^{-\frac{1}{2}[\hat{O}_x,\hat{O}_y]} \tag{2.58}$$

Thus, equation 2.56 can be rewritten as

$$\begin{aligned} |\alpha\rangle &= e^{\alpha\hat{a}^\dagger} e^{-\alpha^*\hat{a}} e^{-\frac{1}{2}[\alpha\hat{a}^\dagger, -\alpha^*\hat{a}]} |0\rangle \\ &= e^{-\frac{|\alpha|^2}{2}} e^{\alpha\hat{a}^\dagger} e^{-\alpha^*\hat{a}} |0\rangle \end{aligned} \tag{2.59}$$

Formulating each exponential as a power series means, with reference to equation 2.40,

$$\begin{aligned} |\alpha\rangle &= e^{-\frac{|\alpha|^2}{2}} e^{\alpha\hat{a}^\dagger} \sum_{\gamma=0}^{\infty} \frac{(-\alpha^*\hat{a})^\gamma}{\gamma!} |0\rangle \\ &= e^{-\frac{|\alpha|^2}{2}} e^{\alpha\hat{a}^\dagger} |0\rangle \\ &= e^{-\frac{|\alpha|^2}{2}} \sum_{\gamma=0}^{\infty} \frac{\left(\alpha\hat{a}^\dagger\right)^\gamma}{\gamma!} |0\rangle \end{aligned} \tag{2.60}$$

Therefore, we can express the coherent state in terms of number states such that

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{\gamma=0}^{\infty} \frac{\alpha^\gamma}{\sqrt{\gamma!}} |\gamma\rangle \tag{2.61}$$

where

$$\alpha = |\alpha| e^{i\theta} \tag{2.62}$$

We define the number operator as $\hat{\gamma} = \hat{a}^\dagger\hat{a}$, because

$$\hat{a}^\dagger\hat{a} |\gamma\rangle = \gamma |\gamma\rangle \tag{2.63}$$

The mean photon number is the expectation value of the number operator. That is,

$$\mu = \langle\alpha| \hat{\gamma} |\alpha\rangle = \langle\alpha| \alpha^*\alpha |\alpha\rangle = |\alpha|^2 \tag{2.64}$$

If $0 \leq \Gamma < \infty$, the probability of a pulse being found to contain Γ photons is given by

$$\begin{aligned} \text{Prob}(\gamma = \Gamma) = \langle\alpha|\Gamma\rangle \langle\Gamma|\alpha\rangle &= |\langle\Gamma|\alpha\rangle|^2 \\ &= \left| e^{-\frac{|\alpha|^2}{2}} \langle\Gamma| \sum_{\gamma=0}^{\infty} \frac{\alpha^\gamma}{\sqrt{\gamma!}} |\gamma\rangle \right|^2 \\ &= \left| e^{-\frac{|\alpha|^2}{2}} \langle\Gamma| \frac{\alpha^\Gamma}{\sqrt{\Gamma!}} |\Gamma\rangle \right|^2 \\ &= e^{-|\alpha|^2} \frac{|\alpha|^{2\Gamma}}{\Gamma!} \\ &= e^{-\mu} \frac{\mu^\Gamma}{\Gamma!} \end{aligned} \tag{2.65}$$

Using similar techniques to above, we can demonstrate the effect of a beam splitter on a pair of coherent states [67], which will be of particular importance in section 3.2.1. Given equation 2.56, the mathematical representation of two coherent states in modes 1 and 2 will be

$$\begin{aligned} |\alpha\rangle_1 |\alpha\rangle_2 &= \hat{D}_1(\alpha_1)\hat{D}_2(\alpha_2)|00\rangle \\ &= e^{\alpha_1 \hat{a}_1^\dagger - \alpha_1^* \hat{a}_1} e^{\alpha_2 \hat{a}_2^\dagger - \alpha_2^* \hat{a}_2} |00\rangle \end{aligned} \tag{2.66}$$

Application of equation 2.52 means

$$|\alpha\rangle_1 |\alpha\rangle_2 \xrightarrow{\text{BS}} e^{\frac{\alpha_1\left(\hat{a}_3^\dagger + \hat{a}_4^\dagger\right) - \alpha_1^*\left(\hat{a}_3 + \hat{a}_4\right)}{\sqrt{2}}} e^{\frac{\alpha_2\left(\hat{a}_3^\dagger - \hat{a}_4^\dagger\right) - \alpha_2^*\left(\hat{a}_3 - \hat{a}_4\right)}{\sqrt{2}}} |00\rangle \tag{2.67}$$

As shown in appendix B,

$$\left[\frac{\alpha_1\left(\hat{a}_3^\dagger + \hat{a}_4^\dagger\right) - \alpha_1^*\left(\hat{a}_3 + \hat{a}_4\right)}{\sqrt{2}}, \frac{\alpha_2\left(\hat{a}_3^\dagger - \hat{a}_4^\dagger\right) - \alpha_2^*\left(\hat{a}_3 - \hat{a}_4\right)}{\sqrt{2}}\right] = 0 \tag{2.68}$$

so we can once again apply Baker-Campbell-Hausdorff (equation 2.58) such that equation 2.67 becomes

$$\begin{aligned} |\alpha\rangle_1 |\alpha\rangle_2 &\xrightarrow{\text{BS}} e^{\frac{\alpha_1\left(\hat{a}_3^\dagger + \hat{a}_4^\dagger\right) - \alpha_1^*\left(\hat{a}_3 + \hat{a}_4\right) + \alpha_2\left(\hat{a}_3^\dagger - \hat{a}_4^\dagger\right) - \alpha_2^*\left(\hat{a}_3 - \hat{a}_4\right)}{\sqrt{2}}} |00\rangle \\ &= e^{\frac{(\alpha_1+\alpha_2)\hat{a}_3^\dagger - \left(\alpha_1^* + \alpha_2^*\right)\hat{a}_3 + (\alpha_1 - \alpha_2)\hat{a}_4^\dagger - \left(\alpha_1^* - \alpha_2^*\right)\hat{a}_4}{\sqrt{2}}} |00\rangle \\ &= e^{\frac{(\alpha_1+\alpha_2)\hat{a}_3^\dagger - \left(\alpha_1^* + \alpha_2^*\right)\hat{a}_3}{\sqrt{2}}} e^{\frac{(\alpha_1-\alpha_2)\hat{a}_4^\dagger - \left(\alpha_1^* - \alpha_2^*\right)\hat{a}_4}{\sqrt{2}}} |00\rangle \\ &= \hat{D}_3\left(\frac{\alpha_1+\alpha_2}{\sqrt{2}}\right)\hat{D}_4\left(\frac{\alpha_1-\alpha_2}{\sqrt{2}}\right)|00\rangle \\ &= \left|\frac{\alpha_1+\alpha_2}{\sqrt{2}}\right\rangle_3 \left|\frac{\alpha_1-\alpha_2}{\sqrt{2}}\right\rangle_4 \end{aligned} \tag{2.69}$$

Here, when applying Baker-Campbell-Hausdorff for a second time,

$$\left[\frac{(\alpha_1+\alpha_2)\hat{a}_3^\dagger - \left(\alpha_1^* + \alpha_2^*\right)\hat{a}_3}{\sqrt{2}}, \frac{(\alpha_1-\alpha_2)\hat{a}_4^\dagger - \left(\alpha_1^* - \alpha_2^*\right)\hat{a}_4}{\sqrt{2}}\right] = 0 \tag{2.70}$$

because $\hat{a}_3$ and $\hat{a}_4$ commute. Now, we place a 100%-efficient single-photon detector on arm 3, that clicks in the presence of anything other than the vacuum (i.e. it has zero dark counts and is non-number-resolving). Based on equation 2.65,

$$\begin{aligned} \text{Prob}(\text{Click in detector 1}) &= 1 - \text{Prob}(\gamma = 0) \\ &= 1 - \frac{|\alpha_1+\alpha_2|^0}{2^0 \times 0!} e^{-\frac{|\alpha_1+\alpha_2|^2}{2}} \\ &= 1 - e^{-\frac{|\alpha_1+\alpha_2|^2}{2}} \end{aligned} \tag{2.71}$$

If we place an identical detector on arm 4,

$$\begin{aligned} \text{Prob}(\text{Click in detector 2}) &= 1 - \text{Prob}(\gamma = 0) \\ &= 1 - \frac{|\alpha_1-\alpha_2|^0}{2^0 \times 0!} e^{-\frac{|\alpha_1-\alpha_2|^2}{2}} \\ &= 1 - e^{-\frac{|\alpha_1-\alpha_2|^2}{2}} \end{aligned} \tag{2.72}$$

Finally, a coincidence will be observed with probability

$$\begin{aligned}\text{Prob}\,(\text{Click in both detectors}) = \text{Prob}\,(\text{Click in detector 1}) \\ \times\, \text{Prob}\,(\text{Click in detector 2})\end{aligned} \tag{2.73}$$

2.3 Quantum Cryptography

In the last part of this chapter, we look at how the physics of the previous section can be used to counteract the catastrophic effect that quantum computers will have on the cryptography used throughout everyday life. To date, many lines of enquiry have been opened into the advantages quantum mechanics can provide, exploring ideas such as quantum bit commitment [68–71], quantum secret sharing [72–74] and quantum digital signatures [75]. However, the greatest focus has been on QKD, as this has the potential to solve the most urgent and important problem: re-securing the exchange of cryptographic keys.

2.3.1 Quantum Key Distribution Protocols

The central premise of QKD is as follows: can we create a method for the secure distribution of cryptographic keys that does not rely on our inability to solve an underlying mathematical problem? Here, we consider a number of different protocols that fulfil this notion.

BB84

The first QKD protocol was invented by Bennett and Brassard in 1984 [76], and this was followed shortly after by a proof-of-principle demonstration in 1992 [77]. Though many alternatives have emerged since, Bennett-Brassard 1984 (BB84) remains one of the most popular choices for experimental implementations of QKD.

In protocol 2.5, we summarise this approach to generating cryptographic keys from quantum states of light. The sifting procedure described in step 4a removes any errors that were introduced as a result of Bob measuring in the wrong basis. However, discarding half of Alice and Bob's raw key will affect the final secret key rate, and so ζ, the sifting efficiency of the protocol, is an important metric to consider. In the case of BB84, it follows that $\zeta = 50\%$.

As can be seen in step 5, the tags used to authenticate the public channel take the form of equation 2.5. The use of a one-time k_M means that authenticating every message at the time of transmission will consume valuable quantum keys to no advantage. In fact, if all the basis announcements were to be treated individually, more key would be consumed than generated, so it is for this reason that BB84 delays authentication until the end.

Protocol 2.5: BB84 [76]

SUMMARY: Alice expands a shared secret with Bob by sending cryptographically-secure bits over a quantum channel, and reconciliation information over an authenticated classical channel.

1. *One-Time Setup.* Two ($|k_{\text{init}}|/2$)-bit secrets are shared between Alice and Bob using out-of-band communications, a trusted third party or a post-quantum public-key algorithm.
2. *Raw Key Exchange.*
   (a) Alice generates a cryptographically-secure random bit, which is used to select a basis $B_i^{\text{A}} \in \{X, Z\}$.
   (b) Bob generates a cryptographically-secure random bit, which is used to select a basis $B_i^{\text{B}} \in \{X, Z\}$.
   (c) Alice prepares a qubit $|\psi\rangle_i$ by generating a cryptographically-secure random number, $b_i \in \{0, 1\}$, and encoding it in the basis B_i^{A}.
   (d) Alice sends $|\psi\rangle_i$ to Bob, who measures in the basis B_i^{B}.
3. *Loop.* Step 2 is repeated for the remaining $N - i$ qubits sent from Alice to Bob.
4. *Post-Processing.*
   (a) Alice and Bob publicly reveal their bases and discard all bits for which $B_i^{\text{A}} \neq B_i^{\text{B}}$. At this stage, Alice can also discard any bits corresponding to qubits that Bob failed to detect.
   (b) Alice and Bob publicly compare an agreed-upon subset of their remaining bits. If these differ by more than the security proof allows (usually 11%), the protocol aborts. Otherwise, the subset is discarded and an error correction protocol such as CASCADE or Low Density Parity Check is applied to the remaining key, reducing the number of errors to zero.
   (c) Privacy amplification is carried out, typically relying on a universal hash function to minimise the information that an eavesdropper has on the key.
5. *Authentication.*
   (a) The first shared secret is split into a one-time key, k_{M}, and a ($|k_{\text{init}}|/2 - |k_{\text{M}}|$)-bit hash key, k_{H}. Here, $|k_{\text{M}}| = \left|h_{k_{\text{H}}}(m)\right|$ where $\forall k_{\text{H}}$, $\left|h_{k_{\text{H}}}(m)\right| =$ constant.
   (b) Alice calculates m, a concatenation of the messages she transmitted and received over the public channel. She computes the tag $\tau = h_{k_{\text{H}}}(m) \oplus k_{\text{M}}$ and sends it to Bob.
   (c) Bob calculates m', a concatenation of the messages he transmitted and received over the public channel. He computes the tag $\tau' = h_{k_{\text{H}}}(m') \oplus k_{\text{M}}$ and compares it with the one he received from Alice. If $\tau \neq \tau'$, the protocol aborts.
   (d) Steps 5a to 5c are repeated for the second shared secret, with Alice and Bob's roles reversed.
   (e) $|k_{\text{init}}|$ bits are taken from the final key and stored for use as the initial shared secrets in the next round of QKD.

SARG04

In the next section (specifically, attack 2.1), we will see that one of the downsides to using an attenuated laser in place of a single-photon source is that it creates an opportunity for photon number splitting (PNS) to be carried out. Scarani-Acín-Ribordy-Gisin 2004 (SARG04) [78] is a way of modifying BB84 such that an eavesdropper who performs PNS attacks on two-photon pulses

is unable to gain any information on the qubit. As described in protocol 2.6, instead of making a simple basis declaration, Alice announces one of the following pairs of states:

$$\left\{|\bar{0}\rangle, |-\rangle\right\} \quad , \quad \left\{|\bar{0}\rangle, |+\rangle\right\} \quad , \quad \left\{|\bar{1}\rangle, |-\rangle\right\} \quad , \quad \left\{|\bar{1}\rangle, |+\rangle\right\} \tag{2.74}$$

Her choice is restricted only in that she must have transmitted one of the states that she announced. For example, if Alice prepared $|\bar{0}\rangle$, she can inform Bob using either $\left\{|\bar{0}\rangle, |-\rangle\right\}$ or $\left\{|\bar{0}\rangle, |+\rangle\right\}$. On the other hand, if she sent $|+\rangle$, then she must choose $\left\{|\bar{0}\rangle, |+\rangle\right\}$ or $\left\{|\bar{1}\rangle, |+\rangle\right\}$.

Bob now has to announce whether his measurement result lets him identify the state that was sent by Alice over the quantum channel. This is effectively unambiguous state discrimination between the pair of qubits that she declared, although as three out of four measurement results will be inconclusive, ζ is reduced to 25%.

Protocol 2.6: SARG04 [78]

SUMMARY: Replaces step 4a in protocol 2.5, changing the information that is transmitted over the classical channel to increase resilience against photon number splitting attacks.

4. *Post-Processing.*

   (a) For each qubit sent, Alice publicly announces a pair of states, one of which she transmitted and one of which is randomly chosen from the unused basis. Bob announces whether or not his measurement outcome is consistent with one, and only one, of the states Alice announced. If his declaration is in the affirmative, the corresponding bit is retained. Else, it is discarded. At this stage, Alice can also discard any bits corresponding to qubits that Bob failed to detect.

Quantum Key Distribution with Decoy States

Another way to prevent PNS is through the use of decoy states, as described in protocol 2.7. Here, Alice varies the mean photon number, μ, that defines each weak coherent pulse, choosing from one of three possible values [79]. The signal-to-decoy ratio is optimised depending on the setup. For example, in [80], $\text{Prob}\left(\mu_{\text{signal}}\right) = 63.5\%$, $\text{Prob}\left(\mu_{\text{weak}}\right) = 20.3\%$ and $\text{Prob}\left(\mu_{\text{vacuum}}\right) = 16.2\%$, where μ_{weak} and μ_{vacuum} both correspond to decoy states.

As an eavesdropper has no way of knowing what μ is for each pulse, she cannot use this information to influence her attack. At the end of the protocol, Bob can see whether the number of detection events for each value of μ are sensibly scaled relative to one another. If the eavesdropper has been blocking single photons and letting multi-photon pulses through, the transmission rate for higher mean photon numbers will be disproportionately large, and so Bob will become aware of the eavesdropper's presence.

Protocol 2.7: Decoy State BB84 [79, 81]

SUMMARY: Replaces steps 2c, 4a and 4b in protocol 2.5, introducing additional intensity states to detect photon number splitting attacks.

2. *Raw Key Exchange.*

   (c) Alice prepares a qubit $|\psi\rangle_i$ by generating a cryptographically-secure random number, $b_i \in \{0,1\}$, and encoding it on a weak coherent pulse in the basis B_i^{A}. She generates a second cryptographically-secure random number and uses this to decide whether the mean photon number should be μ_{signal}, μ_{weak} or μ_{vacuum}.

4. *Post-Processing.*

   (a) Alice announces the mean photon number corresponding to each qubit. If the relative number of detections for μ_{signal}, μ_{weak} and μ_{vacuum} does not match the distribution that we would expect, the protocol aborts. Otherwise, Alice and Bob publicly reveal their bases and discard all bits for which $B_i^{\mathrm{A}} \neq B_i^{\mathrm{B}}$. At this stage, Alice can also discard any bits corresponding to qubits that Bob failed to detect.

   (b) For each μ, Alice and Bob publicly compare agreed-upon subsets of their remaining bits. If these differ by more than the security proof allows, the protocol aborts. Otherwise, each subset is discarded, along with the bit values corresponding to μ_{weak} and μ_{vacuum}. An error correction protocol is applied to the remaining key so as to reduce the number of errors to zero.

Quantum Key Distribution with Biased Bases

It has already been noted that the sifting efficiency, ζ, will affect the final key rate. The question therefore arises as to whether there is a way in which we can increase ζ, without compromising our security. This turns out to be possible by biasing the bases as described in protocol 2.8. Under such a scheme, it has been found that, theoretically, [82]

$$\lim_{N\to\infty} \zeta = 100\% \tag{2.75}$$

where N is the number of qubits exchanged over the course of the protocol. However, experimentally, the optimal bias tends to be between 80% and 90% [83, 84] or, for setups that combine decoy-state and biased basis QKD, between 60% and 95% depending on the loss [85]. As a result, practical increases in efficiency can be somewhat lower than the asymptotic limit.

2.3.2 Attacks on Quantum Key Distribution

We now introduce an eavesdropper (Eve), who is given the challenge of recovering the key from the information that passes over the public and quantum channels during a QKD protocol. She may choose to passively observe the messages going past, or actively interfere in their transmission, and is constrained only by the laws of quantum mechanics. In section 2.2.1, we showed there is no measurement operator that can be used to deterministically distinguish between non-orthogonal states, and that these cannot be deterministically cloned either. Therefore, if Eve intercepts a

Protocol 2.8: Biased Basis BB84 [82]

SUMMARY: Replaces steps 2a, 2b and 4b in protocol 2.5, increasing the sifting efficiency by biasing the bases.

2. *Raw Key Exchange.*

   (a) Alice generates a cryptographically-secure random bit, which is used to select a basis $B_i^{\mathrm{A}} \in \{X, Z\}$, optimally weighted such that $0 < \mathrm{Prob}\left(B_i^{\mathrm{A}} = X\right) < \frac{1}{2}$.

   (b) Bob generates a cryptographically-secure random bit, which is used to select a basis $B_i^{\mathrm{B}} \in \{X, Z\}$, optimally weighted such that $0 < \mathrm{Prob}\left(B_i^{\mathrm{B}} = X\right) < \frac{1}{2}$.

4. *Post-Processing.*

   (b) Alice and Bob publicly compare an agreed-upon subset of their remaining bits that were prepared and measured in the X basis. If these differ by more than the security proof allows (usually 11%), the protocol aborts. Otherwise, the subset is discarded, and this process is repeated for the bits that were prepared and measured in the Z basis. As required by the security analysis [82], any leftover bits that correspond to the X basis are also discarded. An error correction protocol is then applied to the remaining key so as to reduce the number of errors to zero.

single photon, she will be unable to make any copies for further examination, and her optimum measurement strategy will be to guess whether it was prepared in the X basis or the Z basis. She must then generate a new qubit and send it to Bob, encoded with the bit value she observed in the basis she chose. However, if Eve guesses incorrectly, she will return a random result, as demonstrated in equations 2.76 and 2.77, where $|+\rangle$ is measured in the Z basis.

$$\begin{aligned} \langle + | \hat{M}_1 \hat{M}_1 | + \rangle &= \langle + | \overline{0} \rangle \langle \overline{0} | + \rangle \\ &= \left(\frac{\langle \overline{0}| + \langle \overline{1}|}{\sqrt{2}} \right) |\overline{0}\rangle \langle \overline{0}| \left(\frac{|\overline{0}\rangle + |\overline{1}\rangle}{\sqrt{2}} \right) \\ &= \frac{1}{2} \end{aligned} \tag{2.76}$$

$$\begin{aligned} \langle + | \hat{M}_2 \hat{M}_2 | + \rangle &= \langle + | \overline{1} \rangle \langle \overline{1} | + \rangle \\ &= \left(\frac{\langle \overline{0}| + \langle \overline{1}|}{\sqrt{2}} \right) |\overline{1}\rangle \langle \overline{1}| \left(\frac{|\overline{0}\rangle + |\overline{1}\rangle}{\sqrt{2}} \right) \\ &= \frac{1}{2} \end{aligned} \tag{2.77}$$

This additional randomness will cause the quantum bit error rate (QBER) to increase, and so it is possible to tell whether or not an eavesdropper is present, with Alice and Bob terminating the connection if the QBER goes above a critical threshold. Of course, there are numerous attack strategies beyond those covered here; Eve could try to entangle the qubits with her own ancillas, for example. Consequently, full security proofs are required, such as that developed by Shor and Preskill for BB84 [86], which gives a critical QBER of 11%.

We can order Eve's strategies into three groups: individual attacks, collective attacks and general attacks. Individual attacks are the most constrained, as Eve must apply the same strategy to every qubit and measure any ancillas before Alice and Bob perform post-processing. Collective attacks also require Eve to apply a non-adaptive strategy, however she can take advantage of a quantum memory to measure any ancillas in her possession at the point where she will maximise her information gain. Finally, general attacks are the most powerful, wherein Eve can implement any quantum-mechanical operation and adapt her strategy at will [87].

This last sentence is of particular importance. Protocols that resist general attacks are said to be information-theoretically secure, and such a claim is often misinterpreted to mean QKD is unbreakable. While it is true that we no longer need to assume any limits on Eve's computational power, it is not true that we have removed every assumption altogether; a point which has been acknowledged since the earliest security proofs [86, 88, 89]. The most extreme assumption we make is that quantum mechanics represents an inherently probabilistic underlying reality. There is strong evidence that the universe cannot be described by a theory of local hidden variables [90], but superdeterminism will always remain an unclosable loophole, and we are yet to find a way of disproving non-local hidden-variable models like Bohmian mechanics [91, 92]. Some would argue that assumptions of this nature mean statements of security based on the laws of physics are incorrect [93]. However, this is a basic misunderstanding as to what the laws of physics actually are: scientific knowledge based on experimental results [94, 95]. Thus, the set of physical laws is constantly expanding, and untested hypotheses are excluded by definition, especially if, as in the examples above, they lack falsifiable predictions that would distinguish them from any competing proposals.

Yet such a point should not be taken to mean that we make no assumptions of presently-significant impact. Just like in the case of the OTP, the information-theoretic security of QKD says nothing about the possibility of side-channel attacks, as these sit outside the mathematical framework described above. Therefore, for a security proof to remain comprehensively valid when transitioning from theory to experiment, we must assume (quite falsely) that QKD can be perfectly implemented in all scenarios.

Of the attacks on BB84 that arise from this assumption being violated, PNS is perhaps the most well-known. All practical systems use weak coherent states to approximate a qubit, and so some of the pulses that Alice generates will inevitably contain two or more photons, which Eve can then siphon off for herself. While protocols 2.6 and 2.7 provably reduce and eliminate the threat, attack 2.1 can always be mounted on implementations that do not employ some form of countermeasure.

Attack 2.1: Photon Number Splitting. *Eve performs a quantum non-demolition measurement on the number of photons in each pulse. She blocks all single-photon terms, and splits those containing multiple photons. She retains at least one photon in a quantum memory, and allows the remainder to carry on towards Bob. When Alice announces her preparation bases, Eve measures the stored photons, returning the same raw key as Alice (assuming zero errors). This can be sifted correctly when Bob publicly responds to Alice's original announcement.*

Despite the apparently straightforward nature of the above, it should be noted that, from an academic perspective, PNS is a particularly interesting exploit. Unlike most attacks, it is only dangerous if the technology required to carry it out is solely available to Eve. In the case where non-demolition measurements can also be performed by Alice, she could use PNS on herself to create a single-photon source.

Next, although protocol 2.6 allows the secure generation of key from two-photon terms, unambiguous state discrimination can still be carried out on pulses containing three or more photons [78], as attack 2.2 describes.

Attack 2.2: Unambiguous State Discrimination on $\geq$ 3-Photon Pulses. *Eve performs a quantum non-demolition measurement on the number of photons in each pulse. She blocks all single- and two-photon terms, and performs unambiguous state discrimination* [43] *on those containing three or more photons. She returns a proportion of Alice's raw key dependent on the number of photons measured.*

A particularly damaging scenario may unfold if an undisclosed side-channel gives Eve early access to the basis information on each qubit. In this case, she can carry out attack 2.3, which would otherwise be considered impossible.

Attack 2.3: Intercept-Resend. *Eve extracts information on either Alice or Bob's bases through an undisclosed side channel. She then intercepts the qubits, measures each one using a basis that will not increase the QBER, and resends the results she observed in the bases she measured.*

Another way a catastrophic break could occur is if the authentication scheme for the public channel were to be implemented incorrectly. However, at a theoretical level, attack 2.4 is not something with which we usually need to be concerned, because Wegman-Carter MACs are information-theoretically secure.

Attack 2.4: Man-in-the-Middle. *Eve intercepts the qubits, measures each one in a random basis and resends the results she observed in the bases she measured. She conceals this by modifying Alice's bases announcement and Bob's response, along with the authentication tags for each. Eve can now read all communications encrypted and/or authenticated using the key she shares with Alice, before forwarding them with or without modification, having re-encrypted or authenticated using the key she shares with Bob.*

There are also several exploits that do not break the confidentiality of QKD, serving only to disable the link instead. As Eve cannot obtain any information on the message, some may try to argue that weaknesses of this nature are only a minor concern. Yet there is little point in having an unbreakable cryptosystem that cannot be used and so, for this reason, the following attacks should be taken as seriously as any other.

Nonetheless, it would be misleading to categorise these as side-channel attacks, because they are enabled by features that are integral to the theory of QKD. For example, the randomness introduced when Eve tries and fails to implement attack 2.3 would normally be used as a way of detecting her presence. However, as the protocol automatically aborts when the QBER gets too high, this opens up the opportunity for intentional denial of service (DoS), by artificially increasing the error rate on the transmission line (see attack 2.5). While sometimes used as an argument against QKD [96], the risk of this happening is often overstated, as it requires an attacker to have physical access to the optical fibre, so the development of large-scale quantum networks will mitigate a lot of the damage by enabling redirection of the signal.

Attack 2.5: Transmission Line Denial of Service. *Eve artificially increases the QBER of the channel to the point where Alice and Bob become aware of her presence and are unable to distill a secret key. If no alternative channels are available, they must resort to physically locating Eve in order to restore the connection.*

Lastly, the use of a Wegman-Carter MAC to authenticate the public channel means an initial shared secret is required. Protocol 2.5 leaves open the possibility of distributing this using a post-quantum public key, as will be explored in chapter 6. Yet QKD implementations traditionally avoid introducing asymmetric primitives, as then the cryptosystem that they are a part of will no longer be information-theoretically secure. On the other hand, repopulating the initial secret can be challenging if it is not shared in this way and Eve interferes with the basis announcements, causing the authentication step to fail. Even when Alice and Bob have additional keys in reserve, they will be limited in number, so this defence mechanism is of little to no benefit if Eve repeatedly modifies any messages that are sent via the public channel. It is on this weakness that attack 2.6 is predicated.

Attack 2.6: Key Exhaustion. *Eve establishes a low-loss connection with Alice and performs high-bit-rate QKD up to the point where she fails the authentication. She or her agents repeat this until Alice no longer has enough secret key with which to construct a MAC. Now, Alice must switch to an alternative method of key distribution to avoid indefinite denial of service.*

2.4 Summary

In this section, we have provided a general background to modern cryptography, quantum mechanics and quantum technologies, all of which are relevant throughout this thesis. We opened by considering methods for encryption and authentication that rely on Alice and Bob being in possession of a pre-shared key, before progressing to asymmetric alternatives, which generate keys that have both a public part and a private part. The latter system is widely used to transport secret keys for use in symmetric applications.

Next, we covered the principles of quantum mechanics that are fundamental to the security of QKD. A brief overview of quantum computers included a table of resource estimates reviewing the level they will need to reach in order to break public-key cryptography, as well as reduce the security of symmetric-key ciphers and hash functions.

This was followed by a discussion of the different ways in which we can encode information onto quantum states of light. The underlying properties of coherent states were also summarised, as these are used to approximate single photons in experimental systems.

Finally, we introduced the main QKD protocols that will be used in the chapters that follow, with a high-level overview of attacks that can be mounted both in theory and in practice.

CHAPTER 3

TIME-SHARED QUANTUM CRYPTOGRAPHY ON SOFTWARE-DEFINED NETWORKS

Declaration of Work

I developed the initial design for the first generation testbed in collaboration with John Rarity and Reza Nejabati. This was then expanded upon by myself, Alejandro Aguado, Philip Sibson, John Rarity, Emilio Hugues-Salas, Chris Erven, Jake Kennard and Mark Thompson. I constructed the physical layer in collaboration with Emilio Hugues-Salas, Paul Haigh and Alejandro Aguado. The SDN controller was written by Alejandro Aguado and Jaume Marhuenda, based on OpenDaylight. I wrote all of the remaining software used in this chapter, except for QKDSequence which was provided by ID Quantique. The AES-GCM implementation used OpenSSL, and KeyCutter was based on the IDQ3P protocol developed by ID Quantique.

I measured the Clavis^2 QBER and secret key rates, as well as characterising the Polatis unassisted. I took the initialisation data presented herein and performed all of the analysis.

The second generation testbed was designed by myself, Chris Erven and Richard Collins. I assisted Richard Collins in the construction of the physical layer.

The first communication over the Bristol Quantum Network was undertaken with the assistance of Emilio Hugues-Salas. The UK Quantum Network tests were performed in collaboration with Emilio Hugues-Salas and Jake Kennard.

Preliminary results for this work appeared in [97, 98], as well as being presented at QCrypt and BQIT [9, 99]. The results contained within this thesis were presented at YQIS [100].

For a communications technology to be of any practical use, it must be capable of more than just two-party exchanges over a fixed channel. The ability to network large numbers of devices such that they can all interact with each other is the foundation of the internet. However, it is not enough for quantum key distribution (QKD) to easily integrate with the infrastructure of today. It must be compatible with next-generation architectures that will start to become widespread during its lifetime. Much work has already been done towards the former but, prior to the work presented here, very little progress had been made with regard to the latter.

Here, we introduce a promising new paradigm for telecommunications: software-defined networking. We have run experiments demonstrating how QKD can fit into this environment with minimal disruption to the classical setup, particularly emphasising the ability for QKD pairings to be established between different endpoints on a flexible basis, either in the context of a standard network, or in scenarios where there is an asymmetric number of Alices and Bobs. These tests constituted the first physical implementation of QKD in a software-defined network (SDN), as previous research was restricted only to simulations [101, 102]. The topic has since blossomed into a highly active sub-field [103–113].

We open this chapter by reviewing the numerous quantum networks that have been built across the world, before introducing the Bristol software-defined metropolitan-area quantum network, which forms an endpoint to the UK quantum backbone. In section 3.2, we describe the experimental testbed that was built for emulating different network configurations, enabling QKD technologies to be trialled prior to deploying them across the city. Finally, section 3.3 focuses on time-division multiple access QKD, demonstrating the ease with which it can be implemented in an SDN, enhancing its security through the distribution of virtual network functions.

3.1 State-of-the-Art in Telecommunications Networks

Although QKD can still only be deployed in highly bespoke environments, transitioning experimental devices beyond the laboratory is no small feat, and a great deal of research has been carried out to arrive at this point. For countries willing to make large capital investments, purpose-built QKD links are now physically viable for real-world communications, ensuring the security of government data against quantum attacks. Here, we provide an overview of the progress that has been made so far, and summarise the generalised approach to networking with which QKD will need to be shown compatible if it is to achieve widespread deployment.

3.1.1 Quantum Key Distribution Networks

Quantum key distribution has long been mature enough at the device level to be deployed as a rack-mounted solution over dedicated fibre in the field. Table 3.1 and figure 3.2 summarise the history of quantum networks across the world, from the original DARPA implementation in 2004 [114, 115] to the present. Those of particular note include SwissQuantum [121], the world's first international

TABLE 3.1: A history of quantum networks throughout the world [114–145].

June 2004	DARPA Quantum Network | Cambridge, Massachusetts
March 2007	CNC Beijing | Beijing, China
October 2008	SECOQC | Vienna to St Pölten, Austria
October 2008	Hefei Metro-Quantum Network | Hefei, China
February 2009	QuantumCity | Durban, South Africa
March 2009	SwissQuantum | Geneva, Switzerland to CERN, France
May 2009	Quantum Cryptography Network for Government Administration | Wuhu, China
October 2009	Madrid Quantum Network | Madrid, Spain
March 2010	Tokyo QKD Network | Tokyo, Japan
December 2011	Hefei-Chaohu-Wuhu Wide Area Network | Hefei to Wuhu, China
October 2013	Battelle Commercial Network | Columbus to Dublin, Ohio
December 2013	Jinan Metro-Quantum Network | Jinan, China
January 2016	Bristol Quantum Network (part of the UK Quantum Network) | Bristol, United Kingdom
February 2016	SK Telecom Metro Network | Seoul to Seong-nam, South Korea
February 2016	KREONET | Daejeon, South Korea
May 2016	Shanghai Quantum Network | Shanghai, China
May 2016	KPN Data Centre Network | The Hague to Rotterdam, Netherlands
June 2016	Moscow Quantum Network | Moscow, Russia
June 2016	SK Telecom Long-Term Evolution Network | Sejong to Daejeon, South Korea
August 2016	Kazan Quantum Network | Kazan, Russia
September 2016	Shanghai-Hangzhou Trunk Network | Shanghai to Hangzhou, China
November 2016	Cambridge Quantum Network (part of the UK Quantum Network) | Cambridge, United Kingdom
January 2017	Beijing-Shanghai Backbone Network | China
September 2017	Micius Satellite Network | Beijing, China to Vienna, Austria
October 2017	CASIC Wuhan Network | Wuhan, China
June 2018	UKQNtel (part of the UK Quantum Network) | Cambridge to Martlesham Heath, United Kingdom
July 2018	Deutsche Telekom | Berlin, Germany
November 2018	Phio | Manhattan, New York to Newark, New Jersey

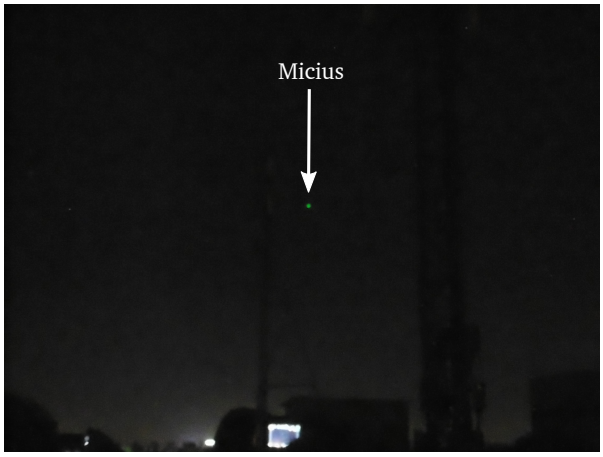


FIGURE 3.1: The Micius quantum satellite as seen from the Shanghai ground station.

quantum network, and the Micius satellite (figure 3.1), part of the first intercontinental QKD link [138, 139]. SECOQC [117] hosted a quantum-secure videoconference, an achievement that has since been replicated in numerous other locations as a way of demonstrating encryption capabilities. Finally, the world's first national quantum backbone runs between Beijing and Shanghai [137, 138], covering over 2000km, and connecting four cities using 32 trusted nodes. Each of the population centres are serviced by their own metro networks which, from the information available, contain at least 94 nodes between them. With a further seven nodes accessible in the form of Micius ground stations, and six on the currently-separate Shanghai-Hangzhou Trunk [136], it seems fair to say that this is the closest precursor we have to the quantum internet.

In table 3.1, each network is dated according to when the first link between remote locations was realised. Where such information was unavailable, the date of the initial press release or journal submission has been used instead. This was preferable over trying to establish a completion date, as many of those listed here continue to grow and evolve. For networks like Hefei [118, 119], multiple generations exist with different architectures. These are grouped into a single timeline entry, dated according to the initial transmission as part of the first iteration.

A consequence of requiring the sender and receiver to be spatially separated is that the Bristol Quantum Network to which this thesis contributes, must be listed as beginning in January 2016, even though preliminary experiments were performed using a loopback configuration in late 2015. Figure 3.2 is also impacted, because implementations like the Advanced Technology Demonstration Network (ATDNet) [146] and the entanglement link in the Tokyo QKD Network [125] were constructed as loopbacks, so have not been marked.

In addition to the above, there are two further criteria for inclusion. We summarise our three requirements as follows:

- The quantum signals must have passed through at least one piece of equipment that is standard to an optical network, not including the main transmission line. For example, a switch.

- A full quantum protocol must have been implemented as part of a specific application. For example, an encryption scheme that is keyed using Bennett-Brassard 1984 (BB84).

- At least one link must have been constructed for the sake of connecting two or more disparate locations, and not solely for the purpose of field-testing a quantum device.

Under these conditions, examples like the 144 km link between La Palma and Tenerife [147], and Micius' early demonstration of entanglement distribution over 1200 km [148] may be considered network experiments, but neither is sufficient to constitute a quantum network.

3.1.2 Software-Defined Networks

SDNs are an emerging communications technology which offer increased reconfigurability and centralised control by deploying data handling rules as software, rather than embedding them in the firmware of devices. This enables versatile network topologies which are better suited to modern needs, and bypasses compatibility issues between different proprietary architectures [149].

Traditionally, each forwarding device in the data plane of a network will contain an instruction set that dictates how different packets should be treated, conditional on characteristics such as port number, protocol and IP address. A node in receipt of a data packet will scan the header for the above information and process it accordingly [150], meaning we can share our communications infrastructure between many end-users without messages arriving at the wrong destination or getting lost en route. However, this model is naturally inflexible because changes cannot be implemented on the fly, motivating a drive towards separating the control plane from the data plane, a technique that is particularly useful for networking trends like cloud computing [149].

As illustrated in figure 3.3, SDNs do just this. Compared to conventional networks, they are simpler to deploy, more efficient to configure, and less error-prone [151]. Each node is centred around a switch, the only component through which all signals must pass. By removing inline devices, and "hanging" them off said switch instead (see figure 3.4), it is possible to achieve full topological reconfigurability.

The SDN controller used in this work is the Lithium release of OpenDaylight, a Java-based open-source Linux Foundation project. By utilising the OpenFlow communications protocol [152], it is possible to modify the forwarding rules contained within a flow table on each switch. Here, we focus on protecting the data plane as a way of demonstrating the compatibility of QKD with SDNs. However, this will ultimately prove inconsequential if the control-data programming interface (PI) and the links between adjacent controllers are not also quantum-secure, as they are both central points of failure that do not exist in traditional networking paradigms. Therefore, the results presented herein must only be the first step on the path towards a fully quantum-enabled SDN.

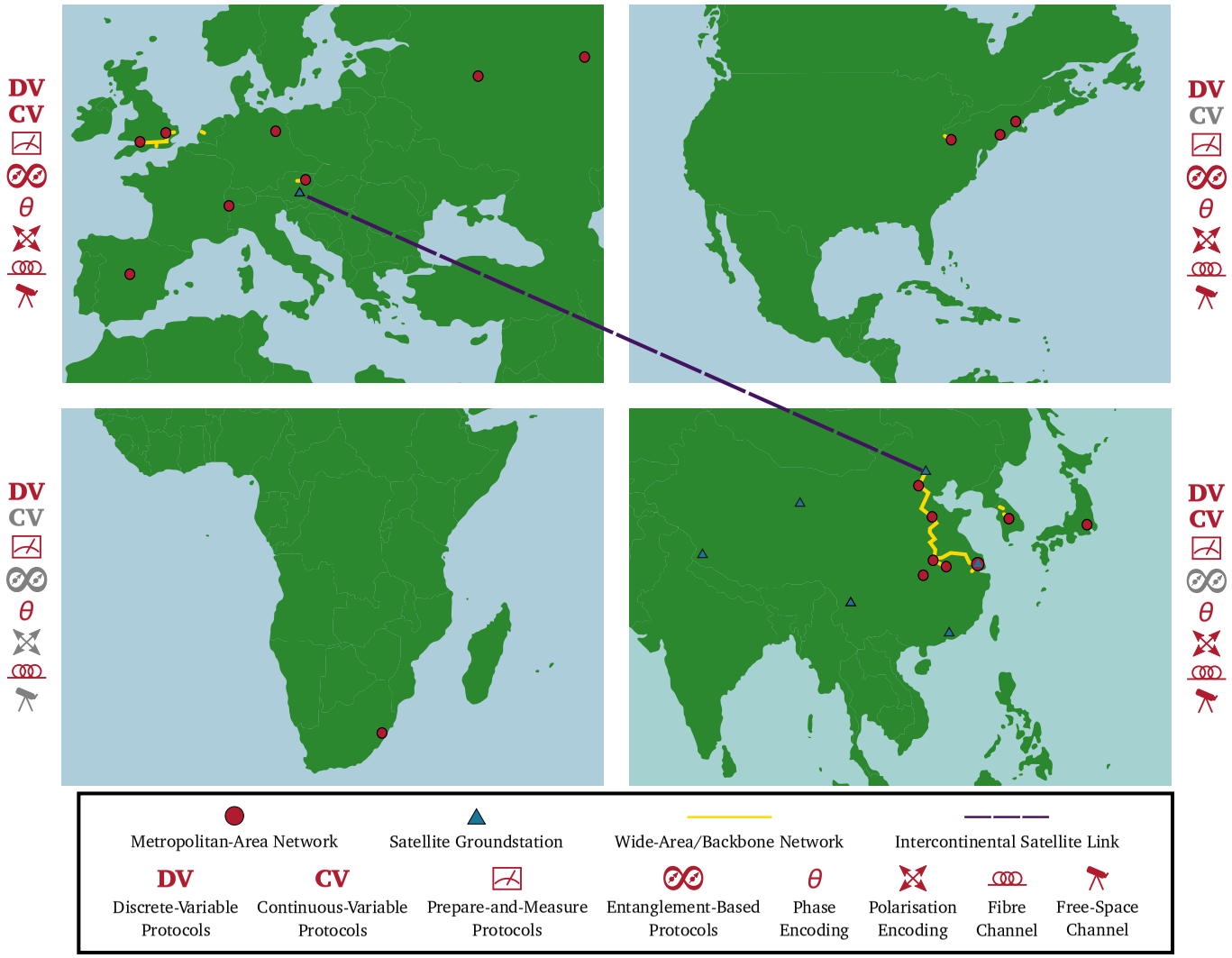


FIGURE 3.2: Showing the distribution of publicly-known quantum networks throughout the world, along with the types of technology that have been implemented on each continent. As of the present time, all rely on trusted nodes for links over which Alice and Bob cannot establish a direct connection [114–144].

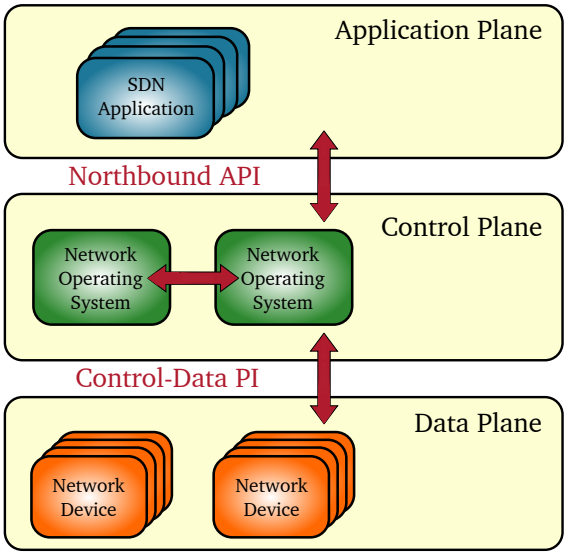


FIGURE 3.3: Illustrating the separation between the control plane and the data plane in software-defined networks, with higher-level applications sitting over the top. In small, isolated environments, only a single operating system may be required, however more generally, the controller must communicate with its peers in addition to accepting requests from the application layer and setting flow rules on network devices. Of these features, the latter two are managed through the northbound application programming interface (API) and the control-data programming interface (PI) respectively.

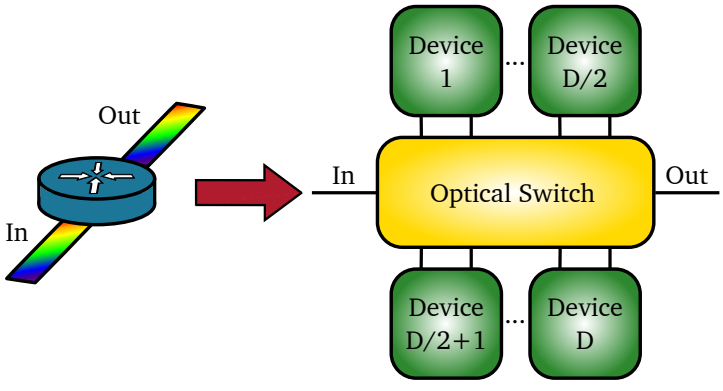


FIGURE 3.4: The internal structure of a single node in a software-defined network. All devices "hang" off a central switch, allowing them to be combined in any arbitrary configuration, tailored according to the transmission.

3.1.3 Next-Generation Quantum Networks

The networks to which this chapter contributes are both hosted on pre-existing hardware, with a software-defined architecture. In the following section, we summarise the topology and physical characteristics of each.

The Bristol Quantum Network

Built around the Bristol is Open (BiO) metropolitan-scale SDN, the Bristol Quantum Network is a primary target for the developments presented herein. Although still a research platform, BiO was designed for prototyping a wide range of technologies, and is representative of future commercial infrastructure. Therefore, any requirements imposed by QKD have not been taken into consideration as part of its design, making it the perfect testbed.

The physical topology is shown in figure 3.5, covering three key areas of Bristol: the university, the city centre, and the railway station. The Centre for Nanoscience & Quantum Information node was added as part of this work, and matches the rest of the network in terms of core equipment. Each link is actualised using a bundle of 144 single-mode fibres (SMFs), and while only a small subset of these are available for each application, the demand-to-capacity ratio was initially low enough that it was possible to run the quantum and classical signals down separate fibres. The nodes are all-optical, with each one centred around an OpenFlow-compatible Polatis switch (see sections 3.2.2 and 3.4.1 for more information).

The first quantum-encrypted message was transmitted over the network at 12:49:19 on 26th January 2016, as detailed in section 3.4.1. After this, responsibility was passed to other researchers who have continued its growth.

The United Kingdom Quantum Network

The UK Quantum Network is underpinned by Aurora2, part of the National Dark Fibre Infrastructure Service, an Engineering and Physical Sciences Research Council National Research Facility. This exists to enable the development of future internet technologies prior to their deployment across government and civilian networks. It passes through Telehouse, a critical internet hub and host of the London Internet Exchange [153]. The quantum layer is a collaboration between the University of Bristol, University of Cambridge, University of York, Toshiba Research Europe Ltd (TREL) and BT (formerly known as British Telecom).

Like on BiO, each node contains a Polatis switch, enabling Aurora2 to be operated as an SDN. However, each link is constructed from only two SMFs, meaning that without a scalable approach to enable the coexistence of classical and quantum signals on the same fibre (see section 7.4.2), we are limited to distributing quantum key during pre-allocated time slots.

Figure 3.6 presents a map of the UK Quantum Network. The Cambridge metropolitan section and the link connecting it to Martlesham Heath have both been officially launched [154, 155], where

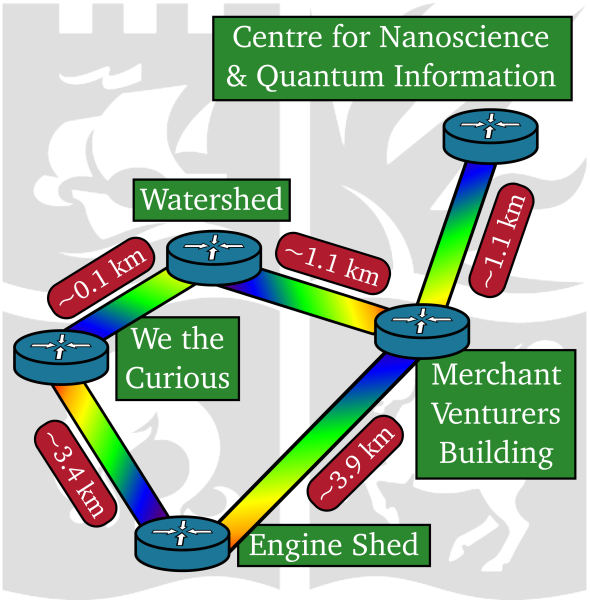


FIGURE 3.5: Physical topology of the Bristol Quantum Network.

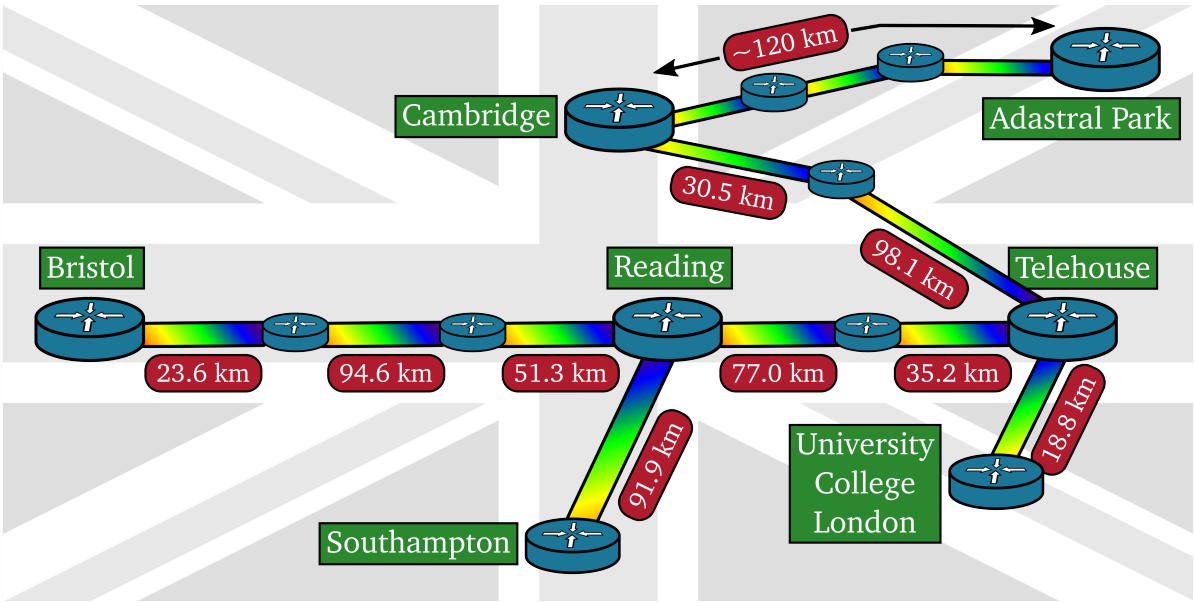


FIGURE 3.6: Physical topology of the UK Quantum Network. The nodes in Southampton and University College London are part of the underlying Aurora2 infrastructure, however they contain no quantum hardware and would need to rely on the work of chapter 6 to communicate with the main backbone in a quantum-safe manner.

the latter of these is a commercial-grade extension to Aurora2, built by BT in collaboration with the University of Cambridge, the University of York, ID Quantique, the National Physical Laboratory and ADVA. Connections on the Bristol-to-Cambridge backbone are still under development, although QKD has been attempted by the author between Bristol and the next-nearest node. Unfortunately, a university firewall prevented the classical QKD channel from being established via the internet, however a solution that has since been developed for the Bristol Quantum Network should also be applicable here, transmitting the public announcements using optical transceivers multiplexed into the data line. Despite issues surrounding the generation of key, it was still possible to successfully characterise the optical link, observing negligible cross-talk and negligible dark counts on both available fibres, with losses of 8.70 and 9.61 dB. These measurements were performed using a continuous-wave laser, scanning between 1530 and 1560 nm in 10 nm steps, with a launch power of -0.97 dBm. The intrinsic dark count of the detector was $(97.0 \pm 0.1) \times 10^3$ counts/s, and it is relative to this that we define a negligible result.

3.2 A First-Generation Testbed for Quantum Key Distribution on Software-Defined Networks

Before any device is installed on a third-party network, there must be sufficient evidence that it will not introduce security holes, performance issues or, in the worst case, generate a conflict that causes a catastrophic failure. To test the compatibility of both new and well-developed quantum technologies with SDNs, an experimental laboratory testbed was built based on BiO (see figure 3.7). It is intended to be used for the last stage of development prior to systems being deployed in the field, although during the infrastructure testing phase it contained only commercial QKD devices that are known to work reliably on their own.

In this section, we first introduce the ID Quantique Clavis^2, with which a quantum link can be established. In section 3.2.2, we present the optical switch that is central to each node on BiO, and demonstrate how it affects the Clavis^2. Section 3.2.3 describes how classical information is transmitted over the network, and section 3.2.4 covers some common devices that are incompatible with QKD at the present time, quantifying their impact wherever possible.

3.2.1 The Clavis^2 Quantum Key Distribution System

The ID Quantique Clavis^2 [156, 157] is a researcher-targeted version of the Cerberus “plug & play” fibre QKD system, capable of automatically compensating for polarisation mode dispersion; an effect that arises when imperfections in the fibre core disrupt the cross-sectional symmetry, causing different polarisations to propagate at different speeds. Figure 3.8 is a simplified representation of the internal optical circuit, and a chronology of operation is given by protocol 3.1. To summarise, Alice receives a pair of pulses, one early and one late. She encodes the former in either the $\{0, \pi\}$ or

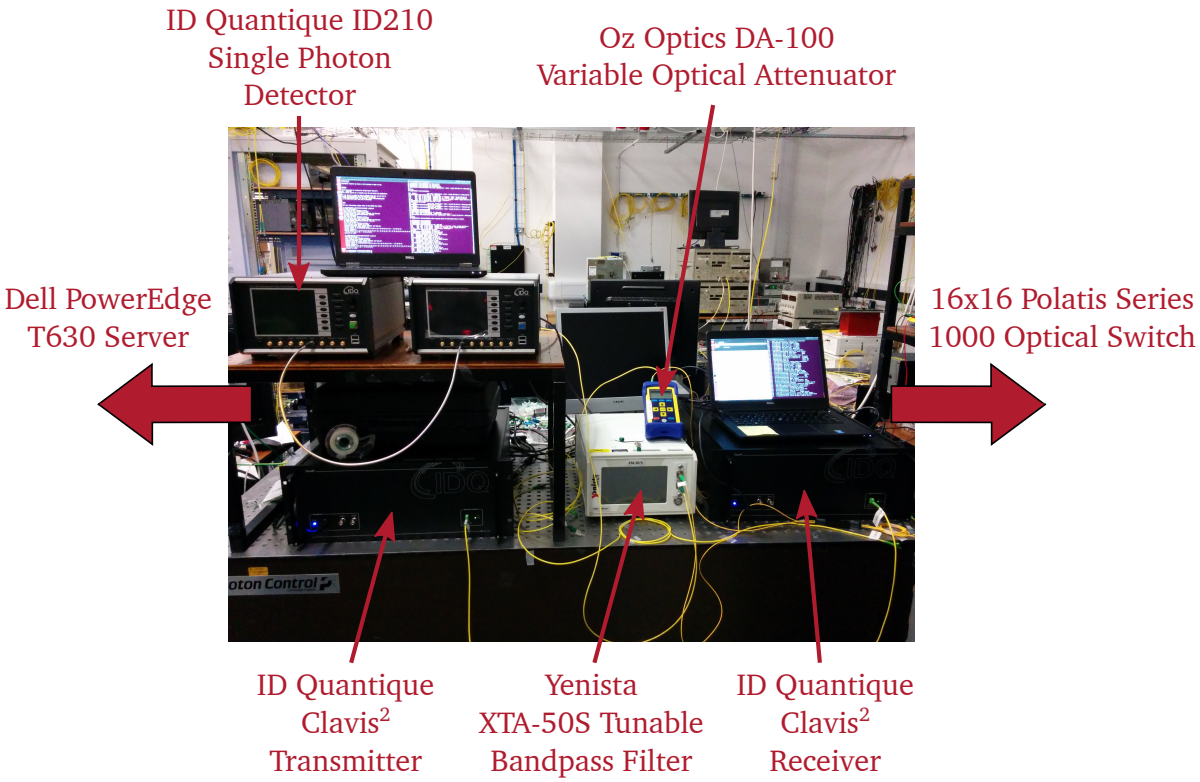


FIGURE 3.7: Part of the first-generation testbed, capable of emulating any configuration of the Bristol Quantum Network. The erbium-doped fibre amplifier and programmable optical processor were loaned from other projects, so are not shown. Similarly, the server and switch were shared between multiple experiments, so are rack-mounted elsewhere in the laboratory. The filter and detectors were used for characterising fibre links, both locally and in the field.

$\left\{\frac{\pi}{2}, \frac{3\pi}{2}\right\}$ basis. Bob measures by applying a $\frac{\pi}{2}$ phase shift to the late pulse or by leaving it untouched. From equation 2.62,

$$\alpha = \begin{cases} |\alpha|, & \text{for } \theta = 0 \\ -|\alpha|, & \text{for } \theta = \pi \\ \mathbb{i}\,|\alpha|, & \text{for } \theta = \frac{\pi}{2} \\ -\mathbb{i}\,|\alpha|, & \text{for } \theta = \frac{3\pi}{2} \end{cases} \tag{3.1}$$

Therefore, if Alice transmitted $\theta = 0$, only detector 1 will click, as evidenced by equations 2.71, 2.72 and 2.73, and assuming that Bob measured in the $\{0, \pi\}$ basis. Similarly, if Alice transmitted $\theta = \pi$ and Bob's measurement choice remains unchanged, the click will be in detector 2. When sampling from $\left\{\frac{\pi}{2}, \frac{3\pi}{2}\right\}$, a click in detector 1 corresponds to Alice sending $\theta = \frac{\pi}{2}$, while a click in detector 2 indicates $\theta = \frac{3\pi}{2}$ was chosen. If Alice and Bob's bases do not match, it is equally probable that

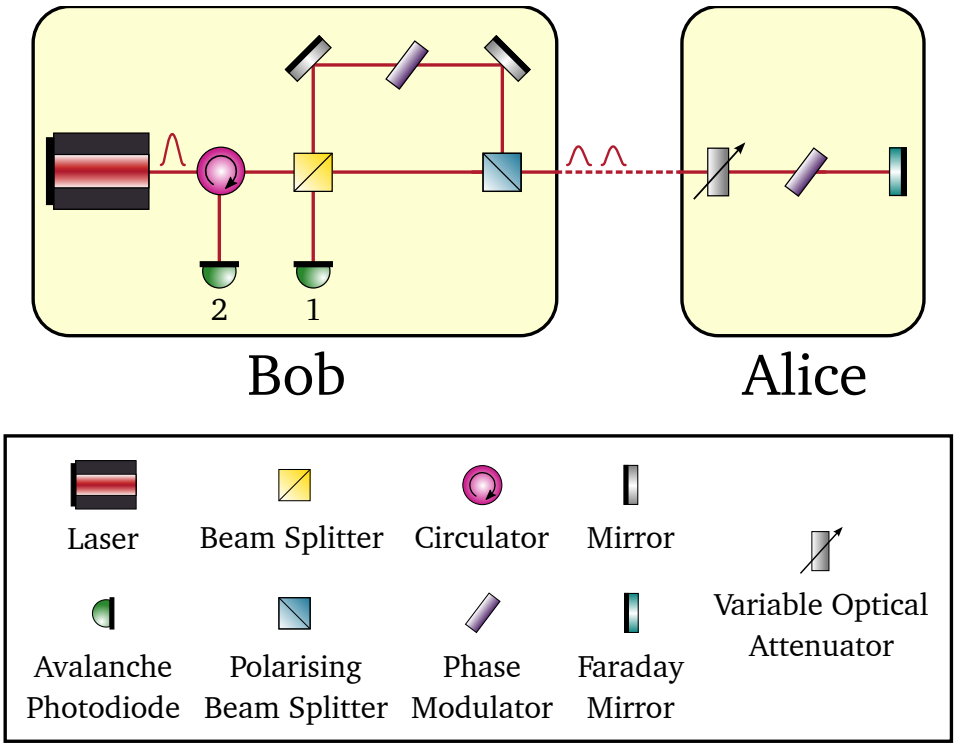


FIGURE 3.8: Optical schematic for the ID Quantique Clavis^2. Although bulk notation has been used, the actual implementation is in fibre. Classical detectors (not shown) are used to synchronise the two devices and detect Trojan Horse attacks. Based on figure 4.1 in [156].

only detector 1 or detector 2 will click, and there is also a chance of a coincidence. Of course, these results are handled in the sifting step.

At the cryptographic level, the Clavis^2 relies predominantly on Scarani-Acín-Ribordy-Gisin 2004 (SARG04), which is described in protocol 2.6. However, for attenuations ≤ 3 dB, it falls back on BB84 (protocol 2.5) as, in this region, SARG04 is not proven secure. The secret key rate and quantum bit error rate (QBER) both depend on loss, as illustrated by the experimental data in figure 3.9, which was taken after Alice and Bob had become fully integrated with the testbed, leading to a 2 dB lower bound on the attenuation. The optical link is characterised as part of the first key generation round, meaning the initial secret key rate is lower than those returned thereafter, and this is not included in the average for each data point. A range of tests are carried out during the characterisation process, measuring features such as the line length and quantum visibility. The Clavis^2 transmits in the C-band (see table 3.2), with an exact wavelength of 1551.7 nm as standard, and occupies 4U in a 19 inch rack, where $1\text{U} = 1.75$ inches.

Protocol 3.1: Plug & Play [156]

SUMMARY: Hardware protocol adhered to by the ID Quantique Clavis^2 QKD system.

1. *Preparation of Strong Laser Pulses.*
   (a) Bob generates a 5 MHz train of bright laser pulses.
   (b) Each pulse is split by a 50:50 beam splitter, which directs the two halves into paths of differing lengths.
   (c) The polarisation of the half-pulse in the long arm is rotated by $\frac{\pi}{2}$.
   (d) The two half-pulses are incident on a 50:50 polarising beam splitter, offset from one another in time due to the difference in their travelled path lengths. Both are output through the same port as a result of the polarisation rotation imparted by the long arm, leaving the Bob unit and heading towards Alice.
2. *State Preparation on Weak Coherent Pulses.*
   (a) As each pair of half-pulses arrives at Alice, 90% of the power is diverted to classical detectors for the purposes of synchronisation and Trojan Horse protection (see attack 3.1). Figure 3.8 omits this step.
   (b) The half-pulses are reflected by a Faraday mirror, rotating their polarisations by $\frac{\pi}{2}$.
   (c) A phase is applied to the later half-pulse in each pair, randomly and uniformly selected from $\left\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\right\}$.
   (d) The light is attenuated into a set of weak coherent pulses before leaving the Alice unit and heading back to Bob.
3. *State Measurement.*
   (a) Bob's polarising beam splitter sends the early weak coherent pulse down the long arm, and the late weak coherent pulse down the short arm, as a result of the rotation imparted by the Faraday mirror.
   (b) A phase is applied to the long arm, randomly and uniformly selected from $\left\{0, \frac{\pi}{2}\right\}$.
   (c) The two weak coherent pulses arrive on the beam splitter at the same time, interfering with one another. In the case where Alice and Bob both sample from $\{0, \pi\}$, only a single detector will click. Bob can establish which phase Alice sent by analysing the output port in which the detection event occurs. If they both chose $\left\{\frac{\pi}{2}, \frac{3\pi}{2}\right\}$, the outcome is analogous. If their bases do not match, the measurement outcome is discarded.

Attack 3.1: Trojan Horse. *Eve fires a bright laser into Alice and detects the backreflections. From this, she gains enough information to perform a successful intercept-resend (see attack 2.3) or read off the bit values directly [158–160].*

3.2.2 The Polatis Optical Switch

Central to the testbed was an OpenFlow-compatible Polatis Series 1000 optical switch with 16 input/output pairs [162]. Inside, are two banks of collimators, each containing 16 segments that

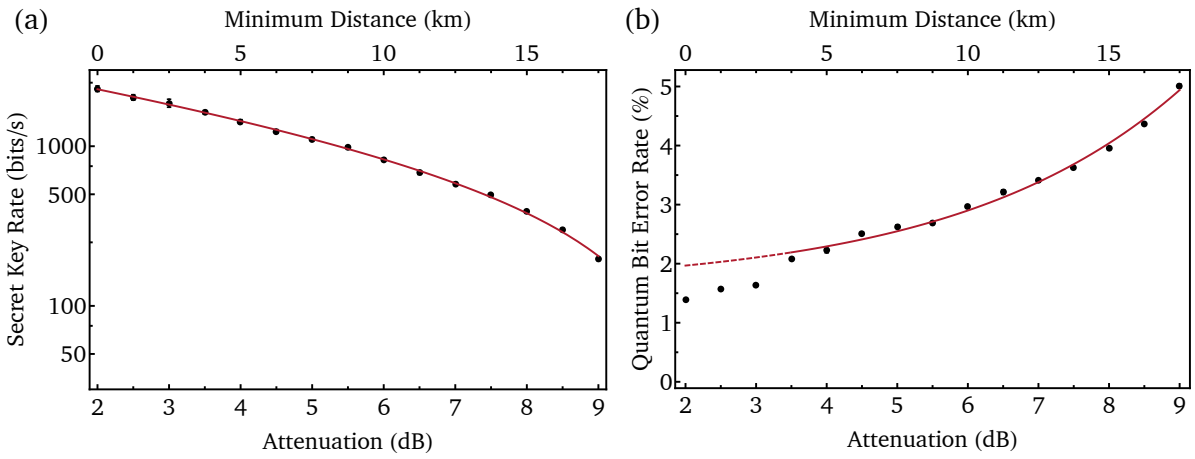


FIGURE 3.9: Showing how (a) the secret key rate and (b) the quantum bit error rate changes with loss for the ID Quantique Clavis^2. Here, connections are established through a variable optical attenuator, and the equivalent fibre lengths are calculated assuming a transmission loss of 0.4 dB/km, the worst-case value given by [161]. Each pass through the optical switch contributes 1 dB of loss, resulting in an extra 2 dB of attenuation across all cases.

TABLE 3.2: Wavelength bands for optical communications, using the values given in [60].

Band	Wavelength (nm)
O (Original)	1260-1360
E (Extended)	1360-1460
S (Short)	1460-1530
C (Conventional)	1530-1565
L (Long)	1565-1625
U (Ultra-Long)	1625-1675

can be aligned using piezoelectric actuators. Light is coupled between the two such that any input can address any output, as summarised in figure 3.10. This is known as DirectLight beam steering, and provides a lower-loss, lower-noise alternative to the techniques used in traditional 3D microelectromechanical system (MEMS) switches.

Figure 3.11 shows the impact of the Polatis on the secret key rate and QBER of the Clavis^2. Each pass through the switch contributes 1 dB of insertion loss, although the quantum signal appears to suffer no other ill effects. The duration of each key generation round varies slightly as a result of small environmental fluctuations, such as vibrations in the vicinity of the fibre. This affects both the amount of post-processing that needs to be performed and the time taken to reach the finite key limit, the latter of which is dependent on loss.

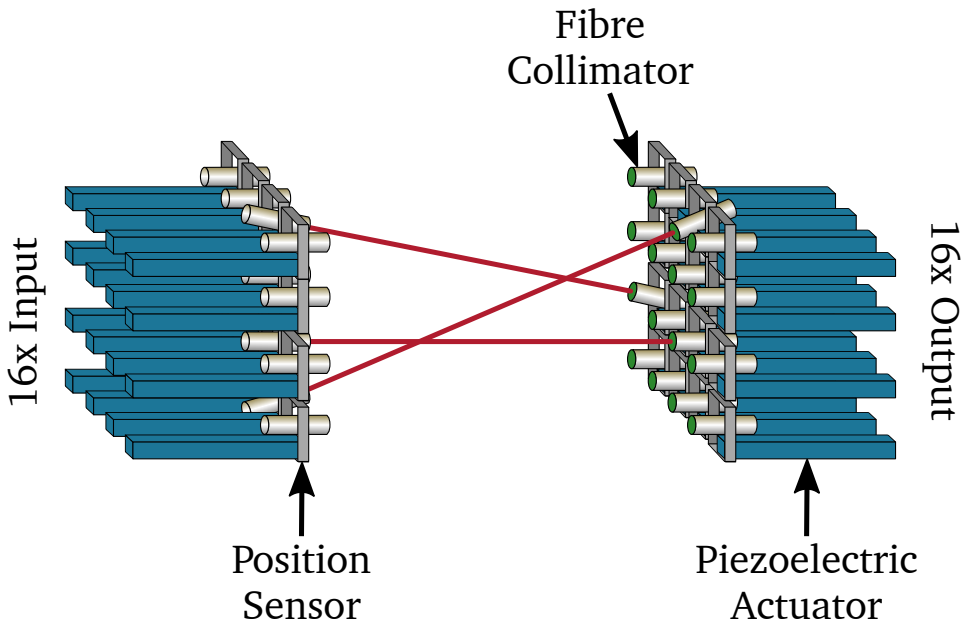


FIGURE 3.10: The internal structure of a Polatis optical switch. Each input port connects to a fibre collimator, and a piezoelectric actuator aligns this with the collimator corresponding to the desired output. Based on the DirectLight figure in [163].

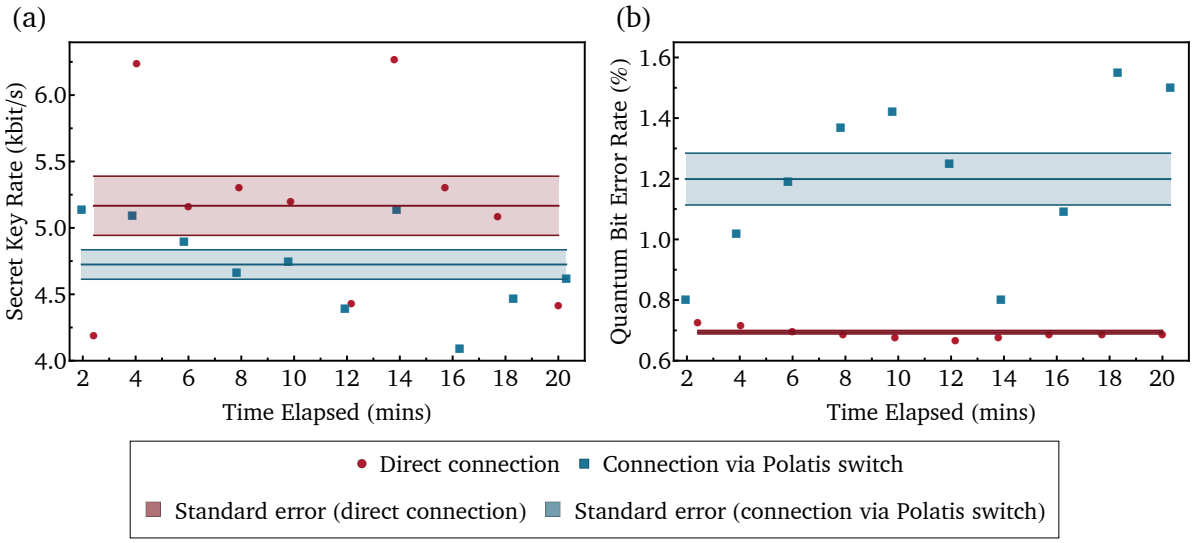


FIGURE 3.11: Showing how (a) the secret key rate and (b) the quantum bit error rate of an ID Quantique Clavis^2 changes depending on whether or not the quantum channel passes through a Polatis switch. Each data point is a single, self-contained round of quantum key distribution, including all post-processing and error analysis. The coloured regions represent the standard error on the mean, and the variations in the time elapsed are a reflection of the time taken to reach the finite key limit.

3.2.3 SFP+ and QSFP+ Transceivers

The classical optical links were established using a mixture of enhanced small form-factor pluggable (SFP+) and enhanced quad small form-factor pluggable (QSFP+) fibre transceivers, which provide data rates of 10 Gbit/s and 40 Gbit/s respectively. SFP+ modules use 64B/66B encoding [164], generating one 66-bit block for every 64 bits of data. The additional control bits ensure the sender and receiver remain synchronised by introducing guaranteed bit transitions for every block, which safeguards clock recovery [165]. This is important for schemes like Non-Return-to-Zero, that do not send a rest condition in between each bit, meaning Alice and Bob's clocks can drift if a long string of successive ones or zeros is transmitted. The QSFP+ specification gives six encoding options, including 64B/66B, Non-Return-to-Zero and Manchester Code [166], the latter of which represents zeros as low-high signals and ones as high-low, or vice versa depending on the convention followed.

Both transceiver types are hot-pluggable, meaning they can be introduced to the network without causing any downtime. The specific modules chosen for the testbed run at 1310 nm, minimising crosstalk-related noise in the quantum channel. They have a maximum range of 10 km without amplification, and those that are QSFP+ utilise 64B/66B, enabling them to communicate in a split configuration with 4× 10 Gbit/s transceivers if required.

3.2.4 Equipment that is Detrimental to Quantum Key Distribution

Unfortunately, not all network devices are as easy to integrate with QKD as the Polatis. Here, we consider the negative effects introduced by amplifiers and programmable optical processors, as well as exploring the unique ways in which SDNs can provide a resolution.

Erbium-Doped Fibre Amplifiers

Erbium-doped fibre amplifiers (EDFAs) contain a length of silica optical fibre to which Er^{3+} ions are introduced. Russell-Saunders notation $\left({}^{2S+1}L_J\right)$ can be used to represent the fine structure of the ion, where I indicates a value of 6 for the total electronic orbital angular momentum quantum number L, S is the total electronic spin quantum number, and J is the total electronic angular momentum quantum number, defined as [167]

$$J = |L-S|, |L-S|+1, \ldots, L+S \tag{3.2}$$

As illustrated in figure 3.12, a pump laser excites the ions from their ground state into ${}^4I_{11/2}$ which, with a lifetime on the order of 1 µs, rapidly transition to the metastable ${}^4I_{13/2}$ level through spontaneous emission. If a carrier photon in the range of 1550 nm now enters the EDFA, it will stimulate decay of the ion back to its ground state, emitting a photon at the same wavelength as the signal. The specified wavelength is inexact because the Stark effect from local electric fields splits each energy level into a manifold. The irregular structure of silica means the hyperfine energies depend on the location of each ion, so the EDFA's amplification region appears continuous [60, 168].

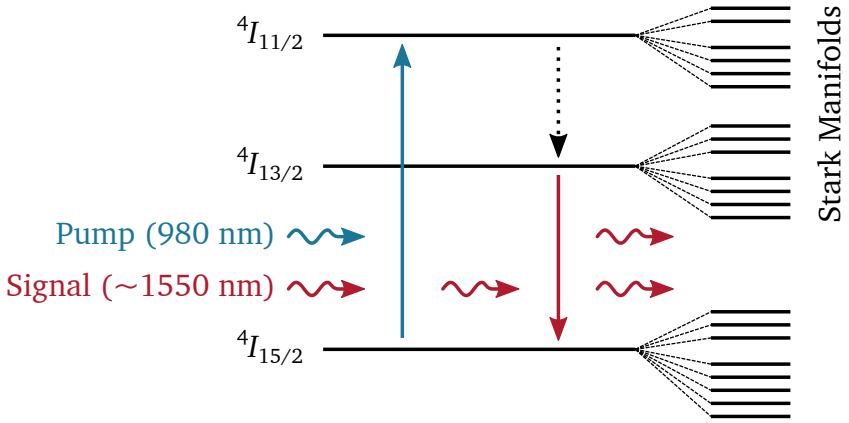


FIGURE 3.12: Illustrating the amplification process for Er^{3+}. A 980 nm pump excites the ion, which quickly decays into a metastable level. Hyperfine splitting is induced by local electric fields, enabling a range of carrier frequencies to be amplified through a process of stimulated emission back to ground.

It is well-established that amplifiers in general are incompatible with QKD by virtue of the no-cloning theorem and the minimum number of photons required for unambiguous state discrimination (see section 2.2.1). This is no bad thing. If perfect amplification of a quantum state were possible, it would destroy the security of QKD. However, it is clear from the above that if quantum signals do enter an EDFA, spurious photons will be generated at the carrier frequency. A simple solution would be to install a bypass for the quantum channel wherever an EDFA is present, but unfortunately, this alone is not enough to enable co-existence with classical communications in arbitrary networks.

In figure 3.13, we show that the noise profile of a Nortel Networks EDFA acting on a 1550 nm laser will easily overwhelm weak coherent pulses at dense wavelength-division multiplexing (DWDM) wavelengths. It should be noted that the author does not advocate spacing quantum and classical signals so closely in the same fibre core (see section 7.4.2 for further discussion). Yet some do see it as a way forward [169–171], and as the aim of this chapter is to begin the transition of QKD into minimally bespoke networks, it is an approach which must be considered. In addition, such a noise profile may be problematic if there is inter-core/inter-fibre crosstalk when using multicore/standard single-mode fibres.

The primary noise source is superluminescence [172], where spontaneously emitted photons are amplified through stimulated emission. Figure 3.13 shows that, when both signals are in the C-band, up to 57.24 dB of out-of-band suppression is required to filter superluminescence out, assuming the Clavis^2 can be approximated as a 5 MHz deterministic single photon source running at 1551.7 nm (i.e. it has an optical output power of -91.94 dBm).

It has previously been suggested that separating the quantum and classical signals into the C-band and O-band respectively would enable the hard-wiring of quantum bypasses wherever an inline EDFA is present, with a 1310 nm beam-dump to protect the quantum channel [173]. However, SDNs offer

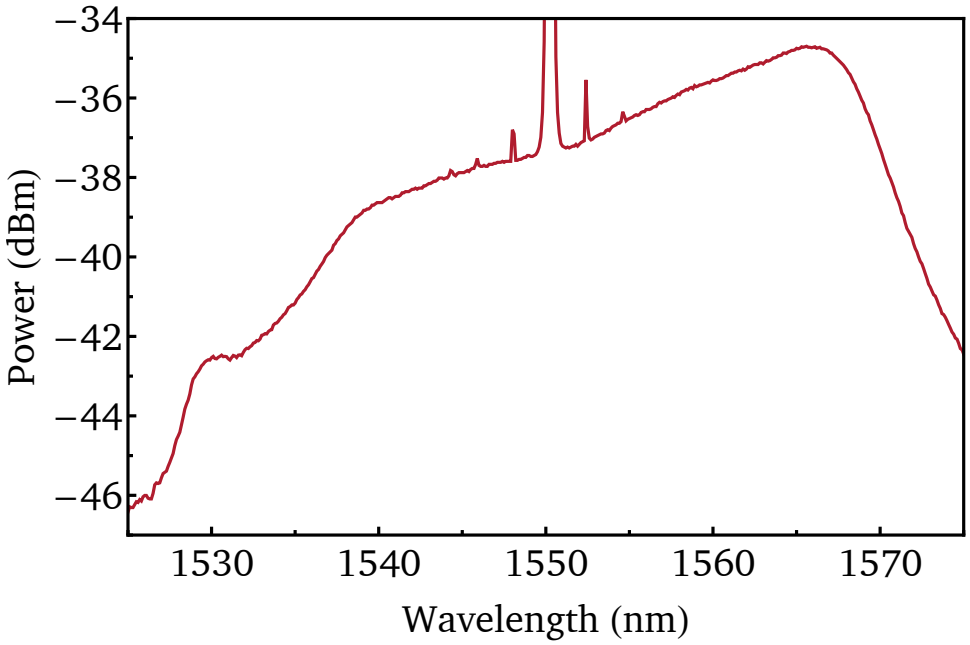


FIGURE 3.13: Noise profile for a Nortel Networks erbium-doped fibre amplifier, acting on a 1550 nm signal.

a simpler and cheaper solution. Their flexibility means amplification is no longer restricted to pre-defined locations, and switch-centralised nodes make it trivial to route around. From the perspective of the classical signal, amplifying before transmission is often synonymous with amplifying after, so under the condition that the classical power remains above the minimum threshold required by the EDFA, it is possible to avoid polluting quantum wavelengths with superluminescent photons. For links where amplification needs to happen prior to the classical light reaching its final destination, SDNs provide a way to intelligently separate it from the quantum channel, whether that involves commandeering fibres that are known to have minimal crosstalk, or sending the classical and quantum signals down different routes entirely.

Programmable Optical Processors

Programmable optical processors are multi-function instruments that can replace a range of devices, including filters, wavelength-selective switches and (de-)multiplexers. In BiO, the 4x16 Finisar Waveshaper 16000s [174] is used, designed around a liquid-crystal-on-silicon optical processor; a type of spatial light modulator. The optical schematic for a 1x4 version is shown in figure 3.14, and figure 3.15 illustrates the impact on a Clavis^2 when it is forced to pass through a Waveshaper configured to act as a bandpass filter that is centred on the quantum channel. The dominant cause behind an increase in the QBER is the Waveshaper's $\sim$ 4.5 dB insertion loss. Naturally, this also leads to a drop in the key rate, meaning it takes longer to reach the finite key limit, which is why there

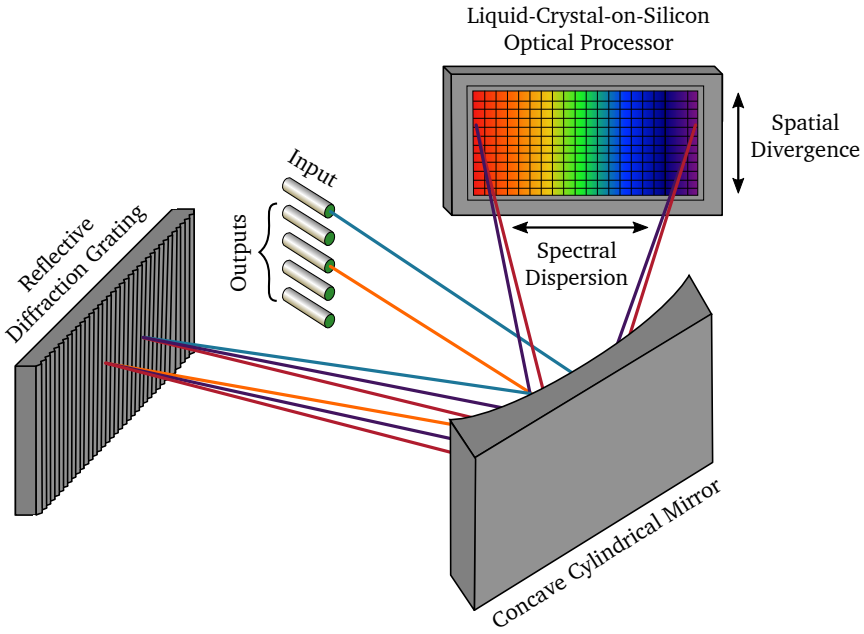


FIGURE 3.14: The internal structure of a Waveshaper programmable optical processor. Each input can be de-multiplexed over four output ports, with additional filtering or signal modulation as required. Based on the schematic in [174].

is a significant difference in the times elapsed for each scenario. From the perspective of classical-quantum co-existence, these effects are not particularly concerning so long as the Waveshaper is used only for classical processing. The kind of noise profile we experience with an EDFA is not present here, so the SDN can simply route quantum signals around any programmable optical processors that are installed in a node. However, in some circumstances, we may wish to wavelength-division multiplex several quantum channels (see chapters 4 and 7). Here, we are unable to take advantage of the general-purpose Waveshaper, so conventional multiplexing technologies must continue to be used.

3.3 Time-Division Multiple Access Quantum Key Distribution

Time-division multiple access (TDMA) is an allocation mechanism that originated in mobile networks for sharing a single base station amongst multiple terminals [175], and has since spread into wired home networks [176]. A time-scheduling algorithm sorts each terminal into one or more non-overlapping slots that can each accommodate a single connection at most. The exact outcome will be decided by factors such as data rates and the number of units requesting base-station access.

In more generic communications networks, where master-slave relationships do not necessarily exist, the situation is less simple, as devices may wish to communicate with multiple partners in quick succession, rather than a lone, centralised hub. Furthermore, application of TDMA techniques

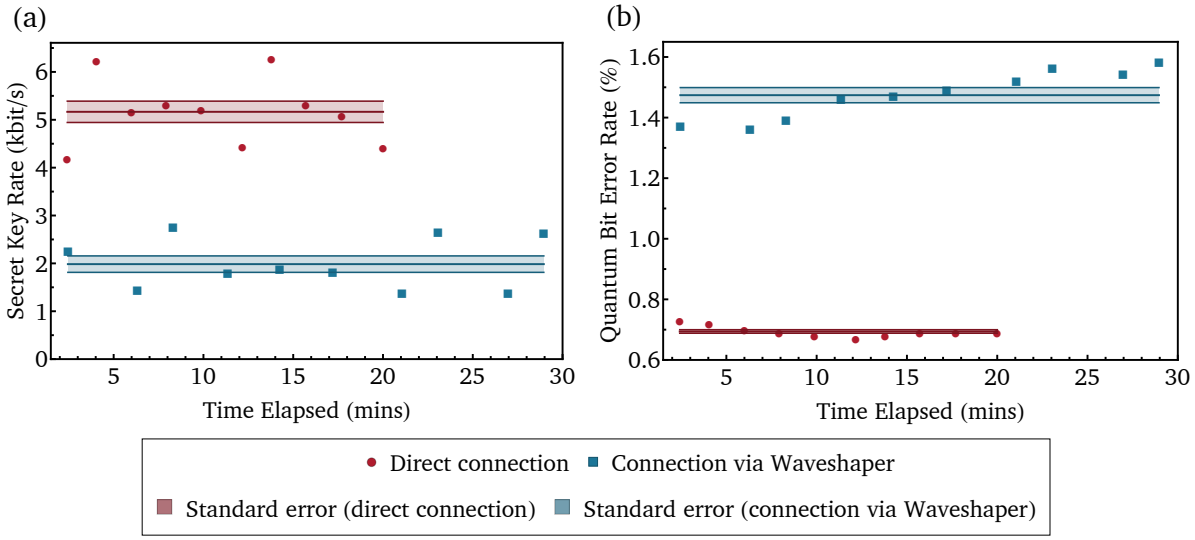


FIGURE 3.15: Showing how (a) the secret key rate and (b) the quantum bit error rate of an ID Quantique Clavis^2 changes depending on whether or not the quantum channel passes through a Waveshaper programmable optical processor. Each data point is a single, self-contained round of quantum key distribution, including all post-processing and error analysis. The coloured regions represent the standard error on the mean, and the variations in the time elapsed are a reflection of the time taken to reach the finite key limit.

to quantum signals will require additional flexibility, as unforeseen changes in key rate could be induced by environmental factors. Luckily, this kind of malleability is exactly what SDNs pledge to provide.

In the following section, we use our newly-built testbed to emulate an arbitrary link on BiO, carrying out both the first demonstration of TDMA-QKD and the first experimental integration of QKD with an SDN. We begin by outlining the time-sharing scenario, before moving on to discuss the configuration of the emulator. We conclude with the results of the experiment, discussing ways in which the performance could be further improved.

3.3.1 A Time-Sharing Model for Cost-Effective Quantum Key Distribution

One of the greatest barriers to widespread deployment of QKD is its financial cost, which is in the region of £100,000 per system. Therefore, to keep spending at a minimum, each network node will ideally contain a single transmitter or receiver, shared between every possible connection. However, without some form of time-scheduling, this will be impossible to manage as networks grow and the demands on each device increase. Additionally, the complexity introduced by user requirements cannot be managed through a fixed-ratio split between each connection.

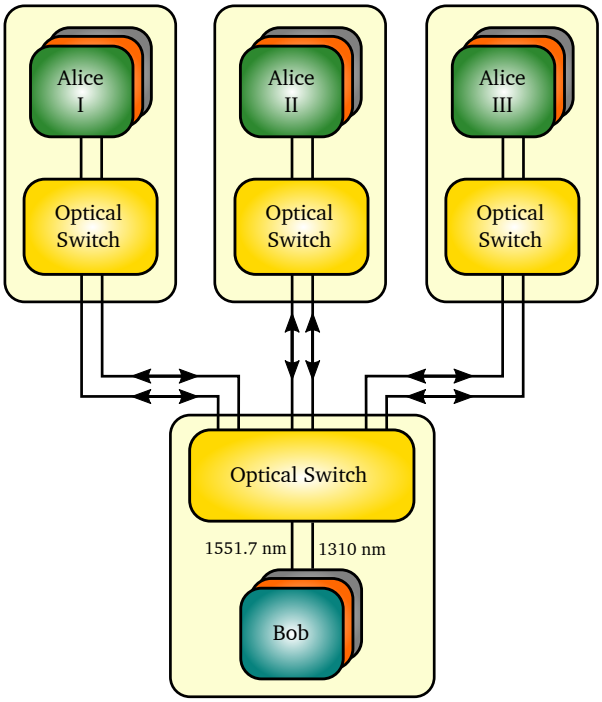


FIGURE 3.16: A logical diagram of the time-sharing setup. Alice I, II and III are realised by a single physical unit that can alternate between multiple initial secret keys. Similarly, the three optical switches are emulated using only one device.

In figure 3.16, we show a logical TDMA configuration, which will be the subject of our emulation. For a "plug & play" system like the Clavis^2, the most expensive components are contained within the receiver unit, so it makes sense in this scenario to have multiple Alices sharing a single Bob. In reality, it is likely that each transmitter will also want to communicate directly with multiple receivers, however this layout is adequate for the benefits we wish to demonstrate.

It is worth noting that, for sufficiently complex networks to which the latter situation applies, the economic impact of choosing which nodes contain an Alice and which nodes contain a Bob may be non-trivial to calculate. A simple example is given in figure 3.17, where uncertainty over the future network topology leads to a dilemma. Even when no ambiguity exists, the optimum configuration is still an interesting problem for networks with large numbers of highly interconnected nodes, though further exploration is outside the scope of this thesis.

The keys generated over each TDMA connection are used to secure the dissemination of virtual network functions. These are a complementary technology to software-defined networking, and replace specialised network hardware with software running on generic servers, instantiating critical services such as firewalls [177]. While network function virtualisation is a central part of BiO, it is also frequently used in data centres where, for distances of up to 10 km, classical information is often transmitted at 1310 nm [178, 179], increasing the potential for commercial 1550 nm QKD devices to be multiplexed with pre-existing technologies straight out of the box. This means the

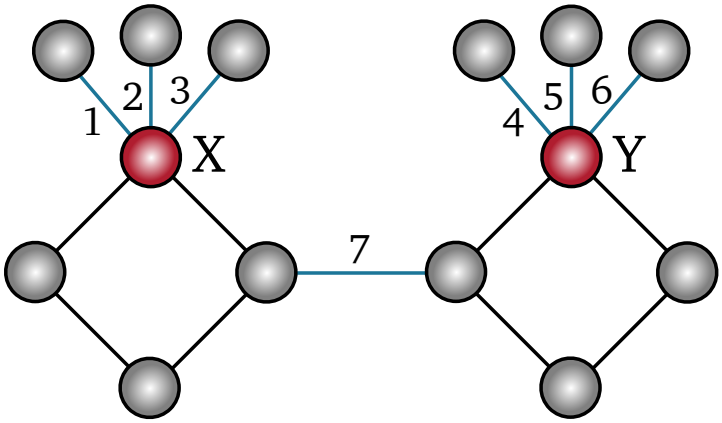


FIGURE 3.17: Consider a pair of long-distance four-node ring networks. Some combination of links 1-7 will be added in the future, however the exact plans are unclear. The simplest two outcomes are for only links 1-6 or only link 7 to be built. In the first case, nodes X and Y should both contain Bobs, for the reasons outlined in this section. In the second case, node X should contain an Alice and node Y should contain a Bob (or vice versa), to ensure the nodes at either end of link 7 can operate with only a single transmitter or receiver in each. However, at the time of initial construction, there is no way of knowing which situation to prepare for, and the only way forward is to apply some form of risk-reward analysis. As the number of combinations and the size of the network increases, so does the complexity of minimising deployment costs, even if all future expansions are pre-determined. For critical pieces of infrastructure, it may not be possible or worthwhile to reconstruct every node if a suboptimal design has been implemented from the beginning.

work we present here has consequences that reach far beyond the Bristol Quantum Network.

3.3.2 Bristol is Open Emulator

With the experiment defined, our next step is to configure the testbed such that it accurately emulates an all-optical SDN. Each node of BiO contains a Series 6000n Polatis switch [180], which is nothing more than a higher-capacity version of the Polatis in our testbed. Therefore, we can set this to route light through spools of SMF-28e fibre and back into itself, as a way of representing multiple nodes in a network. It is over these links that Alice and Bob's quantum channel can be established.

Different fibres were used for each time-share, with lengths of 5 km, 15 km and 25 km, which corresponds to attenuations of 4 dB, 9 dB and 10.5 dB. These were chosen purely based on their availability, rather than because they could be used to model a specific link, and for the most part their loss per km exceeds typical levels due to stresses induced by long-term (mis)use across a large number of experiments. Thus, while real fibre was useful for demonstrating TDMA-QKD, an Oz Optics DA-100 variable optical attenuator was also connected to the Polatis to get a full range of results.

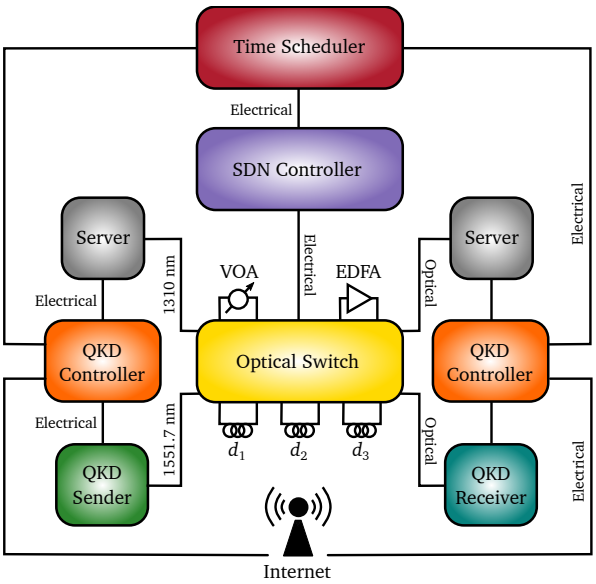


FIGURE 3.18: A physical diagram of the emulator, based on a Bristol is Open node. The virtual network function servers have data storage, software encryption and data transmission capabilities, drawing key from the QKD controller. d_1, d_2 and d_3 are 5 km, 15 km and 25 km long, with attenuations of 4 dB, 9 dB and 10.5 dB respectively. Light can also be routed into a variable optical attenuator (VOA) or erbium-doped fibre amplifier (EDFA). The SDN controller communicates using OpenFlow messages through OpenDaylight.

The classical channel for QKD (referred to as the classical QKD channel hereafter) was created via the internet, so as to reduce the number of connections into the switch, thereby leaving room for future expansion. As already discussed in section 3.1.3, it transpired that this approach did not work when applied to field trials between the University of Bristol and third-party nodes, so the internet connection was eventually superseded by an additional optical link. It is common for data centres to transmit classical signals in the O-band, so the transceivers outlined in section 3.2.3 are adequate for our experiment.

Figure 3.19 shows the interaction of the various software components within the emulator. The time scheduler runs in the application plane (see figure 3.3), taking responsibility for determining when Alices I, II and III should be allowed to communicate with Bob, according to both the amount of key still available on each link and rates of attrition. It differs from a classical time scheduler in that it must react according to changes in environmental conditions that affect the raw key rates. For this experiment, we chose to wait until at least one round of QKD had concluded before allowing a connection to be terminated, rather than defining the width of the time slot in advance. An alternative approach would be to switch to another link at the end of a fixed window and, if key generation is incomplete, use a dynamic priority list in the scheduler to resume the session at a later point. While this prevents other links from running out of key, an avenue that could otherwise be

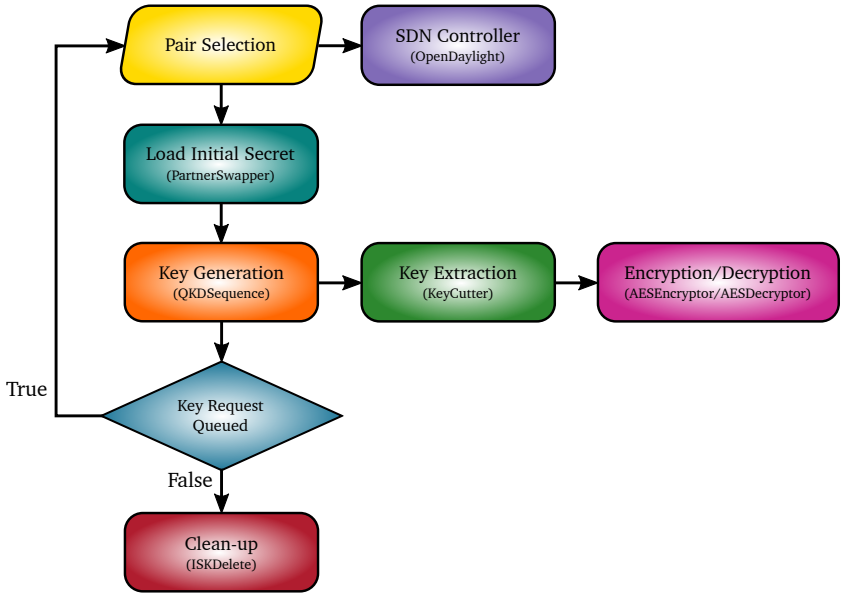


FIGURE 3.19: Workflow for the software layer of time-division multiple access quantum key distribution.

exploited by an attacker looking to denial of service (DoS) the entire network, it introduces greater complexity on the device side, as a mechanism is required for QKD session resumption. In either case, monitoring the raw key rate in real time means the SDN can reconfigure the quantum path to circumvent any bottlenecks, subject to the topology of the network.

Information on the desired Alice-Bob pairing is fed to both the SDN and QKD controllers. Of these, the former was implemented by a collaborator, along with the programming of the time scheduler, so no further details will be provided herein. During key generation, Alice and Bob must authenticate each other using an initial secret key that is stored at an access point on the QKD controller. To allow for partner swapping over an arbitrary number of links without modifying any device-specific software, PartnerSwapper was written. This is a C++ program that cycles Bob's initial secret key depending on which Alice he needs to communicate with, drawing on a dedicated key store. Keeping the shared secret separate from other keys on the system ensures it does not accidentally get used for a different purpose, which would then prevent the store from being replenished after it empties.

The Clavis^2 is controlled by the QKDSequence program, provided by ID Quantique. It also implements all the necessary post-processing, however to use the key as part of a separate application, a programme had to be written that extracted it using the proprietary IDQ3P protocol [181]. This was fed via a key store to the Advanced Encryption Standard running in Galois/Counter Mode (AES-GCM) which, for the work in this thesis, was implemented using OpenSSL, a free and open-source C++ library made available under the Apache License Version 2.0.

If enough key has been generated to terminate the quantum link, and no other requests are

queued, ISKDelete will remove the initial secret key from the access point to ensure it is never reused. This is not strictly necessary so far as functionality is concerned, because PartnerSwapper will overwrite anything already stored there. However, from the perspective of trying to minimise unforeseen exploits, it is an important addition.

3.3.3 Results

Using the setup just described, TDMA-QKD was successfully implemented. Three virtual network functions were securely delivered over spools of optical fibre to separate emulated servers, using in-flight encryption with a 256-bit quantum key. Over an attenuation equivalent to the 10 km maximum range of a 1310 nm data centre network, the Clavis^2 generated 34.8 ± 0.3 kB of secret key. In contrast, the largest virtual network function was 15.9 GB, meaning 457,569 rounds of QKD would have been required if the one-time pad (OTP) had been used as the encryption scheme instead of AES-GCM. From the key rates in figure 3.9, this would have taken over four years to complete, requiring the author to apply for a significant extension to his PhD.

Of course, in the TDMA scenario, links are unlikely to remain active for more than a few rounds, and so the average initialisation time of the Clavis2 will have a greater impact on the performance of the network than would otherwise be expected. The initialisation time is defined as how long it takes for the first key to be generated once the QKD controller has received a command to open a quantum channel, as plotted in figure 3.20. We also calculate a theoretical lower bound, for the situation where the characterisation data from a previous connection can be used without detriment, allowing the hardware measurements to be skipped at launch. For attenuations greater than 9 dB, key generation starts to become intermittent, so while a quantum-secure link can be established for up to 10 dB of loss, the initialisation time is no longer a reliable figure of merit.

Another point to consider is how many Alices can be sustained by a single Bob. Consider the case where the Clavis^2 carries out one round of QKD, generating $|k|$ secret bits. Then, for a block cipher that takes a $|k_C|$-bit key as input, the number of encryption keys generated over a single link will be

$$K_{\max} = \left\lfloor \frac{|k| - |k_{\text{init}}|}{|k_C|} \right\rfloor \tag{3.3}$$

where $|k_{\text{init}}|$ is the length of the initial shared secret and $\lfloor \cdot \rfloor$ is the floor function. In the special case of the Clavis^2 paired with AES-GCM encryption, $|k_{\text{init}}| = |k_C| = 256$. Therefore,

$$K_{\max} = \left\lfloor \frac{|k|}{|k_C|} \right\rfloor - 1 \tag{3.4}$$

If the block cipher can encrypt $|m|_{\max}$ bits of data under a single key then the total number of bits that can be encrypted after one round of QKD is

$$|m|_{\text{total}} = K_{\max} |m|_{\max} \tag{3.5}$$

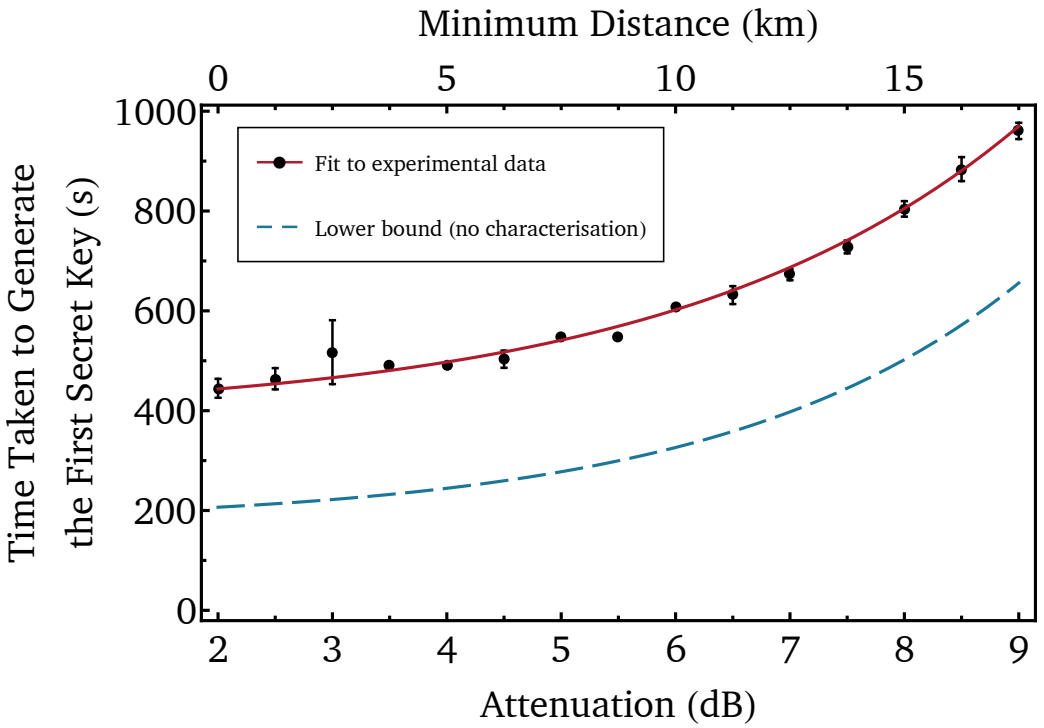


FIGURE 3.20: Showing how the time taken to complete the first round of quantum key distribution changes with loss for the ID Quantique Clavis^2. Here, connections are established through a variable optical attenuator, and the equivalent fibre lengths are calculated assuming a transmission loss of 0.4 dB/km, the worst-case value given by [161]. Each pass through the optical switch contributes 1 dB of loss, resulting in an extra 2 dB of attenuation across all cases.

and so the time taken to exhaust the material provided by the Clavis^2 can be expressed as

$$t_{\text{exhaust}} = \frac{|m|_{\max}}{\varsigma}\left(\left\lfloor \frac{|k|}{|k_{\text{C}}|} \right\rfloor - 1\right) \tag{3.6}$$

Here, ς is the amount of classical data that can be transmitted per unit time, i.e. the total information capacity of the channel minus the number of bits consumed by communication protocol headers. We call this the adjusted channel capacity, more information on which can be found in section 4.1.

From the above, we find that the maximum number of transmitters for a single Clavis^2 receiver is

$$D_{\text{t}} = \left\lfloor \frac{t_{\text{exhaust}}}{t_{\text{init}}} \right\rfloor = \left\lfloor \frac{|m|_{\max}}{\varsigma}\left(\frac{\frac{|k|}{|k_{\text{C}}|} - \left\{\frac{|k|}{|k_{\text{C}}|}\right\}_f}{t_{\text{init}}} - \frac{1}{t_{\text{init}}} \right) \right\rfloor \tag{3.7}$$

where t_{init} is the initialisation time. $\{\cdot\}_f$ indicates the fractional part of a number, which can be expressed as a Fourier series such that

$$\left\{\frac{|k|}{|k_{\text{C}}|}\right\}_f = \frac{1}{2} - \frac{1}{\pi}\sum_{i=1}^{\infty}\frac{1}{i}\sin\left(2\pi i\frac{|k|}{|k_{\text{C}}|}\right) \tag{3.8}$$

Equation 3.7 can now be rearranged, such that

$$D_{\mathrm{t}} = \left\lfloor \frac{|m|_{\max}}{\varsigma} \left[\frac{R_{\mathrm{s/t}}}{|k_{\mathrm{C}}|} - \frac{1}{t_{\mathrm{init}}} \left(1 + \left\{ \frac{|k|}{|k_{\mathrm{C}}|} \right\}_f \right) \right] \right\rfloor \tag{3.9}$$

where $R_{\mathrm{s/t}}$ is the secret key rate of the Clavis^2 with respect to time.

Figure 3.21 plots equation 3.9 against loss, recalling that we encrypt with AES-GCM, meaning $|m|_{\max} = 2^{39} - 256$ (see section 2.1.1). The worst-case scenario is considered, where the classical transmitter has detailed information on the receiver, so the 11584-bit maximum ethernet payload [182] can be used, consuming 95.3% of the total channel capacity. The discontinuity in the maximum number of transmitters around 3 dB stems from a jump in $R_{\mathrm{s/t}}$. A deeper examination of the data uncovers a matching increase in the number of secret bits generated, implying that the number of raw bits exchanged per round went up at this point, perhaps overcompensating for the increase in QBER and reduction in sifting efficiency that arises from the change in QKD protocol. However, this same jump is not present in the secret key rates used to calculate the upper bounds, despite an identical trend in the number of bits generated. Thus, the cause of the discontinuity in $R_{\mathrm{s/t}}$ must lie elsewhere.

The difference between the 3 dB value of $R_{\mathrm{s/t}}$ that we measure and $\widetilde{R}_{\mathrm{s/t}}$, the value predicted by extrapolating a fit that was applied to the higher-attenuation secret key rates, is

$$\Delta R_{\mathrm{s/t}} = R_{\mathrm{s/t}} - \widetilde{R}_{\mathrm{s/t}} = \frac{|k|}{t_{\mathrm{init}}} - \frac{\widetilde{|k|}}{\widetilde{t}_{\mathrm{init}}} \tag{3.10}$$

In a standard initialisation round,

$$\begin{aligned} t_{\mathrm{init}} &= t_{\mathrm{char}} + |k| t_{\mathrm{ssb}} \\ \widetilde{t}_{\mathrm{init}} &= t_{\mathrm{char}} + \widetilde{|k|} t_{\mathrm{ssb}} \end{aligned} \tag{3.11}$$

where t_{ssb} is the average time to generate a single secret bit, and t_{char} is the time taken to perform characterisation. In contrast, for the upper bound on the number of timeshareable devices,

$$\begin{aligned} t_{\mathrm{init}} &= |k| t_{\mathrm{ssb}} \\ \widetilde{t}_{\mathrm{init}} &= \widetilde{|k|} t_{\mathrm{ssb}} \end{aligned} \tag{3.12}$$

Therefore, in the standard case, we can substitute equation 3.11 into equation 3.10 such that

$$\Delta R_{\mathrm{s/t}} = \frac{|k|}{t_{\mathrm{char}} + |k| t_{\mathrm{ssb}}} - \frac{\widetilde{|k|}}{t_{\mathrm{char}} + \widetilde{|k|} t_{\mathrm{ssb}}} \neq 0 \quad \text{i.f.f.} \quad |k| \neq \widetilde{|k|} \tag{3.13}$$

For the upper bound, application of equation 3.12 means equation 3.10 becomes

$$\Delta R_{\mathrm{s/t}} = \frac{|k|}{|k| t_{\mathrm{ssb}}} - \frac{\widetilde{|k|}}{\widetilde{|k|} t_{\mathrm{ssb}}} \equiv 0 \tag{3.14}$$

This explains why, for the initialisation process implemented on the Clavis^2, a jump in the number of secret bits leads to a discontinuity in the secret key rate and, by extension, the number of transmitters

per receiver. It also clarifies why the same behaviour is not present in the case of the upper bounds, and explains why they converge on the data as the attenuation increases, because a higher loss will cause t_{ssb} to go up, while t_{char} remains roughly constant. Therefore, eventually, the key generation step will become the dominant factor in the number of devices that can be time-shared.

It is traditional for TDMA schemes to ensure transmissions from different users do not overlap by introducing an idle period, known as a guard interval, between each time slot. In TDMA-QKD, this may be unnecessary; guard intervals are certainly not required for the setup presented herein, and so figure 3.21 does not take them into account. First, the length of each time slot is flexible, so Alice cannot predict exactly when to open a channel and should only do so when notified that the previous user has disconnected. It should be observed that, for the Clavis^2, Bob does not have the option to specify an IP address for Alice, so this cannot be handled by passing connection initiation responsibilities to him. Second, if he is already occupied and a recusant Alice attempts to open a classical channel through the QKDSequence software, she will find herself unable to connect, without affecting the link already in use. The quantum channel is only triggered on successful establishment of a classical communications line, and is the first to terminate, as post-processing must follow quantum bit (qubit) exchange. Hence, in both cases, it seems unlikely that information from different connections will overlap in the absence of an expressly programmed guard interval.

3.4 Outlook

In this chapter, we have presented the first experimental integration of QKD with an SDN, securing the data plane and successfully time-sharing a single Bob between multiple emulated Alices. TDMA-QKD enables each quantum device to support up to 201 links when deployed in architectures similar to that of the Bristol Quantum Network, allowing asymmetric configurations of QKD devices on a massive scale, and heavily reducing the cost of quantum security. There is potential for expansion to 515 links by changing the way in which the ID Quantique Clavis^2 initialises each connection, with further improvements subject to increases in the key rate. Separation of the time scheduler from the program that loads initial secret keys means the control plane remains hardware-agnostic. Therefore, the work presented herein could be extended to other forms of quantum cryptography as and when they reach a similar stage of maturity to QKD.

The possibility has been shown for commercial QKD devices to operate within normal parameters alongside hardware that is central to an SDN, without a need to modify pre-existing infrastructure. The Polatis optical switch is fully compatible with the Clavis^2, and while EDFAs and programmable optical processors cause issues, they are trivial to circumvent. This is a crucial milestone in the effort to use QKD in real-world networks, removing hurdles that would otherwise have prevented its widespread adoption.

Finally, data centres are a prime target for attackers looking to steal vast quantities of information. They are a key market for SDNs, and transmit classical information in the O-band, freeing up

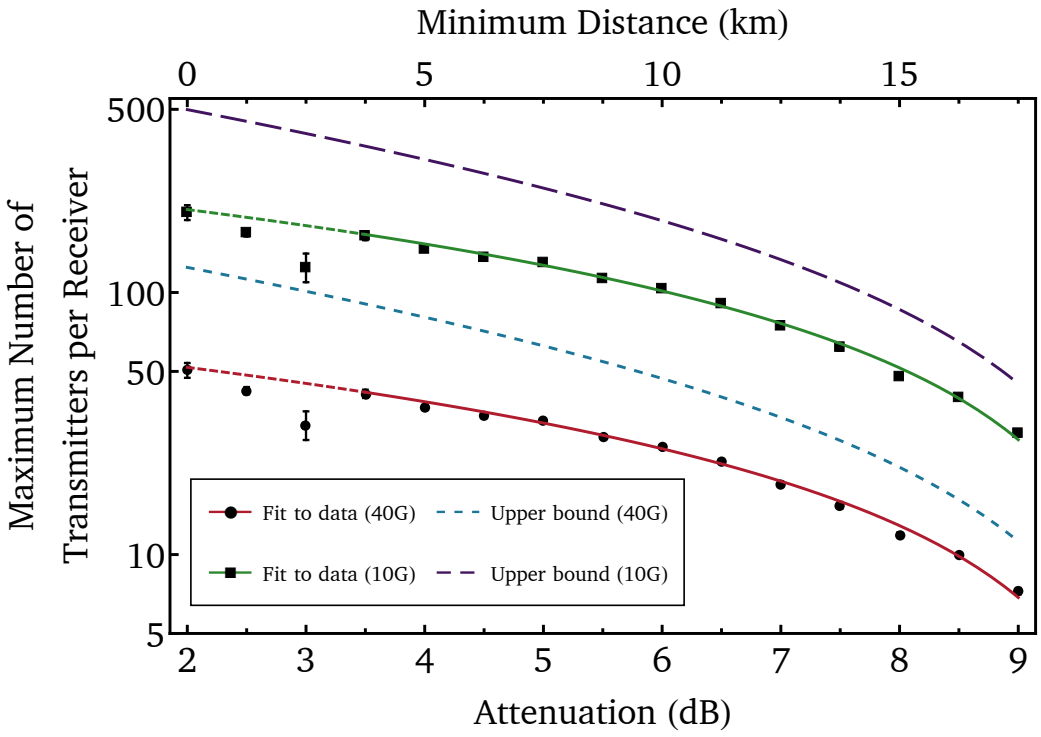


FIGURE 3.21: Showing the maximum number of senders per receiver in a time-division multiple access quantum key distribution network, assuming that all links have the same attenuation. Here, data is encrypted using the Advanced Encryption Standard in Galois/Counter Mode, with keys provided by the ID Quantique Clavis^2. Both 10G and 40G networks are considered, corresponding to data rates of 10 Gbit/s and 40 Gbit/s respectively. Connections are established through a variable optical attenuator, and the equivalent fibre lengths are calculated assuming a transmission loss of 0.4 dB/km, the worst-case value given by [161]. Each pass through the optical switch contributes 1 dB of loss, resulting in an extra 2 dB of attenuation across all cases.

wavelengths in the 1550 nm region. Thus, while the experiments presented herein were aimed towards the Bristol Quantum Network, the results are applicable to other pieces of infrastructure, and the communication models are transferable, illustrating the wider relevance of this work. QKD is also particularly well-suited to network-critical communications, which need to be highly secure and can tolerate lower key rates when compared to many other applications. The obvious next steps for this line of research should, therefore, be to secure the control plane of the SDN using quantum keys, focusing on the OpenFlow messages in particular.

We close by detailing construction of the first two nodes in the Bristol Quantum Network, between which a QKD channel was established, using the key to encrypt data with an OTP. When isolated from the nodes that have been built since, these can double as a distributed second-generation testbed, something which is possible thanks to the reconfigurability of the SDN.

3.4.1 Construction of the Second-Generation Testbed and Bristol Quantum Network

Having shown that QKD could be integrated with an SDN when both Alice and Bob were in the same physical location, the next logical step was to separate them. In doing so, the first two nodes for the Bristol Quantum Network were constructed, capable of being detached from the remainder of the network so as to function as a distributed version of the testbed.

We began by establishing a quantum link between the Centre for Nanoscience & Quantum Information and the Merchant Venturers Building, the relative locations of which are shown in figure 3.5. To simplify troubleshooting, a stripped-down node structure was employed, as depicted in figure 3.22. Here, the optical switch was realised by a 192x192 Polatis used in BiO, replacing the 16x16 version around which the first generation testbed was based. Thus, the qubits transmitted during this experiment were the first to be sent over the Bristol Quantum Network, with the initial QKD-keyed OTP-encrypted message being sent by the author at 12:49:19 on Tuesday 26th January 2016 from the Centre for Nanoscience & Quantum Information to the Merchant Venturers Building, using the ID Quantique Secure Chat software. As shown in figure 3.23, the average secret key rate was 3.30 ± 0.07 kbit/s, with a QBER of $0.713 \pm 0.003\%$, over a period of 3 hours 35 minutes, during which 5.13 MB of key was generated.

Once it had been shown that the link was functioning correctly, the nodes were built up into their current configuration. A 192x192 Polatis was introduced to the Centre for Nanoscience & Quantum Information, upgrading the site to be fully reconfigurable. The internal crosstalk of the switch was characterised between 1500 and 1630 nm, as defined by the wavelength range of the laser available. Only a subset of every possible input/output combination was sampled, incorporating all obvious extremes. This was because, even when we limit our analysis to one classical and one quantum fibre with a fixed laser wavelength, there exist $192^2 \times 191^2 = 1.34 \times 10^9$ ways of configuring the Polatis. Naturally, it is infeasible to test all of these.

The best scenarios were when the quantum and classical channels both exited the switch via outputs adjacent to their inputs, or when the quantum channel had its input and output ports reversed, such that it was counter-propagating with the classical channel. Then, the crosstalk was negligible, as measured by an ID 210 single-photon detector, with a dark count of $(97.0 \pm 0.1) \times 10^3$ counts/s. The worst case was when both links were co-propagating within the switch and their light paths crossed internally, results for which are shown in figure 3.24.

The completed Centre for Nanoscience & Quantum Information node is shown in figure 3.25, with an equivalent setup in the Merchant Venturers Building, and a bundle of 144 fibres connecting the two. When interfacing with the rest of the network, additional challenges were introduced regarding the classical QKD channel. Previously, this was realised by establishing an internet connection between the QKD controllers, through a low-security local network that was physically separate from the rest of the university's communications infrastructure. Unfortunately, it was not possible to set up a similar framework across the entire city, so an alternative solution was required. The most

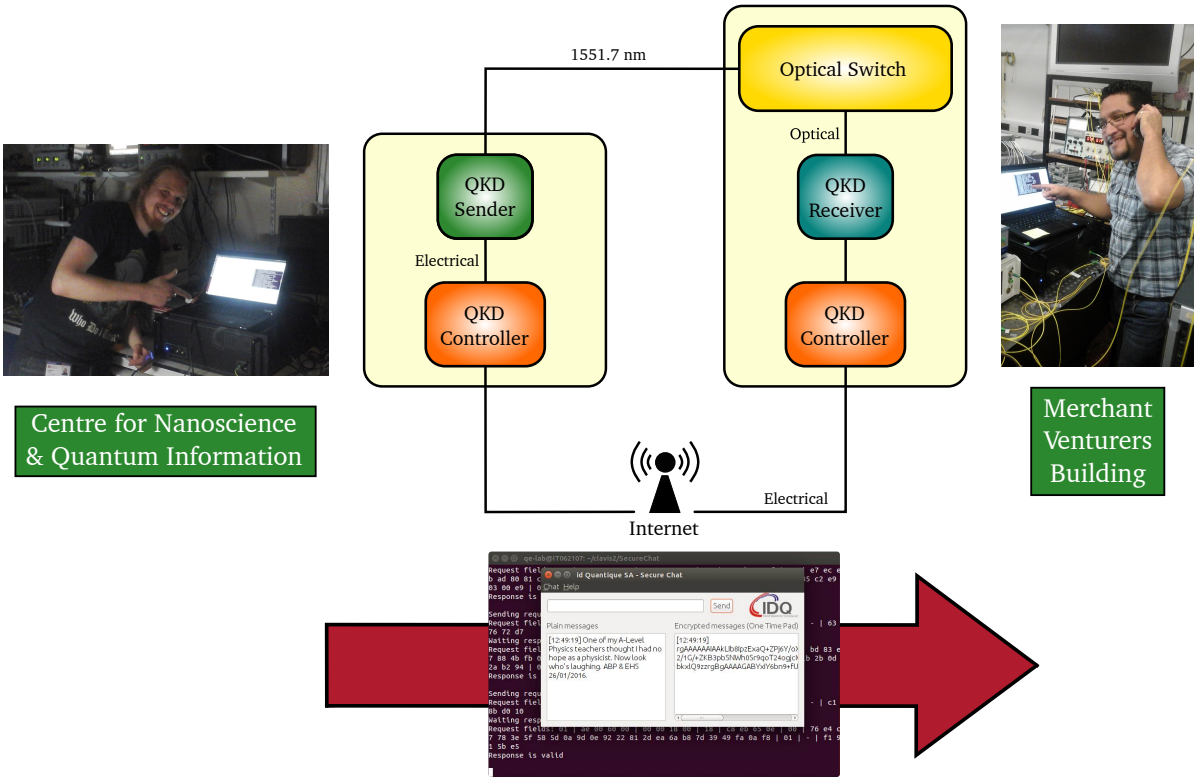


FIGURE 3.22: Illustrating the setup used for the first transmission over the Bristol Quantum Network. An optical switch was subsequently added to the Centre for Nanoscience & Quantum Information as both nodes became fully populated.

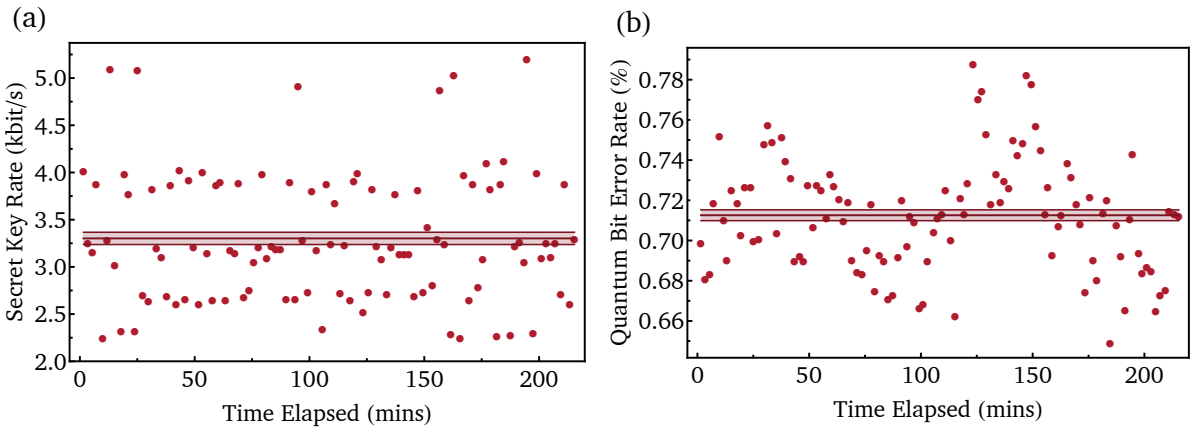


FIGURE 3.23: Showing (a) the secret key rate and (b) the quantum bit error rate for an ID Quantique Clavis^2 installed on the first link of the Bristol Quantum Network, where Alice and Bob were separated by a fibre-distance of ~ 1.1 km. The coloured regions represents the standard error on the mean.

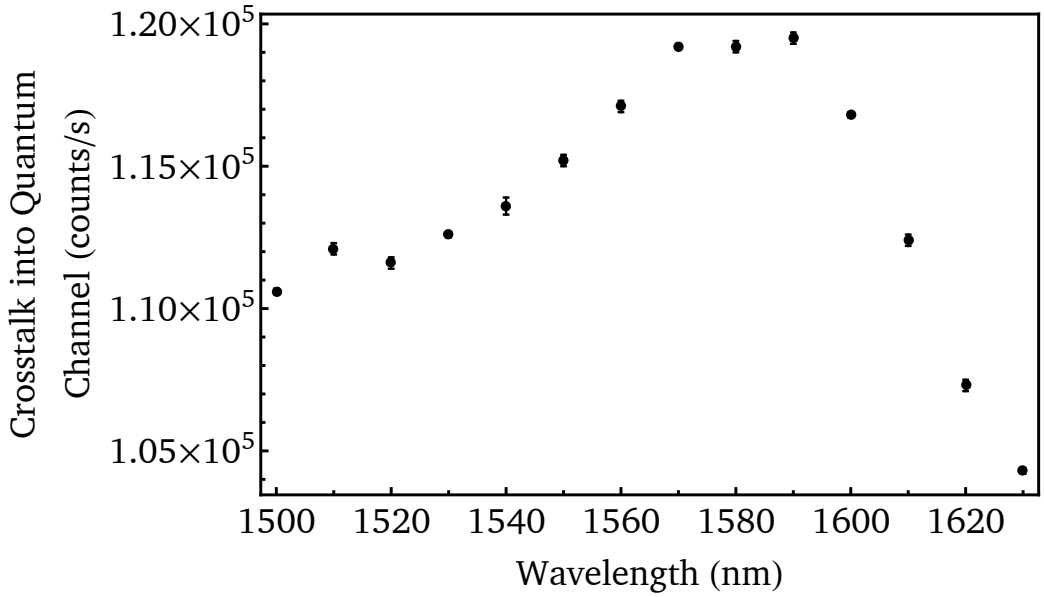


FIGURE 3.24: Showing the crosstalk from a single classical channel into a single quantum channel when their light paths cross inside the Polatis switch. Here, the launch power on the classical link was -7.09 ± 0.01 dBm; the lowest point at which the laser could be operated.

obvious choice was to transmit the public announcements across the same fibres as the encrypted data, which has been successfully implemented and, due to the scale of BiO, continues to be feasible at wavelengths in the region of 1310 nm.

Alice		Bob
		
Layer 2 Switch		Layer 2 Switch
Clavis^3 Transmitter		Clavis^3 Receiver
Optical Patch Panel		Optical Patch Panel
Clavis^2 Transmitter		Clavis^2 Receiver
Centauris Encryptor		Centauris Encryptor
192x192 Polatis Series 6000 Optical Switch		
Dell PowerEdge T630 Server		Dell PowerEdge T630 Server

FIGURE 3.25: The second-generation testbed, capable of emulating any configuration of the Bristol Quantum Network and acting as a fully-fledged fifth node. Original photograph: Richard Collins.

CHAPTER 4

THE IMPRACTICALITY OF THE ONE-TIME PAD FOR EVERYDAY QUANTUM-SECURED COMMUNICATIONS

Declaration of Work

I developed the theory, carried out the experiments that investigate classical overheads, and performed the simulations, all unassisted.

Here, we will justify our choice to use the Advanced Encryption Standard running in Galois/-Counter Mode (AES-GCM) for encrypting data in chapter 3, as it will form the foundation for the rest of this thesis. Since its inception, quantum key distribution (QKD) has been seen as a method for achieving mathematically unbreakable communications by using it in conjunction with the one-time pad (OTP) [76, 183]. While the importance of a provably-secure method for sharing a single-use key is undeniable for the most sensitive of communications [10, 184], the impact on everyday security is less clear. Many recognise that, for the time being at least, it will be necessary to continue using computationally-secure alternatives, because even cutting-edge QKD systems still have relatively low secret key rates [87, 185, 186]. However, very little has been said on when these alternatives can be superseded by the OTP, if at all.

In sections 4.1 and 4.2, we present two arguments as to why it is unlikely that single-qubit discrete-variable quantum key distribution (DV-QKD) will ever be used with OTP encryption in generic networks. Although there are steps that can be taken to improve these odds, they will be challenging to accomplish before the deployment of quantum-safe cryptography becomes a critical concern, and commercial entities will need to be persuaded that the financial impact is worth bearing.

Of course, there are other forms of QKD to which our arguments may not apply. Full analyses of continuous-variable quantum key distribution (CV-QKD) [187], higher-dimensional QKD [188, 189] and floodlight quantum key distribution (FL-QKD) [190, 191] are outside the scope of this thesis, however some preliminary details will be given in section 4.4.1.

It should also be noted that responsibility for everyday information-theoretic security does not fall solely on the shoulders of QKD. Advances must also be made with respect to the OTP, and section 4.3 summarises the developments required for it to become a widespread method of encryption, assuming there exists some efficient way of distributing key.

4.1 The Effect of the Classical Channel on Key Generation

We begin by considering an element of QKD that has not been focused on in the past. It is implicitly assumed that networks in need of quantum security will have enough capacity to support the classical QKD channel. However, experimentally, this is not necessarily true. We introduce the following condition which, while seemingly arbitrary in the amount of data, is a logical starting point that enables the development of a more refined model for fully evaluating the classical requirements imposed by QKD.

Condition 4.1: *Assume a communications link is constantly transmitting data and, in doing so, is operating at half its classical capacity. Assume also that quantum signals can be injected without generating any secondary artifacts that affect the above. We can encrypt all data using a QKD-keyed OTP without artificially capping the classical data rates or increasing the network capacity, so long as* $R_{c/s} \leq 1$*, where* $R_{c/s}$ *is the number of bits that must be sent across the classical QKD channel for every bit of secret key that is generated.*

The Gottesman-Lo-Lütkenhaus-Preskill (GLLP) security proof against general attacks on Bennett-Brassard 1984 (BB84) [89] provides an equation for the secret key rate that can be re-written in terms of physical parameters [192] such that

$$R_{s/p} \geq \zeta \left[-Q_\mu H_2\left(E_\mu\right) + Q_1 \left[1 - H_2\left(E_1\right)\right]\right] \tag{4.1}$$

Here, $R_{s/p}$ is the number of secret bits transmitted per weak coherent pulse. If N is the number of pulses transmitted by Alice then ζ is the fraction of these that contribute to the sifted key (~ 0.5 for vanilla BB84, or less if decoy states are used). $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy function, while E_μ and E_1 represent the total and single-photon quantum bit error rates (QBERs) respectively. Provided Alice and Bob prepared and measured in the same basis, Q_μ is the probability of Bob experiencing a detection as a result of a weak coherent pulse, and

$$Q_\Gamma = Y_\Gamma \times \text{Prob}\left(\gamma = \Gamma\right) = \frac{Y_\Gamma e^{-\mu}\mu^\Gamma}{\Gamma!} \tag{4.2}$$

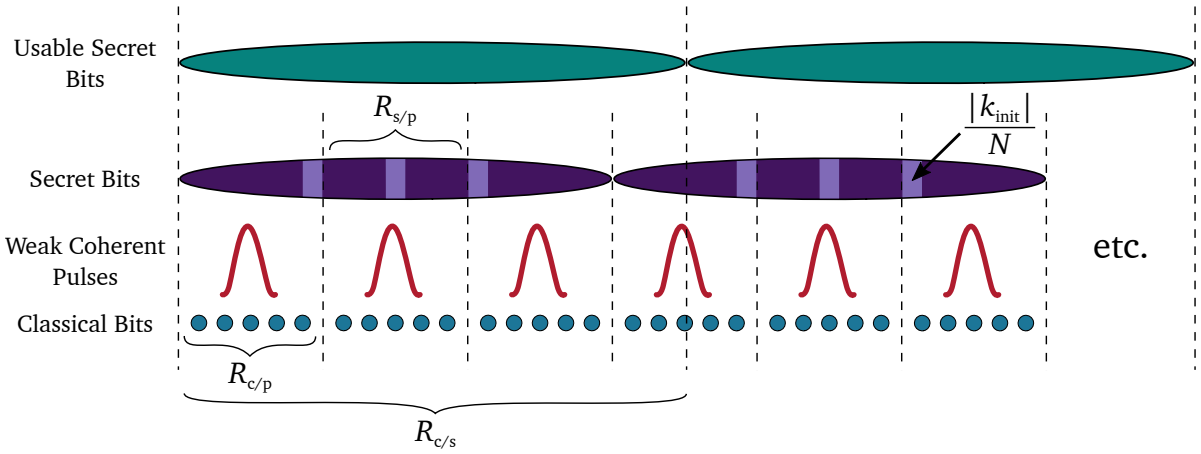


FIGURE 4.1: A graphical representation of the relationships between $R_{c/p}$ (the number of classical bits per pulse), $R_{s/p}$ (the number of secret bits per pulse) and $R_{c/s}$ (the number of classical bits per usable secret bit). Each secret bit will contribute $1-\frac{|k_{init}|}{NR_{s/p}}$ "usable" bits to a terminal application such as encryption, where N is the total number of pulses. The remainder will go towards replenishing the initial secret key, which is $|k_{init}|$ bits in length.

Y_Γ is the probability of Bob experiencing a detection given Alice transmitted a Γ-photon state, meaning Q_1 corresponds to single-photon terms.

The number of classical bits that must be communicated for every pulse is given by

$$R_{c/p} = \frac{|\Omega| + |\Upsilon| + 2|\tau| + |\text{✗}|}{N} \tag{4.3}$$

$|\Omega|$ is the number of bits required both to announce the bases and identify any pulses that failed to arrive, $|\Upsilon|$ is the number of bits that must be communicated during the error correction procedure, $|\tau|$ is the length of the authentication tag, and $|\text{✗}|$ is the number of extraneous bits that would not normally be considered in theoretical treatments of QKD, such as those required for channel characterisation and packet switching, both of which will be addressed in more detail later.

Figure 4.1 illustrates the relationships between each of the R-values. After accounting for the number of bits $|k_{init}|$ that will be used as the initial secret key in the next round of the protocol, we find that for every remaining bit of secret key, the number of bits we must send across the classical QKD channel is

$$R_{c/s} = \frac{R_{c/p}}{R_{s/p} - |k_{init}|/N} \leq \frac{|\Omega| + |\Upsilon| + 2|\tau| + |\text{✗}|}{N\zeta\left[-Q_\mu H_2\left(E_\mu\right) + Q_1\left[1 - H_2\left(E_1\right)\right]\right] - |k_{init}|} \tag{4.4}$$

From this, it is clear that condition 4.1 cannot be fulfilled by DV-QKD in its current form. Consider the limiting (and highly unrealistic) situation where we replace Alice's attenuated laser with a deterministic single-photon source, meaning no decoy states are required and $Q_1 = Y_1$. Through fluke or otherwise, Bob's bases match Alice's perfectly, meaning $\zeta = 1$. Contact between the two parties is a one-off event that will never be repeated, so $|k_{\text{init}}| = 0$. We use a lossless, error-free channel which does not rely on any extraneous communication, and give Bob perfect single-photon detectors, meaning $|\Omega| = 2N$ (this could be reduced with a non-standard approach to the basis announcements if a biased QKD protocol is used), $|\Upsilon| = |\text{✗}| = 0$ and $Y_1 = 1$. $H_2(x) \to 0$ as $x \to 0$, so

$$R_{\text{c/s}} \to 2\left(1 + \frac{|\tau|}{N}\right) \tag{4.5}$$

Of course, while condition 4.1 stipulates that $R_{\text{c/s}} \leq 1$, equation 4.5 only marginally violates this, because we require $N \gtrsim 10^5$ for finite-key security [193] and $|\tau|$ does not typically exceed 128 bits. However, it is difficult to ascertain whether or not the size of the violation matters, because our model fails to quantitatively address the impact of such an outcome on the classical data rates or network capacity. In addition, the assumptions made by condition 4.1 are not necessarily appropriate for many real-world networks, as user demands can fluctuate over time.

To address the above, a more general approach is required. Consider an arbitrary symmetric cipher that can be used to encrypt $|m|_{\text{max}}$ bits of data for every $|k_{\text{C}}|$ bits of key. Each run of a QKD protocol uses $R_{\text{c/s}}|k|$ classical bits to generate $|k|$ bits of key, meaning $\frac{|k||m|_{\text{max}}}{|k_{\text{C}}|}$ bits of data can be encrypted per run.

The network is defined to have a constant level of off-peak traffic from time $t = 0$ to $t = t_1$, and a constant level of on-peak traffic from $t = t_1$ to $t = t_2$. In practice, there will still be some variation on the demand within these windows, however it should be small relative to the difference between the two, as one would expect in a "9-to-5" office building, for example. There is no encryption-related penalty for capping the data rates further than absolutely necessary, so these levels of on-peak and off-peak traffic may be considered upper bounds.

During off-peak periods, the adjusted channel capacity per unit time (recall, the total channel capacity minus the number of bits consumed by communication protocol headers for the data) can be expressed as

$$\varsigma = \varsigma_{\text{V}} + u_{\text{V}} \tag{4.6}$$

where ς_{V} is the number of bits of off-peak data that are transmitted per unit time and u_{V} is the unused remainder.

To encrypt all the off-peak data using symmetric keys generated by QKD, we require

$$u_{\text{V}} \geq \frac{R_{\text{c/s}}\varsigma_{\text{V}}|k_{\text{C}}|}{|m|_{\text{max}}} \tag{4.7}$$

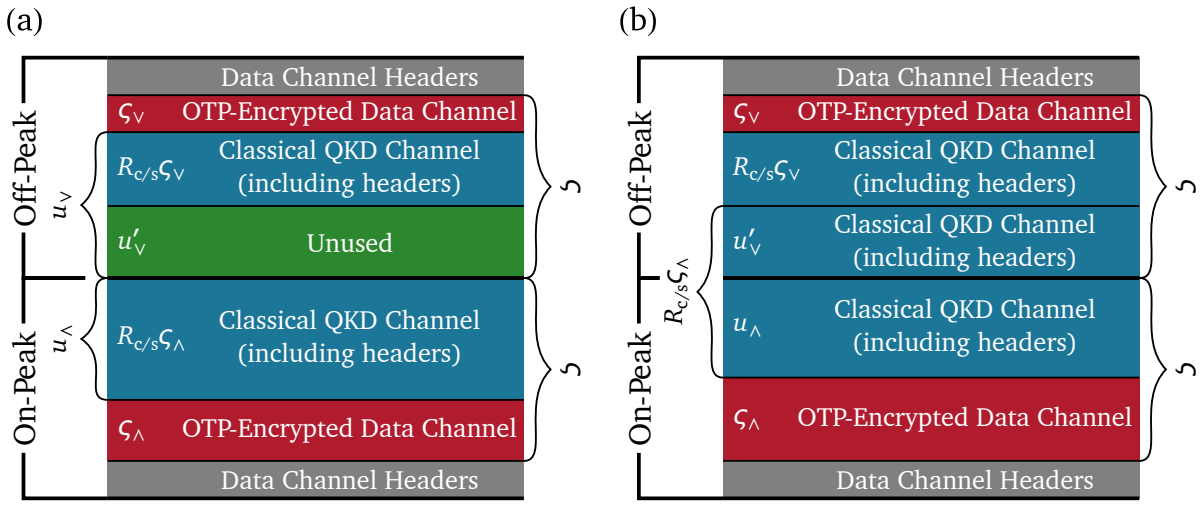


FIGURE 4.2: A graphical representation of the relationships between the channel variables used in this chapter, considering cases when the on-peak channel (a) does not, and (b) does take advantage of any unused off-peak capacity. We consider a simplified scenario where encryption is performed with the one-time pad, meaning 1 bit of key is required for each bit of data, and so $\frac{|k_C|}{|m|_{max}} = 1$. Although the off-peak and on-peak channels are depicted as being next to one another, it is assumed they will be separated in time and realised by the same physical fibre, with the off-peak channel preceding the on-peak.

Here, $|k| = \frac{\varsigma_\vee |k_C|}{|m|_{max}}$ is the number of secret bits that must be generated per unit time to encrypt at a rate defined by $\varsigma_\vee$. Rearranging and substituting equation 4.6 into equation 4.7 gives

$$\varsigma_\vee \leq \frac{\varsigma}{1 + \frac{R_{c/s}|k_C|}{|m|_{max}}} \tag{4.8}$$

Therefore, for encrypted data,

$$\varsigma t_1 = \varsigma_\vee t_1 \left(1 + \frac{R_{c/s}|k_C|}{|m|_{max}}\right) + u'_\vee t_1 \tag{4.9}$$

Here, $u'_\vee$ is the channel capacity that remains unused after the classical QKD link has been introduced, as shown in figure 4.2a. Similarly, during on-peak periods,

$$\varsigma = \varsigma_\wedge + u_\wedge \tag{4.10}$$

where $\varsigma_\wedge$ is the number of bits of on-peak data being transmitted per unit time and $u_\wedge$ is the unused remainder.

When encrypting the on-peak data using keys generated by QKD, we can take advantage of $u'_\vee$ to share additional key before it is required, reducing the amount that needs to be transmitted

during on-peak times (see figure 4.2b). It should be noted that the on-peak and off-peak channels are additive because, for fixed periods of existence, they are independent from one another. As a result, we mandate

$$u_{\wedge}(t_2 - t_1) + u'_{\vee} t_1 \geq \frac{R_{c/s}\varsigma_{\wedge}|k_C|}{|m|_{max}}(t_2 - t_1) \tag{4.11}$$

Rearranging and substituting equations 4.9 and 4.10 into equation 4.11 gives

$$\varsigma - \varsigma_{\wedge} \geq \frac{R_{c/s}\varsigma_{\wedge}|k_C|}{|m|_{max}} - \underbrace{\left[\varsigma - \varsigma_{\vee}\left(1 + \frac{R_{c/s}|k_C|}{|m|_{max}}\right)\right]}_{\dagger}\frac{t_1}{t_2 - t_1} \tag{4.12}$$

We assume † is non-zero, as otherwise equation 4.12 reduces to the trivial case (surplus key cannot be generated during off-peak periods when $u'_{\vee} = 0$). This means equation 4.8 restricts † to always be positive, hence

$$\frac{t_1}{t_2 - t_1} \geq \frac{\varsigma_{\wedge}\left(1 + \frac{R_{c/s}|k_C|}{|m|_{max}}\right) - \varsigma}{\varsigma - \varsigma_{\vee}\left(1 + \frac{R_{c/s}|k_C|}{|m|_{max}}\right)} \tag{4.13}$$

We can put these equations in context by measuring $R_{c/s}$ for a real system. The ID Quantique Clavis^2 is a natural choice, given the work done in chapter 3. In table 4.1, we give values both for a near-lossless channel and at 9 dB attenuation (recall, the highest loss that we can tolerate before key generation becomes intermittent). The former was implemented by placing Alice and Bob next to each other and establishing a direct connection with the shortest fibre available that, to within the precision of the powermeter, had 0 dB loss. At the time of taking measurements for the latter, Alice and Bob were located in separate nodes for metropolitan network tests. The fibre between them contributed 1.4 dB of loss, so the remaining 7.6 dB was introduced using a variable optical attenuator. The number of classical bits broadcast by the QKDSequence control software can be measured using Wireshark, and the Clavis^2 keeps track of the number of secret bits generated in each round. The average $R_{c/s}$ was then calculated from these two values, for a 256-bit initial shared secret. We do not consider any additional overheads that are introduced by the physical layer, as these add linearly, so are incorporated into the channel capacity implicitly.

There are a number of reasons why the results in table 4.1 are so extreme. First, the potential for the classical channel to be a limiting factor has, to the author's knowledge, never previously been scrutinised at this level, so commercial systems are unlikely to have been optimised and there may be scope to reduce the communication resources consumed by the Clavis^2. However, there are also some fundamental restrictions. The Transmission Control Protocol (TCP) [194] forms the basis of the Clavis^2 public channel. It divides data into a series of packets, adding a minimum of 160 bits to each in the form of a header that contains pieces of information like the destination port and a

TABLE 4.1: Average number of classical bits transmitted by the ID Quantique Clavis^2 per secret bit $\left(\overline{R}_{c/s}\right)$ for both the minimum and maximum attenuations at which key is reliably generated. These values are unlikely to have been optimised, so should not be considered lower bounds.

Round Type	Quantum Channel Loss (dB)	$\overline{R}_{c/s}$
Initialisation	$0.00\,^{+0.01}_{-0}$	196.4 ± 0.4
Standard	$0.00\,^{+0.01}_{-0}$	195.9 ± 1.1
Initialisation	9.00 ± 0.01	757.3 ± 9.6
Standard	9.00 ± 0.01	753.9 ± 9.9

checksum. In actuality, the Clavis^2 adds a total of 256 bits on top of the payload due to the inclusion of optional fields. This is then encapsulated in an Internet Protocol version 4 (IPv4) [195] packet with a header that is 160 bits both at minimum and in the case of the Clavis^2. It should be noted that as the Internet Protocol version 6 (IPv6) [196] becomes more prevalent, the minimum header size will increase to 320 bits. Finally, the IPv4 packet is encapsulated in an Ethernet II [182] frame that contributes an extra 144 bits, and requires a 96-bit interframe spacing. This is summarised in figure 4.3.

As one would expect, a higher loss in the quantum channel negatively impacts $\overline{R}_{c/s}$. At 9 dB attenuation, the number of raw bits that contribute to each secret bit is greater than at 0 dB, and so more information must be exchanged per secret bit over the public channel. In addition, the Clavis^2 relies on BB84 when the loss is ≤ 3 dB and Scarani-Acín-Ribordy-Gisin 2004 (SARG04) otherwise. In the case of the latter, Alice announces two states from a choice of four instead of one basis from a choice of two (see protocol 2.6), quadrupling the information she must transmit for each qubit received by Bob.

Finally, it can be seen that, as an overall percentage, relatively little information needs to be communicated during the initialisation period. This makes sense given it mainly consists of calibrative tasks, involving direct measurements of features like the length of the transmission line.

FIGURE 4.3: The encapsulation structure for an Ethernet II frame containing an Internet Protocol version 4 (IPv4) packet, which in turn contains a Transmission Control Protocol (TCP) packet. While in principle it is possible to transmit a 11,584-bit payload, this can only happen if it is known that Bob will accept packets of such size. Otherwise, the maximum payload is restricted to 4288 bits, calculated using the limits given in [197].

Figure 4.4 takes the values of $\overline{R}_{c/s}$ from table 4.1, and plots the minimum time ratio from

equation 4.13, assuming we want to encrypt with a QKD-keyed OTP, meaning $\frac{|k_C|}{|m|_{max}} = 1$. We vary both the on-peak and off-peak data rates, as well as fixing the off-peak traffic to give a clearer picture of the limiting cases. While

$$\frac{t_1}{t_2 - t_1} \to \infty \quad \text{as} \quad \varsigma_\vee \to \frac{\varsigma |m|_{max}}{|m|_{max} + R_{c/s}|k_C|} \tag{4.14}$$

a network operating close to this limit can be simulated by setting

$$\varsigma_\vee = \left\lfloor \frac{\varsigma |m|_{max}}{|m|_{max} + R_{c/s}|k_C|} \right\rfloor_{\mathsf{M}} \tag{4.15}$$

where $\lfloor \cdot \rfloor_{\mathsf{M}}$ means that we round down to the nearest multiple of machine epsilon M; the difference between 1 and the next-closest number that, on a computer, is distinguishably greater than 1. In broader terms, we are using M ($= 2^{-52}$ for the work presented herein) as a foundation for defining the highest value of $\varsigma_\vee$ that can be evaluated before our simulation breaks down.

We plot figure 4.5 in similar fashion, continuing to rely on QKD as a means of distributing the symmetric key, but this time encrypting with AES-GCM, such that $\frac{|k_C|}{|m|_{max}} = \frac{256}{2^{39}-256}$ [18].

The results make clear that networks like the Washington-Moscow hotline [10], which need high security and experience low volumes of traffic for long periods, will be able to use a QKD-keyed OTP if the classical channel is the only limiting factor. However, day-to-day networks will have to continue using computationally-secure encryption. Not only does AES-GCM require off-peak times per second of on-peak time that are orders of magnitude lower than for the OTP, but the off-peak data rates are limited to approaching 99.9999(6)% of the channel capacity at worst (calculated from equation 4.14 for an initialisation round at 9 dB loss). In contrast, the OTP restricts this to approaching 0.5078(7)% at best (a standard round at 0 dB loss), given the values of $\overline{R}_{c/s}$ measured for the Clavis^2. Finally, we can get much closer to this limiting value for AES-GCM before $\frac{t_1}{t_2 - t_1}$ rapidly approaches infinity, as evidenced by comparing subfigures 4.4e and 4.4f with subfigures 4.5e and 4.5f.

We now provide a more comprehensive formulation of the terms that a network must fulfil for the OTP to be used in conjunction with QKD. While we do not explicitly cover cases that can be split into three or more distinct periods of traffic, these can always be approximated by an on-peak/off-peak model, though with slightly pessimistic estimates as a result. Our model is general enough to be representative of most everyday networks, and is summarised by condition 4.2, which reduces to condition 4.1 if $|m|_{max} = |k_C|$ (each bit of key encrypts one bit of data), $t_1 = 0$ while $t_2 - t_1 = 1$ (the amount of traffic remains constant at all times), and $\varsigma_\wedge = \frac{\varsigma}{2}$ (the link operates at half its classical capacity).

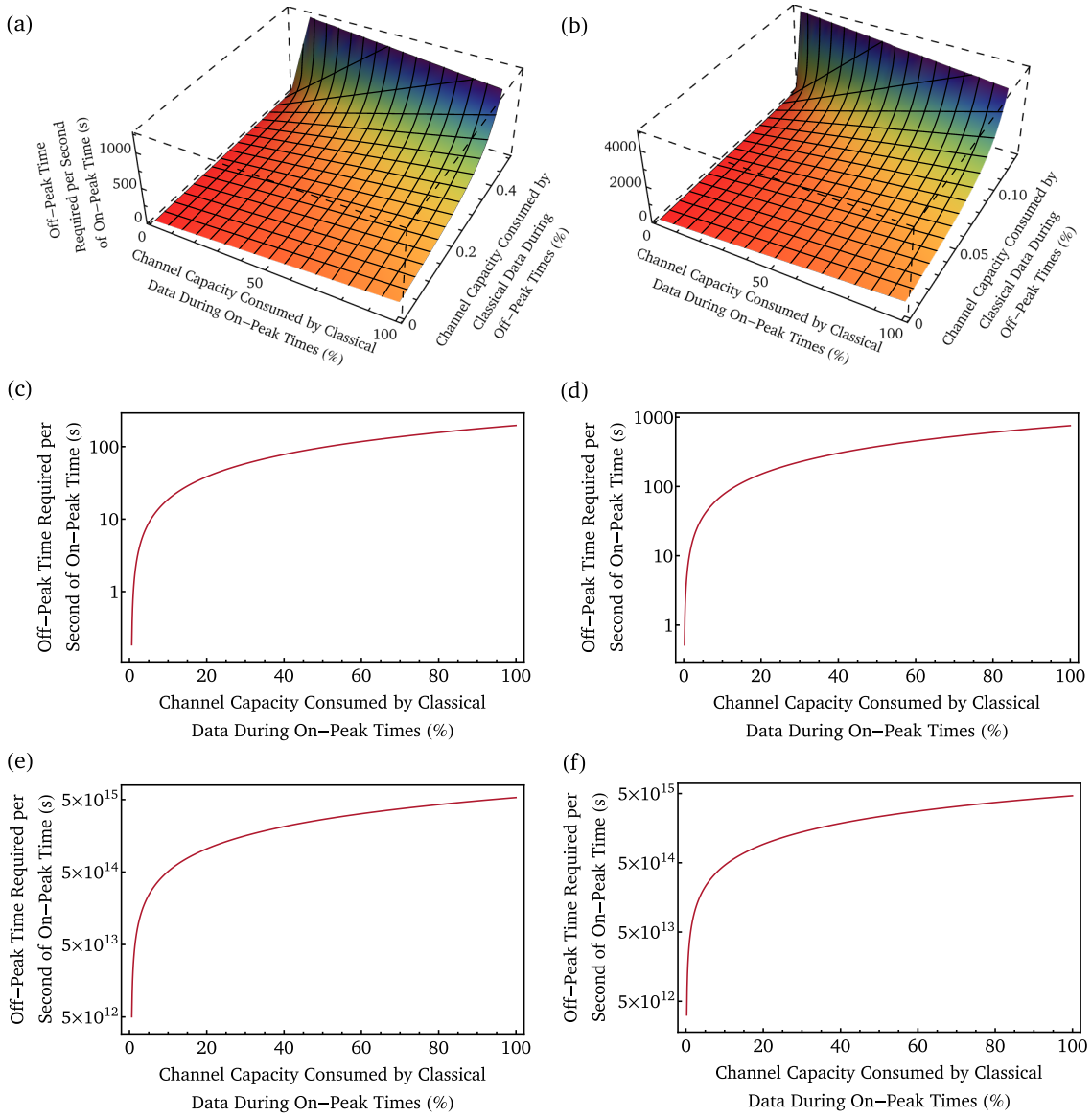


FIGURE 4.4: Showing the amount of off-peak time required per second of on-peak time in order to encrypt all data with a quantum key distribution (QKD)-keyed one-time pad, and considering only limitations imposed by the classical QKD channel for the ID Quantique Clavis^2. We present results for (a) 0 dB loss in the quantum transmission line, with varying on-peak and off-peak traffic (mathematically, the percentage channel capacity consumed by classical data during on-peak and off-peak times is $\varsigma_\wedge/\varsigma$ and $\varsigma_\vee/\varsigma$ respectively); (b) 9 dB loss in the quantum transmission line, with varying on-peak and off-peak traffic; (c) and (d) 0 dB and 9 dB losses in the quantum transmission line respectively, with varying on-peak and no off-peak traffic in both cases; (e) and (f) 0 dB and 9 dB losses in the quantum transmission line respectively, with varying on-peak and $\left\lfloor \frac{\varsigma|m|_{\max}}{|m|_{\max}+R_{c/s}|k_C|} \right\rfloor_M$ off-peak traffic in both cases, where $\lfloor\cdot\rfloor_M$ means that we round down to the nearest multiple of machine epsilon M.

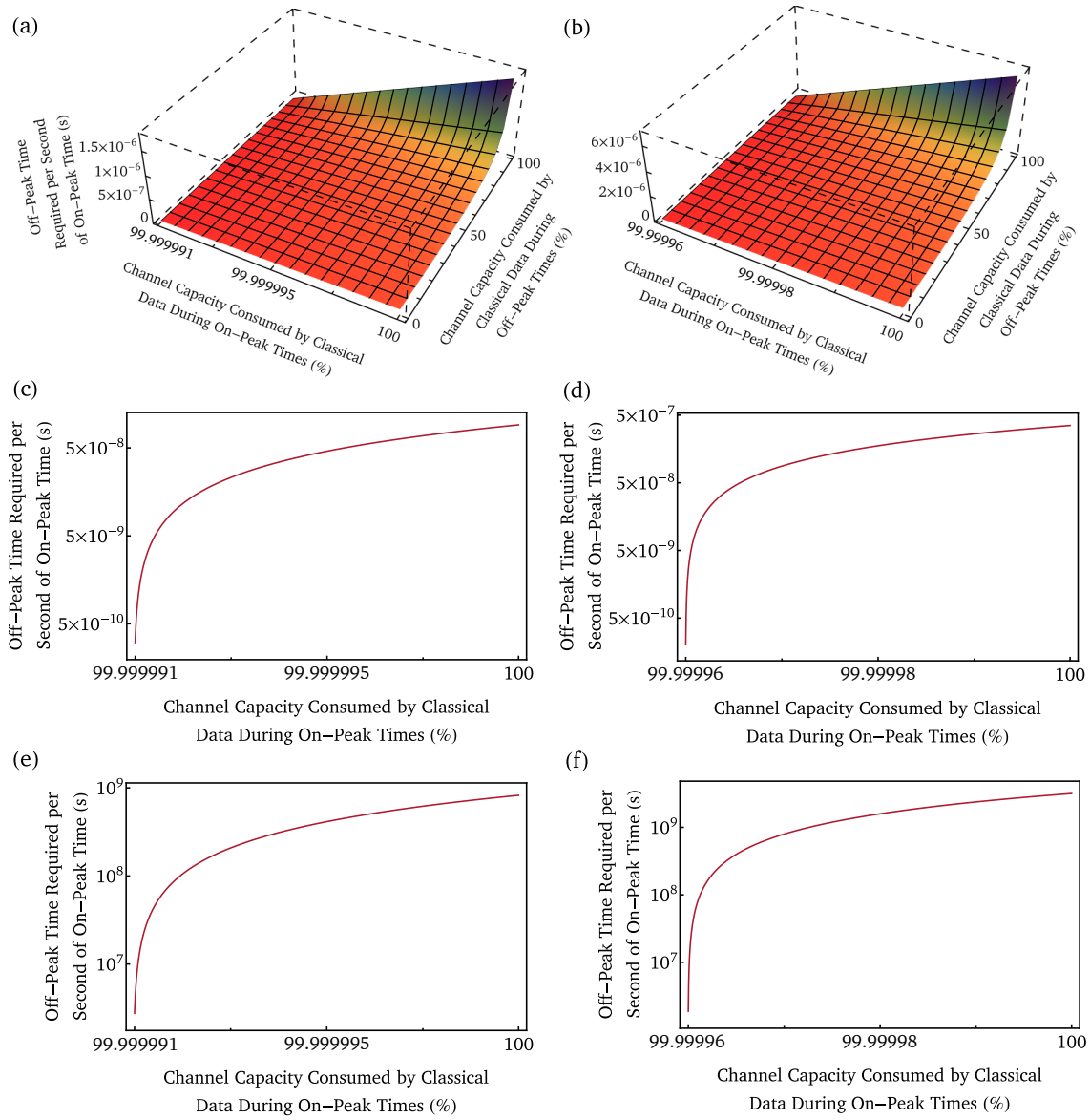


FIGURE 4.5: Showing the amount of off-peak time required per second of on-peak time in order to encrypt all data with the Advanced Encryption Standard running in Galois/Counter Mode, keyed using quantum key distribution (QKD) and considering only limitations imposed by the classical QKD channel for the ID Quantique Clavis^2. We present results for (a) 0 dB loss in the quantum transmission line, with varying on-peak and off-peak traffic (mathematically, the percentage channel capacity consumed by classical data during on-peak and off-peak times is $\varsigma_\wedge/\varsigma$ and $\varsigma_\vee/\varsigma$ respectively); (b) 9 dB loss in the quantum transmission line, with varying on-peak and off-peak traffic; (c) and (d) 0 dB and 9 dB losses in the quantum transmission line respectively, with varying on-peak and no off-peak traffic in both cases; (e) and (f) 0 dB and 9 dB losses in the quantum transmission line respectively, with varying on-peak and $\left\lfloor \frac{\varsigma |m|_{\max}}{|m|_{\max} + R_{c/s}|k_C|} \right\rfloor_{\mathsf{M}}$ off-peak traffic in both cases, where $\lfloor \cdot \rfloor_{\mathsf{M}}$ means that we round down to the nearest multiple of machine epsilon M.

Condition 4.2: *Assume a communications link of classical capacity ς experiences off-peak data rates of $\varsigma_\vee$ for time t_1, on-peak data rates of $\varsigma_\wedge$ for time $t_2 - t_1$, and quantum signals can be injected without generating any secondary artifacts that affect the above. We can encrypt all data using an arbitrary cipher, without artificially capping the classical data rates or increasing the channel capacity, so long as* $R_{c/s} \leq \frac{|m|_{\max}[\varsigma t_2 - \varsigma_\wedge(t_2-t_1) - \varsigma_\vee t_1]}{|k_C|[\varsigma_\wedge(t_2-t_1)+\varsigma_\vee t_1]}$.

4.2 The Effect of the Quantum Channel on Key Generation

Until now, the work in this chapter has implicitly assumed that the bit generation rate for the encryption keys is comparable with classical data rates, taking care to note that the former is distinct from the secret key rate, which does not take into account the bits assigned to refreshing Alice and Bob's initial shared secret. However, as we have already indicated in chapter 3, this assumption is inaccurate, and we must examine the implications of any mismatch.

Consider the situation where

$$R_{p/t}\left(R_{s/p} - |k_{init}|/N\right) < \varsigma_\vee \tag{4.16}$$

The left hand side corresponds to the number of bits generated per unit time that can be used for encryption, and $R_{p/t}$ is the quantum clock rate. Here, the only choice is to use a computationally secure cipher as a basis for our encryption scheme, unless a sufficient number of quantum devices can be multiplexed together. Similarly, if

$$R_{p/t}\left(R_{s/p} - |k_{init}|/N\right) > \varsigma_\wedge \tag{4.17}$$

then, so far as the quantum channel is concerned, there will be no issues with using the OTP. However, when

$$\varsigma_\vee < R_{p/t}\left(R_{s/p} - |k_{init}|/N\right) < \varsigma_\wedge \tag{4.18}$$

the situation becomes more interesting. We define

$$\begin{aligned} \Delta_\vee &= R_{p/t}\left(R_{s/p} - |k_{init}|/N\right) - \varsigma_\vee \\ \Delta_\wedge &= \varsigma_\wedge - R_{p/t}\left(R_{s/p} - |k_{init}|/N\right) \end{aligned} \tag{4.19}$$

To use the OTP, it is required that

$$\Delta_\vee t_1 \geq \Delta_\wedge (t_2 - t_1) \tag{4.20}$$

Thus, by substituting equation 4.19 into 4.20 and rearranging, we find

$$\frac{t_1}{t_2 - t_1} \geq \frac{\varsigma_\wedge - R_{p/t}\left(R_{s/p} - |k_{init}|/N\right)}{R_{p/t}\left(R_{s/p} - |k_{init}|/N\right) - \varsigma_\vee} \tag{4.21}$$

This enables conditions 4.3 and 4.4 to be constructed which, regardless of the efficiency of the public channel, must be fulfilled if we are to cease encrypting with modes of operation that rely on the Advanced Encryption Standard (AES). There is, of course, always the option to curb classical data rates. However, the end-user often prioritises minimal performance improvements over security, as evidenced by the widespread adoption of technologies such as contactless card payments, which have a number of trivially-exploitable vulnerabilities [198–201]. Therefore, it would be naïve to assume that internet users will accept slower speeds in exchange for an increase only in the theoretical security of their data.

Condition 4.3: *Assume* $R_{p/t}\left(R_{s/p} - |k_{init}|/N\right) < \varsigma_\vee$. *We can encrypt all off-peak data using a QKD-keyed OTP without artificially capping the classical data rates, so long as* $D_{mux} = \left\lceil \frac{\varsigma_\vee}{R_{p/t}\left(R_{s/p} - |k_{init}|/N\right)} \right\rceil$ *quantum devices can be multiplexed together and* $\sum_{D_{mux}} R'_{s/t} \approx R_{s/t} D_{mux}$. *Here,* $R_{s/t}$ *is the number of secret bits generated per unit time when only a single QKD device is operational, and* $R'_{s/t}$ *is the number of secret bits generated per unit time by each of those deployed in a multiplexed configuration.*

Condition 4.4: *Assume* $\varsigma_\vee < R_{p/t}\left(R_{s/p} - |k_{init}|/N\right) < \varsigma_\wedge$, *or condition 4.3 has been fulfilled. We can encrypt all on-peak data using a QKD-keyed OTP without artificially capping the classical data rates, so long as* $D_{mux} = \left\lceil \frac{\varsigma_\wedge}{R_{p/t}\left(R_{s/p} - |k_{init}|/N\right)} \right\rceil$ *quantum devices can be multiplexed together and* $\sum_{D_{mux}} R'_{s/t} \approx R_{s/t} D_{mux}$ *, or equation 4.21 can be satisfied.*

The most important question that this raises is, at present, how close to one another are the speeds of the classical and quantum channels? In figure 4.6 we compare $R_{s/t} = R_{p/t} R_{s/p}$ with classical data rates, noting that

$$R_{p/t}\left(R_{s/p} - |k_{init}|/N\right) \approx R_{p/t} R_{s/p} \quad \text{for} \quad N \gg |k_{init}| \tag{4.22}$$

as is the case when taking into account the finite key limit. We split classical communications into (i) a global average for end-user connection speeds, (ii) the data rates given by the Institute of Electrical and Electronics Engineers (IEEE) Ethernet standards, and (iii) record data rates using experimental technology. We see that, in the worst case, the classical rates are seven orders of magnitude greater than $R_{s/t}$. While we would eventually expect to reach a saturation point for the amount of classical information transmissible across a single fibre, commonly referred to as the Shannon limit [202], the size of the gap indicates that this alone will not be enough to close it anytime soon.

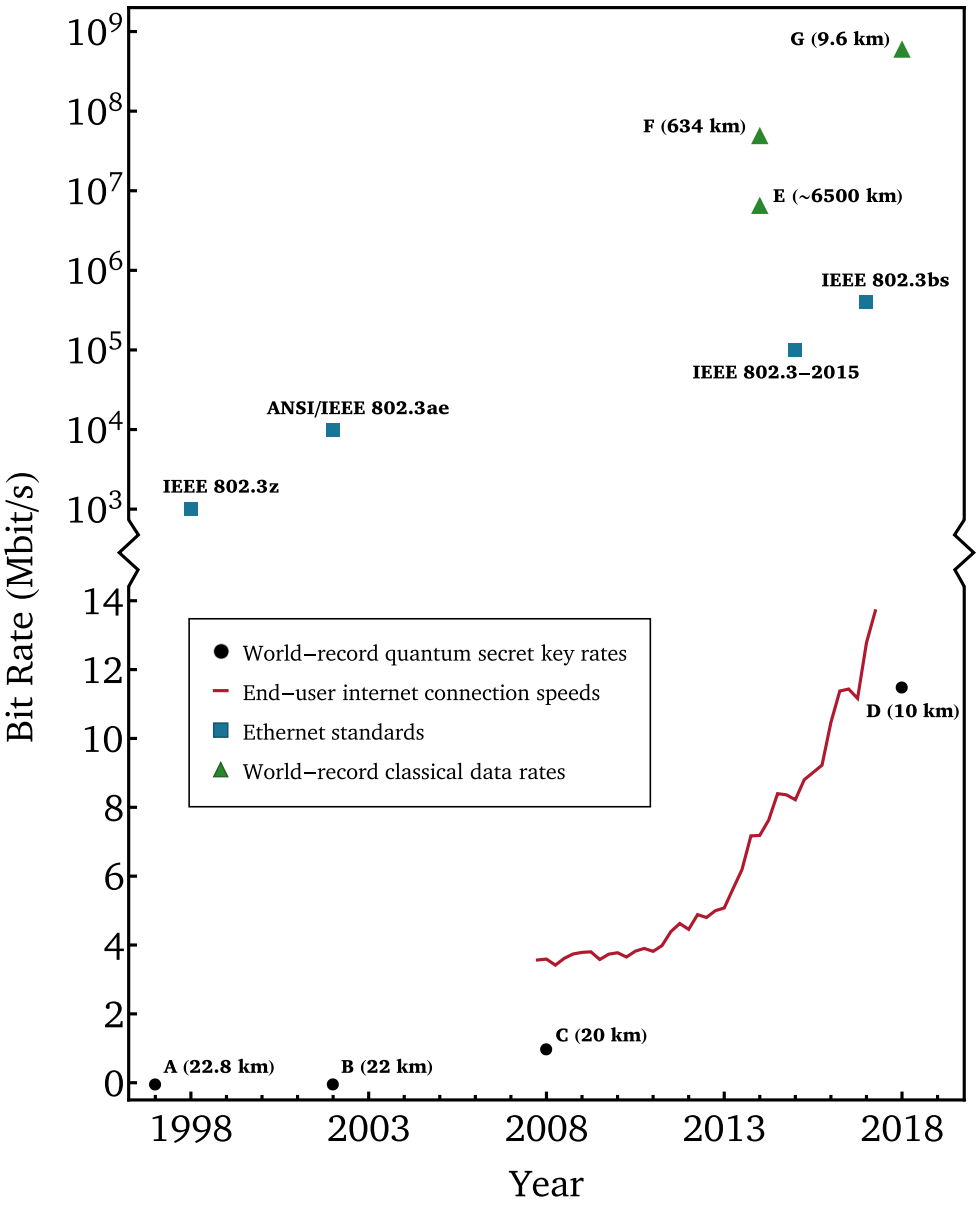


FIGURE 4.6: Comparing world-record quantum secret key rates with average end-user connection speeds, classical data rates from the IEEE Ethernet standards [165, 203–205], and world-record classical data rates using experimental technology. The protocols used for A, B, C and D were B92 [206], BB84 [207], BB84 with decoy states [208] and T12 [209] respectively. E was implemented on the Apollo South submarine cable with no customer disruption [210], F used dispersion-uncompensated single-mode fibre (SMF) [211], and G used a multicore SMF [212]. The end-user internet connection speeds are a global average, weighted by the number of unique Internet Protocol version 4 (IPv4) addresses in each country, and calculated from the data in [213].

In the best-case scenario, where only end-users take advantage of the OTP, it is not unreasonable to expect that QKD may reach the speeds required. However, a side effect of having many individual QKD devices in operation at the same time is that they must be easily multiplexable and, if the requirement of information-theoretic security extends to all parties, the situation becomes equivalent to that of protecting backbone networks rather than end-users. For the time being, we will make no further comment as to how feasible it is to implement such an architecture, though this will be the focus of chapter 7. A more important point is that, in almost all cases, critical infrastructure needs to be at least as secure as the end-user, but with much higher data rates (see, for example, the data centre emulated in chapter 3). Hence, a significant step-change is still required just to get to a point where we are limited by the work in section 4.1. That is not to say progress thus far has been based entirely on incremental improvements to the basic technology. For example, the development of dedicated post-processing modules was responsible for the 11.53 Mbit/s secret key rate set by [209] (see point D in figure 4.6). Yet it seems unlikely that we will ever reach a level where, experimentally,

$$\mathrm{Max}\left(R_{\mathrm{s/t}}\right) \geq \mathrm{Max}\left(\varsigma_{\wedge}\right) \tag{4.23}$$

This can be broken down into two reasons. Any piece of hardware that enables faster single-fibre-single-transmitter binary communication than contemporary classical methods will immediately supersede them, so at best quantum secret key rates can expect to equal classical data rates. However, the post-processing means $R_{\mathrm{p/t}}$ will always be greater than $R_{\mathrm{s/t}}$, and we would expect the R-value for standard communications over a quantum channel to fall between these, as privacy amplification will not be required.

Of course, this is still not enough to rule out everyday OTP deployment on the basis of the quantum channel, as we are yet to determine how easily equation 4.21 can be satisfied. In figure 4.7, we plot $\frac{t_1}{t_2-t_1}$ using the current record for the quantum secret key rate, and

$$0 \leq \varsigma_{\vee} < R_{\mathrm{p/t}}\left(R_{\mathrm{s/p}} - |k_{\mathrm{init}}|/N\right) \tag{4.24}$$

With regards to the on-peak data rates, we consider both the 2018 global average for end-users, weighted by the number of unique IPv4 addresses in each country, as well as the highest experimental data rate thus far achieved (see point G in figure 4.6), where the distance for the latter was 0.4 km less than that over which the record quantum secret key rate was realised. The global end-user average was calculated to be 20.41 ± 0.58 Mbit/s, based on data from [214]. The methods of collection are summarised in [215], from which it is clear that the dataset is suitably representative of real-world speeds available to electronic devices owned by end-users. We diverged from the long-term dataset on which figure 4.6 is based, as it was discontinued after the first quarter of 2017.

From figure 4.7, it can be seen that, with the exception of instances when off-peak end-user data rates are kept at no more than around 50% of their on-peak rates (i.e. scenarios adequately described by figure 4.7a, with $\varsigma_{\vee} \lesssim 0.5 \times 20.41$ Mbit/s), using the OTP remains impractical even if

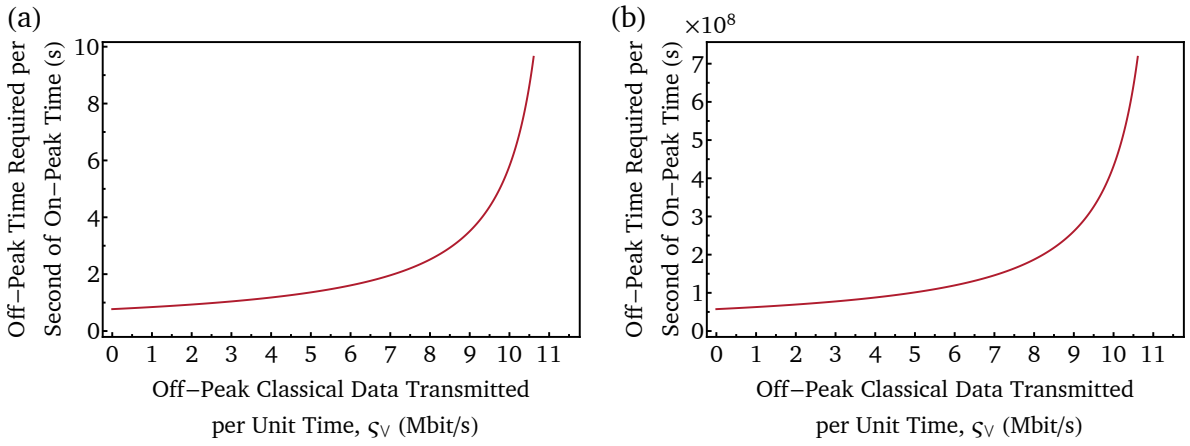


FIGURE 4.7: Showing the amount of off-peak time required per second of on-peak time in order to encrypt all data with a quantum-key-distribution-keyed one-time pad, and considering only limitations imposed by the quantum channel. We use the world-record quantum secret key rate, which was set in 2018 over a distance of 10 km (see figure 4.6). The amount of on-peak data transmitted per unit time is defined by (a) the 2018 global average for end-user data rates, weighted by the number of unique Internet Protocol version 4 (IPv4) addresses in each country, and calculated from the data in [214]; (b) the world-record classical data rate, achieved in 2018 over a distance of 9.6 km (see again figure 4.6).

ignoring the impact of the results from section 4.1. As before, bespoke networks with long periods of inactivity remain a possible application for QKD with OTP encryption. However, without the ability to multiplex several-orders-of-magnitude-worth of QKD devices, we are left with no choice other than to continue relying on computationally-secure ciphers such as AES for near-term protection of core infrastructure.

4.3 State of the One-Time Pad

Here, we summarise the hurdles that remain even when discounting the arguments put forth in sections 4.1 and 4.2. While not scientifically limiting, these are still important considerations if the OTP is to be widely deployed without introducing vulnerabilities. Overcoming them will take time, something that is lacking if QKD is to be used as a defence against quantum computers in the real world.

Furthermore, these issues are only likely to start being addressed if it can be demonstrated that a suitable method of key distribution exists, which does not introduce cumbersome overheads when paired with the OTP. Given the work presented thus far, we contend that DV-QKD does not fulfil such a criterion in its present form, despite the promise originally shown by basic theoretical

treatments, adding even more weight to the argument that AES will continue to be used for the majority of real-world encryption.

We first observe that although authenticated encryption modes exist for block ciphers, these cannot be directly applied to the OTP because they fundamentally rely on the ability to reuse a key in more than one application (see section 2.1.1). Any potential solution must go through standardisation. Otherwise, there is a high risk of implementation errors as end-users, not all of whom will have a strong security background, try to combine encryption and authentication themselves, something which is fraught with insecurities [216].

In addition, the OTP itself is yet to be standardised, due to lack of widespread demand. If the reader is wondering why this is necessary for an encryption scheme that seems so straightforward, consider the following. When logging into a website, the password field is effectively unlimited in length. Without knowing any information on a particular user's password, a sensible place to start might be by trying the most common passwords in use. However, if the user then inputs their password to the website, and that is transmitted using a OTP without some kind of length padding, the attacker suddenly knows how many characters have been sent, and can restrict their attack to the most common passwords of that length. Once again, not having a standardised option means that more knowledgeable programmers will implement custom solutions. However, historically, this has resulted in errors of sometimes fatal consequence (see, for example, the impact on the Battle off Samar when an enciphering clerk padded a request for information with "the world wonders", leading to misinterpretation of the message [10]).

4.4 Outlook

The work of this chapter substantiates the claim that single-qubit DV-QKD is incompatible with the OTP so long as both continue to exist in their current form. We have quantified the well-known fact that, at present, secret key rates are too slow, and explored the impact QKD has on the classical part of the network, finding that the demands are untenable. On the other hand, DV-QKD with AES-GCM is expected to scale well when transitioned from research networks to the real world.

We have stated throughout that our conclusions have no bearing on the use of the OTP in bespoke scenarios but, while we have identified examples of networks that receive infrequent use, we are yet to broach the subject of whether any exist for which the capacity is not fixed. Satellite networks are one example where this might be the case, as the quantum channel is introduced during the assembly process, rather than as a retrofit at a later date. Thus, assuming it is physically possible for each satellite to support the number of classical channels required, the network can be designed with QKD and the OTP in mind.

When it comes to laying more fibre, the story is different. Expanding communications networks is an expensive task, and those trying to address current internet bottlenecks prefer to invest money in other methods [210]. For example, in the United Kingdom, fibre-to-the-premises installations

were planned for only an extra 2 million buildings between 2017 and 2020, with 10 million receiving upgrades to existing copper-wire infrastructure instead [217]. Aside from the obvious impact this will have on deploying QKD nationwide (a solution for which can be found in section 6.5), this is strong evidence that, if the percentage load on an everyday network is too high to support a QKD-keyed OTP, then the number of additional fibres required would not be added quickly enough to protect against quantum attacks.

While other forms of QKD are not the focus of this thesis, the question of how they behave when subject to the analysis presented herein is an important one. We will close by performing a cursory examination of the more-obvious variants, highlighting areas that could benefit from further work.

4.4.1 An Attempt to Circumvent the Restrictions on the Quantum and Classical Channels

When considering alternatives to BB84-style protocols, a natural place to start is with CV-QKD. In its original form, squeezed states were required [218]. While these can now be generated at telecom wavelengths [219], they are heavily affected by losses [220], and are yet to be used as the basis for a practical QKD system. Instead, the focus has largely been on implementations using Gaussian-modulated coherent states, which are capable of reaching a secret key rate of 1 Mbit/s across 25 km of fibre, which equates to 5 dB of loss [221]. This is still below the record key rate for DV-QKD, and the types of information that must be sent over the classical channel remain the same; sifting does not take place per se, but Bob still needs to inform Alice how he measured [222]. Homodyne measurements will always return noise if the quantum bit (qubit) is lost en route, significantly increasing the number of error correction messages that must be transmitted in comparison to DV-QKD, where single-photon detection is used [87]. It is possible to observe both quadratures simultaneously by way of heterodyne measurements [223], removing the need for Bob to make and announce a choice. In a perfect world, this would lead to double the amount of information being retained, however Bob's results will be much noisier, meaning the key rate increases by a factor that is less than this [87]. In addition, post-selection is still required whenever the channel loss is > 3 dB [224], unless reverse reconciliation is used [222]. Thus, while other forms of CV-QKD seem to offer little in regard to sidestepping the arguments with which we are concerned, it is less clear for coherent-state heterodyne schemes, and a full analysis may reveal some benefit.

Another possibility is FL-QKD, for which a secret key rate of 1.3 Gbit/s was recently demonstrated over a channel with 10 dB loss [225]. The only caveat is that this implementation did not include full post-processing, which could lead to more modest key rates if additional bottlenecks are introduced by the parts of the system which are missing (see, for example, reference [209] where custom electronics had to be developed just to reach a 13.72 Mbit/s secret key rate). Unfortunately, while there is no reason to believe that issues of this kind are anything more than engineering challenges, the classical channel in FL-QKD is simply a higher-rate version of the one in BB84 [190], meaning we are still limited by section 4.1.

For protocols such as Ekert 1991 (E91) [226], that rely directly on quantum entanglement, the situation does not seem to get any better. Each entangled pair communicates only a single raw bit of information, though an extra basis compared to BB84 reduces the number of secret bits it carries, and increases the amount of classical information required to make each basis announcement. In addition, a Bell-type inequality is used instead of the QBER to identify whether or not an eavesdropper is present. This involves announcing the results for all measurements where the bases did not match, rather than a small subset of those that did, and so a full implementation of E91 in its originally-published form is likely to need a greater classical channel capacity than BB84.

On the other hand, superdense coding uses only a single qubit to communicate two bits of information, and can be generalised to higher-dimensional systems, transmitting r bits on a maximally entangled state such as [227]

$$|\psi\rangle = \frac{1}{\sqrt{r}} \sum_{\phi=1}^{r} |\phi\rangle\,|\phi\rangle \tag{4.25}$$

So long as we continue to encode in only two bases, the classical information that needs to be transmitted remains unchanged. Unfortunately, with the values for $\overline{R}_{c/s}$ given in table 4.1, the dimensionality required is likely to be on the order of hundreds. However, placing an exact number on this is non-trivial, as the number of secret bits carried by each qudit will not increase linearly with dimension.

Finally, the reusable OTP [228] may in principle help circumvent the arguments in both sections 4.1 and 4.2. There are practical issues to overcome, like how to ensure message completeness in the presence of loss. In addition, the regularity with which key needs to be refreshed is yet to be evaluated. Therefore, without further development, it is unclear as to whether or not the QKD paired with the reusable OTP could form an effective information-theoretically secure cryptosystem.

CHAPTER 5

QUANTUM KEY DISTRIBUTION FOR IMPERFECT ENCRYPTION SCHEMES

Declaration of Work

I identified the endpoint denial of service attack on QKD and developed the BB84-AES protocol unassisted, along with all of its variants. I carried out all of the analysis which followed including, but not limited to, the initial exploration of its security and the comparison with other protocols.

This work has previously appeared in [8], as well as being presented at both QCrypt and BQIT [7, 229]. Where appropriate, parts of the paper and extended abstracts have been reused, as the original text was written by me.

In an ideal world, the best cryptographic protocols would be both mathematically and physically unbreakable. Unfortunately, even if quantum key distribution (QKD) could be implemented such that it were impossible to carry out side-channel attacks, there is still an offensive strategy that will fatally compromise the system. By performing denial of service (DoS) on the quantum channel, Eve can force Alice and Bob to forgo communication or revert to other forms of key distribution, the security of which will depend on mathematical problems that are assumed to be computationally intractable with both quantum and classical resources. However, in the majority of cases, these are yet to be adequately probed.

Here, we use the results of chapter 3 to identify a new DoS attack that leverages provably fake users and is undetectable over its duration. The work of chapter 4 then allows us to introduce suitable DoS countermeasures, by relaxing the mathematical security of QKD such that it relies on the security of the encryption cipher. By making a few additional tweaks, we show that our

computationally secure QKD protocol can generate key from singly-detected two-photon terms, and run at exactly 100% sifting efficiency.

While our protocol may not be mathematically unbreakable, we argue that it is nonetheless a more secure approach for practical deployment if it enables the mitigation of DoS and side-channel attacks. This is particularly prudent in the case of the former, as DoS of classical systems was the third most prevalent network attack in 2017 [230–233] and has the second-highest financial cost per occurrence [234].

5.1 A New Denial of Service Attack on Quantum Key Distribution

In chapter 3, we demonstrated that the time taken for a networked ID Quantique Clavis^2 to generate a secret key is, at best, on the order of minutes. This exposes the system to a DoS attack that is easier to implement than attack 2.5 and has not previously been considered. To prevent man-in-the-middle attacks, it is required that the classical QKD channel be authenticated, and to retain information-theoretic security, this must be done using a Wegman-Carter message authentication code (MAC) [19] keyed with a pre-shared secret. The MAC has to be transmitted at the end of the QKD protocol, authenticating every message sent up to that point [121], as authenticating each message individually would prohibit net positive key generation (see section 2.3.1). Consequently, neither Alice or Bob will know whether the person they are communicating with is genuine until they have finished generating a secret key, so an imposter could deny service to other users simply by opening a connection and performing QKD. Figure 3.20 shows how long this could last for, assuming only one round of key generation is carried out by the attacker, and for a 10 km metropolitan-area network, the Clavis^2 will communicate with an illegitimate party for roughly 10 minutes before realising. We recall that for the same device, key generation starts to become intermittent at attenuations above 9 dB, meaning that while the average time taken for a successful round of QKD at 10 dB is close to 20 minutes, the DoS impact could be greater if other rounds fail, which happens in over 30% of cases. Ultimately, it makes sense for an attacker to maximise the attenuation on their link to keep the systems occupied for as long as possible. We summarise this as follows:

Attack 5.1: Endpoint Denial of Service. *Eve establishes a high-loss connection with Alice and performs low bit rate QKD up to the point where she fails the authentication. During this period, Alice and Bob are unable to generate new shared keys, which may also lead to DoS of their classical communications. The attack can be prolonged if agents of Eve are queued behind her, turning it into a distributed denial of service (DDoS) attack.*

After succumbing to attack 5.1, Alice and Bob may find that they have exhausted their supply of pre-shared secret. This, a well-established vulnerability that also has the potential to be exploited independently (see attack 2.6), has previously been counteracted by using a post-quantum digital signature to authenticate the next round of QKD [235]. So long as Eve cannot break said algorithm

in the short amount of time for which it is useful to her, full security is retained for all keys thereafter. However, by taking this approach, a primitive has been introduced that was not already part of the system, assuming non-cryptographic methods were used to share Alice and Bob's initial secret. The recovery mechanism can also be triggered relatively easily, allowing attack 2.6 to be used as a way of forcing public-key algorithms to be used for every successful round of QKD. Therefore, from both simplicity and security perspectives, a reactive strategy is less than ideal, and our protocol should relying on this kind of approach.

5.2 BB84-AES: A Quantum Key Distribution Protocol for Rapid Denial of Service Detection

We now move to fulfil the main objective of this chapter: preventing attack 5.1. A trivial solution, which preserves the information-theoretic security of Bennett-Brassard 1984 (BB84), would be to implement some form of access control that requests Eve verify her identity before she is allowed to connect. However, if there are no further checks until the end of the protocol, this could easily be circumvented by Eve switching out Bob for herself once key generation begins. Therefore, the most sensible approach is to authenticate every message exchanged by Alice and Bob.

Ideally, this will mean modifying equation 2.5 such that the initial shared secret can be reused without increasing the risk of an attacker being able to decrypt messages that rely on quantum keys. Brassard proposed in [236] that k_M could be defined as the output of a random function. In practice, this can be the cipher used for the data encryption, independently keyed with k_C. As specified in chapter 4, our encryption scheme relies on the Advanced Encryption Standard (AES), so we rewrite equation 2.5 as

$$\tau_i = h_{k_H}(m_i) \oplus \mathrm{AES}_{k_C}(s_i) \tag{5.1}$$

where h is an ε-almost universal hash function keyed by k_H, m_i is an arbitrary message and s_i is a public one-time number, or "nonce". A number of efficient authentication schemes such as poly1305-AES [21], UMAC [237] and VMAC [238] take this form, though their moduli for addition vary.

The choice to include AES-256 in the QKD authentication process is not just for the sake of simplicity, or so we can be confident that our cryptosystem will remain quantum-safe, though as this is our reason for using QKD in the first place, it is obviously important. Suppose that, despite all the analysis carried out thus far, AES has an undisclosed flaw, allowing attack 2.4 to be executed by a select few. The result would be catastrophic. However, it would be no different compared to if the AES-based data encryptor had been paired with canonical BB84 instead, because the encryption can be broken directly in either case, meaning attack 2.4 offers no advantage. Of course, the chances of this happening are thought to be very low, despite being difficult to quantify, and so even if a

bespoke network were to use the one-time pad for data encryption, the comparative reduction in mathematical security is outweighed by increased resilience against DoS attacks.

A further advantage of this approach is that, in a world where Eve cannot compromise AES, she may implement an unsuccessful version of attack 2.4 on only some of the qubits. In standard BB84, Alice and Bob will be aware of her presence, but have no way of knowing which qubits have been targeted, so the entire protocol must be aborted. In our case, the individual authentication of every basis allows Alice and Bob to identify which qubits had been attacked in this way, giving them the option to keep those that were unaffected.

The above changes ensure that, if Eve tries to carry out attack 5.1, she will deny service for fractions of seconds rather than tens of minutes before her presence becomes obvious. The next step is to look at whether we can gain any further benefits by capitalising on our use of a computationally-secure MAC.

Now that every basis announcement is accompanied by an authentication tag, an interesting property emerges. There are only two possible tags for any given key/nonce pair, depending on whether the qubit was prepared in the X basis or the Z basis, though the exact values are unpredictable for anyone not in possession of the key. This means that if Alice decides to send the tags on their own, without the plaintext basis announcement that they authenticate, Bob can compare the tags he would expect for each option, to work out how he should have measured the qubit.

Ideally, lack of knowledge about Alice and Bob's shared secret will prevent Eve from also identifying the correct bases using the authentication tags. That is, if they provide confidentiality, which is not a traditional requirement of a MAC, then she will be restricted in the amount of information she can gain from photon number splitting (PNS), as public basis announcements are a pre-requisite for attack 2.1. This is discussed further in section 5.3 however, in short, transmitting the basis information as proposed means two-photon pulses can contribute to the secure key rate. It is still possible to implement an alternative method for PNS on higher-order multi-photon terms (see attack 2.2), although all protocols are vulnerable to this unless, as in [79] and [239], additional eavesdropper detection mechanisms are implemented in the form of decoy states.

Of course, if the tags provide a level of confidentiality sufficient to prevent attack 2.1, there is no longer any reason for them to be transmitted after Bob has measured the qubits, as Eve is unable to obtain the information required to perform a man-in-the-middle attack. If the tags are transmitted in advance, Bob can work out how he needs to measure before each qubit arrives, thereby removing the stipulation to sift his raw key, a result that is equivalent to increasing the sifting efficiency from 50% to 100%.

Protocol 5.1 pulls together the methods we have developed for performing quantum-safe computationally-secure QKD. A streamlined version is presented in figure 5.1, the details of which can be found in section 5.4.1.

While we have assumed the quantum key will be used in computationally-secure cryptosystems,

it is still sensible to investigate the impact of a user who insists on encrypting their data with the one-time pad in a bespoke setting, despite its low efficiency and lack of authenticated encryption modes. In this scenario, we retain the advantages of our protocol but, as section 5.3 will further dissect, also expect to acquire everlasting security (see definition 5.1).

Definition 5.1: Everlasting Security. *Assume Eve is unable to break the key-exchange protocol over the period for which it is active. A cryptosystem has everlasting security if plaintexts that were encrypted with the corresponding key cannot be recovered by Eve, even when she develops unlimited computational power after key exchange is complete.*

This, along with perfect forward secrecy (see definition 5.2), cannot be achieved if the key is encrypted directly with AES. For such a scheme, perfect forward secrecy is unattainable because anyone who obtains the long-term shared secret can use it to extract past session keys from the ciphertexts, rather than returning a set of bases that are no longer of any use to adversaries who are not also in possession of the qubits.

Definition 5.2: Perfect Forward Secrecy. *Assume Eve is unable to break the key-exchange protocol over the period for which it is active. The protocol has perfect forward secrecy if, after completion, Eve compromises the initial shared secret but cannot recover the key that was distributed between Alice and Bob.*

Therefore, one should take care not to be fooled into thinking direct encryption of the key is a valid simplification of our protocol. Of course, a system based on this would not provide eavesdropper detection either, and compromising previous initial shared secrets at a later date will expose all keys distributed thereafter, even if the secret is updated after every key exchange with material from that session.

5.3 Initial Security Analysis of BB84-AES

While we do not aim to provide a formal security proof for BB84-AES in this thesis, there is a large body of literature that can be leveraged to perform an initial, high-level analysis. In the following section, we will consider each of the main points from our protocol and highlight some additional consequences that have been less prominent up till now.

5.3.1 Rapid Denial of Service Detection

To begin, we show that our choice of authentication tags and the way in which we handle them does not impact their unforgeability. This can be encapsulated as follows:

Protocol 5.1: BB84-AES (basic version)

SUMMARY: Alice expands a shared secret with Bob, using computationally-secure quantum key distribution and quantum-safe primitives.

1. *One-Time Setup.*
   (a) Two $(|k_{\text{init}}|/2)$-bit secrets are shared between Alice and Bob using out-of-band communications, a trusted third party or a post-quantum public-key algorithm.
   (b) A $|v|$-bit initialisation vector is transmitted from Alice to Bob in the clear, where $|v| \leq 64$.
2. *Nonce Generation.* A single-use number s_i is constructed by appending a $(128-|v|)$-bit counter to the initialisation vector. The counter starts at 0 and increments after each call made to the generator. It must be maintained across all rounds of QKD that use the same initial shared secret, and is not to be confused with the index i used in the mathematics of this thesis, where $1 \leq i \leq N$.
3. *Authentication Tags.*
   (a) The first shared secret is split into a 256-bit cipher key, k_{C}, and a $(|k_{\text{init}}|/2-256)$-bit hash key, k_{H}.
   (b) Alice generates a cryptographically-secure random bit, which is used to select a basis $B_i \in \{X, Z\}$, and computes the tag $\tau_i^{\text{A}} = h_{k_{\text{H}}}(B_i) \oplus \text{AES}_{k_{\text{C}}}(s_i)$. h is a universal hash function, the output of which can be called from memory after it has been evaluated once for each basis, and AES is the Advanced Encryption Standard block cipher.
   (c) Bob calculates $\tau_i^X = h_{k_{\text{H}}}(X) \oplus \text{AES}_{k_{\text{C}}}(s_i)$ and $\tau_i^Z = h_{k_{\text{H}}}(Z) \oplus \text{AES}_{k_{\text{C}}}(s_i)$.
4. *Key Exchange.*
   (a) Alice prepares a qubit $|\psi\rangle_i$ by generating a cryptographically-secure random number, $b_i \in \{0, 1\}$, and encoding it in the basis B_i.
   (b) Alice sends τ_i^{A} to Bob, closely followed by $|\psi\rangle_i$.
   (c) Bob compares τ_i^{A} with τ_i^X and τ_i^Z, to identify the basis in which he should measure. Upon receipt of $|\psi\rangle_i$, he will return b_i with probability $100\% - E_\mu$, where E_μ is the quantum bit error rate.
   (d) Bob announces whether or not the qubit arrived, by means of an authenticated response. He should maintain a separate nonce generator to Alice, paired with the second shared secret. As Bob's response need only be "Yes" or "No", he may choose to transmit it in the same way as Alice sends her bases.
5. *Loop.* Steps 3b, 3c and 4 are repeated for the remaining $N-i$ qubits sent from Alice to Bob. As multiple tags can be constructed in parallel, this may begin prior to completion of the previous iteration.
6. *Post-Processing.*
   (a) Error correction and privacy amplification are carried out as in BB84. The messages sent during this step can be authenticated in the same way as above.
   (b) $|k_{\text{init}}|$ bits are taken from the final key and stored for use as the initial shared secrets in the next round of QKD, and a new initialisation vector is publicly agreed upon.

Requirement 5.1: *If Eve tries to impersonate either Alice or Bob, the other party will be alerted to her presence by the authentication tag corresponding to the first qubit she sends after establishing a connection.*

The security of a MAC that accompanies a known message is well established when it takes the form of equation 5.1. For a 128-bit tag, all forgeries will be rejected with probability close to 1, so long as AES cannot be distinguished from a uniform random one-to-one function, an attacker sees no more than $\sqrt{\#\mathcal{K}_{\mathrm{M}}} = 2^{64}$ messages and, as in conventional QKD, our hash function has small differential probabilities (see section 2.1.2) [240]. Here, $\mathrm{AES}_{k_{\mathrm{C}}}(s_i) \in \mathcal{K}_{\mathrm{M}}$ and $\#\mathcal{K}_{\mathrm{M}}$ represents the cardinality of the set.

As a result, just under 2^{64} quantum bits (qubits) can be individually accompanied by a MAC, assuming Bob uses a separate initial secret key with an independent nonce for sending authenticated replies to Alice. A number of tags must also be retained for messages relating to other parts of the protocol, such as error correction. It has already been mentioned in section 4.1 that $\gtrsim 10^5$ raw bits must be exchanged and processed for finite-key security, meaning we can complete up to $\sim 10^{14}$ rounds of QKD before the scheme needs to be rekeyed. Therefore, no obvious concerns present themselves with regards to a simple reduction in the mathematical security of the authentication tags relative to BB84, given we are confident in the security of AES and are unlikely to exceed the maximum number of tags that can be generated under a single key.

Of course, the protocol presented herein takes a further step, choosing to transmit the tags on their own rather than alongside a message. The attacker gains no advantage from such a feature, as the plaintext can always be ignored in the case where the bases are publicly announced, so the bound for rejecting forgeries will remain the same.

The impact of this is two-fold. First, attack 2.6 is no longer viable, as an eavesdropper needs to establish more than eighteen billion billion connections before Alice and Bob will be prevented from constructing any more MACs of the form given by equation 5.1. Second, even if Eve were able to ensure key generation only failed at the very last moment, the number of times she would have to repeat her attack in order to exhaust Alice and Bob's shared secret is still on the order of a hundred trillion, given the rekeying limit specified above, and assuming they only began with the minimum number of bits required to construct a secure MAC. For networks of sufficient size, we would expect them to find a link that she cannot influence long before reaching that limit.

5.3.2 100% Sifting Efficiency

Next, we consider a point of functionality, the proof of which is derived from the security of the MAC. To avoid sifting our raw key, the following must be true:

Requirement 5.2: *Bob can obtain full information on the correct measurement bases from the authentication tags that Alice transmits in advance.*

Bob can only identify the correct basis so long as the MACs that represent each option are distinguishable from one another. Therefore, it is imperative that

$$h_{k_H}(X) \neq h_{k_H}(Z) \tag{5.2}$$

Consider a hash function family that is at least ε-almost universal, a condition fulfilled by those used in both of the MACs that we recommend [237, 238]. Then, the probability of violating equation 5.2 is

$$\text{Prob}(\text{Collision}) \leq \varepsilon \tag{5.3}$$

It is known that the MAC in which the hash family is used can be broken with success probability [241]

$$\text{Prob}(\text{Successful attack}) \leq \varepsilon + \delta \tag{5.4}$$

where δ is the chance of an attacker distinguishing AES from a truly random function, given that block ciphers can be considered pseudorandom functions (PRFs). Therefore,

$$\text{Prob}(\text{Bob cannot obtain basis}) \leq \text{Prob}(\text{Successful attack}) \tag{5.5}$$

and we can be confident that BB84-AES will satisfy requirement 5.2.

5.3.3 Authentication Tag Confidentiality

A radical difference between BB84-AES and all other forms of QKD is that we transmit the basis information ahead of the qubits. Depending on how this is implemented, it may be possible for Eve to carry out a successful intercept-resend attack, as described in section 2.3.2. Requirement 5.3 identifies the properties that the chosen MAC must have to ensure this strategy is no more possible than in standard BB84.

Requirement 5.3: *The authentication tags must provide confidentiality against an eavesdropper, such that she cannot obtain any information on the correct measurement bases.*

Consider an arbitrary message m_j that can be encrypted with the Advanced Encryption Standard running in Counter Mode (AES-CTR) as described in section 2.1.1, meaning

$$c_j = m_j \oplus \text{AES}_{k_C}(s_j) \tag{5.6}$$

where c_j is the ciphertext and s_j is a nonce. The security of Counter Mode with a PRF is discussed in [242], and this forms the foundation for showing that AES-CTR provides confidentiality, by

reason of block ciphers being considered strong pseudorandom permutations (PRPs) that can be treated as PRFs [243]. Up to 2^{64} messages can be encrypted with AES-CTR [242], so long as the counter contained within the nonce is of length 64 bits or more, with the remainder comprised of random bits. This limit is the same as that imposed by section 5.3.1 to ensure unforgeability of the authentication tags.

Because AES-CTR is plaintext agnostic, it is perfectly legitimate to choose

$$m_j = h_{k_H}(m_i) \tag{5.7}$$

where $h_{k_H}(\cdot)$ is a keyed hash function, and m_i is also an arbitrary message. Therefore, equation 5.6 can be rewritten as

$$c_j = h_{k_H}(m_i) \oplus \mathrm{AES}_{k_C}(s_j) \tag{5.8}$$

We observe that when $s_j = s_i$ this is equivalent to equation 5.1, and so

$$\mathcal{T} \subset \mathcal{C} \tag{5.9}$$

where $\mathcal{T}$ is the set of all possible authentication tags that take the form of equation 5.1 and $\mathcal{C}$ is the set of all possible ciphertexts that take the form of equation 5.6.

Hence, our authentication tags provide confidentiality with regards to the output of the hash function, assuming that AES is quantum-safe, and meaning that Eve will be unable to work out which basis to measure in given only a properly implemented 128-bit tag. This is not particularly surprising given the purpose of the exclusive-OR (XOR) in a Wegman-Carter-style MAC is to mask the output of the hash function such that k_H can be reused for multiple messages.

Our tag construction cannot be utilised as an authenticated encryption mode in general, because the hash prevents recovery of m_i upon decryption. So long as equation 5.2 holds, this is of no issue to us, however it is worth noting that true authenticated encryption modes exist and, if we were happy to move further away from vanilla BB84, these could be used instead of our authentication tags. The consequences of making such a choice will be discussed more thoroughly in section 5.6.1.

5.3.4 Resistance to Photon Number Splitting Attacks on Two-Photon Pulses

Requirement 5.4: *It follows from requirement 5.3 that an eavesdropper capable of mounting a two-photon number splitting attack can, at best, obtain the same amount of information on the final key as when Scarani-Acín-Ribordy-Gisin 2004 (SARG04) is used instead.*

In SARG04 (protocol 2.6), Alice publicly declares two possibilities for the state she transmitted, instead of announcing the basis she prepared in. If Eve wants to obtain full information on the key by taking advantage of multi-photon terms, she must carry out attack 2.2, blocking all pulses containing less than three photons and performing unambiguous state discrimination on the remainder [43, 244].

The confidentiality provided by our authentication tags is, from an attacker's perspective, equivalent to Alice not announcing the bases at all. We could choose to announce two possible states as in SARG04, and then the attacker would have the same amount of information on the final key. Not making this announcement gives the attacker zero advantage, as they can always discard the information if it is given to them. Therefore, BB84-AES is at least as resilient as SARG04 against PNS attacks on two-photon pulses. Unambiguous state discrimination does not require an eavesdropper to have access to the public channel, meaning both protocols appear to be equally vulnerable in this regard.

5.3.5 Perfect Forward Secrecy when Combining BB84-AES with Encryption Based on the Advanced Encryption Standard Block Cipher.

Our next requirement comes directly from definition 5.2:

Requirement 5.5: *An attacker who compromises the initial shared secret during the current round of the protocol cannot use this to obtain keys that were distributed using the same initial shared secret in previous rounds of the protocol.*

An attacker who compromises the initial shared secret from a previous round gains the ability to forge tags from that round (though to no effect as key exchange is already complete) and find out the bases used. This also happens in the case of an attacker gaining unlimited computational power. Therefore, if we can prove everlasting security of BB84-AES when encrypting data with the one-time pad (OTP), it follows that requirement 5.5 will be satisfied.

5.3.6 Everlasting Security when Combining BB84-AES with the One-Time Pad Encryption Scheme

Here, we question whether pairing BB84-AES with the OTP results in a cryptosystem with everlasting security. Unlike in previous sections, there are now two requirements to be fulfilled.

Requirement 5.6: *An attacker who gains unlimited computational power after the conclusion of the protocol cannot gain any knowledge on the key from the information transmitted in the authentication tags, assuming AES remained secure for the duration of the protocol.*

In BB84-AES, the authentication tags are used to secretly communicate a subset $\mathcal{I}$ of the classical information exchanged by Alice and Bob. In standard BB84, $\mathcal{I}$ is communicated publicly during the protocol, after all qubits have been exchanged. This means that after the conclusion of BB84, $\mathcal{I}$ is known to the attacker, and the fact this does not compromise the security is of fundamental importance in QKD [86]. Therefore, if an attacker manages to extract $\mathcal{I}$ after the conclusion of BB84-AES, the protocol remains secure, as they have no more information than in the standard case.

Requirement 5.7: *An attacker who gains unlimited computational power after the conclusion of the protocol cannot gain any knowledge on the key by exploiting the newly forgeable authentication tags, assuming AES remained secure for the duration of the protocol.*

In [245], it is shown that, for computationally-secure QKD, bounds on the attacker's classical runtime, quantum runtime and quantum memory need only be applied to ensure the classical channel cannot be tampered with during the course of the protocol. Afterwards, standard QKD arguments hold, whereby the authenticity of the classical channel is no longer of relevance, even in the case of general attacks.

As we are considering an attacker who cannot inject, reorder or modify authentication tags that were sent and received in the past, requirement 5.7 should be satisfied, so long as Eve was sufficiently bounded during the execution of the protocol such that she was unable to break the computationally-secure authentication scheme. For security against quantum computers, this means we are assuming AES is a quantum PRF, although there is no guarantee this will follow from the fact that block ciphers may be considered standard PRFs [246].

5.3.7 The Role of Randomness in BB84-AES

Finally, we will show that in the absence of an attacker, keys output by BB84 and BB84-AES are equally random. Since the authentication tags are used only in the communication of information, this boils down to asking whether Bob's failure to inject additional random numbers has an adverse effect on the entropy of the final key. The short answer is no, and it is important to realise that any answer to the contrary would also apply in the case where Alice and Bob both randomly generate the same set of bases with probability $\frac{1}{2^N}$. If Alice is using an ideal quantum random number generator (QRNG) then the key she transmits will have maximum entropy. In conventional QKD, Bob's random bit deletion becomes a matter of practicality rather than doing anything to further mitigate Eve's ability to guess the final key, assuming he also uses an ideal QRNG. Therefore, removing this step does nothing to reduce the randomness in the output of BB84-AES.

However, in standard BB84, the situation changes somewhat if an insecure or backdoored random number generator (RNG) is used for basis selection at either end. While the outcome is trivial when the same RNG is used for Alice's bit selection (an eavesdropper will be able to obtain the key without further interference), this is not enforced, so we stick to a more general implementation where different RNGs are used for Alice's bits, Alice's bases and Bob's bases. This configuration gives rise to two possible attacks:

Attack 5.2: Predictable Alice. *If Eve can anticipate Alice's random sequence, she will be able to intercept the qubits, measure in the correct basis and resend. Assuming zero errors, her measurements return the same raw key as Alice, which can be correctly sifted when the bases are publicly compared.*

Similarly,

Attack 5.3: Predictable Bob. *If Eve can anticipate Bob's random sequence, she will be able to intercept the qubits, measure using his set of bases and resend. Assuming zero errors, her measurements return the same raw key as Bob which can be correctly sifted when the bases are publicly compared.*

In BB84-AES, attack 5.3 reduces to attack 5.2 without sifting. As Bob is not generating any extra randomness himself, the predictability of his measurement bases is determined by Alice's RNG. Therefore, Bob needs to trust Alice has made sensible implementation decisions, but given attack 5.2 exists in conventional QKD anyway, this is nothing new, and Eve's ability to exploit a faulty RNG remains unaffected.

5.4 Optimising BB84-AES for Resource-Limited Applications

5.4.1 Reduced Processing Variant

While it is perfectly feasible to implement protocol 5.1 as presented in this thesis, there are a number of variations that can reduce demand on the computational and/or communications resources. The first of these is summarised in protocol 5.2, where we allow Bob to check only whether the tag he receives is a match for that corresponding to a measurement in the X basis. This requires marginally less memory and processing time than individual basis authentication in otherwise-standard BB84. The trade-off is that if Eve measures in the Z basis, she no longer needs to be able to forge the corresponding authentication tag, ensuring only that the one she forwards, τ_i^{E}, is different to that sent by Alice. However, Eve still has not broken the authentication scheme, meaning she cannot obtain any basis information or force Bob to measure in the X basis, and so this kind of interference will be exposed by the quantum bit error rate (QBER). Table 5.1 gives the outcomes for all of Eve's possible strategies. By averaging the error probabilities for different combinations of forwarding choices, it is clear that $\tau_i^{\mathrm{E}} \equiv \tau_i^{\mathrm{A}}$ remains optimal.

5.4.2 Reduced Bandwidth Variant

Next, we look at the effect of requiring the classical channel to communicate the bases using 128× the number of bits transferred over the quantum channel. Given the Clavis^2 emits laser pulses clocked at 5 MHz [156], the classical data rate needs to be 640 Mbit/s. For comparison, the Bristol and UK

Protocol 5.2: BB84-AES (reduced processing)

SUMMARY: Replaces steps 3c and 4c in protocol 5.1, halving the number of XOR operations and tag comparisons that Bob has to carry out.

3. *Authentication Tags.*

   (c) Bob calculates $\tau_i^X = h_{k_H}(X) \oplus \mathrm{AES}_{k_C}(s_i)$.

4. *Key Exchange.*

   (c) Bob compares τ_i^A with τ_i^X. If it matches, he will choose to measure in the X basis. Otherwise, he will choose to measure in the Z basis. Upon receipt of $|\psi\rangle_i$, he will return b_i with probability $100\% - E_\mu$, where E_μ is the quantum bit error rate.

Can be combined with: BB84-AES (reduced bandwidth)

TABLE 5.1: Showing the probability of a bit-flip error occurring between Alice and Bob, depending both on the bases chosen by each of the three parties and whether or not Eve blindly modifies the authentication tag.

Alice's Basis	Eve's Basis	Forwarding Choice	Bob's Basis	Prob(error)
X	X	$\tau_i^E = \tau_i^A$	X	0
X	X	$\tau_i^E \neq \tau_i^A$	Z	0.5
X	Z	$\tau_i^E = \tau_i^A$	X	0.5
X	Z	$\tau_i^E \neq \tau_i^A$	Z	0.5
Z	X	$\tau_i^E = \tau_i^A$	Z	0.5
Z	X	$\tau_i^E \neq \tau_i^A$	Z	0.5
Z	Z	$\tau_i^E = \tau_i^A$	Z	0
Z	Z	$\tau_i^E \neq \tau_i^A$	Z	0

quantum networks on which the Clavis[2] systems are being deployed, and which were the focus of chapter 3, both have enhanced small form-factor pluggable (SFP+) and enhanced quad small form-factor pluggable (QSFP+) channels with capacities of 10 Gbit/s and 40 Gbit/s respectively. While the gap appears large between what we need and what we can provide, pre-commercial quantum hardware has been shown to be capable of reaching super-GHz clock speeds [247]. Due to the way in which the BB84 states were encoded in this example, the qubit preparation rate was only 560 MHz, however to avoid a potential future where more efficient encoding techniques mean our protocol necessitates two transceivers be multiplexed together, we can reduce our tag lengths as described in protocol 5.3. This remains secure for up to 2^{32} messages [240], allowing $\sim 10^4$ full rounds of QKD per initial key, and brings the classical communications requirements to within the capabilities of 100 Gbit/s quad small form-factor pluggable (QSFP28) or 100 Gbit/s C form-factor pluggable (CFP4) transceivers.

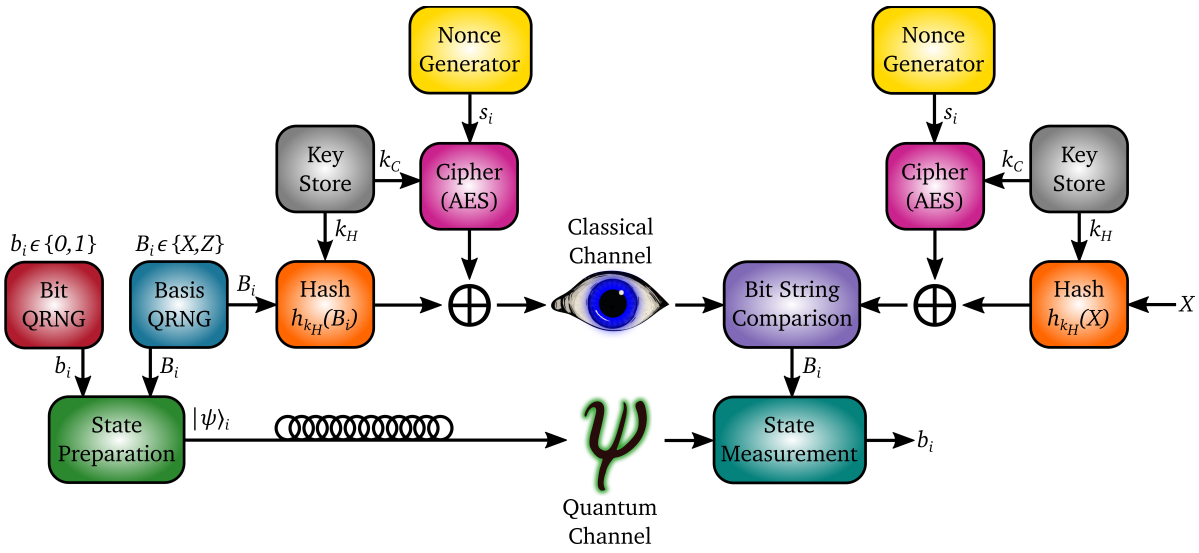


FIGURE 5.1: Block diagram showing the transmission of a single bit of key from Alice to Bob for BB84-AES with reduced processing.

Protocol 5.3: BB84-AES (reduced bandwidth)

SUMMARY: Replaces the 128-bit tags in protocol 5.1 with 64-bit tags of the same form. UMAC [237] and VMAC [238] both provide such functionality, without dropping below the required security level.

Can be combined with: BB84-AES (reduced processing), BB84-AES (dense information transfer)

5.4.3 Dense Information Transfer Variant

The final optimisation reduces demand on the classical channel by grouping multiple bases into a single authentication tag (protocol 5.4). The time taken to establish the presence of a fake user should not change significantly, because the tags are still transmitted ahead of the first qubit in every group. Of course, the processing at Bob's end will be expected to take slightly longer than before, as a MAC that represents ξ bases will have $\beta = 2^{\xi}$ possible values for each key/nonce pair. His method for identifying the correct set of measurements differs from protocol 5.1 in that he must compute all possible hashes and store them in a lookup table. He can then XOR the incoming tag with the AES-generated key, and compare. Combining protocol 5.3 with protocol 5.4 will speed up the hash function [238], thereby reducing the time taken to construct the table. The necessary calculations can be performed during downtime, or in parallel with device and fibre characterisation, or in parallel with a previous round of QKD provided each initial shared secret is used across multiple rounds. An important subtlety, that is also true for protocols 5.1, 5.2 and 5.3, is the hashes only need to be computed once so long as the initial secret remains unchanged, meaning the lookup table only needs to be reconstructed when this is refreshed.

Protocol 5.4: BB84-AES (dense information transfer)

SUMMARY: Replaces steps 3b, 3c, 4a, 4b, 4c and 5 in protocol 5.1, grouping multiple bases into a single tag to reduce the necessary channel capacity by a factor of $|\tau|(\xi-1)$. $|\tau|$ is the tag length in bits, and ξ is the number of bases per tag. We redefine the range of i values such that $1 \leq i \leq \frac{N}{\xi}$.

3. *Authentication Tags.*

   (b) Alice generates ξ cryptographically-secure random bits, which are used to select bases B_η through $B_{\eta+\xi-1}$, where $B_{\eta+\Xi} \in \{X, Z\}$, $\eta = 1+(i-1)\xi$ and $\Xi \in \{0, \ldots, \xi-1\}$. It is required that $1 < \xi \ll N$. She computes the tag $\tau_i^{\mathrm{A}} = h_{k_{\mathrm{H}}}\left(B_\eta || \ldots || B_{\eta+\xi-1}\right) \oplus \mathrm{AES}_{k_{\mathrm{C}}}(s_i)$. h is a universal hash function, AES is the Advanced Encryption Standard block cipher, and $||$ is used to indicate a concatenation.

   (c) Bob calculates $h_{k_{\mathrm{H}}}\left(B_\eta || \ldots || B_{\eta+\xi-1}\right)$ for all 2^ξ possible values of $B_\eta || \ldots || B_{\eta+\xi-1}$, storing the results in ascending order. He also evaluates $\mathrm{AES}_{k_{\mathrm{C}}}(s_i)$ separately.

4. *Key Exchange.*

   (a) Alice prepares the qubits $|\psi\rangle_\eta$ to $|\psi\rangle_{\eta+\xi-1}$. This is done by generating ξ cryptographically-secure random numbers, b_η through $b_{\eta+\xi-1}$ where $b_{\eta+\Xi} \in \{0, 1\}$, and encoding them in the bases B_η through $B_{\eta+\xi-1}$ respectively.

   (b) Alice sends τ_i^{A} to Bob, closely followed by all $|\psi\rangle_{\eta+\Xi}$ for the corresponding value of i.

   (c) Bob computes $\tau_i^{\mathrm{A}} \oplus \mathrm{AES}_{k_{\mathrm{C}}}(s_i)$ and checks it against the lookup table he constructed in step 3c, to identify the bases in which he should measure. Upon receipt of $|\psi\rangle_{\eta+\Xi}$, he will return $b_{\eta+\Xi}$ with probability $100\% - E_\mu$, where E_μ is the quantum bit error rate.

5. *Loop.* Steps 3b, 3c and 4 are repeated for the remaining $N - i\xi$ qubits sent from Alice to Bob. As multiple tags can be constructed in parallel, this may begin prior to completion of the previous iteration.

Can be combined with: BB84-AES (reduced bandwidth)

To prevent a simple timing attack, Alice can never send the qubits until the worst-case lookup time has elapsed, so Bob must take care to select a search algorithm that is optimal in this regard. One possible option would be a binary search [248], which makes no more than $\lfloor \log_2 \beta \rfloor + 1 = \xi + 1$ comparisons.

The exact value of ξ reflects a trade-off between computational and communications resources, and it is clear from figure 5.2 that the greatest benefits can be achieved when $1 < \xi \ll 32$, because of the exponential behaviour demonstrated by both the classical channel capacity and memory requirements. As a concrete example, we will consider the Bristol Quantum Network (see chapter 3), which is hosted on pre-existing infrastructure, with each node's server containing sixty four Intel Xeon E5-2697A v4 processors. By implementing a binary search on a single central processing unit (CPU), without hardware-specific optimisation, we can estimate the performance of our protocol on a real system. If we assume a 64-bit tag and want to employ only a single SFP+ (QSFP+) channel, then $\xi = 8$ ($\xi = 2$) maximises the QKD clock rate while trying to use the least possible memory. In this case, it takes 6.940 ± 0.085 ns (2.085 ± 0.017 ns) to run the search, allowing for a 1.153 ± 0.014 GHz (0.959 ± 0.008 GHz) clock and consuming 2048 bytes (32 bytes) of memory,

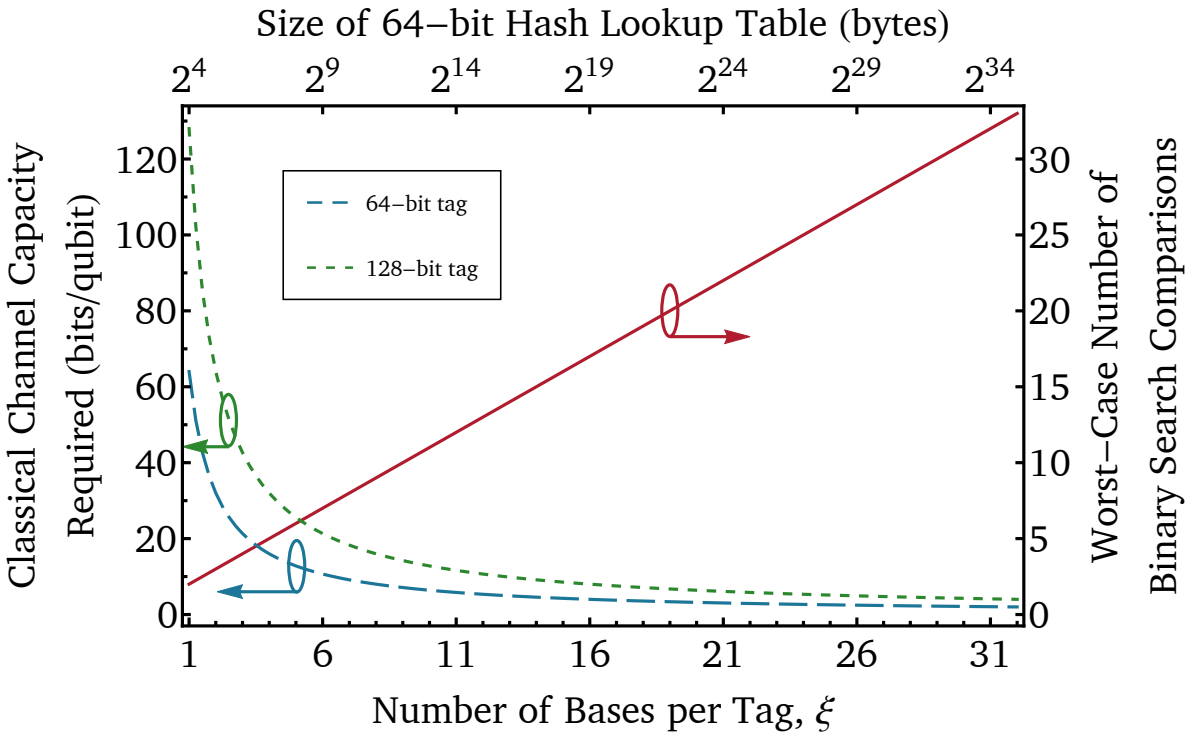


FIGURE 5.2: Illustrating how changing the number of bases represented by a single authentication tag affects both classical communication and computational resource requirements for BB84-AES with dense information transfer. To get a rough estimate for how our protocol will perform on a particular physical system, one can multiply the classical channel capacity by the QKD clock rate, and worst-case number of comparisons by the time taken to perform a single binary search comparison. The size of a 128-bit hash lookup table will always be double that of its 64-bit counterpart.

out of 87.7 GiB available (1 GiB $= 2^{30}$ bytes) and 131.7 GiB total random-access memory (RAM). To run a hypothetical 1.72 GHz-clock BB84 device, based on the technology in [247], would require $\xi = 12$ ($\xi = 3$). In this instance, the search takes 9.692 ± 0.039 ns (2.881 ± 0.036 ns), and 32,768 bytes (64 bytes) of memory is required. However, it is important to note that while these parameters are sufficient to enable the use of presently-installed transceivers, the quantum clock is still capped at 1.238 ± 0.005 GHz (1.041 ± 0.013 GHz) because of the maximum search time. Hence, some parallelisation will also be required, in that each search must begin before the previous one is guaranteed to have finished.

Technically, the higher the value of ξ, the easier it is for Eve to guess one of the $2^{\xi} - 1$ other authentication tags that Bob will accept. A correct guess is still highly improbable, and so she will almost certainly be detected, but even if successful, Eve controls only whether or not Bob measures with the same bases as Alice. Hence, this is nothing more than a restricted version of the strategy she can employ in protocol 5.2 and, in the unlikely case of an odds-defying set of forgeries, Alice

and Bob will be made aware of Eve's presence by the QBER.

5.5 Comparing BB84-AES with Other Photon-Number-Splitting-Resistant and Highly-Efficient Quantum Key Distribution Protocols

While BB84-AES is the only protocol that offers protection against attack 5.1, other solutions exist that increase the sifting efficiency and resist PNS attacks. One may question why we should not use these instead. If we are concerned about DoS, the reasons are obvious, however a more detailed comparison is required for the other characteristics, as summarised in table 5.2.

We first consider biased basis QKD which, conditional on the number of photons transmitted, can be used to asymptotically double the efficiency of BB84 (see protocol 2.8). In rare situations on bespoke networks, there may be an argument in favour of retaining information-theoretic security, however we are concerned with everyday communications, and so have already waived our interest in this. Now, transmitting the tags in advance of the qubits is a slightly preferable solution, partly because the efficiencies of real and simulated biased basis experiments are still noticeably lower than 100% [83–85], however assuming no additional countermeasures are employed, the protocol described in [82] is also vulnerable to a more simplistic PNS attack than that which is applicable to vanilla BB84. This, attack 5.4, is possible due to the recommendation that key be generated from a single basis, with the other used only for eavesdropper detection. The fact that a quantum memory is no longer required makes it a much more realistic exploit for modern-day implementations than attack 2.1, emphasising why it is imperative to use decoy states in any current system relying on biased bases. In contrast, the aforementioned Clavis^2 predominantly uses unbiased SARG04, which has the same level of PNS-resistance as the protocol described herein, and falls back on unbiased BB84 for short distances where SARG04 is not proven secure [244]. This may be considered acceptable so long as quantum memories remain in the early stages of development.

Attack 5.4: Photon Number Splitting Against Biased Bases. *Assume Eve does not possess a quantum memory but is otherwise unchanged. She performs a quantum non-demolition measurement on the number of photons in each pulse and blocks all single-photon terms. For the remainder, she splits off at least one photon from every pulse, and allows at least one photon to carry on towards Bob. Eve immediately measures her copy in the key generation basis. When Alice and Bob publicly sift their qubits, she can identify those used for eavesdropper detection, and discard any information she has on them. Every bit of her final key has now been correctly measured, without revealing her presence.*

SARG04 itself resists two-photon PNS by modifying the public announcements of BB84 (see protocol 2.6). However, as a consequence, the sifting efficiency is reduced to 25%, so there are clear

advantages to using BB84-AES over both biased bases and this.

In contrast, decoy states do offer an improvement over the work of this chapter, in that they can protect against higher-order PNS (attack 2.2). Yet their presence diminishes the overall sifting efficiency, as only signal states contribute to the final key, fundamentally limiting the secret key rate even when combined with either biased basis QKD or BB84-AES. There is currently no clear way round this. If resilience against three-photon number splitting is required, decoy states are the only available solution, and the reduction in efficiency must be accepted. However, it is worth noting that state-of-the-art QKD performances are still a considerable way off any theoretical upper limits so, at present, decoy states actually increase key rates, as they allow for higher mean photon numbers than would otherwise be considered secure.

5.6 Outlook

In this chapter, we have shown that by reducing the mathematical security of BB84, it is possible to almost instantly detect denial of service that leverages provably fake users, a novel attack to which all standard quantum key distribution protocols are vulnerable. Our design is inherently resilient against attempts to exhaust Alice and Bob's supply of initial secret key, but does not lead to large memory overheads because of this, nor does it operate reactively by falling back on public-key cryptography. In changing how and when the bases are announced, we are able to achieve exactly 100% efficiency and, instead of posing a risk to security, two-photon terms now contribute positively to the final key rate. In both cases, this is independent of the distance or the number of bits exchanged, and without further cost.

Such advantages are possible only so long as the output of the cipher used to construct our authenticators is indistinguishable from the output of a random permutation. This criterion is the same as that for ensuring the security of quantum-safe encryption schemes used in day-to-day communications. We have already shown that it is impractical to supersede said cryptosystems with a QKD-keyed OTP, due to the high volume of information transmitted over the classical channel for every quantum bit, and because the secret key rates are orders of magnitude lower than overall network data rates. Therefore, having to sacrifice information-theoretic security is not overly concerning and, in any case, the chances of the indistinguishable-output assumption being violated are far lower than the likelihood of an attacker exploiting one of the weaknesses that our protocol defends against.

Of course, the size of our authentication tags means BB84-AES increases the number of classical bits per quantum bit even further, and we must show that it does not render the Advanced Encryption Standard running in Galois/Counter Mode (AES-GCM) unusable when subject to the analysis of section 4.1. Figure 5.3 presents results for a simulated ID Quantique Clavis^2 implementing BB84-AES in its basic form (protocol 5.1). For a real Clavis^2, we assume that each basis is represented by a single bit in the classical channel, as the actual encoding is unclear. Thus, in the worst-case, we

TABLE 5.2: Comparing BB84-AES, BB84 with biased bases, SARG04 and BB84 with decoy states. It is possible to combine biased basis and decoy state BB84, with sifting efficiency $\lim_{N\to\infty} \zeta = \text{Prob}(\text{Signal})$.

	BB84-AES	Biased Basis BB84	SARG04	Decoy State BB84
Mathematical Security with One-Time Pad	PC (short term) IT (long term)[†]	IT	-- (low loss) IT (higher loss)	IT
Mathematical Security with AES-GCM	PC	PC	-- (low loss) PC (higher loss)	PC
Endpoint Denial of Service Resistance	Yes	No	No	No
Photon Number Splitting Resistance	Two-photon	No	Two-photon	Yes
Sifting Efficiency (ζ)	100%	$\lim_{N\to\infty} \zeta = 100\%$	25%	$\frac{1}{2} \times \text{Prob}(\text{Signal})$
Requires Hardware Changes	No	Sometimes	No	Yes

[†] Here, long-term security works under the assumption that the scheme was not broken at the time of key exchange.

Key: IT = Information Theoretic; PC = Practical Computational; -- = Unproven.

expect an extra 127 classical bits to be transmitted for every secret bit generated by BB84-AES, and this is the scenario we simulate. The outcome is that BB84-AES with AES-GCM sits in between BB84 with the OTP and BB84 with AES-GCM (see figures 4.4 and 4.5 respectively). However, it is close enough to the latter that we can be satisfied the additional classical overhead has not compromised ease of deployment, with the off-peak data rates limited to 99.99998(5)% of the classical channel capacity.

If one were to insist on unconditional security in a bespoke setting, individual basis authentication could be performed using AES-derived tags in standard BB84, reauthenticating everything at the end with a traditional Wegman-Carter MAC. However, attack vectors may still exist for exhausting the initial shared secret and, given the issues we have raised over implementing biased bases without the necessary hardware for decoy states, BB84-AES retains some attraction, particularly for minimalistic implementations and retrofitting systems already in the field.

A final novelty of our protocol is that, by daisy-chaining multiple Alice/Bob pairs, it is possible to supply an arbitrary amount of quantum-safe quantum randomness with everlasting security to someone who cannot directly access a QRNG. Although the resource requirements scale badly (for a chain of d nodes, excluding the root, a QRNG would need to generate 2^{d-1} bit strings, assuming any intermediaries are trusted), it does offer users a unique way of combining randomness from multiple sources, reducing the trust they place in any one provider. As Bob does not need to rely on his own inbuilt RNG during the transmission process, attack 5.3 cannot be used by the manufacturer to obtain the randomness gathered from external sources, regardless of whether it is transmitted as the QKD key, or simply encrypted using this.

In developing the above, we have shown that the intersection between modern and quantum cryptography should be explored in more detail, with greater collaboration between researchers on both sides, as this area still seems largely untapped and ripe for real-world improvements in algorithms and implementations. The remainder of this chapter will focus on tying up loose ends, as we consider the impact of replacing our tags with true authenticated modes of encryption, and present a number of possible extensions to the arguments and techniques we have applied herein.

5.6.1 On the Cryptographic Choices for Communicating the Bases

Until now, our authentication tags have been based solely around AES-256, because of its ubiquity in modern communications, and position as the de facto quantum-safe alternative to the one-time pad. However, should AES ever become compromised in some way, it would be trivial to substitute in an alternative cipher such as Serpent-256, the post-quantum security of which is currently under evaluation [249].

However, we can go a step further, as authenticated modes of encryption have the same properties as our authentication tags. Throughout this work, we have used AES-GCM to protect our data, and the question arises as to what happens when QKD incorporates such a scheme in its entirety, rather than just capitalising on the block cipher.

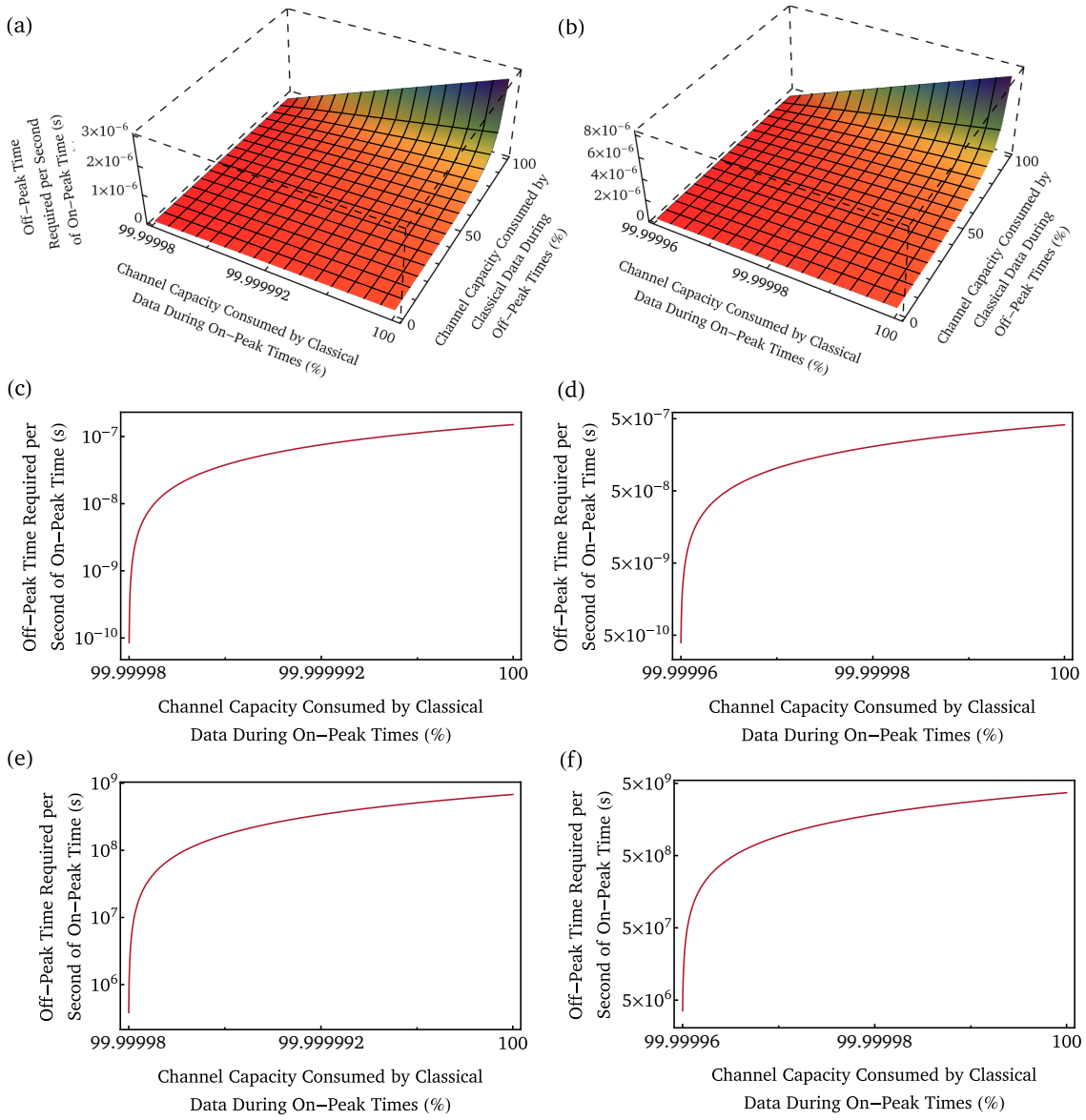


FIGURE 5.3: Showing the amount of off-peak time required per second of on-peak time in order to encrypt all data with the Advanced Encryption Standard running in Galois/Counter Mode, keyed using BB84-AES and considering only limitations imposed by the classical quantum-key-distribution channel, modelled for the ID Quantique Clavis^2 under the pessimistic assumption that the authentication tags contribute an additional 127 classical bits per secret bit. We present results for (a) 0 dB loss in the quantum transmission line with varying on-peak and off-peak traffic (mathematically, the percentage channel capacity consumed by classical data during on-peak and off-peak times is $\varsigma_\wedge/\varsigma$ and $\varsigma_\vee/\varsigma$ respectively); (b) 9 dB loss in the quantum transmission line with varying on-peak and off-peak traffic; (c) and (d) 0 dB and 9 dB losses in the quantum transmission line respectively, with varying on-peak and no off-peak traffic in both cases; (e) and (f) 0 dB and 9 dB losses in the quantum transmission line respectively, with varying on-peak and $\left\lfloor \frac{\varsigma|m|_{\max}}{|m|_{\max}+R_{c/s}|k_C|} \right\rfloor_M$ off-peak traffic in both cases, where $\lfloor\cdot\rfloor_M$ means that we round down to the nearest multiple of machine epsilon M.

BB84-A/G, which supplants the computationally-secure MAC with AES-GCM, should behave in much the same way as BB84-AES, with one important difference. As all of AES-GCM's possible failure criteria are now contained within those for BB84-A/G, the maximum failure probability of the overall system can be defined entirely by the maximum failure probability of BB84-A/G.

This can be expressed mathematically as follows. The ε-security of a confidential cryptosystem that is built from independent and composable subsystems is quantified using [250]

$$\varepsilon_{\text{total}} \leq \varepsilon_{\text{dist}} + \varepsilon_{\text{enc}} \tag{5.10}$$

Here, $\varepsilon_{\text{dist}}$ is the deviation from perfection of a key distribution protocol and its output, while ε_{enc} is the same metric, only applied to the authenticated data encryption.

The composability of BB84-AES is not guaranteed, emphasising the need for a full security proof. Nonetheless, if it does possess this essential property, $\varepsilon_{\text{total}}$ for BB84-AES with AES-GCM encryption will be calculable from equation 5.10. In contrast, AES-GCM never fails on its own when used with BB84-A/G, so we can apply the following:

$$\varepsilon_{\text{total}} = \text{Max}\left(\varepsilon_{\text{dist}}, \varepsilon_{\text{enc}}\right) = \varepsilon_{\text{dist}} \tag{5.11}$$

This comes with one important caveat. As soon as we consider applications beyond AES-GCM or AES-CTR, equation 5.11 no longer applies. Therefore, if BB84-A/G is to be used in an arbitrary cryptosystem, its security should be evaluated under the expectation that the operation in which the key will be used is completely independent.

5.6.2 Beyond Basis Announcements and BB84

Adapting our work for BBM92 [251] (which we call BBM92-AES) and the Six State Protocol [252] (likewise, SSP-AES) is trivial. In the case of the former, the public channel is identical to that of BB84. For the latter, we must compute an extra tag, which we define to be

$$\tau_i^Y = h_{k_{\text{H}}}(Y) \oplus \text{AES}_{k_{\text{C}}}(s_i) \tag{5.12}$$

Consequently, a reduced processing variant would need to test authentication tags corresponding to two out of three bases (c.f. protocol 5.2). Like with the six-state version of SARG04 [253], we expect Eve's attacks on multi-photon terms to be further restricted, such that she can only perform unambiguous state discrimination on weak coherent pulses that contain at least five photons. This is because, given a Γ-photon pulse, the upper bound on the number of states that Eve can discriminate between is $\Gamma + 1$ [254].

The ease with which the techniques of BB84-AES can be applied to other forms of quantum key distribution is less well defined. An advantage can certainly be gained by incorporating decoy states for the basic four-state protocol, but a more detailed analysis would be required with regards to SSP-AES. For example, if we consider the commonly-chosen mean photon number $\mu = 0.1$, then the

probability of generating a pulse containing five or more photons is

$$\begin{aligned} \text{Prob}(\gamma \geq 5) &= 1 - \sum_{\Gamma=0}^{4} \text{Prob}(\gamma = \Gamma) \\ &= 1 - e^{-\mu} \sum_{\Gamma=0}^{4} \frac{\mu^{\Gamma}}{\Gamma!} \\ &= 7.67 \times 10^{-8} \end{aligned} \tag{5.13}$$

As a result, we roughly expect to see a five-photon term only once every 130 keys if the protocol concludes immediately upon reaching the finite key limit ($\sim 10^5$ bits). However, if we now consider $\mu = 0.5$, which is the optimal mean photon number for decoy state QKD [79], then

$$\text{Prob}(\gamma \geq 5) = 1.74 \times 10^{-4} \tag{5.14}$$

Here, several tens of attackable pulses will be transmitted per key. We would expect Alice and Bob to notice the cataclysmic drop in rates if Eve were to block all but these. Yet there may still be attack strategies that allow her to gain useful information by performing unambiguous state discrimination on a fraction of the key, hence the need for a more thorough investigation into the potential role of decoy states in SSP-AES.

Finally, instead of just considering the impact of applying our authentication tags to other QKD protocols, we ask what happens if they are used elsewhere in BB84-AES. Can any advantage be gained if Eve does not know which qubits arrived, because Bob notifies Alice in the same way as she informs him of the correct bases? And what is the effect of using the authentication tags to encrypt error correction parities in CASCADE? This last question is similar to a situation that has previously been considered, in which the parities are encrypted using a OTP as a way of guaranteeing information-theoretic security [88, 255]. Here, the obvious downside is that the number of parity checks must be taken into account when calculating the secret key rate [256]. However, extending our authentication tags to the error correction stage would use no additional key, so while the security implications would need to be thoroughly examined, this may be of benefit.

CHAPTER 6

Implementing Hybrid Quantum/Post-Quantum Security to Defend Against Shor's Algorithm

Declaration of Work

I developed the experimental concept for the work presented in this chapter. I wrote all the software except for QKDSequence, which was provided by ID Quantique. The McEliece implementation was based on that provided by the Botan library, the AES-GCM implementation used OpenSSL and KeyCutter was based on the IDQ3P protocol developed by ID Quantique. The section "Consequences of Computationally Secure Encryption in Quantum-Safe Networks" was conceived after a conversation between myself and Kenny Paterson on that topic. I carried out all of the experiments without assistance.

Some of the results have previously been presented at QCrypt [257]. Where appropriate, parts of the extended abstract may have been reused, as the original text was written by me.

Quantum key distribution (QKD) and post-quantum cryptography have both been proposed as ways of protecting critical communications against the threat posed by quantum computers, yet it is becoming more and more evident that each of these provides unique benefits. In the case of the former, we can guarantee quantum security, whereas with the latter, a necessity for mathematical assumptions is offset by the flexibility provided as a result of easily-implementable trust mechanisms. Therefore, it is likely that both will be taken advantage of in future networks, opening up the opportunity to provide even better functionality by getting these solutions to work in tandem, rather than operating separately.

In this chapter, we investigate possible ways in which QKD and the McEliece post-quantum cryptosystem [258] can be combined. We have chosen McEliece primarily because it has had time to be scrutinised at a level that other post-quantum algorithms have not, which gives us a high level of confidence in its classical security, and a high level of confidence relative to alternatives in its post-quantum security. McEliece is also a contender in the National Institute of Standards and Technology (NIST) post-quantum cryptography competition [259], the winners of which will become defaults for commercial and everyday use. The analysis that follows could easily be rerun, should McEliece not form part of the final recommendations.

We open by exploring some consequences of the work in chapter 5, identifying a crucial area in which QKD can be of use: performing quantum-secure conversions on symmetric keys that have been distributed using public-key solutions, such that the system's immunity against quantum attacks goes from being probable to guaranteed. After justifying our choice to use McEliece, and explaining its operation (section 6.2), we build an experimental system for implementing the above (section 6.3).

The modules developed can also be adapted to create more complex prototypes, capable of demonstrating significant advantages in a number of use cases. We show that the efficiency of QKD can be harnessed to provide fast and automated private-key backups in an otherwise post-quantum world (section 6.4). Finally, we leverage McEliece to reduce the trust in quantum nodes for long-distance communications, and to enable compatibility with legacy connections (section 6.5).

6.1 Consequences of Computationally-Secure Encryption in Quantum-Safe Networks

In the previous chapter, we relaxed the security of QKD to that of the Advanced Encryption Standard (AES), arguing that if the latter turns out not to be quantum-safe, the encryption scheme to which the quantum key is supplied will be compromised regardless. This justification is based on the results of chapter 4, which strongly imply that the one-time pad (OTP) will continue to be less practical than the Advanced Encryption Standard running in Galois/Counter Mode (AES-GCM), except in niche applications.

The obvious riposte to the above is that if we no longer have information-theoretic security, why use quantum physics as a foundation for key distribution in the first place? It should be made clear that the objective of this thesis is security against quantum attacks, rather than a mathematically unbreakable cryptosystem, as such a notion has little significance in the real world if it makes devices difficult to deploy, and introduces avenues for trivial denial of service (DoS) attacks. However, this does not affect the validity of the question posed.

In section 5.2, we explained the reasons why AES-GCM is not a legitimate simplification of BB84-AES. What we failed to establish was whether it can be used as a method for key distribution in situations where perfect forward secrecy is not a concern. The answer is no. AES-GCM can only encrypt $2^{39} - 256$ bits of information [18], after which point it has to be rekeyed by an external

mechanism, meaning it cannot be used as a standalone construct when sharing large numbers of keys. For context, it will take 55.0 s for the slowest link on the Bristol Quantum Network to transmit $2^{39} - 256$ bits of data. One may then ask whether there are any other ways in which key agreement can be carried out, still relying on AES, but with a high enough limit on the number of times it can be called such that the system will never need to be rekeyed. The answer to this is yes.

Key derivation functions (KDFs) take a pre-shared secret and expand it into a longer key that is cryptographically secure. In the case of Transport Layer Security (TLS), on which much of the World Wide Web's security relies, the initial secret can be "established externally or derived from the resumption master secret value from a previous connection" [260]. Thus, from a superficial perspective, KDFs fulfil the same function as QKD and have the same basic requirements, with the difference being that they are built around quantum-safe primitives such as AES [261, 262] or a hash function [263].

For the KDF in [261], $(2^{32} - 1)|p|$ bits of keying material can generated, where $|p|$ is the length of the output from a pseudorandom function (PRF). Therefore, if we define our PRF using AES, and assume the encryption limit on AES-GCM [18] is always reached, we can secure up to ~ 1.18 Zbits of information with a single initial secret key (1 Zbit $= 10^{21}$ bits). For comparison, global IP traffic, which includes but is not limited to all internet traffic, is expected to reach 2.22 Zbits per month by 2021, which is equivalent to a monthly quota of 280 Gbits per capita [264]. On the Bristol Quantum Network, it will take 934.8 years to send 1.18 Zbits of data over the fastest link.

Hence, in situations where perfect forward secrecy is not required, there are more effective approaches to key growing than QKD, assuming an encryption scheme is used that has practical computational security. This is captured by the top two diamond-tiers of the decision tree in figure 6.1, although it should be observed that the diagram applies only to networks of limited capacity. Naturally, if said capacity can be increased arbitrarily, there is nothing in chapter 4 that physically prevents the use of QKD with the OTP in all situations. Yet even if perfect forward secrecy is mandatory for a particular application, it can be implemented as part of public-key cryptosystems by way of session keys, so one may question whether QKD is needed at all if encryption is not realised using the OTP. The answer is relatively simple, as summarised by the bottom two diamond-tiers in figure 6.1. If the initial secret is distributed out-of-band, for example by meeting in person, it will almost certainly not be possible to update it with sufficient regularity to ensure reasonably strong perfect forward secrecy, and QKD will be required. It should be assumed that if, for whatever reason, computationally-secure key exchange has been ruled out when sharing the initial secret, then such a mechanism will also be considered unsuitable for generating session keys. However, given the internet comprises large numbers of widely-distributed entities, it is more likely that the above will continue to be achieved by way of public-key cryptography. In this case, we must ask whether the long-term security of the key needs to be guaranteed against quantum computers. If the answer is yes, then the everlasting security provided by QKD is the only way to erase the information Eve has on symmetric keys distributed using public-key cryptosystems.

FIGURE 6.1: Decision tree for generating quantum-safe symmetric encryption keys in networks of fixed capacity. A number of different building blocks are considered, including quantum key distribution (QKD), key derivation functions (KDFs), the one-time pad (OTP) and the Advanced Encryption Standard (AES).

Elsewhere, the situation is more nuanced, and in particular we note that if the encryption key requires an immediate security guarantee against quantum attacks, then there is no solution at present for cases where it was shared using public-key cryptography. Even in post-quantum systems, a reliance on mathematical assumptions means that there is always a chance, however small, for someone to discover the initial shared secret prior to its use in QKD.

In the author's opinion, it is near-certain that the classical internet of the future will still be based on public-key cryptography. Applications will then be divisible into those that do need a long-term security guarantee and those that do not. To cater for the former, it is of the utmost importance that we demonstrate interoperability between quantum and post-quantum cryptosystems. Doing so is a central goal of this chapter.

6.2 Post-Quantum Cryptography

In this work, we select only two post-quantum algorithms for integration with QKD: McEliece and Niederreiter's variant. Here, we justify this choice, while summarising the other options that were available. We then go on to outline each of the cryptosystems used, and the ways in which they were implemented.

6.2.1 The Post-Quantum Landscape

In recent years, quantum-resistant public-key cryptography has become an increasingly diverse topic of research. Lattice-based constructs are a leading contender, having first been proposed in 1996 [265], less than 2 years after the publication of Shor's algorithm. Popular variants include NTRU [266] (the acronym's root phrase is disputed [267]) and systems built around Learning With Errors (LWE) [268]. However, these were not chosen for the experiments of this chapter because, despite the small key sizes and high speeds that lattice-based cryptography provides, its security is still under question. SOLILOQUY is a notable example for which an efficient quantum attack has been found [269], and this is extendible to a number of other schemes [270]. Although NTRU and LWE are still considered safe, these results demonstrate that our understanding of lattice-based cryptography remains limited so far as quantum computers are concerned, and further analysis is required.

A newer alternative is based on the presumed hardness of computing elliptic curve isogenies, suggested in [271] before being expanded on by [272] and [273]. Unfortunately, the above schemes were also found to be susceptible to quantum attack [274]. By using supersingular elliptic curves, the work of [275] managed to counteract this. It is seen as a candidate for replacing Diffie–Hellman key exchange [276], meaning perfect forward secrecy mechanisms could be implemented as part of a full post-quantum cryptosystem in similar fashion to today. However, given only seven years have passed since the introduction of Supersingular Isogeny Diffie-Hellman (SIDH), it is still far too early to be sure of its security, and so we remove this from consideration also.

It is technically possible to resist attacks on Rivest–Shamir–Adleman (RSA) by increasing the size of its parameters such that, even in the presence of a fully-fledged quantum computer, an infeasible number of qubit operations is required. On the basis of a preliminary analysis, this is believed be achievable with a 1 TB public key and 2^{31} primes, each of which is 4096 bits long [277]. Therefore, while such an approach is academically interesting, it is wholly impractical, made worse by the authors' suggestion of outsourcing key generation to NIST, which only serves to eliminate the security of the scheme.

The security of hash functions is well understood, and while recent attempts have been made to develop generic attack algorithms with a quantum speedup [278], there is still no efficient way of breaking a cryptographic hash. Nonetheless, these will not be used as a basis for the work herein, as our focus is on key distribution, and hash functions can only be used in the construction of signature schemes [279–281]. We do note, though, that proposals such as these are viable candidates for signing public keys on post-quantum Pretty Good Privacy (PGP)-style servers.

Thus, we are left with code-based cryptography, originally proposed in the same year as RSA was first publicly described [258]. While attacks have been found against a number of variants, the original McEliece cryptosystem remains secure. Hence, it is the only post-quantum option for key distribution where we can say the security has been sufficiently explored. In some applications, McEliece's large public key sizes ($>$ 1 MB) would constitute a disadvantage, however this is not a concern for systems capable of running QKD, as the finite key limit means similar amounts of data must be managed regardless. Therefore, given it also provides fast encryption and decryption operations [29], this would seem the sensible choice for integration with QKD as part of a quantum-safe ecosystem.

6.2.2 The McEliece Cryptosystem

Having settled on the type of post-quantum cryptography with which QKD is to be interfaced, we now provide a more in-depth discussion of the protocols used. In the physical world, all digital communications channels are subject to noise, inducing errors on the messages that pass through them. In many cases, this would render such a link unusable, so it is imperative that the noise is somehow compensated for. Error-correcting codes are a way of introducing redundancy into a transmission, mapping each message to a unique vector known as a codeword. In general, greater redundancy means more errors can be corrected because the separation between codewords becomes larger. However, this is subject to selection of an appropriate code.

Binary Goppa codes [282, 283], which are linear with respect to definition 6.1, can correct a relatively high number of errors. Codewords are produced by multiplying messages with the generator for the code (see definition 6.2).

Definition 6.1: Linear Code. *Consider a vector subspace, known hereafter as a code. If any linear combination of vectors sampled from a code produces another vector from the same code, then said code is linear. We refer to each vector as a codeword.*

Definition 6.2: Generator Matrix. *The rows of a generator matrix form the basis of a linear code, meaning that when it is multiplied by an arbitrary input vector, a codeword will be generated.*

In 1978, Robert McEliece put forward a method that used binary Goppa codes to implement public-key cryptography [258]. As shown in protocol 6.1, the randomly-chosen generator (Alice's secret information that gives her an advantage over Eve) is scrambled by a binary matrix (definition 6.3) and permuted (definition 6.4), before being made public. Bob can use this so-called public generator to produce a codeword corresponding to his message, adding it to an error vector of length l and weight v (definition 6.5). Here, the length of the vector is equal to the length of the code (definition 6.6).

Definition 6.3: Binary Matrix. *The elements of a binary matrix take values sampled only from* $\{0, 1\}$.

Definition 6.4: Permutation Matrix. *A permutation matrix is a square, binary matrix. Each row contains only a single element with value 1, and the same is true for each column.*

Definition 6.5: Vector Weight. *The weight of a vector is the number of binary elements it contains with a value of 1.*

Definition 6.6: Code Length. *The length of a code is the number of elements in each of its codewords.*

With her secret knowledge, Alice can use a fast decoding algorithm [284] to correct the errors, thereby decrypting Bob's message. However, Eve is restricted to solving the general decoding problem for linear codes, which is known to be NP-complete [285]. Recall from section 2.2.2 that quantum computers cannot efficiently solve this kind of problem with a black-box approach [46] therefore,

under the assumption that $\mathsf{P} \neq \mathsf{NP}$ and a specific-knowledge quantum algorithm for the general decoding problem does not exist (i.e. $\mathsf{NP} \not\subseteq \mathsf{BQP}$), McEliece would appear to be secure. It should be noted that both of these statements are strongly believed to be true but are, as of yet, unproven.

Protocol 6.1: McEliece Public/Private Key Generation [258]

SUMMARY: Alice creates a public/private key pair for use in protocols 6.2 and 6.3.

1. *Private Key.*
   (a) Alice generates a set of cryptographically-secure random bits, enabling an $r_a \times l$ generator matrix $\mathbf{G}$ to be chosen. The generator corresponds to a binary Goppa code of algebraic dimension r_a (see definition 6.7) and length l, with which υ errors can be corrected.
   (b) Alice generates a second set of cryptographically-secure random numbers, enabling an $l \times l$ permutation matrix $\mathbf{P}$ to be chosen.
   (c) Alice generates a third set of cryptographically-secure random numbers, enabling an $r_a \times r_a$ binary matrix $\mathbf{A}$ to be chosen, constrained such that $\mathbf{A}\mathbf{A}^{-1} = \mathbb{1}$. This is called the scrambler matrix.
   (d) The private key is defined to be $(\mathbf{A}, \mathbf{G}, \mathbf{P})$.
2. *Public Key.*
   (a) Alice computes the $r_a \times l$ public generator matrix $\mathbf{G}'$, where $\mathbf{G}' = \mathbf{AGP}$.
   (b) The public key is defined to be $(\upsilon, \mathbf{G}')$.

Definition 6.7: Algebraic Dimension. *The number of elements in the basis of a vector space is its algebraic dimension.*

We integrate McEliece using the Botan library [286], with the parameters recommended in [249]. Botan was chosen primarily because, at the time, it was the only C++ library to include McEliece. Since then, numerous others have also started to provide their own implementations, such as CEX and QuantumGate, however Botan remains a strong contender after it was tested and endorsed by the Bundesamt für Sicherheit in der Informationstechnik (BSI) in 2017. It is on their behalf that Botan is now maintained, with a commitment to fix functional errors within four weeks of being identified [287]. Another recent development is libpqcrypto, which offers C and Python interfaces for McEliece, but even if it had been available when the work of this chapter first commenced, libpqcrypto does not fulfil our language requirements (C++11, for ease of integration with a QKD network toolkit developed by colleagues).

As with other public-key cryptosystems (see section 2.1.3), McEliece should not be used to directly encrypt a message. Instead, a symmetric key should be distributed using a key encapsulation mechanism (KEM), for use in a protocol such as AES-GCM. Botan's original McEliece KEM is summarised in [286], and is based on the construction in [288], which provides indistinguishability under adaptive chosen ciphertext attack (IND-CCA2), the strongest security notion of its kind (see

appendix C). We take a slightly different approach to symmetric-key generation, as summarised in protocols 6.2 and 6.3. The original implementation implicitly used Key Derivation Function 1 (KDF1) from [289], whereas we used Key Derivation Function 2 (KDF2) from [290] instead. Both take an arbitrary hash function as input, which we define to be Secure Hash Algorithm 512 (SHA-512), from the Secure Hash Algorithm 2 (SHA-2) family [291]. The difference between the two is that KDF2 introduces a counter to increase the amount of key that can be derived with a single master secret. As a result, if a user were to request only a single 256-bit key be returned, the counter would not increment, and KDF2 would be equivalent to KDF1, aside from a slightly modified input.

Protocol 6.2: McEliece Key-Encapsulation-Mechanism Encryption – Based on [258, 286]

SUMMARY: Bob transmits a bit string to Alice by encrypting it with her public key. From this, a symmetric key can be derived.

1. *Symmetric-Key Generation.*
   (a) Bob generates r_a cryptographically-secure random bits and stores them as a message vector $\vec{m}$.
   (b) Bob chooses an error vector $\vec{\epsilon}$ of length l and weight υ, where the elements that have a value of 1 are decided on using a cryptographically-secure random bit generator.
   (c) The symmetric key is defined to be KDF2$(\vec{m}||\vec{\epsilon})$, with SHA-512 as the hash function. Here, $||$ is used to indicate a concatenation.
2. *Symmetric-Key Encryption.* Bob transmits the ciphertext $\vec{c} = \vec{m}\,\mathbf{G}' + \vec{\epsilon}$. In doing so, he has implicitly generated the codeword corresponding to $\vec{m}\mathbf{A}$, permuted it and introduced υ errors. This last step is mathematically equivalent to introducing a permuted error vector, which would still be correctable as its weight is unchanged, and then permuting the result.

Protocol 6.3: McEliece Key-Encapsulation-Mechanism Decryption – Based on [258, 286]

SUMMARY: Using her private key, Alice decrypts the bit string that was transmitted by Bob. From this, a symmetric key can be derived, identical to that generated in protocol 6.2.

1. *Symmetric-Key Decryption.*
   (a) Alice inverts $\mathbf{P}$. As $\mathbf{P}\mathbf{P}^{-1} = \mathbb{1}$, this can be thought of as a "de-permutation" matrix.
   (b) Alice receives $\vec{c}$ and computes $\vec{c}\,\mathbf{P}^{-1} = \vec{m}\,\mathbf{A}\mathbf{G} + \vec{\epsilon}\,\mathbf{P}^{-1}$.
   (c) Alice applies Patterson's Algorithm [284], correcting the errors introduced to the codeword $\vec{m}\,\mathbf{A}\mathbf{G}$ by the error vector $\vec{\epsilon}\,\mathbf{P}^{-1}$, and returning the message vector $\vec{m}\,\mathbf{A}$.
   (d) Alice multiples the inverse of the scrambler matrix by the output of the previous step, such that $\vec{m}\,\mathbf{A} \rightarrow \vec{m}$.
2. *Symmetric-Key Generation.* The symmetric key is defined to be KDF2$(\vec{m}||\vec{\epsilon})$, with SHA-512 as the hash function.

The library had changed significantly by the time the code was written for this thesis, so the examples provided by reference [286] were no longer applicable. At the time, there was an absence

of documentation to supersede this, so much of the development involved working out how the library should be implemented. Further details regarding the exact execution are given in section 6.3.

6.2.3 The Niederreiter Cryptosystem

In addition to vanilla McEliece, there is another code-based construct, which was first proposed by Harald Niederreiter in 1986 [292], and is thought to be secure when used with binary Goppa codes. In particular, it can be shown that the Niederreiter cryptosystem is equivalent to McEliece in this regard. If Niederreiter can be broken, so can McEliece, and vice versa [293].

A high speed C implementation is provided by McBits [294], and is particularly noteworthy because it is faster than RSA, ECC and NTRU [295]. Since this work was carried out, McBits has been added to the liboqs library (part of the Open Quantum Safe project), emphasising its popularity.

While our network was built primarily on software written in C++, it would have been an oversight not to examine the impact of substituting our primary McEliece instantiation for McBits. Yet this was performed only in the context of the experiments presented herein, rather than being fundamentally built into the network infrastructure, and so very little development was required. As a result, we will refrain from providing a full explanation of Niederreiter, although in short, it replaces the generator matrix for a Goppa code with the parity check matrix instead, generating a syndrome that is computationally hard to decode without the private key.

6.3 Scenario I: Symmetric-Key Conversion for Long-Term Quantum Security in a Post-Quantum Ecosystem

We now progress to building a system in which QKD can be used to convert a symmetric key that is only thought to be quantum-safe, into one whereby immunity against quantum attacks is guaranteed. Allowing the user to choose whether or not to perform the conversion is important. If only short-term security is required, there will be a noticeable increase in performance as a result of skipping the QKD step. Using protocol 6.1, a public/private key pair was generated, with the intention that the public portion would be uploaded to a PGP-style key server for Bob to download. Protocols 6.2 and 6.3 were then called to generate a symmetric key and save it to a store, allowing said key to either be used directly in an encryption scheme/message authentication code (MAC) or as the initial secret for QKD. The inclusion of a generic store also means the post-quantum module is agnostic both with regards to manufacturer-specific aspects of the QKD hardware, and the protocol used, meaning it can slot over any arbitrary implementation, including more complex alternatives like measurement-device-independent (MDI)-QKD.

It should be noted that, although our focus is on augmenting quantum-safe public-key cryptography, the above mechanism is the same as that which would be implemented if QKD was the dominant method of key distribution, and Alice had never met Bob, or exhaustion attacks on the initial secret key necessitated a fallback method of authentication. In such a scenario, use of a

```
-----BEGIN MCELIECE PUBLIC KEY-----
MIMQMHswDAYKKwYBBAGBxSoBAwODEDBoADCDEDBiMAcCAhswAgF3BIMQMFQevEeB
y9XE6afIFWRm7WWwgQ0PuFBK3VHuClkO5DQJ6KB6F44y75LkYrSB9aCsUCF34TdG
7lxMezF/oHZxyJzgRTjmqD+cVq4STabYRRCvDQXMJ3hbQP19lycHTIQtDGBQeBYu
q5SkyL/vRrKThgn3PbtfRWb7bdyOQs25NHwoJ/MjUUp7K3zNlZe4TSN79C6h55ZE
                              ⋮
aonslcENEYiMQkpxfCSByRRladz+pqS36NDzW2FEpDsgiGEkR7ckENkOZbYcV0cY
B1mQql5JREIRhGApUGdssU7SV4C6v58j5Lhy5JcovsmUAGg5t6uKFivxMC8OgGUd
n+iVAiVh5Yqarsq77A6Oj/1hrV1tKS5n+Oq1UTLWs/yA/mi8sxrpHQ0vsOEQAAAA
-----END MCELIECE PUBLIC KEY-----
```

FIGURE 6.2: An example of a Privacy-Enhanced-Mail-formatted McEliece public key.

post-quantum digital signature during QKD has previously been investigated [235] however, if one were to repurpose the work of this section instead, it would become clear that a KEM has two distinct advantages. First, the QKD controller can remain unchanged, as it operates independently of any method utilised for sharing the initial secret. Second, the work of chapter 5, while already resilient to Eve's attempts at key exhaustion, mandates the use of MACs rather than digital signatures, meaning our approach enables BB84-AES to continue functioning as designed if, for example, the shared secret were to be accidentally leaked.

Symmetric-key conversion was carried out on the second-generation testbed summarised in section 3.4.1, with one key difference. Instead of relying on the Intel Xeon E5-2697A v4 processors contained within the PowerEdge servers, we carried out the computations required for both the post-quantum algorithms and QKD on an Intel Core i5-5300U processor, which is representative of those used by employees at the University of Bristol. While this has no impact on the above, as we seek only to achieve functionality, the significance of our choice will become apparent as a number of other hybrid scenarios are explored in the sections that follow.

The conversion process is summarised in figure 6.3, with the final key being used for encryption of a message. All the software was written by the author, except for QKDSequence, which was supplied with the ID Quantique Clavis^2.

McAsymmetricKey, McEncryption and McDecryption all work on both Windows and Linux. Randomness is provided by the Hash-Based Message Authentication Code Deterministic Random Bit Generator (HMAC_DRBG) [296], a cryptographically-secure pseudo-random number generator, defined by this experiment to use SHA-512 as the hash function, and seeded from an arbitrary entropy source. This can be a quantum random number generator (QRNG) if one is available, with HMAC_DRBG limiting the impact of any biases introduced by the physical implementation. For compatibility reasons, the public and private key are both saved in Privacy Enhanced Mail (PEM) format, which uses Base64 encoding with a human-readable header and footer for identification purposes (see figure 6.2). The private and symmetric keys are protected with password-based encryption prior to being stored on the hard-drive of the computer.

KeyCutter extracts secret key from the Clavis^2, based on the IDQ3P key extraction protocol and

is the same as the identically-named program that was used in chapter 3. As Linux is required for QKDSequence, this is the only operating system on which KeyCutter has been demonstrated to work.

Finally, AESEncryptor and AESDecryptor have been tested on both Windows and Linux, and rely on the OpenSSL cryptographic library when implementing AES-GCM. OpenSSL was chosen due to its widespread adoption, meaning it is an important library with which to demonstrate interoperability. AESEncryptor and AESDecryptor can easily be switched out, without having to modify any of the surrounding programs, should one wish to use Botan for every non-QKD-related software module.

In this setup, it should be noted that the McEliece-KEM symmetric key acts as a master secret only in the sense that QKD inherently provides key expansion. The key cannot be used securely for more than one round of QKD, because it is applied to a one-time MAC. However, our choice of KDF does allow multiple initial shared secrets to be generated from a single encapsulated key. The duration of the quantum-secure conversion is simply the initialisation time of the Clavis^2, as presented in figure 3.20. Whether or not this is of concern depends on the needs of the user. If additional quantum-secure keys will not be required in the near future, then this another use-case for which improving the secret key rate is important, further motivating the work of chapter 7.

6.4 Scenario II: Quantum Key Distribution as an Entropy Source for Efficient and Automated Private-Key Backups

While the work of section 6.3 is clearly important for protecting the transfer of highly sensitive data such as medical records, which can be sold on the black market for 50× the price of stolen credit card details [297], it is less relevant when the information has a limited lifetime. Thus, having successfully integrated QKD with the McEliece cryptosystem, we now consider a world where everyday cryptography is dominated by post-quantum solutions and long-term security is not required. We ask whether QKD can still be beneficial when even its guaranteed security against quantum computers is inconsequential.

Let us assume McEliece is used to encrypt critical messages between a group of entities, and that if the receiver manages to lose their private key, through system failure or mistakes on the user's behalf, it will be damaging to one or more parties, due to loss of information or the time taken to request the information be retransmitted. An obvious mitigation strategy is to create off-site private-key backups, something which is also useful when considering applications such as cryptocurrencies, because losing the private key to a certificate will result in financial loss.

Here, we propose and implement a scheme that uses QKD for creating off-site backups of the information needed to recreate McEliece private keys (see figure 6.4). It takes the secret key generated by the Clavis^2 and uses this as the entropy source in McEliece, implemented with the programs that were described in the previous section. Therefore, the Clavis^2 is essentially acting as

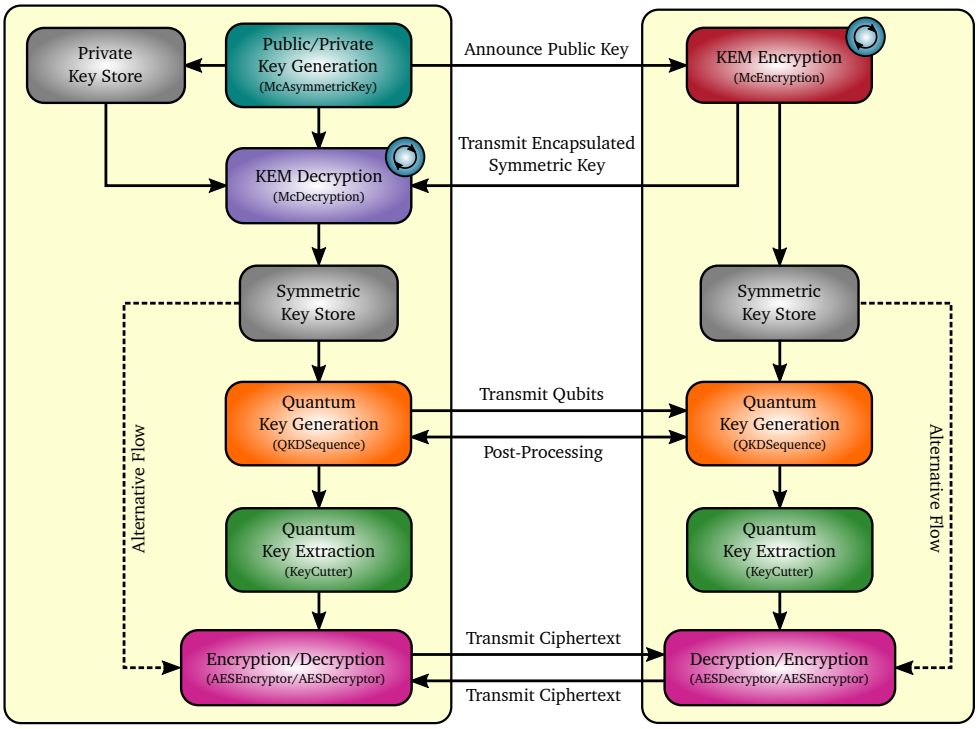


FIGURE 6.3: Workflow for generating symmetric keys using a McEliece key encapsulation mechanism, and performing a quantum-secure conversion, the result of which is supplied to an authenticated encryption scheme. The alternative flows (dashed arrows) indicate the case where quantum-secure conversion is not required, and so the symmetric key is used directly for encryption, rather than acting as the initial shared secret for generating a quantum key.

a hardware random number generator with two identical outputs in separate locations, meaning the backup procedure is entirely automated. At no point does the end-user need to personally make a copy of anything, so long as they use QKD as their sole source of entropy. McAsymmetricKey relies on HMAC_DRBG for deriving cryptographically-secure random bits, which is why the keys can be deterministically reconstructed from the secondary copy of the seed.

Figure 6.5 illustrates the regions in which a QKD-based backup scheme can be more efficient than using a McEliece KEM to share a 256-bit seed between the primary and backup locations. We see that, for the 10 km link considered as part of the data centre model in chapter 3 (4 dB transmission loss + 2 dB switch loss), our scheme is faster than a McEliece (Niederreiter)-driven backup when ≥ 460 (≥ 463) private keys need to be synced. For the range of attenuations considered, it is clear that, overall, this threshold tends to increase with channel loss. Such behaviour is not unexpected, as the secret key rate is diminished at longer distances, so the backup time of our system goes up. However, the exact progression is non-linear, because the mean secret key size of the Clavis^2 is different for each attenuation.

One may question why, from 6.5 to 7.5 dB, the quickest solution alternates between quantum

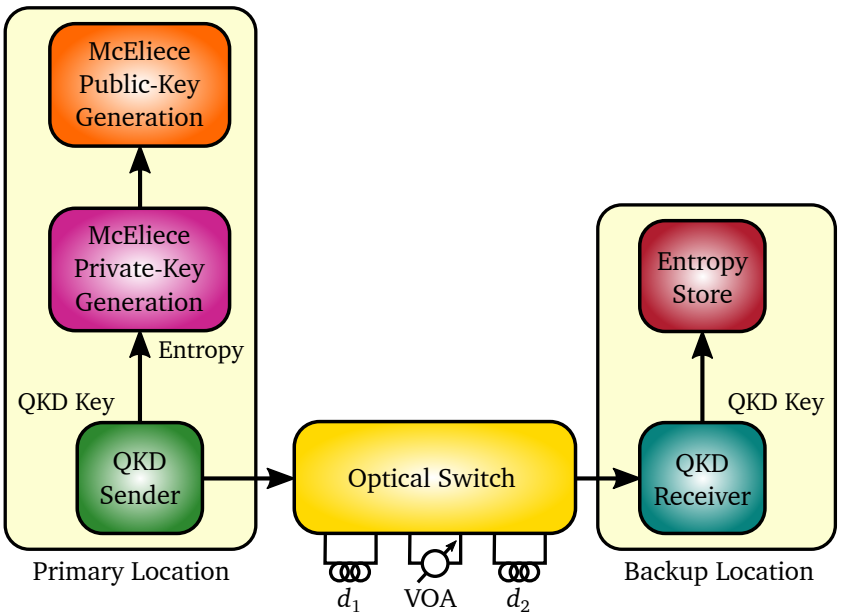


FIGURE 6.4: Illustrating the generation of public/private key pairs, when quantum key distribution is used as an entropy source to enable fast, automated backups. The VOA is a variable optical attenuator and $d_{1,2}$ represent fibres of arbitrary length.

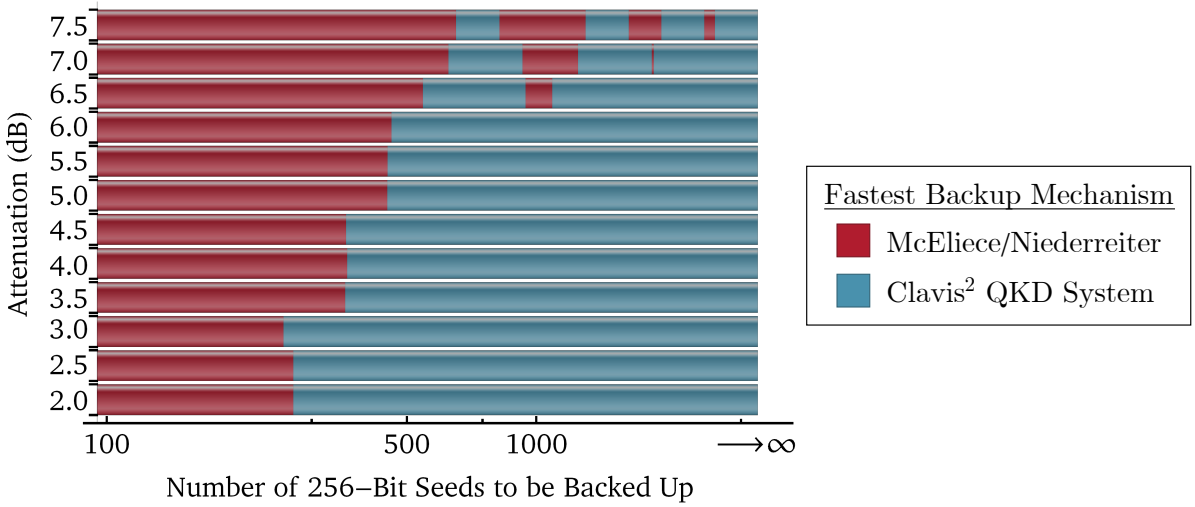


FIGURE 6.5: Illustrating how, for a range of attenuations on the quantum channel, the fastest approach to sequential entropy backups depends on the number of corresponding private keys. McEliece and Niederreiter were experimentally implemented in software, while the QKD links were established using the ID Quantique Clavis^2. For a set attenuation, there are small fluctuations in the number of secret bits generated using QKD. Therefore, we average the final key size for each attenuation, taking care to note that these values are strongly dependent on the loss.

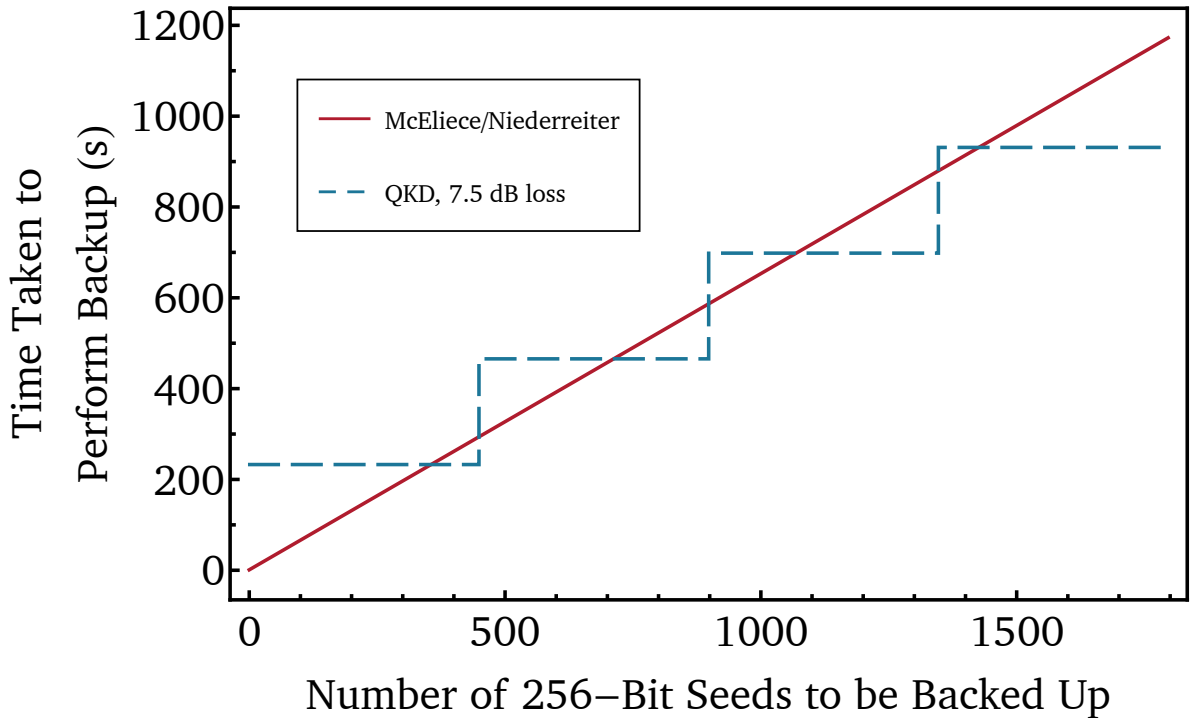


FIGURE 6.6: Showing how, experimentally, the time taken to sequentially perform entropy backups depends on the number of corresponding private keys. We consider backup mechanisms based on both quantum key distribution (QKD) and McEliece/Niederreiter, where QKD follows a step function due to the finite key limit governing minimum block sizes.

and post-quantum. As illustrated in figure 6.6, the time taken for a QKD-based backup follows a step function. This arises as a result of the finite key limit, which means that secret key has to be generated in blocks, and so it takes as long to backup a single private key's worth of entropy as it does to backup several hundred. In this particular instance, the effective gradient of the step function means there are multiple intersections on the graph, therefore the fastest solution alternates.

In figure 6.7, we simulate the effects of constraining the final secret key of the Clavis[2] to $114,944$ bits ($\equiv 449\times$ 256-bit keys), which is the minimum size observed at 9 dB of loss (recall, the highest attenuation at which key can be reliably generated). This gives the lowest bounds on the number of backups required for our scheme to be the quicker approach (see figure 6.8), because it minimises the effective gradient of the step function. Now, for a 10 km link, the switch from McEliece (Niederreiter) to QKD occurs when ≥ 213 (≥ 214) private keys need to be synced; not an unreasonable number for a moderately-sized office building. These thresholds increase linearly with distance, as would be expected in the current scenario, and are roughly the same for McEliece and Niederreiter across all attenuations. The latter trend exists because, although Niederreiter is faster at encryption, the total time elapsed is dominated by common features, such as writing to the backup key store.

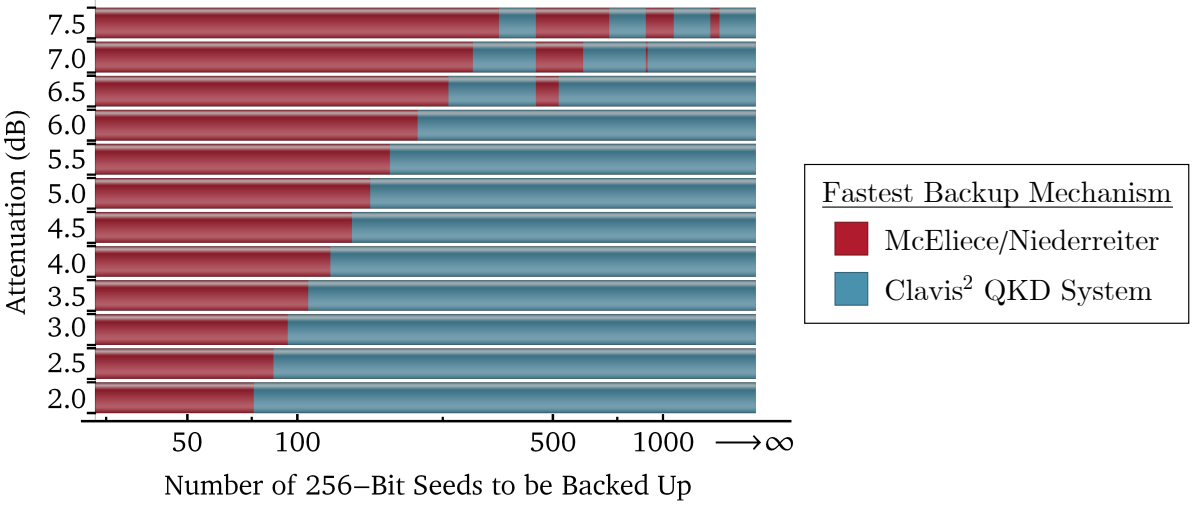


FIGURE 6.7: Simulating how the fastest approach to sequential entropy backups will depend on the number of corresponding private keys when the size of the quantum secret key is fixed at the lowest value observed across all attenuations. McEliece and Niederreiter were implemented in software, while the quantum key distribution links were established using the ID Quantique Clavis^2.

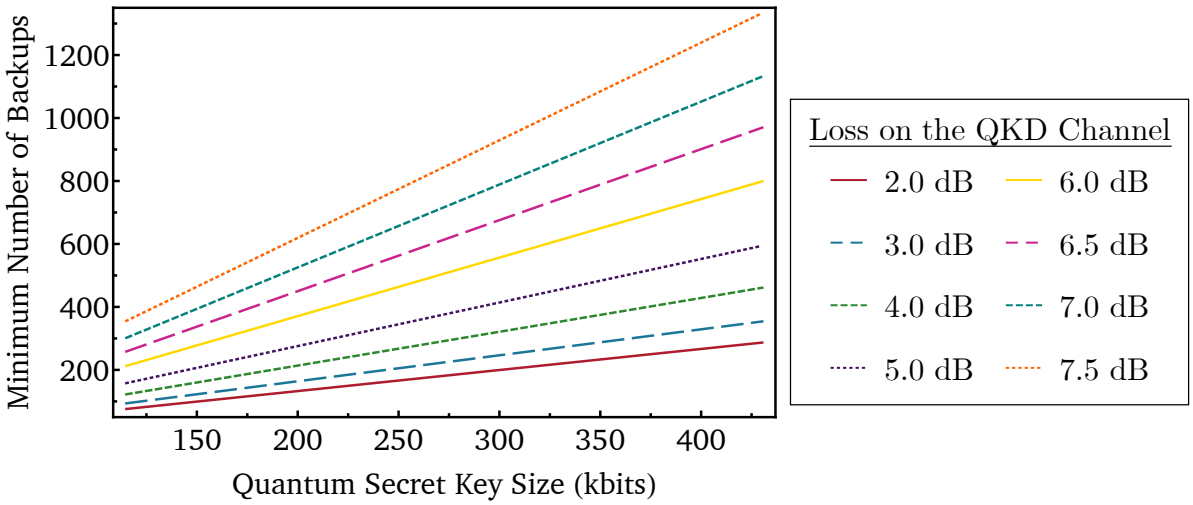


FIGURE 6.8: Simulating how the secret key size of the ID Quantique Clavis^2 affects the minimum number of backups above which quantum key distribution is a faster solution than McEliece. We consider a range of secret key sizes, limited by the upper and lower bounds on those that the Clavis^2 has been observed to produce.

For attenuations $\geq$ 8 dB, the McEliece/Niederreiter backup mechanism is always faster. At lower losses, it would also be possible to speed this up if, at the cost of increasing the load on the system, multiple private keys were to be backed up concurrently. However, there are also commercial and pre-commercial QKD systems that are able to achieve higher key rates than the Clavis^2. Simulating our setup with numbers from [298] shows that, when connected to the Toshiba system, our QKD-based mechanism will always be the faster option for distances up to at least 80 km (exact loss unknown). This is true regardless of whether the equivalent post-quantum scheme backs up sequentially, assuming that the Toshiba block size can be set such that it generates 114,944 bits of secret key for each round of QKD. More specifically, it will take 0.96 s to back up $\leq$ 449 keys when users are 80 km away from the secondary location. In contrast, a Niederreiter-based backup will take 1.12 s for a single key, the same as if all 449 keys were to be backed up concurrently.

Thus, we have demonstrated that in a world where post-quantum cryptography dominates, and the security guarantees of QKD are not required, we can nonetheless gain an advantage thanks to the speed with which we can generate quantum keys.

6.5 Scenario III: Lesser-Trusted Nodes for Long-Distance Quantum Key Distribution & Scenario IV: Introducing Compatibility with Legacy Networks

While we maintain that the majority of quantum-safe networks will not be information-theoretically secure, the final part of this chapter will turn the situation on its head, considering bespoke situations where QKD may be deployed as part of a mathematically-unbreakable cryptosystem, without concern over any physical issues. Isolated quantum satellite networks are one example of such an environment, as each link can be designed to have sufficient classical capacity to support a quantum-keyed OTP, and the barrier to entry is high for anyone trying to mount endpoint DoS (attack 5.1)

However, even if these kind of worries are ignored, challenges still remain that cannot be overlooked. While trusted nodes are widely accepted as the answer to extending the range of QKD without a quantum repeater, allowing an intermediary to access all of Alice and Bob's information constitutes a vulnerability. In scenario III, we look at how post-quantum cryptography can be used to reduce this level of trust, constraining our remit such that, unlike in chapter 5, we are not allowed to use techniques that would modify the security of the QKD protocol itself. The solution we implement is also applicable to the work of section 6.3, if it is found that Alice and Bob are too far apart to establish a direct link in order to perform a quantum-secure conversion.

Scenario IV deals with a bespoke quantum network that, under certain circumstances, also wishes to communicate with an entirely classical outside world. The classical part may comprise legacy devices, that cannot be retrofitted with QKD modules, or high-demand networks servicing large numbers of strangers, for which post-quantum cryptography is the most workable solution.

While scenarios III and IV are very different, the solutions we propose for each are strongly related, and their effectiveness can be measured based on the same metric. In both cases, we use a McEliece KEM to share a symmetric key between the endpoints, however the way this is used differs. For scenario III (reducing trust), Alice and Bob are quantum-enabled by definition, and so they can generate encryption keys by combining the McEliece-distributed secret with that established through QKD (see protocol 6.4). A combination of public-key cryptography and QKD is already used by ID Quantique to ensure the Cerberis[3] does not drop below the minimum security standards required today if it succumbs to a successful side-channel attack [299]. However, as they rely on RSA for this, ours is the first entirely quantum-safe hybrid implementation and, while ID Quantique's objective is to increase device security, we focus on reducing Charlie's knowledge. Here, Charlie is untrusted under the assumption that he does not possess the resources to break McEliece. If this assumption is violated, the scheme becomes a standard QKD trusted node architecture, where Eve (who does not have access to the nodes) still cannot obtain any information without being able to mount a physical attack on the QKD systems.

Protocol 6.4: Lesser-Trusted Nodes

SUMMARY: Alice and Bob derive a shared symmetric key from bit strings agreed upon using quantum key distribution and post-quantum cryptography. All transmissions go via Charlie who, without post-quantum augmentation, would be considered a trusted node.

1. *Quantum Key Distribution.*
   (a) Alice and Charlie establish a secret key $k_{1,3}$ using their preferred method of QKD.
   (b) Charlie and Bob establish a secret key $k_{2,3}$ using their preferred method of QKD.
2. *Post-Quantum Symmetric-Key Distribution.*
   (a) Alice generates a public/private key pair using protocol 6.1 and announces the public part.
   (b) Alice and Bob establish a secret key $k_{1,2}$ using the key encapsulation mechanism defined by protocols 6.2 and 6.3.
3. *Quantum-Key Transport.*
   (a) Charlie computes the ciphertext $c = \text{Enc}\left(k_{2,3}, k'_{1,3}, v\right)$, where $\text{Enc}(\cdot)$ is the encryption function, defined by AES-GCM. $k_{2,3}$ is the plaintext, $k'_{1,3}$ is a 256-bit key extracted from $k_{1,3}$, and v is a 96-bit initialisation vector.
   (b) Alice computes $k_{2,3} = \text{Dec}\left(c, k'_{1,3}, v\right)$, where $\text{Dec}(\cdot)$ is the decryption function, defined by AES-GCM.
4. *Symmetric-Key Generation.*
   (a) Alice and Bob's symmetric key is defined to be $k'_{1,2} = \text{KDF2}\left(k_{1,2}||k_{2,3}\right)$, with SHA-512 as the hash function.

We note that the number of intermediaries is not particularly important, as they can always be reduced to a single entity, so long as they are linked to one another by a secure channel. When

transporting the key Charlie shares with Bob, AES-GCM was chosen over a NIST-style key wrap algorithm [300] as it provides the authenticated encryption properties required, but is more efficient with regards to the number of times the block cipher is invoked, has had its security more thoroughly explored and, if desired, can verify authenticity prior to decryption. We avoid using the OTP as a method for key wrapping, due to the reasons outlined in section 4.3. We assume a PGP-style key server is used for sharing the public keys. Making this quantum-safe is not the focus of our work, and contemporary approaches to key signing will not need to be upgraded as urgently as the methods currently used for key distribution. Therefore, we do not deal with post-quantum authentication here, however one could utilise hash-based signatures, as discussed in section 6.2.1.

We have implemented protocol 6.4 using the software developed in the previous sections, ensuring the information-theoretic security of QKD is retained against eavesdroppers who do not have access to intermediary nodes. Yet, if a trusted node should become compromised, or if our confidence in it turns out to be misplaced, the security of the system is reduced only to the security of McEliece. Figure 6.9 shows the regularity with which the McEliece/Niederreiter-distributed keys can be refreshed relative to the QKD key, and it is from this that we can establish the impact of non-cryptographically exposing both a trusted node and the active post-quantum private key at the same time. As one would expect, it is better to use Niederreiter than McEliece because the encryption rate will be limited by the quantum key generation rate. The fewer encryption cycles we get through before the KEM-distributed key is refreshed from scratch, the better the perfect forward secrecy of the scheme. Therefore, generating fewer QKD keys per post-quantum key as a result of a faster public-key algorithm is better in this regard.

In contrast, scenario IV (legacy connections), does not allow the end-points to access the QKD key, meaning they must encrypt their data directly with the McEliece-KEM-distributed key. A second layer of encryption is then introduced over the top when it reaches the quantum portion of the network; in both cases, the encryption is realised with AES-GCM. This approach is preferable to using McEliece as a mechanism for transporting QKD keys over non-quantum links, because it means the legacy section does not need to be aware of the network configuration, including whether or not the message will pass through any QKD nodes. Similarly, the quantum part does not need to have any knowledge of the post-quantum algorithms that are in use, and can accept all classical inputs without concern as to their origin. Of course, if a quantum-enabled user is the receiver of the message, this does not prevent them from running the same post-quantum software as is in operation outside the QKD network.

However, in this case, one may question why it is worth including a quantum layer of encryption when there are already purely classical links which Eve can try to attack. The answer is that if many legacy devices are communicating over the same quantum backbone, as in figure 6.10, and a weakness were to be found in the post-quantum algorithm, our setup forces an intruder to repeat their attack many times over to get same effect as if they targeted the network core.

Once again, figure 6.9 gives us a way of measuring the performance of our system but, unlike

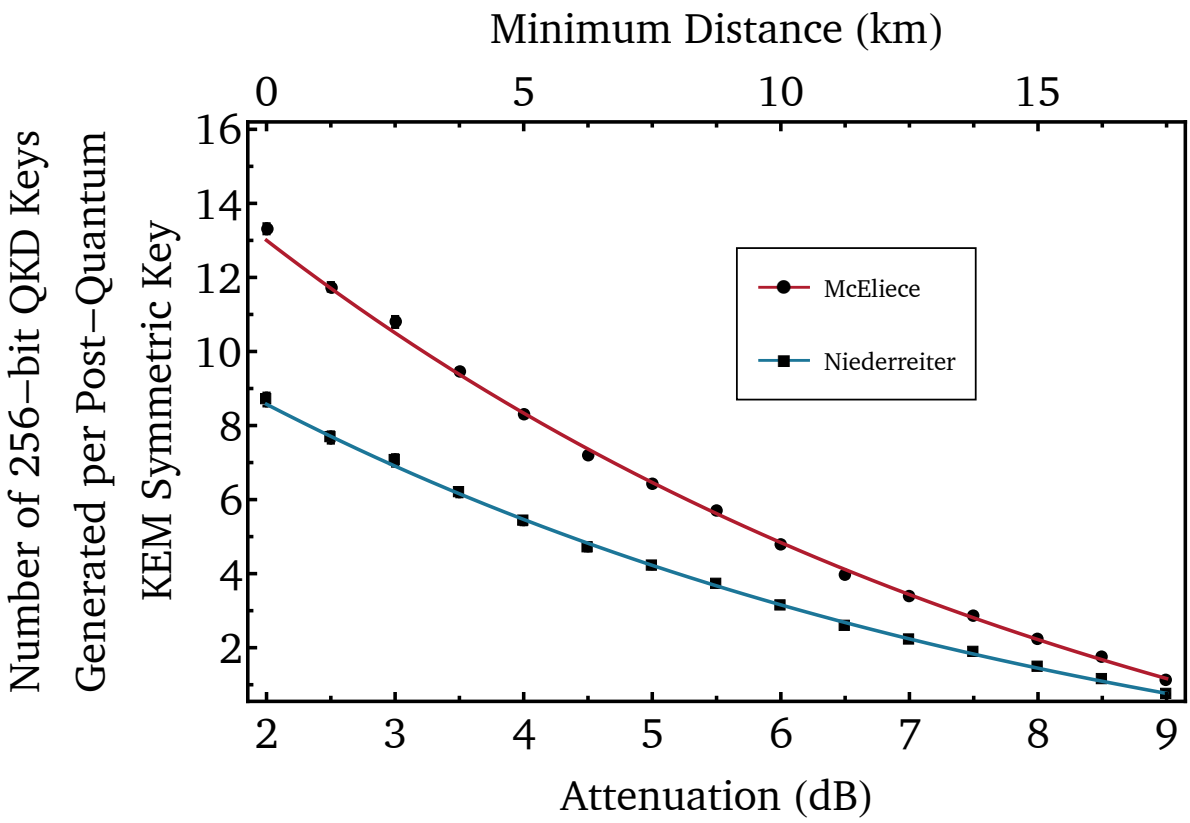


FIGURE 6.9: Rate at which the post-quantum key encapsulation mechanism (KEM)-distributed keys can be refreshed from scratch, relative to each ID Quantique Clavis^2 quantum-key-distribution (QKD) key. Connections are established through an optical switch, introducing 2 dB loss.

in scenario III, Niederreiter gives a worse outcome than McEliece. The faster QKD is relative to the post-quantum algorithm, the more legacy nodes can be supported by a single quantum node. Therefore, while a more efficient post-quantum algorithm is better for the user, it is worse for the network. Furthermore, if the rate of encryption is always defined by the quantum secret key rate, then cases which are a combination of scenarios III and IV will be forced to make a trade-off between perfect forward secrecy and the number of legacy nodes that can be supported.

Finally, we consider the effect of replacing the ID Quantique Clavis^2 with the Toshiba system that was used for the simulations in section 6.4. In [209], the developers performed a number of upgrades to prevent the key rate from saturating at lower attenuations due to the post-processing speeds required. Therefore, based on this version of the system, we find that $(79.7 \pm 4.3) \times 10^3$ QKD keys, each of length 256 bits, can be generated per 256-bit McEliece-KEM symmetric key at 2 dB loss. Similarly, $(52.1 \pm 3.0) \times 10^3$ keys can be generated for every 256-bit Niederreiter-distributed symmetric key. Here, the high errors on our results ($\approx 5\%$) are due to the uncertainty on the key

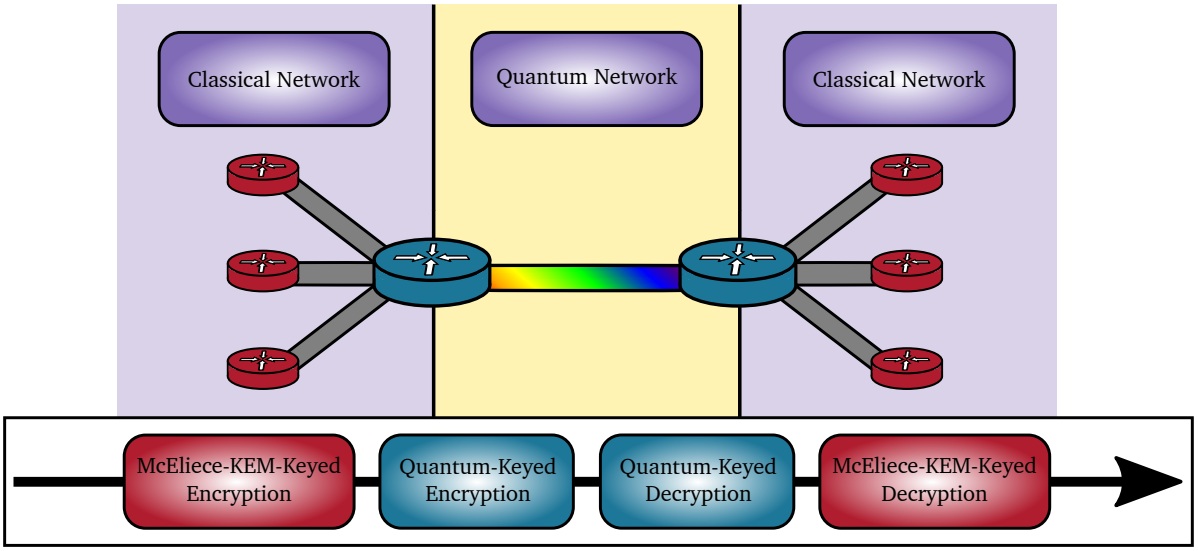


FIGURE 6.10: Illustrating the topology considered for interfacing optical quantum networks with legacy devices. Each classical node (red) can also represent any arbitrary classical network with a single connection to a hybrid quantum/post-quantum node (blue).

rates in [209].

Overall, this is good news concerning the number of connections between legacy devices that future quantum backbones like the UK Quantum Network will be able to support. With regards to lesser-trusted nodes, we have shown that if the purpose of our hybrid approach is simply to add a layer of security against Charlie, then these can certainly be implemented. However, if perfect forward security against Charlie is also required, then our data rates may need to be defined according to the post-quantum algorithm, rather than by QKD.

6.6 Outlook

If we are to build a truly useable quantum-safe ecosystem, it is imperative to demonstrate that QKD and post-quantum cryptography can work together. Only by leveraging the flexibility of public keys and the security provided by the fundamental laws of physics can we be sure that any system we construct will protect our networks, both mathematically and in practice, without a reduction in functionality.

In this chapter, we have developed a prototype for converting keys that are constrained by mathematical assumptions, into keys that are guaranteed quantum-secure. This is the first experimental network implementation capable of performing key distribution using either a post-quantum KEM, QKD, or a combination of the two. Furthermore, the software that has been developed can be repurposed as part of a mechanism for implementing automated backups of the entropy used to

generate private keys, removing the onus on users for whom losing the ability to decrypt certain pieces of information would be incredibly damaging. If the number of backups exceeds a certain threshold, our system is faster than an equivalent setup that relies on the best known instantiation of code-based cryptography. If we were to replace the ID Quantique Clavis^2 with QKD devices built by Toshiba, it is anticipated that our quantum backup mechanism will be quicker for any number of backups, up to a separation of at least 80 km between the primary and secondary storage locations.

Finally, we have shown that hybrid quantum/post-quantum cryptosystems can reduce the trust in intermediary QKD nodes, in addition to enabling compatibility between quantum and legacy networks. All of our setups have been built in a modular fashion, allowing alternative post-quantum algorithms/quantum hardware to be substituted in if desired.

It is hoped that the work of this chapter will provide the foundation for quantum cryptography to be incorporated with other solutions, protecting networks against attacks from quantum computers in the real world.

CHAPTER 7

INTEGRATED PHOTONICS FOR HIGH-SPEED, RECONFIGURABLE QUANTUM KEY DISTRIBUTION

Declaration of Work

The experimental concept for on-chip wavelength-division multiplexed QKD was developed by Philip Sibson, with whom I collaborated when performing the initial characterisation work on devices that he designed. I assisted Philip Sibson and Chris Erven in the compilation of the mask for the monolithic receiver. I also designed and assembled the test transmitter and monolithic receiver packages. I compiled the next-generation silicon masks, with support from Philip Sibson, on whose initial design concepts they were based. The InP, SiO_xN_y and Si devices were fabricated by Oclaro, LioniX, and IME respectively.

Some of the results have previously appeared in [301, 302], in addition to being presented at QCrypt [303].

Throughout this thesis, we have maintained that the traditional motivators for high-speed quantum key distribution (QKD) are perhaps not as important as they initially appear, because quantum solutions are unlikely to be deployed in a fully information-theoretically secure cryptographic environment. However, as we have shown, there are many other reasons why having access to a faster QKD channel can be important.

For the time-division multiple access (TDMA) scheme of chapter 3, the number of transmitters per receiver will increase with key rate, as will the number of legacy devices with which a quantum node can interface in scenario IV of chapter 6. In the same chapter, scenario II illustrates that QKD-based backup mechanisms with higher secret key rates have the potential to perform better

than their post-quantum counterparts.

Beyond this, the arguments of chapter 4 do not apply when using QKD in conjunction with information-theoretically secure message authentication codes (MACs), and it should be highlighted that authentication is often more important than encryption, particularly when considering examples such as news broadcasts and disaster warnings. However, even an authentication tag cannot be constructed before the finite key limit is reached, so once again the secret key rate becomes important. Here, a fast QKD system could reduce the damage caused by a successful denial of service (DoS) attack of the form described in chapter 5, if use of the key in a Wegman-Carter MAC means the user does not wish to relax their security to that provided by BB84-AES. It should be noted, though, that if Bob were to maximise the number of Alices among whom he is divided in TDMA-QKD, then endpoint DoS attacks will be unaffected by higher key rates, as Bob will not have time to replenish the keys of legitimate users if Eve manages to perform QKD with him up to the point of authentication.

Nonetheless, it is clear from the above that the question we must ask is not if, but how one should go about implementing high-speed QKD. A number of different approaches have previously been considered, including the introduction of dedicated electronics for post-processing [209], new protocols [190], noise suppression techniques [304], and improvements to the hardware with which the qubits can be generated and measured [305].

Complementary to most of the above is wavelength-division multiplexing (WDM)-QKD, which takes multiple sender/receiver pairs, assigns a different wavelength to each, and combines the quantum signals on a single fibre. This is a widely used technique in classical communications [306–310], and has been explored in the context of QKD experiments on numerous occasions [116, 311–314]. However, there is a fundamental issue of scalability when using WDM-QKD as a way of achieving higher key rates, due simply to the physical dimensions of Alice and Bob.

In this chapter, we will seek to overcome realistic size constraints by utilising millimetre- and centimetre-scale integrated photonic devices. On-chip QKD has a long history [315–323], with the first full demonstrations of chip-to-chip QKD being performed only recently, using indium phosphide (InP), silicon oxynitride (SiO_xN_y) and silicon-on-insulator (SoI) as fabrication platforms [247, 324]. Pairing these advances in miniaturised quantum-optical circuits with WDM technology makes sense not just from the perspective of attaining higher key rates, but also in the context of this thesis. By manufacturing banks of QKD systems on individual wafers, it may be possible to augment the TDMA-QKD scheme presented herein, such that the software-defined network (SDN) controller can choose whether to set up a few high-speed links, or many more slower connections instead. In addition, multiplexing multiple quantum systems may be the only way to circumvent the limits imposed by section 4.2, for networks to which the arguments of section 4.1 do not apply.

Here, we will open with an overview of the building blocks required for performing chip-based QKD in a range of materials. In section 7.2, we will present contributions which formed part of the first WDM-QKD demonstration using integrated devices. For this, two physically separate transmitter

chips interfaced with a monolithic receiver, demonstrating the viability of the SDN scheme outlined above. Following on, it was important to show that a single transmitter containing multiple Alices was both realisable and would not negatively impact the overall scaling of the key rate. Section 7.3 details our initial steps towards this, in which the number of QKD channels is increased to four per chip.

Finally, in section 7.4, we describe the next-generation chips that were designed and fabricated to explore other applications of WDM in quantum networks, as well as taking the opportunity to explore alternative protocols and transmission media.

7.1 Integrated Photonics

Before we detail the steps taken towards implementing WDM-QKD with integrated optics, we will summarise the underlying technology. In section 7.1.1, we give a brief overview of the materials on which our chips were fabricated, before covering the generation and detection of light in section 7.1.2. We close by describing each of the components used to manipulate and encode weak coherent pulses, which will exhibit equivalent behaviour if one were to switch out the attenuated laser for a single photon source.

7.1.1 Platforms for Integrated Photonics

Indium Phosphide

InP is a compound III-V semiconductor, where "III-V" simply refers to the fact that indium is in the boron group of the periodic table (formerly referred to as group IIIA and IIIB in the US and Europe respectively), and phosphorus is a pnictogen (previously known as group VA or VB). For a long time, InP has been seen as a major competitor in the development of classical transceivers for optical networks [325–328], and its ability to integrate lasers and high-speed optical modulators mean it is an ideal choice for the transmitter in QKD implementations that rely on weak coherent pulses. The InP chips used in this thesis were fabricated by Oclaro, as part of a multi-project wafer using the JePPIX generic integration platform [329].

Silicon Oxynitride

SiO_xN_y offers high-density component integration and low transmission losses at telecom wavelengths. Thus, it seems a particularly suitable choice with which to fabricate QKD receiver units. The Bob chips in this thesis were provided by LioniX, and were manufactured using their TriPleX technology, which is based on alternating layers of silicon nitride (Si_3N_4) and silicon dioxide (SiO_2) [330].

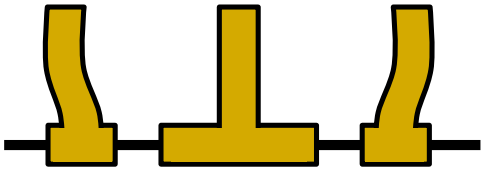


FIGURE 7.1: Circuit symbol for a Fabry-Perot laser. The central element is a semiconductor optical amplifier and the two outer elements are tunable distributed Bragg reflectors.

Silicon-on-Insulator

SoI is perhaps the most well-known of the integrated photonic platforms, having found widespread adoption in both classical and quantum optics, thanks in part to its compatibility with complementary metal–oxide–semiconductor (CMOS) manufacturing processes [331, 332]. Unfortunately, lasers cannot be directly integrated, and the crystalline symmetry of silicon (Si) means it lacks a second-order non-linearity, usually defined by the electric susceptibility $\chi^{(2)}$. As a result, standard electro-optic phase modulators (EOPMs) have no effect [332] and alternative methods for fast phase modulation have had to be developed (see section 7.1.3). Despite these negatives, a number of QKD chip designs were submitted to the Institute of Microelectronics, as the popularity of SoI, combined with its CMOS compatibility, means costs could be much lower compared to other solutions if the technology were to move into high-volume manufacturing.

7.1.2 Sources and Detectors

Lasers

The InP chips rely on a Fabry-Perot laser for the generation of light, which is represented by the circuit symbol in figure 7.1. Two tunable distributed Bragg reflectors (TDBRs) are used to construct a cavity, in the centre of which a semiconductor optical amplifier (SOA) is placed. The SOA is a p-n junction that is forward biased, causing the depletion region to narrow. As a result, electron-hole annihilation becomes possible, leading to spontaneous and stimulated photon emission. The TDBRs are sections of waveguide with a periodic grating structure that reflects light. They are doped to create a p-i-n junction, and modulating the carrier density changes the effective refractive index, thereby tuning the wavelength of reflection [333]. This provides some control over the wavelength at which stimulated emission (and therefore lasing) occurs.

Avalanche Photodiodes

Avalanche photodiodes (APDs) are room-temperature detectors which, depending on the operating conditions, can be used to measure either quantum or classical light. They were superficially touched upon in chapter 3 with regards to the ID Quantique Clavis^2 and, as figure 7.2 shows, we continue to use the same circuit symbol in an integrated setting.

FIGURE 7.2: Circuit symbol for an avalanche photodiode.

FIGURE 7.3: Circuit symbol for a superconducting-nanowire single-photon detector.

A reverse-biased p-n junction is central to the operation of an APD. Incoming photons are absorbed, generating free carriers, which in turn causes avalanche breakdown of the diode [334]. The current that flows as a result signifies a detection event, and ordinarily the efficiency of this process is the main hindrance so far as QKD is concerned, because it has a direct impact on the key rate.

However, when time-bin encoding is used, a low jitter is also required, as this will minimise the number of signals that cross over into adjacent bins, which would lead to an increase in the quantum bit error rate (QBER). Here, jitter refers to the natural deviation in the time taken for an electrical signal to be measured following absorption of a single photon. Unfortunately, the jitter of an APD is not low enough for our requirements, so in this chapter we use them only for classical functions, such as clock synchronisation.

Superconducting Nanowire Single-Photon Detectors

Superconducting nanowire single-photon detectors (SNSPDs) have high detection efficiencies, low dark counts and low jitter (for the PhotonSpot system used in Bristol, these values are $> 85\%$, < 100 Hz, and 70 ps respectively). There are still (presently tolerable) downsides, as SNSPDs are yet to be reliably integrated with photonic circuits, and liquid-helium temperatures are essential. The circuit component for an SNSPD is shown in figure 7.3.

With regards to the method of operation, a 100 nm wire is biased such that the current is just below that for which superconductivity is destroyed. Whenever a photon is absorbed, it disrupts the Cooper pairs in the material and turns the region on which it was incident into a resistive hotspot. Current continues to flow around this, pushing the charge density above the critical point and causing superconductivity to break down. As a consequence, a temporary resistance spike is generated across the width of the wire, with a corresponding measurable voltage [335].

FIGURE 7.4: Circuit symbol for a delay line.

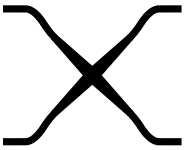


FIGURE 7.5: Circuit symbol for a waveguide crosser.

7.1.3 Photonic Circuit Components

Waveguides

Optical waveguides are a way of confining and directing light through integrated circuits, working in much the same way as the optical fibres that are utilised in communications networks. Waveguides may be used to create delay lines (figure 7.4) and can even cross (figure 7.5), so long as both arms gradually taper out to reduce diffraction at the point where they intersect. For the SoI chips presented here, each waveguide has an initial width of 0.500 μm, linearly expanding to 1.463 μm over a distance of 19.255 μm.

To ensure interoperability of the chips with other systems, light can be coupled out using one of three methods. InP and SiO_xN_y devices both rely on side coupling which, as the name suggests, runs the waveguide to the edge of the chip whereby a spot-size converter expands the beam waist, allowing a lens on the end of a fibre to focus the light into its core. The spot-size converter is essentially a tapered waveguide, sometimes constructed using a lower-index material, and is the reason why damage to the chip facet often results in high coupling losses.

Alternatively, one may decide to use a grating coupler (see figures 7.6 and 7.7). This approach is particularly advantageous in the case of Si fabrication runs, as multiple experiments are grouped onto the same chip, and so access to the edge is often not possible. One-dimensional grating couplers are constructed by introducing rectangular teeth to the upper edge of the waveguide, resulting in off-chip interference. The periodic structure is slightly detuned such that the light exits at an angle that is non-perpendicular to the face of the chip, thereby preventing back-reflection [336].

Two-dimensional grating couplers work in a similar fashion, except they are connected to a pair of orthogonal waveguides. This means horizontally polarised light will be diverted down one arm, and vertically polarised light down the other [337], making it an effective mechanism for converting between path and polarisation encodings.

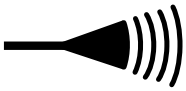


FIGURE 7.6: Circuit symbol for a one-dimensional grating coupler.

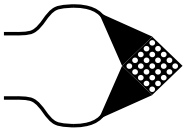


FIGURE 7.7: Circuit symbol for a two-dimensional grating coupler.

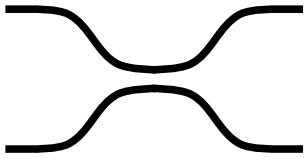


FIGURE 7.8: Circuit symbol for a directional coupler.

Directional Coupler

Directional couplers (see figure 7.8) are the beam splitters of integrated optics. Whenever light is confined to a medium through total internal reflection, evanescent fields are produced. These are zero-energy wave components that are transmitted through the boundary, decaying exponentially with distance [338, 339]. If two waveguides are placed in close vicinity to one another, their evanescent fields will overlap, allowing light to be coupled between them. A full mathematical treatment can be found in [340] but, in short, the interaction is governed by the following equations:

$$\begin{aligned} \frac{\mathrm{d}W_1(z)}{\mathrm{d}z} &= -\mathbb{i}\kappa W_2(z)\, e^{-\mathbb{i}(\rho_2-\rho_1)z} \\ \frac{\mathrm{d}W_2(z)}{\mathrm{d}z} &= -\mathbb{i}\kappa W_1(z)\, e^{\mathbb{i}(\rho_2-\rho_1)z} \end{aligned} \tag{7.1}$$

Here, $W_1(z)$ and $W_2(z)$ are the optical field amplitudes in each waveguide as a function of z, a Cartesian co-ordinate that runs parallel to the direction of propagation, spanning the length of the interaction region. κ is a coupling constant that can be adjusted according to the waveguide separation, and $\rho_2 - \rho_1$ is the difference between the propagation constants of each waveguide, which should be 0 by design.

The resultant system of linear differential equations has the solution

$$\begin{aligned} W_1(z) &= W_1(0)\cos(\kappa z) - \mathbb{i}W_2(0)\sin(\kappa z) \\ W_2(z) &= W_2(0)\cos(\kappa z) - \mathbb{i}W_1(0)\sin(\kappa z) \end{aligned} \tag{7.2}$$

and figure 7.9 plots these for a fixed, arbitrary κ. We can see that the optical field intensity on

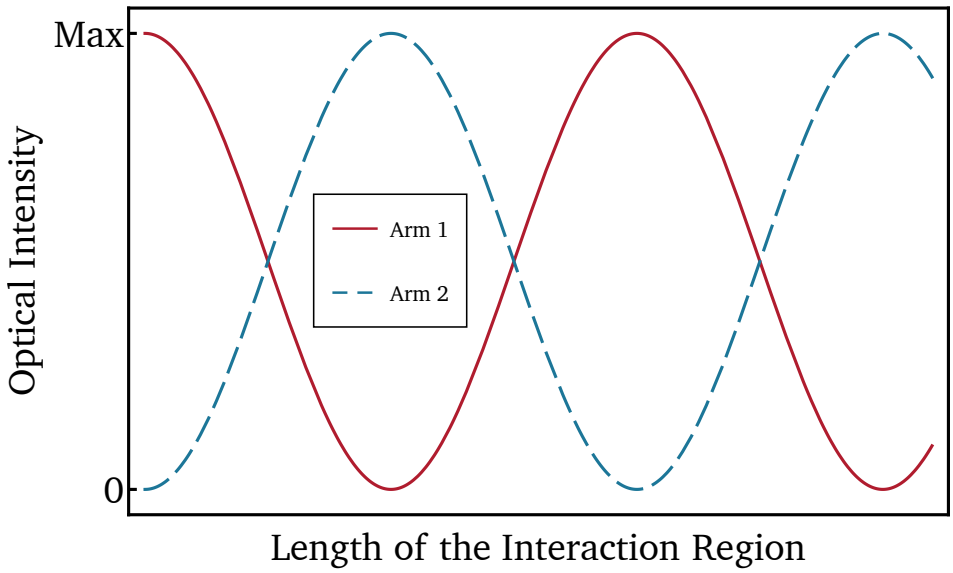


FIGURE 7.9: Illustrating the optical intensity on each output of a directional coupler, for increasing length and an arbitrary coupling constant, κ.

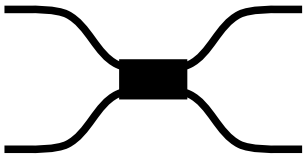


FIGURE 7.10: Circuit symbol for a multi-mode interferometer.

each arm varies periodically according to the length of the interaction region, from which a 50/50 directional coupler can be designed.

Multi-Mode Interferometer

While directional couplers may seem simple to design, they are hard to fabricate with the exact splitting ratio intended. Some platforms offer multi-mode interferometers (MMIs) as an alternative (see figure 7.10), which are designed around the self-imaging principle [341]. Light enters a multi-moded section of waveguide, diffracting due to the change in width. Parts of the wave are reflected off the edges, causing it to interfere with itself. As illustrated in figure 7.11, maxima occur periodically with distance from the input, meaning that once again we have a length dependence which can be exploited to create on-chip beam splitters.

Thermo-Optic Phase Modulator

In our experiments, we will need to modulate the phase of the light for a number of different purposes, including intensity reduction and biasing our measurement bases. This can be achieved

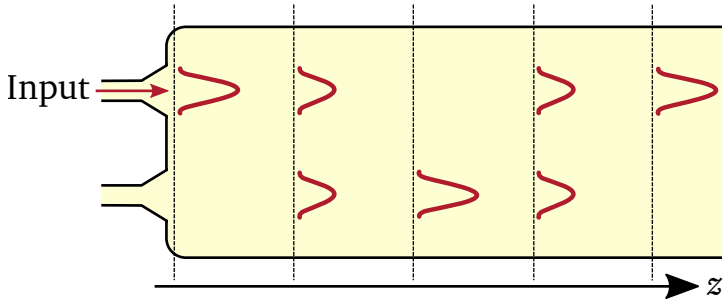


FIGURE 7.11: Illustrating periodic self-imaging of the input signal in a multi-mode interferometer. Based on figure 3 in [341].

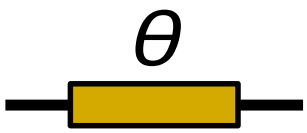


FIGURE 7.12: Circuit symbol for a thermo-optic phase modulator.

using thermo-optic phase modulators (TOPMs), the circuit symbol for which is shown in figure 7.12. TOPMs are short strips of metal that heat up when an electrical signal is applied, taking advantage of the fact that the effective refractive index, n_{eff}, of a waveguide is related to its temperature, T, by [342]

$$\Delta n_{\text{eff}} = \frac{\mathrm{d}n_{\text{eff}}}{\mathrm{d}T}\Delta T \tag{7.3}$$

This in turn leads to a shift in the phase, θ, because

$$\Delta\theta = \frac{2\pi|z|_{\text{H}}}{\lambda}\Delta n_{\text{eff}} \tag{7.4}$$

where $|z|_{\text{H}}$ is the length of the TOPM, and λ is the wavelength of the light in a vacuum.

Electro-Optic Phase Modulator

EOPMs (see figure 7.13) are superficially similar to TOPMs, however they are much faster, with those used in this thesis reaching speeds of up to 10 GHz. Therefore, they are an important component for high-speed QKD, fulfilling functions like phase encoding, that are specific to each individual qubit.

The EOPMs provided by Oclaro rely on the Quantum Confined Stark Effect, in which an electric field is generated that changes the absorption properties of a material. Naturally, this means a variable loss is introduced to the waveguide however, as stated in [343], it also causes a change in the refractive index such that

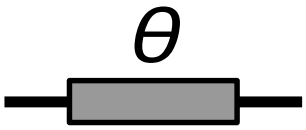


FIGURE 7.13: Circuit symbol for an electro-optic phase modulator.

FIGURE 7.14: Circuit symbol for a carrier-depletion modulator.

$$\Delta n_{\text{eff}} \approx \frac{\sigma}{\pi} \lim_{x \to 0^+} \left[\int_{\omega_1}^{\omega_0 - x} \frac{\Delta\Theta(\omega)}{\omega^2 - \omega_0^2} d\omega + \int_{\omega_0 + x}^{\omega_2} \frac{\Delta\Theta(\omega)}{\omega^2 - \omega_0^2} d\omega \right] \tag{7.5}$$

Here, σ is the speed of light, Θ is the absorption coefficient of the material and ω_0 is the angular frequency of the incident photons, where $\omega_1 < \omega_0 < \omega_2$. We have taken and expanded the Cauchy principal value to handle the singularity at $\omega = \omega_0$.

Reference [343] also demonstrates empirically that this refractive index change can be expressed in the following form:

$$\Delta n_{\text{eff}} \propto |\vec{E}|^2 \tag{7.6}$$

where $|\vec{E}|$ is the magnitude of the electric field. Thus, we can use EOPMs to modulate the refractive index of the waveguide, and generate a phase shift similar to that in equation 7.4.

Carrier-Depletion Modulator

As noted in section 7.1.1, standard EOPMs cannot be implemented in Si. Therefore, to achieve fast phase modulation, a different approach must be taken. Carrier-depletion modulators (CDMs) are a popular choice [344], the circuit symbol for which is shown in figure 7.14. These rely on p-doped and n-doped sections of waveguide, which are fabricated alongside each other to create a p-n junction. Reverse biasing the waveguide pulls the electrons and holes away from each other, thus creating a carrier-free depletion region, the size of which is voltage-dependent. The carrier density affects the effective refractive index of the waveguide, therefore by changing the bias it is possible to induce a phase shift, once again with some associated loss.

Mach-Zehnder Interferometer

By placing a directional coupler or an MMI on either side of a TOPM, EOPM or CDM (see figure 7.15), it is possible to create a Mach-Zehnder interferometer (MZI). This is an important building block, as

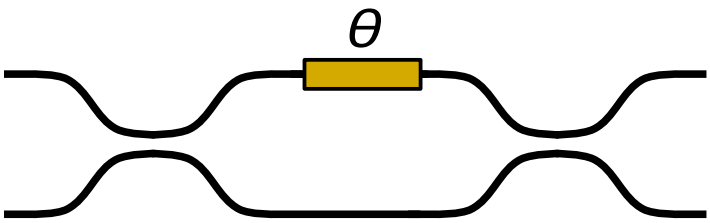


FIGURE 7.15: Circuit diagram for a Mach-Zehnder interferometer constructed from directional couplers and a thermo-optic phase modulator.

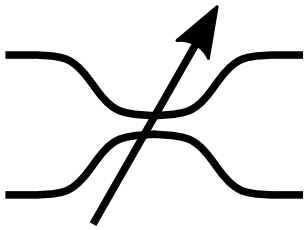


FIGURE 7.16: Circuit symbol for a switch constructed from a Mach-Zehnder interferometer.

it can be used to compensate for imperfect directional coupler splitting ratios, is able to function as a switch (see figure 7.16), and offers a way to modulate properties of the light.

To illustrate, we will consider the case where a single photon is incident on a directional-coupler MZI. Given equation 7.2, we know that the unitary for a 50/50 directional coupler will be

$$\hat{U}_{\mathrm{DC}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & \mathbb{i} \\ \mathbb{i} & 1 \end{bmatrix} \tag{7.7}$$

which is functionally equivalent to the Hadamard used to derive the beam splitter relations in equation 2.52. In a dual rail encoding scheme, TOPMs, EOPMs and CDMs can be represented by the phase-shift gate $\hat{R}_\theta$ (see equation A.1).

We now define arm 1 of the MZI as that containing the phase modulator, and input-output relations can be derived from the unitaries representing each component such that

$$\begin{aligned} |1\rangle_1 |0\rangle_2 = |10\rangle &= \hat{a}_1^\dagger |00\rangle \\ &\xrightarrow{\mathrm{DC}} \frac{1}{\sqrt{2}} \left(\hat{a}_1^\dagger + \mathbb{i}\hat{a}_2^\dagger\right) |00\rangle \\ &\xrightarrow{\theta} \frac{1}{\sqrt{2}} \left(e^{\mathbb{i}\theta}\hat{a}_1^\dagger + \mathbb{i}\hat{a}_2^\dagger\right) |00\rangle \\ &\xrightarrow{\mathrm{DC}} \frac{1}{2} \left[e^{\mathbb{i}\theta}\left(\hat{a}_1^\dagger + \mathbb{i}\hat{a}_2^\dagger\right) + \mathbb{i}\left(\mathbb{i}\hat{a}_1^\dagger + \hat{a}_2^\dagger\right)\right] |00\rangle \\ &= \frac{1}{2} \left[e^{\mathbb{i}\theta}\hat{a}_1^\dagger - \hat{a}_1^\dagger + \mathbb{i}\left(e^{\mathbb{i}\theta}\hat{a}_2^\dagger + \hat{a}_2^\dagger\right)\right] |00\rangle \\ &= \frac{1}{2} \left(e^{\mathbb{i}\theta} - 1\right) |10\rangle + \frac{\mathbb{i}}{2} \left(e^{\mathbb{i}\theta} + 1\right) |01\rangle \end{aligned} \tag{7.8}$$

If, at the output of the MZI, we install detector 1 on arm 1 and detector 2 on arm 2, we find

$$\begin{aligned}\text{Prob}\,(\text{Click in detector 1}) &= \frac{1}{4}\langle 10|\left(e^{\mathbb{i}\theta}-1\right)\left(e^{-\mathbb{i}\theta}-1\right)|10\rangle \\ &= \frac{1}{4}\left(1-e^{\mathbb{i}\theta}-e^{-\mathbb{i}\theta}+1\right) \\ &= \frac{1}{4}\left[2-2\cos(\theta)\right] \\ &= \sin^2\left(\frac{\theta}{2}\right)\end{aligned} \tag{7.9}$$

and

$$\begin{aligned}\text{Prob}\,(\text{Click in detector 2}) &= \frac{1}{4}\langle 01|\left(\mathbb{i}e^{\mathbb{i}\theta}+\mathbb{i}\right)\left(-\mathbb{i}e^{-\mathbb{i}\theta}-\mathbb{i}\right)|01\rangle \\ &= \frac{1}{4}\left(1+e^{\mathbb{i}\theta}+e^{-\mathbb{i}\theta}+1\right) \\ &= \frac{1}{4}\left[2+2\cos(\theta)\right] \\ &= \cos^2\left(\frac{\theta}{2}\right)\end{aligned} \tag{7.10}$$

Therefore, the physical state described by equation 7.8 is equivalent to the path-encoded logical state

$$|\psi\rangle = \sin\left(\frac{\theta}{2}\right)|\overline{0}\rangle + \cos\left(\frac{\theta}{2}\right)|\overline{1}\rangle \tag{7.11}$$

recalling that $|\overline{0}\rangle$ is used to signify logical 0, so as to avoid confusion with the vacuum state $|0\rangle$. From this, we can see that it is possible to tune the phase such that the MZI acts like either a 50/50 beam splitter or a switch. If we were to replace our single photon with a bright light source, we would find that the ratio between the power entering and exiting on arm 1 would be the same as the probability that a single photon causes a click in detector 1. Thus, we can characterise the electrical signals which must be applied to the phase modulator, simply by measuring the optical output with a powermeter.

Asymmetric Mach-Zehnder Interferometer

It is possible to create an asymmetric Mach-Zehnder interferometer (AMZI) by using two waveguides of disparate length to connect a pair of directional couplers (see figure 7.17). If the extension to the long arm is enough to constitute a delay line, then an AMZI can be used for time-bin en/decoding, as described in section 2.2.3.

Shorter differences in length mean that the two half-pulses generated by the first directional coupler will overlap and interfere on the second. A relative phase shift is induced between the arms, which causes specific wavelengths to be split out. As a result, we are able to use the AMZI as a wavelength de-multiplexer.

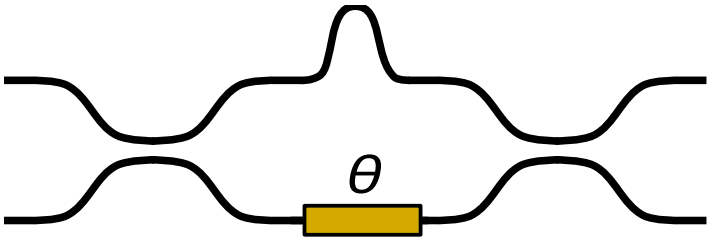


FIGURE 7.17: Circuit diagram for a de-multiplexing asymmetric Mach-Zehnder interferometer. The version used for phase decoding and path-to-time-bin conversion is the same, only with a delay line in place of the longer arm.

It is standard to characterise such a device by its free spectral range, $\Delta\lambda_{\text{FSR}}$. This is the difference in wavelength between two adjacent maxima in the interference pattern on a single output port. Thus, the free spectral range defines our channel spacing, because if we are to de-multiplex two signals with minimal loss, the closest they can be to one another is $\frac{\Delta\lambda_{\text{FSR}}}{2}$.

In order to show how the channel spacing can be engineered, we consider two light pulses travelling down paths that deviate in length by $\Delta|z|_{\text{W}}$, for which it is known that [345]

$$\Delta\theta(\lambda) = \frac{2\pi n_{\text{eff}}\Delta|z|_{\text{W}}}{\lambda} \tag{7.12}$$

If vacuum-wavelengths λ_1 and λ_2 correspond to points of constructive interference at one of the AMZI outputs, then that is the arm into which they will be routed. Maxima in the through port (minima in the cross port) occur whenever

$$\Delta\theta(\lambda) = (2i+1)\pi \quad \text{for} \quad i \in \mathbb{Z} \tag{7.13}$$

Similarly, maxima in the cross port (minima in the through port) occur if

$$\Delta\theta(\lambda) = 2i\pi \quad \text{for} \quad i \in \mathbb{Z} \tag{7.14}$$

In both cases, the maxima are spaced at 2π intervals so, regardless of which port we wish to send λ_1 and λ_2 down, it is required that

$$\Delta\theta(\lambda_1) - \Delta\theta(\lambda_2) = 2\pi \tag{7.15}$$

Equation 7.12 can be substituted into this, such that

$$\frac{2\pi n_{\text{eff}}\Delta|z|_{\text{W}}}{\lambda_1} - \frac{2\pi n_{\text{eff}}\Delta|z|_{\text{W}}}{\lambda_2} = 2\pi \tag{7.16}$$

Finally, by defining $\lambda_0 = \frac{\lambda_1+\lambda_2}{2}$, and rearranging

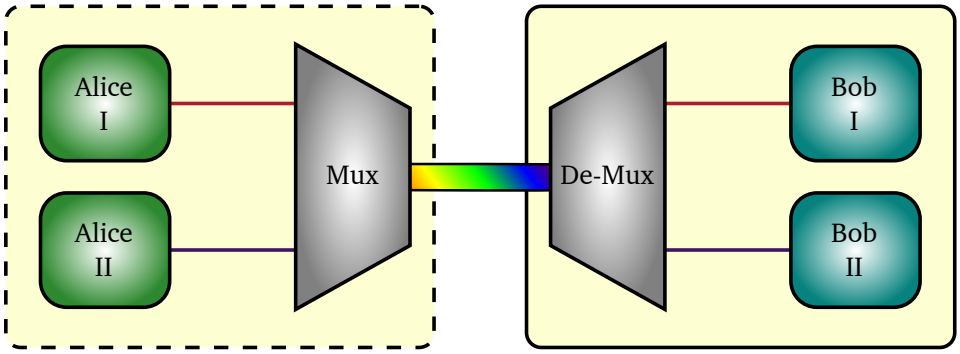


FIGURE 7.18: Illustrating how a wavelength-division multiplexer (mux) is used to combine the outputs from two Alice chips down a single channel. A de-multiplexer (de-mux) is used at the end to split the signals and divert them to different Bobs. Due to the principle of optical reversibility, the mux and de-mux can be physically identical.

$$\begin{aligned}\Delta\lambda_{\text{FSR}} = \lambda_2 - \lambda_1 &= \frac{\lambda_1\lambda_2}{n_{\text{eff}}\Delta|z|_{\text{W}}} \\ &\approx \frac{\lambda_0^2}{n_{\text{eff}}\Delta|z|_{\text{W}}} \quad \text{i.f.f.} \quad \lambda_2 - \lambda_1 \ll \lambda_1, \lambda_2\end{aligned} \tag{7.17}$$

Therefore, we can design an AMZI-based de-multiplexer with a channel spacing defined according to the relative lengths of the waveguides that connect the directional couplers.

7.2 Device Characterisation for On-Chip Wavelength-Division Multiplexed Quantum Key Distribution

In this section, we summarise the contributions that enabled the first demonstration of WDM-QKD using integrated devices (see figure 7.18). The final stages of the overall experiment were carried out by Philip Sibson, who used the operating parameters established herein to return a secret key rate of $\sim$ 1.1 Mbit/s over 4 dB of loss; twice the speed that can be achieved with only a single Alice/Bob pair [247]. In our setup, the multiplexer was realised using a bulk arrayed waveguide grating (AWG), while the de-multiplexer was constructed from an on-chip AMZI, integrated with Bob I and II, as depicted in figure 7.19. Recall, Alice I and II were physically separate devices, a schematic for which is provided by figure 7.20. We note that EOPMs were fabricated on both arms of her MZIs, because they introduce a phase-dependent loss. Therefore, we apply a $\frac{\theta}{2}$ phase shift to one arm, and $-\frac{\theta}{2}$ to the other, generating a relative phase of θ between the two, with the same loss induced across both waveguides.

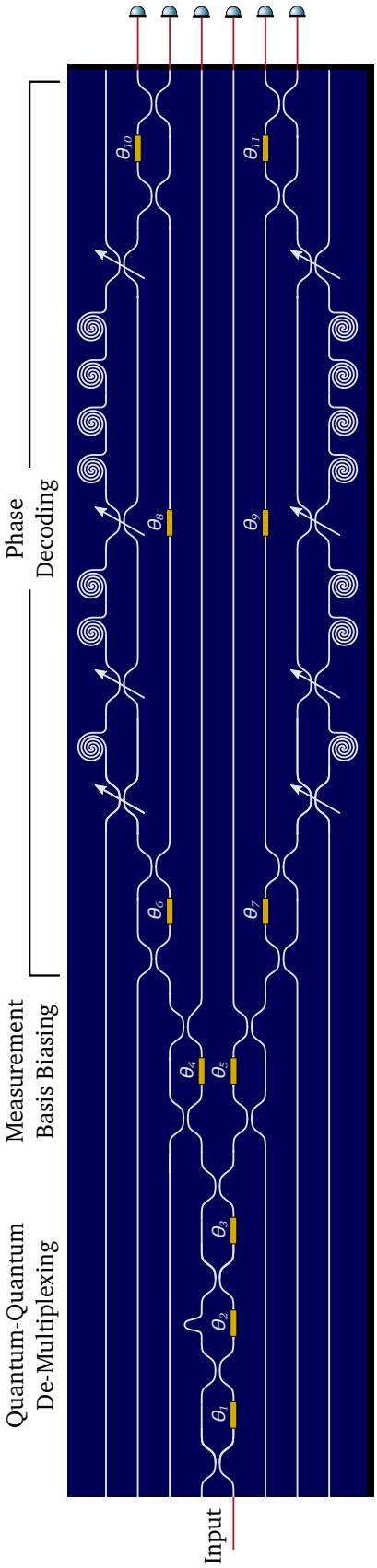


FIGURE 7.19: A schematic of the two-channel Bob chip with wavelength-division de-multiplexing capabilities. The Mach-Zehnder-interferometer switches allow for selection of either a ~ 300 ps, ~ 600 ps or ~ 1200 ps delay, the choice of which is dependent on achievable modulation speeds and on-chip losses. The ~ 600 ps delay lines (which are closer to 580 ps in reality) were deemed the most suitable, and so this was the only option to be included on later designs.

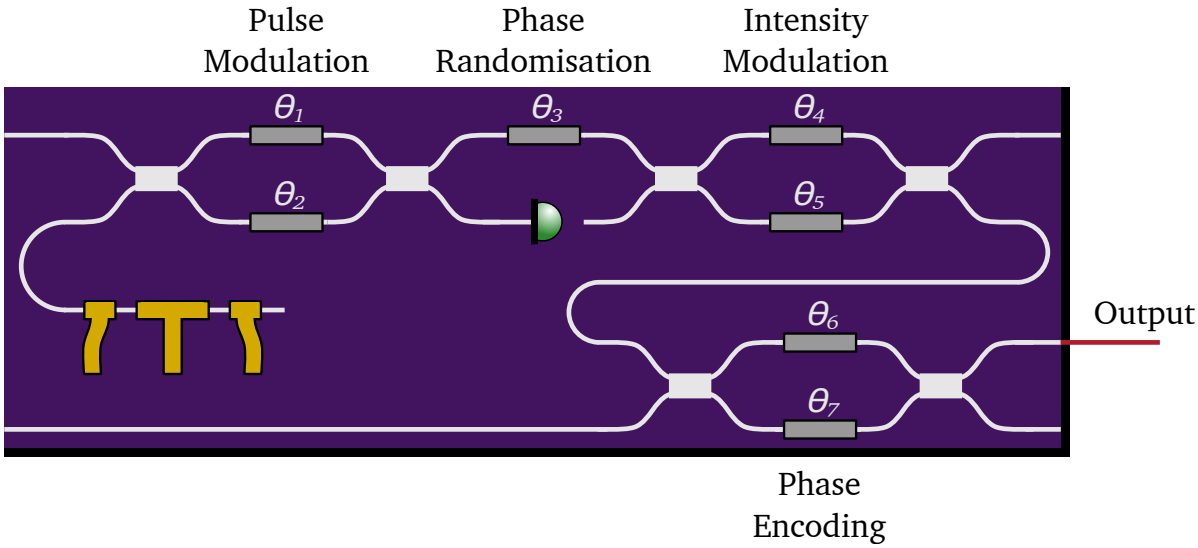


FIGURE 7.20: A schematic of the single-channel Alice chip. Time-bin encoding is achieved through pulse modulation within the > 1.5 ns coherence time of the continuous-wave laser [247], as the propagation loss is too high for a delay line to be incorporated. Phase randomisation is required to prevent unambiguous state discrimination from being used to compromise the security of decoy state protocols [44].

7.2.1 Characterising the Wavelength-Division Multiplexers

Each (de-)multiplexer can only transmit a discrete spectrum of wavelengths, and so in order to identify suitable operating parameters, these needed to be measured. Like in an MMI, light entering a bulk AWG is diffracted into free space and split between multiple waveguides, though here they are of different lengths. The photons are then coupled back out into free space, interfering on the output fibres. Thus, the AWG is very similar to an AMZI, in that it is designed to have a free spectral range, determined by relative path lengths. We can measure this using white light to address the input, and an optical spectrum analyser which scans across all outputs. While we are technically operating the AWG in a demultiplexing configuration, optical reversibility means the results we obtain are equally valid when it is used as a multiplexer. The signals on each output of the AWG are shown in figure 7.21, and from this we can see that a single ~ 1 nm peak is present in every channel.

When it comes to implementing full WDM-QKD, we will want to minimise any crosstalk between the different Alice/Bob pairs, which is quantifiable as a power ratio between the peak transmission of a particular output, and the point where it intercepts any adjacent outputs in figure 7.21. Photons exiting through unused ports will only serve to increase the insertion loss of the AWG, however if they were to be routed into the wrong Bob chip, they would become an active source of error. Therefore, based on the data, it is clear that only every other channel should be occupied.

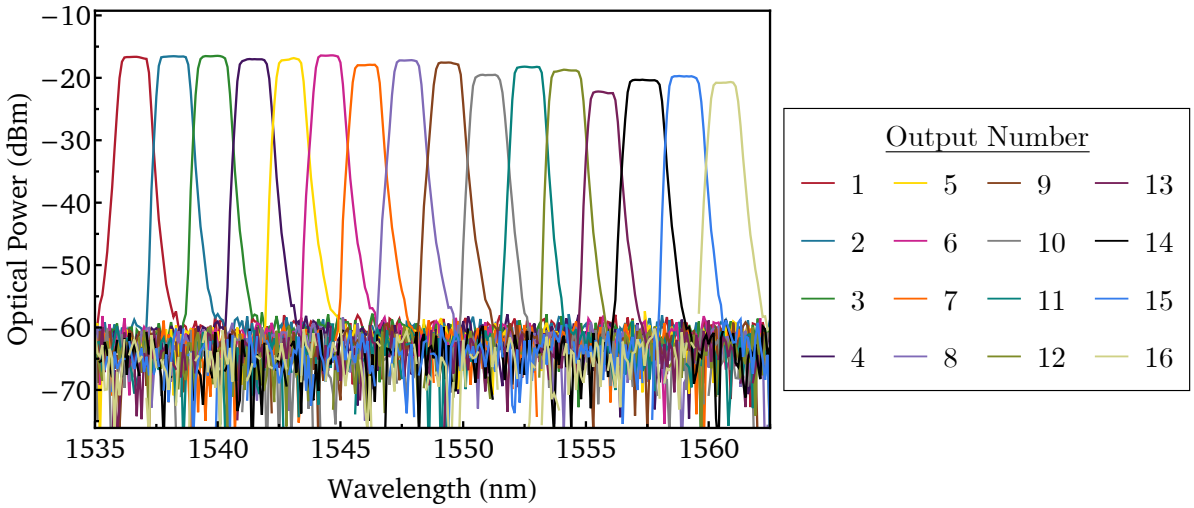


FIGURE 7.21: Wavelength-division de-multiplexing white light using the bulk arrayed waveguide grating (AWG). The peak input power was 0 dBm. Measurements were taken on an optical spectrum analyser, and each coloured line corresponds to a different output channel of the AWG. Due to the principle of optical reversibility, we can switch the input and output ports to operate it as a multiplexer instead.

The integrated AMZI can be characterised in exactly the same way, although there are now only two outputs. In figure 7.22, we measure on each arm and see that, in both cases, multiple wavelengths can be supported. This is important as it provides flexibility with regards to wavelength selection, and also allows for several AMZIs to be concatenated, increasing the number of channels that can be demultiplexed. However, fabrication imperfections mean we cannot guarantee that it will be optimally aligned with the AWG in all cases. Luckily, such an issue can be resolved by modulating the voltage applied to the Peltier cooler that is responsible for thermally stabilising the chip. Figure 7.23 demonstrates that the temperature shift allows for the wavelength peaks to be fine-tuned over a range of roughly 2 nm, although any change is applied globally. Yet on this basis, the integrated AMZI and bulk AWG seem fully compatible.

7.2.2 Characterising the Integrated Laser

Of course, integrated WDM-QKD will only be practical if we can precisely and accurately control the wavelength of the laser, such that we are able to address any of the AWG channels without having to modify the cavity design. Figure 7.24 shows that there exists a linear temperature dependence due to the expansion of the material between 21 and 25 °C, which can be exploited to provide coarse wavelength tuning. At 20 °C, we observe a departure from this trend, due to the temperature dependence of the SOA. As can be seen in figure 7.24a, the cavity actually supports two wavelengths, however between 21 and 25 °C, the SOA predominantly amplifies the upper of these. When we

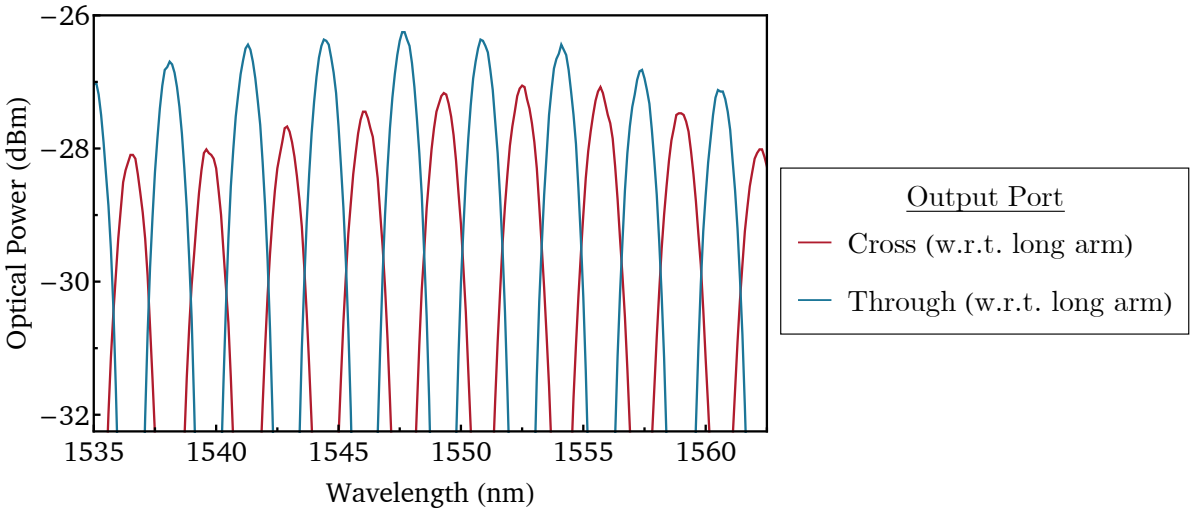


FIGURE 7.22: Wavelength-division de-multiplexing white light using the asymmetric Mach Zehnder interferometer (AMZI) on the Bob chip. The peak input power was 0 dBm. Measurements were taken using an optical spectrum analyser, and each coloured line corresponds to a different output channel of the AMZI.

reach 20 °C, this behaviour changes, and the lower wavelength is amplified the most, leading to a discontinuity in figure 7.24b. Such a point is not overly concerning as, when we transition to a monolithic set of transmitters, it will not be possible to apply a different temperature to each, so these results mainly emphasise the necessity of thermal stabilisation.

A much finer tuning can be achieved by modulating the voltage applied to the TDBRs, and figure 7.25 illustrates the range over which this is possible, where the underlying data has a minimum resolution of 0.01 nm. The presented results can also be used in conjunction with those of section 7.2.1 to identify the optimal wavelength for each channel. We find 1544.77 nm and 1547.92 nm to be the most suitable values, corresponding to International Telecommunications Union dense wavelength-division multiplexing (DWDM) channels 41 and 37. This means the TDBR voltages should be set to 0.75 V and 1 V for the first transmitter, followed by 0.95 V and 0.8 V for the second. 13.28 V should be applied to the Peltier cooler that controls the temperature of the AMZI, resulting in a wavelength shift of −1.38 nm.

7.2.3 Modulating the Asymmetricity of a Mach-Zehnder Interferometer

While the work done so far is sufficient to enable an initial demonstration of on-chip WDM-QKD, our approach to modulating the peak AMZI wavelengths will not help in the situation where four or more channels are de-multiplexed on the same chip but fabrication imperfections mean each AMZI is slightly different. In this case, we ask whether application of an electric field to individual AMZIs could produce a phase offset, compensating for their lack of uniformity and allowing for the

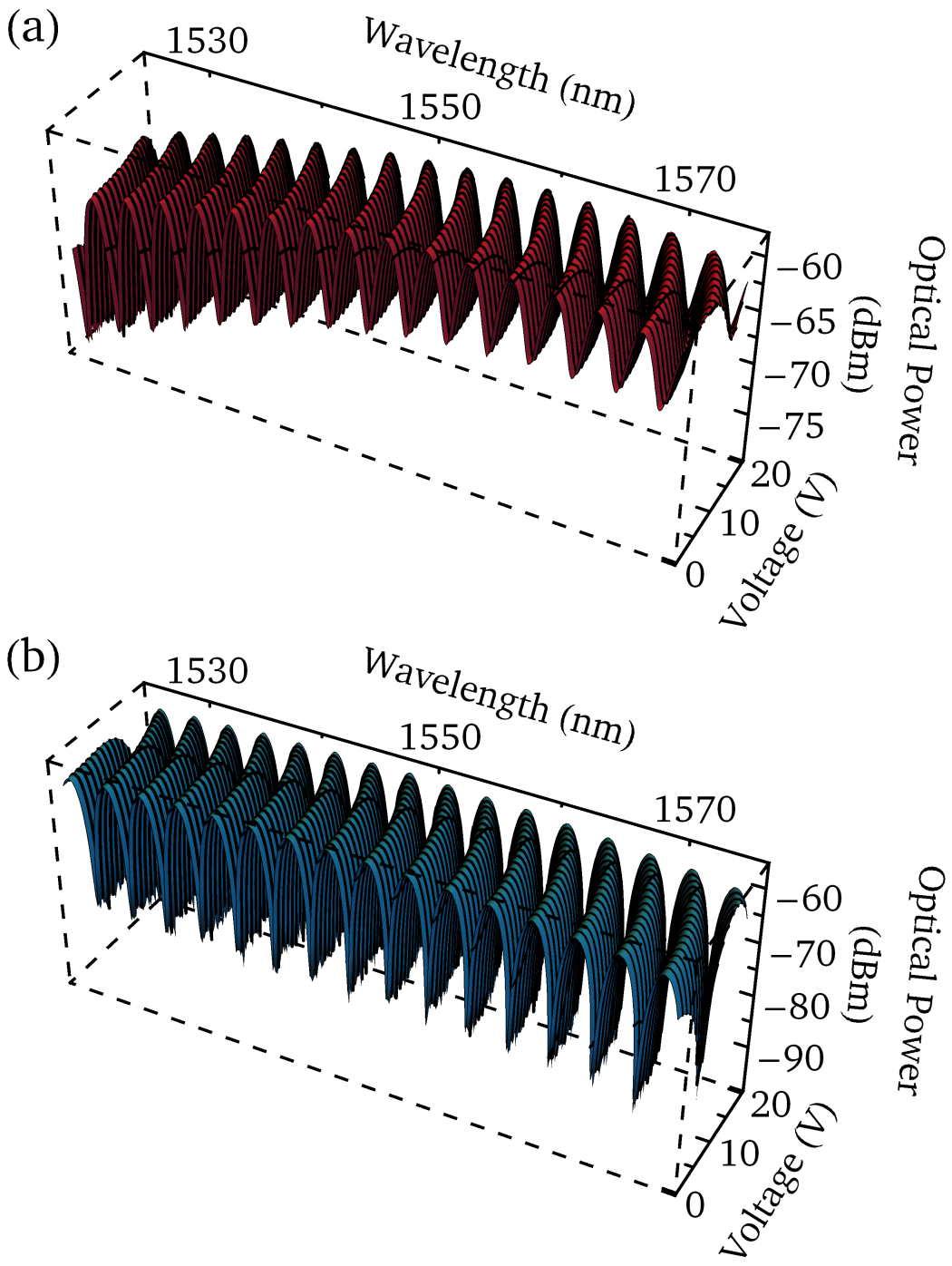


FIGURE 7.23: Temperature-tuning the asymmetric Mach-Zehnder interferometer (AMZI) on the Bob chip, by modulating the voltage applied to the Peltier cooler. Measurements were taken using an optical spectrum analyser on (a) the cross port and (b) the through port of the AMZI, both with respect to the longer of the two arms.

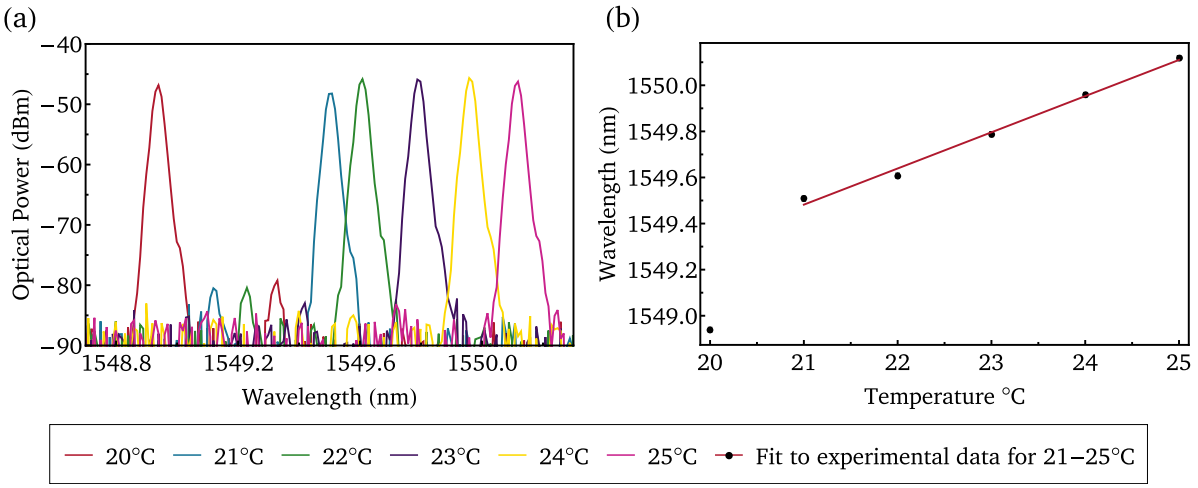


FIGURE 7.24: (a) Optical spectra for the integrated laser on the Alice chip over a range of different temperatures. (b) Plotting the peak wavelength of the integrated laser against the temperature at which the chip is stabilised. From this, we can see that coarse wavelength-tuning is possible.

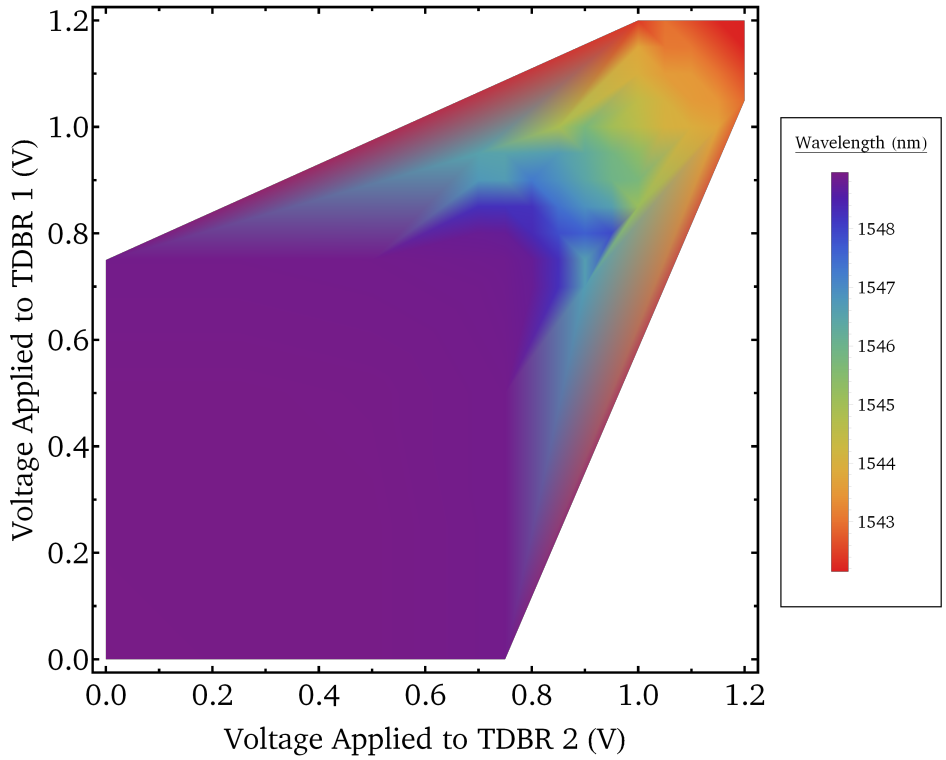


FIGURE 7.25: Fine-tuning the peak wavelength for the integrated laser on the Alice chip by applying a range of different voltages to the tunable distributed Bragg reflectors (TDBRs). Here, TDBR 1 is that closest to the laser output.

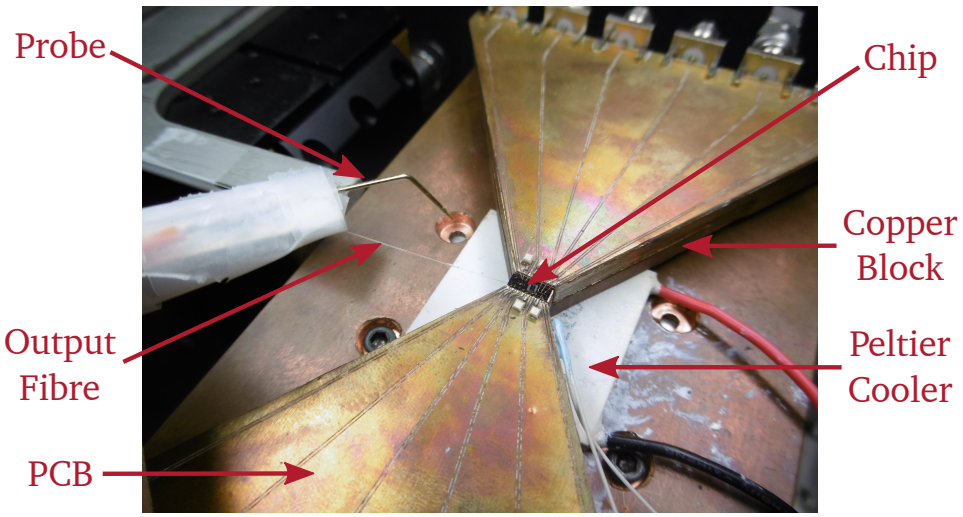


FIGURE 7.26: Showing the physical setup of the Alice chip, with an external probe on a temporary mount. In future evolutions of the hardware, an integrated version of the probe can be added to the optical circuit, so as to mimic its functionality.

wavelength-tuning methods of section 7.2.1 to regain their usefulness.

To find out, an external probe was lowered onto a TOPM bond pad (see figure 7.26), generating a voltage gradient across the phase shifter. We avoided accidentally destroying one of the two-channel Bob chips by carrying this out on an old device, which only contained a standard MZI, however there is no reason why the results obtained herein should not be directly applicable to its asymmetric counterpart.

We found we were able to modulate the MZI as desired, and figure 7.27 shows how the absolute phase induced by the MZI changes with voltage. While the data is a little noisy, this is likely down to the rudimentary way in which the electric field was applied, so a fully integrated solution can be expected to follow the quadratic trend more closely.

7.3 Monolithic Wavelength-Division Multiplexed Quantum Key Distribution

In the previous section, we presented the initial steps towards on-chip WDM-QKD, which a colleague subsequently realised. The overall secret key rate scaled linearly with the number of channels, meaning we can move ahead with expanding the system from two wavelengths to four, monolithically integrating all Alices using a set of colourless MMIs in place of the bulk AWG, and providing the option to daisy-chain up to 12 additional Bobs, for a total of 16. We note that the MMIs were chosen because of their design simplicity when compared to alternatives, however they only work for implementations that rely on weak coherent pulses. Each MMI (of which there are three) should introduce 3 dB of loss if there are no imperfections, meaning the rest of the chip must be calibrated

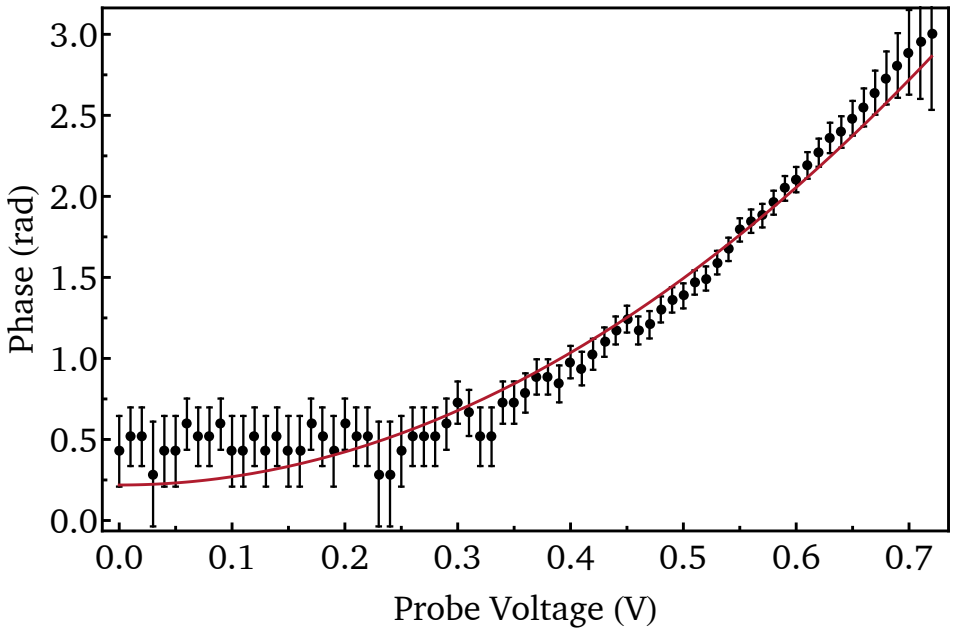


FIGURE 7.27: Showing how the absolute phase shift across a Mach-Zehnder interferometer varies according to the voltage applied by an external probe. The red line is a parabolic fit to the experimental data.

accordingly. As the Oclaro fabrication process had changed since the original transmitters were manufactured, a set of individual Alices was developed for testing purposes. Their schematics are identical to that in figure 7.20, with the exception of newly-available TOPMs having been added to handle functions such as attenuating the laser, where fast modulation is not required.

Thus far, a test transmitter has been electrically packaged and mounted on a copper block (see figure 7.28), so its present state is awaiting optical characterisation. In order to control the on-chip modulators, a printed circuit board (PCB) was manufactured in Rogers 6006ns, the same material used for the transmitter PCBs in section 7.2. Its high relative permittivity means the transmission lines leading to the EOPMs can be separated by as little as 100 μm for radio-frequency signals, and so we choose this to be our minimum spacing. For the PCB shown in figure 7.26, the transmission lines were further apart, hence we are able to achieve a reduction in physical size from 12.5 × 8.1 cm to 2.9 × 5.4 cm.

The copper block was designed in a modular style, such that either side of the PCB could be replaced, allowing the testing of an independent quantum random number generator (QRNG) that was fabricated on the same chip. The size of each copper module is now the main restriction when it comes to further miniaturisation, as they are limited by the amount of material required to prevent flexing, which was a major problem for the previous Alice chip. We also note that it would not have been possible to test both Alice and the QRNG using a single PCB, as the narrowness of the bond pad spacing would have prevented wirebonding. Even if this were not the case, such a fine pitch

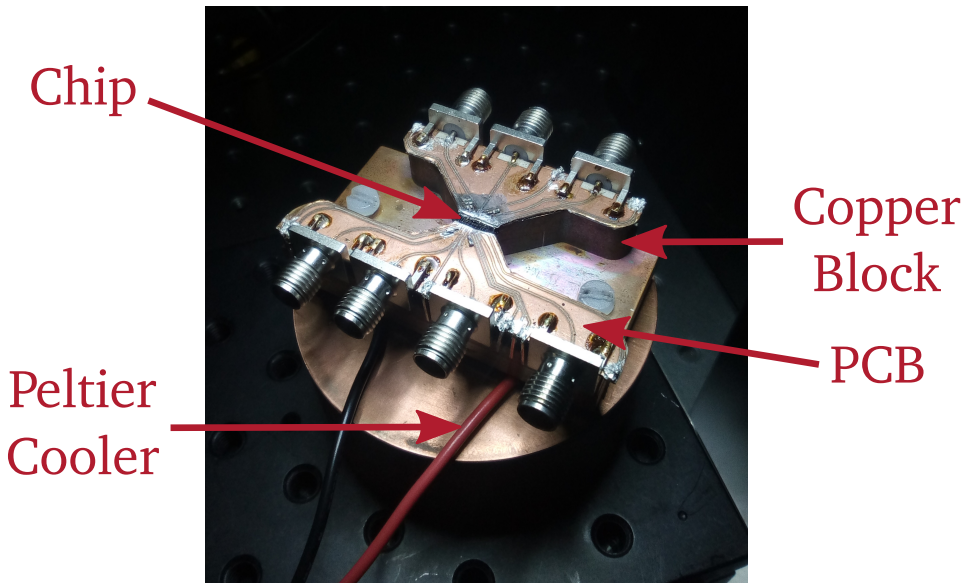


FIGURE 7.28: The test transmitter for monolithic wavelength-division multiplexed quantum key distribution. The chip has been electrically packaged and mounted on a modular copper block, allowing for PCB interchangeability, with a flex-resistant design.

would have affected the characteristic impedance of the transmission lines, to the detriment of the high-speed electrical signals. Identifying constraints such as these is informative for the full transmitter, as there are many more connections, and so a multi-tiered PCB will need to be designed, research into which is ongoing.

A schematic for the four-channel receiver is shown in figure 7.29. In contrast to the previous QKD devices that Bristol has developed, a decision was made not to mount it on a chip rig, which would usually comprise an optical table with manual alignment stages and a floating fibre. This was because the heat from the number of TOPMs would cause the chip to expand and decouple from the input and output fibres during characterisation. Instead, a 24-fibre Oz Optics V-Groove array (VGA) was glued to each side, chosen because it was the largest VGA available that had a 127 μm pitch and did not exceed the width of the chip. We were able to address all of the inputs and outputs corresponding to each of the Bobs, and some of the test structures that were fabricated alongside them. Naturally, fewer fibres would be required in a commercial version of the device, as WDM-QKD means the signal is confined to a single input. The remaining connections exist simply for testing purposes.

Figure 7.30 shows the chip in the final stages of the gluing process (see appendix D for more details). The vacuum chucks, which held the VGAs in place prior to the glue being applied, were each mounted on a six-axis Thorlabs NanoMax alignment stage. The PCB was made from aluminium clad in copper, so that a Peltier could be placed underneath to keep the chip cool. When attaching the PCB to the receiver, Fischer Elektronik's Thermally Conductive Adhesive WLK was used, as it

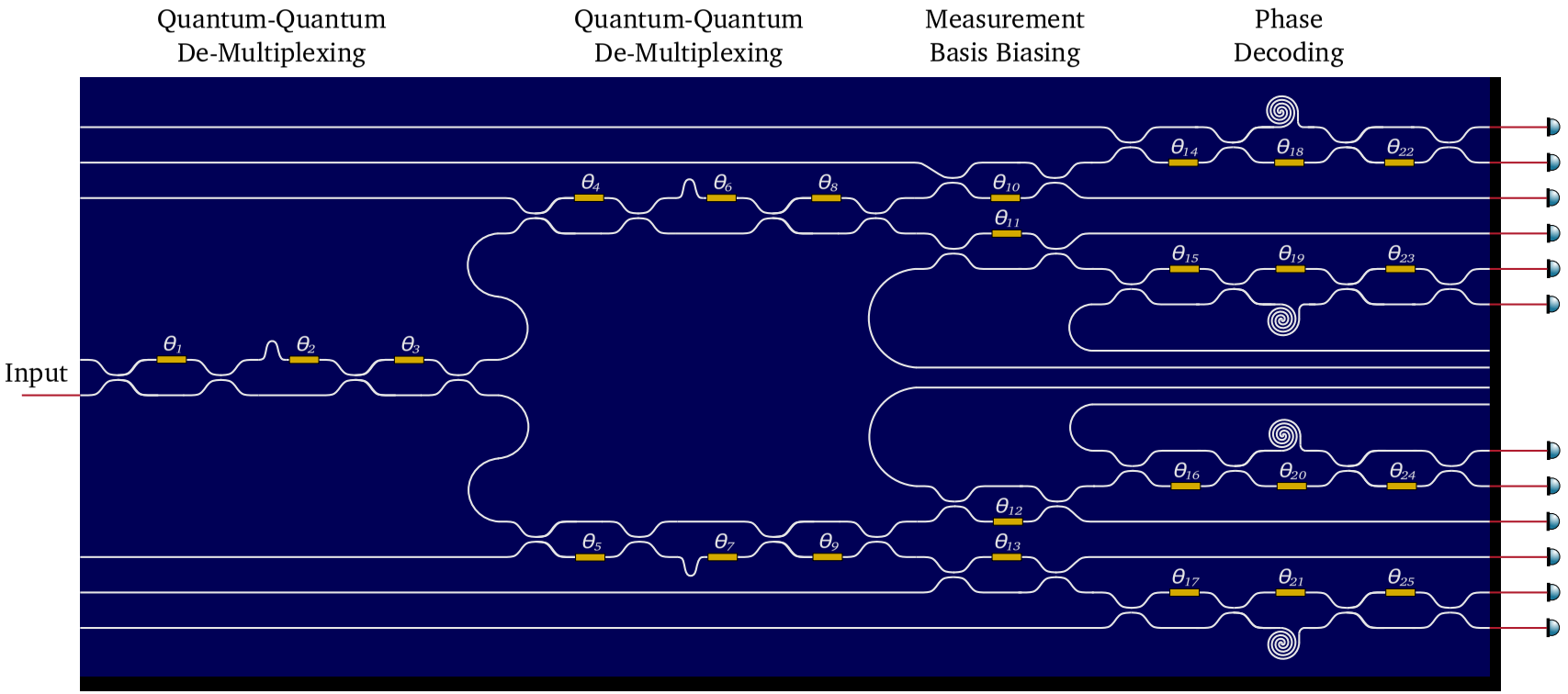


FIGURE 7.29: A simplified schematic of the four-channel Bob chip with wavelength-division de-multiplexing capabilities and 580 ps phase-decoding delays. Multiple monolithic devices can be daisy-chained if additional channels are required.

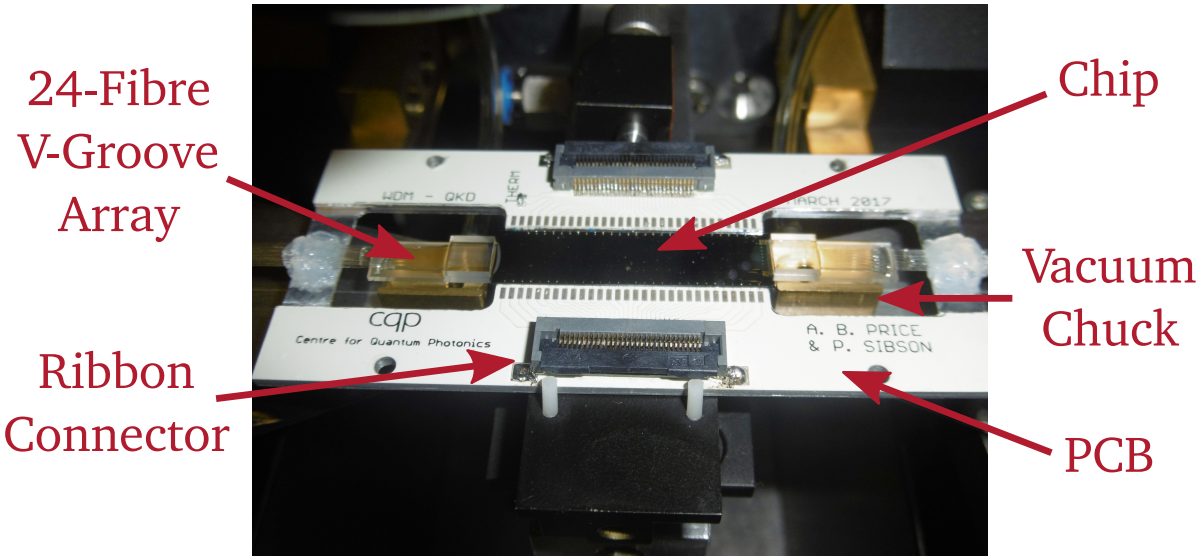


FIGURE 7.30: The fully packaged receiver chip for monolithic wavelength-division multiplexed quantum key distribution. This photograph was taken after the initial 24-hour dose of UV radiation, which allowed the vacuum chucks to be dropped away. The curing process was completed by placing the chip in a biological steriliser and bathing it in strong UV.

had the lowest viscosity of the epoxies available, falling somewhere between 0.25 and 0.30 Pa · s. This was an important consideration, because the adhesive had to evenly cover the entire area of the chip underside, relying solely on the weight of the receiver causing it to spread. The only downside to the epoxy is that it has to be applied in a fume cupboard, due to the potential carcinogenicity of its constituent parts, and this may make it unsuitable for a mass-production environment.

The four-channel receiver was the largest chip to have been optically packaged in Bristol. Initially, the VGAs were attached with Norland Optical Adhesive 86 because, of the three glues known to work well, it had the highest tensile strength at 7834 pound-force per square inch (psi), and the size of the VGA means higher forces are expected to be exerted. However, over a period of several weeks, the glue began to leak out, despite having been properly cured, until eventually the VGAs were no longer attached. A second round of gluing was therefore required, and this time Norland Optical Adhesive 63 was chosen, which had the greatest hardness of the three options, with a Shore D value of 90. The chip has now been fully packaged for over five months, in a router-sized box that is complete with driving electronics. No further structural failures have been observed.

Figure 7.31 presents a series of loss measurements made prior to gluing, over four sections of waveguide that were free of optical components and whose length was known. The anomalous result is due to a damaged facet on the chip however, from the remaining points, we estimate the propagation loss to be 0.17 dB/mm, with a coupling loss of 2.83 dB for every chip-to-air interface. As Norland Optical Adhesive is index matching, we expect the latter attenuation to have slightly

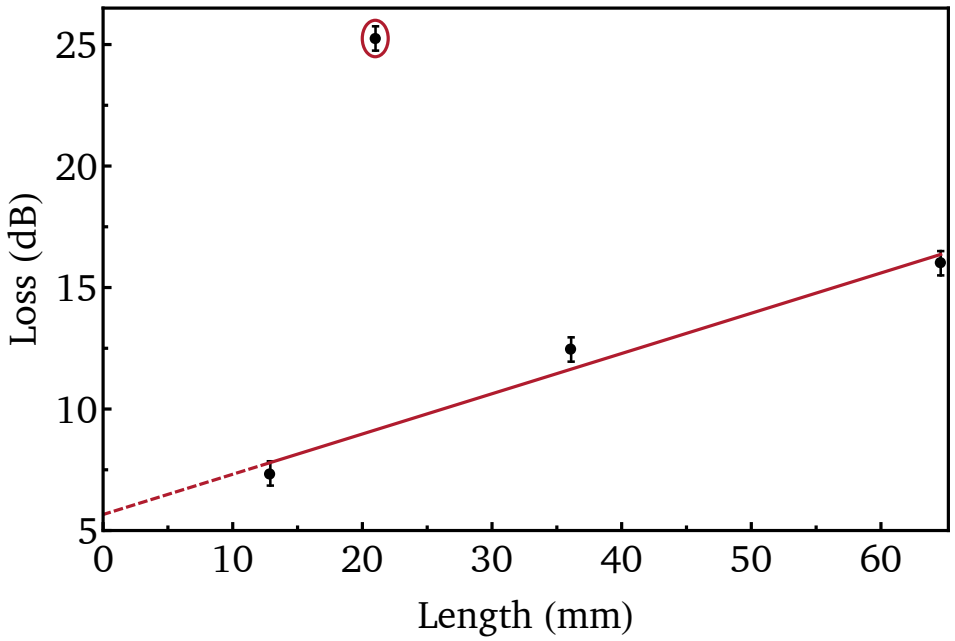


FIGURE 7.31: Plotting the absolute loss for different lengths of component-free waveguide on the four-channel Bob chip. The circled anomaly is likely as a result of damage to the optical facet. The gradient of the fitted line (0.17 dB/mm) corresponds to the propagation loss, and the extrapolated y-intercept (5.66 dB) is 2× the coupling loss.

decreased since the receiver was glued, however some of the loopbacks can no longer be addressed, due to the size of the VGAs, so there is no way of confirming this.

Figure 7.32 shows that, as expected, the voltage-current relationship for the TOPMs is linear. By monitoring the optical output power, we find that the phase shift this induces begins to saturate above 17 V, however we can comfortably reach 5.34 ± 0.07 rad without exceeding the capabilities of our driving electronics.

Finally, a test structure for an integrated AWG was included on the receiver, to establish whether it could supersede the AMZIs in a future design. We found that it operated well in terms of the wavelengths transmitted, with peaks at 200 GHz intervals over a 100 nm range. However, it is 31.01 dB lossier than an AMZI, so further developments are clearly required.

7.4 Next-Generation Silicon Photonic Chip Design

Chip fabrication runs happen every few months, however it can take over a year to get from an initial design to a physical device. As a result, the masks for next-generation QKD systems must be compiled prior to the completion of experiments involving earlier devices. Here, we present four designs, each named after a famous transmitter or receiver of messages. All were fabricated in Si, as part of an Institute of Microelectronics multi-project wafer, and the complete mask is presented

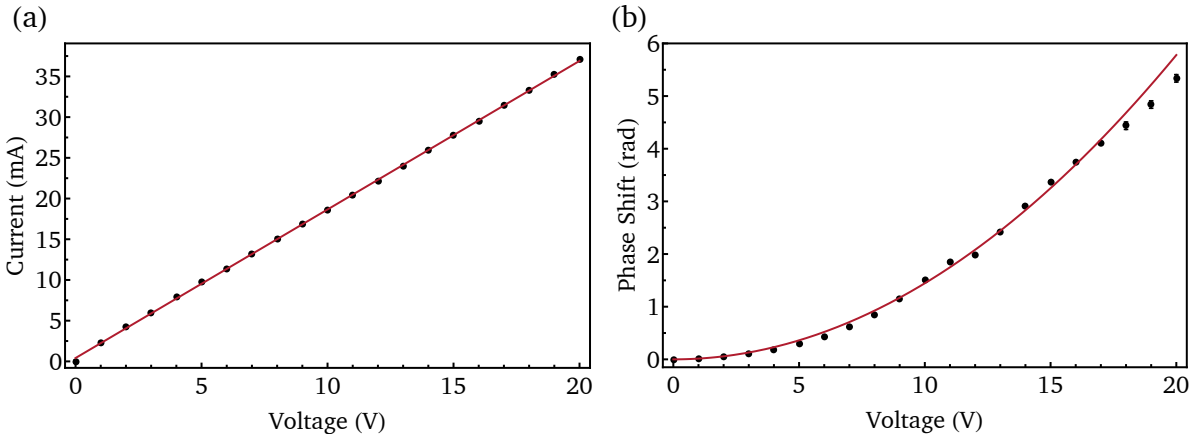


FIGURE 7.32: Plotting (a) the current-voltage relationship for a thermo-optic phase modulator on the Bob chip, with a linear fit to the experimental data, and (b) the voltage-dependent relative phase shift of the Mach-Zehnder interferometer in which it is embedded, with a parabolic fit to the experimental data. In the case of the latter, saturation begins to occur at higher voltages due to imperfectly fabricated directional couplers.

in appendix E.

7.4.1 A Reference-Frame-Independent Quantum Key Distribution Transmitter

We first present Anubis, which is a reference-frame-independent (RFI)-QKD transmitter capable of either polarisation or time-bin encoding. The intention is for it to communicate with a low-cost bulk receiver, designed and built by Dr. David Lowndes. RFI-QKD [346] uses a reference-frame-invariant basis to enable key generation between two parties who are moving in an otherwise detrimental manner relative to one another. For example, in the case of a rotating satellite, the polarisations that may be considered "horizontal" and "vertical" are constantly changing with respect to the ground. However, the handedness of circularly polarised light will remain unaffected, so we can use this as the key generation basis, and bound Eve's knowledge by measuring correlations between the slowly-changing, arbitrarily-named horizontal/vertical and diagonal/anti-diagonal polarisations. The exact details of the protocol are unimportant at this stage, as all we need to know for the purposes of chip design is that it will be necessary to prepare $\{|\mathbb{i}\rangle, |-\mathbb{i}\rangle\}$ in addition to the usual $\{|\bar{0}\rangle, |\bar{1}\rangle\}$ and $\{|+\rangle, |-\rangle\}$.

The schematic for Anubis is shown in figure 7.33. A continuous-wave off-chip laser is coupled in on the left-hand side of the diagram, with the first MZI attenuating it down to just above the single-photon level. The light is then split into two parallel sets of dual rails, and a second MZI is used for pulse carving, with further attenuation if required.

It has been established in previous work that the CDMs saturate before reaching a full π phase

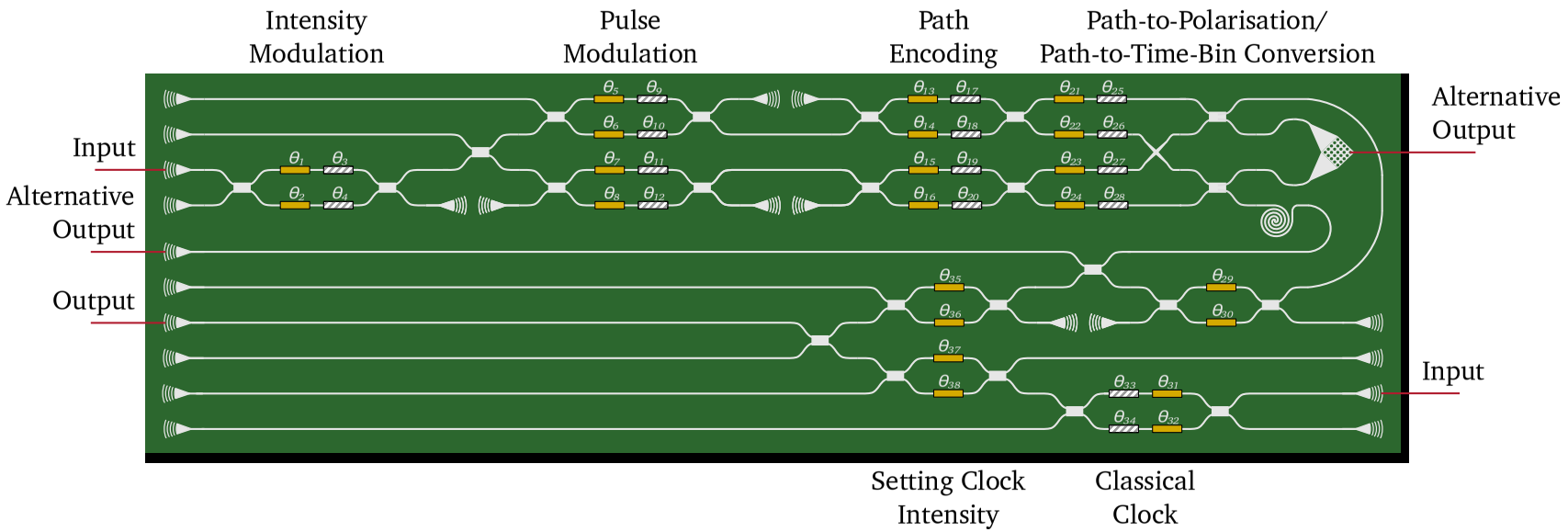


FIGURE 7.33: A schematic for Anubis, the 1550 nm reference-frame-independent quantum key distribution transmitter chip. Polarisation or time-bin encoded qubits are generated using an off-chip laser as the optical source. These can be multiplexed on-chip with a classical clock, once again using a separate laser.

shift [324]. To get around this, the TOPMs can be used in the path encoding step to prepare the state $|\mathbb{i}\rangle = \frac{|\bar{0}\rangle + \mathbb{i}|\bar{1}\rangle}{\sqrt{2}}$, meaning that the CDMs only need to deliver $\frac{\pi}{2}$ phase shifts in order to generate any of the Bennett-Brassard 1984 (BB84) states. However, in RFI-QKD, $|-\mathbb{i}\rangle = \frac{|\bar{0}\rangle - \mathbb{i}|\bar{1}\rangle}{\sqrt{2}}$ must also be transmitted, which the CDMs cannot reach on their own if we are modulating about $|\mathbb{i}\rangle$. It is for this reason that are now using two sets of dual rails for path encoding. By preparing $|\mathbb{i}\rangle$ with the TOPMs on one arm, and $|+\rangle$ with the TOPMs on the other, we can use the corresponding CDMs to realise $\{|\bar{0}\rangle, |\bar{1}\rangle, |+\rangle, |-\rangle\}$ and $\{|\bar{0}\rangle, |\bar{1}\rangle, |\mathbb{i}\rangle, |-\mathbb{i}\rangle\}$.

Following this, either polarisation or time-bin conversion can be implemented in the standard fashion, merging the two state preparation arms in the process. There is the option to dense wavelength-division multiplex the quantum signal with a classical clock, combining them on an MMI, just as we do with pure QKD channels on the monolithic WDM-QKD transmitter. While we will argue in section 7.4.2 that this is unlikely to scale well when considering large numbers of clock signals on arbitrary networks, on-chip classical-quantum DWDM is the first step towards the more complex task of coarse wavelength-division multiplexing the 1310 nm structures we develop later with the 1550 nm structures here.

The mask for Anubis is presented in figure 7.34, compiled using IPKISS from source code written in Python. It was based around a component library developed internally by the Centre for Quantum Photonics, and an additional 3366 lines of code were written by the author to produce Anubis, Big Ear, Cher Ami and Dzakar. In order to minimise the attenuation of the delays, we increase the width of the waveguide whenever a straight section is encountered. This reduces scattering from the sides of the waveguide which, due to the surface roughness, is the dominant source of loss [347]. A gradual taper is included to suppress diffraction as this would otherwise lead to excitation of higher order modes, like in an MMI. Further design choices will be discussed in the sections that follow.

7.4.2 A Transmitter and Receiver for Chip-to-Chip Quantum Key Distribution at 1310 nm

Thus far, this thesis has aimed to identify and address some of the practical challenges that face real-world applications of QKD. Of course, such an effort would not be complete without at least touching on the issue of classical-quantum co-existence. A number of solutions have been previously implemented, such as spatial-division multiplexing over multicore fibre [348] and WDM approaches that are not too dissimilar to those used for combining quantum signals in this thesis. Of these options, the latter is by far the most explored, though scalability issues do exist. If DWDM wavelengths are required, Raman scattering becomes a source of noise, transferring optical power from the classical signal to adjacent wavelengths through a process of absorption and re-emission [349, 350]. While many experiments have been carried out in this regime [169–171, 351, 352], those that rely on the careful placement of quantum signals at low-noise wavelengths will quickly begin to struggle as more classical signals are added and the noise profile moves towards being homogeneous. Furthermore, as illustrated by figure 7.35, additional sources of noise on the Bristol Quantum Network reduce

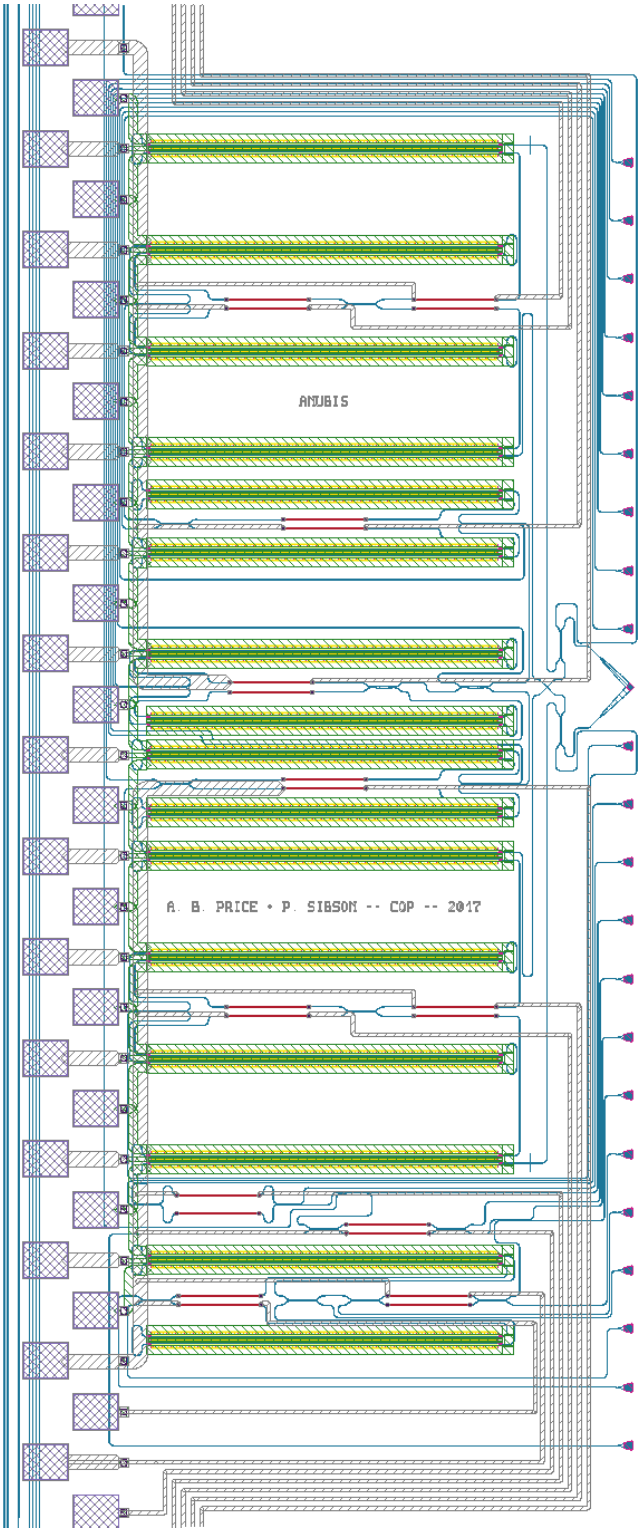


FIGURE 7.34: The mask for Anubis, compiled from source code written in Python. Annotations identifying each component are provided in figures 7.39 and 7.41.

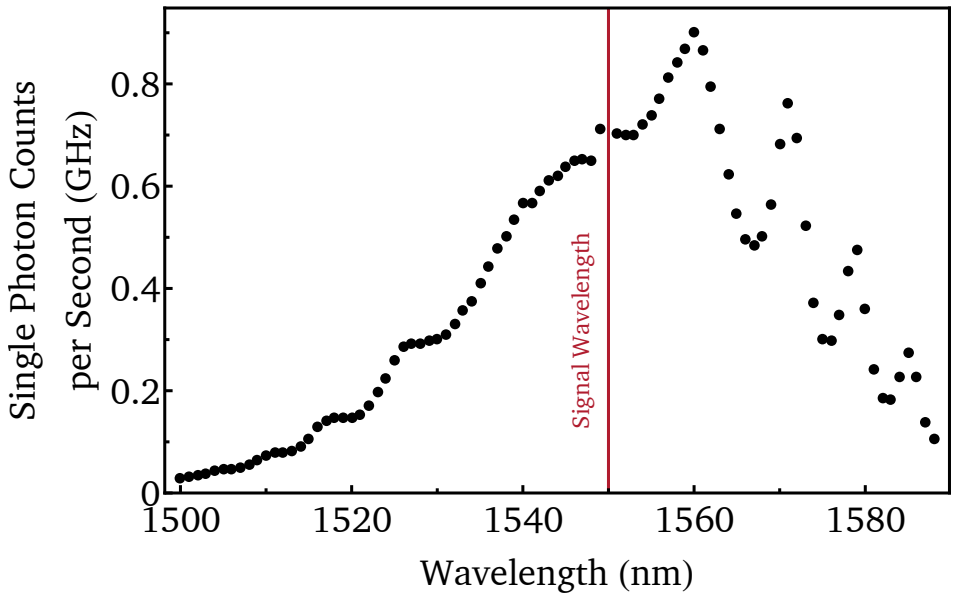


FIGURE 7.35: Raman noise for a single classical signal emulated by a 1550 nm continuous-wave laser with a -4.8 dBm launch power. Measurements were carried out using an ID Quantique ID210 single-photon detector on the Bristol Quantum Network, between the Centre for Nanoscience & Quantum Information and the Merchant Venturers Building (see section 3.1.3). Here, the detector efficiency, gate width and gate frequency have all been taken into account. A bandpass filter with a 50 pm full-width half-maximum was used to scan across the spectrum.

the size of the dips that are introduced by the Raman gain profile. When these measurements were first carried out on an indirect, temporary link between the Centre for Nanoscience & Quantum Information and the Merchant Venturers Building, the situation was even worse, as the number of server-room connections meant no dips could be found. Therefore, strategies that exploit these do not scale to arbitrary networks. However, we note that as the wavelength decreases in figure 7.35, the noise from Raman scattering of the 1550 nm laser tends towards zero, raising the possibility of running QKD at 1310 nm in longer-distance environments where, unlike the data centres emulated in chapter 3, classical light occupies the C-band. This has previously been implemented in [353, 354], although a full O-band on-chip QKD solution is yet to be demonstrated. Therefore, in this section, we present a 1310 nm receiver (Big Ear) and a 1310 nm transmitter (Cher Ami), schematics for which are provided in figures 7.36 and 7.38 respectively. The corresponding masks can be found in figures 7.37 and 7.39.

The 1310 nm chip designs are very similar to those of the original InP and SiO_xN_y devices, with the main differences being in the transmitter. As described in section 7.4.1, it is possible to fabricate low-loss delay lines in SoI, meaning we can use a passive time-bin encoding scheme [62] rather than having to pulse modulate within the coherence time of the laser.

All of the mask components have been physically scaled to ensure compatibility with 1310 nm

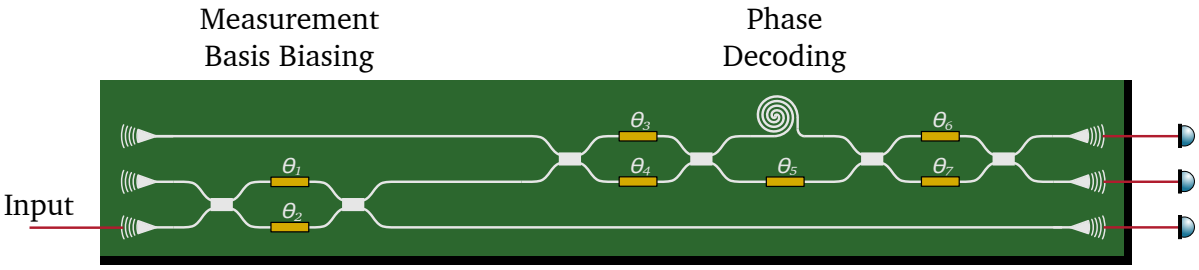


FIGURE 7.36: A schematic for Big Ear, the 1310 nm quantum key distribution receiver chip. This follows the same layout as the original 1550 nm SiO_xN_y receivers, and can therefore be used to implement the BB84 with decoy states, Differential Phase Shift [355] or Coherent One Way [239] protocols.

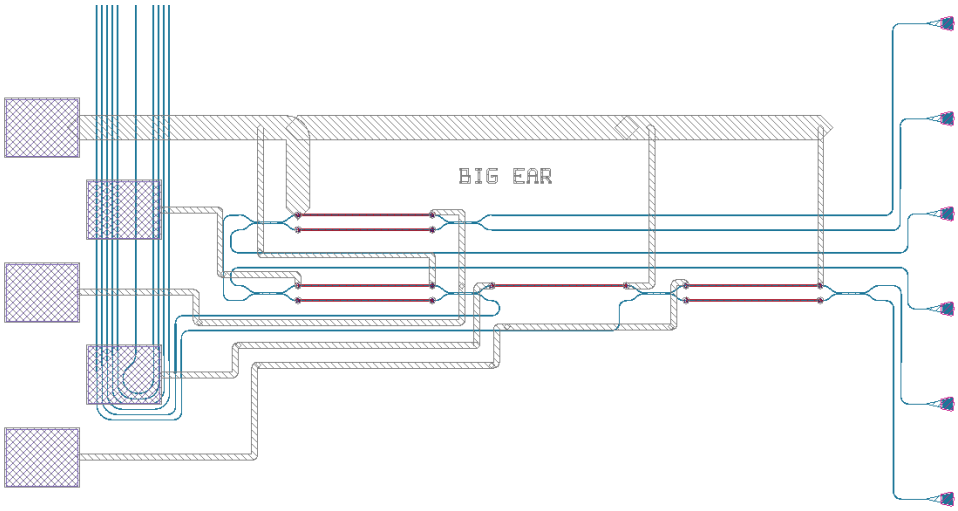


FIGURE 7.37: The mask for Big Ear, compiled from source code written in Python. Annotations identifying each component are provided in figures 7.39 and 7.41.

light. A folded design was developed for the CDMs in both this and the previous section, reducing the width of the chip so as to keep it within the design boundaries. When connecting the CDMs to bond pads, vias were used to transition the track into a metal layer that was further away from the waveguides. This prevented the electrical signals from accidentally modulating light travelling down the delay line that is positioned underneath.

7.4.3 A Polarisation-Compensating Receiver for Time-Bin-Encoded Quantum Key Distribution

The final chip design (Dzakar) can be operated in one of two ways. It may either de-multiplex QKD signals from a classical clock and act as a receiver for both, or it may be used to compensate for

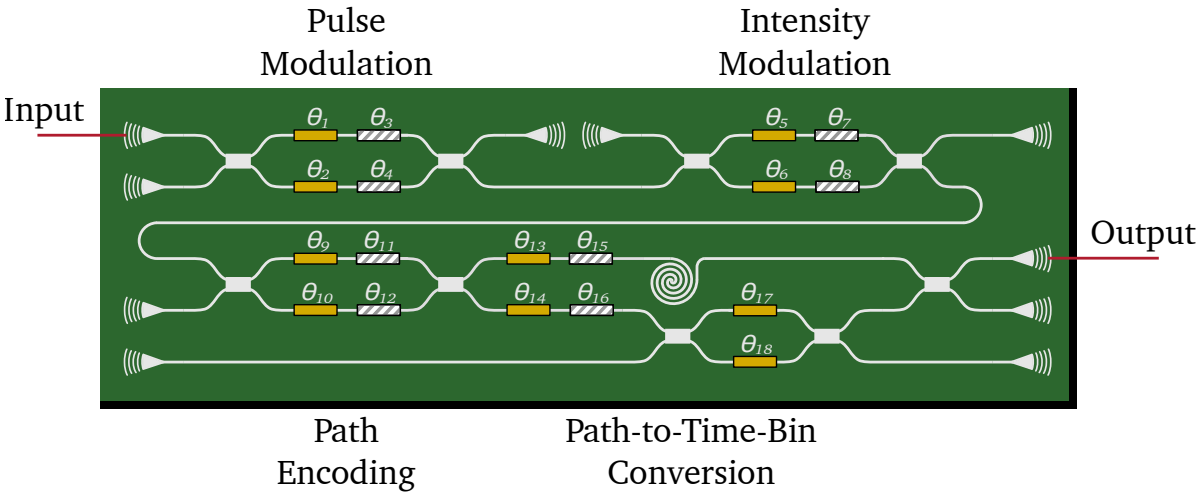


FIGURE 7.38: A schematic for Cher Ami, the 1310 nm quantum key distribution transmitter chip that can be used to implement the BB84 with decoy states, Differential Phase Shift or Coherent One Way protocols. Time-bin encoded qubits are generated by exploiting a low-loss delay line, using an off-chip laser as the optical source.

polarisation drift in the time-bin-encoded quantum signal. A schematic is shown in figure 7.40, and the mask is in figure 7.41. Here, the classical-quantum de-multiplexer is an AMZI, as was used for WDM-QKD earlier in this chapter. It directs the clock into an on-chip APD, and the qubits into a standard time-bin receiver circuit.

The transverse electric (TE) and transverse magnetic (TM) modes of a waveguide couple to off-chip transmission media with orthogonal polarisations. In addition, the transmission angle is polarisation-dependent when 1D grating couplers are used, so only TE modes can be efficiently transferred out of the waveguide [337]. As always, the reverse is also true, and polarisations corresponding to TM modes will not couple onto the chip. Hence, we will experience a drop in key rate if the polarisation of the quantum signal drifts unpredictably, as is the case for single-mode fibre (SMF) deployed in the field.

For this reason, we have implemented a circuit designed to maximise throughput on Dzakar. Recall that 2D grating couplers are a method for transferring orthogonal polarisations into the TE modes of two separate waveguides. Therefore, by incorporating an MZI immediately after, we can recombine the signal and counteract the drift that would have otherwise been highly detrimental to QKD.

7.5 Outlook

In this chapter, we have characterised the devices that were later used in the first demonstration of chip-based WDM-QKD. We found that 1544.77 nm and 1547.92 nm (ITU channels 41 and 37)

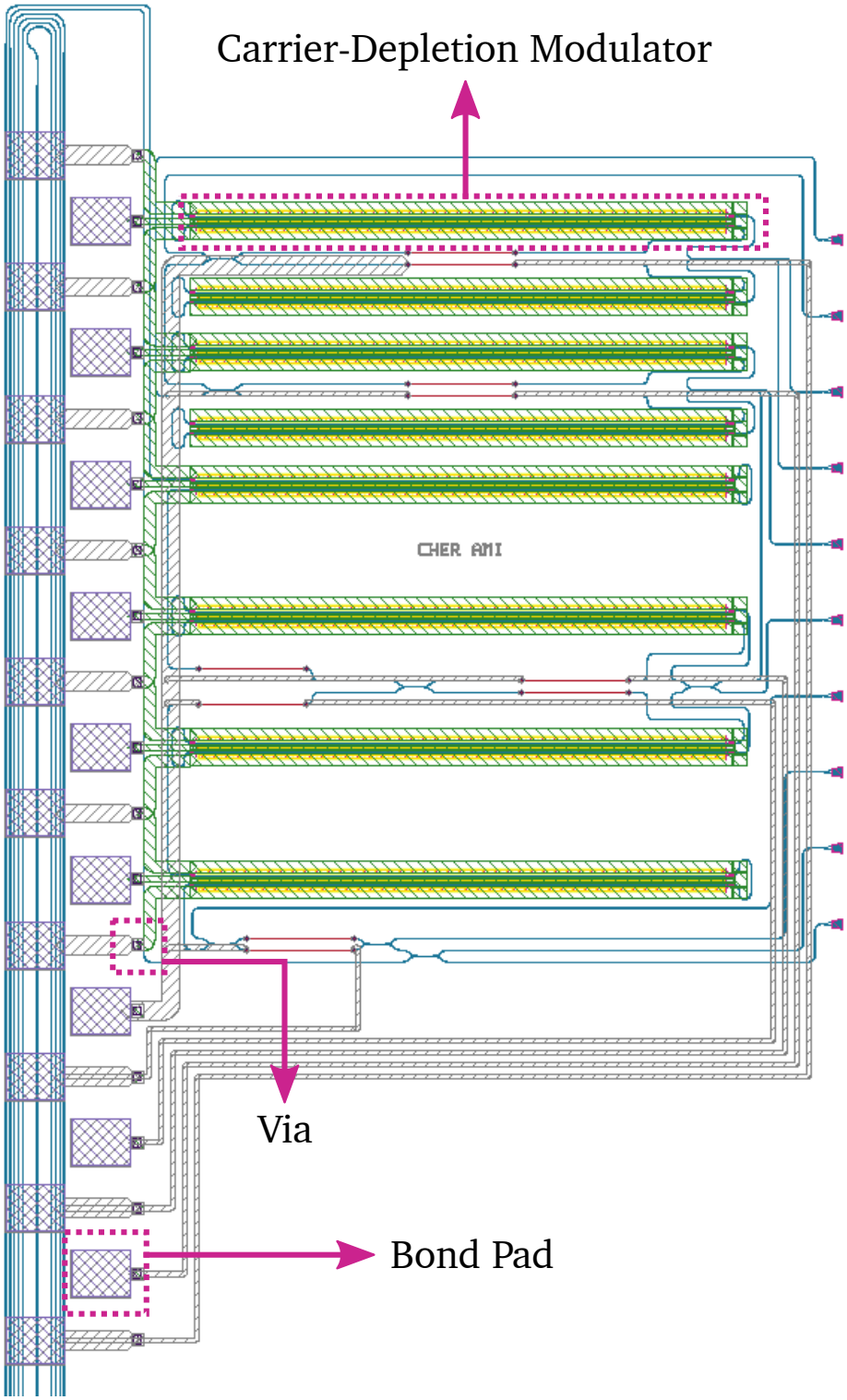


FIGURE 7.39: The mask for Cher Ami, compiled from source code written in Python. Additional annotations are provided in figure 7.41, identifying the components not labelled here.

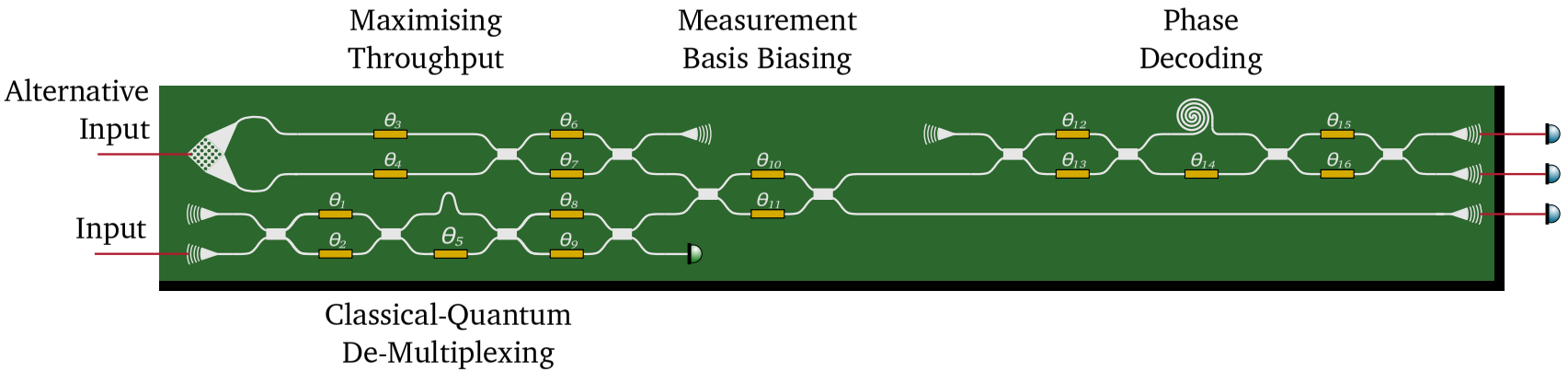


FIGURE 7.40: A schematic for Dzakar, the 1550 nm quantum key distribution chip with clock de-multiplexing or polarisation compensating capabilities. It can be used to implement the BB84 with decoy states, Differential Phase Shift or Coherent One Way protocols.

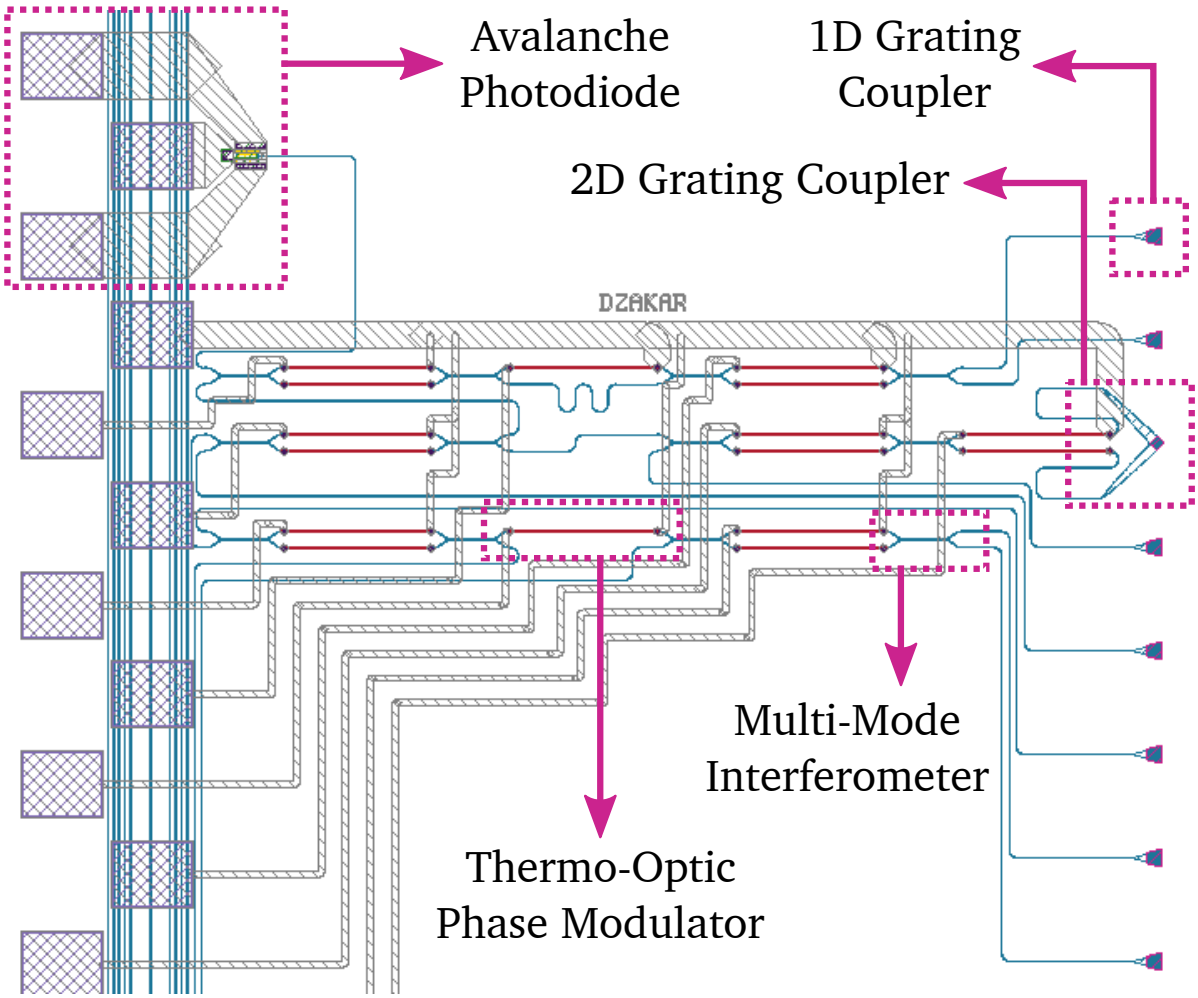


FIGURE 7.41: The mask for Dzakar, compiled from source code written in Python. Additional annotations are provided in figure 7.39, identifying the components not labelled here.

were the optimal wavelengths for each signal and, based on this, a colleague was able to double the secret key rate in a two-channel WDM experiment.

Moving forward, we must demonstrate that the same results can be obtained with a fully monolithic transmitter, and show that the key rate continues to scale linearly when moving from two channels to four. A receiver containing concatenated AMZIs that de-multiplex into four Bobs has been electrically and optically packaged. This is the first QKD chip that no longer needs to be mounted on a chip rig composed of alignment stages and an optical table. Along with the TOPM driving electronics, it is now housed in a 3D-printed router-sized box ($18.5 \times 16.0 \times 4.0$ cm^3). We have conducted extensive electrical tests, and preliminary characterisation of the optics indicates that they should be able to provide the functionality required,

A single transmitter has been packaged to test the photonic components that have become available from Oclaro since the previous fabrication run. A modular copper block was designed, allowing access to other experiments on the same physical chip by substituting out the PCB. The PCB itself has been miniaturised, with a footprint that is 15.5% the size of its predecessor. However, it will be essential that we transition to a multi-tiered PCB for the quadruple-Alice version, as it is not possible to achieve the electrical pad spacing that would otherwise be required.

Finally, four next-generation masks have been designed on Si. These advance the state-of-the-art in multiple ways, using on-chip (de-)multiplexing to combine QKD with classical signals, and exploring the use of 1310 nm light in chip-based quantum communications. The most impressive design is that for an RFI-QKD transmitter chip, which is by far the most complex QKD circuit implemented to date. As these have now returned from the foundry, they can begin to be packaged in parallel with the monolithic WDM-QKD experimental work that is still ongoing.

CHAPTER 8

CONCLUSION

It is now 35 years since the first quantum key distribution (QKD) protocol was proposed by Bennett and Brassard, and 23 years since the publication of Shor's algorithm in its definitive form. Yet quantum cryptography still has not been widely adopted. In part, this is because the road to maturity is far from simple when considering highly-advanced technologies. However, equally significant is the time taken for public concern to be raised over everyday practices that will eventually become a source of catastrophe. Even now, many laymen are not fully aware of the degree to which their entire lives depend on being able to implement strong cryptography, and this lack of public education makes QKD a hard sell to the everyday consumer. Nonetheless, attitudes are starting to change, as national and supranational governments have established a wide range of quantum technology initiatives, and companies are beginning to ask what can be done to keep their data safe from quantum attacks.

Thus, we find ourselves in a position where it must be demonstrated that QKD is a robust and scalable technology, capable of being integrated with generic communications networks that were not designed with quantum devices in mind. To do so is of the highest priority, as the National Institute of Standards and Technology (NIST) post-quantum cryptography competition is now well underway [356], meaning QKD risks becoming obsolete if it does not keep pace with, and demonstrate complementarity to, what some would perceive to be a rival solution.

With this in mind, the work presented herein advances the state of the technology in several ways. We have carried out the first demonstration of time-division multiple access QKD, and pioneered its experimental integration in software-defined networks, reducing the need for radical changes to be made to pre-established architectures when incorporating quantum devices, thereby increasing ease of adoption. In addition, we have quantified the intuition that, for everyday quantum-safe networks, contemporary ciphers will continue to dominate indefinitely, and so optimising QKD systems for use with the one-time pad should not be a primary concern.

Based on this, we have developed a novel QKD protocol that resists two-photon number splitting, has 100% sifting efficiency and, most importantly, detects a newly-identified denial of service (DoS) attack, to which all other protocols are vulnerable. While DoS was discussed in the context of an eavesdropper who had access to an illegitimate QKD unit, the same result can be achieved even if she does not possess any quantum hardware. For example, Eve may spoof Bob's IP address and inject additional messages on the classical channel, that do not interfere with the sifting or error correction, but still cause the authentication step to fail. In principle, a single extra bit is all that would be required to DoS the system. However, BB84-AES will not only detect this as soon as it occurs, but will also be able to identify exactly which bits were sent by an eavesdropper. The trade-off is that we relax the security of QKD to that of our encryption scheme, and while we shall not reiterate our arguments in favour of such a decision, anyone still uncomfortable with the idea should consider the following. There is little point in developing a mathematically-unbreakable cryptosystem that cannot be used, and so it is far better to create a computationally-secure cryptosystem that can be.

We also implemented the first hybrid quantum/post-quantum prototype network, taking symmetric keys distributed under mathematical assumptions and converting them into keys that are guaranteed to be quantum-safe. The software that was developed can also be used to introduce compatibility between QKD links and legacy devices, as well as circumvent the distance limitation on quantum signals, by implementing an architecture based on lesser-trusted nodes. Although these are named in reference to the fact that trust is only reduced under the assumptions governing the security of the post-quantum algorithm, there is another reason why, in such a model, third-party trust can never be fully removed. If, as we assume, authentication of the post-quantum keys takes place using a public-key infrastructure, there is always a chance that the certificate authority will go rogue or become compromised. Nevertheless, our approach is still an improvement over using fully trusted nodes, which have a larger physical attack surface because of the sheer number required.

Finally, we have detailed contributions that enabled the first chip-scale demonstration of wavelength-division multiplexing QKD, increasing the secret key rate by a factor of two while maintaining a small footprint. Steps have been taken towards implementing a four-channel version, with monolithic transmitter and receiver chips that have the potential to be repurposed as reconfigurable banks of QKD devices in software-defined networks.

In reflecting upon the above, it seems appropriate to close with two quotes from the well-known cryptographer Bruce Schneier [357]:

> *"One-time pads might be theoretically secure, but in practical terms they are unusable for anything other than specialized niche applications. Today, only crackpots try to build general-use systems based on one-time pads and cryptographers laugh at them*"

> *"I know that quantum key distribution is a potential replacement for public-key cryptography. But come on - does anyone expect a system that requires specialized communications hardware and cables to be useful for anything but niche applications?*"

This thesis agrees with the first quote. Even with quantum key distribution, the one-time pad is not a general-purpose algorithm. However, it disagrees with the second. Chip-scale QKD will ultimately converge with standard transceiver technology to realise software-defined, reconfigurable devices, capable of transmitting both classical and quantum data which, when combined with post-quantum cryptography to overcome distance limitations, is a general-purpose solution to enable internet communications that are safe against quantum cyber attacks. While QKD may not be used for end-to-end security by members of the public, it is still important for protecting the core parts of the networks on which they rely, as well as our critical infrastructure. Yet for this to become a reality, the more controversial aspects of this thesis must be built upon to generate new, mainstream lines of enquiry, and not simply be treated as esoteric offshoots of the noble but impossible quest towards a cryptosystem that cannot be compromised.

BIBLIOGRAPHY

[1] A. Kandala, A. Mezzacapo, K. Temme, M. Takita, M. Brink, J. M. Chow, and J. M. Gambetta, "Hardware-Efficient Variational Quantum Eigensolver for Small Molecules and Quantum Magnets," *Nature*, vol. 549, pp. 242–246, 2017.

[2] Y. Nam, J.-S. Chen, N. C. Pisenti, K. Wright, C. Delaney, D. Maslov, K. R. Brown, S. Allen, J. M. Amini, J. Apisdorf, K. M. Beck, A. Blinov, V. Chaplin, M. Chmielewski, C. Collins, S. Debnath, A. M. Ducore, K. M. Hudek, M. Keesan, S. M. Kreikemeier, J. Mizrahi, P. Solomon, M. Williams, J. D. Wong-Campos, C. Monroe, and J. Kim, "Ground-State Energy Estimation of the Water Molecule on a Trapped Ion Quantum Computer," *arXiv:1902.10171 [quant-ph]*, 2019.

[3] P. Wittek, "Quantum Machine Learning: What Quantum Computing Means to Data Mining," *Academic Press*, 2014.

[4] J. C. Adcock, E. Allen, M. Day, S. Frick, J. Hinchliff, M. Johnson, S. Morley-Short, S. Pallister, A. B. Price, and S. Stanisic, "Advances in Quantum Machine Learning," *arXiv:1512.02900 [quant-ph]*, 2015.

[5] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, "Quantum Machine Learning," *Nature*, vol. 549, pp. 195–202, 2017.

[6] J. D. Fernandez and A. E. Fernandez, "SCADA systems: Vulnerabilities and Remediation," *Journal of Computing Sciences in Colleges*, vol. 20, no. 4, pp. 160–168, 2005.

[7] A. B. Price, J. G. Rarity, and C. Erven, "Quantum Key Distribution Without Sifting," *7th International Conference on Quantum Cryptography (QCRYPT)*, 2017.

[8] A. B. Price, J. G. Rarity, and C. Erven, "A Quantum Key Distribution Protocol for Rapid Denial of Service Detection," *arXiv:1707.03331 [quant-ph]*, 2017.

[9] A. B. Price, A. Aguado, E. Hugues-Salas, P. A. Haigh, P. Sibson, J. Marhuenda, J. Kennard, J. G. Rarity, M. G. Thompson, R. Nejabati, D. Simeonidou, and C. Erven, "Scalable Quantum Key Distribution on Software Defined Networks," *4th Bristol Quantum Information Technologies Workshop (BQIT)*, 2017.

[10] D. Kahn, "The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet," *Scribner*, 1996.

[11] F. Miller, "Telegraphic Code to Insure Privacy and Secrecy in the Transmission of Telegrams," *Charles M. Cornwell*, 1882.

[12] G. S. Vernam (inventor) and American Telephone and Telegraph Company (assignee), "Secret Signaling System," United States Patent 1310719, 1919.

[13] C. E. Shannon, "Communication Theory of Secrecy Systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[14] NIST, "Specification for the Advanced Encryption Standard (AES)," *Federal Information Processing Standards Publication 197*, 2001.

[15] W. Diffie and M. E. Hellman, "Privacy and Authentication: An Introduction to Cryptography," *Proceedings of the IEEE*, vol. 67, no. 3, pp. 397–427, 1979.

[16] M. Dworkin, "NIST SP 800-38A. Recommendation for Block Cipher Modes of Operation," *National Institute of Standards and Technology*, 2001.

[17] D. A. McGrew and J. Viega, "The Galois/Counter Mode of Operation (GCM)," Submission to *NIST Modes of Operation Process*, 2004.

[18] M. Dworkin, "NIST SP 800-38D. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC," *National Institute of Standards and Technology*, 2007.

[19] M. N. Wegman and J. L. Carter, "New Hash Functions and Their Use in Authentication and Set Equality," *Journal of Computer and System Sciences*, vol. 22, pp. 265–279, 1981.

[20] J. L. Carter and M. N. Wegman, "Universal Classes of Hash Functions," *Journal of Computer and System Sciences*, vol. 18, no. 2, pp. 143–154, 1979.

[21] D. J. Bernstein, "The Poly1305-AES Message-Authentication Code," in *Fast Software Encryption. FSE 2005. Lecture Notes in Computer Science* (H. Gilbert and H. Handschuh, eds.), vol. 3557, pp. 32–49, Springer, 2005.

[22] M. Atici and D. R. Stinson, "Universal Hashing and Multiple Authentication," in *Advances in Cryptology – CRYPTO '96. Lecture Notes in Computer Science* (N. Koblitz, ed.), vol. 1109, pp. 16–30, Springer, 1996.

[23] A. Abidin, "On Security of Universal Hash Function Based Multiple Authentication," in *Information and Communications Security. Lecture Notes in Computer Science* (T. W. Chim and T. H. Yuen, eds.), vol. 7618, pp. 303–310, Springer, 2012.

[24] J. H. Ellis, "The Possibility of Secure Non-Secret Digital Encryption," Research Report No. 3006, *Communications-Electronic Security Group (CESG), part of the Government Communications Headquarters (GCHQ)*, 1970.

[25] R. C. Merkle, "Secure Communications Over Insecure Channels," *Communications of the ACM*, vol. 21, no. 4, pp. 294–299, 1978.

[26] W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[27] M. J. Williamson, "Non-Secret Encryption Using a Finite Field," Internal Paper, *Communications-Electronic Security Group (CESG), part of the Government Communications Headquarters (GCHQ)*, 1974.

[28] E. Barker, L. Chen, A. Roginsky, A. Vassilev, and R. Davis, "NIST SP 800-56A. Revision 3. Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography," *National Institute of Standards and Technology*, 2018.

[29] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, "Handbook of Applied Cryptography," *CRC Press*, 1997.

[30] C. C. Cocks, "A Note on 'Non-Secret Encryption'," Internal Paper, *Communications-Electronic Security Group (CESG), part of the Government Communications Headquarters (GCHQ)*, 1973.

[31] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[32] M. Agrawal, N. Kayal, and N. Saxena, "PRIMES is in P," *Annals of Mathematics*, vol. 160, no. 2, pp. 781–793, 2004.

[33] J. Randall, B. Kaliski, J. Brainard, and S. Turner, "Use of the RSA-KEM Key Transport Algorithm in the Cryptographic Message Syntax (CMS)," *Internet Engineering Task Force. RFC:5990*, 2010.

[34] K. Moriarty and B. Kaliski and J. Jonsson and A. Rusch, "PKCS #1: RSA Cryptography Specifications Version 2.2," *Internet Engineering Task Force. RFC:8017*, 2016.

[35] M. Bellare and P. Rogaway, "Optimal Asymmetric Encryption," in *Advances in Cryptology – EUROCRYPT '94. Lecture Notes in Computer Science* (A. De Santis, ed.), vol. 950, pp. 92–111, Springer, 1995.

[36] J. J. Sakurai, "Modern Quantum Mechanics," Revised Edition, *Addison Wesley*, 1993.

[37] M. A. Nielsen and I. L. Chuang, "Quantum Computation and Quantum Information," 10th Anniversary Edition, *Cambridge University Press*, 2010.

[38] H. P. Yuen, "Amplification of Quantum States and Noiseless Photon Amplifiers," *Physics Letters A*, vol. 113, no. 8, pp. 405–407, 1986.

[39] W. K. Wootters and W. H. Zurek, "A Single Quantum Cannot be Cloned," *Nature*, vol. 299, pp. 802–803, 1982.

[40] D. Dieks, "Communication by EPR Devices," *Physics Letters*, vol. 92A, no. 6, pp. 271–272, 1982.

[41] H. Fan, Y.-N. Wang, L. Jing, J.-D. Yue, H.-D. Shi, Y.-L. Zhang, and L.-Z. Mu, "Quantum Cloning Machines and the Applications," *Physics Reports*, vol. 544, no. 3, pp. 241–322, 2014.

[42] B. Huttner, A. Muller, J. D. Gautier, H. Zbinden, and N. Gisin, "Unambiguous Quantum Measurement of Nonorthogonal States," *Physical Review A*, vol. 54, no. 5, pp. 3783–3789, 1996.

[43] S. J. van Enk, "Unambiguous State Discrimination of Coherent States with Linear Optics: Application to Quantum Cryptography," *Physical Review A*, vol. 66, no. 4, p. 042313, 2002.

[44] Y.-L. Tang, H.-L. Yin, X. Ma, C.-H. F. Fung, Y. Liu, H.-L. Yong, T.-Y. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, "Source Attack of Decoy-State Quantum Key Distribution Using Phase Information," *Physical Review A*, vol. 88, no. 2, p. 022308, 2013.

[45] M. H. Alsuwaiyel, "Algorithms: Design Techniques And Analysis (Revised Edition). Lecture Notes Series on Computing - Vol. 14," *World Scientific*, 2016.

[46] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, "Strengths and Weaknesses of Quantum Computing," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1510–1523, 1997.

[47] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Review*, vol. 41, no. 2, pp. 303–332, 1996.

[48] L. K. Grover, "A Fast Quantum Mechanical Algorithm for Database Search," in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing (STOC '96)* (G. L. Miller, ed.), pp. 212–219, Association for Computing Machinery, 1996.

[49] P. Kim, D. Han, and K. C. Jeong, "Time-Space Complexity of Quantum Search Algorithms in Symmetric Cryptanalysis: Applying to AES and SHA-2," *Quantum Information Processing*, vol. 17, p. 339, 2018.

[50] J. P. Buhler, H. W. Lenstra Jr., and C. Pomerance, "Factoring Integers with the Number Field Sieve," in *The Development of the Number Field Sieve. Lecture Notes in Mathematics* (A. K. Lenstra and H. W. Lenstra Jr., eds.), vol. 1554, pp. 50–94, Springer, 1993.

[51] E. Barker, "NIST SP 800-57 Part 1. Revision 4. Recommendation for Key Management. Part 1: General," *National Institute of Standards and Technology*, 2016.

[52] J. M. Pollard, "Monte Carlo Methods for Index Computation (mod p)," *Mathematics of Computation*, vol. 32, no. 143, pp. 918–924, 1978.

[53] B. Pring, "Exploiting Preprocessing for Quantum Search to Break Parameters for $\mathcal{MQ}$ Cryptosystems," in *Arithmetic of Finite Fields. Lecture Notes in Computer Science* (L. Budaghyan and F. Rodríguez-Henríquez, eds.), vol. 11321, pp. 291–307, Springer, 2018.

[54] M. Roetteler, M. Naehrig, K. M. Svore, and K. Lauter, "Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms," in *Advances in Cryptology – ASIACRYPT 2017. Lecture Notes in Computer Science* (T. Takagi and T. Peyrin, eds.), vol. 10625, pp. 241–270, Springer, 2017.

[55] E. Barker and A. Roginsky, "NIST Special Publication 800-131A. Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths," *National Institute of Standards and Technology*, 2011.

[56] T. Häner, M. Roetteler, and K. M. Svore, "Factoring Using $2n+2$ Qubits with Toffoli Based Modular Multiplication," *Quantum Information and Computation*, vol. 17, no. 7 & 8, pp. 0673–0684, 2017.

[57] A. Bocharov, M. Roetteler, and K. M. Svore, "Factoring with Qutrits: Shor's Algorithm on Ternary and Metaplectic Quantum Architectures," *Physical Review A*, vol. 96, no. 1, p. 012306, 2017.

[58] M. Grassl, B. Langenberg, M. Roetteler, and R. Steinwandt, "Applying Grover's Algorithm to AES: Quantum Resource Estimates," in *Post-Quantum Cryptography. PQCrypto 2016. Lecture Notes in Computer Science* (T. Takagi, ed.), vol. 9606, pp. 29–43, Springer, 2016.

[59] M. Amy, O. Di Matteo, V. Gheorghiu, M. Mosca, A. Parent, and J. Schanck, "Estimating the Cost of Generic Quantum Pre-Image Attacks on SHA-2 and SHA-3," in *Selected Areas in Cryptography - SAC 2016. Lecture Notes in Computer Science* (R. Avanzi and H. Heys, eds.), vol. 10532, pp. 317–337, Springer, 2017.

[60] R. Ramaswami, K. Sivarajan, and G. Sasaki, "Optical Networks: A Practical Perspective," 3rd Edition, *Morgan Kaufmann*, 2009.

[61] C. C. Gerry and P. L. Knight, "Introductory Quantum Optics," *Cambridge University Press*, 2004.

[62] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden, "Pulsed Energy-Time Entangled Twin-Photon Source for Quantum Communication," *Physical Review Letters*, vol. 82, no. 12, pp. 2594–2597, 1999.

[63] H.-W. Li, S. Wang, J.-Z. Huang, W. Chen, Z.-Q. Yin, F.-Y. Li, Z. Zhou, D. Liu, Y. Zhang, G.-C. Guo, W.-S. Bao, and Z.-F. Han, "Attacking a Practical Quantum-Key-Distribution System with Wavelength-Dependent Beam-Splitter and Multiwavelength Sources," *Physical Review A*, vol. 84, no. 6, p. 062308, 2011.

[64] B. C. Sanders, "Review of Entangled Coherent States," *Journal of Physics A: Mathematical and Theoretical*, vol. 45, no. 24, p. 244002, 2012.

[65] C. C. Gerry, J. Mimih, and A. Benmoussa, "Maximally Entangled Coherent States and Strong Violations of Bell-Type Inequalities," *Physical Review A*, vol. 80, no. 2, p. 022111, 2009.

[66] J. Joo, W. J. Munro, and T. P. Spiller, "Quantum Metrology with Entangled Coherent States," *Physical Review Letters*, vol. 107, no. 8, p. 083601, 2011.

[67] H. Chen, X.-B. An, J. Wu, Z.-Q. Yin, S. Wang, W. Chen, and Z.-F. Han, "Hong–Ou–Mandel Interference with Two Independent Weak Coherent States," *Chinese Physics B*, vol. 25, no. 2, p. 020305, 2016.

[68] D. Mayers, "Unconditionally Secure Quantum Bit Commitment is Impossible," *Physical Review Letters*, vol. 78, no. 17, pp. 3414–3417, 1997.

[69] H.-K. Lo and H. F. Chau, "Why Quantum Bit Commitment and Ideal Quantum Coin Tossing are Impossible," *Physica D*, vol. 120, no. 1-2, pp. 177–187, 1998.

[70] G. Brassard, C. Crépeau, D. Mayers, and L. Salvail, "A Brief Review on the Impossibility of Quantum Bit Commitment," *arXiv:quant-ph/9712023*, 1997.

[71] Á. J. Almeida, R. Loura, N. Paunković, N. A. Silva, N. J. Muga, P. Mateus, P. S. André, and A. Nolasco Pinto, "A Brief Review on Quantum Bit Commitment," in *Proceedings of SPIE, Second International Conference on Applications of Optics and Photonics* (M. F. P. C. Martins Costa and R. Nunes Nogueira, eds.), vol. 9286, p. 92861C, SPIE, 2014.

[72] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum Secret Sharing," *Physical Review A*, vol. 59, no. 3, pp. 1829–1834, 1999.

[73] R. Cleve, D. Gottesman, and H.-K. Lo, "How to Share a Quantum Secret," *Physical Review Letters*, vol. 83, no. 3, pp. 648–651, 1999.

[74] D. Gottesman, "Theory of Quantum Secret Sharing," *Physical Review A*, vol. 61, no. 4, p. 042311, 2000.

[75] D. Gottesman and I. Chuang, "Quantum Digital Signatures," *arXiv:quant-ph/0105032*, 2001.

[76] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, vol. 1, pp. 175–179, IEEE, 1984.

[77] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental Quantum Cryptography," *Journal of Cryptology*, vol. 5, no. 1, pp. 3–28, 1992.

[78] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations," *Physical Review Letters*, vol. 92, no. 5, p. 057901, 2004.

[79] H.-K. Lo, X. Ma, and K. Chen, "Decoy State Quantum Key Distribution," *Physical Review Letters*, vol. 94, no. 23, p. 230504, 2005.

[80] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, "Simulation and Implementation of Decoy State Quantum Key Distribution over 60km Telecom Fiber," in *2006 IEEE International Symposium on Information Theory*, pp. 2094–2098, IEEE, 2006.

[81] W.-Y. Hwang, "Quantum Key Distribution with High Loss: Toward Global Secure Communication," *Physical Review Letters*, vol. 91, no. 5, p. 057901, 2003.

[82] H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient Quantum Key Distribution Scheme and a Proof of its Unconditional Security," *Journal of Cryptology*, vol. 18, no. 2, pp. 133–165, 2005.

[83] C. Erven, X. Ma, R. Laflamme, and G. Weihs, "Entangled Quantum Key Distribution with a Biased Basis Choice," *New Journal of Physics*, vol. 11, no. 4, p. 045025, 2009.

[84] Y. Cao, H. Liang, J. Yin, H.-L. Yong, F. Zhou, Y.-P. Wu, J.-G. Ren, Y.-H. Li, G.-S. Pan, T. Yang, X. Ma, C.-Z. Peng, and J.-W. Pan, "Entanglement-Based Quantum Key Distribution with Biased Basis Choice via Free Space," *Optics Express*, vol. 21, no. 22, pp. 27260–27268, 2013.

[85] Z. Wei, W. Wang, Z. Zhang, M. Gao, Z. Ma, and X. Ma, "Decoy-State Quantum Key Distribution with Biased Basis Choice," *Scientific Reports*, vol. 3, p. 2453, 2013.

[86] P. W. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Physical Review Letters*, vol. 85, no. 2, pp. 441–444, 2000.

[87] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The Security of Practical Quantum Key Distribution," *Reviews of Modern Physics*, vol. 81, no. 3, pp. 1301–1350, 2009.

[88] N. Lütkenhaus, "Estimates for Practical Quantum Cryptography," *Physical Review A*, vol. 59, no. 5, pp. 3301–3319, 1999.

[89] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of Quantum Key Distribution with Imperfect Devices," *Quantum Information and Computation*, vol. 4, no. 5, pp. 325–360, 2004.

[90] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, "Loophole-Free Bell Inequality Violation Using Electron Spins Separated by 1.3 Kilometres," *Nature*, vol. 526, pp. 682–686, 2015.

[91] D. Bohm, "A Suggested Interpretation of the Quantum Theory in Terms of "Hidden" Variables. I," *Physical Review*, vol. 85, no. 2, pp. 166–179, 1952.

[92] D. Bohm, "A Suggested Interpretation of the Quantum Theory in Terms of "Hidden" Variables. II," *Physical Review*, vol. 85, no. 2, pp. 180–193, 1952.

[93] D. J. Bernstein, "Is the Security of Quantum Cryptography Guaranteed by the Laws of Physics?," *arXiv:1803.04520 [quant-ph]*, 2018.

[94] "Law," in *Chambers 21st Century Dictionary* (M. Robinson and G. W. Davidson, eds.), Chambers, 1999.

[95] "Physical Law," in *McGraw-Hill Concise Encyclopedia of Science and Technology*, *6th Edition,* McGraw-Hill Publishing Company, 2009.

[96] Communications-Electronic Security Group (CESG), part of the Government Communications Headquarters (GCHQ), "Quantum Key Distribution," White Paper, 2016.

[97] A. Aguado, E. Hugues-Salas, P. A. Haigh, J. Marhuenda, A. B. Price, P. Sibson, J. Kennard, C. Erven, J. G. Rarity, M. G. Thompson, A. Lord, R. Nejabati, and D. Simeonidou, "First Experimental Demonstration of Secure NFV Orchestration over an SDN-Controlled Optical Network with Time-Shared Quantum Key Distribution Resources," in *Proceedings of 42nd European Conference on Optical Communication (ECOC)*, pp. 512–514, VDE, 2016.

[98] A. Aguado, E. Hugues-Salas, P. A. Haigh, J. Marhuenda, A. B. Price, P. Sibson, J. Kennard, C. Erven, J. G. Rarity, M. G. Thompson, A. Lord, R. Nejabati, and D. Simeonidou, "Secure NFV Orchestration Over an SDN-Controlled Optical Network with Time-Shared Quantum

Key Distribution Resources," *Journal of Lightwave Technology*, vol. 35, no. 8, pp. 1357–1362, 2017.

[99] A. B. Price, A. Aguado, E. Hugues-Salas, P. A. Haigh, P. Sibson, J. Marhuenda, J. Kennard, J. G. Rarity, M. G. Thompson, R. Nejabati, D. Simeonidou, and C. Erven, "Towards the Deployment of Quantum Key Distribution Systems in a Software Defined Networking Environment," *6th International Conference on Quantum Cryptography (QCRYPT)*, 2016.

[100] A. B. Price, A. Aguado, E. Hugues-Salas, P. A. Haigh, P. Sibson, J. Marhuenda, J. Kennard, J. G. Rarity, M. G. Thompson, R. Nejabati, D. Simeonidou, and C. Erven, "Practical Integration of Quantum Key Distribution with Next-Generation Networks," *2nd International Conference for Young Quantum Information Scientists (YQIS)*, 2016.

[101] T. S. Humble and R. J. Sadlier, "Software-Defined Quantum Communication Systems," *Optical Engineering*, vol. 53, no. 8, p. 086103, 2014.

[102] V. R. Dasari, R. J. Sadlier, R. Prout, B. P. Williams, and T. S. Humble, "Programmable Multi-Node Quantum Network Design and Simulation," in *Proceedings of SPIE, Quantum Information and Computation IX* (E. Donkor and M. Hayduk, eds.), vol. 9873, p. 98730B, SPIE, 2016.

[103] Y. Cao, Y. Zhao, C. Colman-Meixner, X. Yu, and J. Zhang, "Key on Demand (KoD) for Software-Defined Optical Networks Secured by Quantum Key Distribution (QKD)," *Optics Express*, vol. 25, no. 22, pp. 26453–26467, 2017.

[104] Y. Cao, Y. Zhao, X. Yu, and Y. Wu, "Resource Assignment Strategy in Optical Networks Integrated with Quantum Key Distribution," *Journal of Optical Communications and Networking*, vol. 9, no. 11, pp. 995–1004, 2017.

[105] V. V. Chistyakov, O. L. Sadov, A. B. Vasiliev, V. I. Egorov, M. V. Kompaniets, P. V. Fedchenkov, O. I. Lazo, A. E. Shevel, N. V. Buldakov, A. V. Gleim, and S. E. Khoruzhnikov, "Software-Defined Subcarrier Wave Quantum Networking Operated by OpenFlow Protocol," *arXiv:1709.09081 [quant-ph]*, 2017.

[106] Y. Peng, C. Wu, B. Zhao, W. Yu, B. Liu, and S. Qiao, "QKDFlow: QKD Based Secure Communication Towards the OpenFlow Interface in SDN," in *Geo-Spatial Knowledge and Intelligence. GRMSE 2016. Communications in Computer and Information Science* (H. Yuan, J. Geng, and F. Bian, eds.), vol. 699, pp. 410–415, Springer, 2017.

[107] M. Seong Im and V. R. Dasari, "Optimization and Synchronization of Programmable Quantum Communication Channels," in *Proceedings of SPIE, Quantum Information Science, Sensing, and Computation X* (E. Donkor and M. Hayduk, eds.), vol. 10660, p. 106600N, SPIE, 2018.

[108] H. Wang, Y. Zhao, Y. Li, X. Yu, J. Zhang, C. Liu, and Q. Shao, "A Flexible Key-Updating Method for Software-Defined Optical Networks Secured by Quantum Key Distribution," *Optical Fibre Technology*, vol. 45, pp. 195–200, 2018.

[109] P. Humberto Saavedra (inventor) and Teloip (assignee), "System, Apparatus and Method for Encrypting Overlay Networks Using Quantum Key Distribution," United States Patent US 2018/0013556 A1, 2017.

[110] C. Su, L. Lu, S. Hu, X. Luo (inventors), and Huawei Technologies (assignee), "Quantum Key Relay Method and Device Based On Centralized Management and Control Network," World Intellectual Property Organisation Patent WO/2018/082345, 2017.

[111] X. Yu, Y. Cao, Y. Zhao, H. Zhang, J. Zhang (inventors), and Beijing University of Posts and Telecommunications (assignee), "Safety Guarantee Method for SDN (Software-Defined Network) Control Channel," China Patent CN 107294960 A, 2017.

[112] J. Zhang, Y. Cao, Y. Zhao, H. Zhang, X. Yu (inventors), and Beijing University of Posts and Telecommunications (assignee), "Quantum Key Distribution Method and System," China Patent CN 106850204 A, 2017.

[113] T. R. Mong, S. F. Bush (inventors), and General Electric (assignee), "Locomotive Control System," United States Patent US 2018/0237040 A1, 2018.

[114] C. Elliott, "The DARPA Quantum Network," *arXiv:quant-ph/0412029*, 2004.

[115] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current Status of the DARPA Quantum Network," *arXiv:quant-ph/0503058*, 2005.

[116] W. Chen, Z.-F. Han, T. Zhang, H. Wen, Z.-Q. Yin, F.-X. Xu, Q.-L. Wu, Y. Liu, Y. Zhang, X.-F. Mo, Y.-Z. Gui, G. Wei, and G.-C. Guo, "Field Experiment on a "Star Type" Metropolitan Quantum Key Distribution Network," *IEEE Photonics Technology Letters*, vol. 21, no. 9, pp. 575–577, 2009.

[117] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, "The SECOQC Quantum Key Distribution Network in Vienna," *New Journal of Physics*, vol. 11, no. 7, p. 075001, 2009.

[118] T.-Y. Chen, H. Liang, Y. Liu, W.-Q. Cai, L. Ju, W.-Y. Liu, J. Wang, H. Yin, K. Chen, Z.-B. Chen, C.-Z. Peng, and J.-W. Pan, "Field Test of a Practical Secure Communication Network with Decoy-State Quantum Cryptography," *Optics Express*, vol. 17, no. 8, pp. 6540–6549, 2009.

[119] T.-Y. Chen, J. Wang, H. Liang, W.-Y. Liu, Y. Liu, X. Jiang, Y. Wang, X. Wan, W.-Q. Cai, L. Ju, L.-K. Chen, L.-J. Wang, Y. Gao, K. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, "Metropolitan All-Pass and Inter-City Quantum Communication Network," *Optics Express*, vol. 18, no. 26, pp. 27217–27225, 2010.

[120] A. Mirza and F. Petruccione, "Realizing Long-Term Quantum Cryptography," *Journal of the Optical Society of America B*, vol. 27, no. 6, pp. A185–A188, 2010.

[121] D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat, J.-B. Page, D. Perroud, G. Ribordy, A. Rochas, S. Robyr, J. Tavares, R. Thew, P. Trinkler, S. Ventura, R. Voirol, N. Walenta, and H. Zbinden, "Long-Term Performance of the SwissQuantum Quantum Key Distribution Network in a Field Environment," *New Journal of Physics*, vol. 13, no. 12, p. 123001, 2011.

[122] F.-X. Xu, W. Chen, S. Wang, Z.-Q. Yin, Y. Zhang, Y. Liu, Z. Zhou, Y.-B. Zhao, H.-W. Li, D. Liu, Z.-F. Han, and G.-C. Guo, "Field Experiment on a Robust Hierarchical Metropolitan Quantum Cryptography Network," *Chinese Science Bulletin*, vol. 54, no. 17, pp. 2991–2997, 2009.

[123] D. Lancho, J. Martinez, D. Elkouss, M. Soto, and V. Martin, "QKD in Standard Optical Telecommunications Networks," in *International Conference on Quantum Comunication and Quantum Networking. QuantumComm 2009. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering* (A. Sergienko, S. Pascazio, and P. Villoresi, eds.), vol. 36, pp. 142–149, Springer, 2009.

[124] A. Ciurana, J. Martínez-Mateo, M. Peev, A. Poppe, N. Walenta, H. Zbinden, and V. Martín, "Quantum Metropolitan Optical Network Based on Wavelength Division Multiplexing," *Optics Express*, vol. 22, no. 2, pp. 1576–1593, 2014.

[125] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, "Field Test of Quantum Key Distribution in the Tokyo QKD Network," *Optics Express*, vol. 19, no. 11, pp. 10387–10409, 2011.

[126] S. Wang, W. Chen, Z.-Q. Yin, H.-W. Li, D.-Y. He, Y.-H. Li, Z. Zhou, X.-T. Song, F.-Y. Li, D. Wang, H. Chen, Y.-G. Han, J.-Z. Huang, J.-F. Guo, P.-L. Hao, M. Li, C.-M. Zhang, D. Liu, W.-Y.

Liang, C.-H. Miao, P. Wu, G.-C. Guo, and Z.-F. Han, "Field and Long-Term Demonstration of a Wide Area Quantum Key Distribution Network," *Optics Express*, vol. 22, no. 18, pp. 21739–21756, 2014.

[127] Battelle, "Battelle Installs First Commercial Quantum Key Distribution Protected Network in U.S.," Press Release, 2013.

[128] Y. Zhao, "QuantumCTek Quantum Secure Communication Networks: Products and Solutions," *4th International Conference on Quantum Cryptography (QCRYPT)*, 2014.

[129] J.-S. Cho, "Quantum Technology for Network Security," *4th ETSI/IQC Workshop on Quantum-Safe Cryptography*, 2016.

[130] B. Cho and J. Kim, "KREONET Optical Network and Quantum Communication Testbed," *9th CEF Networks Workshop*, 2017.

[131] D. Huang, P. Huang, H. Li, T. Wang, Y. Zhou, and G. Zeng, "Field Demonstration of a Continuous-Variable Quantum Key Distribution Network," *Optics Letters*, vol. 41, no. 15, pp. 3511–3514, 2016.

[132] ID Quantique, "KPN Implements End-to-End QKD Connection," Press Release, 2016.

[133] ITMO University, "ITMO University and Kazan Quantum Center Launch the First Multinode Quantum Network in CIS," Press Release, 2017.

[134] E. O. Kiktenko, N. O. Pozhar, A. V. Duplinskiy, A. A. Kanapin, A. S. Sokolov, S. S. Vorobey, A. V. Miller, V. E. Ustimchik, M. N. Anufriev, A. T. Trushechkin, R. R. Yunusov, V. L. Kurochkin, Y. V. Kurochkin, and A. K. Fedorov, "Demonstration of a Quantum Key Distribution Network in Urban Fibre-Optic Communication Lines," *Quantum Electronics*, vol. 47, no. 9, pp. 798–802, 2017.

[135] S. Kwak, "Ongoing Efforts on Development of Quantum Technology by SK Telecom," *7th International Conference on Quantum Cryptography (QCRYPT)*, 2017.

[136] ID Quantique, "ID Quantique & China Quantum Technologies (QTEC) Announce Joint-Venture," Press Release, 2016.

[137] Y. Liu, "Beijing-Shanghai Quantum Communication Network Put into Use," Press Release, *University of Science and Technology of China News Center*, 2017.

[138] Q. Zhang, F. Xu, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, "Large Scale Quantum Key Distribution: Challenges and Solutions," *Optics Express*, vol. 26, no. 18, pp. 24260–24273, 2018.

[139] Chinese Academy of Sciences Headquarters, "China Builds World's First Space-Ground Integrated Quantum Communication Network," Press Release, 2017.

[140] L. Zhao, "Wuhan Launches World-Leading Quantum Network," *China Daily*, 2017.

[141] BT, "Quantum Leap Towards Un-Hackable Networks," Press Release, 2018.

[142] UK National Quantum Technologies Programme, "UK Quantum Technology Hub for Quantum Communication Technologies Annual Report 2015-2016," Research Report, 2016.

[143] Y. Won-Chang, "SK Telecom Speeds Up Development of Quantum Cryptographic Communication Technology," *Business Korea*, 2018.

[144] C. Metz and R. Zhong, "The Race Is On to Protect Data From the Next Leap in Computers. And China Has the Lead," *The New York Times*, 2018.

[145] Quantum Xchange, "Renowned Cryptographer Dr. Whitfield Diffie Joins Quantum Xchange's Advisory Board," Press Release, 2018.

[146] T. E. Chapuran, P. Toliver, N. A. Peters, J. Jackel, M. S. Goodman, R. J. Runser, S. R. McNown, N. Dallmann, R. J. Hughes, K. P. McCabe, J. E. Nordholt, C. G. Peterson, K. T. Tyagi, L. Mercer, and H. Dardy, "Optical Networking for Quantum Key Distribution and Quantum Communications," *New Journal of Physics*, vol. 11, no. 10, p. 105001, 2009.

[147] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, "Entanglement-Based Quantum Communication Over 144 km," *Nature Physics*, vol. 3, pp. 481–486, 2007.

[148] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, G.-B. Li, Q.-M. Lu, Y.-H. Gong, Y. Xu, S.-L. Li, F.-Z. Li, Y.-Y. Yin, Z.-Q. Jiang, M. Li, J.-J. Jia, G. Ren, D. He, Y.-L. Zhou, X.-X. Zhang, N. Wang, X. Chang, Z.-C. Zhu, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-Based Entanglement Distribution Over 1200 Kilometers," *Science*, vol. 356, no. 6343, pp. 1140–1144, 2017.

[149] F. Hu, Q. Hao, and K. Bao, "A Survey on Software-Defined Network and OpenFlow: From Concept to Implementation," *IEEE Communication Surveys & Tutorials*, vol. 16, no. 4, pp. 2181–2206, 2014.

[150] M. A. Bakke, E. J. Fiore (inventors), and Storage Technology Corporation (assignee), "Method and Apparatus for Accelerated Packet Forwarding," United States Patent US 5,566,170, 1996.

[151] K. Benzekki, A. El Fergougui, and A. Elbelrhiti Elalaoui, "Software-Defined Networking (SDN): A Survey," *Security and Communication Networks*, vol. 9, no. 18, pp. 5803–5833, 2016.

[152] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "OpenFlow: Enabling Innovation in Campus Networks," *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 2, pp. 69–74, 2008.

[153] Telehouse, "Global Data Center Solutions," Corporate Brochure, 2016.

[154] University of Cambridge, "Cambridge Launches UK's First Quantum Network," Press Release, 2018.

[155] National Physical Laboratory, "UK Launches World's First Commercial-Grade Quantum Communications Testing Link," Press Release, 2019.

[156] ID Quantique, "Quantum Key Distribution System Clavis2 User Guide (v 3.0)," Product Manual, 2013.

[157] ID Quantique, "Clavis^2 The Most Versatile Quantum Key Distribution Research Platform," Datasheet, 2014.

[158] A. Vakhitov, V. Makarov, and D. R. Hjelme, "Large Pulse Attack as a Method of Conventional Optical Eavesdropping in Quantum Cryptography," *Journal of Modern Optics*, vol. 48, no. 13, pp. 2023–2038, 2001.

[159] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, "Trojan-Horse Attacks on Quantum-Key-Distribution Systems," *Physical Review A*, vol. 73, no. 2, p. 022320, 2006.

[160] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, "Trojan-Horse Attacks Threaten the Security of Practical Quantum Cryptography," *New Journal of Physics*, vol. 16, no. 12, p. 123030, 2014.

[161] Cisco Systems, "Calculating the Maximum Attenuation for Optical Fiber Links," Technical Note 27042, 2006.

[162] Polatis, "Series 1000," Datasheet, 2009.

[163] Jenco Technologies, "Polatis Overview Rev. 1," White Paper, 2013.

[164] Small Form Factor Committee, "Specification for SFP+ 10 Gb/s and Low Speed Electrical Interface, Rev 4.1," *Storage Networking Industry Association. SFF-8431*, 2009.

[165] IEEE Computer Society, "802.3ae. IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements. Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications. Amendment 1: Media Access Control (MAC) Parameters, Physical Layers, and Management Parameters for 10 Gb/s Operation," *IEEE. Std 802.3ae-2002*, 2002.

[166] Small Form Factor Committee, "Specification for QSFP+ 4X 10 Gb/s Pluggable Transceiver, Rev 4.9," *Storage Networking Industry Association. SFF-8436*, 2018.

[167] B. H. Bransden and C. J. Joachain, "Physics of Atoms and Molecules," 2nd Edition, *Pearson*, 2003.

[168] Y. Huang, M. Mortier, and F. Auzel, "Stark Levels Analysis for Er^{3+}-Doped Oxide Glasses: Germanate and Silicate," *Optical Materials*, vol. 15, no. 4, pp. 243–260, 2001.

[169] T. J. Xia, D. Z. Chen, G. A. Wellbrock, A. Zavriyev, A. C. Beal, and K. M. Lee, "In-Band Quantum Key Distribution (QKD) on Fiber Populated by High-Speed Classical Data Channels," in *Optical Fiber Communication Conference and Exposition and The National Fiber Optic Engineers Conference, Techical Digest*, Optical Society of America, 2006.

[170] N. A. Peters, P. Toliver, T. E. Chapuran, R. J. Runser, S. R. McNown, C. G. Peterson, D. Rosenberg, N. Dallmann, R. J. Hughes, and K. P. McCabe, "Dense Wavelength Multiplexing of 1550 nm QKD with Strong Classical Channels in Reconfigurable Networking Environments," *New Journal of Physics*, vol. 11, no. 4, p. 045012, 2009.

[171] P. Eraerds, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, "Quantum Key Distribution and 1 Gbps Data Encryption Over a Single Fibre," *New Journal of Physics*, vol. 12, no. 6, p. 063027, 2010.

[172] R. Paschotta, "Amplified Spontaneous Emission," in *Encyclopedia of Laser Physics and Technology*, Wiley-VCH, 2008.

[173] R. J. Runser, T. Chapuran, P. Toliver, N. A. Peters, M. S. Goodman, J. T. Kosloski, N. Nweke, S. R. McNown, R. J. Hughes, D. Rosenberg, C. G. Peterson, K. P. McCabe, J. E. Nordholt, K. Tyagi, P. A. Hiskett, and N. Dallmann, "Progress Toward Quantum Communications Networks: Opportunities and Challenges," in *Proceedings of SPIE, Optoelectronic Integrated Circuits IX* (L. A. Eldada and E.-H. Lee, eds.), vol. 6476, p. 64760I, SPIE, 2007.

[174] Finisar, "Product Guide: WaveShaper® Series A Family of Programmable Optical Processors," Datasheet, 2016.

[175] G. Miao, J. Zander, K. W. Sung, and S. Ben Slimane, "Fundamentals of Mobile Data Networks," *Cambridge University Press*, 2016.

[176] International Telecommunication Union, "Series G: Transmission Systems and Media, Digital Systems and Networks. Access Networks - In Premises Networks. Unified High-Speed Wireline-Based Home Networking Transceivers - Data Link Layer Specification," *Recommendation ITU-T G.9961*, 2015.

[177] M. Chiosi, D. Clarke, P. Willis, A. Reid, J. Feger, M. Bugenhagen, W. Khan, M. el Fargano, C. Cui, H. Deng, J. Benitez, U. Michel, H. Damker, K. Ogaki, T. Matsuzaki, M. Fukui, K. Shimano, D. Delisle, Q. Loudier, C. Kolias, I. Guardini, E. Demaria, R. Minerva, A. Manzalini, D. López, F. J. Ramón Salguero, F. Ruhl, and P. Sen, "Network Functions Virtualisation: An Introduction, Benefits, Enablers, Challenges & Call for Action," White Paper*, ETSI*, 2012.

[178] B. Boughzala, R. B. Ali, M. Lemay, Y. Lemieux, and O. Cherkaoui, "OpenFlow Supporting Inter-Domain Virtual Machine Migration," in *2011 Eighth International Conference on Wireless and Optical Communications Networks*, pp. 1–7, IEEE, 2011.

[179] Cisco Systems, "Data Center High Availability Clusters Design Guide," Technical Design Guide, 2006.

[180] Polatis, "Series 6000n: Network Optical Matrix Switch," Datasheet, 2013.

[181] ID Quantique, "Key Request Protocol IDQ3P," White Paper, 2014.

[182] Digital Equipment Corporation, Intel Corporation, and Xerox Corporation, "The Ethernet: A Local Area Network. Data Link Layer and Physical Layer Specifications," 1982.

[183] H.-K. Lo, M. Curty, and K. Tamaki, "Secure Quantum Key Distribution," *Nature Photonics*, vol. 8, pp. 595–604, 2014.

[184] D. G. Boak, "A History of U.S. Communications Security (Volumes I and II); The David G. Boak Lectures (2015 Declassification)," *National Security Agency (NSA)*, 1973.

[185] R. Alléaume, C. Branciard, J. Bouda, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, N. Lütkenhaus, C. Monyk, P. Painchault, M. Peev, A. Poppe, T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A.Shields, H. Weinfurter, and A. Zeilinger, "Using Quantum Key Distribution for Cryptographic Purposes: A Survey," *Theoretical Computer Science*, vol. 560, no. 1, pp. 62–81, 2014.

[186] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical Challenges in Quantum Key Distribution," *npj Quantum Information*, vol. 2, p. 16025, 2016.

[187] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, "Continuous-Variable Quantum Key Distribution with Gaussian Modulation — The Theory of Practical Implementations," *Advanced Quantum Technologies*, p. 1800011, Early View Version, 2018.

[188] H. Bechmann-Pasquinucci and W. Tittel, "Quantum Cryptography Using Larger Alphabets," *Physical Review A*, vol. 61, no. 6, p. 062308, 2000.

[189] H. Bechmann-Pasquinucci and A. Peres, "Quantum Cryptography with 3-State Systems," *Physical Review Letters*, vol. 85, no. 15, pp. 3313–3316, 2000.

[190] Q. Zhuang, Z. Zhang, J. Dove, F. N. C. Wong, and J. H. Shapiro, "Floodlight Quantum Key Distribution: A Practical Route to Gigabit-per-Second Secret-Key Rates," *Physical Review A*, vol. 94, no. 1, p. 012322, 2016.

[191] Z. Zhang, Q. Zhuang, F. N. C. Wong, and J. H. Shapiro, "Floodlight Quantum Key Distribution: Demonstrating a Framework For High-Rate Secure Communication," *Physical Review A*, vol. 95, no. 1, p. 012332, 2017.

[192] X. Ma, "Unconditional Security at a Low Cost," *Physical Review A*, vol. 74, no. 5, p. 052325, 2006.

[193] V. Scarani and R. Renner, "Quantum Cryptography with Finite Resources: Unconditional Security Bound for Discrete-Variable Protocols with One-Way Postprocessing," *Physical Review Letters*, vol. 100, no. 20, p. 200501, 2008.

[194] Information Sciences Institute, "Transmission Control Protocol. DARPA Internet Program Protocol Specification," *Internet Engineering Task Force. RFC:793*, 1981.

[195] Information Sciences Institute, "Internet Protocol. DARPA Internet Program Protocol Specification," *Internet Engineering Task Force. RFC:791*, 1981.

[196] S. E. Deering and R. M. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," *Network Working Group, The Internet Society*, 1998.

[197] J. Postel, "The TCP Maximum Segment Size and Related Topics," *Internet Engineering Task Force. RFC:879*, 1981.

[198] Smart Payment Association, "An Overview of Contactless Payment Benefits and Worldwide Deployments," White Paper, 2016.

[199] T. P. Diakos, J. A. Briffa, T. W. C. Brown, and S. Wesemeyer, "Eavesdropping Near-Field Contactless Payments: A Quantitative Analysis," *The Journal of Engineering*, vol. 2013, no. 10, pp. 48–54, 2013.

[200] J. Vila and R. J. Rodríguez, "Relay Attacks in EMV Contactless Cards with Android OTS Devices," *6th Annual Hack in the Box Security Conference*, 2015.

[201] J. Ervin, "Which? Reveals Contactless Card Flaw," Press Release*, Which?*, 2015.

[202] C. E. Shannon, "A Mathematical Theory of Communication," *The Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423 and 623–656, 1948.

[203] H. Frazier, "The 802.3z Gigabit Ethernet Standard," *IEEE Network*, vol. 12, no. 3, pp. 6–7, 1998.

[204] IEEE Computer Society, "IEEE Standard for Ethernet," *IEEE. Std 802.3-2015*, 2015.

[205] IEEE Computer Society, "IEEE Standard for Ethernet. Amendment 10: Media Access Control Parameters, Physical Layers, and Management Parameters for 200 Gb/s and 400 Gb/s Operation," *IEEE. Std 802.3bs-2017*, 2017.

[206] H. Zbinden, J. D. Gautier, N. Gisin, B. Huttner, A. Muller, and W. Tittel, "Interferometry with Faraday Mirrors for Quantum Cryptography," *Electronics Letters*, vol. 33, no. 7, pp. 586–588, 1997.

[207] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum Key Distribution Over 67 km with a Plug&play System," *New Journal of Physics*, vol. 4, no. 41, pp. 41.1–41.8, 2002.

[208] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. Sharpe, and A. J. Shields, "Gigahertz Decoy Quantum Key Distribution with 1 Mbit/s Secure Key Rate," *Optics Express*, vol. 16, no. 23, pp. 18790–18797, 2008.

[209] Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. W. Sharpe, A. R. Dixon, E. Lavelle, J. F. Dynes, A. Murakami, M. Kujiraoka, M. Lucamarini, Y. Tanizawa, H. Sato, and A. J. Shields, "10-Mb/s Quantum Key Distribution," *Journal of Lightwave Technology*, vol. 36, no. 16, pp. 3427–3433, 2018.

[210] Alcatel-Lucent, "Alcatel-Lucent Reports Q2 2014 Results," Press Release, 2014.

[211] M.-F. Huang, A. Tanaka, E. Ip, Y.-K. Huang, D. Qian, Y. Zhang, S. Zhang, P. N. Ji, I. B. Djordjevic, T. Wang, Y. Aono, S. Murakami, T. Tajima, T. J. Xia, and G. A. Wellbrock, "Terabit/s Nyquist Superchannels in High Capacity Fiber Field Trials Using DP-16QAM and DP-8QAM Modulation Formats," *Optics Express*, vol. 23, no. 13, pp. 17511–17519, 2015.

[212] H. Hu, F. D. Ros, M. Pu, F. Ye, K. Ingerslev, E. P. da Silva, M. Nooruzzaman, Y. Amma, Y. Sasaki, T. Mizuno, Y. Miyamoto, L. Ottaviano, E. Semenova, P. Guan, D. Zibar, M. Galili, K. Yvind, T. Morioka, and L. K. Oxenløwe, "Single-Source Chip-Based Frequency Comb Enabling Extreme Parallel Data Transmission," *Nature Photonics*, vol. 12, pp. 469–473, 2018.

[213] Akamai Technologies, "State of the Internet/Connectivity Reports," Data Files, 2007-2017. [Last Accessed: 04/10/17, Archived Source: `https://web.archive.org/web/20171004045051/https://www.akamai.com/us/en/about/our-thinking/state-of-the-internet-report/global-state-of-the-internet-connectivity-reports.jsp`].

[214] M-Lab and Cable, "Worldwide Broadband Speed League 2018," Data File, 2017-2018. [Last Accessed: 16/09/18, Archived Source: `https://web.archive.org/web/20180916140815/https://www.cable.co.uk/broadband/research/worldwide-broadband-speed-league-2018/`].

[215] M-Lab and Cable, "Worldwide Broadband Speed League 2018 Methodology," White Paper, 2018. [Last Accessed: 16/09/18, Archived Source: `https://web.archive.org/web/20180916140815/https://www.cable.co.uk/broadband/research/worldwide-broadband-speed-league-2018/`].

[216] M. Bellare and C. Namprempre, "Authenticated Encryption: Relations Among Notions and Analysis of the Generic Composition Paradigm," in *Advances in Cryptology – ASIACRYPT 2000. Lecture Notes in Computer Science* (T. Okamoto, ed.), vol. 1976, pp. 531–545, Springer, 2000.

[217] Openreach, "Your Guide to Openreach," Company Overview Booklet, 2017.

[218] N. J. Cerf, M. Lévy, and G. van Assche, "Quantum Distribution of Gaussian Keys Using Squeezed States," *Physical Review A*, vol. 63, no. 5, p. 052311, 2001.

[219] M. Mehmet, S. Ast, T. Eberle, S. Steinlechner, H. Vahlbruch, and R. Schnabel, "Squeezed Light at 1550nm with a Quantum Noise Reduction of 12.3 dB," *Optics Express*, vol. 19, no. 25, pp. 25763–25772, 2011.

[220] R. Schnabel, "Squeezed States of Light and Their Applications in Laser Interferometers," *Physics Reports*, vol. 684, pp. 1–51, 2017.

[221] D. Huang, D. Lin, C. Wang, W. Liu, S. Fang, J. Peng, P. Huang, and G. Zeng, "Continuous-Variable Quantum Key Distribution with 1 Mbps Secure Key Rate," *Journal of Lightwave Technology*, vol. 32, no. 4, pp. 776–782, 2014.

[222] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum Key Distribution Using Gaussian-Modulated Coherent States," *Nature*, vol. 421, pp. 238–241, 2003.

[223] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, "Quantum Cryptography Without Switching," *Physical Review Letters*, vol. 93, no. 17, p. 170504, 2004.

[224] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. Koy Lam, "No-Switching Quantum Key Distribution Using Broadband Modulated Coherent Light," *Physical Review Letters*, vol. 95, no. 18, p. 180503, 2005.

[225] Z. Zhang, C. Chen, Q. Zhuang, F. N. C. Wong, and J. H. Shapiro, "Experimental Quantum Key Distribution at 1.3 Gigabit-per-Second Secret-Key Rate Over a 10dB Loss Channel," *Quantum Science and Technology*, vol. 3, no. 2, p. 025007, 2018.

[226] A. K. Ekert, "Quantum Cryptography Based on Bell's Theorem," *Physical Review Letters*, vol. 67, no. 6, pp. 661–663, 1991.

[227] C. H. Bennett and S. J. Wiesner, "Communication via One- and Two-Particle Operators on Einstein-Podolsky-Rosen States," *Physical Review Letters*, vol. 69, no. 20, pp. 2881–2884, 1992.

[228] C. H. Bennett, G. Brassard, and S. Breidbart, "Quantum Cryptography II: How to Re-Use a One-Time Pad Safely Even if P=NP," *Natural Computing*, vol. 13, no. 4, pp. 453–458, 2014.

[229] A. B. Price, J. G. Rarity, and C. Erven, "A Quantum Key Distribution Protocol for Rapid Denial of Service Detection," *5th Bristol Quantum Information Technologies Workshop (BQIT)*, 2018.

[230] C. Beek, D. Dinkar, Y. Gund, G. Lancioni, N. Minihan, F. Moreno, E. Peterson, T. Roccia, C. Schmugar, R. Simon, D. Sommer, B. Sun, R. Tiwari, and V. Weafer, "McAfee Labs Threat Report: June 2017," Research Report, *McAfee*, 2017.

[231] C. Beek, D. Dinkar, D. Frosst, E. Grandjean, F. Moreno, E. Peterson, P. Rao, R. Samani, C. Schmugar, R. Simon, D. Sommer, B. Sun, I. Valenzuela, and V. Weafer, "McAfee Labs Threat Report: September 2017," Research Report, *McAfee*, 2017.

[232] N. Minihane, F. Moreno, E. Peterson, R. Samani, C. Schmugar, D. Sommer, and B. Sun, "McAfee Labs Threat Report: December 2017," Research Report, *McAfee*, 2017.

[233] A. Bassett, C. Beek, N. Minihane, E. Peterson, R. Samani, C. Schmugar, R. Sims, D. Sommer, and B. Sun, "McAfee Labs Threat Report: March 2018," Research Report, *McAfee*, 2018.

[234] K. Richards, R. LaSalle, M. Devost, F. van den Dool, and J. Kennedy-White, "2017 Cost of Cybercrime Study: Insights on the Security Investments That Make a Difference," Research Report, *Ponemon Institute*, 2017.

[235] R. Roscino, K. Layat, G. Ribordy, B. Huttner, and D. Caselunghe, "Applicability of a Post-Quantum Signature in a QKD Public Channel," *6th International Conference on Quantum Cryptography (QCRYPT)*, 2016.

[236] G. Brassard, "On Computationally Secure Authentication Tags Requiring Short Secret Shared Keys," in *Advances in Cryptology: Proceedings of Crypto 82* (D. Chaum, R. L. Rivest, and A. T. Sherman, eds.), pp. 79–86, Springer, 1983.

[237] J. Black, S. Halevi, A. Hevia, H. Krawczyk, and T. Krovetz (ed.), "UMAC: Message Authentication Code Using Universal Hashing," *Network Working Group, The Internet Society*, 2006.

[238] T. Krovetz, "Message Authentication on 64-Bit Architectures," in *Selected Areas in Cryptography: 13th International Workshop. SAC 2006 Revised Selected Papers. Lecture Notes in Computer Science* (E. Biham and A. M. Youssef, eds.), vol. 4356, pp. 327–341, Springer, 2007.

[239] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and Simple One-Way Quantum Key Distribution," *Applied Physics Letters*, vol. 87, no. 19, p. 194108, 2005.

[240] D. J. Bernstein, "Stronger Security Bounds for Wegman-Carter-Shoup Authenticators," in *Advances in Cryptology – EUROCRYPT 2005. Lecture Notes in Computer Science* (R. Cramer, ed.), vol. 3494, pp. 164–180, Springer, 2005.

[241] T. D. Krovetz, "Software-Optimized Universal Hashing and Message Authentication," PhD Thesis, *University of California Davis*, 2000.

[242] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway, "A Concrete Security Treatment of Symmetric Encryption," in *Proceedings of the 38th Symposium on Foundations of Computer Science*, pp. 394–403, IEEE, 1997. Full version available from `http://web.cs.ucdavis.edu/~rogaway/papers/sym-enc.pdf` [Last Accessed: 07/04/17].

[243] J. Katz and Y. Lindell, "Introduction to Modern Cryptography," *Chapman & Hall/CRC*, 2008.

[244] C. Branciard, N. Gisin, B. Kraus, and V. Scarani, "Security of Two Quantum Cryptography Protocols Using the Same Four Qubit States," *Physical Review A*, vol. 72, no. 3, p. 032301, 2005.

[245] M. Mosca, D. Stebila, and B. Ustaoğlu, "Quantum Key Distribution in the Classical Authenticated Key Exchange Framework," in *Post-Quantum Cryptography. PQCrypto 2013. Lecture Notes in Computer Science* (P. Gaborit, ed.), vol. 7932, pp. 136–154, Springer, 2013.

[246] M. Zhandry, "How to Construct Quantum Random Functions," in *Proceedings of the 53rd Symposium on Foundations of Computer Science*, pp. 679–687, IEEE, 2012.

[247] P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. L. O'Brien, and M. G. Thompson, "Chip-Based Quantum Key Distribution," *Nature Communications*, vol. 8, p. 13984, 2017.

[248] D. E. Knuth, "The Art of Computer Programming," 2nd Edition, *Addison-Wesley*, vol. 3, 1998.

[249] D. Augot, L. Batina, D. J. Bernstein, J. Bos, J. Buchmann, W. Castryck, O. Dunkelman, T. Güneysu, S. Gueron, A. Hülsing, T. Lange, M. S. E. Mohamed, C. Rechberger, P. Schwabe, N. Sendrier, F. Vercauteren, and B.-Y. Yang, "Initial Recommendations of Long-Term Secure Post-Quantum Systems," White Paper*, PQCRYPTO*, 2015.

[250] J. Müller-Quade and R. Renner, "Composability in Quantum Cryptography," *New Journal of Physics*, vol. 11, no. 8, p. 085006, 2009.

[251] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum Cryptography Without Bell's Theorem," *Physical Review Letters*, vol. 68, no. 5, pp. 557–559, 1992.

[252] H. Bechmann-Pasquinucci and N. Gisin, "Incoherent and Coherent Eavesdropping in the Six-State Protocol of Quantum Cryptography," *Physical Review A*, vol. 59, no. 6, pp. 4238–4248, 1999.

[253] K. Tamaki and H.-K. Lo, "Unconditional Secure Key Distillation From Multiphotons," *Physical Review A*, vol. 73, no. 1, p. 010302(R), 2006.

[254] A. Chefles, "Unambiguous Discrimination Between Linearly Dependent States with Multiple Copies," *Physical Review A*, vol. 64, no. 6, p. 062305, 2001.

[255] H.-K. Lo, "Method for Decoupling Error Correction From Privacy Amplification," *New Journal of Physics*, vol. 5, no. 36, pp. 36.1–36.24, 2003.

[256] X. Ma and N. Lütkenhaus, "Improved Data Post-Processing in Quantum Key Distribution and Application to Loss Thresholds in Device Independent QKD," *Quantum Information & Computation*, vol. 12, no. 3-4, pp. 203–214, 2012.

[257] A. B. Price, J. G. Rarity, and C. Erven, "Implementing Hybrid Quantum-Postquantum Security in a Prototype Network," *8th International Conference on Quantum Cryptography (QCRYPT)*, 2018.

[258] R. J. McEliece, "A Public-Key Cryptosystem Based On Algebraic Coding Theory," *The Deep Space Network Progress Report (NASA JPL)*, vol. 42-44, pp. 114–116, 1978.

[259] G. Alagic, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, Y.-K. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, and D. Smith-Tone, "NISTIR 8240. Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process," *National Institute of Standards and Technology*, 2019.

[260] E. Rescorla, M. Abadi, C. Allen, R. Barnes, S. M. Bellovin, D. Benjamin, B. Beurdouche, K. Bhargavan, S. Blake-Wilson, N. Bolyard, R. Canetti, M. Caswell, S. Checkoway, P. Chown, K. Cohn-Gordon, C. Cremers, A. Delignat-Lavaud, T. Dierks, R. DuToit, T. Elgamal, P. Eronen, C. Fournet, A. Gangolli, D. M. Garrett, I. Gerasymchuk, A. Ghedini, D. K. Gillmor,

M. Green, J. Guballa, F. Guenther, V. Gupta, C. Hawk, K. Hickman, A. Hoenes, D. Hopwood, M. Horvat, J. Hoyland, S. Iyengar, B. Kaduk, H. Kario, P. Karlton, L. Klingele, P. Kocher, H. Krawczyk, A. Langley, O. Levillain, X. Liu, I. Liusvaara, A. Luykx, C. MacCarthaigh, C. Mehner, J. Mikkelsen, B. Moeller, K. Nekritz, E. Nygren, M. Nystrom, K. Oku, K. Paterson, C. Patton, A. Pironti, A. Popov, M. Ray, R. Relyea, K. Rose, J. Roskind, M. Sabin, J. Salowey, R. Salz, D. Schinazi, S. Scott, T. Shrimpton, D. Simon, B. Smith, B. Sniffen, N. Sullivan, B. Tackmann, T. Taubert, M. Thomson, H. Tschofenig, S. Turner, S. Valdez, F. Valsorda, T. van der Merwe, V. Vasiliev, H. Wee, T. Weinstein, D. Wong, C. A. Wood, T. Wright, P. Wu, and K. Yamamoto, "The Transport Layer Security (TLS) Protocol Version 1.3," *Internet Engineering Task Force. RFC:8446*, 2018.

[261] L. Chen, "NIST SP 800-108. Recommendation for Key Derivation Using Pseudorandom Functions (Revised)," *National Institute of Standards and Technology*, 2010.

[262] M. Dworkin, "NIST SP 800-38B. Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication," *National Institute of Standards and Technology*, 2005.

[263] H. Krawczyk and P. Eronen, "HMAC-Based Extract-and-Expand Key Derivation Function (HKDF)," *Internet Engineering Task Force. RFC:5869*, 2010.

[264] Cisco, "The Zettabyte Era: Trends and Analysis," White Paper, 2017.

[265] M. Ajtai, "Generating Hard Instances of Lattice Problems," in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing (STOC '96)* (G. L. Miller, ed.), pp. 99–108, Association for Computing Machinery, 1996.

[266] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A Ring-Based Public Key Cryptosystem," in *Algorithmic Number Theory. ANTS 1998. Lecture Notes in Computer Science* (J. P. Buhler, ed.), vol. 1423, pp. 267–288, Springer, 1998.

[267] W. Whyte, "NTRU," in *Encyclopedia of Cryptography and Security* (H. C. van Tilborg, ed.), pp. 427–430, Springer, 2005.

[268] O. Regev, "On Lattices, Learning with Errors, Random Linear Codes, and Cryptography," in *Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing (STOC '05)* (H. Gabow and R. Fagin, eds.), pp. 84–93, Association for Computing Machinery, 2005.

[269] P. Campbell, M. Groves, and D. Shepherd, "SOLILOQUY: A Cautionary Tale," *2nd ETSI/IQC Workshop on Quantum-Safe Cryptography*, 2014.

[270] R. Cramer, L. Ducas, and B. Wesolowski, "Short Stickelberger Class Relations and Application to Ideal-SVP," in *Advances in Cryptology – EUROCRYPT 2017. Lecture Notes in Computer Science* (J.-S. Coron and J. B. Nielsen, eds.), vol. 10210, pp. 324–348, Springer, 2017.

[271] J.-M. Couveignes, "Hard Homogeneous Spaces," *Cryptology ePrint Archive: Report 2006/291*, 2006.

[272] A. Rostovtsev and A. Stolbunov, "Public-Key Cryptosystem Based on Isogenies," *Cryptology ePrint Archive: Report 2006/145*, 2006.

[273] A. Stolbunov, "Constructing Public-Key Cryptographic Schemes Based on Class Group Action on a Set of Isogenous Elliptic Curves," *Advances in Mathematics of Communications*, vol. 4, no. 2, pp. 215–235, 2010.

[274] A. Childs, D. Jao, and V. Soukharev, "Constructing Elliptic Curve Isogenies in Quantum Subexponential Time," *Journal of Mathematical Cryptology*, vol. 8, no. 1, pp. 1–29, 2013. Erratum released as arXiv:1012.4019v3 [quant-ph].

[275] D. Jao and L. D. Feo, "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies," in *Post-Quantum Cryptography. PQCrypto 2011. Lecture Notes in Computer Science* (B.-Y. Yang, ed.), vol. 7071, pp. 19–34, Springer, 2011.

[276] S. D. Galbraith and F. Vercauteren, "Computational Problems in Supersingular Elliptic Curve Isogenies," *Quantum Information Processing*, vol. 17, no. 10, p. 265, 2018.

[277] D. J. Bernstein, N. Heninger, P. Lou, and L. Valenta, "Post-Quantum RSA," in *Post-Quantum Cryptography. PQCrypto 2017. Lecture Notes in Computer Science* (T. Lange and T. Takagi, eds.), vol. 10346, pp. 311–329, Springer, 2017.

[278] A. Chailloux, M. Naya-Plasencia, and A. Schrottenloher, "An Efficient Quantum Collision Search Algorithm and Implications on Symmetric Cryptography," *Advances in Cryptology – ASIACRYPT 2017. Lecture Notes in Computer Science*, vol. 10625, pp. 211–240, 2017.

[279] R. C. Merkle, "A Certified Digital Signature," in *Advances in Cryptology — CRYPTO' 89 Proceedings. Lecture Notes in Computer Science* (G. Brassard, ed.), vol. 435, pp. 218–238, Springer, 1989.

[280] J. Buchmann, E. Dahmen, and A. Hülsing, "XMSS - A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions," in *Post-Quantum Cryptography. PQCrypto 2011. Lecture Notes in Computer Science* (B.-Y. Yang, ed.), vol. 7071, pp. 117–129, Springer, 2011.

[281] D. J. Bernstein, D. Hopwood, A. Hülsing, T. Lange, R. Niederhagen, L. Papachristodoulou, M. Schneider, P. Schwabe, and Z. Wilcox-O'Hearn, "SPHINCS: Practical Stateless Hash-Based Signatures," in *Advances in Cryptology – EUROCRYPT 2015. Lecture Notes in Computer Science* (E. Oswald and M. Fischlin, eds.), vol. 9056, pp. 368–397, Springer, 2015.

[282] V. D. Goppa, "A New Class of Linear Correcting Codes," *Problemy Peredachi Informatsii*, vol. 6, no. 3, pp. 24–30, 1970.

[283] E. R. Berlekamp, "Goppa Codes," *IEEE Transactions on Information Theory*, vol. 19, no. 5, pp. 590–592, 1973.

[284] N. Patterson, "The Algebraic Decoding of Goppa Codes," *IEEE Transactions on Information Theory*, vol. 21, no. 2, pp. 203–207, 1975.

[285] E. R. Berlekamp, R. J. McEliece, and H. C. A. van Tilborg, "On the Inherent Intractability of Certain Coding Problems," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 384–386, 1978.

[286] F. Strenzke, "Botan's Implementation of the McEliece PKC," White Paper*, cryptosource GmbH*, 2014.

[287] D. Neus, K. Michaelis, R. Korthaus, P. Weber, C. Mainka, M. Gierlings, J. Schwenk, J. Somorovsky, and T. Niemann, "Projekt 197: Sichere Implementierung einer allgemeinen Kryptobibliothek. Projektzusammenfassung," White Paper*, Bundesamt für Sicherheit in der Informationstechnik*, 2017.

[288] E. Persichetti, "Secure and Anonymous Hybrid Encryption from Coding Theory," in *Post-Quantum Cryptography. PQCrypto 2013. Lecture Notes in Computer Science* (P. Gaborit, ed.), vol. 7932, pp. 174–187, Springer, 2013.

[289] IEEE Computer Society, "IEEE Standard Specifications for Public-Key Cryptography," *IEEE. Std 1363-2000*, 2000.

[290] IEEE Computer Society, "1363a. IEEE Standard Specifications for Public-Key Cryptography - Amendment 1: Additional Techniques," *IEEE. Std 1363a-2004*, 2004.

[291] NIST, "Secure Hash Standard (SHS)," *Federal Information Processing Standards Publication 180-4*, 2015.

[292] H. Niederreiter, "Knapsack-Type Cryptosystems and Algebraic Coding Theory," *Problems of Control and Information Theory*, vol. 15, no. 2, pp. 159–166, 1986.

[293] Y. X. Li, R. H. Deng, and X. M. Wang, "On the Equivalence of McEliece's and Niederreiter's Public-Key Cryptosystems," *IEEE Transactions on Information Theory*, vol. 40, no. 1, pp. 271–273, 1994.

[294] T. Chou, "McBits Revisited," in *Cryptographic Hardware and Embedded Systems. CHES 2017. Lecture Notes in Computer Science* (W. Fischer and N. Homma, eds.), vol. 10529, pp. 213–231, Springer, 2017.

[295] D. J. Bernstein, T. Chou, and P. Schwabe, "McBits: Fast Constant-Time Code-Based Cryptography," in *Cryptographic Hardware and Embedded Systems – CHES 2013. Lecture Notes in Computer Science* (G. Bertoni and J.-S. Coron, eds.), vol. 8086, pp. 250–272, Springer, 2013.

[296] E. Barker and J. Kelsey, "NIST SP 800-90A. Revision 1. Recommendation for Random Number Generation Using Deterministic Random Bit Generators," *National Institute of Standards and Technology*, 2015.

[297] FBI Cyber Division, "Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain," Private Industry Notification (Unclassified), 2014.

[298] M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Efficient Decoy-State Quantum Key Distribution with Quantified Security," *Optics Express*, vol. 21, no. 21, pp. 24550–24565, 2013.

[299] ID Quantique, "Redefining Security. Cerberis^3 QKD System: State-of-the-Art Quantum Key Distribution," Product Brochure, 2018.

[300] M. Dworkin, "NIST SP 800-38F. Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping," *National Institute of Standards and Technology*, 2012.

[301] A. B. Price, P. Sibson, C. Erven, J. G. Rarity, and M. G. Thompson, "High-Speed Quantum Key Distribution with Wavelength-Division Multiplexing on Integrated Photonic Devices," in *Conference on Lasers and Electro-Optics (CLEO), OSA Technical Digest*, Optical Society of America, 2018.

[302] P. Sibson, C. Erven, J. Kennard, A. B. Price, D. Llewellyn, J. Wang, and M. G. Thompson, "Chip-Based Quantum Communications," in *2018 European Conference on Optical Communication (ECOC)*, pp. 1–3, IEEE, 2018.

[303] P. Sibson, A. B. Price, S. Stanisic, J. Kennard, C. Erven, J. L. O'Brien, and M. G. Thompson, "Integrated Photonics for Quantum Key Distribution," *6th International Conference on Quantum Cryptography (QCRYPT)*, 2016.

[304] A. Tomita, K.-i. Yoshino, Y. Nambu, A. Tajima, A. Tanaka, S. Takahashi, W. Maeda, S. Miki, Z. Wang, M. Fujiwara, and M. Sasaki, "High Speed Quantum Key Distribution System," *Optical Fiber Technology*, vol. 16, no. 1, pp. 55–62, 2010.

[305] S. Wang, W. Chen, J.-F. Guo, Z.-Q. Yin, H.-W. Li, Z. Zhou, G.-C. Guo, and Z.-F. Han, "2 GHz Clock Quantum Key Distribution Over 260 km of Standard Telecom Fiber," *Optics Letters*, vol. 37, no. 6, pp. 1008–1010, 2012.

[306] H. Ishio, J. Minowa, and K. Nosu, "Review and Status of Wavelength-Division-Multiplexing Technology and Its Application," *Journal of Lightwave Technology*, vol. 2, no. 4, pp. 448–463, 1984.

[307] C. A. Brackett, "Dense Wavelength Division Multiplexing Networks: Principles and Applications," *IEEE Journal on Selected Areas in Communications*, vol. 8, no. 6, pp. 948–964, 1990.

[308] A. Banerjee, Y. Park, F. Clarke, H. Song, S. Yang, G. Kramer, K. Kim, and B. Mukherjee, "Wavelength-Division-Multiplexed Passive Optical Network (WDM-PON) Technologies for Broadband Access: A Review," *Journal of Optical Networking*, vol. 4, no. 11, pp. 737–758, 2005.

[309] International Telecommunication Union, "Series G: Transmission Systems and Media, Digital Systems and Networks. Transmission Media Characteristics - Characteristics of Optical Components and Subsystems. Spectral Grids for WDM Applications: CWDM Wavelength Grid," *Recommendation ITU-T G.694.2*, 2003.

[310] International Telecommunication Union, "Series G: Transmission Systems and Media, Digital Systems and Networks. Transmission Media Characteristics - Characteristics of Optical Components and Subsystems. Spectral Grids for WDM Applications: DWDM Wavelength Grid," *Recommendation ITU-T G.694.1*, 2012.

[311] G. Brassard, F. Bussieres, N. Godbout, and S. Lacroix, "Multiuser Quantum Key Distribution Using Wavelength Division Multiplexing," in *Proceedings of SPIE, Applications of Photonic Technology 6* (R. A. Lessard and G. A. Lampropoulos, eds.), vol. 5260, pp. 149–153, SPIE, 2003.

[312] A. Tanaka, M. Fujiwara, K.-i. Yoshino, S. Takahashi, Y. Nambu, A. Tomita, S. Miki, T. Yamashita, Z. Wang, M. Sasaki, and A. Tajima, "High-Speed Quantum Key Distribution System for 1-Mbps Real-Time Key Generation," *IEEE Journal of Quantum Electronics*, vol. 48, no. 4, pp. 542–550, 2012.

[313] K.-i. Yoshino, M. Fujiwara, A. Tanaka, S. Takahashi, Y. Nambu, A. Tomita, S. Miki, T. Yamashita, Z. Wang, M. Sasaki, and A. Tajima, "High-Speed Wavelength-Division Multiplexing Quantum Key Distribution System," *Optics Letters*, vol. 37, no. 2, pp. 223–225, 2012.

[314] K.-i. Yoshino, T. Ochi, M. Fujiwara, M. Sasaki, and A. Tajima, "Maintenance-Free Operation of WDM Quantum Key Distribution System Through a Field Fiber Over 30 Days," *Optics Express*, vol. 21, no. 25, pp. 31395–31401, 2013.

[315] E. Diamanti, H. Takesue, C. Langrock, M. M. Fejer, and Y. Yamamoto, "100 km Differential Phase Shift Quantum Key Distribution Experiment with Low Jitter Up-Conversion Detectors," *Optics Express*, vol. 14, no. 26, pp. 13073–13082, 2006.

[316] A. Tanaka, M. Fujiwara, S. W. Nam, Y. Nambu, S. Takahashi, W. Maeda, K.-i. Yoshino, S. Miki, B. Baek, Z. Wang, A. Tajima, M. Sasaki, and A. Tomita, "Ultra Fast Quantum Key Distribution Over a 97 km Installed Telecom Fiber with Wavelength Division Multiplexing Clock Synchronization," *Optics Express*, vol. 16, no. 15, pp. 11354–11360, 2008.

[317] R. J. Hughes, J. E. Nordholt, K. P. McCabe, R. T. Newell, C. G. Peterson, and R. D. Somma, "Network-Centric Quantum Communications with Application to Critical Infrastructure Protection," *arXiv:1305.0305 [quant-ph]*, 2013.

[318] P. Zhang, K. Aungskunsiri, E. Martín-López, J. Wabnig, M. Lobino, R. W. Nock, J. Munns, D. Bonneau, P. Jiang, H. W. Li, A. Laing, J. G. Rarity, A. O. Niskanen, M. G. Thompson, and J. L. O'Brien, "Reference-Frame-Independent Quantum-Key-Distribution Server with a Telecom Tether for an On-Chip Client," *Physical Review Letters*, vol. 112, no. 13, p. 130501, 2014.

[319] C. Ma, W. D. Sacher, Z. Tang, J. C. Mikkelsen, Y. Yang, F. Xu, T. Thiessen, H.-K. Lo, and J. K. S. Poon, "Silicon Photonic Transmitter for Polarization-Encoded Quantum Key Distribution," *Optica*, vol. 3, no. 11, pp. 1274–1278, 2016.

[320] H. Cai, C. M. Long, C. T. DeRose, N. Boynton, J. Urayama, R. Camacho, A. Pomerene, A. L. Starbuck, D. C. Trotter, P. S. Davids, and A. L. Lentine, "Silicon Photonic Transceiver Circuit for High-Speed Polarization-Based Discrete Variable Quantum Key Distribution," *Optics Express*, vol. 25, no. 11, pp. 12282–12294, 2017.

[321] Y. Ding, D. Bacco, K. Dalgaard, X. Cai, X. Zhou, K. Rottwitt, and L. K. Oxenløwe, "High-Dimensional Quantum Key Distribution Based on Multicore Fiber Using Silicon Photonic Integrated Circuits," *npj Quantum Information*, vol. 3, no. 1, p. 25, 2017.

[322] D. Bunandar, A. Lentine, C. Lee, H. Cai, C. M. Long, N. Boynton, N. Martinez, C. DeRose, C. Chen, M. Grein, D. Trotter, A. Starbuck, A. Pomerene, S. Hamilton, F. N. Wong, R. Camacho, P. Davids, J. Urayama, and D. Englund, "Metropolitan Quantum Key Distribution with Silicon Photonics," *Physical Review X*, vol. 8, no. 2, p. 021009, 2018.

[323] A. Vaquero-Stainer, R. A. Kirkwood, V. Burenkov, C. J. Chunnilall, A. G. Sinclair, A. Hart, H. Semenenko, P. Sibson, C. Erven, and M. G. Thompson, "Measurements Towards Providing Security Assurance for a Chip-Scale QKD System," in *Proceedings of SPIE, Quantum Technologies 2018* (J. Stuhler, A. J. Shields, and M. J. Padgett, eds.), vol. 10674, p. 106741A, SPIE, 2018.

[324] P. Sibson, J. E. Kennard, S. Stanisic, C. Erven, J. L. O'Brien, and M. G. Thompson, "Integrated Silicon Photonics for High-Speed Quantum Key Distribution," *Optica*, vol. 4, no. 2, pp. 172–177, 2017.

[325] T. L. Koch and U. Koren, "InP-Based Photonic Integrated Circuits," *IEE Proceedings J - Optoelectronics*, vol. 138, no. 2, pp. 139–147, 1991.

[326] R. Matz, J. G. Bauer, P. Clemens, G. Heise, H. F. Mahlein, W. Metzger, H. Michel, and G. Schulte-Roth, "Development of a Photonic Integrated Transceiver Chip for WDM Transmission," *IEEE Photonics Technology Letters*, vol. 6, no. 11, pp. 1327 – 1329, 1994.

[327] R. Kaiser, M. Hamacher, H. Heidrich, P. Albrecht, W. Ebert, R. Gibis, H. Künzel, R. Löffler, S. Malchow, M. Mohrle, W. Rehbein, and H. Schroeter-Janßen, "Monolithically Integrated Transceivers on InP: The Development of a Generic Integration Concept and Its Technological Challenges," in *Conference Proceedings. 1998 International Conference on Indium Phosphide and Related Materials*, pp. 431–434, IEEE, 1998.

[328] E. R. H. Fuchs, R. E. Kirchain, and S. Liu, "The Future of Silicon Photonics: Not So Fast? Insights From 100G Ethernet LAN Transceivers," *Journal of Lightwave Technology*, vol. 29, no. 15, pp. 2319–2326, 2011.

[329] X. Leijtens, "JePPIX: The Platform for Indium Phosphide-Based Photonics," *IET Optoelectronics*, vol. 5, no. 5, pp. 202–206, 2010.

[330] W. Hoving, R. Heideman, D. Geuzebroek, A. Leinse, E. Klein, and R. Dekker, "Low Loss, High Contrast Planar Optical Waveguides Based on Low-Cost CMOS Compatible LPCVD Processing," in *Proceedings of SPIE, Silicon Photonics and Photonic Integrated Circuits* (G. C. Righini, S. K. Honkanen, L. Pavesi, and L. Vivien, eds.), vol. 6996, p. 699612, SPIE, 2008.

[331] R. Soref, "The Past, Present, and Future of Silicon Photonics," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 12, no. 6, pp. 1678–1687, 2006.

[332] J. W. Silverstone, D. Bonneau, J. L. O'Brien, and M. G. Thompson, "Silicon Quantum Photonics," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 22, no. 6, pp. 390–402, 2016.

[333] M. Smit, X. Leijtens, H. Ambrosius, E. Bente, J. van der Tol, B. Smalbrugge, T. de Vries, E.-J. Geluk, J. Bolk, R. van Veldhoven, L. Augustin, P. Thijs, D. D'Agostino, H. Rabbani, K. Lawniczuk, S. Stopinski, S. Tahvili, A. Corradi, E. Kleijn, D. Dzibrou, M. Felicetti, E. Bitincka, V. Moskalenko, J. Zhao, R. Santos, G. Gilardi, W. Yao, K. Williams, P. Stabile, P. Kuindersma, J. Pello, S. Bhat, Y. Jiao, D. Heiss, G. Roelkens, M. Wale, P. Firth, F. Soares, N. Grote, M. Schell, H. Debregeas, M. Achouche, J.-L. Gentner, A. Bakker, T. Korthorst, D. Gallagher, A. Dabbs, A. Melloni, F. Morichetti, D. Melati, A. Wonfor, R. Penty, R. Broeke, B. Musk, and D. Robbins, "An Introduction to InP-Based Generic Integration Technology," *Semiconductor Science and Technology*, vol. 29, no. 8, p. 083001, 2014.

[334] R. H. Hadfield, "Single-Photon Detectors for Optical Quantum Information Applications," *Nature Photonics*, vol. 3, pp. 696–705, 2009.

[335] C. M. Natarajan, M. G. Tanner, and R. H. Hadfield, "Superconducting Nanowire Single-Photon Detectors: Physics and Applications," *Superconductor Science and Technology*, vol. 25, no. 6, p. 063001, 2012.

[336] D. Taillaert, F. van Laere, M. Ayre, W. Bogaerts, D. van Thourhout, P. Bienstman, and R. Baets, "Grating Couplers for Coupling between Optical Fibers and Nanophotonic Waveguides," *Japanese Journal of Applied Physics*, vol. 45, no. 8A, pp. 6071–6077, 2006.

[337] D. Taillaert, H. Chong, P. I. Borel, L. H. Frandsen, R. M. De La Rue, and R. Baets, "A Compact Two-Dimensional Grating Coupler Used as a Polarization Splitter," *IEEE Photonics Technology Letters*, vol. 15, no. 9, pp. 1249–1251, 2003.

[338] E. Hecht, "Optics," 4th Edition, *Pearson Education*, 2002.

[339] A. Macleod, "The Critical Angle and Beyond," *SVC Bulletin, Fall Edition*, pp. 14–20, 2009.

[340] G. Lifante, "Integrated Photonics: Fundamentals," *Wiley*, 2003.

[341] L. B. Soldano and E. C. M. Pennings, "Optical Multi-Mode Interference Devices Based on Self-Imaging: Principles and Applications," *Journal of Lightwave Technologies*, vol. 13, no. 4, pp. 615–627, 1995.

[342] R. L. Espinola, M.-C. Tsai, J. T. Yardley, and R. M. Osgood, "Fast and Low-Power Thermooptic Switch on Thin Silicon-on-Insulator," *IEEE Photonics Technology Letters*, vol. 15, no. 10, pp. 1366–1368, 2003.

[343] J. S. Weiner, D. A. B. Miller, and D. S. Chemla, "Quadratic Electro-Optic Effect Due to the Quantum-Confined Stark Effect in Quantum Wells," *Applied Physics Letters*, vol. 50, no. 13, pp. 842–844, 1987.

[344] G. T. Reed, G. Mashanovich, F. Y. Gardes, and D. J. Thomson, "Silicon Optical Modulators," *Nature Photonics*, vol. 4, pp. 518–526, 2010.

[345] Q. Lai, M. Lanker, W. Hunziker, and H. Melchior, "Tunable Wavelength-Selection Switch and Multiplexer/Demultiplexer Based on Asymmetric Silica-on-Silicon Mach-Zehnder Interferometer," *Electronics Letters*, vol. 34, no. 3, pp. 266–267, 1998.

[346] A. Laing, V. Scarani, J. G. Rarity, and J. L. O'Brien, "Reference-Frame-Independent Quantum Key Distribution," *Physical Review A*, vol. 82, no. 1, p. 012304, 2010.

[347] K. K. Lee, D. R. Lim, H.-C. Luan, A. Agarwal, J. Foresi, and L. C. Kimerling, "Effect of Size and Roughness on Light Transmission in a Si/SiO_2 Waveguide: Experiments and Model," *Applied Physics Letters*, vol. 77, no. 11, pp. 1617–1619, 2000.

[348] J. F. Dynes, S. J. Kindness, S. W.-B. Tam, A. Plews, A. W. Sharpe, M. Lucamarini, B. Fröhlich, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Quantum Key Distribution Over Multicore Fiber," *Optics Express*, vol. 24, no. 8, pp. 8081–8087, 2016.

[349] C. V. Raman, "A New Radiation," *Indian Journal of Physics*, vol. 2, pp. 387–398, 1927.

[350] G. Agrawal, "Nonlinear Fiber Optics," 5th Edition, *Academic Press*, 2013.

[351] N. Walenta, A. Burg, D. Caselunghe, J. Constantin, N. Gisin, O. Guinnard, R. Houlmann, P. Junod, B. Korzh, N. Kulesza, M. Legré, C. W. Lim, T. Lunghi, L. Monat, C. Portmann, M. Soucarros, R. T. Thew, P. Trinkler, G. Trolliet, F. Vannel, and H. Zbinden, "A Fast and Versatile Quantum Key Distribution System with Hardware Key Distillation and Wavelength Multiplexing," *New Journal of Physics*, vol. 16, no. 1, p. 013047, 2014.

[352] I. Choi, Y. Rong Zhou, J. F. Dynes, Z. Yuan, A. Klar, A. Sharpe, A. Plews, M. Lucamarini, C. Radig, J. Neubert, H. Griesser, M. Eiselt, C. Chunnilall, G. Lepert, A. Sinclair, J.-P. Elbers, A. Lord, and A. Shields, "Field Trial of a Quantum Secured 10 Gb/s DWDM Transmission System Over a Single Installed Fiber," *Optics Express*, vol. 22, no. 19, pp. 23121–23128, 2014.

[353] P. D. Townsend, "Simultaneous Quantum Cryptographic Key Distribution and Conventional Data Transmission Over Installed Fibre Using Wavelength-Division Multiplexing," *Electronics Letters*, vol. 33, no. 3, pp. 188–190, 1997.

[354] N. I. Nweket, P. Toliver, R. J. Runser, S. R. McNown, T. Chapuran, M. S. Goodman, R. J. Hughes, C. G. Peterson, K. McCabe, J. E. Nordholt, K. Tyagi, P. Hiskett, and N. Dallmann, "Experimental Characterization of Wavelength Separation for "QKD+WDM" Co-Existence," in *(CLEO). Conference on Lasers and Electro-Optics, 2005*, vol. 2, pp. 1503–1505, IEEE, 2005.

[355] K. Inoue, E. Waks, and Y. Yamamoto, "Differential Phase-Shift Quantum Key Distribution," in *Proceedings of SPIE, Quantum Optics in Computing and Communications* (S. Liu, G. Guo, H.-K. Lo, and N. Imoto, eds.), vol. 4917, pp. 32–39, SPIE, 2002.

[356] NIST, "Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process," Call for Proposals, 2016.

[357] B. Schneier, "Cryptography after the Aliens Land," *IEEE Security & Privacy*, vol. 16, no. 5, pp. 86–88, 2018.

[358] S. Bravyi and A. Kitaev, "Universal Quantum Computation with Ideal Clifford Gates and Noisy Ancillas," *Physical Review A*, vol. 71, no. 2, p. 022316, 2005.

[359] E. T. Campbell, H. Anwar, and D. E. Browne, "Magic-State Distillation in All Prime Dimensions Using Quantum Reed-Muller Codes," *Physical Review X*, vol. 2, no. 4, p. 041021, 2012.

[360] R. P. Feynman, "Quantum Mechanical Computers," *Foundations of Physics*, vol. 16, no. 6, pp. 507–531, 1986.

[361] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway, "Relations Among Notions of Security for Public-Key Encryption Schemes," in *Advances in Cryptology – CRYPTO '98. Lecture Notes in Computer Science* (H. Krawczyk, ed.), vol. 1462, pp. 26–45, Springer, 1998.

[362] D. Bleichenbacher, "Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1," in *Advances in Cryptology – CRYPTO '98. Lecture Notes in Computer Science* (H. Krawczyk, ed.), vol. 1462, pp. 1–12, Springer, 1998.

[363] H. Böck, J. Somorovsky, and C. Young, "Return Of Bleichenbacher's Oracle Threat (ROBOT)," in *Proceedings of the 27th USENIX Security Symposium (USENIX Security 18)*, pp. 817–849, USENIX Association, 2018.

[364] E. Ronen, R. Gillham, D. Genkin, A. Shamir, D. Wong, and Y. Yarom, "The 9 Lives of Bleichenbacher's CAT: New Cache ATtacks on TLS Implementations," *Cryptology ePrint Archive: Report 2018/1173*, 2018.

APPENDIX $|A\rangle$

APPENDIX TO CHAPTER 2: QUANTUM LOGIC GATES

Here, we summarise a subset of the logic gates that can be implemented on a quantum computer, so as to aid the reader's understanding of table 2.3. In physical terms, a quantum logic gate is simply an operator, utilised as part of an information processing circuit. All the single-qubit gates are written in the Z basis, the two-qubit gates in $\{|\overline{00}\rangle, |\overline{01}\rangle, |\overline{10}\rangle, |\overline{11}\rangle\}$, and the three-qubit gates in $\{|\overline{000}\rangle, |\overline{001}\rangle, |\overline{010}\rangle, |\overline{100}\rangle, |\overline{011}\rangle, |\overline{101}\rangle, |\overline{110}\rangle, |\overline{111}\rangle\}$.

We first introduce the phase-shift gate

$$\hat{R}_\theta = \begin{bmatrix} 1 & 0 \\ 0 & e^{\mathbb{i}\theta} \end{bmatrix} \tag{A.1}$$

The T gate is a specific instance of $\hat{R}_\theta$, for the case where $\theta = \frac{\pi}{4}$ [37]:

$$\hat{T} = \begin{bmatrix} 1 & 0 \\ 0 & e^{\mathbb{i}\frac{\pi}{4}} \end{bmatrix} \tag{A.2}$$

The Clifford group is a non-universal gate set that can be generated by the Hadamard ($\hat{H}$), phase gate ($\hat{S}$), and controlled-NOT (CNOT) [358]:

$$\hat{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad , \quad \hat{S} = \begin{bmatrix} 1 & 0 \\ 0 & \mathbb{i} \end{bmatrix} \quad , \quad \text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{A.3}$$

Like with the T gate, $\hat{S}$ can be viewed as an instantiation of $\hat{R}_\theta$, only this time for $\theta = \frac{\pi}{2}$. Universality is achievable through the addition of a gate from outside the Clifford set to those in equation A.3 [359].

Finally, the Toffoli gate, also known as the controlled-controlled-NOT [360], is defined as

$$\text{CCNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \tag{A.4}$$

APPENDIX $|B\rangle$

APPENDIX TO CHAPTER 2: THE EXPONENTS OF THE COHERENT-STATE BEAM-SPLITTER OUTPUT COMMUTE

$$
\begin{aligned}
\left[\hat{O}_x,\hat{O}_y\right] &= \left[\frac{\alpha_1\left(\hat{a}_3^\dagger+\hat{a}_4^\dagger\right)-\alpha_1^*\left(\hat{a}_3+\hat{a}_4\right)}{\sqrt{2}},\frac{\alpha_2\left(\hat{a}_3^\dagger-\hat{a}_4^\dagger\right)-\alpha_2^*\left(\hat{a}_3-\hat{a}_4\right)}{\sqrt{2}}\right] \\
&= \frac{\alpha_1\left(\hat{a}_3^\dagger+\hat{a}_4^\dagger\right)-\alpha_1^*\left(\hat{a}_3+\hat{a}_4\right)}{\sqrt{2}}\frac{\alpha_2\left(\hat{a}_3^\dagger-\hat{a}_4^\dagger\right)-\alpha_2^*\left(\hat{a}_3-\hat{a}_4\right)}{\sqrt{2}} \\
&\quad - \frac{\alpha_2\left(\hat{a}_3^\dagger-\hat{a}_4^\dagger\right)-\alpha_2^*\left(\hat{a}_3-\hat{a}_4\right)}{\sqrt{2}}\frac{\alpha_1\left(\hat{a}_3^\dagger+\hat{a}_4^\dagger\right)-\alpha_1^*\left(\hat{a}_3+\hat{a}_4\right)}{\sqrt{2}} \\
&= \frac{1}{2}\left(\alpha_1\alpha_2\hat{a}_3^\dagger\hat{a}_3^\dagger-\alpha_1\alpha_2\hat{a}_3^\dagger\hat{a}_4^\dagger-\alpha_1\alpha_2^*\hat{a}_3^\dagger\hat{a}_3+\alpha_1\alpha_2^*\hat{a}_3^\dagger\hat{a}_4+\alpha_1\alpha_2\hat{a}_4^\dagger\hat{a}_3^\dagger\right. \\
&\quad -\alpha_1\alpha_2\hat{a}_4^\dagger\hat{a}_4^\dagger-\alpha_1\alpha_2^*\hat{a}_4^\dagger\hat{a}_3+\alpha_1\alpha_2^*\hat{a}_4^\dagger\hat{a}_4-\alpha_1^*\alpha_2\hat{a}_3\hat{a}_3^\dagger+\alpha_1^*\alpha_2\hat{a}_3\hat{a}_4^\dagger \\
&\quad +\alpha_1^*\alpha_2^*\hat{a}_3\hat{a}_3-\alpha_1^*\alpha_2^*\hat{a}_3\hat{a}_4-\alpha_1^*\alpha_2\hat{a}_4\hat{a}_3^\dagger+\alpha_1^*\alpha_2\hat{a}_4\hat{a}_4^\dagger+\alpha_1^*\alpha_2^*\hat{a}_4\hat{a}_3 \\
&\quad -\alpha_1^*\alpha_2^*\hat{a}_4\hat{a}_4-\alpha_2\alpha_1\hat{a}_3^\dagger\hat{a}_3^\dagger-\alpha_2\alpha_1\hat{a}_3^\dagger\hat{a}_4^\dagger+\alpha_2\alpha_1^*\hat{a}_3^\dagger\hat{a}_3+\alpha_2\alpha_1^*\hat{a}_3^\dagger\hat{a}_4 \\
&\quad +\alpha_2\alpha_1\hat{a}_4^\dagger\hat{a}_3^\dagger+\alpha_2\alpha_1\hat{a}_4^\dagger\hat{a}_4^\dagger-\alpha_2\alpha_1^*\hat{a}_4^\dagger\hat{a}_3-\alpha_2\alpha_1^*\hat{a}_4^\dagger\hat{a}_4+\alpha_2^*\alpha_1\hat{a}_3\hat{a}_3^\dagger \\
&\quad +\alpha_2^*\alpha_1\hat{a}_3\hat{a}_4^\dagger-\alpha_2^*\alpha_1^*\hat{a}_3\hat{a}_3-\alpha_2^*\alpha_1^*\hat{a}_3\hat{a}_4-\alpha_2^*\alpha_1\hat{a}_4\hat{a}_3^\dagger-\alpha_2^*\alpha_1\hat{a}_4\hat{a}_4^\dagger \\
&\quad \left.+\alpha_2^*\alpha_1^*\hat{a}_4\hat{a}_3+\alpha_2^*\alpha_1^*\hat{a}_4\hat{a}_4\right) \\
&= \frac{1}{2}\left(\alpha_1\alpha_2\left[\hat{a}_4^\dagger,\hat{a}_3^\dagger\right]+\alpha_1\alpha_2^*\left[\hat{a}_3,\hat{a}_3^\dagger\right]+\alpha_1\alpha_2^*\left[\hat{a}_3^\dagger,\hat{a}_4\right]+\alpha_1\alpha_2^*\left[\hat{a}_3,\hat{a}_4^\dagger\right]\right. \\
&\quad +\alpha_1\alpha_2^*\left[\hat{a}_4^\dagger,\hat{a}_4\right]+\alpha_1^*\alpha_2\left[\hat{a}_3^\dagger,\hat{a}_3\right]\alpha_1^*\alpha_2\left[\hat{a}_3,\hat{a}_4^\dagger\right]+\alpha_1^*\alpha_2^*\left[\hat{a}_4,\hat{a}_3\right] \\
&\quad \left.+\alpha_1^*\alpha_2\left[\hat{a}_3^\dagger,\hat{a}_4\right]+\alpha_1^*\alpha_2\left[\hat{a}_4,\hat{a}_4^\dagger\right]+\alpha_1^*\alpha_2^*\left[\hat{a}_4,\hat{a}_3\right]+\alpha_2\alpha_1\left[\hat{a}_4^\dagger,\hat{a}_3^\dagger\right]\right)
\end{aligned}
\tag{B.1}
$$

From equation 2.41, $\left[\hat{a}_3,\hat{a}_3^\dagger\right]=\left[\hat{a}_4,\hat{a}_4^\dagger\right]=1$ and $\left[\hat{a}_3^\dagger,\hat{a}_3\right]=\left[\hat{a}_4^\dagger,\hat{a}_4\right]=-1$. We also observe that $\left[\hat{a}_3,\hat{a}_4^\dagger\right]=\left[\hat{a}_4,\hat{a}_3\right]=\left[\hat{a}_3^\dagger,\hat{a}_4\right]=\left[\hat{a}_4^\dagger,\hat{a}_3^\dagger\right]=0$. Therefore,

$$\begin{aligned}\left[\hat{O}_x, \hat{O}_y\right] &= \frac{1}{2}\left(\alpha_1\alpha_2^* - \alpha_1\alpha_2^* - \alpha_1^*\alpha_2 + \alpha_1^*\alpha_2\right) \\ &= 0\end{aligned} \tag{B.2}$$

APPENDIX $|C\rangle$

APPENDIX TO CHAPTER 6: SUMMARISING CIPHERTEXT INDISTINGUISHABILITY

Here, we provide a high-level description of ciphertext indistinguishability, a more formal treatment of which can be found in [361]. In ascending order of security, the three notions to be considered are indistinguishability under chosen plaintext attack (IND-CPA), indistinguishability under non-adaptive chosen ciphertext attack (IND-CCA1), and indistinguishability under adaptive chosen ciphertext attack (IND-CCA2). As can be seen from the definitions below, IND-CCA2 implies IND-CCA1, which implies IND-CPA. However, IND-CPA does not imply IND-CCA1 and neither IND-CPA nor IND-CCA1 imply IND-CCA2. Breaks in the IND-CCA2 security of Rivest–Shamir–Adleman (RSA) implementations have been found in the real world, with widespread applicability [362–364]. As popular countermeasures seem to be ineffective, it has been recommended that key exchanges based around RSA encryption should be deprecated [363]. This will mean reverting to elliptic-curve alternatives so, interestingly, in order to remain secure against classical computers, we will become more vulnerable to quantum attacks.

Definition C.1: IND-CPA. *Eve can encrypt any plaintext she chooses and view the corresponding ciphertext. For public-key cryptography, this is trivially achievable and can be repeated multiple times. After a number of ciphertexts have been generated for the purposes of accumulating information on the encryption scheme, a challenger randomly selects and encrypts one of two non-identical plaintexts chosen by Eve. The encryption scheme has IND-CPA security if Eve's probability of guessing which plaintext was selected is at most* $\frac{1}{2}$ *plus a negligible term.*

Definition C.2: IND-CCA1. *Eve can encrypt any plaintext she chooses and view the corresponding ciphertext. Prior to a challenge being issued, she may also use an oracle to decrypt any ciphertext she chooses and view the corresponding plaintext. After a number of ciphertexts and plaintexts have been generated for the purposes of accumulating information on the encryption scheme, a challenger randomly selects and encrypts one of two non-identical plaintexts chosen by Eve. The encryption scheme has IND-CCA1 security if Eve's probability of guessing which plaintext was selected is at most* $\frac{1}{2}$ *plus a negligible term.*

Definition C.3: IND-CCA2. *Eve can encrypt any plaintext she chooses and view the corresponding ciphertext. She may also use an oracle to decrypt any ciphertext she chooses and view the corresponding plaintext. After a number of ciphertexts and plaintexts have been generated for the purposes of accumulating information on the encryption scheme, a challenger randomly selects and encrypts one of two non-identical plaintexts chosen by Eve. After the ciphertext has been published, Eve can make additional calls to the decryption oracle, provided she does not use it to decrypt the challenge. The encryption scheme has IND-CCA2 security if Eve's probability of guessing which plaintext was selected is at most* $\frac{1}{2}$ *plus a negligible term.*

APPENDIX $|D\rangle$

Appendix to Chapter 7: A Description of the Gluing Process for the Four-Channel Integrated Receiver

Using a syringe, glue was applied to the optical facet of the chip. As this was only 135 ± 15 μm thick, a camera was mounted overhead such that it became clear when the tip of the needle was in the right place, based on how in-focus it was.

Adhesive was dispensed by hand until roughly 80% of the chip edge was coated. To prevent any tremors, both hands were required, so a helper moved the camera while the person performing the gluing progressed along the chip. It was of the upmost importance that the needle itself did not touch the facet, as this would have damaged the spot-size converter, preventing use of the waveguide to which it was connected.

Once a single line of glue had been deposited, the V-Groove array (VGA) was slowly eased backwards and forwards into it, ensuring there were no air gaps. Some of the adhesive naturally overflowed onto the top of the chip, which is unavoidable and harmless in small quantities. However, the interface between the VGA and the waveguides was obscured as a result, so the only way to tell when contact had been made was to watch a fixed point on the chip. When the VGA nudged the edge, this moved a few microns, at which point we stopped. Care should be taken not to cause a larger collision as, again, this would lead to damage.

The next step was to illuminate the interface with a diffuse ultraviolet (UV) lamp, in order to cure the glue. The intensity was slowly increased, rather than going straight to full brightness, as this reduced the risk of misalignment. After 24 hours, the vacuum was turned off, releasing the chuck from the VGA, which was now supported entirely by the adhesive, meaning the chuck could be lowered out of the way. Gluing only commenced for the second VGA after this was complete.

Finally, silicone was used to bond the fibres to the edge of the printed circuit board (PCB), as a way of providing strain relief. The entire package was placed in a biological steriliser, bathing it in

strong UV for a further 24 hours, with a mirror underneath the PCB to ensure the glue was cured from both sides.

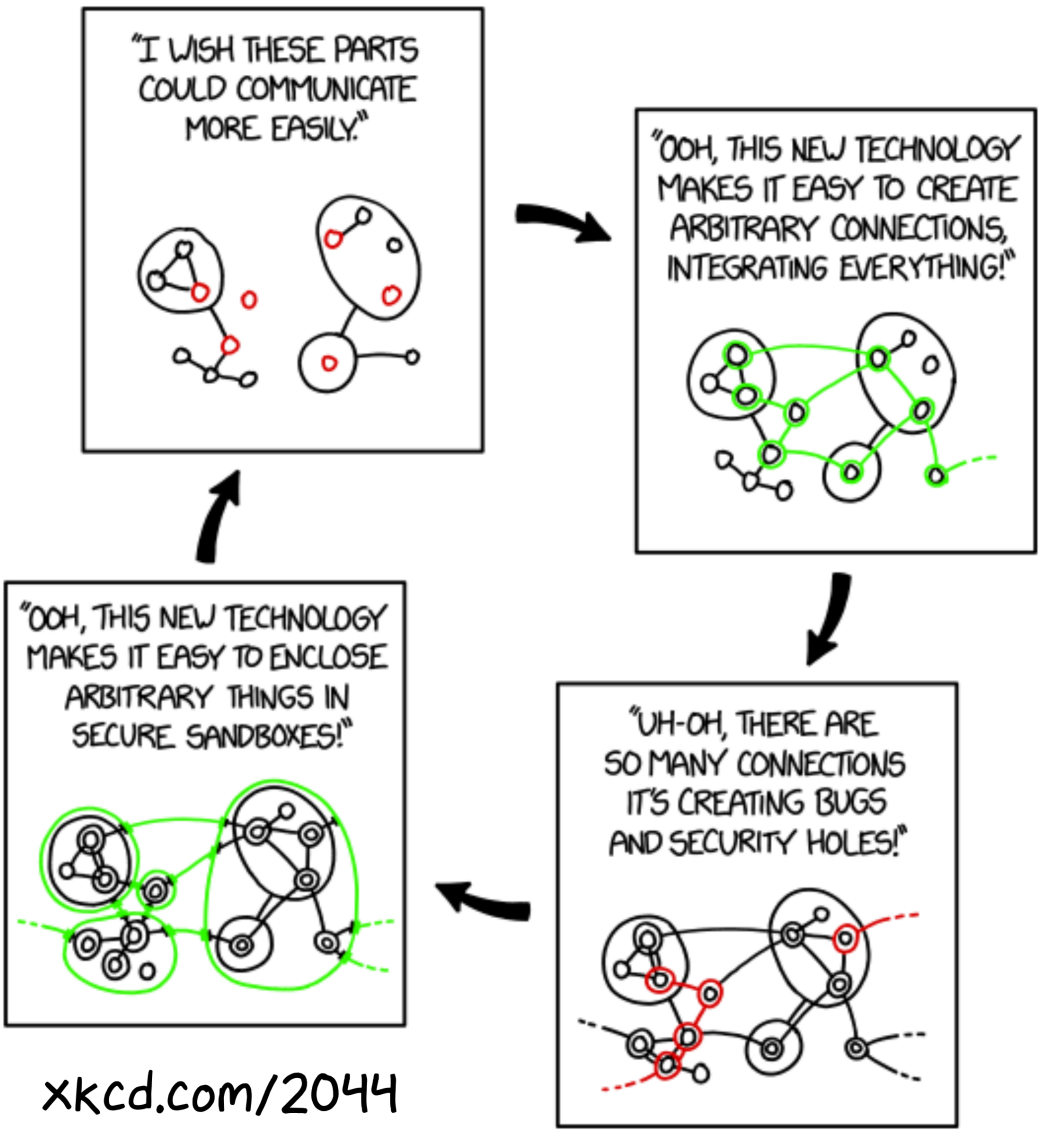
APPENDIX E⟩

Appendix to Chapter 7: Consequences of Tesselating Multiple Silicon Chips on a Single Wafer

All four of the silicon (Si) chips were fabricated alongside other experiments on a single wafer, and figure E.1 shows how they fit together inside the pink hatched design area. While some delay lines do extend beyond this, they fit comfortably into a waveguide-free region behind a colleague's design.

If Big Ear, Cher Ami or Dzakar were to be manufactured individually, the delay lines for each could encircle the rest of the design to reduce its overall footprint. However, this would decrease the length of the multi-moded segments, thus increasing the loss, and affecting state preparation or detection. Such an issue could be resolved if, as in the rest of chapter 7, we were to wavelength-division multiplex several devices, enabling their delay lines to be interleaved similarly to here.

FIGURE E.1: Showing the complete mask for the silicon quantum key distribution devices Anubis, Big Ear, Cher Ami and Dzakar. The pink hatched rectangle is the design area, and the delay lines that extend beyond this sit behind a colleague's design on the same physical chip.



xkcd.com/2044