Security and Entanglement in Differential-Phase-Shift Quantum Key Distribution

by

Adriana Marais

Submitted in fulfillment of the academic requirements for the degree of
Master of Science in the School of Physics,
University of KwaZulu-Natal, Durban

November, 2009

As the candidate's supervisor I have approved this dissertation for submission.

Signed: _____ Name: _____ Date: _____

Signed: _____ Name: _____ Date: _____

Abstract

Quantum key distribution (QKD) aims at the creation of a secret key in the two locations of partners, traditionally Alice and Bob, wishing to communicate in private. A generic QKD protocol utilises a quantum channel and an authenticated classical channel for exchanges between partners in Phases 1 and 2 of the protocol, respectively. Phase 1 can be described as a prepare-and-measure (P&M) or equivalently as an entanglement-based (EB) phase. Bob performs the same measurement in both descriptions. Subsequent to measurement, Phase 2 is commenced, the aim of which is to distill a secret key from the measurement outcomes resulting from Phase 1.

A necessary condition for the security of a QKD protocol is that the measurement performed by Bob in Phase 1 must be described by non-commuting POVM elements. One method of proving the unconditional security of a QKD protocol is to show that the complete protocol (including Phases 1 and 2) is equivalent to an entanglement distillation protocol. A first step towards showing such an equivalence for a given P&M QKD protocol is to describe an EB translation of Phase 1, where the condition on Bob's measurement is met.

Differential-phase-shift (DPS) QKD is a member of the class of distributed-phase-reference QKD protocols. Unconditional security proofs for this class of protocols do not yet exist. Phase 1 of DPSQKD is here described and formalised as both a P&M and an EB phase, and Bob's measurement is shown to be described by non-commuting POVM elements. This description of an equivalent EB translation of DPSQKD where the condition on Bob's measurement is met, is a first step towards a potential unconditional security proof for the protocol based on entanglement distillation.

Preface

The work described in this dissertation was carried out in the School of Physics, University of KwaZulu-Natal, Durban, from February 2007 to November 2009, under the supervision of Professor Francesco Petruccione and Professor Thomas Konrad.

These studies represent original work by the author and have not otherwise been submitted in any form for any degree or diploma to any tertiary institution. Where use has been made of the work of others it is duly acknowledged in the text.

Declaration 1- Plagiarism

I, _____ declare that

i. The research reported in this thesis, except where otherwise indicated, is my original research.

ii. This thesis has not been submitted for any degree or examination at any other university.

iii. This thesis does not contain other persons' data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.

iv. This thesis does not contain other persons' writing, unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then:
a. Their words have been re-written but the general information attributed to them has been referenced;
b. Where their exact words have been used, their writing has been placed inside quotation marks, and referenced.

v. This thesis does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the source being detailed in the thesis and in the References sections.

Signed: _____

Declaration 2- Publications

Publication 1

A. Marais, T. Konrad and F. Petruccione, "Security and Entanglement in Differential-Phase-Shift Quantum Key Distribution" (2009).

(submitted)

Signed: _____

Acknowledgements

I would like to thank my supervisors Professor Francesco Petruccione and Professor Thomas Konrad for all of their help, advice and support during these studies, and in particular for encouraging, participating in, and facilitating all the discussions without which this work would not have been possible.

This research is supported by the South African Research Chair Initiative of the Department of Science and Technology and National Research Foundation.

Contents

Chapter 1

Introduction

"Two can keep a secret if one is dead."

- Unknown

1.1 The problem of secure communication

Communication is the transfer of information from one location to another. Given the requirement of secure communication, (one aspect of) cryptography emerged as the study of transforming the information to be transferred such that it is intelligible only to those in possession of additional knowledge, referred to as a *key*.

An example of such a transformation is the encryption of binary information (information stored in *binary digits*, or *bits*, which can take the value 0 or 1) by modulo 2 addition to a binary key. Shannon showed in 1949 [1] that if the binary key is *truly random* (see Sec. 4.3.1), the same length as the message and used only once, then the encrypted message contains absolutely no information about the actual message. This algorithm, known as the *one-time pad* (see Sec. 2.2) [2], is the only provably secure encryption algorithm known to date.

The problem of secure communication thus becomes the problem of distributing a provably secret, truly random binary key of specified length, for each transfer of information between communicating parties, traditionally

called Alice and Bob. But distributing the key must involve a transfer of information between Alice and Bob, so has any headway towards a solution really been made? There are two important differences between the problems of secure communication and secure key distribution.

Firstly, access by an eavesdropping adversary, traditionally Eve, to key information cannot be prevented by encryption *again*; the information must be protected by other means.

Secondly, the requirement of no possible access to information by Eve can be relaxed to a requirement of no possible undetected access, since the key contains no information about the message itself, and if compromised can be redistributed.

The problem is thus reduced to a search for a courier of key information that can be trusted to report eavesdropping in all cases.

1.2 The photon as a courier of information

'Information is physical' [3] because inevitably information is represented in physical systems. Light is a natural candidate as a carrier of information in classical communications, owing to its propagation speed, neutral charge and bosonic nature, which means bits can be encoded in large average amplitudes of light pulses created at one location, then transferred and detected at another.

However, since 1900 when Planck [4] proposed that radiation is emitted and absorbed in discrete quanta to account for the electromagnetic spectra of thermal bodies, it became clear that a classical wave theory of light, although adequately able to account for the observed properties of light beams, was insufficient. Although the word *photon* was later coined by Lewis [5] as 'not light', but a 'carrier of radiant energy' between atoms, it was Einstein who first understood these light quanta to be representative of light itself, thereby explaining the photoelectric effect [6].

In the years 1927-1932 Fermi and Dirac (amongst others) developed the contemporary conception of the photon (see [7], [8] and Sec 5.1), as a fundamen-

tally quantum object thus subject to the laws of quantum mechanics. Now the task is the investigation of the implications of representing information in quantum systems such as photons.

1.3 The counter-intuitive behaviour of elementary particles

Elementary particles obey the laws of quantum mechanics with some counter-intuitive results. In the language of quantum mechanics, an elementary particle is completely described by a quantum state (see Sec. 4.1), usually written in *Dirac notation* [9] as $|\psi\rangle$. Subsequent to a measurement being performed on the particle, the particle takes the result of the measurement as a state regardless of the actual initial state. Thus, in general, quantum measurement (see Sec. 4.3) can be seen as destructive since information about the original state is lost.

This means that eavesdropping (a quantum measurement) generally results in a destruction of information, which is detectable owing to a non-correspondence between an initial state $|\psi\rangle$, and resulting state $|\gamma\rangle$.

Returning to the consideration that information is represented in physical systems, and that the required physical system here is one that can be trusted to report eavesdropping in all cases, it seems quantum couriers are ideal nominees.

It remains to describe how information, here specifically a random binary string which will constitute a possible key, may be represented in elementary particles such as photons.

1.4 Encoding random bits in quantum couriers

In classical information theory, the unit of information is the bit, or the set $\{0, 1\}$. Moving to a quantum representation, an example of a two-level quantum system is the polarisation of a photon. Such a two-level quantum

system, termed a qubit, is the unit of information in quantum information theory (see Sec. 4.2). A qubit is described by two complex numbers as the set

$$\{\alpha|0\rangle \ + \ \beta|1\rangle \ : \ |\alpha|^2 \ + \ |\beta|^2 \ = \ 1, \ \alpha, \beta \in \mathbb{C}\}$$

where $|0\rangle$ and $|1\rangle$ correspond to two orthogonal states in a quantum system, and are the quantum representation of the classical 0 and 1. For example, $|0\rangle$ and $|1\rangle$ can correspond to horizontal and vertical photon polarisations, respectively. For α and β both non-zero, there are a multitude of corresponding qubit states, for which the qubit is said to be in a *superposition* of the states $|0\rangle$ and $|1\rangle$. Examples of such states are $|+\rangle$ and $|-\rangle$ given by

$$|+\rangle \ = \ \frac{1}{\sqrt{2}}|0\rangle \ + \ \frac{1}{\sqrt{2}}|1\rangle, \tag{1.1}$$

$$|-\rangle \ = \ \frac{1}{\sqrt{2}}|0\rangle \ - \frac{1}{\sqrt{2}}|1\rangle. \tag{1.2}$$

The usefulness of encoding information in qubits depends on how effectively the information can be decoded. But first, a discussion of non-orthogonality is required.

1.5 Non-orthogonal quantum states

Two qubit states $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and $|\gamma\rangle = \alpha'|0\rangle + \beta'|1\rangle$ are said to be *orthogonal* (or have an inner product of zero, see Sec. 4.1 and 4.2) if and only if

$$\alpha^*\alpha' + \beta^*\beta' = 0. \tag{1.3}$$

It can thus be shown that as well as $|0\rangle$ and $|1\rangle$, the states $|+\rangle$ and $|-\rangle$ are orthogonal, while other pairs of states giving a non-zero outcome to Eq. (1.3) are said to be non-orthogonal.

There exists a quantum measurement to discern two orthogonal quantum states. For example, if Alice sends the classical bit 0 or 1 encoded as $|0\rangle$ or $|1\rangle$, respectively, both Eve and Bob can perform a measurement on that qubit, and determine the value of the initial classical bit. This measurement will always have an outcome of $|0\rangle$ or $|1\rangle$, therefore let this measurement be called the '$|0\rangle, |1\rangle$' measurement. However, if Alice sometimes encodes 0 or

1 as $|+\rangle$ or $|-\rangle$, respectively, and if Eve and Bob perform the same measurement as in the case above, the '$|0\rangle, |1\rangle$' measurement, then as described previously the qubit will take the result of the measurement as its state. This will always be $|0\rangle$ or $|1\rangle$, each with probability $\frac{1}{2}$, in spite of this not having been the sent state.

This is an illustration of the statement (see Sec. 4.4):

> Two unknown non-orthogonal quantum states cannot be distinguished reliably.

With the goal of key distribution in mind, this means that if Alice randomly varies between using the states $|+\rangle(|-\rangle)$ and $|0\rangle(|1\rangle)$ to encode for 0(1), neither Eve nor Bob will know whether to perform a '$|0\rangle, |1\rangle$' or a '$|+\rangle, |-\rangle$' measurement. An incorrect choice will result in a destruction of information sometimes manifested as a decoding error. But what hope does this leave for the creation of key shared by Alice and Bob that is secret?

1.6 BB84 as an illustration of distributing a secret key

The potential for the kind of reasoning followed above has existed since the conception of quantum mechanics. Eventually, in 1984 Bennett and Brassard [10] proposed the first quantum key distribution (QKD) protocol (where protocol refers to a set of steps or instructions), commonly called BB84, which still serves as a useful model of a generic QKD protocol today.

1.6.1 Phase 1 of BB84

Phase 1 of the BB84 protocol can be understood in terms of the following steps:

1. Alice generates two independent random bit strings, S_{1A} and S_{2A}, of equal length, say $2(N + l)$, where the message that she intends to encode using the generated key is of length n. S_{2A} is the potential key that Alice aims to share with Bob, while S_{1A} is used to choose between two types of encoding for the string S_{2A}: encoding 0(1) in the single photon quantum

state $|0\rangle(|1\rangle)$ is one type of encoding; the other uses the single photon state $|+\rangle(|-\rangle)$.

2. Alice consequently sends one of the single photon states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ with equal probability, $2(N + l)$ times, along a *quantum channel* (which is just a medium for the transmission of quantum objects and could be an optical fibre or free space) to Bob's location.

3. Bob also generates a random bit string S_{1B} of length $2(N + l)$ according to which he chooses between performing '$|0\rangle, |1\rangle$' or '$|+\rangle, |-\rangle$' measurements on the incoming photons.

4. Bob decodes the signal which entails associating the measurement outcomes $\{|0\rangle, |+\rangle\}$ or $\{|1\rangle, |-\rangle\}$ with the classical bit 0 or 1, respectively, for each photon measured, and recording these outcomes in a final bit string, S_{2B}.

The protocol is complete when $S_{2A} = S_{2B}$. The assumption is that no one but Alice has any knowledge of S_{1A}, therefore by following this procedure, Bob will choose the correct type of measurement with probability $\frac{1}{2}$, and therefore on average only $\frac{3}{4}$ of S_{2B} will agree with S_{2A}, since even when he measures incorrectly, the probability of recording the correct classical outcome is $\frac{1}{2}$.

This average agreement will be reduced if a simple eavesdropping strategy has been implemented by Eve. In the so-called *intercept-and-resend* attack, Eve intercepts and measures each of the photons sent by Alice, and then resends the photon state resulting from each of her measurements to Bob. This attack introduces error with probability $\frac{1}{4}$ on the portion of Bob's key corresponding to his measuring correctly, since Eve also performs the correct measurement with probability $\frac{1}{2}$, and is lucky half of the time in other cases. Thus, in the case of the intercept-and-resend attack, on average only $\frac{5}{8}$ of S_{2B} will agree with S_{2A}, while Eve can construct a bit string of which $\frac{3}{4}$ agrees with S_{2A}!

The above steps 1-4 constitute Phase 1 of the protocol which is implemented on the quantum channel. But it seems that BB84, and indeed the generic QKD protocol, cannot be complete if Alice and Bob are connected only by a quantum channel. As illustrated for the above attack, this single connection

leaves Bob with a smaller probability than Eve of sharing an identical bit string with Alice, since Eve measures the photons first and destroys information. However, the above problems are solved through the introduction of an *authenticated* (see Sec. 2.3) *public classical channel*, which is a medium for the transmission of classical information between partners (a phone line, or a computer cable link), which need not be secure, but it must have been verified that Alice and Bob are the users of the channel. Use of the classical channel constitutes Phase 2 of a generic QKD protocol. Phase 2 of BB84 is described in the following subsection.

1.6.2 Phase 2 of BB84

5. Alice and Bob perform what is called *basis reconciliation*. Subsequent to the performance of all measurements, Alice communicates the bit string S_{1A} to Bob on the classical channel. Note that S_{1A} contains no information about S_{2A}. Alice and Bob then discard the bits from S_{2A} and S_{2B} corresponding to instances when $S_{1A} \neq S_{1B}$, in other words when Bob performed an incorrect type of measurement. On average, they are left with $N + l$ bits each, termed the *sifted key*.

6. Alice and Bob perform *parameter estimation*, which entails revealing l bits of the key (remember that the required length of the final secret key is n) and comparing their respective values. This step enables Alice and Bob to calculate (amongst other parameters) the bit error rate, e_l, given by the number of errors per bit. They then discard this portion of the key. The bit error rate for this portion provides an estimate of e, the bit error rate for the entire transmission, and is an indication of whether an eavesdropper has caused disturbance in the transmission.

7. If there is evidence of eavesdropping, i.e., if for the l bits compared, $S^l_{2A} \neq S^l_{2B}$, Alice and Bob can abort the protocol without having compromised the message, and begin again with step 1.

Realistically, this means Alice and Bob can never communicate in secret, because at the present time there does not exist a single photon source, a device encoding information into quantum states, a medium facilitating transmission, nor a signal detector that can perform without any error all the time, and Alice and Bob have no way of discerning this kind of error

from that resulting from eavesdropping.

But an amendment of step 7 to 7' and further use of the classical channel to implement techniques from classical information theory solve this problem.

7'. Using e_l as an estimate of e, and conservatively attributing all error to eavesdropping, Alice and Bob can calculate I_E, an upper bound to the information potentially gained by Eve.

8. Alice and Bob now perform *secret-key distillation* (SKD) on their remaining N bits, termed the *raw keys*, which are not yet perfectly correlated nor perfectly secret. SKD is a classical processing technique comprising two steps:
i) *Error correction*
Alice and Bob implement an error correction protocol (see Sec. 3.4.3) on the classical channel, the result of which is that Alice and Bob share an identical key of length N.
ii) *Privacy amplification*
Privacy amplification (see Sec 3.4.4) involves further reduction of the key length by, roughly speaking, the total number of bits possibly learnt by Eve through eavesdropping, I_E, and during the above error correction procedure. Thus, Eve's information on the resulting secure key of length $n < N$ shared by Alice and Bob is reduced to zero.

So by following steps 1-8 which describe Phases 1 and 2 of the BB84 protocol, it is possible to generate one secret key in the two locations of Alice and Bob, which since it is random and of adjustable length, can be used as a one-time pad for secret communication.

1.7 The meaning of unconditional security

What if Eve is particularly clever and on the occasion when Alice's imperfect single photon source sends two photons instead of one, Eve keeps one, stores it with a device she's developed with a quantum memory, and measures it only after step 6, thereby learning one key bit while remaining undetected? This attack is known as the *photon-number splitting attack*. Or what if she

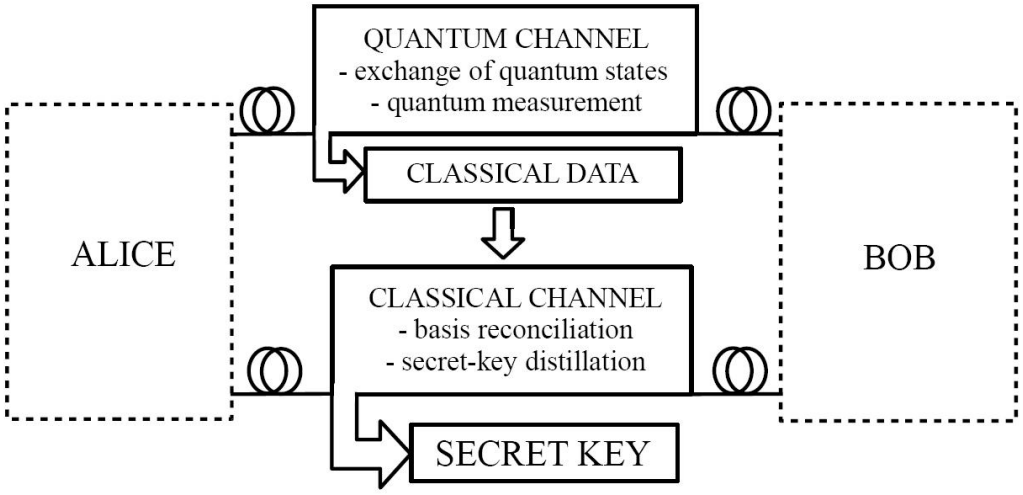

Figure 1.1: General quantum key distribution protocols utilise a quantum and an authenticated classical channel for exchanges between partners in Phases 1 and 2 of the protocol respectively.

develops her own optical fibre capable of error-free transmission, replaces Alice and Bob's fibre with this, and ensures that any error she introduces through eavesdropping remains below the bit error rate associated with Alice and Bob's original fibre? Or what if she develops a quantum cloning device which she uses to make two copies of all the states sent by Alice, performs one type of measurement on each, sends the original states to Bob, and after step 6 keeps the relevant results?

Unfortunately for Eve, the final eavesdropping strategy will not work, since the laws of quantum mechanics imply the *no-cloning theorem* (see Sec. 4.6) [11], which states that an unknown quantum state cannot be copied. But with respect to other strategies:

The point of *unconditional security* is that it does not impose any restrictions on the computational resources or on the manipulation techniques available to a potential eavesdropper. For a protocol to be *unconditionally secure* means that: In spite of an existing bit error rate e on the sifted key (as estimated after basis reconciliation, possibly arising from eavesdropping and

certainly from realistic devices) which is conservatively attributed to eavesdropping only, and in spite of the fact that Eve has the potential to perform any action and use any device imaginable within the laws of quantum physics, Alice and Bob can still perform a processing procedure, SKD, that will reduce Eve's information to zero, and result in an identical shared key.

Sometimes e is too high to salvage a shared key even assuming perfect processing techniques. Thus, to say a protocol is unconditionally secure, is to state a maximum value for e such that secret key rate remains positive for a given processing procedure.

1.8 The security of BB84

Assuming perfect one-way processing techniques (see Sec. 3.4), perfect devices, and considering individual attacks (such as the intercept-and-resend and photon-number splitting attacks mentioned in the previous section) only, the secret key rate is given by the difference between the information shared by Alice and Bob, and the information gained by Eve (see Sec. 3.4).

However, the difficulty in proving the unconditional security of a QKD protocol like BB84, is in calculating the information potentially gained by Eve. And Eve is assumed to be able to acquire information not only through individual attacks, which are limited to identical measurements on individual photons which are assumed to be implemented before SKD, but through all possible eavesdropping strategies allowed by the laws of quantum mechanics, including *joint measurements* (see Sec. 4.9) on any combination of signals at any time.

The main ideas behind an unconditional security proof of BB84 were first presented by Mayers at a workshop in 1996 [12], however, at the time 'no one in the audience understood Mayers' explanation' [13]. A second unconditional security proof published in a symposium proceedings by Biham et al. in 1999 [14] is said to be 'quite difficult' [15] and 'quite complex' [16].

Luckily the story of the unconditional security of BB84 does not end here-first a discussion of the quantum phenomenon called *entanglement*.

1.9 Entanglement

Entanglement, a term coined by Schrödinger in 1935 [17], is a quantum phenomenon that is another example of the counter-intuitive behaviour of elementary particles (see Sec. 4.7). The correlations between composite elementary particles in what are called *entangled states* are unlike any observed correlations between classical objects, and are thus termed *quantum correlations*.

First, recall the single qubit state (1.1)

$$|+\rangle \;=\; \frac{1}{\sqrt{2}}|0\rangle \;+\; \frac{1}{\sqrt{2}}|1\rangle, \tag{1.4}$$

where the qubit is in a superposition of the states $|0\rangle$ and $|1\rangle$. This means that with probability $\frac{1}{2}$, a '$|0\rangle, |1\rangle$' measurement will result in the state $|0\rangle$, or, similarly, with probability $\frac{1}{2}$, in the state $|1\rangle$.

In the famous 'EPR' paper of 1935 by Einstein, Podolsky and Rosen [18], the properties of a two-qubit system formed from the decay of a radioactive source were described. While in this kind of decay the state of each emitted qubit is given by (1.4), the mutual dependence of measurement outcomes to measurements performed on the pair means that the qubits cannot be considered independent of each other, and the two-qubit system is thus said to be in a *maximally entangled state*.

An example of a maximally entangled state is the state

$$|\Phi^+\rangle \;=\; \frac{1}{\sqrt{2}}|0\rangle_A|0\rangle_B \;+\; \frac{1}{\sqrt{2}}|1\rangle_A|1\rangle_B \tag{1.5}$$

where the subscript A refers to one qubit of the pair, and B to the other. The above state has the following properties, where measurements are assumed to be '$|0\rangle, |1\rangle$' measurements:

1. Measurements performed independently on each qubit have random outcomes, i.e., the resulting state is $|0\rangle$ or $|1\rangle$ each with probability $\frac{1}{2}$.

2. Measurement outcomes on each qubit are always perfectly correlated,

i.e., a measurement on one qubit allows the result of a measurement on the other qubit to be predicted with certainty.

Ekert [19] had the idea of performing QKD using a source that emits entangled qubit pairs. If Alice and Bob perform the same kind of measurement on one of each of the pairs, their correlated measurement results can be used as a key. The security of this protocol, called E91 after the year of its proposal, discussed only very briefly here, arises from the fact that the distributed signals contain no key information owing to their state of superposition until the legitimate users have both performed their measurements.

But what relevance could entanglement have for the unconditional security of BB84?

1.10 Entanglement and the unconditional security of BB84

Among others, two important developments led to an unconditional security proof of BB84 involving entanglement.

Firstly, in 1992 Bennett, Brassard and Mermin [20] proposed the QKD protocol referred to as BBM92 which is described in the following steps:

1. Alice prepares $2(N + l)$ entangled two-qubit states of the form of $|\Phi^+\rangle$ (1.5). She generates a random bit string S_{1A} according to which she performs a '$|0\rangle, |1\rangle$' or '$|+\rangle, |-\rangle$' measurement on one of each pair of the qubits. She records her measurement outcomes as the bit string S_{2A}.

2. Alice consequently sends one of the single photon states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ with equal probability, $2(N + l)$ times, along a quantum channel to Bob's location.

3. Bob also generates a random bit string S_{1B} of length $2(N + l)$ according to which he chooses between performing '$|0\rangle, |1\rangle$' or '$|+\rangle, |-\rangle$' measurements on the incoming photons.

4. Bob records his measurement outcomes in a final bit string, S_{2B}.

It can be seen that steps 2-4 are the same as steps 2-4 in BB84.

BBM92 is referred to as the equivalent entanglement-based (EB) version of the prepare-and-measure (P&M) BB84. Although Alice uses different preparation methods for the quantum states sent to Bob, from all perspectives other than Alice's, the two protocols are identical. This equivalence means that security proofs for the EB protocol will also apply to the P&M scheme and vice versa.

Secondly, in 1996 Bennett et al. [21] proposed the first entanglement distillation (ED) protocol. ED protocols aim at the distillation of pure maximally entangled states from a larger set of mixed non-maximally entangled states, through quantum operations (see Sec. 4.3) performed in the two locations of Alice and Bob, who share each pair, and may communicate on an authenticated classical channel. The resulting pure maximally entangled states are uncorrelated with the environment, including Eve, so that when Alice and Bob perform measurements, the correlated measurement results can be used as a secret key.

Building on these two developments, in 2000 Shor and Preskill [15] gave a 'simple proof of security' of the BB84 QKD protocol. They showed that there exists an unconditionally secure ED protocol using quantum error-correcting codes called *Calderbank-Shor-Steane (CSS) codes* [22, 23] (see Sec. 4.9.2), that is equivalent to BB84, thereby proving BB84 unconditionally secure. This proof is based on a similar proof by Lo and Chau [24], but with the requirement of quantum computation replaced by the use of CSS codes.

Without going into much detail, the signal preparation in the Shor-Preskill protocol is related to that in the EB version of BB84, namely BBM92. After transmission and possible eavesdropping Alice and Bob share a large set of mixed non-maximally entangled states. A set of pure maximally entangled states is then distilled from the larger set of mixed non-maximally entangled states using CSS codes. The properties of CSS codes are used to establish the equivalence between this ED process and the SKD procedure in the original BB84 protocol (consisting of error-correction and privacy amplification). Subsequent measurements performed by Alice and Bob on their maximally

entangled subsystems complete the Shor-Preskill protocol, resulting in a perfectly correlated key about which Eve has no information.

The proof by Shor and Preskill provides an example of how a QKD protocol can be proved unconditionally secure via showing its equivalence to an unconditionally secure ED protocol. That an unconditionally secure ED protocol exists that is equivalent to BB84 is surprising, and gives insight into how entanglement is tied to security in QKD protocols.

1.11 Necessary and sufficient conditions for security

Considering a general QKD protocol, a sufficient condition for unconditional security is to show that the total protocol including Phases 1 and 2 is equivalent to an ED protocol, which has been shown to be unconditionally secure.

Given a general P&M QKD protocol, a necessary first step to showing such an equivalence is to translate Phase 1 of the protocol into an equivalent EB phase.

A more fundamental question to ask before tackling an unconditional security proof however, is whether the protocol has any 'quantumness' that could lead to security or not.

A basic necessary condition for the security of a QKD protocol, whether considering the P&M or the EB description, is that the key information is encoded in non-orthogonal states. A set of orthogonal quantum states resembles a set of classical states in that Eve can intercept the signals and perform a measurement, a *projective measurement* (see Sec. 4.3.2), that decodes the entire set, which she could then reconstruct and send to Bob without being detected.

Recall that the P&M and the EB versions of a protocol are identical from Bob's point of view, and therefore that Bob performs the same measurement in both versions. A necessary condition for security on Bob's measurement is that it should be described by *non-commuting POVM elements* (see Sec.'s

4.3.3 and 4.5). Bob's measurement must be described by non-commuting POVM elements since then there exists no measurement suitable for decoding that could possibly commute with his and thus be performed undetected by Eve in an intercept-and-resend attack.

Returning to the observation that entanglement plays a fundamental role in security proofs of QKD protocols, this necessary condition on Bob's measurement can also be understood in terms of the fact that in the EB translation of a protocol, it is not enough that the effectively distributed state is an entangled state: Alice and Bob must be able to detect this entanglement through the probability distributions of their measurement outcomes. This detection is only possible if Bob's measurement is described by non-commuting POVM elements (see Sec. 6.4 for a proof).

These necessary conditions are an illustration of the statement that the classical data produced in a secure QKD protocol must imply non-classical correlations [25] between the systems held by Alice and Bob in the EB translation, which not only restricts the kind of states into which information is encoded, but also the kind of measurements that are performed to decode the information.

1.12 In conclusion: The Point

After a lengthy introduction, it is now necessary to come to the point.

Phase 1 of a general QKD protocol can be described as a P&M or equivalently as an EB phase, as was illustrated for BB84 in steps 1-4 in Sec. 1.6.1, and steps 1-4 in Sec. 1.10, respectively. While other methods do exist to prove the unconditional security of QKD schemes [12, 14, 26] they can be complicated and long. A simple unconditional security proof of BB84 [15] is based on ED, and the same method has been applied to other QKD protocols [27]. The method consists of showing the equivalence of the total protocol including Phases 1 and 2 to an unconditionally secure ED protocol which will then imply the unconditional security of the original scheme.

Given a general P&M QKD protocol, a necessary first step to proving the protocol unconditionally secure through such an equivalence, is to describe

an equivalent EB translation of Phase 1.

Furthermore, Bob's measurement must be described by non-commuting POVM elements when considering the P&M or the EB version of the protocol.

In the forthcoming Chap.'s 2 to 5, aspects of reviews of classical cryptography, classical information, quantum information and quantum optics that are relevant to this work are given.

In Chap. 6, Phase 1 of a general QKD protocol is described as both a P&M and an EB phase. 'Entanglement as a precondition for security' [28] is discussed and the condition on Bob's measurements in the EB scheme derived. Finally, a brief discussion of unconditional security based on ED is given.

The differential-phase-shift (DPS) QKD protocol was proposed by Inoue et al. in 2002 [29]. In Chap. 7 the modified version of the DPSQKD protocol proposed the next year [30] is considered. The DPSQKD protocol is a member of the class of distributed-phase-reference QKD protocols, for which unconditional security proofs do not yet exist. Phase 1 of DPSQKD is here described and formalised as both a P&M and an EB phase. Bob's measurement is shown to be described by non-commuting POVM elements. The EB translation of Phase 1 of DPSQKD given here is a necessary first step towards an unconditional security proof for the protocol based on ED. Finally, thoughts on a potential unconditional security proof based on ED for a DPSQKD-like protocol are given.

In Chap. 8 this thesis is concluded, and an outlook for potential future work surrounding the security of the DPSQKD protocol given.

Chapter 2

Classical cryptography

"All data is illegal - all you need is the appropriate one-time pad."

-Employee, Aman Corporation

The word *cryptography* is derived from the Greek expression $\kappa\rho\upsilon\pi\tau\acute{o}\varsigma\ \gamma\rho\acute{\alpha}\varphi\omega$ meaning 'hidden writing' [31], although besides ensuring *confidentiality* of information, cryptography also includes aspects such as *authentication*, *secret sharing*, *non-repudiation*, and *signature*.

In this chapter, *confidentiality* and *authentication* will be discussed, being the aim and a requirement of QKD, respectively. *Confidentiality* can be achieved by transforming the information to be transferred or stored, the so-called *plaintext*, into what is termed *ciphertext*, such that it is intelligible only to those in possession of additional knowledge, usually referred to as a *key*. Methods of transformation, or *ciphers*, come in two main classes: *asymmetrical* and *symmetrical* ciphers. *Authentication* is the process of verifying that a sent message has arrived unmodified from the legitimate sender. [32]

Asymmetrical and symmetrical ciphers are firstly discussed, and next authentication techniques are described.

2.1 Asymmetrical ciphers

Asymmetrical or public-key ciphers use two different keys: a public key for *encryption* (the transformation from plaintext to ciphertext); and a private key for *decryption* (the recovery of the original plaintext). The relation between public and private keys in this cipher is based on the properties of so-called *one way functions*, f [33]. Briefly, the intended recipient of some communication chooses a private key, say x, and computes the public key $f(x)$ which is disclosed freely. The sender uses this public key to encrypt a message which is sent to the recipient, who decrypts with the private key x. Security is based on the computational complexity of determining x from $f(x)$. This means that the probability of cracking the encryption key using current computational technology and algorithms within a reasonable time is extremely small.

For example, the public-key cipher known as RSA, after the names of its inventors Rivest, Shamir and Adleman, was first implemented in 1978 [34] and is still widely used [13]. Bob, the intended recipient of some communication, begins by selecting two prime numbers p and q, which he multiplies to obtain the product n. He also selects a number $3 \leq a < n$ such that a and n have no common factor, and calculates b such that $ab = 1 \ (\mathrm{mod}(p-1)(q-1))$. The public key (a, n) is published, while Bob's private key (b, n) is kept secret. Alice, the sender, then encrypts some plaintext message $m \in \{0, 1, ..., n-1\}$ (the set with mod n addition and multiplication) via $c = m^a \bmod n$ [16]. Owing to the form of the product ab given above, and to the properties of modular exponentiation, Bob can decrypt the message through the following computation:

$$c^b \bmod n = m^{ab} \bmod n = m. \tag{2.1}$$

The security of RSA is based on the difficulty of factorising of large integers. It is easy to compute a product of prime numbers, but the time taken to find the prime factors, p and q, of a large integer, n, even using the fastest known algorithms, increases faster than any polynomial in $\log n$, written poly($\log n$). Factorisation and other such problems constitute the set of *non-deterministic polynomial* (NP) problems [35]. A 'large' integer is usually bigger than 1000 bits, which is over 300 decimal digits [16]. In 1999 Shamir [36] announced the design for TWINKLE, an electro-optical sieving device claimed to execute sieve-based factoring algorithms approximately two to three orders of mag-

nitude as fast as a conventional fast PC. Using a set of 45 000 such devices it would take 6 to 7 million months (500 000 years) to factorise a 1024-bit number.

However, current algorithms for factorisation have not been shown to be optimal, and there exists no proof that RSA and factorisation are computationally equivalent [16]. Indeed this year in 2009, Sarkar and Maitra [37] claimed that one can factor two integers, each of bit string length n, simultaneously in poly(log$n$) time under several assumptions. For RSA, and indeed for all public-key systems, security that is not conditional on computational power has not been proven.

2.2 Symmetrical ciphers

Symmetrical ciphers use the same key for encryption and decryption. A classical example is the Vernam/Mauborgne *one-time pad* proposed in 1926 [2]. The *one-time pad* encrypts binary plaintext by adding it modulo 2 to a random binary key, or pad, that is used only once. The original plaintext is regained by adding the resulting ciphertext modulo 2 to the key. Let the plaintext be modelled by the random variable (see Sec. 3.1.1) M, which can take one of the character values m from a finite alphabet $\mathcal{M}$, let the random variable C with realisations $c \in \mathcal{C}$ model the corresponding ciphertext symbols, and let the random variable K with realisations $k \in \mathcal{K}$ model the key. For each m and k, the original message is encoded into ciphertext as $m \oplus k$, where $\oplus$ denotes addition modulo 2, and is decoded as follows

$$(m \oplus k) \oplus k = m \oplus (k \oplus k) = m \oplus 0 = m. \tag{2.2}$$

Note, a binary number added modulo 2 to itself always gives zero.

A cipher is secure if and only if for all $m \in \mathcal{M}$ and $c \in \mathcal{C}$

$$\mathrm{p}(M = m | c = C) = \mathrm{p}(M = m) \tag{2.3}$$

where $p(X = x)$ is the probability with which a random variable X takes the character value x (see Sec. 3.1.1), and $p(x|y)$ is the conditional probability that $X = x$ given that $Y = y$ (see Sec. 3.2.2). The one-time pad's status of being the only provably secure cipher known to date was established by

Shannon in 1949 [1], who showed that the above condition is met, i.e., that the ciphertext contains no information on the statistical distribution of the plaintext.

If the one-time pad is used more than once the above condition is no longer met, since two ciphertext bits c_i and c_j encoded with same key bit k can be added modulo 2 to obtain $m_i \oplus m_j$, and this constitutes information on the statistical distribution of the plaintext.

2.3 Authentication

A requirement for the creation of a secure key using QKD is that a classical channel is utilised by Alice and Bob to perform basis reconciliation and secret key distillation on the resulting classical information. For these processes to be successful, both Alice and Bob need to be sure that all communications on the classical channel have arrived unmodified from the legitimate sender, although the channel need not be private. In other words, each use of the channel needs to be *authenticated*.

Authentication is achieved by the legitimate users of the channel sharing an initial key. For example when Alice sends a message to Bob, she calculates a message authentication code (MAC) as a function of the message and the key, which she attaches to the message. Bob recalculates the MAC using the received message and the key. Authentication is complete if his MAC matches that sent by Alice [16].

2.4 Conclusion

In this chapter two aspects of cryptography: confidentiality and authentication have been summarised. Confidentiality can be achieved through symmetrical or asymmetrical ciphers. While asymmetrical ciphers have not been shown to be unconditionally secure, symmetrical ciphers require that a new key be distributed for each use of the cipher. It will be explained in upcoming chapters how quantum cryptography solves the problem of key distribution through the use of a quantum channel as well as an authenticated classical channel, on which basis reconciliation and SKD are performed.

Chapter 3

Information theory

"Structure is more important than content in the transmission of information."

- Abbie Hoffman

Generic QKD protocols utilise a quantum channel and an authenticated classical channel for exchanges between partners in Phases 1 and 2 of the protocol, respectively. The quantum channel is generally noisy, which means that the outcomes of measurements on the transmitted quantum objects, even after the sifting process, do not result in perfectly correlated key bits shared by Alice and Bob. Alice and Bob therefore implement Phase 2 of the QKD protocol, using the authenticated classical channel to perform SKD on their data, which consists of classical error-correction and privacy amplification algorithms, to obtain a shorter perfectly correlated key about which any information Eve may have gained has been reduced to zero.

The mathematical theory of information and communication as founded by Shannon in 1948 [38] deals amongst other things with optimal representation and transmission of data. Pertaining to QKD, Shannon's noisy channel coding theorem quantifies the amount of information that can reliably be transmitted through a noisy channel.

In Sec. 3.1 *Shannon's noiseless coding theorem* is described. Further definitions from probability and information theory used later in this work are given in Sec. 3.2, and in Sec. 3.3 *Shannon's noisy coding theorem* is described.

Finally in Sec. 3.4, secret key rates are given in terms of information theoretic quantities, and error correction and privacy amplification are discussed.

3.1 Shannon's noiseless coding theorem

A fundamental question in information theory is: How can information be quantified? If information is physical because of representation in physical systems, then to quantify information is to quantify the resources necessary to store the information. That is, the question can be rephrased: What is the minimum storage rate for information that is to be reliably retrieved? Assuming that information is represented in an alphabet with character values that will be allocated codewords for storage purposes, the observation that the storage rate of information can be decreased by assigning shorter codewords to more frequent characters, suggests a relationship between a character's probability of occurring, and the resources needed to store it.

In the following sections these intuitions are made more rigorous, and *Shannon's noiseless coding theorem* is shown to provide an answer to this question.

3.1.1 Random variables and independent and i.i.d. sources

Consider a discrete classical *random variable* X which can take one of the character values x from a finite alphabet $\mathcal{X}$ with probability distribution $Pr(X = x)$ which is written $p(x)$ [39].

An information source can be modelled as a sequence of random variables whose values represent the output of the source. If each use of the source is *independent*, and *identically distributed* (i.e., each random variable has the same probability distribution), then the information source is said to be an i.i.d. source [40]. Information sources in the forthcoming sections are assumed to be i.i.d. sources.

3.1.2 Shannon's entropy

The *Shannon entropy* $H(X)$ [38] of the random variable X is defined as a function of the probability distribution $p(x)$ of X as

$$H(X) \equiv -\sum_x p(x) \log p(x). \tag{3.1}$$

$H(X)$ is the optimal compression rate for the information source modelled by the random variable X given that the input must be completely retrievable from the output.

This last statement is the result of *Shannon's noiseless coding theorem*.

The Shannon entropy can also be interpreted as follows: $-\log p(x)$ is the uncertainty in the occurrence of the symbol x. Weighting with the probability $p(x)$ and summing over all x leads to $H(X)$ forming a measure of the average uncertainty associated with each output of the source. Complementarily, $H(X)$ quantifies how much information is gained on average by learning the value of the random variable X.

3.2 More definitions

3.2.1 Binary entropy

In general, the size of the alphabet $\mathcal{X}$ is assumed to be arbitrary. However, in classical information theory, the unit of information is commonly the *bit*, or the set $\{0, 1\}$. Assume that $p(0) = p$ and $p(1) = 1 - p$, then this special case of the Shannon entropy for a binary source modelled by the random variable X_B, the *binary entropy* $H(X_B)$ [40], is given by

$$H(X_B) = -p \log p - (1 - p) \log(1 - p). \tag{3.2}$$

3.2.2 Joint and conditional probabilities

Let X and Y be random variables with probability distributions $p(x)$ and $p(y)$, respectively. The *conditional probability* $p(x|y)$ [40] that $X = x$ given that $Y = y$ is defined as

$$p(x|y) \equiv \frac{p(x, y)}{p(y)}, \tag{3.3}$$

where $p(x, y)$ is the *joint probability* [41] that $X = x$ *and* $Y = y$.

3.2.3 Relative entropy

The *relative entropy* $H(X||X')$ [39] of two information sources modelled by the random variables X and X' with the same alphabet $\mathcal{X}$, with probability distributions $p(x)$ and $q(x)$, respectively, is defined as

$$H(X||X') \equiv \sum_x p(x) \log \frac{p(x)}{q(x)} = -H(X) - \sum_x p(x) \log q(x). \tag{3.4}$$

The relative entropy is a measure of the distance between probability distributions $p(x)$ and $q(x)$ for the same alphabet $\mathcal{X}$ [39].

3.2.4 Joint Entropy

The *joint entropy* $H(X, Y)$ [42] of a pair of information sources modelled by the random variables X and Y is defined as

$$H(X, Y) \equiv -\sum_{x,y} p(x, y) \log p(x, y). \tag{3.5}$$

The joint entropy is a measure of the information content, or the average uncertainty, associated with each of the joint outputs of a pair of sources modelled by the random variables X and Y [40].

3.2.5 Conditional entropy

The *conditional entropy* $H(X|Y)$ [39] of two information sources modelled by the random variables X and Y is defined as

$$H(X|Y) \equiv -\sum_{x,y} p(x|y) \log p(x|y) = \sum_y p(y) H(X|y) = H(X, Y) - H(Y). \tag{3.6}$$

The conditional entropy is the expected value of the information content, or the average uncertainty, associated with the random variable X, given that Y is known [40].

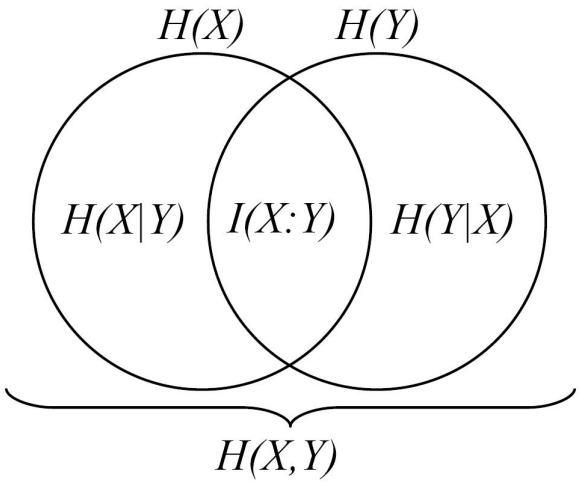

Figure 3.1: A set-theoretical visualisation of entropies.

3.2.6 Mutual information

The *mutual information* $I(X:Y)$ [40] of two information sources modelled by the random variables X and Y is defined as

$$I(X:Y) \equiv H(X) + H(Y) - H(X,Y) = I(Y:X). \tag{3.7}$$

The mutual information is the difference between the sum of the uncertainties of the outputs of two individual sources modelled by the random variables X and Y, and the uncertainty of the joint outputs of the same pair of sources X and Y. The mutual information is thus a reduction in the uncertainty of X due to Y [39].

3.2.7 Conditional mutual information

The mutual information of two information sources modelled by the random variables X and Y, conditional on another information source Z, is defined as

$$\begin{aligned} I(X:Y|Z) &\equiv H(X|Z) + H(Y|Z) - H(X,Y|Z) \\ &= \sum_z p(z)[H(X|z) + H(Y|z) - H(X,Y|z)]. \end{aligned} \tag{3.8}$$

and termed the *conditional mutual information*. The conditional mutual information $I(X : Y|Z)$ is the reduction in the uncertainty of X due to knowledge of Y when Z is given. [39]

3.2.8 Intrinsic information

The *intrinsic information* $I(X : Y \downarrow Z)$ was first defined by Maurer and Wolf in 1999 [43], and can be defined in terms of the conditional mutual information $I(X : Y|Z)$ as

$$I(X : Y \downarrow Z) \equiv \inf_P I(X : Y|Z) \tag{3.9}$$

where P is the set of possible extensions of the observable probability distribution $P(X, Y)$ to $P(X, Y, Z)$, corresponding to all possible individual attacks that Eve could perform [28].

See Sec. 3.4.2 for further details on the intrinsic information.

3.3 Shannon's noisy channel coding theorem

Having answered the question of the minimal resources required to represent information, a second fundamental question in information theory is: What is the most efficient way to transmit this information from one location to another given that errors may occur during transmission? Referring to a transmission medium that has the potential to induce errors in the transmitted objects as a *noisy channel*, and to the maximum rate for reliable transmission through a channel as the channel's *capacity*, the question can be rephrased: What is the maximum capacity of a noisy channel?

3.3.1 A noisy channel

Suppose that Alice sends a series of character values x with probabilities $p(x)$ from her information source modelled by the random variable X to Bob. Assume that since she transmits the symbols along a noisy channel N, the probability for the character value y to be read when the letter x is sent is given by the conditional probability $p(y|x) \geq 1$ where $\sum_x p(y|x) = 1$ for all x [40]. The output at Bob's location is modelled by the random variable Y with probability distribution $p(y)$.

The mutual information $I(X : Y)$ is a reduction in the uncertainty associated with X due to Y, or alternatively, a quantification of the information gained, on average, about x when y is learnt. If $p(y|x)$ characterises a noisy channel, $I(X : Y)$ is the information per letter which can be sent via the channel given the probability distribution of X [41].

Shannon's noisy channel coding theorem states that the *maximum capacity* C [41] of a noisy channel N is given by the maximum of $I(X : Y)$ over the ensemble of probability distributions $p(x)$ of Alice's random variable X:

$$C(N) = \max_{p(x)} I(X : Y). \tag{3.10}$$

The capacity of the channel provides the fundamental upper bound for the rate of error-free transmission in bits per use of a noisy channel [39].

A special case of a channel is described in the next subsection.

3.3.2 The symmetric binary channel

Consider the *symmetric binary channel* [41] defined by

$$p(x = 0|y = 0) = p(x = 1|y = 1) = 1 - p \tag{3.11}$$
$$p(x = 0|y = 1) = p(x = 1|y = 0) = p, \tag{3.12}$$

where the mutual information between the input source X and output source Y is given by

$$I(X : Y) = H(X) - H(p). \tag{3.13}$$

The maximal value of $H(X)$ is 1, therefore the capacity of a binary symmetric channel $C(p)$ is given by

$$C(p) = 1 - H(p). \tag{3.14}$$

3.4 Secret key rate

After Phase 1 and the processes of basis reconciliation and parameter estimation in a QKD protocol are complete, Alice and Bob each hold a set of classical data, the raw keys. Assuming that eavesdropping has taken place, Eve also holds a classical data set. These data can be modelled as the random

outputs of a binary symmetric i.i.d. information source over three individual, not necessarily independent, binary symmetric channels [44]. Let the outputs of the channels at the locations of Alice, Bob and Eve, be modelled by the random variables A, B and E, respectively, with joint probability distribution $p(a, b, e)$. Alice and Bob process their raw key data, which are the sequence of realisations of A and B, respectively, by communication on a public authenticated classical channel in a process termed SKD. The aim of SKD is to extract one secret key from their partially correlated, partially secret raw keys [16].

The rate K at which the final secret key of a QKD protocol is produced is the product of the raw key rate R and the secret fraction r. The value of the raw key rate R depends on the protocol itself, and on the hardware used in the implementation of the protocol [45]. The secret fraction r is defined as the maximum rate at which Alice and Bob can agree on a secret key such that the rate at which Eve obtains information about the key is arbitrarily small [46]. The secret fraction r depends on the distribution $p(a, b, e)$ and the corresponding amount of secret correlation between Alice's and Bob's raw keys that is extractable using a given SKD procedure [44]. Here, the focus is on the secret fraction r, which will henceforth be referred to as the *secret key rate*.

SKD consists of two procedures: error correction and privacy amplification. The result of Shannon's noisy coding theorem (see Sec. 3.3) is that the fraction of perfectly correlated symbols that can be extracted from a sequence of partially correlated symbols is bounded by the mutual information of the random variables A and B with a joint probability distribution $p(a, b)$ given by $I(A : B) = H(A) + H(B) - H(A, B)$, where H is the Shannon entropy. Error-correcting codes operate within this bound and are discussed in Sec. 3.4.3. Privacy amplification (see Sec. 3.4.4) aims to reduce Eve's information on one of Alice or Bob's raw keys to zero [45]. The fraction by which the raw key must be reduced is therefore given by $\min(I(A : E), I(B : E))$, which depends on the chosen communication direction [48].

3.4.1 Lower bound

The *Csiszár-Körner bound* [47] is a lower bound for the secret key rate r given by

$$r \geq \max\{I(A:B) - I(A:E), I(B:A) - I(B:E)\}. \tag{3.15}$$

The above bound is derived for one-way SKD, defined by the partner holding the reference raw key (usually Alice) sending classical information through the public channel to the other partner (Bob), who may process his data but does not send a reply [45]. It has been shown that the secret key rate can be positive even when $I(A:B) < I(A:E)$ and $I(B:A) < I(B:E)$ hold [46], but no key can be generated unless the mutual information shared by Alice and Bob as seen by Eve's best choice of all possible points of view is greater than zero [49] (see Sec. 3.4.2).

Note, the Csiszár-Körner bound is a lower bound for security under the restriction that Eve performs identical individual attacks on each signal obtaining measurement results immediately, since A, B and E are assumed to be i.i.d. classical random variables [48].

3.4.2 Upper bound

The intrinsic information $I(A:B \downarrow E)$ (3.9) was first defined by Maurer and Wolf [43] as an upper bound for the secret key rate r:

$$r \leq I(A:B \downarrow E). \tag{3.16}$$

The intrinsic information $I(A:B \downarrow E)$ can be interpreted as the mutual information shared only by Alice and Bob after Eve has performed an optimal individual attack. It is therefore only possible to perform successful SKD consisting of error correction and privacy amplification if $I(A:B \downarrow E) > 0$.

Renner and Wolf [49] found a stronger upper bound for the secret key rate r, given by the *reduced intrinsic information of A and B given E*, $I(A:B \downarrow\downarrow E)$.

Note, using two-way classical processing techniques such as the *Cascade error-correction protocol* (see next section) generally improves the bounds

given here for the secret key rate (see for example an article by Kraus et al. [50]), but optimal procedures are not generally known. An example of how classical *preprocessing* can improve bounds for the secret key rate for a selection of protocols can be found in [26].

3.4.3 Error correction

Phase 1 of a QKD protocol is implemented on a quantum channel, which is generally noisy, such that the outcomes of measurements on the transmitted quantum objects do not result in perfectly correlated key bits shared by Alice and Bob. SKD is therefore implemented on an authenticated classical channel in Phase 2 of the protocol. SKD includes the implementation of an error-correction protocol, the result of which is that Alice and Bob share identical bit strings with a high probability. [16]

A simple example of an error-correcting code is a 3-bit repetition code which maps 0 to 000 and 1 to 111. Assuming that at most one error occurs per transmission, and that Alice wishes to send the bit 1, Bob can correct a string such as 101 to 111, and thus retrieve a 1. This kind of procedure is effective in classical communications with a typical error rate of around 10^{-5}, but requires a large amount of computing power in quantum communications where the error rate is of the order of a few percent [51]. Such methods are also unable to asymptotically guarantee that a set of data can be transmitted without error.

Error-correcting protocols that use two-way communication between Alice and Bob are able to achieve higher computational efficiency rates than one-way processes such as bit repetition codes. *Cascade* is an error-correction protocol proposed by Brassard and Salvail in 1993 [52] and uses two-way communication. It is a recursive parity-based protocol which performs within 10% of the Shannon limit at low bit error rates [53], and is therefore successful in minimising the amount of information exchanged (publicly) during the process. The unconditional security of discrete variable QKD schemes using Cascade has been shown [51]. (More recently the performance of Cascade is claimed to be improved upon at error rates of 5% and above by a protocol using *low density parity check codes*, see the article by Elkouss et al. [53] for further details.)

Prior to implementing Cascade, Alice and Bob perform two preliminary steps. Firstly, they compare a sample of their data to estimate the error rate of the entire transmission. They proceed if this is below a certain threshold and discard this sample. Transmission errors possibly resulting from eavesdropping are likely to occur in sequences rather than being randomly scattered throughout the data. Thus, Alice and Bob secondly agree upon a random permutation of the remaining bits in their strings such that the errors are uniformly distributed. This process ensures that Bob's data can now be assumed to result from a binary symmetric channel where each bit is independently exposed to noise.

The Cascade error correction protocol is subsequently initiated:

Alice and Bob divide their data into blocks such that each block is unlikely to contain more than one error. Alice then sends the parity of each of her blocks to Bob. The parity of a group of bits refers to the evenness or oddness of the number of 1's within that group. For each pair of blocks with unequal parities, Alice and Bob examine the parities of halves of that block and so on until the error is found and corrected. Thus, all of Bob's blocks now contain an even number of errors. Alice and Bob then again randomise their data, divide it into blocks and repeat the procedure, until after multiple repetitions they share identical keys with a high probability. However, although these keys are identical, they are not yet completely private.

3.4.4 Privacy amplification

Error correction is the first of two stages constituting the SKD procedure in Phase 2 of a QKD protocol. The second stage is termed *privacy amplification*, the result of which is a reduction in the length of the identical shared keys by, roughly speaking, the number of bits about which Eve has potential knowledge. [16]

Eve's partial information about the key consists of information about physical bits and parity bits, acquired through eavesdropping and during the public error-correction procedure, respectively. Given that an upper limit to the total number of bits Eve potentially knows can be calculated, privacy amplification allows Alice and Bob to compute a key of reduced length about which Eve's information is below a certain threshold.

Alice and Bob compute this secret key using a class of *universal hash functions* [54] from which they randomly select one. The class of *universal hash functions* $\mathcal{G}$ map the set of n-bit strings $\mathcal{A}$ to the set of m-bit strings $\mathcal{B}$ such that for any distinct $a_1, a_2 \in \mathcal{A}$, the probability of a *hash collision*, or of $g(a_1) = g(a_2)$, is at most $1/|\mathcal{B}|$ [40]. The main property of the class $\mathcal{G}$ is that given an input element $a_1 \in \mathcal{A}$, it is computationally hard to find another element $a_2 \in \mathcal{A}$ which collides with a_1 [54]. This means that Alice and Bob can apply a chosen g to their shared bit string, about which Eve has partial information, thereby maximising her uncertainty about the new string of reduced length [40]. Thus, using a class of universal hash functions, Alice and Bob obtain a shorter perfectly correlated key about which any information Eve may have gained has been reduced to an arbitrarily small amount.

At this point a QKD protocol is complete, since one secret key has been distributed in the two locations of Alice and Bob.

3.5 Conclusion

In this chapter elements of information theory relevant to QKD have been discussed, and definitions of information theoretic quantities used in this work given. Importantly, before initialising the SKD phase of a QKD protocol, Alice, Bob and Eve have sets of data in their two locations, which can be modelled as sequences of outcomes of the classical random variables A, B and E. A necessary condition for being able to filter a secure key from these data using classical algorithms is that the intrinsic information $I(A : B \downarrow E)$ must be greater than zero. However, modelling Eve's information as a classical random variable assumes that Eve performs an individual attack, and this form of attack is not optimal. Assuming that Eve really can do *anything* allowed by the laws of quantum mechanics requires that Eve's information is represented as quantum information.

Chapter 4

Quantum information theory

"... the 'paradox' is only a conflict between reality and your feeling of what reality ought to be."

- Richard Feynman

In Phase 1 of a generic QKD protocol, a quantum channel is utilised for the exchange of quantum states into which information has been encoded. Quantum information deals with the implications of representing information in quantum systems such as photons. Here, aspects of quantum information theory relevant to QKD are discussed. Since quantum systems are subject to the laws of quantum mechanics, a broad overview of the principles of quantum mechanics is also given. A quantum analogue of SKD is described briefly. Finally, unconditionally secure key rates are given in terms of quantum information theoretic quantities.

4.1 Quantum states

Quantum mechanics [55] is a mathematical framework that identifies any isolated physical system with a complex vector space with inner product, called the Hilbert space of the system. A state of the system is described by a complex unit vector in this space, termed a *state vector*, and is usually written in *Dirac notation* [9] as $|\psi\rangle$. [40]

A general state can be expressed as a *superposition*, or normalised complex

linear combination, of the orthonormal basis vectors spanning the Hilbert space of the system.

The inner product associates any pair of state vectors, $|\psi\rangle$ and $|\psi'\rangle$, with a complex number and is written as $\langle\psi|\psi'\rangle$ where the notation $\langle\psi|$ is used for the *dual vector* to $|\psi\rangle$ [40]. The inner product provides a formalism with which to define geometric notions such as the length of a vector, and the angle between two vectors, where an inner product of zero is associated with orthogonal vectors.

As an example of a quantum state, the *qubit* is considered in the following section.

4.2 The qubit

The simplest quantum mechanical system and fundamental unit of quantum information is a two-level system, or *qubit* (a term coined by Schumacher in 1995 [56]). A qubit is a mathematical object with a two-dimensional Hilbert space, and is typically realised in physical systems such as an atom with a ground and first excited state, a photon with its two polarisation states, or an electron with spin 'up' and 'down'.

In Dirac notation, the states $|0\rangle$ and $|1\rangle$ form an orthonormal basis for the Hilbert space of the qubit, and are termed the computational basis [40]. The states $|0\rangle$ and $|1\rangle$ are two possible states of a qubit, however, an arbitrary state in this space can be written as a superposition of the basis vectors. A qubit is therefore described in general by two complex numbers as the set

$$\{\alpha|0\rangle \ + \ \beta|1\rangle \ : \ |\alpha|^2 \ + \ |\beta|^2 \ = \ 1, \ \alpha, \beta \in \mathbb{C}\}. \tag{4.1}$$

The *decomposition coefficients*, α and β can be parametrised, omitting the unobservable global phase factor, as

$$\alpha \ = \ \cos\frac{\theta}{2}, \tag{4.2}$$

$$\beta \ = \ \mathrm{e}^{i\varphi}\sin\frac{\theta}{2}. \tag{4.3}$$

The two angles θ and φ define a point on the surface of a sphere of unit radius called termed the *Bloch sphere* (see Fig. 4.1). Each point on the surface of

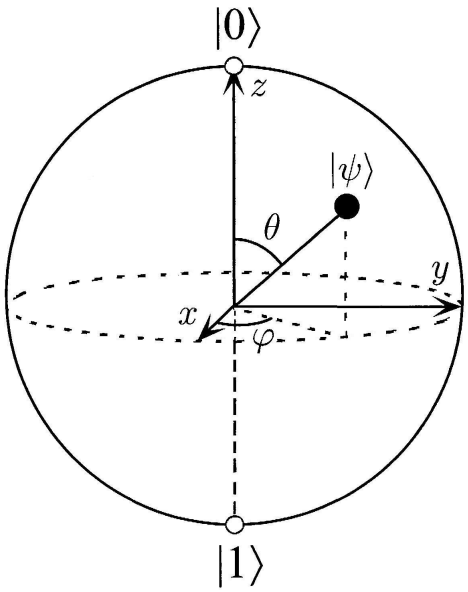

Figure 4.1: Bloch sphere representation of qubit states.

this sphere corresponds to a qubit state, for which the qubit is said to be in a superposition of the states $|0\rangle$ and $|1\rangle$, in contrast with the classical bit which has only two possible states, '0' and '1'.

Let the qubit state $|\psi\rangle$ be defined as

$$|\psi\rangle = \alpha|0\rangle \ + \ \beta|1\rangle. \tag{4.4}$$

The condition that the state $|\psi\rangle$ be a vector of unit length is expressed as

$$\langle\psi|\psi\rangle = |\alpha|^2 + |\beta|^2 = 1 \tag{4.5}$$

and is termed the *normalisation condition*.

The decomposition coefficients can also be written as the inner products

$$\alpha = \langle 0|\psi\rangle \tag{4.6}$$
$$\beta = \langle 1|\psi\rangle. \tag{4.7}$$

The inner product between two qubit states $|\psi\rangle$ and $|\psi'\rangle$ is then given by

$$\begin{aligned}\langle\psi|\psi'\rangle = \langle\psi'|\psi\rangle^* &= \langle\psi|0\rangle\langle 0|\psi'\rangle + \langle\psi|1\rangle\langle 1|\psi'\rangle \\ &= \alpha^*\alpha' + \beta^*\beta'. \end{aligned} \tag{4.8}$$

These states are said to be orthogonal if and only if

$$\alpha^*\alpha' + \beta^*\beta' = 0. \tag{4.9}$$

The states $|0\rangle$ and $|+\rangle$ are an example of a pair of non-orthogonal states, their inner product is given by

$$\begin{aligned}\langle 0|+\rangle &= \langle 0|\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\} \\ &= \frac{1}{\sqrt{2}}. \end{aligned} \tag{4.10}$$

It can be seen that the existence of non-orthogonal states is a result of the existence of superposition states in the quantum regime. Examples of neither such states are found classically.

4.3 Quantum measurement

The evolution of a closed quantum system is described by a unitary transformation $\mathcal{U}$, which is an invertible linear operator that preserves the norm of the state [16]. If the initial condition of the system is $|\psi\rangle$, then at a later time the system evolves to a state $\mathcal{U}|\psi\rangle$. A measurement of a quantum system implies an interaction of the system with a classical measurement apparatus, rendering it no longer closed, and thus not necessarily subject to unitary evolution. A measurement is described by its effect on the system as follows:

A quantum measurement is described by a set of measurement operators M_m which act on the state space of the system being measured. Each operator is associated with a measurement outcome m. The probability of a particular measurement outcome being realised, $p(m)$, and the state of the system after this measurement, can be calculated in terms of the measurement operator M_m, and the initial state of the system. That the probabilities $p(m)$ must sum to one is equivalent to the measurement set $\{M_m\}$ satisfying the *completeness relation*. [40]

4.3.1 Measuring a qubit

As an example of a quantum measurement, a measurement of a qubit in the computational basis is considered.

Let the qubit state be defined as in Eq. (4.4), then the two possible measurement outcomes $m = 0$ and $m = 1$ are associated with the operators M_0 and M_1, respectively, given by

$$M_0 = |0\rangle\langle 0| \tag{4.11}$$
$$M_1 = |1\rangle\langle 1|. \tag{4.12}$$

The probability of measurement outcome $m = 0$ is given by

$$p(0) = \langle\psi|M_0|\psi\rangle = |\alpha|^2, \tag{4.13}$$

while the probability of measurement outcome $m = 1$ is given by

$$p(1) = \langle\psi|M_1|\psi\rangle = |\beta|^2. \tag{4.14}$$

The completeness relation is satisfied since the qubit state (4.4) is defined with $|\alpha|^2 + |\beta|^2 = 1$.

An aside on *true randomness*:

The word 'random' has been used more than once in this work, and the security of QKD protocols depend on its correct interpretation.

A specific case of a classical random variable as referred to in Sec. 3.1.1, is a binary random variable X that can take one of the character values $\{0, 1\}$ with equal probability $p(0) = p(1) = \frac{1}{2}$. A fundamental assumption when implementing a QKD protocol is that the random binary strings, the randomisation procedures, and the random selection processes used by Alice and Bob are *truly random* rather than pseudo-random. This means that the random variables used in each case should be generated by truly random processes, where possible biases in measurement have been compensated for, rather than by deterministic processes with a very high degree of apparent randomness [13]. It is difficult to distinguish these cases statistically.

'RANDOM.ORG offers *true* random numbers to anyone on the Internet' [57],

generated from atmospheric noise which is considered random. According to the laws of quantum mechanics, truly random processes include radioactive decay, shot noise [58], the random choice of a single photon at a beamsplitter [59] (see Sec. 5.4 for a description of a beamsplitter), and also the process of measuring a qubit.

Consider the qubit state from Eq. (4.4) and a measurement with operators given in Eq.'s (4.11) and (4.12).

Since the two possible measurement outcomes ideally occur randomly with equal probability, associating the outcome '0' with the bit zero, and the outcome '1' with the bit one results in the generation of a truly random variable. In a realistic experimental setting, biases in the preparation of the qubit state and measurement implementations would also have to be taken into account before measurement outcomes could be considered truly random [13]. Prototypes using quantum processes to generate random numbers are commercially available [60].

4.3.2 Projective measurement

In the case where a quantum measurement satisfies the completeness relation and where each operator P_m is an *orthogonal projector*, then the measurement is termed a *projective measurement* and described by the *observable* M which is given by

$$M = \sum_m m P_m. \tag{4.15}$$

A measurement operator is an *orthogonal projector* if and only if it is Hermitian and satisfies $P_m P_{m'} = \delta_{mm'} P_m$. The set of measurement outcomes m is associated with a set of states $|m\rangle$ which form an orthonormal basis for the system under consideration, hence the expression 'measuring in the $|m\rangle$ basis' in reference to performing a projective measurement with projectors $P_m = |m\rangle\langle m|$ [40]. Note, the measurement of a qubit in the computational basis considered in Sec. 4.3.1 is an example of a projective measurement since $M_m M_{m'} = \delta_{mm'} M_m$. In such cases, $M_m \equiv P_m^\dagger P_m = P_m$.

4.3.3 POVM

A projective measurement is a special case of a more general quantum measurement. A set of operators $E_m \equiv M_m^\dagger M_m$, where M_m are measurement operators, are in general non-commuting (see Sec. 4.5) and satisfy

$$\sum_m E_m = I \tag{4.16}$$

with I being the identity operator. The probability of measurement outcome m is given by

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle = \langle\psi|E_m|\psi\rangle. \tag{4.17}$$

This general measurement $\{E_m\}$ is called a *positive operator-valued measure* (POVM) [61] because each operator E_m, also termed an *effect* or a *POVM element*, is a *positive operator*, i.e., $\langle\psi|E_m|\psi\rangle \geq 0$ for all states $|\psi\rangle$. [62]

A POVM is termed *informationally complete* if its statistics determine completely the quantum state on which the measurement is carried out [63]. However, for a general POVM, the number of elements can be greater than the dimension of the space of the states being measured [64].

The *Stinespring-Kraus theorem* [65] relates quantum operations to unitary transformations, stating in particular that any quantum operation realized on a system A corresponds to a unitary transformation U performed on a larger system with Hilbert space $\mathcal{H}_{AB}$ [66].

Moreover, a generalised quantum measurement, or POVM, represented by a set of effects $\{E_m\}$, can be understood as a projective measurement represented by a set of orthogonal projectors $\{P_m\}$ performed on the larger system [61]. The *Neumark theorem* (see, e.g. [67]) states that for each POVM $\{E_m\}$ there exists a projective measurement $\{P_m\}$ on a larger Hilbert space $\mathcal{H}_{AB}$ where

$$\mathrm{Tr}\{\rho_A E_m\} = \mathrm{Tr}\{(\rho_A \otimes \sigma_B)P_m\} \tag{4.18}$$

for all states ρ_A of system A, where σ_B is a suitably chosen state of system B. [66] These theorems will be referred to in Chap. 7.

4.4 Distinguishing non-orthogonal quantum states

In the classical world states of objects are in principle distinguishable. However, on a quantum level this is not always the case.

Consider the non-orthogonal quantum states $|\psi\rangle$ and $|\gamma\rangle$ identified with non-orthogonal state vectors in the Hilbert space of the system. It is possible to express the state $|\psi\rangle$ in terms of one component which is parallel and one which is perpendicular to the state $|\gamma\rangle$. A non-zero component of $|\psi\rangle$ parallel to $|\gamma\rangle$ will always result in a non-zero probability of the measurement outcome associated with the state $|\gamma\rangle$ also occurring when the measurement is applied to the state $|\psi\rangle$. Since states are not observable, but measurement outcomes are, there is therefore no measurement that can reliably determine which of two non-orthogonal states was measured. (See p. 87 of the book by Nielsen and Chuang [40] for a simple proof by contradiction that two non-orthogonal states cannot be distinguished reliably.)

In the special case of orthogonal states, there does exist a measurement to discern the states. The projective measurement consisting of orthogonal projectors onto each of these states as well as an additional operator defined such that the completeness relation is satisfied is such a measurement.

4.5 The commutator

Mathematically, the *commutator* gives an indication of the extent to which two operations fail to be commutative. In quantum mechanics, the *commutator* of two measurement operators E_m and $E_{m'}$ written $[E_m, E_{m'}]$ is defined as

$$[E_m, E_{m'}] = E_m E_{m'} - E_{m'} E_m. \tag{4.19}$$

If E_m and $E_{m'}$ can be expressed in at least one common orthonormal basis consisting of the set of states corresponding to the possible measurement outcomes for each, then the commutator is zero and the operators are said to commute. The converse is also true.

In the case of a projective measurement as defined in Sec. 4.3.2, the projec-

tors constituting the measurement are orthogonal projectors, and the commutator between any two operators is evaluated as

$$[P_m, P_{m'}] = \delta_{mm'} P_m - \delta_{m'm} P_{m'} = 0. \tag{4.20}$$

A projective measurement is effective in determining which of a set of orthogonal states has been measured.

For an example of a measurement containing non-commuting operators, consider a POVM that attempts to distinguish two arbitrary non-orthogonal states, $|\psi\rangle$ and $|\gamma\rangle$. The POVM elements are given by

$$\begin{aligned} E_1 &= |\psi\rangle\langle\psi| && (4.21)\\ E_2 &= |\gamma\rangle\langle\gamma| && (4.22)\\ E_3 &= I - (E_1 + E_2). && (4.23) \end{aligned}$$

Measurement outcome 1 (2) corresponds to the POVM element E_1 (E_2) and determines that $|\psi\rangle$ ($|\gamma\rangle$) was the state measured. The third possible measurement outcome yields no information about the measured state, rendering this measurement not reliable in every case in determining which of $|\psi\rangle$ or $|\gamma\rangle$ was the measured state.

Where c is the complex inner product of the states $|\psi\rangle$ and $|\gamma\rangle$, the commutator between E_1 and E_2 is given by

$$\begin{aligned} [E_1, E_2] &= |\psi\rangle\langle\psi|\gamma\rangle\langle\gamma| - |\gamma\rangle\langle\gamma|\psi\rangle\langle\psi| \\ &= c|\psi\rangle\langle\gamma| - c^*|\gamma\rangle\langle\psi| && (4.24) \end{aligned}$$

which in general is non-zero.

Thus, it can be seen that as a result of $|\psi\rangle$ and $|\gamma\rangle$ being different, and being non-orthogonal states, which implies that the inner product c is non-zero, a POVM constructed to (sometimes) distinguish the states, contains non-commuting elements.

In general, if two operators do not commute, then it is not possible to determine the measurement outcomes associated with each operator simultaneously with total precision.

4.6 No-cloning theorem

As mentioned in Sec. 1.7, a necessary condition for the security of a QKD protocol is that the states transmitted by Alice to Bob cannot be intercepted and perfectly copied by Eve who would then gain full information on the key undetected. The theorem by Wootters and Zurek in 1982 [11] states that a general unknown quantum state cannot be copied exactly.

To demonstrate how quantum cloning is not possible, consider an unknown state $|\psi_1\rangle$. Let the system in which the copy will be realised be $|\varphi\rangle$. The evolution of the state vector containing both states is of the form

$$|\psi_1 \otimes \varphi\rangle \rightarrow |\psi_1 \otimes \psi_1\rangle, \tag{4.25}$$

where the symbol $\otimes$ represents the tensor product. This evolution is associated with a unitary operator U

$$|U(\psi_1 \otimes \varphi)\rangle = |\psi_1 \otimes \psi_1\rangle. \tag{4.26}$$

The unitary operator U must be independent of $|\psi_1\rangle$ [41], therefore for a second state $|\psi_2\rangle$

$$|U(\psi_2 \otimes \varphi)\rangle = |\psi_2 \otimes \psi_2\rangle. \tag{4.27}$$

The scalar product

$$\langle\psi_1 \otimes \varphi|U^\dagger U(\psi_2 \otimes \varphi)\rangle \tag{4.28}$$

can be evaluated in two ways

$$\begin{array}{ll} (1) & \langle\psi_1 \otimes \varphi|\psi_2 \otimes \varphi\rangle = \langle\psi_1|\psi_2\rangle, \\ (2) & \langle\psi_1 \otimes \psi_1|\psi_2 \otimes \psi_2\rangle = (\langle\psi_1|\psi_2\rangle)^2. \end{array}$$

Therefore either $|\psi_1\rangle = |\psi_2\rangle$, or $\langle\psi_1|\psi_2\rangle = 0$, and therefore only states that are orthogonal to each other can be copied. Hence the theorem that it is impossible in general to clone an unknown quantum state. [41]

4.7 Entanglement

Entanglement is a quantum phenomenon, the counter-intuitive nature of which led Einstein, Podolsky and Rosen in 1935 [18] to find quantum theory to be in conflict with their feeling of what reality ought to be. Before illustrating the so-called *EPR paradox*, *entangled states* are defined.

4.7.1 Entangled states

The Hilbert space $\mathcal{H}$ associated with a composite system is a tensor product of the Hilbert spaces $\mathcal{H}_i$ associated with the individual systems i. According to the *superposition principle* a general state in the Hilbert space $\mathcal{H}$ is a normalised complex linear combination of the orthonormal basis vectors spanning the Hilbert space of the system [68].

For a bipartite quantum system with Hilbert space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$, a general state can be written as

$$|\psi\rangle = \sum_{i,j} c_{ij} |i\rangle_1 \otimes |j\rangle_2 = \sum_{i,j} c_{ij} |ij\rangle \tag{4.29}$$

where the first index in $|ij\rangle$ refers to a state residing in the Hilbert space $\mathcal{H}_1$, and the second to a state in $\mathcal{H}_2$.

By definition, a state in $\mathcal{H}$ is said to be *entangled*, or *non-separable*, if it cannot be written as a tensor product of a state $|\alpha\rangle_1$ in $\mathcal{H}_1$ and a state $|\beta\rangle_2$ in $\mathcal{H}_2$. On the other hand, if a state $|\psi\rangle$ can be written as

$$|\psi\rangle = |\alpha\rangle_1 \otimes |\beta\rangle_2, \tag{4.30}$$

the state is said to be *separable*. [68]

4.7.2 The EPR paradox

The authors of the EPR paper make several assumptions. They assume the *principle of reality* which states that if the value of a physical quantity of a system can be predicted with certainty, then this value has a physical reality independent of observation. For example, if the state of a system $|\psi\rangle$ is an *eigenstate* of an operator A, that is, if

$$A|\psi\rangle = a|\psi\rangle, \tag{4.31}$$

then the *eigenvalue* a of the observable A is an element of physical reality.

The authors define a *complete theory* as one where every element of physical reality has a counterpart in the physical theory.

The authors assume the *principle of locality* which states that if two systems are causally separated, a measurement performed on one system can not influence the outcome of a measurement performed on the second system.

With these assumptions, taking quantum theory to be correct is shown to lead to a contradiction. Bohm in 1953 [69] illustrated the *EPR paradox* with the following example:

Consider a source that emits a pair of spin-$\frac{1}{2}$ particles in the entangled state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{4.32}$$

which is a maximally entangled state, and termed a *spin-singlet* state. One particle is sent to Alice, and the other to Bob at a causally separate location. Note, where σ_z is the observable corresponding to the z component of the spin of each particle, the states $|0\rangle$ and $|1\rangle$ are the eigenstates of σ_z, corresponding to the eigenvalues +1 and -1, respectively. If Alice measures the observable $\sigma_z^{(A)} = +1$ on her particle, then the state (4.32) collapses to $|01\rangle$. Subsequently, if Bob measures the z component of the spin of his particle, he will get the outcome $\sigma_z^{(B)} = -1$ with probability one.

The singlet state (4.32) can also be written as

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|+-\rangle - |-+\rangle) \tag{4.33}$$

where the states $|+\rangle$ (1.1) and $|-\rangle$ (1.2) are the eigenstates of σ_x corresponding to the eigenvalues +1 and -1, respectively. In this case if Alice measures the observable $\sigma_x^{(A)} = +1$ on her particle, then the state (4.33) collapses to $|+-\rangle$, and if Bob measures $\sigma_z^{(B)}$, he will get the outcome $\sigma_z^{(B)} = -1$ with probability one.

Since in both cases it is possible for Alice to predict Bob's measurement result on the state $|\psi\rangle$ with certainty, both $\sigma_z^{(B)}$ and $\sigma_x^{(B)}$ must correspond to elements of physical reality. But quantum theory states that it is impossible to assign physical reality to both observables simultaneously since they do not commute, $[\sigma_z^{(B)}, \sigma_x^{(B)}] \neq 0$, and total knowledge of one of two non-commuting observables precludes total knowledge of the other (see Sec.

4.5). The implication, given the assumptions outlined above, and result of the EPR paper, is that a quantum mechanical description of reality is incomplete.

More recently there have been a number of experiments (summarised in [70]) the results of which confirm the predictions made by quantum theory, and refute so-called *local-realistic* theories which assume both the principles of realism and locality. The EPR paradox is thus resolved in a contemporary interpretation of quantum mechanics that does not accept a local-realistic description of the way reality is.

4.7.3 Entanglement as a physical resource

The amount of information contained in an entangled state of N qubits grows exponentially with N, rather than linearly as in the case of the classical bit, and quantum parallelism and quantum computing are based on the properties of entanglement [41]. As well as in quantum computing, entangled states are a valuable resource in many areas of quantum information [40], including in QKD, the details of which will be discussed further in upcoming sections.

4.8 Definitions

4.8.1 Density operator

The introduction of the *density operator* by von Neumann [55] and Landau [71] provided a formalism to extend the tools of classical statistical mechanics to the quantum domain. The density operator carries maximal information about a quantum system that is not completely known. Suppose a quantum system is in one of a number of normalised states $|\psi_i\rangle$ each with probability p_i. The *density operator* represents a statistical mixture of states for the system and is defined by

$$\rho \equiv \sum_i p_i |\psi_i\rangle\langle\psi_i|. \tag{4.34}$$

Density operators describe quantum states in the same way that probability distributions can describe classical states. In general, there exist an infinite number of decompositions of the type (4.34) [41].

4.8.2 Von Neumann entropy

The *von Neumann entropy* [55] is defined in terms of the density operator as

$$S(\rho) \equiv -\mathrm{Tr}(\rho \log \rho). \tag{4.35}$$

An analogous question to that asked in Sec. 3.1 is: What is the minimum storage rate for an i.i.d. quantum information source that outputs the quantum states $|\psi_i\rangle$ with probabilities p_i given that the output must be completely retrievable? Schumacher's *quantum noiseless channel coding theorem* [56], the quantum analogue of Shannons noiseless coding theorem, provides the answer to this question, namely, for optimal compression, the average number of quantum states required per output state is given by the von Neumann entropy $S(\rho)$ of the density operator ρ associated with the source.

For an ensemble of orthogonal states the von Neumann entropy is analogous to the Shannon entropy.

4.8.3 The Holevo bound

Suppose that Alice prepares a state ρ_X where $X = 0, ...n$ with probabilities $p_0, ..., p_n$, and Bob performs a measurement described by the POVM elements $\{E_y\} = \{E_0, ..., E_m\}$ on that state, with measurement outcome Y. The *Holevo bound* [72] is an upper bound to the resulting mutual information between Alice and Bob for any measurement that Bob may perform:

$$I(X:Y) \leq S(\rho) - \sum_x p(x) S(\rho_x) = \chi, \tag{4.36}$$

where $\rho = \sum_x p(x)\rho_x$. The right hand quantity χ is termed the *Holevo quantity* [40]. If a source emits *pure* quantum states (states that are described by state vectors rather than density operators), the Holevo bound becomes the von Neumann entropy $S(\rho)$. This result indicates that the amount of information that is accessible from the source does not exceed the amount of information that the source outputs [73].

4.9 Secret key rate

In Sec. 3.4 bounds for the secret key rate were derived under the assumption that Eve has access to many independent realisations of the classical variable

E resulting from measurements performed independently on individual signals and with a consistent strategy. Therefore, at the beginning of the SKD process, all measurements being complete, Alice, Bob and Eve hold classical data sets corresponding to the random variables A, B and E, respectively, with joint probability distribution $p(a, b, e)$. This constitutes a condition on Eve's eavesdropping technique (namely, that she perform only individual attacks) and therefore the secret key rate r discussed in the preceding chapter is *not* an unconditionally secure key rate.

4.9.1 Lower bound

A *collective attack* is characterised by Eve attacking each signal independently with a consistent strategy, but she can wait until after the SKD procedure to perform the best measurement compatible with what she has learnt. In this case, the secret key rate r is bounded below by the *Devetak-Winter bound* [74] given similarly to Eq. (3.15) by

$$r \geq \max\{\chi(A:B) - \chi(A:E), \chi(B:A) - \chi(B:E)\}. \tag{4.37}$$

But here the classical mutual information has been replaced by the Holevo quantity χ (4.38), given by

$$\chi(A:E) = S(\rho_E) - \sum_a p(a) S(\rho_{E|a}). \tag{4.38}$$

The quantity S denotes the von Neumann entropy, a and $p(a)$ are the realisations and probabilities, respectively, associated with Alice's classical random variable A, $\rho_{E|a}$ is the density operator corresponding to the state of Eve's subsystem and $\rho_E = \sum_a p(a)\rho_{E|a}$ is Eve's partial state [45].

There exists a stronger form of attack termed a *joint attack* which is the most general form of attack [45]. Here, Eve treats the whole sequence of quantum signals as a single system. She interacts this system with a system of her own, and then unitarily evolves the combined system. She forwards a subsystem to Bob, and keeps the remaining subsystem for eavesdropping purposes. An unconditionally secure QKD scheme must be secure for any unitary operation performed by Eve. For protocols where bounds on the secret key rate for unconditional security have been found, these bounds have been shown to be the same as for collective attacks [45]. To understand why,

consider a general QKD protocol (see Sec. 6.1) that specifies a quantum state $|\Psi(S)\rangle$ that encodes a sequence of N symbols $S = \{s_1, ..., s_N\}$ prepared by Alice. In many QKD protocols, $|\Psi(S)\rangle$ can be written in tensor product form where there is a one-to-one correspondence between each symbol s_i and each state $|\psi(s_i)\rangle$ that encodes that symbol:

$$|\Psi(S)\rangle \;=\; \bigotimes_{i=1}^{N} |\psi(s_i)\rangle. \tag{4.39}$$

As a result, there are no correlations between signals transmitted on the quantum channel from which Eve would benefit by learning. However, in QKD protocols where $|\Psi(S)\rangle$ cannot be written in tensor product form, and the symbols s_i are encoded in the correlations between the states $|\psi(s_i')\rangle$ (see Sec. 7.2), Eve would benefit from a joint manipulation of the signals. This is a difficult problem, and indeed bounds for the unconditionally secure key rate for such protocols have not yet been found.

4.9.2 Quantum SKD

In EB BB84 Alice gives half of each pair of a number of copies of the maximally entangled state $|\phi^+\rangle$ (1.5) to Bob. Because of noise and eavesdropping on the channel, the resulting state may be impure and is described by the density operator ρ. Alice and Bob then perform local operations and classical communication (LOCC) to distill a key. Eve's information is bounded by Holevo's bound. This implies that if the the LOCC result in Alice and Bob sharing a reduced number of entangled pairs with a fidelity of 1 to the maximally entangled state $|\phi^+\rangle$, then the protocol is secure [16]. One way to implement the LOCC necessary for security is to use CSS codes (introduced in Sec. 1.10). CSS codes are a large class of quantum error-correcting codes, and an important subclass of the more general class of stabiliser codes. Decoding from a randomly chosen CSS code can be thought of as performing error-correction and privacy amplification [40].

The observation that the secret key rate obtainable after SKD coincides with the achievable qubit transmission rate for CSS codes over noisy communication channels is the foundation of the unconditional security proof of BB84 by Shor and Preskill [10]. Shor and Preskill prove BB84 unconditionally secure by showing it equivalent to an unconditionally secure ED protocol

(introduced in Sec 1.10) through the use of CSS codes. Using an ED protocol for communication on a quantum channel connecting two parties Alice and Bob who exchange qubits may work even when traditional quantum error correction procedures fail, since ED protocols are known that can produce a non-zero rate of communication even when traditional quantum error correction does not allow classical communication to take place [40].

4.10 Conclusion

So far the quantum systems into which information is encoded have been described without much detail as 'photons', 'signals' or 'fundamentally quantum objects'. In QKD protocols optical signals are generally used as carriers of information, and hence in the next chapter a more detailed description of the quantum nature of light is given.

Chapter 5

Quantum optics

"All the fifty years of conscious brooding have brought me no closer to answer the question, 'What are light quanta?' Of course today every rascal thinks he knows the answer, but he is deluding himself."

- Albert Einstein

Light is a physical system that permits quantum mechanical description via the quantisation of the electromagnetic field. These quanta are called *photons*, however, naming something can give an illusory sense of it being a simple or well-understood object. Quantum optics is the study of the quantum mechanical properties of light, and in this chapter a selection of aspects of quantum optics relevant to this discussion of QKD are presented: an overview of the history of the quantum theory of light is given and the concept of the photon introduced, the coherent state of light is formalised, and finally the effects of phase shifters, beamsplitters and detectors on light are described.

5.1 The quantum theory of light

Since the turn of the last century it has been clear that a classical wave theory of light, although adequately able to account for the observed properties of light beams, was insufficient.

In 1900 Planck [4] proposed that the energy of a harmonic oscillator is quantised in order to account for the spectral distribution of thermal light. That is, each mode of the electromagnetic field is associated with a quantum harmonic oscillator [75]. Unlike in the classical case, in the quantum domain coupling to the external world becomes very small, and the possible states of the system are found to be quantised, or limited to having energies (up to a fixed offset given by the *zero point energy* $\hbar\omega/2$) of $E_n = n\hbar\omega$, where n is an integer, ω the angular frequency of the electromagnetic field, and $\hbar = \frac{h}{2\pi}$, where h is Planck's constant [40].

For a single mode of light, a state with energy E_n contains n quanta of energy $\hbar\omega$ (in addition to the zero point energy), and to use a term coined by Lewis in 1926 [5], these quanta are called *photons* [75].

In 1905, in confirmation of Planck's hypothesis that light is emitted or absorbed only in integer multiples of a basic quantum of energy, Einstein [6] showed that the photoelectric effect could also be explained on the hypothesis of the quantisation of the electromagnetic field. The postulation that light consists of a beam of photons each having an energy of $h\nu$, where ν is the frequency of the light, explains how the energies of the electrons emitted from the surface of some metal exposed to electromagnetic radiation do not depend on the intensity of the incident light, but only on its wavelength.

Since then, the theory describing light as a beam of elementary particles called photons has received broad experimental confirmation [68], and given rise to many applications, for example, QKD.

5.2 States of light

In 1957 Gould [76] wrote the first prescription for building a viable optical laser, and in 1960 Maiman [77] built the first laser, which enabled the generation of light fields whose strength and range of correlation was unprecedented at optical frequencies. In response to resulting experiments, Glauber [78] proposed a quantum theory of coherence by providing a definition of correlation functions for complex optical field strengths.

Coherent states are very easy to create, for instance, the field generated by

a highly stabilised laser operating well above threshold, is a coherent state [79]. To reduce the average number of photons, an attenuator can be used to lower the pulse intensity, and to create a *weak coherent state* with an average photon number of much less than one, such that more than one photon is rarely created [16]. However, to create single photon states on demand, or indeed any definite number of photons in the field, is difficult [79]. Both *number states* and *coherent states* of the electromagnetic field are now described in more detail.

The result of the quantisation of the electromagnetic field is the introduction of the non-Hermitian, and therefore non-observable [80], operators a and $a^\dagger$, which satisfy the following commutation relations [79]:

$$[a, a] \;=\; [a^\dagger, a^\dagger] = 0, \quad [a, a^\dagger] = 1. \tag{5.1}$$

The operators a and $a^\dagger$ are termed *annihilation* and *creation operators*, respectively [79], of photons in a single mode of the electromagnetic field [81], based on the outcome of their application to the *number states*, or *Fock states*.

The *number states* $|n\rangle$ form a complete orthogonal set. They are eigenstates of the number operator $N \;=\; a^\dagger a$

$$a^\dagger a|n\rangle \;=\; n|n\rangle. \tag{5.2}$$

The vacuum state of the field mode is defined by

$$a|0\rangle \;=\; 0. \tag{5.3}$$

Application of the annihilation and creation operators, respectively, to the number states yields

$$a|n\rangle \;=\; \sqrt{n}|n-1\rangle,\; a^\dagger|n\rangle \;=\; \sqrt{(n+1)}|n+1\rangle. \tag{5.4}$$

Another useful basis in which to represent the state space of the quantum state of light, is the basis of *coherent states*. The *coherent states* of the electromagnetic field modes $|\alpha\rangle$ may be defined as right eigenstates of the annihilation operator a with complex eigenvalue α

$$a|\alpha\rangle \;=\; \alpha|\alpha\rangle. \tag{5.5}$$

The conjugate state $\langle\alpha|$ is then the left eigenstate of the creation operator $a^\dagger$, as can be seen by taking the Hermitian conjugate of (5.5).

A coherent state representation is useful in terms of describing an indefinite number of photons that are in phase with each other. Using the orthogonality of the number states and normalising to unity, the coherent state $|\alpha\rangle$ is represented in the basis formed by the number states as

$$|\alpha\rangle \;=\; \mathrm{e}^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle, \tag{5.6}$$

where $|\alpha|^2$ is the expectation value of n, or the average photon number. The probability distribution of photons in a coherent state is a Poisson distribution

$$P(n) = |\langle n|\alpha\rangle|^2 = \frac{|\alpha|^{2n}\mathrm{e}^{-|\alpha|^2}}{n!}. \tag{5.7}$$

Due to the orthogonality of the number states, the inner product of coherent states is given by

$$\langle\alpha|\beta\rangle \;=\; \exp(-\frac{|\alpha|^2}{2}-\frac{|\beta|^2}{2}+\alpha^*\beta). \tag{5.8}$$

It follows that coherent states with average photon number of less than one are non-orthogonal when they have opposite phases

$$\langle\alpha|-\alpha\rangle \;=\; \mathrm{e}^{-2|\alpha|^2}. \tag{5.9}$$

A coherent state $|\alpha\rangle$ can also be created by a unitary transformation of the vacuum

$$|\alpha\rangle = D(\alpha)|0\rangle, \tag{5.10}$$

where $D(\alpha)$ is termed the *displacement operator*, and given by

$$D(\alpha) \equiv \mathrm{e}^{\alpha a^\dagger-\alpha^* a}. \tag{5.11}$$

The coherent state has the minimum uncertainty in amplitude and phase allowed by the uncertainty principle [82], and hence is the closest quantum mechanical state to a classical field [79]. Coherent states are particularly appropriate for the description of the electromagnetic fields generated by coherent sources, like lasers and parametric oscillators [81].

For more detail on the above description, see among others the books by Mandel and Wolf [81] and Walls and Milburn [79].

More recently, real single photon sources are nearing the reach of existing technologies. For example, there are qubit systems that can emit only one photon when the state makes a transition from the upper to lower energy level. Such systems may be trapped atoms or ions, or nitrogen-vacancy colour centres in diamond [16]. For a review of these and other approaches, see [83].

5.3 Phase modulation

The phase of a state of light changes as it evolves in time. A phase shifter is a transparent object that causes a state passing through it to evolve at a rate different to that in vacuum by a factor depending on the properties of the medium [40], thereby modulating the phase.

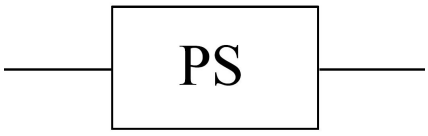

Figure 5.1: Symbolic diagram of a phase shifter.

The phase shift operator may be represented as $\mathrm{e}^{i\phi a^\dagger a}$, and the action of phase modulation on the coherent state $|\alpha\rangle$ calculated as

$$\begin{aligned} |\alpha\rangle &\stackrel{PS}{\rightarrow} \mathrm{e}^{i\phi a^\dagger a}|\alpha\rangle \\ &= \mathrm{e}^{-|\alpha|^2/2}\sum_{n=0}^{\infty}(\frac{\alpha}{\sqrt{n!}}\mathrm{e}^{i\phi})^n|n\rangle \\ &= |\alpha\mathrm{e}^{i\phi}\rangle. \end{aligned} \tag{5.12}$$

5.4 Beamsplitters

A beamsplitter can be realised by partially silvered glass, and is represented by a (complex) reflectance r and transmittance t. Consider a beamsplitter that acts on two input paths 0 and 1 which we will describe by creation operators $a_0^\dagger$ and $a_1^\dagger$ (see Fig. 5.2). Note, the beamsplitter transformation also applies to classical light, and the lines indicating the paths taken by the light correspond to these classical light rays, rather than the path taken by the photons [64]. Beamsplitter transformations for these operators in terms of creation operators $a_2^\dagger$ and $a_3^\dagger$ for output paths 2 and 3 are

$$a_0^\dagger \overset{BS}{\rightarrow} t' a_2^\dagger + r' a_3^\dagger, \quad a_1^\dagger \overset{BS}{\rightarrow} r a_2^\dagger + t a_3^\dagger. \tag{5.13}$$

To satisfy the commutation relations (5.1), the following relations must hold

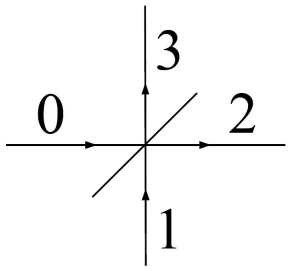

Figure 5.2: Symbolic diagram of a beamsplitter.

$$|r'| = |r|,\ |t| = |t'|,\ |r|^2 + |t|^2 = 1,\ r^* t' + r' t^* = 0 \text{ and } r^* t + r' t'^* = 0. \tag{5.14}$$

It is easy to show that these relations (5.14) are satisfied if

$$t = t' = \cos\theta,\ r = -\mathrm{e}^{-i\phi} \sin\theta \text{ and } r' = \mathrm{e}^{i\phi} \sin\theta. \tag{5.15}$$

These are the transmission and reflection coefficients, respectively, for a general beamsplitter with associated angles θ and ϕ. Collecting terms, the following relations between input paths 0 and 1 and output paths 2 and 3 are obtained

$$a_0^\dagger \overset{\text{BS}}{\rightarrow} \cos\theta a_2^\dagger + \mathrm{e}^{-i\phi} \sin\theta a_3^\dagger, \tag{5.16}$$

$$a_1^\dagger \overset{\text{BS}}{\rightarrow} -\mathrm{e}^{i\phi} \sin\theta a_2^\dagger + \cos\theta a_3^\dagger. \tag{5.17}$$

The matrix representation is more compact:

$$\begin{pmatrix} a_2^\dagger \\ a_3^\dagger \end{pmatrix} = \begin{pmatrix} \cos\theta & -\mathrm{e}^{i\phi}\sin\theta \\ \mathrm{e}^{-i\phi}\sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} a_0^\dagger \\ a_1^\dagger \end{pmatrix}. \tag{5.18}$$

The action of a beamsplitter on a coherent state in path 0 and the vacuum in path 1 is given in terms of the displacement operator $D(\alpha)$ (5.12) by

$$\begin{aligned} |\alpha\rangle_0|0\rangle_1 &= D_0(\alpha)|0\rangle_0|0\rangle_1 \\ &= \exp(\alpha a_0^\dagger - \alpha^* a_0)|0\rangle_0|0\rangle_1 \\ &\overset{\text{BS}}{\rightarrow} \exp[\alpha(\cos\theta a_2^\dagger + \mathrm{e}^{-i\phi}\sin\theta a_3^\dagger) \\ &\quad -\alpha^*(\cos\theta a_2 + \mathrm{e}^{i\phi}\sin\theta a_3)]|0\rangle_2|0\rangle_3 \\ &= \exp[(\alpha\cos\theta a_2^\dagger - \alpha^*\cos\theta a_2) \\ &\quad +(\alpha\mathrm{e}^{-i\phi}\sin\theta a_3^\dagger - \alpha^*\mathrm{e}^{i\phi}\sin\theta a_3)]|0\rangle_2|0\rangle_3 \\ &= D_2(\alpha\cos\theta)D_3(\alpha\mathrm{e}^{-i\phi}\sin\theta)|0\rangle_2|0\rangle_3 \\ &= |\alpha\cos\theta\rangle_2|\alpha\mathrm{e}^{-i\phi}\sin\theta\rangle_3. \end{aligned} \tag{5.19}$$

The action of a beamsplitter on coherent states in paths 0 and 1 is given by

$$\begin{aligned} |\alpha\rangle_0|\beta\rangle_1 &= D_0(\alpha)D_1(\beta)|0\rangle_0|0\rangle_1 \\ &= \exp(\alpha a_0^\dagger - \alpha^* a_0)\exp(\beta a_1^\dagger - \beta^* a_1)|0\rangle_0|0\rangle_1 \\ &\overset{\text{BS}}{\rightarrow} \exp[\alpha(\cos\theta a_2^\dagger + \mathrm{e}^{-i\phi}\sin\theta a_3^\dagger) - \alpha^*(\cos\theta a_2 + \mathrm{e}^{i\phi}\sin\theta a_3)] \\ &\quad \exp[\beta(-\mathrm{e}^{i\phi}\sin\theta a_2^\dagger + \cos\theta a_3^\dagger) + \beta^*(\mathrm{e}^{-i\phi}\sin\theta a_2 - \cos\theta a_3)]|0\rangle_2|0\rangle_3 \\ &= \exp[(\alpha\cos\theta a_2^\dagger - \alpha^*\cos\theta a_2) + (\alpha\mathrm{e}^{-i\phi}\sin\theta a_3^\dagger) - \alpha^*\mathrm{e}^{i\phi}\sin\theta a_3)] \times \\ &\quad \exp[-(\beta\mathrm{e}^{i\phi}\sin\theta a_2^\dagger - \beta^*\mathrm{e}^{-i\phi}\sin\theta a_2) + (\beta\cos\theta a_3^\dagger - \beta^*\cos\theta a_3)]|0\rangle_2|0\rangle_3 \\ &= D_2(\alpha\cos\theta - \beta\mathrm{e}^{i\phi}\sin\theta)D_3(\alpha\mathrm{e}^{-i\phi}\sin\theta + \beta\cos\theta)|0\rangle_2|0\rangle_3 \\ &= |\alpha\cos\theta - \beta\mathrm{e}^{i\phi}\sin\theta\rangle_2|\alpha\mathrm{e}^{-i\phi}\sin\theta + \beta\cos\theta\rangle_3. \end{aligned} \tag{5.20}$$

Here it is used that $D(\alpha)D(\beta) = \exp[(\alpha\beta^* - \alpha^*\beta)/2]D(\alpha+\beta)$, and in this case the exponential term contributes a factor of one to the overall phase.

5.5 Detectors

Photon detectors for *discrete variable* QKD (see Sec. 6.3) are usually avalanche photodiodes [45]. An electrical voltage is applied to semi-conductor, such

as silicon, germanium or indium gallium arsenide. The applied voltage is kept above the breakdown threshold so that when a photon hits the semiconductor, it is absorbed and causes an avalanche of electrons, which produces an electrical signal [16]. A *single-photon avalanche diode* is able to detect low intensity signals (down to a single photon) and to signal the arrival times of the photons with a jitter of a few tens of picoseconds [84].

However, the most commonly available photo-detectors are so-called *bucket detectors*, which can distinguish only between no photons, and one or more photons [85]. The action of a detector D that does not resolve photon num-

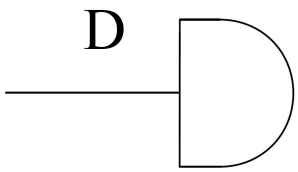

Figure 5.3: Symbolic diagram of a detector.

ber is described mathematically as a projective measurement $\{D_0, D_1\}$, with operators projecting onto the eigenspace of vacuum, or one or more photon number states. 'No click' corresponds to measurement outcome '0' which corresponds to an input of vacuum, and a 'click' corresponds to measurement outcome '1' which corresponds to the detection of a one or more photons. The projectors are given by

$$\begin{aligned} D_0 &= |0\rangle\langle 0| \\ D_1 &= \sum_{n=1}^{\infty} |n\rangle\langle n|. \end{aligned} \tag{5.21}$$

The probability of a click $p(D_1)$ when the input state is a coherent state is

$$\begin{aligned} p(D_1) &= 1 - \langle\alpha|0\rangle\langle 0|\alpha\rangle \\ &= 1 - \mathrm{e}^{-|\alpha|^2}. \end{aligned} \tag{5.22}$$

5.6 Conclusion

Quantum optics is the study of the nature and effects of light as a quantum system, and in this chapter a selection of aspects of quantum optics were

described in order to understand and provide a formal description of the *differential-phase-shift* (DPS) QKD protocol which is done is Chap. 7.

Chapter 6

Security and entanglement in general QKD protocols

"The future ability of quantum computers might be a decade or two away, their future ability to break public-key cryptography has important implications for the encryption of highly sensitive information today. For these applications, we must already design new ... cryptosystems ... that are immune to quantum cryptanalysis."

- ARDA, Report of the Quantum Information Science and Technology Experts Panel, 2004

QKD is a means of distributing a secure key to be used as a one-time pad between two parties, traditionally Alice and Bob, who wish to communicate privately.

A method of proving the unconditional security of the key, is to show that the QKD protocol is equivalent to an ED protocol (introduced in Sec. 1.10, further discussed in Sec 4.9).

For a general P&M QKD protocol to be equivalent to an ED protocol, Phase 1 of the protocol must first be shown to permit equivalent description as an EB QKD protocol where both Alice and Bob can use the available measurement results to show the existence of entanglement in the quantum state that is effectively distributed between them [28]. This implies that Bob's measurement must be described by non-commuting POVM elements (see Sec. 4.3.3).

Here, a general P&M protocol is described, and an EB translation of the protocol given. The condition on Bob's measurements in the EB scheme is derived. Finally, a brief discussion of unconditional security based on ED is given.

6.1 A P&M description of Phase 1 for a general QKD protocol

In 'P&M' terminology, Phase 1 of a general QKD protocol involves Alice preparing a set of quantum states into which a sequence of symbols has been encoded. More precisely:

A general P&M protocol specifies a quantum state $|\Psi(S)\rangle$ that encodes a sequence of N symbols $S = \{s_1, ..., s_N\}$ prepared by Alice. In many QKD protocols, $|\Psi(S)\rangle$ can be written in tensor product form where there is a one-to-one correspondence between each symbol s_i and each state $|\psi(s_i)\rangle$ that encodes that symbol:

$$|\Psi(S)\rangle \;=\; \bigotimes_{i=1}^{N} |\psi(s_i)\rangle. \tag{6.1}$$

The s_i's are independent and the state sent in each time interval i can be considered discretely as the state $|\psi(s_i)\rangle$. Note that the states $|\psi(s_i)\rangle$ must be non-orthogonal since a set of orthogonal states can be perfectly copied by a potential eavesdropper.

These states are then sent to Bob, who performs a set of measurements to decode the signal. Bob's measurement results are used in Phase 2 of the protocol which makes use of a public classical channel of which Alice and Bob are the authenticated users, to estimate the noise introduced by the quantum channel, visible through errors on the raw key which are conservatively attributed to eavesdropping. Subsequently, the classical channel is used to filter a secure key out of the initial sequence of symbols.

6.2 An EB description of Phase 1 of a general QKD protocol

The existence of an equivalent EB translation for a P&M QKD protocol was first shown by Bennett et al. in 1992 [20]. They showed that Phase 1 of BB84 (described in steps 1-4 in Sec. 1.6.1) can be equivalently described as an EB phase, described in steps 1-4 in Sec. 1.10, while Phase 2 of each protocol is identical. An equivalent EB translation of Phase 1 of a general P&M QKD protocol is attained through replacing Alice's preparation of a set of signals by Alice's preparation of a set of bipartite entangled states. She keeps one half of each pair and performs a measurement on her subsystem, sending the other to Bob, and effectively preparing the same set of quantum states described in the P&M picture. From Bob's perspective, the protocols are identical. More precisely:

In the EB translation of a general protocol, the bipartite entangled state

$$\begin{aligned} |\Phi\rangle_{AB} &= \frac{1}{\sqrt{D}} \sum_S |S\rangle_A |\Psi(S)\rangle_B \\ &= \frac{1}{\sqrt{D}} \sum_S |S\rangle_A \{ \bigotimes_{i=1}^{N} |\psi(s_i)\rangle \}_B \end{aligned} \tag{6.2}$$

is prepared, where D is the number of possible S sequences and the states $|S\rangle_A$ form an orthogonal basis. By measuring in this basis, Alice learns one sequence S and the corresponding $|\Psi(S)\rangle$ is effectively sent to Bob.

Since the s_i's are independent (and let them be of an alphabet of size d), $|\Phi\rangle_{AB}$ can also be written as

$$|\Phi\rangle_{AB} = \bigotimes_{i=0}^{N} (\frac{1}{\sqrt{d}} \sum_{s_i} |s_i\rangle_A \otimes |\psi(s_i)\rangle_B), \tag{6.3}$$

where the states $|s_i\rangle$ form an orthogonal basis.

Bob performs the same set of measurements on his subsystem as in the P&M scheme. Next in Phase 2 of the protocol, an authenticated public classical channel is employed to estimate the noise introduced by the quantum channel, visible through errors on the raw key which are conservatively attributed

to eavesdropping, and subsequently to filter a secure key out of the initial sequence of symbols.

6.3 Entanglement as precondition for security

QKD protocols can be divided into three families: *discrete-variable* (DV), *continuous-variable* (CV) and *distributed-phase-reference* (DPR) protocols [45].

A number of techniques have been used to show the unconditional security of DV protocols [12, 24, 15, 26], and security proofs for CV protocols are developing to a similar level [86]. For DV and CV protocols, the notion of virtual entanglement plays an essential role in security proofs based on ED [24, 15], which involve showing the equivalence of the protocol to an unconditionally secure ED protocol. For a general prepare-and-measure (P&M) QKD protocol to be equivalent to an ED protocol, Phase 1 of the protocol must permit equivalent description as an entanglement-based (EB) phase. Note that the EB version is not necessarily implemented (hence the word 'virtual'), but serves as a theoretical tool owing to its equivalence to the P&M scheme.

Curty et al. [28] demonstrated that a necessary precondition for unconditionally secure QKD is that both sender and receiver can use the available measurement results after Phase 1 is complete to prove the existence of entanglement in the quantum state that is effectively distributed between them in the EB translation of Phase 1. Such detection may involve only observed data and is realised by using the class of *entanglement witness operators* that can be constructed from these data.

That entanglement is a precondition for security is now demonstrated by assuming that Eve is limited to performing individual attacks. This limitation does not influence the necessity of the condition for security.

Let the classical data sets held by Alice, Bob and Eve during a QKD protocol before SKD is commenced be modelled by the random variables A, B and E,

respectively, with associated probabilities $p(a), p(b)$ and $p(e)$, respectively. The mutual information between the sender and receiver, Alice and Bob, conditional on the information that Eve has been estimated to have gained through eavesdropping $I(A:B|E)$ (3.8) is given by

$$I(A:B|E) = \sum_e p(e)[H(A|e) + H(B|e) - H(A,B|e)], \tag{6.4}$$

where $\sum_e p(e)H(A(B)|e)$ is the conditional Shannon entropy (3.6) of $A(B)$ given E, and $\sum_e p(e)H(A,B|e)$ is the joint Shannon entropy of A and B (3.5) conditional on E. The intrinsic information $I(A:B\downarrow E)$ (3.9) is defined in terms of the conditional mutual information $I(A:B|E)$ as:

$$I(A:B\downarrow E) = \inf_P I(A:B|E), \tag{6.5}$$

where P is the set of all possible extensions of the observable probability distribution $p(a,b)$ to $p(a,b,e)$, i.e. the set of all possible individual eavesdropping attacks on the communication between Alice and Bob.

Consider an EB description of Phase 1 of a general P&M QKD protocol as outlined in Sec. 6.2, in the case where the observable data $p(a,b)$, which describe the measurement outcomes of Alice and Bob, can be explained as having come from a mixed separable state

$$\sigma_{AB} = \frac{1}{d}\sum_{s_i} |s_i\rangle_A\langle s_i| \otimes |\psi(s_i)\rangle_B\langle\psi(s_i)|. \tag{6.6}$$

A separable reduced density matrix σ_{AB} can always be extended to a pure state of higher dimension:

$$\sigma_{AB} \;\rightarrow\; |\Psi\rangle_{ABE} = \frac{1}{\sqrt{d}}\sum_{s_i} |s_i\rangle_A|\psi(s_i)\rangle_B|e_i\rangle_E, \tag{6.7}$$

since

$$\begin{aligned}
\mathrm{Tr}_E\{|\Psi\rangle_{ABE}\langle\Psi|\} &= \mathrm{Tr}_E\{\frac{1}{d}\sum_{s_i} |s_i\rangle_A|\psi_i\rangle_B|e_i\rangle_E\langle s_i|_A\langle\psi_i|_B\langle e_i|_E\} \\
&= \frac{1}{d}\sum_{s_i} |s_i\rangle_A\langle s_i| \otimes |\psi_i\rangle_B\langle\phi_i| \otimes |\mathrm{Tr}\{|e_i\rangle_E\langle e_i|\} \\
&= \sigma_{AB}.
\end{aligned} \tag{6.8}$$

If Eve performs an attack that results in an extension of σ_{AB} to $|\Psi\rangle_{ABE}$ then a measurement of her subsystem in the basis $|e_j\rangle$ results in

$$|\Psi'\rangle_{ABE} = |s_j\rangle_A|\psi_j\rangle_B|e_j\rangle_E. \tag{6.9}$$

The conditional probability $p(a|e)$ on the state $|\Psi'\rangle_{ABE}$ is given by

$$\begin{aligned} p(a|e) &= \langle\Psi'|p(a)\otimes 1_B\otimes 1_E|\Psi'\rangle \\ &= \langle s_j|p(a)|s_j\rangle, \end{aligned} \tag{6.10}$$

the conditional probability $p(b|e)$ by

$$\begin{aligned} p(b|e) &= \langle\Psi'|1_A\otimes p(b)\otimes 1_E|\Psi'\rangle \\ &= \langle\psi(s_j)|p(b)|\psi(s_j)\rangle, \end{aligned} \tag{6.11}$$

and the joint conditional probability by

$$\begin{aligned} p(a,b|e) &= \langle\Psi'|p(a)\otimes p(b)\otimes 1_E|\Psi'\rangle \\ &= \langle s_j|p(a)|s_j\rangle\langle\psi(s_j)|p(b)|\psi(s_j)\rangle \\ &= p(a|e)p(b|e). \end{aligned} \tag{6.12}$$

It is not hard to show that if $p(a,b) = p(a)p(b)$, then $H(A,B) = H(A) + H(B)$, which implies that the mutual information $I(A:B|E) = 0$. Therefore, the intrinsic information $I(A:B\downarrow E)$ is also zero.

So, in the case where the observable data $p(a,b)$, which are the measurement outcomes of Alice and Bob, can be interpreted as having come from a mixed separable state σ_{AB}, there exists an attack such that the mutual information between Alice and Bob, conditional on the information that Eve has gained through eavesdropping, is zero, and thus, no secret key can be distilled via classical communication.

Having shown that a protocol can be secure only if $p(a,b)$ can be interpreted as having come from an entangled state, it remains to consider how Alice and Bob can use the available measurement results to prove the existence of entanglement in the entangled quantum state that is effectively distributed between them.

A theorem by Curty et al. [28] provides the answer to this question and

is stated formally below:

Entanglement as a precondition for secure QKD
A necessary precondition for a set of POVM elements $F_a \otimes G_b$ together with the probability distribution of their occurrence $p(a,b)$ to lead to a secret key via public communication is that the presence of entanglement in the effectively distributed state $|\Phi\rangle_{AB}$ can be detected via an entanglement witness $W = \sum_{ab} c_{ab} F_a \otimes G_b$ with c_{ab} real such that $Tr(W\sigma) \geq 0$ for all separable states and $Tr(W\rho) < 0$ for at least one entangled state.

Here, the theorem itself is not examined further, but the implication that Bob's measurement must contain some non-commuting operators is shown.

6.4 Bob's measurement

Suppose $W = \sum_{ab} c_{ab} F_a \otimes G_b$ is an entanglement witness with c_{ab} real such that $\mathrm{Tr}(W\sigma) \geq 0$ for all separable states and $\mathrm{Tr}(W\rho) < 0$ for at least one entangled state, and that F_a and G_b are Alice and Bob's POVM elements in the EB translation of a QKD protocol. Assume that in each time interval Alice projects onto the set of orthogonal states $|A\rangle$, and that Bob projects onto the set of orthogonal states $|B\rangle$. Then W is diagonal in the basis $\{|A\rangle_A, |B\rangle_B\}$:

$$W = \sum_{A,B} \lambda_{AB} |A\rangle_A\langle A| \otimes |B\rangle_B\langle B|. \tag{6.13}$$

Since W is a witness and $\mathrm{Tr}(W\sigma) \geq 0$ for all separable states σ, it follows that the expectation value of the witness W $\langle \Psi_{\mathrm{sep}}|W|\Psi_{\mathrm{sep}}\rangle$ is greater than or equal to zero for all pure bipartite separable states, including the state

$$|\Psi_{\mathrm{sep}}\rangle = |\alpha\rangle_A|\beta\rangle_B. \tag{6.14}$$

Thus

$$\langle\alpha|_A\langle\beta|_B\{\sum_{A,B} \lambda_{AB}|A\rangle_A\langle A| \otimes |B\rangle_B\langle B|\}|\alpha\rangle_A|\beta\rangle_B \;\geq\; 0, \tag{6.15}$$

which implies that

$$\sum_{A,B} \lambda_{AB}\langle\alpha|A\rangle\langle\beta|B\rangle\langle A|\alpha\rangle\langle B|\beta\rangle \;\geq\; 0, \tag{6.16}$$

which in turn implies that

$$\lambda_{AB} \geq 0. \tag{6.17}$$

Since W has diagonal representation $\sum_i \lambda_i |i\rangle\langle i|$ with λ_i non-negative, W is a positive operator. Therefore, $\langle\psi|W|\psi\rangle \geq 0$ for all $|\psi\rangle$ including all entangled states and as a result, W cannot be an entanglement witness and the protocol cannot lead to a secret key via public communication.

In the EB translation of a P&M protocol, Alice is assumed to project onto a set of orthogonal states. Therefore, a necessary condition for the security of a QKD protocol is that the POVM elements constituting Bob's measurement, which are the same in both translations, are not all mutually commuting. This result should not be surprising since in an intercept-and-resend attack on a P&M protocol where Bob's measurement is described by only commuting operators, an eavesdropper could measure an observable which commutes with all of Bob's operators without changing the statistics of Bob's measurement, thus remaining undetected. Therefore, a precondition for security is that some of the POVM elements describing Bob's measurement must be non-commuting.

6.5 Entanglement distillation

ED protocols aim at the distillation of pure maximally entangled states from a larger set of mixed non-maximally entangled states, through the performance by Alice and Bob of LOCC (see Sec. 4.9.2, and the article by Lo and Chau [24] for further details). If the resulting entangled states have a fidelity of close to 1 to a maximally entangled state like that in Eq. (1.5), then Eve's information approaches zero for all possible attacks allowed by the laws of quantum mechanics, and Alice and Bob's perfectly correlated measurement results can be used as a secret key.

Showing that a QKD protocol is equivalent to such an unconditionally secure ED protocol will thus imply the unconditional security of the original protocol.

6.6 Conclusion

Here, a general P&M protocol was discussed as an introduction to the next chapter, where a similar analysis of the *Differential-Phase-Shift* QKD protocol is performed.

Chapter 7

Security and entanglement in DPSQKD

"... distributed-phase-reference protocols were invented by experimentalists, looking for practical solutions. ... It has not yet been possible to derive a bound for [their] unconditional security, because the existing techniques apply only when $|\Psi(S)\rangle$ can be decomposed in independent signals."

- Scarani et al. [45]

In 2003 Inoue et al. [30] proposed the modified version of the DPSQKD protocol, an example of a DPR protocol. Along with other DPR protocols, like the coherent-one-way (COW) [87, 88] QKD protocol, a bound for the unconditional security of DPSQKD, has not yet been found.

Here a brief history of DPSQKD is given. Then Phase 1 of DPSQKD is described and formalised as both a P&M and an EB phase. Bob's measurement is shown to be described by non-commuting POVM elements. The EB translation of DPSQKD given here is a necessary first step towards an unconditional security proof for the protocol based on ED. Finally, thoughts on a potential unconditional security proof based on ED for a DPSQKD-like protocol are given.

7.1 A brief history of the protocol

The DPSQKD protocol was first proposed by Inoue et al. in 2002 [29]. The modified version of DPSQKD to be discussed here was proposed by the same authors in the next year [30], as a scheme offering a higher key creation efficiency than conventional fibre-based BB84. In 2006 Waks et al. [89] derived a proof of the security of DPSQKD under the assumption that Eve is restricted to individual attacks. They showed that individual attacks are more powerful than certain so-called sequential attacks, thus ensuring security against this form of attack also. In the same year Diamanti et al. [90] reported an implementation of DPSQKD secure against individual attacks over 100km. In 2007 Tsurumaru [91] introduced an improved version of the aforementioned sequential attack that decreases the distance over which DPSQKD is secure to less than 95km, thus rendering the above implementation insecure. In 2008 Zhao et al. [92] showed the security of DPSQKD against collective attacks in the noiseless case. In 2009 Ma et al. [93] reported an implementation of DPSQKD using superconducting single-photon detectors, with a quantum bit error rate of less than 4%. Later in 2009, a proof of the unconditional security of a protocol related to DPSQKD, using single photons instead of coherent pulses, was published by Wen et al. [94]. However, this proof does not imply the unconditional security of the original DPSQKD protocol.

There are a number of practical advantages to DPSQKD, namely: its suitability for fibre transmissions; use of readily available telecommunication tools; no requirement for a single photon source (the generated states are assumed to be easily produced coherent states) and thus high communication efficiency. However, bounds for the unconditional security of DPSQKD, and other examples of DPR like the COW protocol, have not yet been found. An EB translation of a P&M QKD protocol where the precondition for security on Bob's measurement is satisfied, is a necessary first step towards a potential unconditional security proof for the protocol based on ED. Such an EB translation of DPSQKD is absent from the literature: the starting point is a P&M description of Phase 1 of the protocol.

7.2 A P&M description of Phase 1 of the DPSQKD protocol

In DPSQKD Alice prepares a sequence of $N+1$ symbols $S' = \{s'_0, ..., s'_N\}$, $s'_i \in \{0, 1\}$, according to which she modulates the phase of each of $N+1$ attenuated coherent pulses by $\{0, \pi\}$. The pulses are separated by a time Δt. After modulation the phase of the i^{th} pulse is given by $\phi_i = s'_i \pi$. From the bit string S' Alice calculates the potential key bit string S via the relation $s_i = s'_{i-1} \oplus s'_i$, where $\oplus$ represents addition modulo 2. Let the time intervals in which Alice sends the pulses be $i = 0, ..., N$. The quantum state $|\Psi(S')\rangle_{DPS}$ that encodes the sequence S' can then be written as

$$|\Psi(S')\rangle_{DPS} = \bigotimes_{i=0}^{N} |(-1)^{s'_i}\alpha\rangle \tag{7.1}$$

(compare with Eq. (6.1)). The requirement of non-orthogonality of the states $|\psi(s'_i)\rangle$ (compare with $|\psi(s_i)\rangle$ from Sec. 6.1) is met, since the coherent pulses have an average photon number $|\alpha|^2$ of less than one (see Eq. (5.9)).

The state sent in each time interval i can be considered independently if written (as above) as $|(-1)^{s'_i}\alpha\rangle$. Here, there is a one-to-one correspondence between each symbol s'_i and each state $|\psi(s'_i)\rangle$ encoding that symbol, but since the consecutive elements of S are not independent there is no such correspondence between potential key bits and prepared states, as in the general case in Sec 6.1. And this is the reason existing methods of proving unconditional security cannot be applied to the DPSQKD protocol, since they rely on the mutual independence of all potential key bits. However, the form of Eq. (7.1) allows a formulation of P&M DPSQKD as an equivalent EB scheme, which is done in the next section.

At Bob's location, the i^{th} incoming pulse is split at BS_1. The part which propagates on path 3 arrives at BS_2 simultaneously with the part of the $(i+1)^{\text{th}}$ pulse coming from path 2. Bob's measurement is initiated at a time Δt after the first pulse has entered his interferometer, in time interval $i = 1$, and there is the possibility of a detection event that can contribute to the key in this and subsequent time intervals up to $i = N$. The transformation of $|\Psi(S)\rangle_{DPS}$ in Bob's interferometer forms part of his measurement (see Fig. 7.1) and is described by the following transformations:

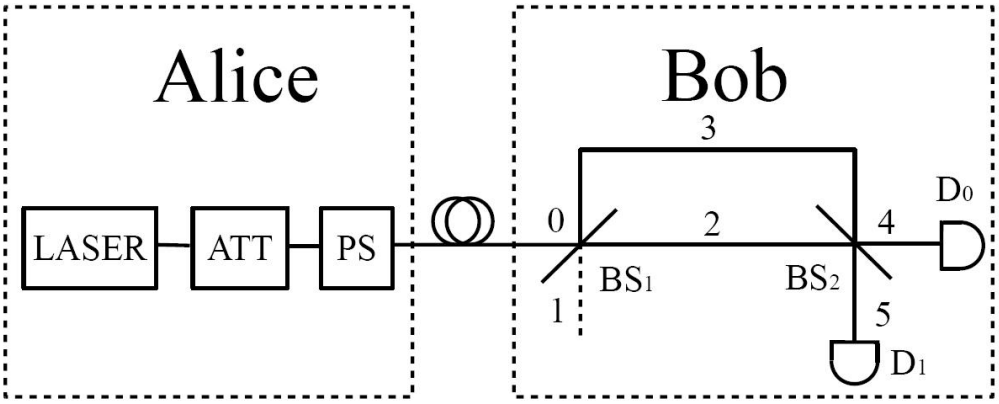

Figure 7.1: Quantum key distribution system for the implementation of the DPSQKD protocol. The paths through Bob's interferometer are labelled 0-5. LASER: coherent light source, ATT: attenuator, PS: phase shifter, BS: symmetric beamsplitter, D: detector.

The incoming pulses enter symmetric beamsplitter 1 (BS_1) in the path labelled 0 and are described by creation operators $a_0^\dagger$, while path 1 contains vacuum. The beamsplitter transformation for $a_0^\dagger$ in terms of operators $a_2^\dagger$ and $a_3^\dagger$ for the output paths labelled 2 and 3 (see Sec. 5.4) is

$$a_0^\dagger \overset{BS1}{\rightarrow} \frac{1}{\sqrt{2}} a_2^\dagger + \mathrm{e}^{-i\phi_1} \frac{1}{\sqrt{2}} a_3^\dagger. \tag{7.2}$$

Transformations for symmetric beamsplitter 2 (BS_2) (with an orientation rotated through $\frac{\pi}{2}$ relative to BS_1) in terms of operators $a_4^\dagger$ and $a_5^\dagger$ for the output paths labelled 4 and 5, are then derived to be

$$a_2^\dagger \overset{BS2}{\rightarrow} \frac{1}{\sqrt{2}} a_4^\dagger - \mathrm{e}^{i\phi_2} \frac{1}{\sqrt{2}} a_5^\dagger, \tag{7.3}$$

$$a_3^\dagger \overset{BS2}{\rightarrow} \mathrm{e}^{-i\phi_2} \frac{1}{\sqrt{2}} a_4^\dagger + \frac{1}{\sqrt{2}} a_5^\dagger. \tag{7.4}$$

In terms of the creation operators for each time interval i for the signals entering Bob's interferometer in path 0, $a_0^{\dagger i}$, and the two outgoing paths, $a_4^{\dagger i}$

and $a_5^{\dagger i}$, the total action of the interferometer is described as

$$\begin{aligned} a_0^{\dagger i} &\xrightarrow{I} \frac{1}{2}(a_4^{\dagger i} - \mathrm{e}^{i\phi_2} a_5^{\dagger i} + \mathrm{e}^{i(\phi_{\Delta t}-\phi_1)}(\mathrm{e}^{-i\phi_2} a_4^{\dagger(i+1)} + a_5^{\dagger(i+1)}),) \\ &= \frac{1}{2}(a_4^{\dagger i} - \mathrm{e}^{i\phi_2} a_5^{\dagger i} + a_4^{\dagger(i+1)} + \mathrm{e}^{i\phi_2} a_5^{\dagger(i+1)}), \end{aligned} \tag{7.5}$$

where the beamsplitters are chosen such that their relative phase shifts compensate the phase shift associated with the time delay in the interferometer, i.e., $\phi_1 + \phi_2 = \phi_{\Delta t}$. The time delay Δt in the interferometer must be equal to the time separation between incoming pulses in path 0, so that components of consecutive pulses can interfere at BS2.

If Alice sends the state $|\Psi(S')\rangle_{DPS}$, the state $|\Psi'(S')\rangle_{DPS}$ entering Bob's detectors in time intervals i in paths 4 and 5 after transformation in the interferometer, is expanded as

$$\begin{aligned} |\Psi'(S')\rangle_{DPS} &= \bigotimes_{i=1}^{N} |\frac{1}{2}\alpha(\mathrm{e}^{i\phi_i} + \mathrm{e}^{i\phi_{i-1}})\rangle_4^i |\frac{1}{2}\alpha \mathrm{e}^{i\phi_2}(\mathrm{e}^{i\phi_i} - \mathrm{e}^{i\phi_{i-1}})\rangle_5^i \\ &= \bigotimes_{i=1}^{N} |\frac{1}{2}\alpha((-1)^{s'_i} + (-1)^{s'_{i-1}})\rangle_4^i |\frac{1}{2}\alpha \mathrm{e}^{i\phi_2}((-1)^{s'_i} - (-1)^{s'_{i-1}})\rangle_5^i, \end{aligned} \tag{7.6}$$

recalling that $\phi_i = s'_i \pi$.

Bob uses detectors D_0 and D_1 that discern vacuum from one or more photons (so-called bucket detectors see Sec. 5.5), in paths 4 and 5, respectively. A detector 'click' will occur when one or more photons are detected. For an incoming coherent state $|\beta\rangle_4 (|\beta\rangle_5)$, detector $D_0(D_1)$ will click with probability $1 - \mathrm{e}^{-|\beta|^2}$. These probabilities depend on the phase modulation performed by Alice, which is determined by the bit string S'. For $s'_i + s'_{i-1} = s_i = 0(1)$, the probability of $D_1(D_0)$ clicking is zero, and hence a click in $D_0(D_1)$ corresponds to $s_i = 0(1)$. This situation is summarised in Table 1.

Note, the probability of a detector firing is independent of the phase, and therefore Bob cannot distinguish the two states $|\alpha\rangle^i$ and $|-\alpha\rangle^i$ that correspond to one s_i.

Table 7.1: DPSQKD detection and key extraction table

s'_{i-1}	s'_i	s_i	$\|\psi\rangle^i$	$p(D_0)$	$p(D_1)$
0	0	0	$\|\alpha\rangle_4\|0\rangle_5$	$1-\mathrm{e}^{-\|\alpha\|^2}$	0
1	1	0	$\|-\alpha\rangle_4\|0\rangle_5$	$1-\mathrm{e}^{-\|\alpha\|^2}$	0
0	1	1	$\|0\rangle_4\|\alpha\mathrm{e}^{\phi_2}\rangle_5$	0	$1-\mathrm{e}^{-\|\alpha\|^2}$
1	0	1	$\|0\rangle_4\|-\alpha\mathrm{e}^{\phi_2}\rangle_5$	0	$1-\mathrm{e}^{-\|\alpha\|^2}$

Bob then utilises the authenticated classical channel to communicate to Alice the time intervals i^* in which he recorded a detection event in one of his detectors (which is not in every time interval since the average photon number $|\alpha|^2$ per pulse is less than one). This process serves to filter a secure key S^* out of the initial sequence S, since (in the absence of error) for each i^* Alice and Bob can add an identical bit, s_{i^*}, to the secure filtered key.

7.3 An EB description of Phase 1 of the DPSQKD protocol

In the EB translation of DPSQKD, the bipartite entangled state

$$\begin{aligned} |\Phi_{DPS}\rangle_{AB} &= \frac{1}{\sqrt{2^{N+1}}}\sum_{S'}|S'\rangle_A\otimes(|\Psi(S')\rangle_{DPS})_B \\ &= \frac{1}{\sqrt{2^{N+1}}}\sum_{S'}|S'\rangle_A\otimes(\bigotimes_{i=0}^{N}|(-1)^{s'_i}\alpha\rangle)_B, \end{aligned} \tag{7.7}$$

is prepared (compare with Eq. (6.2)).

The total entangled state $|\Phi_{DPS}\rangle_{AB}$ can also be written as

$$\begin{aligned} |\Phi_{DPS}\rangle_{AB} &= \bigotimes_{i=0}^{N} \left(\frac{1}{\sqrt{2}} \sum_{s'_i=0,1} |s'_i\rangle_A \otimes |\psi(s'_i)\rangle_B \right) \\ &= \bigotimes_{i=0}^{N} \left(\frac{1}{\sqrt{2}} \sum_{s'_i=0,1} |s'_i\rangle_A \otimes |(-1)^{s'_i}\alpha\rangle_B \right) \\ &= \bigotimes_{i=0}^{N} \left(\frac{1}{\sqrt{2}} \{|0\rangle_A \otimes |\alpha\rangle_B + |1\rangle_A \otimes |-\alpha\rangle_B\} \right)^i \end{aligned} \tag{7.8}$$

where the states $|0\rangle$ and $|1\rangle$ form the arbitrary orthogonal basis in which Alice measures, and correspond to $s'_i = 0$ or 1 respectively. Again, there is a one-to-one correspondence between each s'_i and each state $|\psi(s'_i)\rangle$ encoding that symbol, although the potential key bits s_i are not independent of each other.

Consequences of this non-independence are that Alice must keep track of the time intervals to which her measurement outcomes correspond, thus incrementally building her knowledge of the string S via the relation $s_i = s'_{i-1} + s'_i$. Subsequent to Alice's projections in the arbitrary orthogonal basis $\{|0\rangle, |1\rangle\}$ performed on her subsystem, the resulting string of attenuated coherent pulses that form Bob's subsystem must be separated by the same time delay associated with the delay in Bob's interferometer, Δt. Bob learns a fraction $|\alpha|^2$ of the key bits s_i in string S by interfering consecutive pulses to learn their relative phases. He performs the same total measurement as in the P&M description.

7.4 Bob's measurement

Bob's measurement can be described conveniently in the framework of generalised measurements, where the measurement statistics are given by a POVM (see Sec. 4.3.3). The POVM associates with each measurement result m, a positive operator E_m, termed a POVM element, or an *effect*. The expectation value of the effect E_m determines the probability to obtain result m:

$$p_m = \langle\psi|E_m|\psi\rangle \,, \tag{7.9}$$

where $|\psi\rangle$ is the state just before the measurement is carried out. The effects satisfy $\sum_m E_m = 1$ in order to guarantee that the probabilities sum up to unity. In this formalism, projection measurements (see Sec. 4.3.2) of quantum mechanical observables are described by effects which are mutually commuting projectors onto the eigenspaces corresponding to the measurement results. In general, however, the effects are neither projectors nor do they commute.

A necessary requirement for the shared bit string to be secret is that the performed measurements must be able to detect entanglement in the state effectively distributed between Alice and Bob in the EB scheme [28]. This is not possible if Bob's measurement results correspond only to mutually commuting effects (see Sec. 6.4). This condition applies also to the P&M version of any QKD protocol, where the measurements must be the same as in the equivalent EB transcription. In an intercept-and-resend attack on a P&M protocol where Bob's measurement is described by only commuting effects, an eavesdropper could measure an observable which commutes with all of Bob's effects without changing the statistics of Bob's measurement and thus remain undetected. Therefore, a precondition for security is that some of the effects constituting Bob's measurement must be non-commuting.

In DPSQKD, Bob's measurement is associated with a total number 2^{2N} of possible results and as many corresponding effects, since in the time intervals $i \in \{1, ..., N\}$, he projects either onto vacuum or a one-or-more photon state in two detectors, D_0 and D_1. He obtains an average of $|\alpha|^2 N$ detection events which contribute to the key. The effects constituting Bob's measurement are written as follows:

$$
\begin{aligned}
G_1 &= |0\rangle_4^1\langle 0| \otimes |0\rangle_5^1\langle 0| \otimes |0\rangle_4^2\langle 0| \otimes |0\rangle_5^2\langle 0| ... \otimes |0\rangle_4^N\langle 0| \otimes |0\rangle_5^N\langle 0|, \\
G_2 &= \sum_{n=1}^{\infty} |n\rangle_4^1|n\langle \otimes |0\rangle_5^1\langle 0| \otimes |0\rangle_4^2\langle 0| \otimes |0\rangle_5^2\langle 0| ... \otimes |0\rangle_4^N\langle 0| \otimes |0\rangle_5^N\langle 0|, \\
G_3 &= |0\rangle_4^1\langle 0| \otimes |0\rangle_5^1\langle 0| \otimes |0\rangle_4^2\langle 0| \otimes \sum_{n=1}^{\infty} |n\rangle_5^2\langle n| ... \otimes |0\rangle_4^N\langle 0| \otimes |0\rangle_4^N\langle 0| \\
&\vdots \quad , \\
G_{2^{2N}} &= \sum_{n=1}^{\infty} |n\rangle_4^1\langle n| \otimes \sum_{n=1}^{\infty} |n\rangle_5^1\langle n| ... \sum_{n=1}^{\infty} |n\rangle_4^N\langle n| \otimes \sum_{n=1}^{\infty} |n\rangle_5^N\langle n|. \qquad (7.10)
\end{aligned}
$$

Bob's measurement is thus seen to be a degenerate projection measurement of photon number, where $[G_x, G_y] = 0$ for all x, y, since the inner product of vacuum with a one-or-more photon state is always zero. It is easy to show that this result does not change if Bob's interferometer is considered as part of his measurement apparatus. Since the action of an interferometer is unitary, the result for the transformed effects remains the same: $[U^\dagger G_x U, U^\dagger G_y U] = 0$. At this point the protocol appears to be insecure! In the remainder of this section it will be shown that the necessary condition on Bob's measurement - the non-commutativity of effects- nevertheless is met.

For this purpose, recall that Bob's interferometer has two input paths (path 0 and path 1, see Fig. 7.1). Only path 0 is populated, it carries the light sent by Alice in state $|\psi\rangle_0 \equiv |\Psi(S')\rangle_{DPS}$ (see Eq. (7.1)), while path 1 contains the vacuum state $|0\rangle_0$ at all times. When including the interferometer in Bob's measurement, the probability to obtain any result $m \in \{1, 2..., 2^{2N}\}$ can be expressed by means of the state $|\Phi\rangle \equiv |\psi\rangle_0 \otimes |0\rangle_1$ of the light entering the interferometer as:

$$\begin{aligned} p_m &= \langle\Phi|U^\dagger G_m U|\Phi\rangle = {}_0\langle\psi|E_m|\psi\rangle_0 \\ \text{with} \quad E_m &\equiv {}_1\langle 0|U^\dagger G_m U|0\rangle_1 \,. \end{aligned} \tag{7.11}$$

While the action of the interferometer is represented by the operator U which maps the incoming state in paths 0 and 1 to the the outgoing state in paths 4 and 5, the new effects E_m are operators that act only on states in path 0. The expectation value with respect to the vacuum state in path 1 reduces the action of the operator $U^\dagger G_m U$ to the subspace of states in path 0, similarly to a partial trace. According to Eq. (7.11), the probability for any of Bob's measurement results can thus be expressed only in terms of the state sent by Alice using effects E_m. It is well known that such a reduction of a projective-measurement as given by the effects $U^\dagger G_m U$ can result in a POVM with non-commuting effects. In fact, any POVM can be represented as a projective measurement acting on a higher dimensional Hilbert space (see Sec. 4.3.3 and Neumark's theorem [67]).

In illustration, recall the action of the interferometer (7.5) on the signals entering Bob's interferometer in path 0, $a_0^{\dagger i}$, and the two outgoing paths, $a_4^{\dagger i}$

and $a_5^{\dagger i}$:

$$\begin{aligned} a_0^{\dagger i} &\xrightarrow{I} \frac{1}{2}(a_4^{\dagger i} - \mathrm{e}^{i\phi_2} a_5^{\dagger i} + \mathrm{e}^{i(\phi_{\Delta t} - \phi_1)}(\mathrm{e}^{-i\phi_2} a_4^{\dagger (i+1)} + a_5^{\dagger (i+1)})), \\ &= \frac{1}{2}(a_4^{\dagger i} - \mathrm{e}^{i\phi_2} a_5^{\dagger i} + a_4^{\dagger (i+1)} + \mathrm{e}^{i\phi_2} a_5^{\dagger (i+1)}). \end{aligned} \tag{7.12}$$

The matrix M_I corresponding to the action of the interferometer on the reduced Hilbert space of the relevant input paths *only* in each time interval is non-unitary, and is given by

$$M_I = \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 0 & \dots & 0 \\ -\mathrm{e}^{i\phi_2} & 0 & 0 & 0 & \dots & 0 \\ 1 & 1 & 0 & 0 & \dots & 0 \\ \mathrm{e}^{i\phi_2} & -\mathrm{e}^{i\phi_2} & 0 & 0 & \dots & 0 \\ 0 & 1 & 1 & 0 & \dots & 0 \\ 0 & \mathrm{e}^{i\phi_2} & -\mathrm{e}^{i\phi_2} & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & \mathrm{e}^{i\phi_2} \end{pmatrix}.$$

The non-unitarity of M_I is easily understood via the Stinespring-Kraus theorem [65], which states that any quantum operation realised in system A corresponds to a unitary transformation performed on a system with a larger Hilbert space $\mathcal{H}_{AB}$ (see Sec. 4.3.3).

With respect to the necessary condition on Bob's measurements, indeed, the resulting effects E_m are not all mutually commuting, and therefore satisfy the necessary condition for security. Consider the effects E_2 and E_3 that correspond to a click in D_0 in time interval 1 and a click in D_1 in time interval 2, respectively:

$$E_2 = {}_1\langle 0|U^\dagger G_2 U|0\rangle_1 = M_I^\dagger G_2 M_I = \sum_{n=1}^{\infty} \frac{1}{4^n n!}(a_0^{\dagger 0} + a_0^{\dagger 1})^n |0\rangle\langle 0|(a_0^0 + a_0^1)^n, \tag{7.13}$$

$$E_3 = {}_1\langle 0|U^\dagger G_3 U|0\rangle_1 = M_I^\dagger G_3 M_I = \sum_{m=1}^{\infty} \frac{1}{4^m m!}(a_0^{\dagger 1} - a_0^{\dagger 2})^m |0\rangle\langle 0|(a_0^1 - a_0^2)^m. \tag{7.14}$$

The commutator $[E_2, E_3]$ is given by:

$$\begin{aligned}[E_2, E_3] &= \sum_{n=1}^{\infty} \frac{1}{4^n n!}(a_0^{\dagger 0} + a_0^{\dagger 1})^n |0\rangle T \sum_{m=1}^{\infty} \frac{1}{4^m m!}\langle 0|(a_0^1 - a_0^2)^m \\ &\quad - \sum_{m=1}^{\infty} \frac{1}{4^m m!}(a_0^{\dagger 1} - a_0^{\dagger 2})^m |0\rangle T \sum_{n=1}^{\infty} \frac{1}{4^n n!}\langle 0|(a_0^0 + a_0^1)^n, \quad (7.15)\end{aligned}$$

where the term T is defined and evaluated as:

$$\begin{aligned}T &\equiv \langle 0|(a_0^0 + a_0^1)^n (a_0^{\dagger 1} - a_0^{\dagger 2})^m |0\rangle \\ &= \sum_{k=0}^{n}\sum_{l=0}^{m} \binom{n}{k}\binom{m}{l}(-1)^l \langle 0|(a_0^0)^{n-k}(a_0^1)^k (a_0^{\dagger 1})^{m-l}(a_0^{\dagger 2})^l |0\rangle \\ &= n!, \quad (7.16) \\ &\text{with} \quad n = m = k \,\text{and}\, l = 0.\end{aligned}$$

Note that $T = T^*$ is a non-zero real number.

The commutator $[E_2, E_3]$ is then given by:

$$\begin{aligned}[E_2, E_3] &= \sum_{n=1}^{\infty}\sum_{l=0}^{n}\sum_{k=0}^{n} \frac{1}{16^n n!}\binom{n}{l}\binom{n}{k} \\ &\quad \times \{(-1)^k (a_0^{\dagger 0})^{n-l}(a_0^{\dagger 1})^l |0\rangle\langle 0|(a_0^1)^{n-k}(a_0^2)^k \\ &\quad -(-1)^l (a_0^{\dagger 1})^{n-l}(a_0^{\dagger 2})^l |0\rangle\langle 0|(a_0^0)^{n-k}(a_0^1)^k\} \\ &\neq 0. \quad (7.17)\end{aligned}$$

Since the operators $a_0^{(\dagger)0}$, $a_0^{(\dagger)1}$ and $a_0^{(\dagger)2}$ act on different Hilbert spaces, the matrix elements do not cancel. Therefore all terms in the sum are non-zero.

It has therefore been shown that there do exist non-commuting POVM elements in Bob's measurement in the EB translation of DPSQKD, i.e., $[E_2, E_3] \neq 0$, which is a necessary requirement for the detection of entanglement in the effectively distributed state. This result can be understood in terms of Neumark's theorem [67], from which it follows that a non-commuting generalised measurement on a certain Hilbert space can be realised as a projective measurement on a higher dimensional Hilbert space.

The protocol has thus been shown to satisfy a necessary condition for security, i.e. that Bob's measurement involves non-commuting effects. An EB translation of a P&M QKD protocol where the condition on Bob's measurement is met, is a necessary first step towards a security proof based on ED. It remains to show whether an unconditional security proof based on ED can be performed.

7.5 Thoughts

Following Phase 1 of DPSQKD which was described in Sec. 7.2 and 7.3 as a P&M and an EB phase respectively, Phase 2 of the protocol is commenced.

This involves Bob utilising the authenticated classical channel to communicate to Alice the time intervals i^* in which he recorded a detection event in one of his detectors (which is not in every time interval since the average photon number $|\alpha|^2$ per pulse is less than one). In the absence of error Alice and Bob can then add an identical bit s_{i^*} to the filtered key S^* for each time interval i^*. Given that imperfect devices and possible eavesdropping result in errors in the key, classical error correction and privacy amplification algorithms can then be implemented. The difficulty in proving unconditional security is to estimate an upper limit on Eve's information given the average bit error rate on the key, assuming that she is allowed to perform any action allowed by the laws of quantum mechanics.

With regard to the aim of showing DPSQKD equivalent to an ED protocol thereby proving its unconditional security, the question is whether Phase 2 of DPSQKD can be related to a process that distills entanglement from the $N + 1$ pairs shared by Alice and Bob after the EB description of Phase 1.

The difficulty in deriving a bound for the unconditional security of DPSQKD is that unlike in general QKD protocols where there is a one-to-one correspondence between each symbol s_i and each state $|\psi(s_i)\rangle$ encoding that symbol, in DPSQKD, the consecutive elements of S are not independent and there is no such correspondence between potential key bits and prepared states. And this is the reason existing methods of proving unconditional security cannot be applied to the DPSQKD protocol, since they rely on the mutual

independence of all potential key bits.

This problem is circumvented in the following novel EB DPSQKD-like protocol:

7.6 EB DPSQKD-like protocol

Consider an EB QKD protocol where the following bipartite entangled state $|\Phi\rangle_{AB}$ is prepared:

$$\begin{aligned} |\Phi\rangle_{AB} &= \bigotimes_{i=0}^{N}\{\frac{1}{\sqrt{2}}(|\alpha\rangle^i_{A_0}|\alpha\rangle^i_{B_0} + |-\alpha\rangle^i_{A_0}|-\alpha\rangle^i_{B_0})\} \\ &= \frac{1}{\sqrt{2}^{(N+1)}}\{(|\alpha\rangle^0_{A_0}|\alpha\rangle^0_{B_0} + |-\alpha\rangle^0_{A_0}|-\alpha\rangle^0_{B_0}) \\ &\quad \otimes(|\alpha\rangle^1_{A_0}|\alpha\rangle^1_{B_0} + |-\alpha\rangle^1_{A_0}|-\alpha\rangle^1_{B_0}) \\ &\quad \otimes(|\alpha\rangle^2_{A_0}|\alpha\rangle^2_{B_0} + |-\alpha\rangle^2_{A_0}|-\alpha\rangle^2_{B_0}) \otimes ...\}. \end{aligned} \tag{7.18}$$

Here i represents a time interval of size Δt, $|\alpha|^2$ the average photon number in the coherent state $|\alpha\rangle$, A Alice's subsystem, B Bob's, and the subscript 0 the initial path zero as labelled in Fig. 7.2.

The action of Alice's interferometer with a delay in the long arm of Δt is given by

$$\hat{a}_0^{\dagger i} \overset{I_A}{\rightarrow} \frac{1}{2}(\hat{a}_4^{\dagger i} + \mathrm{e}^{-i\phi_2}\hat{a}_5^{\dagger i} + \hat{a}_4^{\dagger(i+1)} - \mathrm{e}^{-i\phi_2}\hat{a}_5^{\dagger(i+1)}). \tag{7.19}$$

The action of Bob's interferometer with a delay in the long arm of Δt is given by

$$\hat{a}_0^{\dagger i} \overset{I_A}{\rightarrow} \frac{1}{2}(\hat{a}_4^{\dagger i} - \mathrm{e}^{i\phi_2}\hat{a}_5^{\dagger i} + \hat{a}_4^{\dagger(i+1)} + \mathrm{e}^{i\phi_2}\hat{a}_5^{\dagger(i+1)}). \tag{7.20}$$

Let the states $|\psi\rangle$ and $|\gamma\rangle$ be defined as

$$\begin{aligned} |\psi\rangle &\equiv |0\rangle_{A4}|\alpha\mathrm{e}^{-i\phi_2}\rangle_{A5}|0\rangle_{B4}|\alpha\mathrm{e}^{-i\phi_2}\rangle_{B5} \\ |\gamma\rangle &\equiv |\alpha\rangle_{A4}|0\rangle_{A5}|\alpha\rangle_{B4}|0\rangle_{B5}. \end{aligned} \tag{7.21}$$

Discarding the part of the zeroth pulse that travelled on the short path in the interferometer in each subsystem, the entangled state shared by Alice and

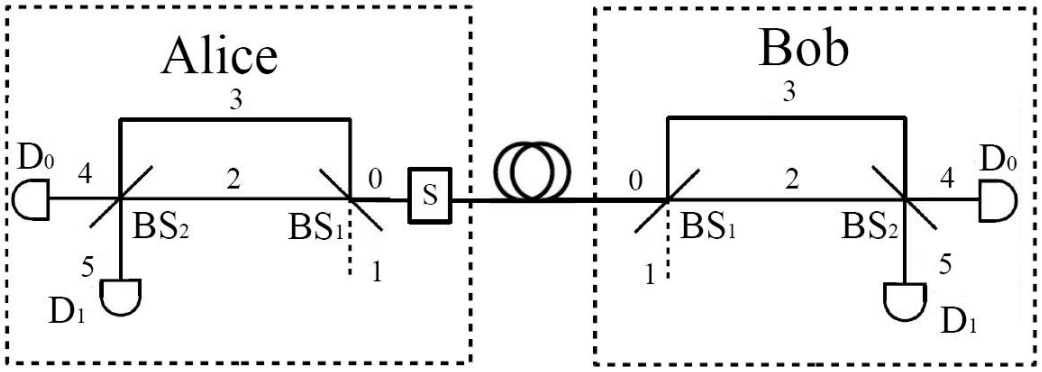

Figure 7.2: Quantum key distribution system for an entanglement-based protocol. BS: symmetric beamsplitter, D: non-number-resolving photon detector, S: source of entangled pairs.

Bob after the action of both interferometers and before detection is calculated to be

$$
\begin{aligned}
|\Phi\rangle_{AB} \xrightarrow{I} \frac{1}{2^N}\{ \quad & |\gamma\rangle^1|\gamma\rangle^2 \ldots + \\
& |\gamma\rangle^1|\gamma\rangle^2 \ldots + \\
& |\gamma\rangle^1|\psi\rangle^2 \ldots + \\
& |\gamma\rangle^1|\psi\rangle^2 \ldots + \\
& |\psi\rangle^1|\gamma\rangle^2 \ldots + \\
& |\psi\rangle^1|\gamma\rangle^2 \ldots + \\
& |\psi\rangle^1|\psi\rangle^2 \ldots + \\
& |\psi\rangle^1|\psi\rangle^2 \ldots + \\
& \vdots \qquad\qquad \}.
\end{aligned} \tag{7.22}
$$

7.7 Comments

Although the above state was only calculated explicitly for the first three pulses, it seems that the terms in the sum represent all possible permutations of states in all time intervals arising after the transformation of $|\Phi\rangle_{AB}$ in both interfermometers. Note, in each time interval Alice and Bob's states are perfectly correlated, and also that the state factorises i.e., the states in

different time intervals are independent. The states $|\psi\rangle$ and $|\gamma\rangle$ are non-orthogonal owing to the contribution of the vacuum state in the coherent state, and are therefore not perfectly distinguishable.

Two QKD protocols are equivalent if from any perspective outside Alice's laboratory, the two cannot be told apart. Phase 1 of the P&M DPSQKD protocol involves Alice preparing $N + 1$ coherent pulses, randomly modulating the phase of each by either 0 or π, and then sending these to Bob. Phase 1 of the EB protocol outlined above is similar to the P&M DPSQKD protocol, if Alice first performs a non-photon-number-resolving measurement on her subsystem in each time interval, since this results in Bob receiving a chain of $N + 1$ coherent pulses with random relative phases of 0 or π.

The difference between the schemes appears to be that in this EB scheme Alice measures in a non-orthogonal basis, and her knowledge of the key to be shared with Bob is therefore only partial, in the sense that she only knows what Bob has been sent in the time intervals in which she gets a detection event, while in P&M DPSQKD she has full knowledge of the bit string S' according to which she modulates the phases of the pulses sent to Bob.

As a result, in this EB protocol, Alice and Bob will record a key of shorter length if $N + 1$ entangled pairs of pulses are prepared. Considering an error-free channel, in the P&M DPS QKD protocol Alice and Bob can record a secret key bit in all the time intervals in which Bob records a detection event, and this happens with a probability of $1 - \mathrm{e}^{-|\alpha|^2}$. On the other hand, in the new EB protocol, to add a secret bit to their key, both Alice and Bob must observe a detection event, and the joint probability of this happening is given by $(1 - \mathrm{e}^{-|\alpha|^2})^2$.

The unconditional security proof [27] for B92 [95], a protocol using two non-orthogonal states, is based on ED and may possibly be applicable to this EB protocol, where the effectively distributed state factorises in terms of time intervals. The next step would be either to show that it is equivalent to the P&M DPS QKD protocol, or to propose a P&M protocol equivalent to this EB scheme that is feasible to implement.

7.8 Conclusion

DPSQKD, an example of a DPR protocol, has here been described firstly as a P&M scheme, and secondly translated into an EB scheme, thus fitting into the framework of description for generic QKD protocols. DPSQKD has been shown to satisfy a necessary condition for security, i.e., that Bob's measurements are non-commuting in the EB translation of the protocol. An EB translation of a DPR protocol is a necessary first step towards an unconditional security proof based on ED. Finally, thoughts on a potential unconditional security proof based on ED for a DPSQKD-like protocol are given.

Chapter 8

Conclusion and outlook

"The very word 'secrecy' is repugnant in a free and open society."

- John F. Kennedy

8.1 Background

Quantum key distribution (QKD) aims at the creation of a secret key in the two locations of partners, traditionally Alice and Bob, wishing to communicate in private. Phase 1 of a general QKD protocol can be described as a prepare-and-measure (P&M) or equivalently as an entanglement-based (EB) phase. The aim of Phase 2 is to distill a secret key from the measurement outcomes resulting from Phase 1. One method of proving the unconditional security of a QKD protocol consists of showing the equivalence of the total protocol including Phases 1 and 2 to an unconditionally secure entanglement distillation (ED) protocol, which will then imply the unconditional security of the original scheme.

The classical data produced in a secure QKD protocol must imply non-classical correlations between the systems held by Alice and Bob in the EB translation. Therefore, a necessary condition for the security of a QKD protocol is that the measurements performed by Alice and Bob in the EB translation must detect entanglement in the effectively distributed state, which in turn implies that Bob's measurement must consist of non-commuting POVM elements. Given a general P&M QKD protocol, a necessary first step to

proving the protocol unconditionally secure through such an equivalence, is to describe an equivalent EB translation of Phase 1 where this condition on Bob's measurement is met.

8.2 DPSQKD

There are a number of practical advantages to the differential-phase-shift (DPS) QKD protocol, however, it is a member of the class of QKD protocols for which bounds for unconditional security have not yet been found. In the DPSQKD protocol, consecutive potential key bits are not independent and there is no one-to-one correspondence between potential key bits and prepared states, as in general QKD protocols. This is the reason existing methods of proving unconditional security cannot be applied to the DPSQKD protocol, since they rely on the mutual independence of all potential key bits.

However, the formulation of P&M DPSQKD given here facilitates the translation of the protocol into an equivalent EB scheme. The EB translation of DPSQKD given here was previously missing from the literature.

With respect to Bob's measurements, which are the same in both the EB and P&M descriptions: On the large Hilbert space consisting of all input and output modes in Bob's interferometer and all time intervals, Bob's measurement, which consists of the combined action of his interferometer and his detectors, is mathematically described as a degenerate projection measurement, consisting only of orthogonal projectors. At this point, the protocol appears to be insecure, since the condition on Bob's measurements is not met!

However, a POVM with non-commuting effects can be represented by a projective measurement on a higher dimensional Hilbert space. And indeed, when Bob's measurement in DPSQKD acts on the reduced Hilbert space of populated modes only, it is shown that his measurement is described by a POVM with non-commuting elements. This discussion was also absent from the literature.

The EB translation of DPSQKD formalised here, where the necessary condition on Bob's measurement is shown to be met, is a necessary first step towards a potential unconditional security proof for the protocol based on

ED.

8.3 Outlook

Whether Phase 2 of DPSQKD can be related to a process that distills entanglement from the bipartite states shared by Alice and Bob after the EB description of Phase 1 given here remains to be shown. The difficulty is that there is not a one-to-one correspondence between potential key bits and prepared states. To this end, a new DPSQKD-like protocol is proposed finally, where there is such a correspondence. The next step would either be to show that this new protocol is equivalent to the original P&M DPSQKD protocol, or to propose a new P&M protocol equivalent to this EB scheme that is feasible to implement. It is possible that given this correspondence in the DPSQKD-like protocol, existing methods of proving the unconditional security of protocols using two non-orthogonal states can be applied.

In conclusion, although the security status of the DPSQKD protocol remains to be determined, some useful contributions to and discussions of the endeavour have been made here.

Appendix

List of acronyms and abbreviations

BB84	the protocol of Bennett and Brassard published in 1984 [10]
QKD	quantum key distribution
SKD	secret-key distillation
EPR	Einstein-Podolsky-Rosen
E91	the protocol of Ekert published in 1991 [19]
BBM92	the protocol of Bennett, Brassard and Mermin published in 1992 [20]
EB	entanglement-based
P&M	prepare-and-measure
ED	entanglement distillation
CSS	Calderbank-Shor-Steane
DPS	Differential-Phase-Shift
RSA	the public-key cipher of Rivest, Shamir and Adleman published in 1978 [34]
NP	non-deterministic polynomial
MAC	message authentication code
i.i.d.	independent and identically distributed
POVM	positive operator-valued measure
LOCC	local operations and classical communication
DV	discrete-variable
CV	continuous-variable
DPR	distributed-phase-reference
COW	Coherent-one-way
$BS_{1(2)}$	beamsplitter 1(2)
$D_{0(1)}$	bucket detector 0(1)

Bibliography

[1] C. Shannon, "Communication Theory of Secrecy Systems", Bell Syst. Tech. J. **28**, 656 (1949).

[2] G. Vernam, "Cypher printing telegraph systems for secret wire and radio telegraphic communications", J. of IEEE **55**, 109 (1926).

[3] R. Landauer, "Information is Physical", Physics Today, 23 (1991).

[4] M. Planck, "Ueber eine Verbesserung der Wien'schen Spectralgleichung", "Zur Theorie des Gesetzes der Energieverteilung im Normalspectrum", Verhandl. Deutsch. Phys. Ges. **2**, 202, 237 (1900).

[5] G. N. Lewis, "The Conservation of Photons", Nature **118**, 874 (1926).

[6] A. Einstein, "Über einen die Erzeugung und Verwandlung des Lichtes betreffenden heuristischen Gesichtspunkt", Ann. Phys. (Leipzig) **17**, 132 (1905).

[7] E. Fermi, "Quantum Theory of Radiation", Rev. Mod. Phys. **4**, 87 (1932).

[8] P. Dirac, "The quantum theory of the emission and absorption of radiation", *Proc. R. Soc. Lond A* (Royal Society, London) **114**, 243 (1927).

[9] P. A. M. Dirac, *The principles of quantum mechanics* (4th ed.) (Oxford University Press, Oxford) (1982).

[10] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing", *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York), 175 (1984).

[11] W. K. Wootters and W.H. Zurek, "A Single Quantum Cannot be Cloned", Nature **299**, 802 (1982).

[12] D. Mayers, "Unconditional Security in Quantum Cryptography", *Advances in Cryptology- Proceedings of Crypto '96* (Springer Verlag, Berlin), 343 (1996).

[13] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, "Quantum cryptography", Rev. Mod. Phys. **74**, 145 (2002).

[14] E. Biham, M. Boyer, P. O. Boykin, T. Mor and V. Roychowdhury, "A Proof of the Security of Quantum Key Distribution", *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing* (ACM Press, New York), 715 (2000).

[15] P. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol", Phys. Rev. Lett. **85**, 441 (2000).

[16] G. Van Assche, *Quantum Cryptography and Secret-Key Distillation* (Cambridge University Press, Cambridge), 210 (2006).

[17] E. Schrödinger, "Die gegenwärtige Situation in der Quantenmechanik", Die Naturwissenschaften **23**, 807, 823, 844 (1935).

[18] A. Einstein, B. Podolsky and N. Rosen, "Can a Quantum-Mechanical Description of Physical Reality be Considered Complete?", Phys. Rev. **47**, 777 (1935).

[19] A. K. Ekert, "Quantum Cryptography Based on Bells Theorem", Phys. Rev. Lett. **67**, 661 (1991).

[20] C. H. Bennett, G. Brassard and N. D. Mermin, "Quantum Cryptography without Bell's Theorem", Phys. Rev. Lett. **68**, 557 (1992).

[21] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, W. K. Wootters, "Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels", Phys. Rev. Lett. **76**, 722 (1996).

[22] A. R. Calderbank and P. W. Shor, "Good quantum error correcting codes exist," Phys. Rev. A **54**, 10981105 (1996).

[23] A. M. Steane, "Multiple particle interference and quantum error correction," Proc. Roy. Soc. Lond. A **452**, 2551 (1996).

[24] H. -K. Lo and H.F. Chau, "Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances", Science **283**, 2050 (1999).

[25] A. Acín and N. Gisin, "From Bells Theorem to Secure Quantum Key Distribution", Phys. Rev. Lett. **97**, 120405 (2006).

[26] B. Kraus, N. Gisin and R. Renner, "Lower and Upper Bounds on the Secret-Key Rate for Quantum Key Distribution Protocols Using One-Way Classical Communication", Phys. Rev. Lett. **95**, 080501 (2005).

[27] K. Tamaki, M Koashi and N. Imoto, "Unconditionally Secure Key Distribution Based on Two Nonorthogonal States", Phys. Rev. Lett. **90**, 167904 (2003).

[28] M. Curty, M. Lewenstein and N. Lütkenhaus, "Entanglement as a Precondition for Secure Quantum Key Distribution", Phys. Rev. Lett. **92**, 21 (2004).

[29] K. Inoue, E. Waks and Y. Yamamoto, "Differential Phase Shift Quantum Key Distribution", Phys. Rev. Lett **89**, 037902 (2002).

[30] K. Inoue, E. Waks and Y. Yamamoto, "Differential-phase-shift quantum key distribution using coherent light", Phys. Rev. A **68**, 022317 (2003).

[31] H. G. Liddell, R. Scott and H. Drisler, *A Greek-English lexicon: based on the German work of Francis Passow'* (Harper and Brothers Publishers, New York) (1846).

[32] S. Vaudenay, *A Classical Introduction to Cryptography: Applications for Communications Security* (Springer, US) (2006).

[33] L. A. Levin, "The Tale of One-Way Functions", Probl. Inform. Transm. **39**, 92 (2003).

[34] R. L. Rivest, A. Shamir and L. M. Adleman, "A method of obtaining digital signitures and public-key cryptosystems", Commun. ACM **21**, 120 (1978).

[35] L. Fortnow, "The status of the P versus NP problem", Commun. ACM **52** No. 9, 78 (2009).

[36] A. Shamir, "Factoring Large Numbers with the TWINKLE Device", C .K. Koc and C. Paar (Eds.): *CHES'99, LNCS* (Springer-Verlag Berlin, Heidelberg) **1717**, 2 (1999).

[37] S. Sarkar and S. Maitra, "Further Results on Implicit Factoring in Polynomial Time", AMC **3**, 205 (2009).

[38] C. E. Shannon, "A Mathematical Theory of Communication", Bell Syst. Tech. J. **27**, 623 (1948).

[39] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (John Wiley, New York) (1991).

[40] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge), (2000).

[41] M. Le Ballac, *A Short Introduction to Quantum Information and Quantum Computation* (Cambridge University Press, Cambridge) (2006).

[42] R. Ash, *Information Theory* (Interscience Publishers, New York), (1965).

[43] U. M. Maurer and S. Wolf, "Unconditionally secure key agreement and the intrinsic conditional information", IEEE Trans. Inf. Theory, **45**, 499 (1999).

[44] U. M. Maurer, "On the Secret-Key Rate of Binary Random Variables", *Proceedings of IEEE International Symposium on Information Theory*, 351 (1994).

[45] V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušek, N. Lutkenhaus and M. Peev, "A Framework for Practical Quantum Cryptography", arXiv:0802.4155v1 [quant-ph] (2008).

[46] U.M. Maurer, "Secret key agreement by public discussion from common information", IEEE Trans. Inf. Theory, **39** No. 3, 733 (1993).

[47] I. Csiszár and J. Körner, "Broadcast channels with confidential messages", IEEE Trans. Inf. Theory **24**, 339 (1978).

[48] M. Dušek, N. Lütkenhaus and M. Hendrych, "Quantum Cryptography", *Progress in Optics Vol. 42*, edited by E. Wolf, (Elsevier, Amsterdam), 219 (2006).

[49] R. Renner and S. Wolf, "New bounds in secret-key agreement: the gap between formation and secrecy extraction", *Advances in Cryptology- Proceedings of Eurorypt '03*, LNCS **2656**, 563 (2003).

[50] B. Kraus, C. Branciard and R. Renner, "Security of quantum key distribution protocols using two-way classical communication or weak coherent pulses", Phys. Rev. A **75**, 012316 (2007).

[51] H.-K. Lo, "Method for decoupling error correction from privacy amplification", New J. Phys. **5**, 36 (2003).

[52] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion", *Advances in Cryptology - Eurocrypt 93*, LNCS **765** (Springer Verlag, Berlin), 410 (1993).

[53] D. Elkouss, A. Leverrier, R. Alléaume and J. Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution", *Proceedings of IEEE International Symposium on Information Theory*, 1879 (2009).

[54] M. Naor, M. Yung, "Universal one-way hash functions and their cryptographic applications", *Proceedings of the 21st Annual Symposium on Theory of Computing* (ACM, New York), 33 (1989).

[55] J. von Neumann, *Mathematical Foundations of Quantum Mechanics*, translated by R. T. Beyer, (Princeton University Press, Princeton) (1955).

[56] B. Schumacher, "Quantum Coding", Phys. Rev. A **51**, 2738 (1995).

[57] http://www.random.org (14 November 2009).

[58] T. Ritter, "Random Electrical Noise: A Literature Survey" in *Research Comments from Ciphers By Ritter* (2004) http://www.ciphersbyritter.com/RES/NOISE.HTM (14 November 2009).

[59] J. G. Rarity, and P. R. Tapster, *Photons and Quantum Fluctuations*, edited by E. R. Pike and H. Walther, (Hilger, Bristol), 122 (1988).

[60] http://www.idquantique.com/products/quantis.htm (14 November 2009).

[61] P. Busch, M. Grabowski and P. J. Lahti, *Operational Quantum Physics* (New York: Springer-Verlag) 7 (1995).

[62] A. Peres, *Fundamental Theories of Physics* (Kluwer Academic Publishers, Netherlands) (1995).

[63] J. M. Renes, R. Blume-Kohout, A. J. Scott and C. M. Caves, "Symmetric informationally complete quantum measurements", J. Math. Phys. **45**, 2171 (2004).

[64] J. Audretsch, *Entangled Systems* (Wiley VCH, Darmstadt) (2007).

[65] D.E. Evans and J.T. Lewis, "Dilations of Irreversible Evolutions in Algebraic Quantum Theory", Comm. Dublin Inst. Adv. Studies A (Theoretical Physics), No. 24 (DIAS, Dublin) (1977).

[66] M. Ziman and V. Bužek, "Realization of POVMs using measurement-assisted programmable quantum processors", arXiv:quant-ph/0411135 (2004).

[67] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam) (1982).

[68] G. Beneti, G. Casati and G. Strini, *Principles of Quantum Computation and Information Volume 1: Basic Concepts* (World Scientific Publishing, Singapore) (2004).

[69] D. Bohm, *Quantum Theory* (Prentice Hall, New York) (1951).

[70] J. P. Paz and W. H. Zurek, "Environment-Induced Decoherence and the Transition from Quantum to Classical", *Fundamentals of Quantum Information*, edited by D. Heiss, (Springer-Verlag, Berlin), 77 (2002).

[71] L. D. Landau and E. M. Lifshitz, *Quantum Mechanics Non-Relativistic Theory: Volume 3* (Butterworth-Heinemann) (1960).

[72] A. S. Holevo, "Statistical Problems in Quantum Physics", *Proceedings of the Second Japan-USSR Symposium on Probability Theory* edited by G. Maruyama and J. V. Prokhorov (Springer-Verlag, Berlin), 104 (1973).

[73] M. Ban, M. Osaki, and O. Hirota, "Upper bound of the accessible information and lower bound of the Bayes cost in quantum signal-detection processes", Phys. Rev. A **54**, No.4 (1996).

[74] I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states", Proc. R. Soc. Lond. A **461**, 207 (2005).

[75] R. Loudon, *The Quantum Theory of Light* (Clarendon Press, Oxford) (1973).

[76] N. Taylor, *LASER: The inventor, the Nobel laureate, and the thirty-year patent war* (Simon and Schuster, New York) (2000).

[77] T. H. Maiman, "Stimulated optical radiation in ruby", Nature **187**, 493 (1960).

[78] R. J. Glauber, "The Quantum Theory of Optical Coherence", Phys. Rev. **130**, 2529 (1963).

[79] D.F. Walls and G.J. Milburn, *Quantum optics*, 2nd edition (Springer Verlag, Berlin) (2008).

[80] C. C. Gerry and P. L. Knight, *Introductory Quantum Optics* (Cambridge University Press, Cambridge) (2005).

[81] L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics* (Cambridge University Press, Cambridge), 525 (1996).

[82] W. Heisenberg, "Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik", Z. Phys. **43**, 172 (1927).

[83] B. Sanders, J. Vučković and P. Grangier, "Single photons on demand", Europhys. News **36**, 56 (2005).

[84] S. Cova, M. Ghioni, A. Lacaita, C. Samori, and F. Zappa, "Avalanche photodiodes and quenching circuits for single-photon detection", Applied Optics **35**, Issue 12, 1956 (1996).

[85] P. P. Rohde, J. G. Webb, E. H. Huntington and T. C. Ralph, "Photon number projection using non-number-resolving detectors", New J. Phys. **9**, 233 (2007).

[86] M. Navascués and A. Acín, "Security Bounds for Continuous Variables Quantum Key Distribution", Phys. Rev. Lett. **94**, 020505 (2005).

[87] N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner and V. Scarani, eprint quant-ph/0411022 (2004)

[88] D. Stucki, M. Brunner, N. Gisin, V. Scarani and H. Zbinden, Appl. Phys. Lett. **87**, 194108 (2005)

[89] E. Waks, H. Takasue and Y. Yamamoto, "Security of differential-phase-shift quantum key distribution against individual attacks", Phys. Rev. A **73**, 012344 (2006)

[90] E. Diamanti, H. Takasue, C. Langlock, M. M. Fejer and Y. Yamamoto, "100 km differential phase shift quantum key distribution experiment with low jitter up-conversion detectors", Opt. Express **14**, 13073 (2006)

[91] T. Tsurumaru, "Sequential attack with intensity modulation on the differential-phase-shift quantum-key-distribution protocol", Phys. Rev. A **75**, 062319 (2006).

[92] Y.-B. Zhao, C.-H. F. Fung, Z.-F. Han and G.-C. Guo, "Security proof of differential phase shift quantum key distribution in the noiseless case", Phys. Rev. A **78**, 042330 (2008).

[93] L. Ma, S. Nam, H. Xu, B. Baek, T. Chang, O. Slattery, A. Mink and X. Tang, New J. Phys. **11**, 045020 (2009).

[94] K. Wen, K. Tamaki and Y. Yamamoto, "Unconditional Security of Single-Photon Differential Phase Shift Quantum Key Distribution" Phys. Rev. Lett. **103**, 170503 (2009).

[95] C. H. Bennett, "Quantum Cryptography Using Any Two Nonorthogonal States", Phys. Rev. Lett **68**, 3121 (1992).