A prototype of a free-space QKD scheme based on the B92 protocol

A prototype of a free-space QKD scheme based on the B92 protocol

M. Canale, D. Bacco, S. Calimani, F. Renna, N. Laurenti, G. Vallone, P. Villoresi
Department of Information Engineering, University of Padua
{canalema, baccodav, calimani, frarenna, nil, vallone, villoresi}@dei.unipd.it

ABSTRACT

We describe the architecture of *QuAKE (Quantum Advanced Key Exchanger)*, an experimental setup for quantum key distribution (QKD) over a free-space quantum channel based on the B92 protocol [1]. The system consists of a transmitter (Alice) and a receiver (Bob) that are connected through a free-space quantum channel over a distance of approximately 50 m, and are each driven by a field-programmable gate array (FPGA). The raw key shared by Alice and Bob is processed in four subsequent steps (i.e., sifting, channel estimation, key reconciliation and privacy amplification) which are implemented in Matlab. Finally, public discussion is implemented with the user datagram protocol (UDP) transport protocol running over the Internet protocol (IP) network protocol, while 802.11g underlies the physical layer transmission.

Categories and Subject Descriptors

C.2.0 [**Computer-communication networks**]: General—*Security and protection*; E.3 [**Data**]: Data encryption

General Terms

Security

Keywords

QKD, quantum cryptography, B92 protocol, free-space quantum channel

1. INTRODUCTION

Quantum cryptography, or more precisely QKD, represents a valuable tool to share unconditionally secure keys between nodes in a network by leveraging the fundamental laws of quantum mechanics. In particular, the no-cloning theorem and the characteristics of quantum measurements offer to legitimate nodes the possibility of detecting eavesdropping attacks with high statistical confidence. The key material obtained from the quantum channel is then processed during a public discussion stage performed over a noiseless, authenticated, public channel. In this phase, results on classical information-theoretic analysis are used in order to design algorithms that ensure the reliability and security of the key-sharing protocol.

When moving from the theoretical formulation of the problem to the actual implementation of a QKD system, the effects introduced by the transmission channel and the non-idealities in the devices must be taken into account in order to limit possible ensuing security flaws and devise proper countermeasures. In the last years, experimental and practical implementations of QKD systems have been deployed over optical fiber links (the DARPA [2] and the SECOQC [3] QKD networks are arguably the best known), and even commercial solutions are nowadays available. More recently, free-space QKD systems have gathered a growing interest. The advantages of such solutions lie in increased flexibility and lower costs for deploying the actual physical link. Moreover, free-space QKD seems the only possible solution to provide perfectly secure satellite-to-satellite and ground-to-satellite communication channels.

Some implementations of free-space QKD architectures can already be found in the literature. For example, in [4] a 10 km, free-space, QKD system based on the BB84 protocol has been made operative in both daylight and night conditions. Another example of such systems is presented in [5], in which a laboratory setup for free-space QKD has been deployed and his performance results are collected in terms of sifted key rate and relative quantum bit error rate (QBER). In [6] a free-space QKD system was able to cover the distance of 144 km by using *decoy states* [7] to effectively protect transmission from photon number splitting (PNS) attacks.

The remainder of the paper is organized as follows. Section 2 describes the qubit transmission format used and the attack models considered. Section 3 explains the processing steps and public communication needed for distillation of the secure keys, while Section 4 provides results of our experimental testing.

2. QUANTUM PHYSICAL LAYER

2.1 Transmission setup and protocol

The optical setup for our prototype is shown in Fig. 1 The transmitter (Alice) uses two infrared (850 nm) attenuated diode lasers to send the bits 0 and 1, encoded in the vertical $|\updownarrow\rangle$ and +45° linear $|\nearrow\rangle$ polarization of the photons, respec-

ISABEL '11, October 26–29, Barcelona, Spain

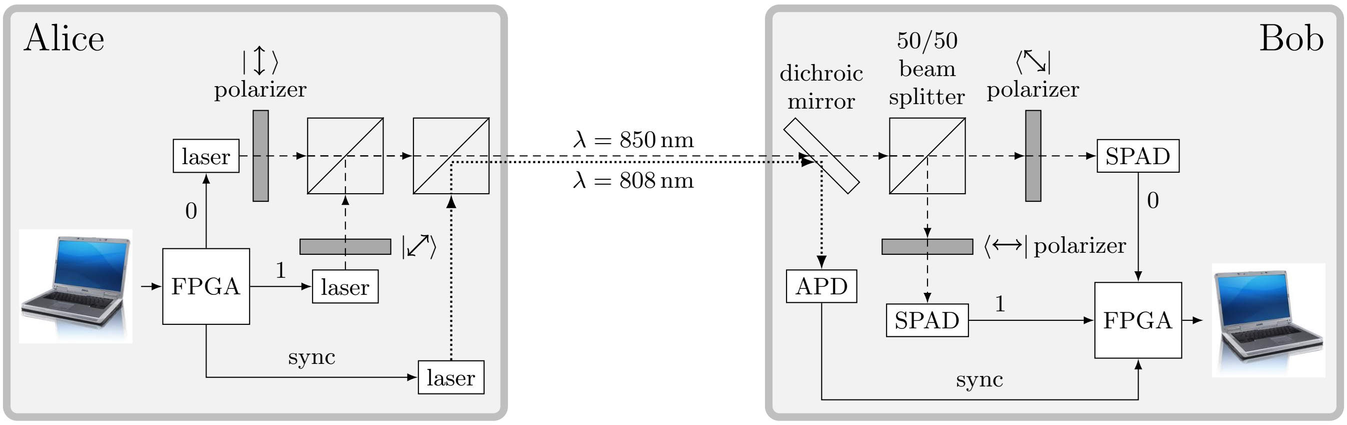

Figure 1: Schematic representation of our optical setup

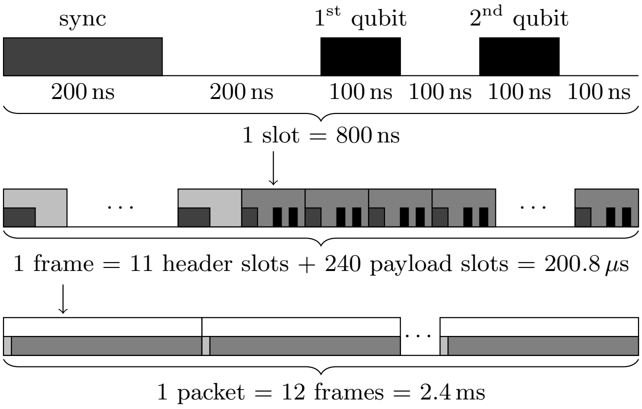

Figure 2: Data frame structure

tively. A 808 nm laser beam is also used along for synchronization. The receiver (Bob) uses a dichroic mirror (DM) to separate the information qubits from the synchronization signal: the latter is reflected and detected by an avalanche photodiode, whereas the qubits, trasmitted by the DM, impinge on a 50/50 beam splitter (BS). On either output of the BS, a polarizer and a single photon avalanche photodiode (SPAD) detect the −45° linear ⟨⤡| or horizontal ⟨↔| polarization photons respectively. Each click of either SPAD corresponds to the reception of a sifted 0 or 1, respectively.

The transmitted data structure is shown in Fig. 2. A raw key of 288 kbit is divided into 50 packets of 5760 bits each, which are in turn divided into 12 frames for the ease of synchronization. In fact, each frame consists of 11 header slots and 240 payload slots, each with a duration of 800 ns. The header exhibits the pattern '100000xxxx1', where 'xxxx' is the 4-bit frame number, encoded one bit per slot in a pulse-duration modulation of the synchronization beam (a 400 ns or 200 ns pulse encode the bit 1 or 0, respectively). As regards the payload slots, the first 200 ns are used to send the synchronization beam, then, after the synchro-laser, Alice waits 200 ns and then sends two bits separated by 200 ns. The resulting raw key rate is therefore upper bounded as $R_{\mathrm{raw}} \leq 2.39\,\mathrm{Mbit/s}$.

The measured sifted key rate R_{sift} allows to estimate the total loss along the source / channel / detector chain $\alpha = R_{\mathrm{sift}}/R_{\mathrm{raw}}$. This includes also the fraction of pulses that carry no photons, due to the Poissonian statistics of the faint source, and the B92 protocol efficiency $\eta = 1/4$.

2.2 Attack model

We consider selective individual attacks, where Eve measures each photon independently with probability $0 < q < 1$, using either basis, (⟨↔|, ⟨↕|) or (⟨⤢|, ⟨⤡|), randomly chosen. In the *intercept and resend (IS)* attack [8], each measured bit is resent with the same encoding as used by Alice, thus increasing the error rate at Bob. In particular, observe that by considering Alice and Bob's sifted keys as input and output, respectively, the quantum channel can be modeled as a binary symmetric channel (BSC) with some error probability ε. When a single qubit is observed by Eve according to an IS attack, the error probability at Bob for the corresponding bit is set to 1/4 due to the random and independent choice of the basis used by Alice and Eve. More precisely, it was shown in [9] that 1/4 is a lower bound on the error probability induced by the IS attack, for any basis chosen by the eavesdropper to measure the incoming qubits and resend them to Bob. Hence, an individual IS attack with probability q increases the QBER value to

$$\varepsilon' = (1-q)\varepsilon + \frac{1}{4} = \varepsilon + q\left(\frac{1}{4} - \varepsilon\right), \tag{1}$$

whereas it is conservatively assumed to leave channel losses unaffected.

On the other hand, in the *unambiguous state discrimination (USD)* attack [10] only the 0's that are measured with the (⟨⤢|, ⟨⤡|) basis and the 1's that are measured with the (⟨↔|, ⟨↕|) basis are retransmitted to Bob, thereby introducing further losses at the legitimate receiver but no additional errors. When a qubit is observed by Eve and resent according to the USD scheme, the random choice of the basis introduces a further loss factor of 1/4. Hence, individual USD attacks with probability q increase channel losses to the value

$$\alpha' = (1-q)\alpha + q\frac{\alpha}{4} = \alpha - \frac{3}{4}q\alpha. \tag{2}$$

We also consider the *PNS* attack [11]. In this case, qubits carried by two or more photons might be observed by Eve without introducing any effect at Bob's receiver. However, since this attack can only be successfully carried out on multiple photon bits, the probability that one bit of the sifted key is observed by the adversary is upper bounded by

$$q_{\mathrm{PNS}} \leq P[n_{\mathrm{ph}} > 1 | n_{\mathrm{ph}} > 0] = \frac{1 - e^{-\mu}(1+\mu)}{1 - e^{-\mu}}. \quad (3)$$

where n_{ph} is the number of photons in a generic bit at the transmitter output, that is Poisson distributed with mean μ.

Eventually, in considering with the above attacks for the purpose of privacy amplification we will upper bound the amount of information available the eavesdropper with what she would get by correctly detecting all the observed qubits.[1]

3. KEY PROCESSING ALGORITHMS

3.1 Channel estimation

In each round of the key-agreement protocol, Bob sends the positions of the received qubits over the public channel and discloses the value of a fraction of them, in order to allow the transmitter to estimate the channel losses and the QBER. The objective of channel estimation is twofold: it predicts losses and the error rate introduced by the noisy quantum channel in order to properly perform the *key reconciliation* stage. Moreover, it is used to reveal the presence of an eavesdropper,that is, to determine the probability q that a photon has been observed by Eve, according to the attack schemes described in Section 2.2. A miss detection probability lower than P_{miss} is assured, where the miss detection event represents the case in which Eve is observing on average more photons than the number predicted by the channel estimation protocol.

The QBER is estimated at each round by randomly choosing N_{qber} bits from the sifted key to be disclosed over the public channel. Then, the maximum likelihood (ML) estimate of ε is simply defined as

$$\varepsilon_{\mathrm{ML}} = \frac{1}{N_{\mathrm{qber}}} \sum_{i=1}^{N_{\mathrm{qber}}} e_i, \quad (4)$$

where $e_i = 1$ if there is an error in the corresponding bit of the publicly disclosed portion of the sifted key, and $e_i = 0$ otherwise. Then, the estimator $\varepsilon_{\mathrm{ML}}$ is a random variable that exhibits a different statistical description conditioned on the fact that an adversary is implementing the IS attack or not. More in details, the mean and standard deviation of $\varepsilon_{\mathrm{ML}}$ are given by

$$m_{\mathrm{ML}} = \varepsilon \quad , \quad \sigma_{\mathrm{ML}} = \sqrt{\frac{\varepsilon(1-\varepsilon)}{N_{\mathrm{qber}}}}. \quad (5)$$

when the photons sent by Alice are not measured by any eavesdropper, whereas

$$m'_{\mathrm{ML}} = \varepsilon' \quad , \quad \sigma'_{\mathrm{ML}} = \sqrt{\frac{\varepsilon'(1-\varepsilon')}{N_{\mathrm{qber}}}}. \quad (6)$$

when the system is subject to an IS attack. In order to be able to reveal the presence of an eavesdropper that is carrying IS attacks with a given probability q_{IS}, the legitimate parties guarantee that the number of qubits used for QBER estimation is high enough to discriminate the case in which the BSC error probability is ε or ε'. In other words, it must hold

$$m_{\mathrm{ML}} + \beta\sigma_{\mathrm{ML}} < m'_{\mathrm{ML}} - \beta\sigma'_{\mathrm{ML}}, \quad (7)$$

with β denoting an appropriate multiplicative factor that determine the confidence interval of the QBER estimate. For the sake of tractability, we approximate the random variable $\varepsilon_{\mathrm{ML}}$ with a Gaussian random variable with same mean and same standard deviation. Then, it is possible to guarantee a miss detection probability up to $P_{\mathrm{miss}} = 5 \cdot 10^{-3}$ by imposing

$$\beta = Q^{-1}(P_{\mathrm{miss}}) \approx 2.6, \quad (8)$$

with $Q^{-1}(\cdot)$ denoting the inverse of the Q-function, $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp\left(-\frac{u^2}{2}\right) du$. Then, on substituting (1), (5) and (6) in (7), after simple algebraic manipulations, it is possible to determine the maximal undetectable IS attack probability as a function of the parameter N_{qber}, namely

$$q_{\mathrm{IS}} = \frac{\left(\frac{1}{4} - \varepsilon\right) \cdot \left(2\beta\sqrt{\frac{\varepsilon(1-\varepsilon)}{N_{\mathrm{qber}}}} + \frac{\beta^2}{N_{\mathrm{qber}}}\right) + \frac{\beta^2}{N_{\mathrm{qber}}}\left(2\varepsilon^2 - \frac{\varepsilon}{2}\right)}{\left(\frac{1}{4} - \varepsilon\right)^2 - \frac{\beta^2}{N_{\mathrm{qber}}}\left(\frac{\varepsilon}{2} - \varepsilon^2 - \frac{1}{16}\right)}. \quad (9)$$

On assuming that all the errors introduced by the quantum channel are corrected during the key reconciliation phase, the QBER estimate can also be refined at Bob by counting the number of bits that are flipped after reconciliation. In this way, it is possible to decrease the maximal undetectable IS attack probability to the value obtained by substituting N_{qber} with N_{sift} in (9).

Analogously, channel losses are estimated by counting all Bob's sifted bits. Similarly to the case for the QBER estimation, the ML estimator for channel losses is obtained as

$$\alpha_{\mathrm{ML}} = \frac{1}{N_{\mathrm{raw}}} \sum_{i=1}^{N_{\mathrm{raw}}} a_i, \quad (10)$$

where $a_i = 1$ for the indexes corresponding to bits in the raw key that made Bob's detectors click, and $a_i = 0$ otherwise. Again, the channel losses estimator α_{ML} is a random variable with mean and standard deviation given by

$$m_{\mathrm{ML}} = \alpha \quad , \quad \sigma_{\mathrm{ML}} = \sqrt{\frac{\alpha(1-\alpha)}{N_{\mathrm{raw}}}}, \quad (11)$$

or

$$m'_{\mathrm{ML}} = \alpha' \quad , \quad \sigma'_{\mathrm{ML}} = \sqrt{\frac{\alpha'(1-\alpha')}{N_{\mathrm{raw}}}}, \quad (12)$$

depending on the presence of an eavesdropper carrying a USD attack. By following closely similar steps to those used

[1] Selective individual attacks were shown in [9] to provide Eve the correct value of each transmitted bit with probability at most $(2+\sqrt{2})/4$. This is the case when the eavesdropper is measuring the observed qubits with the Breidbart basis [12].

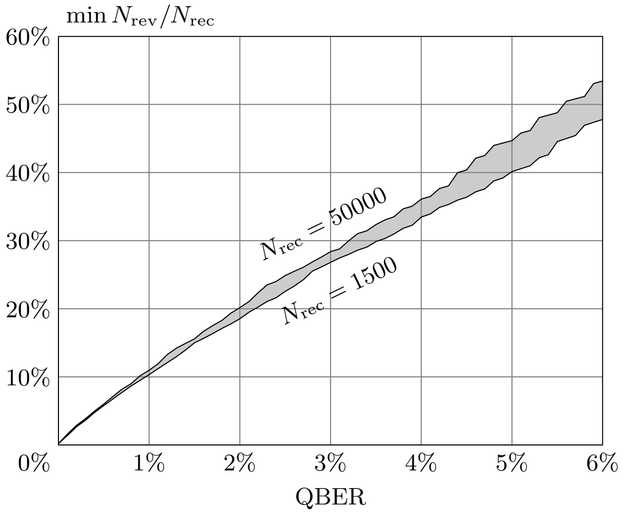

Figure 3: Minimum number of bits that need to be revealed over the public channel in the Winnow key reconciliation scheme, versus channel QBER. Here the target $P_{\text{fail}} = 0.02$ and curves are drawn for two different sifted key lengths.

to determine q_{IS} in (9), the maximal undetectable USD attack probability can be found as

$$q_{\text{USD}} = \frac{\frac{3}{2}\beta\left(\sqrt{\frac{\alpha(1-\alpha)}{N_{\text{raw}}}} - \left(\frac{1}{2}-\alpha\right)\frac{\beta}{N_{\text{raw}}}\right)}{\frac{9}{16}\alpha\left(1+\frac{\beta^2}{N_{\text{raw}}}\right)}. \tag{13}$$

3.2 Key reconciliation

Errors introduced on the sifted key by the quantum channel (polarization degradation due to the atmosphere, noise in the devices, etc) are corrected by implementing the Winnow scheme [13]. The probability of a reconciliation failure is kept below a fixed value P_{fail}, by guaranteeing a residual BER on the reconciled key smaller than $P_{\text{fail}}/N_{\text{rec}}$, where $N_{\text{rec}} = N_{\text{sift}} - N_{\text{qber}}$ is the number of sifted . Given these constraints, the number of iterations of the protocol and the block sizes for parity checking are chosen to minimize the number of bits N_{rev} revealed over the public channel.

As an example, for QBER = 3%, $P_{\text{fail}} = 0.02$ and $N_{\text{rec}} = 15000$, we choose 4 iterations with increasing block sizes $8, 32, 128, 512$, respectively. As can be seen from Fig. 3, this choice leads to approximately $N_{\text{rev}} = 0.29N_{\text{rec}}$.

3.3 Privacy amplification

The reconciled keys at Alice and Bob are compressed following a two steps procedure aiming at reducing the information leakage to Eve to the target value $I_{\text{tar}} = 1$ bit per key. First, N_{rev} out of the $N_{\text{rec}} = N_{\text{sift}} - N_{\text{qber}}$ bits of the reconciled key are deleted according to the procedure of *bit deletion* described in [13, Section 3], in order to eliminate the information revealed over the public channel to perform key reconciliation. In this way, the information leaked to the eavesdropper during the key reconciliation stage is reduced exactly to zero, as can be shown by applying [14, Proposition 1].

After bit deletion, privacy amplification is obtained by hashing with a full column rank, random, binary Toeplitz matrix [15], renewed at each round. The number of rows in the Toeplitz matrix is a design parameter for this phase of the key processing, depending on the amount of information on the key that Eve is estimated to have gathered during the previous stages of the protocol.

For instance, the system described in [16] complies with two different methods in estimating the information gathered by Eve with IS attacks. One method is due to Bennett [9] and it links the number of errors revealed after key reconciliation with the information gained by the eavesdropper. More precisely, on denoting with e the total number of errors revealed on the sifted key, the information leaked to the eavesdropper is approximated by the value

$$\frac{4e}{\sqrt{2}} + \beta\sqrt{(4+\sqrt{2})e}, \tag{14}$$

in which the confidence margin was chosen as $\beta = 5$. A second estimate, provided in [17] defines an upper bound on Eve's Renyi entropy in the limit of long transmissions, that is when $N_{\text{sift}} \to \infty$. Then, the information leakage due to multiphoton pulses is handled separately, and added to the previous quantity.

On the other hand, in our experiment, according to the three attack models and the channel estimation scheme described in the previous sections, each bit in the reconciled key is assumed to have been observed by the eavesdropper with probability not larger than $q_{\text{tot}} = q_{\text{IS}} + q_{\text{USD}} + q_{\text{PNS}}$, independently from the others. Then Eve's Renyi information on the reconciled key is a binomially distributed random variable $t \sim \mathcal{B}(N_{\text{rec}} - N_{\text{rev}}, q_{\text{tot}})$, and we can use the results in [18] to determine a probabilistic upper bound on the information I_{leak} leaked to Eve after privacy amplification. In fact, with probability at least $1 - P_{\text{miss}}$, it is

$$I_{\text{leak}} \leq I_{\text{tar}}(N_{\text{sec}}, b) = N_{\text{sec}}\,\text{P}\left[t > b\right] + \frac{1}{2^{(N_{\text{rec}}-N_{\text{rev}}-N_{\text{sec}}-b)}\ln 2}, \tag{15}$$

for any value of b, and with N_{sec} denoting the length of the secure key at the output of the privacy amplification stage. Under the constraint that $I_{\text{leak}} < \delta$ be assured, the secure key rate is thus maximized by choosing

$$N_{\text{sec}} = \max\left\{a \,:\, \min_b I_{\text{tar}}(a,b) \leq \delta\right\}$$

3.4 Authentication and transmission over the public channel

In our prototype, communication on the public discussion channel between Alice and Bob is implemented with UDP over IP, and by means of 802.11g wireless transmissions. Therefore no security services are leveraged other than the unconditionally secure authentication we provide at the application layer.

The concatenation of all messages transmitted by a terminal in a protocol round is hashed by means of a keyed function to a 100 bit tag, which is then XORed with a one time pad (OTP). The hash function is chosen from the Stinson ε-almost strongly universal$_2$ class [19], and is renewed every 25 rounds. The hashing key and the OTP altogether require

Transmission parameters	
packet rate	$R_{\text{ptk}} = 12.5\,\text{pkt/s}$
raw key rate	$R_{\text{raw}} = 72\,\text{kbit/s}$
Channel parameters	
overall loss rate	$\alpha = 6.4 \cdot 10^{-2}$
quantum bit error rate	$\varepsilon = 2.1 \cdot 10^{-2}$
sifted key rate	$R_{\text{sift}} = 4.6\,\text{kbit/s}$
undetected eavesdropper rate	$q_{\text{tot}} < 0.41$
Security parameters	
secret key rate	$R_{\text{sk}} = 600\,\text{bit/s}$
prob. of failed reconciliation	$P_{\text{fail}} < 0.02$
information leakage rate	$R_{\text{leak}} \leq 0.2\,\text{kbit/s}$
prob. of higher leakage	$P_{\text{miss}} < 5 \cdot 10^{-3}$

Table 1: Performance measurements at the Palazzo della Ragione experiment

250 secure bits per round, that are taken from the previously generated keys, thus lowering the *net key rate.*

4. EXPERIMENTAL RESULTS

Our prototype was publicly demonstrated on October 3-4, 2011 at Palazzo della Ragione in Padua with indoor daylight conditions over a 50 m distance along the south wall of the Great Hall. It was kept up and running for 5 hours on October 3rd, and for 8 hours on October 4th. Along with the key agreement procedure the two terminals carried out the secure exchange text messages and images provided by guests and visitors over a wireless radio link. The distilled secure keys were used for OTP encryption and decryption at the transmitted and receiver side, respectively. As for the communication, we employed the transport control protocol (TCP) over IP and IEEE 802.11g wireless transmission.

The measured performance parameters for the QKD system in the setting are summarized in Tab. 1.

5. CONCLUSIONS

We have described a prototype system for free-space QKD, that employs the two-state B92 protocol, thus requiring only two laser sources and two single photon detectors. The key distillation processing was properly designed to thwart selective individual attacks that might be undetected, leaving the eavesdropper with only negligible information on the keys. The prototype has been publicly demonstrated, yielding continuous operation for hours.

6. ACKNOWLEDGEMENTS

This work was supported by the University of Padua under Project *QuantumFuture* (prot. STPD08ZXSJ)

7. REFERENCES

[1] C. H. Bennett, “Quantum cryptography using any two nonorthogonal states,” *Phy. Rev. Lett.*, vol. 68, no. 21, pp. 3121–3124, May 1992.

[2] C. Elliott, “Building the quantum network,” *New Journal of Physics*, vol. 4, no. 1, pp. 46.1–46.12, Jul. 2002.

[3] R. Alléaume *et al.*, “SECOQC White Paper on Quantum Key Distribution and Cryptography,” *ArXiv*, pp. 1–28, Jan. 2007, Arxiv preprint: arXiv:quant-ph/0403065v2.

[4] R. Hughes, J. Nordholt, D. Derkacs, and C. Peterson, “Practical free-space quantum key distribution over 10 km in daylight and at night,” *New J. Phys.*, vol. 43, no. 4, July 2002.

[5] Y.-S. Kim, Y.-C. Jeong, and Y.-H. Kim, “Implementation of polarization-coded free-space bb84 quantum key distribution,” *Laser Physics*, vol. 18, no. 6, pp. 810–814, June 2008.

[6] T. Schmitt-Manderbach *et al.*, “Experimental demonstration of free-space decoy-state quantum key distribution over 144 km,” *Phy. Rev. Lett.*, vol. 98, no. 010504, pp. 1–4, January 2007.

[7] H.-K. Lo, X. Ma, and K. Chen, “Decoy State Quantum Key Distribution,” *Physical Review Letters*, vol. 94, no. 23, 2005.

[8] B. Huttner, N. Imoto, N. Gisin, and T. Mor, “Quantum cryptography using any two nonorthogonal states,” *Phy. Rev. Lett.*, vol. 51, no. 3, pp. 1863–1869, March 1992.

[9] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, “Experimental quantum cryptography,” *J. Cryptology*, vol. 5, no. 1, pp. 3–28, 1992.

[10] M. Dušek, M. Jahma, and N. Lütkenhaus, “Unambiguous state discrimination in quantum cryptography with weak coherent states,” *Phy. Rev. A*, vol. 62, no. 022306, pp. 1–9, July 2000.

[11] N. Lütkenhaus, “Security against individual attacks for realistic quantum key distribution,” *Phy. Rev. A*, vol. 61, no. 052304, pp. 1–9, April 2000.

[12] C. H. Bennett, G. Brassard, S. Breidbard, and S. Wiesner, “Quantum cryptography, or unforgeable subway tokens.” in *Advances in Cryptology: Proceedings of CRYPTO ’82*, 1982, pp. 267–275.

[13] W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. H. Nickel, C. H. Donahue, and C. G. Peterson, “Fast, efficient error reconciliation for quantum cryptography,” *Phy. Rev. A*, vol. 67, no. 052303, pp. 1–9, May 2003.

[14] M. Canale, F. Renna, and N. Laurenti, “QKD secrecy for privacy amplification matrices with selective individual attacks,” in *Proc. QCRYPT 2011*, Zurich, Switzerland, September 2011.

[15] C.-H. Fung, X. Ma, and H. F. Chau, “Practical issue in quantum-key-distribution postprocessing,” *Phy. Rev. A*, vol. 81, no. 012318, pp. 1–9, January 2010.

[16] C. Elliott, D. Pearson, and G. Troxel, “Quantum cryptography in practice,” in *ACM SIGCOMM*, 2003, pp. 227–238.

[17] B. Slutsky, R. Rao, P. Sun, L. Tancevski, and S. Fainman, “Defense frontier analysis of quantum cryptographic systems,” *Applied Optics*, vol. 37, no. 14, pp. 2869–2878, 1998.

[18] C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, “Generalized privacy amplification,” *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, November 1995.

[19] D. R. Stinson, “Universal hashing and authentication codes,” *Designs, Codes and Cryptography*, vol. 4, no. 369, 1994.