Public Keys and Private Keys

in

Quantum Cryptography

Thesis submitted for the degree of
Doctor of Philosophy

by

Ido Bregman

Submitted to the Senate of the Hebrew University

May 2008

This work was carried out under the supervision of

Prof. Dorit Aharonov and Prof. Michael Ben-Or

Abstract

This work is about developing tools for secure communications using quantum protocols. The work focuses on ways to transfer classical information using quantum communication channels, and exploiting the properties of quantum information theory to achieve secrecy.

Quantum cryptography and classical cryptography essentially deal with the same tasks, such as, just to mention a few, private communication, message authentication, zero knowledge proofs etc. The big difference is that the communication is done using qubits instead of classical bits. Due to the basic fundamentals of quantum mechanics it is not possible in general to passively eavesdrop to quantum messages, unlike when classical bits are used. This is because quantum states that are used to encode information need not be orthogonal, and as a consequence measuring them usually cause disturbance which might be detected.

Quantum information theory allows us to encode classical data on quantum states, in a way that any attempt of an unauthorized entity to extract the secret data leads to one of the two possibilities - either the attempt fails, and the amount of information revealed is negligible, or the measurement performed by that entity damages the coherence of the quantum signals, and by that reveals its presence.

In classical cryptography it is traditional to distinguish between two types of secure communications, which are essentially different. In one type the legitimate parties use a private key to encode their messages, and in the other type they use public-key encoding. An encryption key is commonly termed private if it is only known to the sender and receiver of a message, and not to anybody else. This requirement is a critical demand for such a scheme to work. When a number, n, of participants need to securely communicate pairwise then each pair must have their own independent private key, so the total number of keys in the system is of order n^2. In contrast, a classical public key system usually consists of a list of keys which is accessible to everybody. When one participant wishes to send a secret message to another participant, he just has to look at the latter's public key as appears in the list, and use it for encryption. Thus there are n keys in the system. Both types of encryption schemes have advantages and disadvantages. As I mentioned, with public keys there are less keys. In addition, with public keys you don't need to worry about secure distribution of keys, since they are public data. On the other hand, classical private key cryptography is unconditionally secure, while classical public key cryptography is only secure under

restrictive assumptions on the computational power of the adversary.

Distribution of private keys is not possible in the framework of classical information theory while, on the other hand, it is possible to distribute private keys, and even in nowaday's technology, using quantum communication. Therefore, naturally, the research in quantum cryptography has so far focused mainly on the issue of private key distribution, and much less on cryptography with public keys. To the best of our knowledge, quantum public keys were explicitly used in the literature only in the work of [36], which does not relate to the direct use of private communication, but rather relate to another use - quantum digital signatures. The major advantage of quantum public key encryption with respect to the classical counterpart is that, like classical private key encryption, it is unconditionally secure, regardless of the adversary's computational capabilities. The advantage of quantum public keys over quantum private keys is mainly the symmetry - the fact that all users get the same key allow applications such as digital signatures [36], anonymity (which is discussed in depth in this thesis), and maybe many others yet to be explored.

This work contributes to both types of quantum cryptography. According to this, it is divided into two parts: **quantum public keys** and **quantum private keys**.

Quantum public keys. A quantum public key is a quantum state drawn from a set of non-orthogonal states. Multiple copies of the same key can be issued and distributed to different participants in a system. To my best knowledge this concept was first defined in [36]. Such states can be used to encode classical information privately, because by the principles of quantum theory the states cannot be fully distinguished. The natural way to encode classical information on quantum states is to apply some quantum operation which represents the information on the quantum state.

This part's contribution is in that here, in the first time, it is considered to use quantum public key encryption for its direct and natural purpose - secure communication. In this part the emphasis is on the advantages of this method with respect to private key cryptography. Other uses of public keys in quantum cryptography include quantum fingerprinting, quantum digital signatures and quantum string commitment. In each of these cases a choice of the set of non orthogonal states is made suitable for the particular application. In the case of secure communication, discussed in this thesis, the quantum states must have the property that they can easily be used for encoding of classical information by a person without knowing which of the states from the set was chosen.

In Chapter 1 of the thesis we give a definition of a quantum public key, and discuss the properties

of this method of encryption. The contribution of this definition is a rigorous description of the parameters of a quantum public key. We give simple and efficient protocols for distribution of public keys, and of encoding and decoding of classical information using these keys. The protocols are divided into two types - those where the key distribution phase is quantum, but the encodings and decodings of messages are classical, and those where also the encoding and decoding procedures involve quantum communication. Each protocol comes with a thorough analysis of its security.

In Chapter 2 we describe a natural use of quantum public key encryption, and in particular the protocols described in Chapter 1, in a construction of an anonymous communication network. The good properties of this method of encryption allow us to have a network where the content of the exchanged messages, as well as the identities of senders and receivers of messages, are kept secret from any unauthorized entity. This unauthorized entity (the *adversary*) is assumed to control an arbitrary fraction (smaller than 1) of the users/players in the network. The network provides unconditional security in both these two aspects. In terms of communication complexity the main parameter is the number of users of the network. With respect to this parameter we have protocols that require for a delivery of a single message a polylogarithmic number of communication rounds. The total amount of communication per message delivery is also polylogarithmic in this parameter.

Classically, according to what is currently known, tolerating an arbitrary fraction of adversary-controlled users can be achieved efficiently only with computational security (to be considered efficient a protocol has to operate with both polylogarithmic number of rounds and polylogarithmic total communication per message). Proving this fact is an open problem; however if unconditional security is required then the only known classical solutions either limit the power of the adversary to controll at most half of the players in the network, or are highly inefficient in terms of communication cost in the network. To be more specific, these solutions require at least a linear number of communication rounds per single message delivery (which is far from being acceptable), and the total amount of communication per message is polynomial. We discuss these issued in detail in Chapter 2.

In addition, an important contribution of Chapter 2 is a proof that it is impossible to reconstruct the special properties of quantum public key encryption classically, and even when the classical protocol is allowed to use quantum key distribution as a black box. This result adds yet another natural example to the list of cryptographic and computational tasks which are achievable in the framework of quantum information, but intractable using classical tools.

The results in Chapters 1 and 2 are joint work with Amnon Ta-Shma.

Quantum private keys. In this part we examine the possibility to design quantum key distribution protocols with the same simplicity, but with improved level of security, with respect to today's common single photon protocols, such as BB84 and the six-state protocol [16, 22, 7]. In particular, we seek for protocols that can be implemented with todays simplest and cheapest technology, but with better parameters. For this purpose, we examine the use of biphotons as the physical realization of ternary logic, and the possibility to perform QKD with only single-photon operations. This way we achieve quantum key distribution based on trits instead of bits, with the idea to have an improved communication rate and improved security. The central question we ask is whether it is possible to improve security despite the limitation that comes from the use of single photon operations.

In Chapter 3 we review some known general schemes for QKD. We discuss the general structure of these schemes, the security requirements, and the known level of security which they provide.

In Chapter 4 we give a convenient geometric interpretation of the single photon operations constraint applied to biphotons (qutrits). From the geometric picture it is easy to get descriptions of QKD protocols which fulfill the constraint. Among these protocols, some have simple and symmetric structure. In this chapter there is a detailed analysis of the security of one such protocol against coherent attacks, which are the most severe attacks allowed by the quantum laws. The analysis comes with a comparison to common single photon QKD protocols, and with a comparison to a biphoton protocol that uses four mutually unbiased bases (the bases that are described in [8]), which cannot be implemented with single photon operations only. It is known that four is the maximal number of mutually unbiased bases in three dimensional Hilbert space, and furthermore, in any dimension, the QKD protocol with best known key rate is the one that employs the maximal number of mutually unbiased bases in this dimension. However I am not sure if there is a proof of this claim. The comparison shows that, despite the single photon operation limitation, the key rate of our protocol is much higher than that of single photon protocols, and also, on the other hand, that it is not significantly less than the key rate of the protocol that uses four mutually unbiased bases (whose implementation is much more expensive and complicated). To the best of my knowledge, here is the first place to give a complete analysis of the security of qutrits protocols against coherent attacks. In particular, we show that with an error rate of 17.7% the protocol is still able to produce secure trits in non-negative rate. This should be compared with a known [63] upper bound of 16.3% for the single photon protocol known as the six state protocol. This comparison is important since the six state protocol is composed of three mutually unbiased bases,

which is the maximal number of mutually unbiased bases in two dimensional Hilbert space, and thus the single photon protocol with the highest known key rate. In addition, we also analyze the four mutually unbiased bases protocol, and show a lower bound of 20.7% on the error rate that it can stand.

Because simplicity is an important factor in our analysis, we focus in this thesis only on protocols with one way communications. We note that two way protocols usually achieve better key rates (see [37], for example).

An important remark is that the error rate, which is the fraction of damaged signals, behaves differently when the signals are qutrits instead of qubits. In particular, it is clear that in principle the same quantum channel might induce different error rate when it is used for transmission of biphotons than with single photons. However the exact correspondence is not known. In general it is reasonable to assume that the same channel will induce higher error rate with biphotons than with single photons, because biphotons are more sensitive to interaction with the environment. But on the other hand, currently used quantum channels involve only single photon operations when describing the interaction with the transmitted quantum systems. Consequently, the error rate can be much less than with the most general possible type of interaction. This interesting question, of the different effect of the same quantum channel on qutrits compared to qubits, is subject to further research which is not discussed in this thesis.

The results in Chapter 4 are joint work with Hagai Eisenberg.

Contents

Part I

Introduction

Ever since the discovery of quantum key distribution [16], and even more after the discovery of a general and elegant proof of its security [62], many attempts have been made to exploit the unique properties of quantum mechanics to provide new cryptographic primitives. One attempt which failed was that of quantum bit commitment; subsequently, less powerful but still interesting primitives such as quantum bit escrow [3] and quantum string commitment [42] were introduced. Many other examples, which lay beyond cryptography, such as, e.g., quantum fingerprinting [24] and quantum random access codes [4, 51], were discovered.

People are enthusiastic about quantum cryptography because it has two major promises. One is the possibility to take existing classical cryptographic primitives which can be realized only under certain computational assumptions and relax these assumptions to get information theoretic security. One such example is the quantum digital signature [36]. Another potential major benefit is to achieve cryptographic primitives which are not achievable in the framework of classical information theory, the most famous example being quantum key distribution.

In classical cryptography we traditionally distinguish between two essentially different types of protocols: *private key* and *public key* protocols.

A classical private key is a string of bits known only to the sender and receiver of a message, and not to anybody else. This requirement is a critical demand for such a scheme to work. When a few of the participants need to securely communicate pairwise then each pair must have their own independent private key. In contrast, a classical public key system usually consists of a list of keys which is accessible to everybody. When one participant wishes to send a secret message to another participant, he just has to look at the latter's public key as appears in the list, and use it for encryption

Each of these two types has its advantages and disadvantages. The common classical public key schemes are only secure against a computationally bounded adversary, as opposed to private key schemes, which are unconditionally secure. On the other hand, In the classical world, public key schemes have some appealing features which private keys do not have. Two such advantages over private keys are:

- Public key schemes are *symmetric* - every recipient has the same public key, and also every recipient applies the same encryption strategy to produce encrypted messages. The symmetry property contributes to simplicity, and also reduces the security requirements involved in key distribution - a public key can be safely given to an opponent without endangering the security of the protocol. Key distribution is a problematic issue in private key schemes, because it is

well known that distribution of secret bits over an unsecure classical channel is impossible by virtue of information theory. The symmetry becomes a key feature in certain applications, such as network anonymity discussed in Chapter 2, and such as digital signatures (see, e.g., [36]).

- Unlike public keys an information theoretic secure private key is a one time pad - it cannot be secure unless it is used once only, and unless the key is at least as long as the cleartext. The exact amount of information that leaks when we attempt to use the same key more than once depends on the specific method of public keys in use.

  It is worth mentioning that a private key is not necessarily a one time pad. For example, a private key may be generated using an underlying Diffie-Hellman protocol, (which is only computationally secure), and then be used in a symmetric ancryption scheme.

The first part of this thesis focuses on importing the ideas of classical public key cryptography into the quantum world. The goal is to replace the computational security of classical public key schemes with information theoretic security, while preserving the primary advantages of classical public key cryptography in a quantum setting. This can allow us to maintain the same applications but with a substantially higher level of security. This process was first initiated in the work of [36], who considered using quantum public keys to achieve information theoretic secure digital signatures. We extend the work of [36] in the following ways: first we give formal definitions of what is a quantum public key and what are the main properties of such keys, and second we describe how to use this notion for an application other than digital signatures - the application of an anonymous network.

Some mathematical problems are easy to compute, but hard to invert. Problems of this type are called one way functions. The security of all classical public key schemes depends on the inability of a computationally bounded eavesdropper to invert a one way function. One famous example is RSA [59], which corresponds to the problem of multiplying together two numbers, the inverse being factoring the product.

To design quantum public key cryptography, we borrow some ideas from the classical public key cryptography. In classical public key cryptography the main concept is the one way function (OWF). The quantum analog to this notion is the quantum one way function (QOWF), which is an information theoretic secure counterpart to the classical OWF.

The advantages of quantum cryptography over classical in this context comes from the promise

of quantum cryptography to replace computational security with information theoretic security. This is especially important in presence of an efficient quantum factoring algorithm [61], which makes widely used classical computational encryption methods insecure.

As mentioned, classical public key schemes are created out of one way functions. $f(x)$ is a one way function if it is easy to compute $f(x)$ given x, but computing x given $f(x)$ is very difficult. While there are many candidate OWFs, none has been proved to be secure, and some, such as multiplying together two primes (the inverse being factoring the product), become insecure in the presence of quantum computers. This motivates studying the properties of QOWFs which, unlike any classical one way function, are provably secure from an information theoretic standpoint, no matter how powerful the adversary's computers are.

The concept of a quantum one way function was first introduced in [36], and was used there to build an information theoretically secure quantum digital signature scheme. Quantum one way functions were also used for quantum string commitment [23]. A quantum one way function f is a one to one mapping of classical strings x to quantum states $\rho_f(x)$, such that the quantum state can be produced from the classical string, but given the quantum state it is impossible to restore the string associated with it. Such a function can be used to produce a quantum public key by choosing a random classical string x and distributing many identical copies of the state $\rho_f(x)$ (while keeping x private). There are additional requirements from the set of states $\{\rho_f(x)\}_x$, depending on the particular cryptographic application it is used for. In the case of a digital signature, for instance, it should be possible to determine whether $x = y$ using the states $\rho_f(x)$ and $\rho_f(y)$. When the required application is private communication, which is the one being discussed in this thesis, f should come with an appropriate encoding function E, such that for two different messages m and m', $E(m, \rho_f(x))$ is indistinguishable from $E(m', \rho_f(x))$, unless you know x, which naturally is only known to the legitimate recipient of the message.

A cryptographic scheme based on the notion of a quantum one way function can enjoy both worlds - that of private key cryptography and that of public key cryptography. A quantum key produced from a quantum one way function can be both public and private at the same time! It is public since a copy of the same state is given to all participants, and it is private since none of them can actually learn the classical description of the state from the quantum system in his hands.

Unlike classical schemes, when we use quantum public keys only a limited number of copies of the public key can be issued, if only a small amount of information about the key is allowed to be

exposed. The relation between the number of copies and security level is a property of the QOWF f, and in general there is no upper bound on the number of copies per given security level. A choice of which QOWF to use should be based on this tradeoff, together with other considerations such as computation and communication complexity, and other parameters depending on the particular application that is being designed.

In addition to the issue of number of copies of a key, like classical private keys, and unlike classical public keys, all known quantum public keys have length (in qubits) at least as long as the length (in bits) of the messages. The schemes that we exhibit in this work use keys with length longer the length of the message to be encrypted. The question of whether it is possible to have a quantum public key shorter, or at least with same length, as the message length is left open.

There are some difficulties with quantum public keys that do not exist in the classical analog. For instance, unlike classical one way functions, where a computationally bounded adversary can learn nothing at all about the input, the quantum state always leaks some (limited) amount of information. Furthermore, quantum cheating strategies become available; for example, how can we be sure that all the copies of the public key in the system are identical? Along the same lines, the 'dealer' who distributes the keys might prepare an entangled initial state (instead of a key which is in product state with the rest of the world) which can be manipulated later to bias the output of the protocol; the ability to do so is the key observation in proving that quantum one way functions cannot be used to perform bit commitment [49, 44], which is one important application of classical one way functions. In this sense QOWFs are disappointing compared to classical OWFs - the latter can be used for (computationally secure) bit commitment, while the former can't be used for (unconditionally secure) bit commitment.

Most of the new difficulties introduced by using quantum states as a public key can be dealt with by using many public keys, instead of just one, and performing some testing, which destroys some of them, to make sure that the rest can be used safely. However the kind of difficulty that makes quantum bit commitment impossible cannot, of course, be overcome.

Quantum public keys are, as explained, more difficult to deal with, and in some sense more limited, than classical public keys; however they remain more powerful than the classical analog, because they provide information theoretic security. The existence of unconditionally secure public key schemes suggests that the potential of quantum public key cryptography has not been fully realized yet.

A complete and rigorous treatment of quantum public key cryptography is an important contribution of this thesis. This is done in Chapter 1, where a formal treatment of quantum public key cryptography, including a definition and discussion of the parameters and characteristics of a quantum key system, and the connections of these parameters to the communication cost of a protocol, is given. The definition captures the precise meaning and intuition of a public key. The chapter also contains three examples of protocols for quantum public keys, with a thorough analysis of their parameters according to the definitions there. The protocols are "the random access code (RAC) protocol", "the modified RAC protocol" and "the oblivious rotations (OBR) protocol". The RAC protocol provides perfect protection for the identity of the sender of a message. The amount of protection to the content of a message depends on the choice of parameters of the protocol, which also determine the relation of the key length and message length, and the relation of the key length and number of users of the protocol. If the number of users is n, and we encrypt a message of length l with a key of length at least $l + polylog(l \cdot n)$ we get polynomially small security (in n and l). By "polynomially small security" we mean that an eavesdropper can get only polynomially small amount of information about the content of a message. The MRAC protocol provides the same amount of protection as the RAC protocol, but potentially uses shorter keys (how much shorter is an open question, since we do not know how to exactly analyze this). The OBR protocol perfectly protects the identities of communicating parties, but to achieve good protection to the content of a message it requires a key of length exponential in the number of users (actually the number of *dishonest users* is what matters, but in the worst case this is linear in the total number of users).

One natural context to use quantum public keys in, is the problem of network anonymity, which has great practical interest. This problem can be formulated as a special case of the more general problem of secure multi-party computation (SMPC). SMPC was introduced by [35], and received a considerable amount of attention in the literature. In this scenario, there are n players in a network, synchronized with a common clock, and communicating in rounds (one round corresponds to one tick of the clock). A player can at each round send messages of arbitrary length to any number of other players. A message that one player sends in the current round to another player, who is connected to the first player with a communication link, will reach its destination in the next round. Each player i has an input x_i, and the players want to run a protocol to collectively compute some joint function $f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)$, such that player i gets the part f_i. The challenge is that no player can learn any information beyond the value of (his part of) the computed function, and the information contained in his input. Players that deviate from the protocol, and who

are trying to learn more information than they are supposed to, are called *dishonest* players. Such dishonest players can also work in collaboration. For convenience we usually relate all the dishonest activity to a single entity, the adversary, who is assumed to control the behavior of all the dishonest players. The adversary is also assumed to control all the communication links in the system, i.e. has access to all the data that is transferred through them. In the network anonymity subproblem the inputs x_i is a list of messages and destinations telling player i in the current round what messages to send to what other players. The output $f_i(x_1, \ldots, x_n)$ is a list of all the messages that are initiated in the current round and are aimed to player i (and are to be received by player i in some future round). Goldreich et al. [35] proved that under computational assumptions, secure multi-party evaluation of any function is possible provided that there are no more than $t < n/2$ dishonest players (and provided that the adversary is computationally bounded). Beaver et. al. [5] show that if a trapdoor function[1] exists then every polynomial time computable function (such as the function that corresponds to network anonymity) has a SMPC protocol which deals with $n/2$ dishonest players, takes a constant number of rounds, and the amount of communication in each round is polynomial in the number of players. Subsequently, Ben-Or et al. [9] and Chaum et al. [30] independently proved that tolerating up to $t < n/3$ was possible without computational assumptions, provided that every pair of participants is connected by a secure channel. The bound of $n/3$ for information-theoretically SMPC (i.e. when the adversary is unbounded) was broken by Rabin and Ben-Or [53] and Beaver [6], who showed that assuming the existence of a reliable broadcast channel, then one can in fact tolerate up to $n/2$ dishonest players without computational assumptions. Their protocols introduce a small error probability, which is provably unavoidable [53].

To summarize these results in the context on network anonymity, the current situation is that in both the computational (i.e. computationally bounded adversary) and the information theoretic (i.e. unbounded adversary) cases there is a solution to the network anonymity problem provided that the adversary controlls no more than half of the players in the network. The solution in the unconditional case requires a reliable broadcast channel. Both solutions require only a constant number of rounds per message delivery, but the total communication cost per message delivery is polynomial.

Another limitation with regard to SMPC protocols is that they are not *scalably efficient*, mean-

[1] A trapdoor function is a special case of OWF with the property that it is computationally easy to invert $f(x)$ given some additional information y (x is not a function of y). y is called the trapdoor.

ing that the communication complexity of the protocols described in the literature grows superlinearly with the size of the inputs. This superlinear increase happens because of the use of techniques such as *zero-knowledge proofs* as an ingredient [54]. In the context of network anonymity this means that increasing the length of the messages being sent results in a superliner growth of communications in the network.

In Chapter 2 we focus on approaching the network anonymity subproblem directly. In its general form, there are n players $P_1, \ldots, P_n$, and at each round each player i may want to send a message m_i to some receiver P_j. We require that an adversary, who might control a fraction of the processors in the network, as well as communication links, can not link senders to receivers (this property is sometimes referred to as *unlinkability*), and also that only the receivers learn the content of the message that was sent to them (privacy). We ask if the restriction to a special case allows us to find better solutions than in the general SMPC protocols, both in the computational and information theoretic cases, and both in the cases where the adversary controls all, or just an arbitrary < 1 fraction, of the communication links. Specifically, for each of the above cases the following questions arise:

1. Can we tolerate a fraction of dishonest players larger than $\frac{1}{2}$?

2. Can we achieve better round-complexity or better total communication-complexity?

3. Would it be helpful in this context to use quantum communication rather than classical?

There is a large body of work on this problem in the *classical* setting, e.g. [28, 29, 54, 55, 17, 2, 56]. See also [31]. There have also been some prior work on anonymous messages using quantum information, [33, 47, 19] to mention a few. These address the problem of anonymous communication in a simplified settings, and give only partial, or none at all, analysis.

Approaching the network anonymity problem directly, without reduction to SMPC, allows some improvements.

Classically (i.e. without quantum communication), in the model of a polynomially bounded adversary who controlls all the communication links, there is a solution that tolerates an arbitrary fraction of dishonest players (instead of $\frac{1}{2}$), and takes a polylogarithmic number of rounds per message, and $O(n \cdot polylog(n))$ total communication cost per message [54]. In the model where the polynomially bounded adversary controlls only a fraction of the links (though it can be an arbitrarily large fraction), the total communication per message improves to be also polylogarithmic [17].

Still in the classical world, but now considering the information theoretic model (i.e. unbounded adversary), there has been much less effort done. There is a solution in the information theoretic model [39], which we describe in Section 2.4, and which allows the adversary to control all the communication links and an arbitrary fraction of the users. This solution has linear round complexity and linear communication complexity. In the information theoretic case, and in the model where the adversary might control more than $\frac{1}{2}$ of the users, no classical solution is known to have better efficiency than this solution, even when the adversary is assumed to control just a fraction of the communication links, and not all of them.

In Chapter 2 we focus on improving both the round complexity and the communication complexity in the information theoretical security setting, using quantum communication.

When quantum communication comes into picture, it is shown in Section 2.2 how to achieve a solution in the information theoretic model, with an arbitrary fraction of dishonest players, which has polylogarithmic round complexity. In the case where the adversary controlls all the communication links, the communication complexity of the quantum solution is $O(n \cdot polylog(n))$. In the case where the adversary controlls only a fraction of the links, the communication complexity of this solution is polylogarithmic (i.e. $O(polylog(n))$). Thus, in both settings (adversary controls all or just an arbitrary fraction of the links) we provide significant improvements over the best known classical solutions in the information theoretical setting. As mentioned, our quantum results should be compared to the following classical results: if the fraction of dishonest players is $< 1/2$ SMPC can be used, and it gives constant round complexity and polynomial communication complexity, regardless of the number of communication links that the adversary controls (it can be all of the links). The solution of [39] gives linear round complexity and linear communication complexity in both the cases where the adversary controls $< 1/2$ or $> 1/2$ of the users, again regardless of the number of communication links that the adversary controls.

The improvement is achieved by improving the key distribution (which we also call encryption) protocols, to derive quantum information theoretical secure protocols which are local, as we explain soon. These are then plugged as black box to existing classical reductions to the network anonymity problem, as we explain later.

We now get into more details about the structure of the computational and of the information theoretic solutions.

The general problem of network anonymity (either computational or information theoretic) can be reduced into two parts, as was shown in [54, 17]:

Definition 0.1. *An anonymous network has the two parts:*

- *(Privacy and Symmetry) It is an encryption scheme with the properties that an encrypted message is unreadable to anyone but the intended recipient (privacy), and that the content of the encrypted message has no information about the identity of the sender (symmetry).*

- *(Traffic anonymity) Even when symmetry is guaranteed, an adversary can still try and learn the pattern of communications in the network by simply monitoring channel uses, checking which message goes from where to whom. This is called traffic analysis. Traffic anonymity is achieved if, assuming privacy and symmetry, nothing can be studied about the identity of the sender given the view of the traffic (rather than the content) of the messages in the network.*

The crucial observation is that solutions of these two questions can, in some situations that will soon be described, be combined to achieve a solution to the network anonymity problem. Moreover, the solution to the first part is simply plugged, as a black box, in the solution to the second part - whether the solution to the first part is quantum or classical, computational or unconditional. If the solution to the first (privacy and symmetry) part is computationally secure then we get an anonymous network in the computationally bounded adversary model. And if, on the other hand, the solution to the first part is unconditionally secure then we get an anonymous network in the information theoretic case.

In this line of thought, in 1979 Chaum showed how to use public key cryptography to solve the first part (symmetry and privacy problem) in the presence of a computationally bounded adversary, and then use this to reduce the problem of constructing anonymous networks to the second part (traffic analysis problem). He suggested a protocol, that was later modified and proved for certain attack models [54, 17]. These protocols are robust against an arbitrary fraction of dishonest players, and are relatively efficient, requiring only a polylogarithmic number of rounds per message delivery. The amount of communication per round depends, as previously explained, on the assumptions about the fraction of communication links under adversarial control.

In the information theoretic setting things are more difficult. In a later work [29] Chaum showed how to achieve symmetry (but not privacy) also in the information theoretic setting. To be accurate with historical facts, in his 1988 paper Chaum treated anonymity without privacy, thus solving a somewhat simpler problem, where only the identities of communicating parties have to be concealed, and not the actual information communicated. However his idea can be extended

to include both privacy and symmetry [2]. However, the resulting information theoretic solution is much less efficient (in terms of its communication cost) than the computational ones, because each message delivery requires at least the same communication rounds as the number of players, i.e. n rounds. The reason for this huge overhead in communication rounds is, generally speaking, that each message requires the cooperation and participation of ALL players. A description of the protocol, as well as a discussion of its properties (including number of rounds) is given in Section 2.4.

The superior efficiency of the classical computational solutions compared to the classical information theoretic solution [39] is thanks to the use of public keys, such as, e.g., the ones produced using RSA, in the computational solutions, as the underlying cryptosystem with which messages are encrypted. Let us now focus on this observation.

Public key cryptography obviously provides privacy and symmetry (Definition 0.1), because encryption depends only on public information. What makes it especially suitable for solving the problem of network anonymity efficiently is one special and important feature that common public key protocols have. We call this special feature *locality*, which actually means two things:

Definition 0.2. *We call an encryption scheme (protocol) 'local' if*

1. *the ciphertext e that it produces depends only on information known to the player who generated it, and not on information of any other player. In other words, a player does not depend on cooperation with any other player to send his messages.*

2. *message delivery is performed in one way and one round communication from sender to receiver.*

This locality property is a very nice feature of public-key based encryptions, which contributes to the simplicity and efficiency of the communications by eliminating the dependency on cooperation of other players to deliver a message.

The downside of using classical public key cryptosystems is, however, that their security relies on computational assumptions and thus they cannot be used in an information theoretic setting.

So we see that good solutions to the network anonymity problem are known against computationally-bounded adversaries that control an arbitrary fraction of the processors in a network. Much of the

[2] I am grateful to Yuval Ishai [39] for showing me how to extend Chaum's idea to include both privacy and symmetry. See Section 2.4 for a description of Ishai's solution

reason why such relatively efficient protocols exist is that they exploit the locality property (Definition 0.2) of public key encryption. This locality eliminates the dependency of one player on others, and allows using the *symmetry and privacy* property (Definition 0.1) as an ingredient in a protocol for fooling *traffic analysis* (second part of Definition 0.1). If we could also have an information theoretic local, private and symmetric cryptosystem, like the computational one (RSA), we could solve the network anonymity problem with the same efficiency also in an information theoretic sense. This is because, as we said before, this local, private and symmetric protocol can be plugged into an existing solution to the traffic anonymity problem, as a black box.

Solutions to the traffic anonymity problem are known, that use results from classical information theory, and take polylogarithmic round complexity and polylogarithmic communication complexity [54, 17].

So the main question we ask is:

- Can a cryptosystem (encryption scheme) be local, private and symmetric, also in an information theoretic sense?

Well, the answer is YES - this is exactly what is shown in Chapter 1 - the quantum tools allow us to create a local, private and symmetric encryption scheme against an unbounded adversary!

Theorem 0.3. (rough version) *There are quantum public key based encryption schemes which are local and also information theoretic private and symmetric.*

On the other hand, it is shown in Section 2.3 that if we restrict ourselves to the classical world then the answer to the above question becomes No:

Theorem 0.4. (rough version) *No classical cryptosystem can be local and at the same time unconditionally private and symmetric.*

The result of Section 2.3 is actually even much stronger than what is expressed in the above theorem. It is shown there that even if a classical protocol is allowed to use quantum key distribution as a black box, still it cannot have the desired properties.

Section 2.2 describes how to use the usual reduction (of symmetry+privacy to traffic anonymity) to achieve efficient information theoretic network anonymity. It is done by plugging the quantum protocol as an ingredient into existing protocols for the problem of traffic analysis. This gives:

Theorem 0.5. (rough version) *For an adversary who controlls an arbitrary (less than* 1*) fraction of the users, and of the communication links in a network, there is an information theoretic solution to the network anonymity problem, based on quantum communications, that requires just a polylogarithmic number of communication rounds per message, and also only polylogarithmic amount of total communication cost (measured in qubits) per message.*

If the adversary controlls ALL the communication links in the system, and not just a fraction of them like in Theorem 0.5, then a linear number of users are required to participate in each round, regardless of whether they wish to send a message or not (in which case the user who does not have a real message to send can simply send a dummy message). In this situation, which is discussed in [54], the communication complexity of the solution to the traffic anonymity problem (Definition 0.1) is linear in the number of players, and in the size of the messages. In this case Theorem 0.5 changes such that the total communication cost per one message is $O(n \cdot polylog(n))$ instead of just $O(polylog(n))$ (where n is the number of users in the network). This is discussed in Section 2.2.

We note here that the classical information theoretic solution, [39], based on Chaum's ideas ([29]) is not local, which means that you have to rely on cooperation of other participants to deliver your messages. There are two penalties for this "non-locality": one is a tremendous increase in communication rounds per single message, namely linear instead of polylogarithmic. The other is the same increase in the total communication cost per message - again from polylogarithmic to linear. This point is further clarified in Section 2.4.

The second part of the thesis deals with private quantum key distribution, rather than public. We refer to such protocols as quantum key distribution (QKD), following the literature. The focus is on seeking new QKD protocols, that would be on one hand as simple as possible, and on the other hand have improved security.

In a quantum key distribution protocol Alice distributes a classical string key to Bob (usually, but not always, it is a bit-string. In this thesis I focus on protocols for the distribution of a key composed of *trits*). The key string of length k is encoded into the state of $n > k$ quantum systems, which are sent to Bob over a quantum public channel, which might be subject to eavesdropping and to some noise. It is assumed that in addition to the quantum channel Alice and Bob are also connected by an authenticated classical channel. This can be realized by either assuming that the classical channel can only be subject to passive eavesdropping by Eve, or that Alice and Bob share an initial short authentication key at the beginning of the process (this is why QKD

is sometimes referred to as quantum key expansion rather than key distribution). The basic idea is that logical values (0 and 1 in the case of bits) are encoded by Alice on quantum states which are not necessarily orthogonal and thus, by the fundamental laws of quantum mechanics, Eve cannot gain any amount of information about the key without causing some disturbance to the quantum states. Any interaction with the quantum states in order to gain information introduces disturbance to the signals, and this disturbance can be detected by Alice and Bob and cause the abortion of the protocol. The main idea is, therefore, that if the amount of disturbance caused by Eve is higher than a certain threshold then she is to be exposed by Alice and Bob with very high probability. If, on the other hand, the disturbance is low, then the amount of information available to Eve is bounded from above, in such a way that using some standard classical techniques such as privacy amplification, Eve's information can be reduced exponentially, leaving Alice and Bob with an agreed key which Eve has only a negligible information about.

The first quantum key distribution protocol was proposed by Bennett and Brassard in 1984 [16]. This simple protocol was followed by numerous other variants and protocols over the years, all following the same principle ideas from quantum information theory.

The protocols for quantum key distribution generally have a structure which consists of four stages - *quantum* stage (in which the quantum particles are sent and measured), *parameter estimation* (in which it is verified that the amount of disturbance is indeed below a certain value), *information reconciliation* (which corrects Bob's bit-errors to the true values of Alice) and *privacy amplification* (which reduces Eve's information to a negligible amount).

The first stage is the only stage that is 'quantum' - the other three are purely classical, and use the classical authenticated channel to communicate. The classical stages can be carried out with one way communications from Alice to Bob. Protocols with two ways communications are also considered in the literature (e.g. [37]), and are known to allow higher maximum tolerable channel noise over the one way counterpart, but they are less simple for implementation.

The security of QKD protocols against various possible eavesdropping attacks was discussed extensively over the years. It was not until 1998 that a general proof, unlimited to any specific type of attack, was presented for the BB84 protocol by Mayers [48]. Another general proof, published around that same time, is due to Biham, Boyer, Brassard, van de Graaf and Mor [18]. Unlike these two proofs, which are quite complicated, there is a simple proof given by Lo and Chau [45]. However, this proof is for a variant of the BB84 protocol which unlike the original BB84 requires that the communicating parties have the ability to perform certain quantum computations rather

than just having the ability to prepare and to measure certain one qubit states, as in the original BB84. It is usually more difficult to prove the security of protocols like BB84, which requires only very simple 'prepare and measure' capabilities of Alice and Bob, than protocols that use quantum computers or entanglement. In principle one can say that 'the simpler the protocol the harder the proof'.

In the year 2000 Preskill and Shor [62] gave another proof of the security of the BB84 protocol against general attacks. Applying a series of simple reduction steps, they showed that BB84 has the same level of security as a simple protocol based on a CSS quantum error correcting code. The proof of Preskill and Shor is the most simple and elegant proof that was ever given to the security of the BB84 protocol.

The maximum tolerable error rate of the underlying CSS code was used to give a lower bound on the maximal tolerable error rate of the corresponding QKD protocol. This is the maximal amount of error for which the key rate is still positive, i.e. for which it is still possible to distill random secret bits. In the case of BB84 it was estimated that up to 11% error rate is acceptable.

A different proof technique, covering a large class of QKD protocols, was devised by Kraus et. al. in 2003 [57]. They showed that the estimate of the maximum error rate can sometimes be improved if Alice adds some random noise to her classical data, before the information reconciliation stage of the protocol. Using this method they get 12.4% tolerable error rate for BB84.

A further improvement, stretching the lower bound to 12.92%, was later demonstrated by [63]. This improvement comes from the application of degenerate block coding.

An advantage of the approach of [57] over other proofs is that it can be extended (as we do in this thesis) to protocols that use d-level quantum systems with d larger than 2.

In Chapter 4 we use three-level systems for quantum key distribution. The private key generated this way is composed of *trits* instead of bits. Using higher dimensional systems for quantum key distribution has the advantage of a higher secret key rate than what is obtainable with qubits, for a given amount of noise in the system. However, they are believed to be technically more complex to implement.

In contrast, we show in Chapter 4 that there are one-way quantum key distribution protocols, based on three level systems (using biphotons), which have a very simple implementation, and yet admit higher key rates than the best two-level protocols. By "simple implementation" we mean that the protocol employs only computational basis states, and states which can be produced from computational basis states using only the set of quantum operators allowed in two-level protocols.

The detailed definition of the term "simple implementation", as well as the derivation of this set of operations, and the construction of the protocols, are all given in Chapter 4. A more succinct version of the results can also be found at [21].

From the experimental viewpoint, there are several ways of physically realizing qutrits using photons. The first possibility is to utilize multiport beam splitters, and more specifically those that split the incoming single light beam into three [68]. The second one exploits the polarization degree of freedom of a biphoton [38, 25]. A third possibility, which uses only one photon per qutrit, exploits the spatial angular momentum of photons [46]. Finally, another realization of qutrits exploits time bins [65].

In our realization we implement ternary logic using biphotons (instead of the usual implementation of binary logic with photons) as the underlying three level quantum systems. It is demonstrated that qutrit quantum key distribution can be as simple as qubit protocols where, as already mentioned, "simple" means that we are allowed to use only qubit operators (2×2 unitaries), applied to qutrits. This is possible with biphotons, since a single-photon operator can be applied to both members of a biphoton. Thus, quantum cryptographic protocols that use qutrits instead of qubits lie in the reach of the current state-of-the-art quantum optical techniques; they are as easily implementable as qubit protocols, whereas they are (a) - more efficient in terms of channel use and, (b) - they admit a higher key rate for a given noise level.

This result is joint work with Hagai Eisenberg. In particular we show that

Theorem 0.6. (rough version) *There exist three-level quantum key distribution protocols, implemented with biphotons and with single photon operators, that have the ability to produce non-zero key rates in much higher noise levels than all known two-level protocols, namely, to tolerate stronger levels of noise. The maximum tolerable noise level is* 17.4%.

The significance of this result is discussed in Section 4.2.3, where it is compared to known results for other protocols. In particular, the noise level of 17.7% should be compared to an upper bound of 16.3% for the six states protocol, which is the best known single photon protocol.

The analysis technique we used is an extension of [57] to quantum systems with 3 dimensions. Using this technique we derived a convex optimization problem which we solved numerically, and whose solution is the 17.7% lower bound on the tolerable error rate. For the solution of the convex optimization problem we used the cvxopt library of the Python programming language [1].

There is an important remark about this result. This is that the error rate in the system (induced

by quantum channel noise or, equivalently, by eavesdropping activity), which is the fraction of damaged signals, can behave differently when the signals are qutrits instead of qubits. In principle, the same quantum channel is likely to induce higher error rate when it is used for transmission of biphotons than with single photons, simply because it is a bigger quantum system. On the other hand, to model the effect of practical quantum channels it is usually sufficient to consider just the set of single photon operations, rather than arbitrary biphoton operations. This restriction to single photon operations can reduce the channel induced error rate on biphotons significantly. The exact relation between the error levels of the same channel when used to communicate single photons and biphotons is still an open question under research. Therefore, there should be some sort of a normalization factor when comparing error rates in protocols based on photons and on biphotons. The value of this normalization factor is yet unknown.

Part II

Quantum Public Keys

Chapter 1

Quantum public key cryptography

1.1 Preliminaries

We assume here familiarity with the notion of density matrices, Hilbert spaces and quantum states. For background on this, see [52].

1.1.1 Fidelity and trace distance

Let ρ be a mixed state with support in a Hilbert space $\mathcal{H}$. A *purification* of ρ is any pure state $|\phi\rangle$ in an extended Hilbert space $\mathcal{H} \otimes \mathcal{K}$ such that $\mathrm{Tr}_{\mathcal{K}}|\phi\rangle\langle\phi| = \rho$. Given two density matrices ρ_1, ρ_2 on the same Hilbert space $\mathcal{H}$, their *fidelity* is defined as

$$F(\rho_1, \rho_2) \;=\; \sup |\langle \phi_1 \,|\, \phi_2 \rangle|^2 \,,$$

where the supremum is taken over all purifications $|\phi_i\rangle$ of ρ_i in the same Hilbert space.

The *trace norm* of a matrix A is defined as

$$\| A \|_{\mathrm{tr}} = \mathrm{Tr}\, |A| \,,$$

where $|A| = \sqrt{A^\dagger A}$.

Jozsa [41] gave a simple proof, for the finite dimensional case, of the following remarkable equivalence first established by Uhlmann [66].

Fact 1.1 (Jozsa)**.** *For any two density matrices ρ_1, ρ_2 on the same finite dimensional space $\mathcal{H}$,*

$$F(\rho_1, \rho_2) \;=\; \left[\mathrm{Tr}\left(\sqrt{{\rho_1}^{1/2}\,\rho_2\,{\rho_1}^{1/2}}\right)\right]^2 \;=\; \|\,\sqrt{\rho_1}\sqrt{\rho_2}\,\|_{\mathrm{tr}}^2\,.$$

Using this equivalence, Fuchs and van de Graaf [32] relate fidelity to the trace distance.

Fact 1.2 (Fuchs, van de Graaf)**.** *For any two mixed states ρ_1, ρ_2,*

$$1 - \sqrt{F(\rho_1, \rho_2)} \;\leq\; \frac{1}{2}\,\|\,\rho_1 - \rho_2\,\|_{\mathrm{tr}} \;\leq\; \sqrt{1 - F(\rho_1, \rho_2)}.$$

Also, $\sqrt{F}$ is concave (see [52], Theorem 9.7).

1.1.2 Local transition between bipartite states

Jozsa [41] proved:

Lemma 1.3 (Jozsa)**.** *Suppose $|\phi_1\rangle, |\phi_2\rangle \in \mathcal{H}\otimes\mathcal{K}$ are the purifications of two density matrices ρ_1, ρ_2 in $\mathcal{H}$. Then, there is a local unitary transformation U on $\mathcal{K}$ such that $F(\rho_1, \rho_2) = |\langle\phi_1|(I\otimes U)|\phi_2\rangle|^2$.*

As noticed by Lo and Chau [44] and Mayers [49], Lemma 1.3 immediately implies that if two states have close reduced density matrices, than there exists a *local* unitary transformation transforming one state close to the other. Formally,

Lemma 1.4. *(based on [44, 49, 41, 32]) Let ρ_1, ρ_2 be two mixed states with support in a Hilbert space $\mathcal{H}$. Let $\mathcal{K}$ be any Hilbert space of dimension at least* $\dim(\mathcal{H})$*, and $|\phi_i\rangle$ any purifications of ρ_i in $\mathcal{H}\otimes\mathcal{K}$.*

Then, there is a local unitary transformation U on $\mathcal{K}$ that maps $|\phi_2\rangle$ to $|\phi_2'\rangle = I\otimes U|\phi_2\rangle$ such that

$$\left\|\,|\phi_1\rangle\langle\phi_1| - |\phi_2'\rangle\langle\phi_2'|\,\right\|_{\mathrm{tr}} \;\leq\; 2\sqrt{1 - F(\rho_1, \rho_2)}.$$

1.1.3 Trace distance and distinguishability

The trace distance between two density matrices tells us how well we can distinguish them via quantum measurement.

A general measurement, called a *POVM (Positive Operator-Valued Measure)*, is a set of positive operators $\{E_i\}$ that satisfies

$$\sum_i E_i = I.$$

Given two density matrices ρ_1 and ρ_2, A POVM $\{E_i\}$ induces two probability distributions, P, Q, over measurement outcomes. Let $p_i \equiv \mathrm{Tr}(\rho_1 E_i)$ and $q_i \equiv \mathrm{Tr}(\rho_2 E_i)$ be the probabilities to obtain measurement result labeled by i. The l_1 distance of the two distributions is $|P-Q|_1 = \sum_i |p_i - q_i|$. Lemma 1.5 connects the trace distance between the density operators to the l_1 distance of the corresponding probability distributions. Fact 1.6 gives the connection to the success probability of distinguishing the two density operators.

Lemma 1.5.

$$\| \rho_1 - \rho_2 \|_{\mathrm{tr}} = \max_{\{E_i\}} |P-Q|_1 ,$$

where the maximization is over all POVMs $\{E_i\}$.

Proof. First note that the matrix $\rho_1 - \rho_2$ may be written as $R_1 - R_2$, where R_1 and R_2 are positive operators with support on orthogonal vector spaces. To see this we use the spectral decomposition to write $\rho_1 - \rho_2 = UDU^\dagger$, and then split the diagonal matrix D into positive and negative parts. Also note that $|\rho_1 - \rho_2| = R_1 + R_2$.

Now

$$|P-Q|_1 = \sum_i |\mathrm{Tr}(E_i(\rho_1 - \rho_2))|,$$

and

$$\begin{aligned} |\mathrm{Tr}E_i(\rho_1 - \rho_2)| &= |\mathrm{Tr}(E_i(R_1 - R_2))| \\ &\leq \mathrm{Tr}(E_i(R_1 + R_2)) \\ &= \mathrm{Tr}(E_i\,|\rho_1 - \rho_2|). \end{aligned}$$

Thus

$$\begin{aligned} |P-Q|_1 &\leq \sum_i \mathrm{Tr}(E_i\,|\rho_1 - \rho_2|) \\ &= \mathrm{Tr}((\sum_i E_i)\,|\rho_1 - \rho_2|) \\ &= \mathrm{Tr}(|\rho_1 - \rho_2|) \\ &= \| \rho_1 - \rho_2 \|_{\mathrm{tr}} , \end{aligned}$$

where we used the fact that for a POVM $\{E_i\}$, $\sum_i E_i = I$.

To turn the first inequality into an equality we can simply choose $\{E_i\}$ to be projections onto

the support of R_1 and R_2. This way we see that there exist a measurement such that $\| \rho_1 - \rho_2 \|_{\mathrm{tr}} = |P - Q|_1$. □

Fact 1.6. *Suppose we are given a random sample from either probability distribution P or probability distribution Q, and we are asked to guess from which of the distributions it was taken.*

Denote $\frac{1}{2} + \epsilon$ the success probability of the best guess, then

$$\epsilon = \frac{1}{4} |P - Q|_1 .$$

Proof. Define a binary indicator random variable X, which can take values 0 or 1, with equal probability $\frac{1}{2}$. The value 0 corresponds to the event that the probability distribution P was chosen, and 1 corresponds to Q being chosen.

Given a random sample a from either P or Q, one can verify that the best guess would be P if $P(a) \geq Q(a)$, and Q otherwise. The success probability according to this strategy is

$$\begin{aligned}
&\Pr(\mathit{success}) = \\
&= \frac{1}{2} + \epsilon \\
&= \sum_{a|P(a)\geq Q(a)} (\Pr(a) \Pr(X = 0|a)) + \sum_{a|Q(a)>P(a)} (\Pr(a) \Pr(X = 1|a)) \\
&= \sum_{a|P(a)\geq Q(a)} (\Pr(X = 0) \Pr(a|X = 0)) + \sum_{a|Q(a)>P(a)} (\Pr(X = 1) \Pr(a|X = 1)) \\
&= \frac{1}{2}(\sum_{a|P(a)\geq Q(a)} (P(a)) + \sum_{a|Q(a)>P(a)} (Q(a))),
\end{aligned}$$

from where we see that

$$\begin{aligned}
\epsilon &= \frac{1}{2}(\sum_{a|P(a)\geq Q(a)} (P(a)) + \sum_{a|Q(a)>P(a)} (Q(a)) - 1) \\
&= \frac{1}{2}(\sum_{a|P(a)\geq Q(a)} (P(a)) - \sum_{a|P(a)\geq Q(a)} (Q(a)))
\end{aligned}$$

and in the same way

$$\epsilon = \frac{1}{2}(\sum_{a|Q(a)\geq P(a)} (Q(a)) - \sum_{a|Q(a)\geq P(a)} (P(a))).$$

Summing the last two equalities gives

$$\epsilon = \frac{1}{4} |P - Q| .$$

□

1.1.4 Trace distance and information

Given a probability distribution P, the Shannon entropy of P is defined as $H(P) = -\sum p_i \log p_i$. The Von-Neumann entropy $S(A)$, of a quantum system A whose state is described by a density matrix ρ_A is $S(A) = -\operatorname{Tr} \rho_A \log \rho_A$. This is sometimes denoted $S(\rho_A)$ instead of $S(A)$, which is equivalent. Given a density operator ρ_{AB}, describing the state of a composite system AB, let ρ_A denote the reduced density matrix of subsystem A (and similarly define ρ_B). The joint entropy for the composite system AB is $S(A, B) = -\operatorname{Tr} \rho_{A,B} \log \rho_{A,B}$. The conditional entropy of system A given system B is $S(A|B) = S(A, B) - S(B)$. The mutual information of A and B is $I(A : B) = S(A) + S(B) - S(AB)$. This quantity is non-negative. Similarly, $I(A : B|C) = S(A|C) + S(B|C) - S(AB|C)$.

Theorem 1.7. (Joint entropy theorem) *Suppose P is a probability distribution, which assigns to i the probability p_i. Let $|i\rangle$ be orthogonal states for a system A, and ρ_i is any set of density operators for another system, B. Then $S(\sum_i p_i |i\rangle\langle i| \otimes \rho_i) = H(P) + \sum_i p_i S(\rho_i)$.*

Proof. The proof appears in [52], Theorem 11.8, fifth item. □

The following is a simple fact, whose proof is omitted.

Fact 1.8. *Let ρ_{AB}, σ_{AB} be two density matrices, then $\| \rho_A - \sigma_A \|_{\mathrm{tr}} \leq \| \rho_{AB} - \sigma_{AB} \|_{\mathrm{tr}}$.*

Lemma 1.9 (Fannes inequality)**.** *Let ρ, σ be two density matrices in a Hilbert space of dimension d. Let $\delta = \| \rho - \sigma \|_{\mathrm{tr}}$, then*

$$|S(\rho) - S(\sigma)| \leq \delta(\log d + \log \frac{1}{\delta})$$

The proof of lemma 1.9 can be found at [52], Box 11.2. A simple corollary is:

Claim 1.10. *Let ρ_{AB}, σ_{AB} be two density matrices. Assume that,*

- *$F(\rho_{AB}, \sigma_{AB}) \geq 1 - \eta$, and*
- *$I(\sigma_A : \sigma_B) \leq \zeta$*

Then, $I(\rho_A : \rho_B) \leq \zeta + O(\log(dim(AB)) \cdot \sqrt{\eta})$.

Proof. By Fact 1.2

$$\| \sigma_{AB} - \rho_{AB} \|_{\mathrm{tr}} \leq 2\sqrt{1 - F(\rho_{AB}, \sigma_{AB})} \leq 2\sqrt{\eta}.$$

we can use Fact 1.8 and Lemma 1.9 and get

$$\begin{aligned} I(\rho_A : \rho_B) &= S(\rho_A) + S(\rho_B) - S(\rho_{AB}) \\ &\leq S(\sigma_A) + S(\sigma_B) - S(\sigma_{AB}) + O(\log(dim(AB)) \cdot \sqrt{\eta}) \\ &= I(\sigma_A : \sigma_B) + O(\log(dim(AB)) \cdot \sqrt{\eta}) \\ &\leq \zeta + O(\log(dim(AB)) \cdot \sqrt{\eta}) \end{aligned}$$

□

Note that Claim 1.10 is also true for conditional entropies, i.e. when the second assumption is replaced with an expression of the form $I(\sigma_A : \sigma_B|\sigma_C) \leq \zeta$. We will make use of this form of Claim 1.10 in Section 1.3.

1.2 A model of quantum public keys

Consider a system involving some players P_1 to P_n, and some distinct player Alice. We consider a situation in which one of the players is chosen according to some distribution, to send a message to Alice. The message sent is also chosen according to some distribution (that may depend on the player). Each player P_i has working space $\mathcal{P}_i$ initialized at $|\vec{0}\rangle$. Each player also has a key register $\mathcal{S}_i$, which is initialized as follows: Alice picks a secret s, creates a pure state $|\psi_s\rangle$ (the quantum public key) and sends an independent copy of $|\psi_s\rangle$ to each player. A unique active player P_i is picked at random from some probability distribution over players, and the message m is picked at random from some probability distribution over messages, and stored in a register $\mathcal{M}$ to which only the active player has access. The active player uses his copy of $|\psi_s\rangle$ to encrypt m. This is done by applying a superoperator E (the encoding procedure) jointly on registers $\mathcal{S}_i, \mathcal{P}_i, \mathcal{M}$. He then sends the resulting register $\mathcal{P}_i$ to Alice. To decode, Alice applies a POVM D (the decoding procedure) on the received message.

Unlike classical public keys, quantum public keys are one time pads - a key has at least the same

length as the data it is used to encrypt, and if a key is used more than once its security decreases.

Nevertheless, there is a worthwhile distinction to be made. While the quantum state of a single public key can only be used once, it is quite possible to send more than one message using different copies of the quantum public key with the same private key held by Alice. This means that the full distribution of the quantum states does not need to be performed for each new message, but only once the stock of public keys originally distributed runs low.

Definition 1.11 (correctness)**.** *We say a protocol is α-correct if for every message m and every player i, the probability (over the secret s and the measurements) that Alice decodes the message to be m is at least α. We say the protocol is* correct *if $\alpha = 1$.*

Definition 1.12 (privacy)**.** *We say a protocol is β-private against a coalition of k players, if for every i, and every k players $P_{j_1}, \ldots, P_{j_k}$ other than P_i,*

$$I(BE : M) \quad < \quad \beta$$

where B is the quantum register of the qubits held by $P_{j_1}, \ldots, P_{j_k}$ (namely, the qubits in the registers $\mathcal{P}_{j,i}, \mathcal{S}_{j,i}, i = 1, \ldots, k$), E is the quantum register holding the encrypted message and M is the quantum register holding the classical value $m \in \mathcal{M}$. If $\beta = 0$ we say the protocol is private*.*

Definition 1.13 (symmetry)**.** *We say a protocol is γ-symmetric if for every (possibly dishonest) Alice, for every i and m, if P_i is the active player and m is the message,*

$$I(AE : R) \quad < \quad \gamma$$

where A is the quantum register of Alice in $\rho(i, m)$ ($\rho(i, m)$ denotes the density matrix of the system when the active player is i and the message is m.), E is the quantum register holding the encrypted message and R is the quantum register holding the classical value $i \in \mathcal{I}$. If $\gamma = 0$ we say the protocol is symmetric*.*

1.3 Honest key distribution

In this section we present three protocols all having the same overall structure, of two phases. At the key distribution phase, the players distribute quantum systems (keys) to other players, and at

the second phase these keys are used to encrypt messages.

However, these protocols will not satisfy the requirements of quantum key distribution given in Section 1.2: they will not be secure against cheating in the first phase. In other words, we will prove their symmetry, privacy and correctness only under the assumption of "honest key distribution", namely, that everyone plays honestly during the key distribution phase: Alice plays according to the protocol, and no eavesdropping is performed by the other players.

In Section 1.4 we will show a general way to convert any honest quantum key distribution protocol, to a public key distribution protocol, by adding an additional phase.

1.3.1 Protocols

The random access code protocol (RAC protocol)

The first protocol is called *the random access code protocol (RAC)* because the proof of its security can be viewed as some version of the random access code lower bound due to Nayak [51].

THE RANDOM ACCESS CODE (RAC) PROTOCOL

Key distribution : To send a message of length L_1, Alice picks a random function $s : \{0,1\}^{L_2} \to \{0,1\}^{L_1}$, prepares the state $|\psi\rangle = \frac{1}{\sqrt{|\mathcal{M}|}} \sum_{\ell \in \{0,1\}^{L_2}} |\ell, s(\ell)\rangle$ and sends a copy of $|\psi\rangle$ to each of the other n players. Each player P_j measures his copy in the standard basis, and records the result $(\ell_j, s(\ell_j))$.

The parameter L_2 is a security parameter.

Encoding : To send message $m \in \mathcal{M} = \{0,1\}^{L_1}$, player P_i sends the pair $(\ell_i, m \oplus s(\ell_i))$ to Alice.

Decoding : Alice xors $(m \oplus s(\ell_i))$ with $s(\ell_i)$ to get m.

The total number of qubits that are communicated during the RAC protocol is linear in $n \cdot (L_1 + L_2)$ (remember n is the number of players).

The idea behind the protocol is that P_i can easily sample a random label ℓ and its associated value $s(\ell)$, while a coalition of bad players should find it difficult to extract the value associated with the *specific* label ℓ from their joint state. In addition, each player can choose when to use his key regardless of what other players do; it remains safe even if other players use their keys before. Formally,

Theorem 1.14. *Under the assumption of honest key distribution the RAC protocol is correct, symmetric and has $\beta = O(k^{\frac{3}{2}}(L_1 + L_2)2^{-\frac{L_2}{2}})$ privacy against collusions of size $k < n$.*

We can therefore choose

$$L_2 = O(polylog(n)) \tag{1.1}$$

to get β polynomially small. If a smaller β is desirable, we simply need to pay for the improved security with a longer key.

Proof. Since all players get identical copies of the same quantum state $|\psi\rangle$, and apply the same encryption strategy, then clearly the protocol is symmetric. The correctness is also clear. We are left with proving privacy. Let L and S_l denote the classical random variables holding the values ℓ and $s(\ell)$ respectively. B is the quantum register held by the coalition of bad players. We first prove:

Claim 1.15. *$I(B : S_l|E) \leq O(k^{\frac{3}{2}}(L_1+L_2)2^{-\frac{L_2}{2}})$ where B is the quantum register of the joint system of the coalition of k bad players and E is the register of the encoded message (the ciphertext) sent to Alice.*

Proof. (Of Claim 1.15)

$$\begin{aligned} I(B : S_l|E) &= \sum_{\ell} \Pr(L = \ell) \cdot I(B : S_l|L = \ell, M \oplus S_l) \\ &= \frac{1}{2^{L_2}} \sum_{\ell} I(B : S_l|L = \ell, M \oplus S_l) \end{aligned}$$

where the first equality is because $E = (L, M \oplus S_l)$, and since L is a classical random variable we can use Theorem 1.7. The second equality is by definition.

Now, recall that the state of register B is described by $|\psi\rangle = (\frac{1}{\sqrt{2^{L_2}}} \sum_i |i, s(i)\rangle)^{\otimes k}$ and it is in product with the rest of the system. For every ℓ we define the state $|\psi_\ell\rangle = (\frac{1}{\sqrt{2^{L_2}-1}} \sum_{i \neq \ell} |i, s(i)\rangle)^{\otimes k}$. Denote B_ℓ a register which is the same as register B, but with the state $|\psi_\ell\rangle$ replacing the state $|\psi\rangle$. Let ρ_ℓ denote the density matrix of the whole system where $|\psi_\ell\rangle$ replaces $|\psi\rangle$ in register B. We have $\langle\psi\,|\,\psi_\ell\rangle = (1 - 2^{-L_2})^{\frac{k}{2}}$, so by Fact 1.2 (and by the fact that register B is in product with the rest of the system) we get that $\| \rho - \rho_\ell \|_{\text{tr}} \leq 2\sqrt{1 - (1 - 2^{-L_2})^{\frac{k}{2}}}$. By Claim 1.10 (which, as already noted before, is also true for conditional entropies), together with the fact that B is a $k(L_1 + L_2)$ qubit register we have:

$$
\begin{aligned}
I(B:S_l|E) &= \frac{1}{2^{L_2}}\sum_{\ell} I(B:S_l|L=\ell, M\oplus S_l) \\
&\leq \frac{1}{2^{L_2}}\sum_{\ell} I(B_\ell:S_l|L=\ell, M\oplus S_l) + O(k(L_1+L_2)\cdot 2\sqrt{1-(1-2^{-L_2})^{\frac{k}{2}}}) \\
&= 0 + O(k^{\frac{3}{2}}(L_1+L_2)2^{-\frac{L_2}{2}})
\end{aligned}
$$

where the last equality holds because B_ℓ and S_l are independent of each other (also when conditioned on $L=\ell, M\oplus S_l$). In the last equality we also replace $(1-2^{-L_2})^{\frac{k}{2}} \approx 1-\frac{k}{2}e^{-L_2}$, which is only correct assuming that $ke^{-L_2} << 1$. As mentioned before, we will usually take L_2 to be polylogarithmic in n, and of course $k < n$. □

We also have:

$$
\begin{aligned}
I(BE:M) &= S(B,E)+S(M)-S(B,E,M) \\
&= S(E)+S(B|E)+S(M)-S(E)-S(B,M|E) \\
&= S(B|E)+S(M|E)-S(B,M|E) \;=\; I(B:M|E)
\end{aligned}
$$

where the first and second equalities are by definition, and the third because M is independent of $E=(L, M\oplus S_l)$. We can now proceed to have:

$$
\begin{aligned}
I(B:M|E) &= S(B|E)-S(B|E,M) \\
&= S(B|E)-S(B|E,S_l) \\
&= I(B:S_l|E)
\end{aligned}
$$

where the first and third equalities are because $I(Z_1:Z_2)=S(Z_1)-S(Z_1|Z_2)$. The second equality is because $(E,M)=(L,M,M\oplus S_l)$ determines $(L,S_l,M\oplus S_l)=(E,S_l)$ and vice versa.

Together with Claim 1.15 this completes the proof of Theorem 1.14. □

Note that after the key distribution phase of the RAC protocol, which involves quantum communication, the rest of the protocol is purely classical.

The modified RAC (MRAC) protocol

In the RAC protocol the public key is usually much longer than the messages it is used to encode. How much longer depends on the choice of the security parameter L_2, which, in turn, depends on the number of players,. Each secret key s comes with a label ℓ. The message m is XORed with the key s and the result is sent together with the corresponding label ℓ. Using the information of the label Alice knows which key from the set of all keys she must use to open the encrypted message. The first intuition says that without knowing the label she will not be able to read the message, as she cannot decide which key s to use to decrypt. However, counter intuitively, this is not true. Alice can read the message even without receiving the information about the label, as long as she can keep the quantum state in superposition without measuring the register that contains the specific choice of the function she used. If she does that, the density matrices that correspond to the different messages that she can get are almost orthogonal, and thus can be distinguished, which means that Alice can decipher the messages. This is the idea behind the MRAC protocol. The MRAC protocol is a modified version of the RAC protocol, which makes use of this observation and thus does not use labels. It requires Alice to maintain superpositions over time, and it has non perfect correctness - Alice has some (asymptotically vanishing) error probability. The motivating idea behind the MRAC protocol is to try and save in the length of the quantum public key.

THE MODIFIED RAC PROTOCOL

Key distribution : Alice picks a random subset $S \subset \{0,1\}^{L_1}$, of $|S| = 2^{L_2}$ distinct elements. She prepares the uniform superposition

$$|\psi\rangle = \frac{1}{2^{L_2/2}} \cdot \sum_{s \in S} |s\rangle,$$

and sends a copy of $|\psi\rangle$ to each of the other players. Now the complete system of Alice and the n other players can be described by the state

$$\frac{1}{2^{L_2/2}} \cdot \frac{1}{\sqrt{\begin{pmatrix} 2^{L_1} \\ 2^{L_2} \end{pmatrix}}} \cdot \sum_{\substack{S \subset \{0,1\}^{L_1} \\ |S| = 2^{L_2}}} |S\rangle_{Alice} \otimes \left(\sum_{s \in S} |s\rangle \right)^{\otimes n}.$$

Alice keeps the left register without projecting it on any specific S.

Each player P_j measures his copy in the standard basis, and records the result s.

Encoding : Let M be a fixed subset of $\{0,1\}^{L_1}$. To send a message $m \in M$, player P_i sends $m \oplus s$ to Alice.

When Alice receives an encrypted message, the state of her system is

$$\rho_m = \frac{1}{2^{L_1}} \cdot \sum_{s \in \{0,1\}^{L_1}} |s \oplus m\rangle\langle s \oplus m| \otimes |\psi_s\rangle\langle\psi_s|,$$

where

$$|\psi_s\rangle = \frac{1}{\sqrt{\begin{pmatrix} 2^{L_1} - 1 \\ 2^{L_2} - 1 \end{pmatrix}}} \cdot \sum_{S | s \in S} |S\rangle.$$

Decoding : Alice performs an optimal POVM to deduce m.

The total number of qubits that are communicated during the MRAC protocol is linear in $n \cdot L_1$ (remember n is the number of players).

To understand what is the optimal POVM for Alice, and what is the corresponding success probability, we first have to examine the states ρ_m more closely, which is what we do in the following.

It is straightforward to see that the modified RAC protocol is symmetric. It is also $O(k^{\frac{3}{2}}(L_1 + L_2)2^{-\frac{L_2}{2}})$-private, just like the RAC protocol. The proof of this fact follows the same ideas as the proof of privacy of the RAC protocol, and so we don't repeat it here.

We are now left with analyzing the amount of correctness that the protocol can provide.

Denote $\sigma_s = |\psi_s\rangle\langle\psi_s|$, then ρ_m can also be written as

$$\rho_m = \frac{1}{2^{L_1}} \cdot \sum_{s \in \{0,1\}^{L_1}} |s\rangle\langle s| \otimes \sigma_{s \oplus m}, \tag{1.2}$$

which is a block diagonal matrix, with the matrices $\sigma_{s\oplus m}$ (for all values of s) being the blocks on the diagonal.

Note that $\sqrt{\rho_m} = 2^{L_1/2}\rho_m$, and also note that for every two distinct s, s'

$$|\langle\psi_s \,|\, \psi_{s'}\rangle| = \frac{\begin{pmatrix} 2^{L_1} - 2 \\ 2^{L_2} - 2 \end{pmatrix}}{\begin{pmatrix} 2^{L_1} - 1 \\ 2^{L_2} - 1 \end{pmatrix}} = \frac{2^{L_2} - 1}{2^{L_1} - 1}. \tag{1.3}$$

Using this, and using Fact 1.1, we see that for any two distinct m, m'

$$\begin{aligned} F(\rho_m, \rho_{m'}) = & & (1.4)\\ = & \left[\mathrm{Tr}\sqrt{\rho_m^{\frac{1}{2}}\rho_{m'}\rho_m^{\frac{1}{2}}}\right]^2 & (1.5)\\ = & \| \sqrt{\rho_m}\sqrt{\rho_{m'}} \|_{\mathrm{tr}}^2 & (1.6)\\ = & 2^{2L_1} \| \rho_m\rho_{m'} \|_{\mathrm{tr}}^2 & (1.7)\\ = & \left(\frac{2^{L_2} - 1}{2^{L_1} - 1}\right)^2 & (1.8) \end{aligned}$$

The last equality (1.8) is directly from the definition of ρ_m according to (1.2), and from (1.3).

From Fact 1.2 we get

$$\frac{1}{2} \| \rho_m - \rho_{m'} \|_{\mathrm{tr}} \geq 1 - \frac{2^{L_2} - 1}{2^{L_1} - 1} \geq 1 - 2^{L_2 - L_1}. \tag{1.9}$$

Alice may choose a measurement to distinguish between the case where the message is m and the case where it is m'. Let D_m and $D_{m'}$ be the probability distributions over measurement results in the case of m being the message, and in the case of m', respectively. Assume that the optimal measurement has been chosen by Alice, i.e. the one which maximizes her success probability. Then Lemma 1.5 relates the trace distance between ρ_m and $\rho_{m'}$ to the l_1 norm of $D_m - D_{m'}$,

$$\| \rho_m - \rho_{m'} \|_{\mathrm{tr}} = |D_m - D_{m'}|_1 .$$

From Fact 1.6 we conclude that Alice can distinguish the two cases with success probability $\frac{1}{2} + \frac{1}{4} |D_m - D_{m'}|_1$. Inequality 1.9 says that this means

$$Probability(success) \geq 1 - 2^{L_2 - L_1 - 1}.$$

The case where the size of the message space is $|M| = 2$, i.e there are only two ρ_m's, for $m = 0, 1$, is of course not very interesting. What we would really like to have is message length as close as possible to L_1 - the length of the public key. In other words, we would like to analyze the case where the number of ρ_m's is as close as possible to 2^{L_1}. However it is an open question to lower bound Alice's success probability with larger message sets. This can be stated as a general open question, relating the size of a set of density matrices, and the fidelity between pairs of states from the set, to the level of distinguishability of the states in the set:

- Given a set of n quantum states, with pairwise fidelity F (where F is very small), how well can we distinguish the states via quantum measurement?

Going back to our special case it is in particular not clear how large can the set of messages be such that Alice's success probability in decoding a message correctly is still exponentially (or even polynomially) close to 1. So at this point we can only safely use the MRAC protocol to encrypt a one bit message using L_1 bits key. If we wish to send longer messages, we can just use the MRAC protocol repeatedly for each bit of our message. The number of key bits that we consume this way would be L_1 bits of a key per one bit of a message. Doing so would of course miss the whole point of the use of the MRAC protocol, which was in the first place to save key bits. However we strongly believe, without being able to prove it, that the MRAC protocol can be safely used with much a better ratio between key length and message length (perhaps even arbitrarily close to 1 from above). The reason why we believe so is that, as we showed, the fidelity of any pair of ρ_m and $\rho_{m'}$, for any $m \neq m'$, is very small, which should mean that given any one ρ_m, it should be

possible to distinguish it from all the other $\rho_{m'}$, and thus to infer m. Note that one cannot hope to have ratio exactly 1 or less, because the fidelities are in general not zero, i.e. the states are not completely orthogonal. If it is possible to have a quantum public key scheme with key to message length rate equal to one, it must be a different protocol than the ones presented so far in the thesis (RAC and MRAC protocol), and also from the next one to be presented (the OBR protocol). So the point of finding a protocol with key length to message length ratio exactly one (or less...), or maybe, on the other hand proving this to be impossible, is yet another interesting question that remains open.

The oblivious rotations protocol (OBR protocol)

We now present a protocol communicating one-bit messages $m \in \mathcal{M} = \{0,1\}$. While the protocol uses only single qubit operations, which makes it very simple, it is quantum in both the key distribution phase and the encryption phase.

THE OBLIVIOUS ROTATIONS (OBR) PROTOCOL

key distribution : Alice chooses L random vectors $|\phi_1\rangle, \ldots, |\phi_L\rangle$, each uniformly selected from the four vectors $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ (where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$). A copy of the state $|\psi\rangle = |\phi_1\rangle \otimes \ldots \otimes |\phi_L\rangle$ is handed to each of the other players.

Encoding : Given a message $m \in \{0,1\}$, the active player P_i chooses $t_1, \ldots, t_L \in \{0,1\}$ such that their parity is m, $\sum t_i (\text{mod} 2) = m$. P_i then applies $Y^{t_1} \otimes \ldots \otimes Y^{t_L}$ on $|\psi\rangle$ and sends the result to Alice, where $Y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $Y^0 = I$ and $Y^1 = Y$.

Decoding : For every $i \in [L]$ Alice looks at $|\phi_i\rangle$. If $|\phi_i\rangle \in \{|0\rangle, |1\rangle\}$ she measures in the $\{|0\rangle, |1\rangle\}$ basis, otherwise she measures in the $\{|+\rangle, |-\rangle\}$ basis. If the result is $|\phi_i\rangle$ she concludes $t_i = 0$ and otherwise $t_i = 1$. Finally, she sets $m = \sum t_i (\text{mod} 2)$.

The total number of qubits that are communicated during the OBR protocol is linear in $n \cdot L$ (remember n is the number of players).

Theorem 1.16. *The OBR protocol is correct, symmetric and has $\beta = kLe^{-\Omega(L/2^k)}$ privacy against coalitions of size $k < n$.*

Proof. Notice that the operator Y when acting on the states $|0\rangle, |1\rangle$ performs a bit flip, i.e. turns $|0\rangle$ to $|1\rangle$ and vice-versa. It also has the same flipping effect when acting on the states $|+\rangle$ and $|-\rangle$. It follows that for every i Alice's decoding procedure correctly determines t_i, and, in particular, Alice always correctly determines m, thus the OBR protocol is correct. Like in the case of the RAC protocol discussed earlier, the symmetry of the key and of the encryption procedures applied by the players implies that the OBR protocol is also symmetric.

Let $\rho_m^{k,L}$ denote the reduced density matrix of the register BE (as usual, BE is the joint register B of the bad players (their number is k), together with the register E of the ciphertext), when the active player encodes the message $m \in \{0,1\}$. We demonstrate the privacy of the protocol by first showing that:

Lemma 1.17.

$$\left\| \rho_0^{k,L} - \rho_1^{k,L} \right\|_{\text{tr}} \leq (1/2)^{(L-1)} \left\| \rho_0^{k,1} - \rho_1^{k,1} \right\|_{\text{tr}}^L \tag{1.10}$$

$$\left\| \rho_0^{k,1} - \rho_1^{k,1} \right\|_{\text{tr}} = 1 + \sqrt{1 - (1/2)^{k-1}} \tag{1.11}$$

The two items of Lemma 1.17 give together:

Corollary 1.18. $\left\| \rho_0^{k,L} - \rho_1^{k,L} \right\|_{\text{tr}} \leq 2 \left(\frac{1+\sqrt{1-(1/2)^{k-1}}}{2} \right)^L < 2e^{-\left(\frac{1}{2}\right)^{k+1} L}$,

where the last inequality in the corollary is derived by taking the Taylor expansion of the left-hand side expression.

Proof. (Of Lemma 1.17, first item) We prove by induction. The base case $L = 1$ is immediate. For a lager L we express the two density matrices $\rho_0^{k,L}$ and $\rho_1^{k,L}$ as:

$$\begin{aligned} \rho_0^{k,L} &= \frac{1}{2}\rho_0^{k,1} \otimes \rho_0^{k,L-1} + \frac{1}{2}\rho_1^{k,1} \otimes \rho_1^{k,L-1} \\ \rho_1^{k,L} &= \frac{1}{2}\rho_0^{k,1} \otimes \rho_1^{k,L-1} + \frac{1}{2}\rho_1^{k,1} \otimes \rho_0^{k,L-1}. \end{aligned}$$

The trace distance is:

$$\begin{aligned} \left\| \rho_0^{k,L} - \rho_1^{k,L} \right\|_{\text{tr}} &= \frac{1}{2} \left\| (\rho_0^{k,1} - \rho_1^{k,1}) \otimes (\rho_0^{k,L-1} - \rho_1^{k,L-1}) \right\|_{\text{tr}} \\ &= \frac{1}{2} \left\| \rho_0^{k,1} - \rho_1^{k,1} \right\|_{\text{tr}} \cdot \left\| \rho_0^{k,L-1} - \rho_1^{k,L-1} \right\|_{\text{tr}} \end{aligned}$$

where in the last equality we used the fact that for any two matrices A, B $\| A \otimes B \|_{\mathrm{tr}} = \| A \|_{\mathrm{tr}} \| B \|_{\mathrm{tr}}$. Now, by the induction hypothesis we have that

$$\left\| \rho_0^{k,L-1} - \rho_1^{k,L-1} \right\|_{\mathrm{tr}} = \left(\frac{1}{2}\right)^{(L-2)} \left\| \rho_0^{k,1} - \rho_1^{k,1} \right\|_{\mathrm{tr}}^{L-1}$$

and the lemma follows. □

Proof. (Of Lemma 1.17, second item) Let us first describe the density matrix $\rho_0^{k,1}$. We have $k+1$ qubits, the first k qubits belong to the coalition of k bad players, and the last qubit is the one communicated by P_i. With probability 1/4 Alice sends $|0\rangle$ to all players, with probability 1/4 she sends $|1\rangle$, $|+\rangle$ or $|-\rangle$ to all players. Also, in $\rho_0^{k,1}$ we have $b = 0$ and so P_i applies identity on his qubit and then sends it. The situation for $\rho_1^{k,1}$ is similar except that $b = 1$ and P_i applies Y on his qubit. Thus, if we denote $|\overline{0}\rangle = |0..00\rangle$, $|\overline{0}'\rangle = (I \otimes \ldots \otimes I \otimes Y)|\overline{0}\rangle = |0..01\rangle$ and similarly for $|\overline{1}\rangle$,$|\overline{1}'\rangle$,$|\overline{+}\rangle$,$|\overline{+}'\rangle$,$|\overline{-}\rangle$,$|\overline{-}'\rangle$, then

$$\begin{aligned} \rho_0^{k,1} &= \frac{1}{4}[\ |\overline{0}\rangle\langle\overline{0}| + |\overline{1}\rangle\langle\overline{1}| + |\overline{+}\rangle\langle\overline{+}| + |\overline{-}\rangle\langle\overline{-}|\ ] \\ \rho_1^{k,1} &= \frac{1}{4}[\ |\overline{0}'\rangle\langle\overline{0}'| + |\overline{1}'\rangle\langle\overline{1}'| + |\overline{+}'\rangle\langle\overline{+}'| + |\overline{-}'\rangle\langle\overline{-}'|\ ] \end{aligned}$$

and the matrix $\rho_0^{k,1} - \rho_1^{k,1}$ is a 2^{k+1} by 2^{k+1} matrix of rank 8, being non-zero only on the subspace spanned by $\left\{\overline{0}, \overline{0}', \overline{1}, \overline{1}', \overline{+}, \overline{+}', \overline{-}, \overline{-}'\right\}$. Thus, computing the eigenvectors and eigenvalues can be done on the 8×8 matrix. When k is even the eight eigenvalues turn out to be $\alpha, -\alpha, \beta, -\beta, \gamma, \gamma, -\gamma, -\gamma$ where $\alpha = \frac{1}{4}(1 + (1/2)^{\frac{k-1}{2}})$, $\beta = \frac{1}{4}(1 - (1/2)^{\frac{k-1}{2}})$ and $\gamma = \frac{1}{4}\sqrt{1 - (1/2)^{k-1}}$. Summing up the absolute values of these eigenvalues yields the desired trace-distance. If the size of the bad coalition is odd, we allow it to be larger by 1, thus having k even, while only increasing the power of the bad players. □

Let us now denote, for short, $\rho_0 = \rho_0^{k,L}$ and $\rho_1 = \rho_1^{k,L}$. Remember that the mutual information between two quantum states is always non-negative. We have

$$
\begin{aligned}
I(BE:M) &= S(BE) - S(BE|M) \\
&= |S(p_0 \cdot \rho_0 \ + \ p_1 \cdot \rho_1) - p_0 \cdot S(\rho_0) - p_1 \cdot S(\rho_1)| \\
&= |p_0[S(p_0\rho_0 + p_1\rho_1) - S(\rho_0)] + p_1[S(p_0\rho_0 + p_1\rho_1) - S(\rho_1)]| \\
&\leq p_0 \, |S(p_0\rho_0 + p_1\rho_1) - S(\rho_0)| + p_1 \, |S(p_0\rho_0 + p_1\rho_1) - S(\rho_1)| \, .
\end{aligned}
$$

We now notice that

$$
\| \, (p_0\rho_0 + p_1\rho_1) - \rho_0 \, \|_{\mathrm{tr}} \ = \ p_1 \, \| \, \rho_1 - \rho_0 \, \|_{\mathrm{tr}}
$$

and similarly

$$
\| \, (p_0\rho_0 + p_1\rho_1) - \rho_1 \, \|_{\mathrm{tr}} \ = \ p_0 \, \| \, \rho_0 - \rho_1 \, \|_{\mathrm{tr}} \, .
$$

However, we saw that (Corollary (1.18)),

$$
\| \, \rho_0 - \rho_1 \, \|_{\mathrm{tr}} \ \leq \ \delta = e^{-\Omega(L/2^k)}
$$

and by Fannes' inequality (see Lemma 1.9) it follows that

$$
\begin{aligned}
& p_0 \, |S(p_0\rho_0 + p_1\rho_1) - S(\rho_0)| \\
& \quad \leq \ p_0 p_1 \delta [kL + \log \frac{1}{p_1 \delta}] \\
& \quad \leq \ \frac{1}{2} kL e^{-\Omega(L/2^k)} .
\end{aligned}
$$

Similarly

$$
\begin{aligned}
& p_1 \, |S(p_0\rho_0 + p_1\rho_1) - S(\rho_1)| \\
& \quad \leq \ p_1 p_0 \delta [kL + \log \frac{1}{p_0 \delta}] \\
& \quad \leq \ \frac{1}{2} kL e^{-\Omega(L/2^k)} .
\end{aligned}
$$

and together we have $I(BE:M) \leq kLe^{-\Omega(L/2^k)}$, which completes the proof.

□

1.4 Dishonest key distribution

A dishonest Alice might try to cheat by not sending the same key to all the players. Doing so, upon receiving a message from some player, it might be possible for her to identify the sender. For example, if in the RAC protocol Alice sends each player a different single pair $(\ell, s(\ell))$, instead of the superposition of pairs she is supposed to send, then she can identify the sender from ℓ. This simple example of an attack does not even use Alice's ability to keep entanglement with the messages she sends.

Other players can also behave in a dishonest manner during key distribution, by eavesdropping on the communications from Alice, and making quantum interactions with each other's key on transfer from Alice to their destinations. For example, if in the RAC protocol player P_j measures P_i's key, he can infer the pair $(\ell, s(\ell))$ that P_i will use to send a message, and therefore easily decipher P_i's message.

We describe a reduction from general protocols to protocols with honest key distribution (done as described in Section 1.3). The reduction introduces a testing phase which is general, i.e. does not depend on the specific protocol used, as long as this protocol is correct, private and symmetric when its preprocessing phase is honest.

We call the pure state description of the whole system, that results from performing honest key distribution, an *honest* state. In the modified protocols Alice creates many independent copies of the game, the players test part of these copies to see that they are indeed in honest states. Suppose the test passes with success, then when P_i wants to send a message to Alice he picks a random single copy from the remaining (untested) ones and uses it to encode his message. In addition to the encoded message he also indicates which copy was used.

1.4.1 A basic test

Suppose we have a protocol which is symmetric and β-private against coalitions of size k, in the honest key distribution scenario as defined in Section 1.3. In such a protocol, Alice is supposed to produce a product state $|v\rangle = |\phi\rangle_{P_1} \otimes \ldots |\phi\rangle_{P_n}$ for some pure state $|\phi\rangle$. Assume $|\phi\rangle$ comes from a 2^d dimensional Hilbert space.

We examine the following test:

A Basic Test

- Alice sends a description of a vector $|\phi\rangle$.
- All players project their qubits on $|\phi\rangle$ and the subspace orthogonal to $|\phi\rangle$. Each of them announces his outcome, and they accept iff all players get $|\phi\rangle$.

Suppose the set of honest players is $P_1, \ldots, P_h$, and let $\rho_{P_1,\ldots,P_h}$ be the reduced density matrix of their subsystem. Suppose that the pure state $|\psi\rangle$, which describes the state of the complete system immediately after the key distribution phase, has the form $|\psi\rangle = \sum |w\rangle_{rest} \otimes |v_w\rangle_{P_1,\ldots,P_h} \otimes |c_w\rangle_{channel}$, with the states $|w\rangle$ being mutually orthogonal states describing the rest of the system, the states $|v_w\rangle$ are of the form $|v_w\rangle = |\phi_w\rangle^{\otimes h}$ for some $|\phi_w\rangle$, and c_w is a classical description provided by Alice to the state $|\phi_w\rangle$. Then we say that the system is in a *correct* state, and we also say that the reduced density matrix $\rho_{P_1,\ldots,P_h}$, describing the subspace of the honest players, is a *correct* density matrix.

Clearly if the system is in a correct state then the basic test passes with certainty. We show that if the test passes with good probability then the state of the system must be close to a correct state.

Two density matrices ρ_1, ρ_2 are said to be δ-close to each other if they have fidelity greater than $1-\delta$, i.e., $|F(\rho_1, \rho_2)| \geq 1 - \delta$.

Lemma 1.19. *If* $\Pr(\textit{test fails}) \leq \alpha$ *then there exists a* correct *state* $|\tilde{\psi}\rangle$ *that is* $3\sqrt{\alpha}$*-close to the state* $|\psi\rangle$ *of the system.*

Proof. Let Alice be arbitrary and $|\psi\rangle$ be the pure state describing the complete system. Alice is supposed to send a classical description of a pure-state $|\phi\rangle$. Let us say that the description Alice sends is obtained by doing some POVM $\{M_{w'}\}$ with result w' on her register. The result w' corresponds to a projection $P_{w'}$ onto a subspace $H_{w'}$ of Alice's system. Let the states $|w\rangle$ form a complete orthonormal basis to the space of Alice's system, such that each $H_{w'}$ is spanned by a (distinct) subset of the set of states $\{|w\rangle\}$. In the basis $\{|w\rangle\}$ we can represent $|\psi\rangle$ as:

$$|\psi\rangle \quad = \quad \sum \alpha_w |w\rangle |v_w\rangle |c_w\rangle$$

We say an index w is ϵ*-good* if c_w describes a state $|\widetilde{v}_w\rangle$ such that $|\langle v_w | \widetilde{v}_w\rangle| > 1 - \epsilon$, we say w

is *bad* otherwise (ϵ is to be fixed later).

We express $|\psi\rangle$ as

$$|\psi\rangle \;=\; \sum_{\text{good } w} \alpha_w |w\rangle|v_w\rangle|c_w\rangle + \sum_{\text{bad } w} \alpha_w |w\rangle|v_w\rangle|c_w\rangle$$

For every bad w the players pass the test with probability $|\langle v_w \,|\, \widetilde{v}_w\rangle|^2 \leq (1-\epsilon)^2 \leq 1-\epsilon$. Thus, $\Pr(\text{test fails}) \geq p_{bad}\epsilon$, where $p_{bad} = \sum_{\text{bad } w} |\alpha_w|^2$. We conclude that $p_{bad} \leq \frac{\alpha}{\epsilon}$. Choosing $\epsilon = \sqrt{\alpha}$, we have $p_{bad} \leq \sqrt{\alpha}$.

Also, for every good w, there exists a vector $\widetilde{v_w}$ such that $|\langle v_w \,|\, \widetilde{v}_w\rangle| > 1-\epsilon$. We let

$$|\widetilde{\psi}\rangle \;=\; \frac{1}{\sqrt{p_{good}}} \cdot \sum_{\text{good } w} \alpha_w |w\rangle|\widetilde{v}_w\rangle|c_w\rangle$$

where $p_{good} = 1 - p_{bad}$. By definition, $|\widetilde{\psi}\rangle$ is correct. Also, let $\rho = |\psi\rangle\langle\psi|$ and $\widetilde{\rho} = |\widetilde{\psi}\rangle\langle\widetilde{\psi}|$ then

$$\begin{aligned} F(\widetilde{\rho}, \rho) &= |\langle \psi \,|\, \widetilde{\psi}\rangle|^2 \\ &\geq (1-\epsilon)^2 p_{good} \geq (1-\epsilon)^2(1-\sqrt{\alpha}) \\ &\geq (1-2\epsilon)(1-\sqrt{\alpha}) \;\geq\; 1 - 3\sqrt{\alpha} \end{aligned}$$

□

1.4.2 Reduction to the honest case

We first describe the new protocol. A honest Alice is supposed to send T independent copies of a basic game, i.e., to distribute vectors $|\psi^{(1)}\rangle, \ldots, |\psi^{(T)}\rangle$ among the n players $P_1, \ldots, P_n$, such that each $|\psi^{(i)}\rangle$ is a product of n copies of some vector. Let 2^d be the dimension of the whole system (including the registers that hold the classical values $i \in \mathcal{I}$ and $m \in \mathcal{M}$).

After Alice distributed the states each player independently chooses a random subset of size t_0 of the copies to be tested. If all the tests (of all players) pass with success, the active player chooses a copy among the remaining (untested) ones and uses it to run the original protocol.

THE MODIFIED PROTOCOL

Distributing keys : Alice distributes T vectors $|\psi^{(1)}\rangle, \ldots, |\psi^{(T)}\rangle$ among the n players $P_1, \ldots, P_n$ such that each P_i gets a copy of each of the $\psi^{(j)}$s.

Testing some of the keys : Each player P_i independently chooses a random subset $S_0 \subseteq [T]$ of size $t_0 = T^{\frac{3}{4}}$ of these systems. For each j that was chosen by some player the players run the basic test of the previous subsection. If any of the tests fails they abort the protocol.

Running the original protocol : The active player P_i chooses a random index j of the remaining untested systems. The protocol is then executed using the j'th system (P_i appends j to the beginning of the encoded message e, so that Alice knows which copy is used as the key and thus she knows how to decode the message).

We now upper bound the symmetry and privacy of the modified protocol in the dishonest key distribution scenario (the amount of correctness of the protocol is irrelevant in this context):

Theorem 1.20. *Suppose we have a protocol which is correct, symmetric and also β-private against coalitions of size k, in the honest key distribution scenario as defined in Section 1.3. Then the modified protocol is correct, $O(d \cdot T^{-\frac{1}{32}})$- symmetric, and also $(\beta + O(d \cdot T^{-\frac{1}{32}}))$-private against coalitions of size k.*

Proof. Let P be *any* honest player. We fix $\epsilon = T^{-1/16}$. We denote by ρ_0 the (pure) state of the whole system after the distribution stage of the protocol. We say i is *good* for ρ_0 if $\rho_0^{(i)} \equiv (\rho_0)_{P_{1,i},\ldots,P_{n,i}}$ is ϵ–close to some correct density matrix $\widetilde{\rho}_0^{(i)}$, and *bad* otherwise. We let

$$BAD_0 = \{1 \leq i \leq T \mid i \text{ is bad for } \rho_0\}.$$

Similarly, ρ_t denote the density matrix of the whole system given that the first $t-1$ tests of P passed with success, i.e. conditioned on the previous $t-1$ measurements. We say i is *good* for ρ_t if $\rho_t^{(i)} \equiv (\rho_t)_{P_{1,i},\ldots,P_{n,i}}$ (the reduced state of the ith out of T copies) is ϵ–close to some correct density matrix $\widetilde{\rho}_t^{(i)}$, and *bad* otherwise and we let $BAD_t = \{1 \leq i \leq T \mid i \text{ is bad for } \rho_t\}$.

The honest player P does t_0 tests. Let G be the event that for some t, $|BAD_t| \leq \sqrt{T}$. Remember

that M, A, B, E stand for the quantum registers that hold the message m, Alice's information, the joint information of the collusion of bad players and the ciphertext, e, respectively. We prove:

Claim 1.21. *Let R be the random variable holding the value i (the identity of the active player). We also use R to denote the quantum register where the value i is stored.*

- $I(AE : R|\neg G) \leq de^{-\Omega(\frac{\epsilon^2 t_0}{\sqrt{T}})}$ *and* $I(BE : M|\neg G) \leq de^{-\Omega(\frac{\epsilon^2 t_0}{\sqrt{T}})}$.
- $I(AE : R|G) \leq O(d\sqrt{\epsilon})$ *and* $I(BE : M|G) \leq \beta + O(d\sqrt{\epsilon})$

which together completes the proof. □

We now prove the claim:

Proof. (Of Claim 1.21, first item)

When the event G does not happen, then for every t there is probability at least $\frac{\sqrt{T}}{T}$ that P picks a bad index to test, and then by Lemma 1.19 there is probability at least $\epsilon^2/9$ that he rejects, and altogether $\Pr(t\text{'th test rejects} \mid \neg G, \text{first } t-1 \text{ tests accepted}) \geq \frac{\epsilon^2}{9\sqrt{T}}$. Thus,

$$\begin{aligned}\Pr(\text{Test accepts} \mid \neg G) &\leq \prod_{t=0}^{t_0} \Pr(t\text{'th test accepts} \mid \neg G, \text{first } t-1 \text{ tests accepted}) \\ &\leq (1 - \frac{\epsilon^2}{9\sqrt{T}})^{t_0} \leq e^{-\Omega(\frac{\epsilon^2 t_0}{\sqrt{T}})}\end{aligned}$$

and therefore

$$\begin{aligned}I(AE : R|\neg G) = & \quad (1.12)\\ = \; & I(AE : R|\text{Test accepts}, \neg G) \cdot \Pr(\text{Test accepts} \mid \neg G) \quad (1.13)\\ + \; & I(AE : R|\text{Test rejects}, \neg G) \cdot \Pr(\text{Test rejects} \mid \neg G) \quad (1.14)\\ \leq \; & d \cdot \Pr(\text{Test accepts} \mid \neg G) + 0 \cdot \Pr(\text{Test rejects} \mid \neg G) \quad (1.15)\\ \leq \; & de^{-\Omega(\frac{\epsilon^2 t_0}{\sqrt{T}})}. \quad (1.16)\end{aligned}$$

In the same way it is also true that $I(BE : M|\neg G) \leq de^{-\Omega(\frac{\epsilon^2 t_0}{\sqrt{T}})}$.

□

Proof. (Of Claim 1.21, second item)

When G does happen, for some t $|BAD_t| \leq \sqrt{T}$. We focus on the jth system that P chooses to play with, and we ignore all the additional $t, \ldots, t_0$ tests P does (by looking at the values of the other tests, and quitting the protocol if one of them fails, P can only reduce the amount of information that might leak to either Alice or the other players). Now, since $|BAD_t| \leq \sqrt{T}$ then except for with probability $\frac{\sqrt{T}}{T-nt_0} \leq \frac{\sqrt{T}}{T/2} = \frac{2}{\sqrt{T}}$ the index j is good (where we choose $T \geq 2nt_0$).

When G does happen and j is good the state of the actual copy that the players play with is ϵ-close to a correct density matrix $\widetilde{\rho}^{(j)}$. Using the concavity of the function $\sqrt{F}$ we conclude that when G happens the state $\rho^{(j)}$ has high fidelity with the correct state $\widetilde{\rho}^{(j)}$:

$$F(\widetilde{\rho}^{(j)}, \rho^{(j)}) \;\; \geq \;\; (1 - \frac{2}{\sqrt{T}})^2 \cdot (1 - \epsilon) \;\; \geq \;\; 1 - (\epsilon + O(\frac{1}{\sqrt{T}})) \;\; \geq \;\; 1 - O(\epsilon).$$

Let us first examine the simpler (and ideal) case when the state of the system is a correct state. We have $I(AE : R) = 0$ even if Alice is dishonest, as the keys resulting from a correct state are identical to all the players. If, on the other hand, Alice is honest, but some other players are not, then the correct state of the system differs from the one that would have resulted from a truly honest behavior of all the players by only a local operation on registers held by the dishonest players. Since local operations cannot increase the dishonest players' information we still have $I(BE : M) \leq \beta$, just as in the honest scenario.

Now, for the general (non ideal) case, we apply Claim 1.10 to conclude that $I(AE : R) \leq 0 \; + \; O(d \cdot \sqrt{\epsilon})$ and $I(BE : M) \leq \beta \; + \; O(d \cdot \sqrt{\epsilon})$. $\square$

Chapter 2

Network anonymity

2.1 Background

An anonymous network with n players $P_1, \ldots, P_n$ is one that allows every player to send messages to any other player with privacy and with unlinkability, which means that an unauthorized entity is unable to either read messages nor to tell the matching of a sender-to-receiver of a message. The players $P_1, \ldots, P_n$ are synchronized with a common clock. All messages that are transmitted in the network during one clock-cycle are referred to as being sent during the same *round* of the protocol. A protocol would be considered a good solution to the problem of constructing an anonymous network if in addition to good privacy and unlinkability parameters it also works efficiently, which is mainly measured in two aspects - the number of communication rounds, and the total channel uses, required for the delivery of a single message. The solution to this problem crucially depends on the attack model of the adversary, which is an entity to whom all "illegal" activity, such as eavesdropping, deleting messages, sending false messages, etc., is attributed. It is traditional to distinguish between three types of possible adversaries, according to the severity of their actions:

- Passive adversaries, that follow the specified protocol but collect information (such an adversary is sometimes also called 'curious but honest'),

- Active adversaries that may initiate messages not according to the protocol, but do not change (or delete) messages they are asked to deliver, and,

- Malicious adversaries that may modify or delete messages.

An adversary may control both users and communication links in the network. A user under adversary control (a dishonest user) performs according to the strategy of the adversary, whereas a honest user performs according to the protocol. A link under adversary control is available for adversary inspection (eavesdropping), unlike a link which is not under adversary control.

The problem of network anonymity can be solved in the framework of secure multiparty computation (SMPC), as explained in Part I. In this framework there is a solution both in the case of a computationally bounded adversary, as well as in the case of an unbounded adversary. In both cases the solution is limited to deal with an adversary who controls at most a fraction of $\frac{1}{2}$ of the users in the network, and in both cases the solution takes a constant number of rounds (per message), and polynomial communication complexity (see Part I). There are many works suggesting protocols for the problem, which are designed to address the problem of network anonymity directly, without using SMPC. The motivation to do this is to try and find better solutions, in terms of the number of dishonest players as well as in terms of efficiency, as explained in Part I. Many of these suggested protocols are based on the seminal work of Chaum [28]. But there are only few of these works that come with rigorous model definitions and analysis of their suggested protocols ([54, 17], for instance). Most of these works, with maybe only few exceptions, are in the computational rather than information theoretic model. This means that the adversary is assumed to have only polynomial computation power. Actually the only exception I am aware of is the solution suggested by Yuval Ishai [39], which to my best knowledge this thesis is the only place where it is presented (see Section 2.4). Ishai's solution, as explained in Section 2.4, is far less efficient than the computational solutions in terms of communication complexity. The idea behind this solution is a simple variation on the *DC-network* idea of Chaum [29], and is described in Section 2.4. The original work of Chaum [29], which deals with information theoretic network anonymity, refer to a rather simplified model, in which only unlinkability matters, while privacy is of no concern. Needless to say, this kind of model is far less interesting, because of limited potential uses.

The central idea in the computational solution of Chaum [28], which is also the basis to most of the later works (but not in the protocol of [39]), is the idea of the *mix*. A mix is a subgraph of the network (usually one vertex, as in the original work [28]). The simple idea behind the mix is that different messages that arrive at a mix in a given round (i.e. simultaneously) of a protocol would leave the mix to their next destination in random order. This way, an adversary who is trying to follow some message of his interest to learn its destination, and who is confined to doing only traffic analysis (i.e. without being able to compare the *contents* of different messages), loses track of the

message after it passes through only a few number of mixes in a random path of the network graph. It turns out that a polylogarithmic number of mixes is enough for this purpose. This fact can be proved using classical results about mixing in random processes, using coupling and Markov chain arguments. More detailed discussion can be found in [54, 17].

Preventing the adversary from comparing the *contents* of messages, and thus overcoming the mixes, is easy - you just make sure that an incoming encrypted message that enters a mix, and the corresponding outgoing one, would look uncorrelated in the eyes of the adversary. This is achieved with the cooperation of the mix itself, which alters the encryption of the messages in a predefined way. The newly encrypted (outgoing) message, after the processing of the mix, looks completely random compared to the old (incoming) one. This was originally done in [28] with the use of RSA public key cryptosystem, and similarly in all the works that followed it. Assuming that a constant fraction of the nodes in the network are honest users, although it can be in principle a very small fraction, with high probability a polylogarithmic length random path would contain a polylogarithmic number of honest mixes, i.e. mixes that would operate properly according to the protocol. The fact that a message has to travel through a random path of polylogarithmic length from source to destination implies that the number of communication rounds per message delivery is polylogarithmic in the size of the network. A protocol with this number of rounds is considered an efficient solution in terms of *round complexity*.

The use of RSA has another added value other than making the message going out-from and into a mix look uncorrelated to the adversary. This added value is that the adversary cannot read any of the encrypted messages (unless he himself is the intended recipient of a message). This way the two security aspects of network anonymity, namely privacy and unlinkability, are covered.

In this thesis we too build the solution to the network anonymity problem around the idea of *mixing*, but contrary to most other works in this area, our solution is in the information theoretic model, and uses quantum rather than classical communication. In mix-based solutions (either with quantum or classical communication) players choose a random path for delivering their message. The *symmetry* property (Definition 0.1) of public-key schemes, and the privacy property, are used to reduce the problem of network anonymity to the traffic analysis simpler problem (see the discussion in Part I). The traffic analysis problem is in turn solved using classical results about mixing. So far the works that used the idea of mixing usually studied the active adversary model, whereas the malicious adversary model, which allows deleting messages, requires different additional techniques and is less understood (see [54], Section 3.4). Here we also focus on the active adversary model, and leave the malicious adversary model for additional future research.

In the computationally-bounded active-adversary model a secure solution with polylogarithmic long paths is possible, even if the adversary controls all edges and most of the vertices (see [54] for exact details). This solution, however, requires linear number of players to participate in the protocol at all times, even if they only rarely want to send a message themselves. If we relax the model, and only assume the adversary controls a (possibly very large) fraction of the edges, then players need to participate at the game about the same times as the number of times they want to send a message themselves (see [17] for details).

What we want to demonstrate here is that our quantum symmetric protocols from Chapter 1 can be used as a black box, to reduce the anonymous network problem to the traffic analysis problem (which we already know to solve classically), but now in an unconditional information theoretic setting. Again, the structure of this kind of solution is exactly the same as the classical solutions following the ideas of [28], i.e. a mix-based solution (unlike the classical information theoretic solution of [39]). The main difference of this solution from the classical solution of [39] is in the efficiency parameters (round complexity and communication complexity). The calculation of the efficiency of the resulting quantum solution, both in terms of round complexity and of communication complexity, can be borrowed directly from the known classical mix-based (computational) results [54, 17]. This is true in both the model where the adversary controls all edges or only a fraction of them, however, for concreteness, and because the solution in the latter case is somewhat simpler, we focus on the latter case. We now give some more details about the model we use, and about the way the classical computational mix-based solution works.

2.1.1 The model

The anonymous network consists of n users connected to each other with a communication link, and it is supposed to support sending messages of constant length L_0, from any one user to any other user. For the current discussion we adopt the definitions from [17], i.e. the adversary controlls a (possibly large) fraction of the users, and of the communication links in the network. The users under adversary control may deviate from the protocol by initiating messages not according to the protocol (i.e. active adversary). The requirements from a protocol are correctness, privacy and unlinkability - all in the information theoretic sense.

- Correctness means that a message initiated by player i and aimed for player j can successfully be read by the intended recipient, player j.
- Privacy means that a message initiated by player i and aimed for player j cannot be read

by any player other than i or j, except with probability polynomially small in the number of users (players) n in the network.

- Unlinkability means that even though the identities of users sending messages, and users receiving messages, at any given time, may be known to the adversary, he may gain only a polynomially small (in n) amount of mutual information with the *matching* between senders and receivers. In other words, the adversary may know a list of senders, and a list of recipients, but he must not be able to tell which sender communicates with which recipient.

A formal definition and discussion on unlinkability, in the language of mutual information between the knowledge of the adversary and the true matching of senders and receivers of messages, can be found in [17]. Although the definitions there relate to the *computationally bounded* adversary, the extension to the information theoretic case is straightforward.

For a protocol to be considered *efficient* it is required that the number of rounds required per message delivery is $O(polylog(n))$. In addition, the total communication cost per single message delivery should be $O(polylog(n))$ in the case where the adversary controlls a *fraction* < 1 of the links in the network. If *all* the links are under adversary control then a linear, or close to linear, amount of communication per message is satisfying.

2.1.2 Structure of the mix-based classical computational solution

As mentioned above, mix-based solutions to the network anonymity problem use a logarithmic length random path to deliver a message from one user to another. Relying on the idea of information from crossing paths being "mixed" with each other whenever simultaneously reaching a honest user (namely a mix), the adversary's mutual information with the final matching of senders and receivers reduces rapidly to a negligible amount.

Assuming that the public key (usually with RSA being the underlying public key cryptosystem) of every player is known to all other players, this can be done as follows: To send a message to player P_j, the player P_i selects a random length k path in the network, with $k = O(Polylog(n))$. The random path includes k nodes (players) $P_{i,0}, P_{i,1}, \ldots, P_{i,k-1}$, with the two ends of the path being $P_i = P_{i,0}$ and $P_j = P_{i,k-1}$. Denote $E_l(m)$ the cyphertext obtained when encrypting the message m with the public key of player P_l. Player P_i applies a "cascade" of encryptions using the public keys of the players $P_{i,1}, P_{i,2}, \ldots, P_{i,k-1}$ in the random path, in reverse order. He first encodes the message m using the public key of player P_j. This step ensures that the only one that will be able to open the encryption and read m is P_j. The result $E_j(m)$ (which can also be written $E_{i,k-1}(m)$)

is appended with the information $(i, k-1)$, and the composite string $(i, k-1), E_{i,k-1}(m)$ is encoded with the key of player $P_{i,k-2}$, to obtain $E_{i,k-2}((i, k-1), E_{i,k-1}(m))$. If we give this encryption to player $P_{i,k-2}$ he can decrypt to get $(i, k-1), E_{i,k-1}(m)$, which tells him to relay $E_{i,k-1}(m)$ to $P_{i,k-1}$. This cascade of encryptions goes on with the keys of $P_{i,k-3}, P_{i,k-4}$ and so on, until $P_{i,1}$. The whole process of encryption results in the composite ciphertext

$$E = E_{i,1}((i, 2), E_{i,2}((i, 3), E_{i,3}(\ldots E_{i,k-2}((i, k-1), E_{i,k-1}(m))\ldots). \tag{2.1}$$

This composite ciphertext is sent from player $P_{i,0}$ to $P_{i,1}$, who decrypts (i.e. inverts $E_{i,1}$) to get

$$(i, 2), E_{i,2}((i, 3), E_{i,3}(\ldots E_{i,k-2}((i, k-1), E_{i,k-1}(m))\ldots).$$

In the next round player $P_{i,1}$ sends

$$E_{i,2}((i, 3), E_{i,3}(\ldots E_{i,k-2}((i, k-1), E_{i,k-1}(m))\ldots)$$

to player $P_{i,2}$, who decrypts to get

$$(i, 3), E_{i,3}(\ldots E_{i,k-2}((i, k-1), E_{i,k-1}(m))\ldots).$$

This process of gradual decryption goes on, until $P_{i,k-1}$ gets $E_{i,k-1}(m)$, which he can decrypt and get m. At each stage of this process a player "peels off" one layer of the cascade of encryptions. The only information that is revealed to an intermediate player $P_{i,l}$ is the identity of the next player in the random path (to whom he should relay the resulting ciphertext), and nothing else. The number of communication rounds needed until the message arrives at P_j is the same as the length of the random path, i.e. polylogarithmic in n. The total length of the ciphertext E from Equation (2.1) is also $O(polylog(n))$, which is the communication complexity per single message of the protocol, in the case where the adversary controlls only a fraction of communication links in the network. If the adversary controlls all the communication links then players have to send dummy messages when they don't have real messages to send (see [54, 17]), and in this case the communication complexity per message becomes $O(n \cdot polylog(n))$.

2.2 Information theoretic anonymous networks with quantum public keys

The method described in Section 2.1.2 gives privacy and unlinkability only with respect to a computationally bounded adversary, because of the underlying classical public key cryptosytem. The idea of our solution is to replace the use of classical public key cryptography with quantum public keys (while all the rest stays the same). For this purpose we choose to use one of our quantum information theoretic private and symmetric protocols from Section 1.3 - the RAC protocol.

In the RAC protocol each player distributes a quantum public key to each other player. The player who receives the quantum key measures it to obtain two random classical strings, which can also be thought of as a *private* key, s, that he shares with the player who sent him the quantum key, and a label, l, associated with that private key. The interesting property of that classical private key is that the sender does not know the result of the receiver's measurement, and thus cannot be certain about which classical string s he obtained. Nevertheless they can still communicate privately using the private key s. To achieve this, the ciphertext that corresponds to a message m is the pair $(l, E(m)) = (l, m \oplus s)$. With the help of the label l the recipient of this ciphertext can infer s and thus decrypt to get m.

Instead of using public keys from a classical public key cryptosystem, the cascade of encryptions described in Section 2.1.2 is formed with the private keys extracted from the quantum public keys of the RAC protocol. The composite ciphertext obtained from a message m, similar to Equation (2.1), is

$$E = s_{i,1} \oplus ((i,2), l_{i,2}, s_{i,2} \oplus ((i,3), l_{i,3}, s_{i,3} \oplus \ldots s_{i,k-2} \oplus ((i,k-1), l_{i,k-1}, s_{i,k-1} \oplus m)) \ldots). \quad (2.2)$$

Note that the only difference from Equation (2.1) is that the labels l are added, to allow the intermediate players in the random path to decrypt their respective parts of the composite ciphertext.

Notice that with the RAC quantum public key protocol the ith layer in the cascade of encryptions uses a key of length $L_0 + i(log(n) + polylog(n))$, because each additional layer increases the length of the data by $log(n) + polylog(n)$. The $log(n)$ part is due to the necessity to tell every intermediate player in the path what is the next address in the path, and the $polylog(n)$ part is the contribution of the labels, l, which have length $O(polylog(n))$ (Equation (1.1)).

The protocol involves a preprocessing stage for distribution of quantum public keys. This stage is independent of the actual message delivery stage, and can be done in advance, such that a large

enough number of keys are distributed to allow the protocol function for a sufficiently long time before fresh keys need to be produced. The distribution of keys require a polynomial amount of communications, of order $O(n^2)$, as each user distributes a key to every other user. The details about how key distribution is done are given in Section 1.4.

Unlike classical public keys, the keys formed by the RAC protocol are one time pads, and so each use of a key disposes of that key. Therefore, every once in a while a new session of key distribution using the RAC protocol has to be performed.

The Correctness of the network anonymity protocol just described, and its information theoretic privacy, are a direct consequence of the corresponding properties of the underlying RAC protocol.

Because the RAC quantum public key protocol provides us, just like classical public key schemes such as RSA, with symmetry (Definition 0.1), the usual reduction of *unlinkability* to *traffic analysis* (see the discussion in Part I) can be applied in our quantum anonymous network protocol (based on the RAC protocol) in the same way as this is done in the classical computational solutions (based on RSA, see [54, 17]).

As in the computational classical solutions the number of rounds is $O(polylog(n))$. The keys that are used in Equation (2.2) have length $O(polylog(n))$, and thus the total length (in qubits) of the ciphertext E of Equation (2.2) is also $O(polylog(n))$. We thus proved Theorem 0.5, i.e. that our quantum network anonymity protocol takes $O(polylog(n))$ rounds per message delivery, and in the model where only a (arbitrarily large) fraction of the communication links is adversarial, the total amount of communications per one message is $O(polylog(n))$. We also conclude that in the model where *all* the links are adversarial the communication complexity per one message is $O(n \cdot polylog(n))$.

A question that can be asked now is whether we can save something in the communication complexity of our solution if we use a different quantum public key scheme than the RAC protocol. As mentioned in Section 1.3 it is an open question to determine the best possible ratio between the length of the public key and the length of the message, in the case of the MRAC protocol (which is presented in Section 1.3). Another open question is whether it is possible to have a quantum public key scheme with a key that is shorter than the message it is used to encrypt. We note here that regardless of the length of the public key, the per-message communication complexity would remain $n \cdot polylog(n)$ in the case where the adversary controls all the communication links in the system, and $polylog(n)$ when he controls only a fraction of them (exactly as in the classical computational mix-based solution). The RAC protocol is therefore optimal in this sense. The reason for this is that the cascade of encryptions (Eq. (2.1) in the classical case and Eq. (2.2) in

the quantum case) has polylogarithmic length, which implies that the amount of communication along one random path is polylogarithmic with any possible key length (even if the key was one bit long, you still have to send at least one bit over a path of polylog length, which means a total of polylog communication...).

Another remark that I would like to make here is that the OBR protocol, which is the third quantum public key protocol presented in Section 1.3, is completely unadequate for the use in quantum mix-based solution for network anonymity. This is because in this protocol, unlike the RAC and MRAC protocols, the quantum communication is two sided, i.e. both the key distribution part and the encryption part of the protocol are quantum. As a consequence, it is not possible to form a cascade of encryptions as in Eq. (2.2), because this would require the encryption of a quantum message using a quantum public key, whereas the OBR protocol is only designed to encrypt *classical* messages (with quantum keys).

2.3 A classical impossibility result

In this section we go back from discussing network anonymity protocols to the discussion of their basic ingredient - the underlying public key. We saw in the previous sections how a classical public key can be used to to design a computationally secure anonymous network, and we saw how a quantum public key can be used to design an information theoretic secure anonymous network. We now ask whether it is possible to have a classical, rather than quantum, local (see Definition 0.2) and symmetric protocol in the information-theoretic setting. If the answer was a yes, then we could use this protocol in exactly the same way as we did with our quantum protocol (the RAC protocol), to design an information theoretic anonymous network as efficient (in terms of communication complexity) as our quantum solution. Unfortunately, as we prove in Theorem 2.2, the answer is no.

This does not mean that a classical efficient information theoretic secure anonymous network does not exist. This conjecture we can neither prove nor refute, and it is left as an open question for future research. However, what Theorem 2.2 does show is that if there exists a classical, efficient and information theoretic secure solution it must necessarily be designed with a different approach than the one used in the classical computational solutions (for instance, [54, 17]), and in our quantum information theoretic solution.

As in Section 1.2, we consider some set of players $P_1, \ldots, P_n$, and another player, Alice. We assume that the players share secret information with each other. Although the distribution of such

secrets is by itself already known to be unachievable in the classical world, we nevertheless allow for the initialization of the system in this way, to make the impossibility result interesting. We show that even under these initial conditions no such protocol exists. To strengthen the result even more, one may further allow protocols having more than one round of communications. With some modifications to the proof it can be shown that even then no such classical protocol exist. However, for the sake of simplicity of the presentation we restrict the discussion to one round protocols.

2.3.1 The communication model

As in Section 1.2, a unique *active* player P_a (with $a \in \{1, \ldots, n\}$) is picked according to some arbitrary probability distribution over the players $P_1, \ldots, P_n$. The choice of the active player is not known to any of the other players. The active player P_a chooses a message $m \in \mathcal{M}$, and his goal is to communicate the message m to Alice.

We assume some string $\overline{s} = (s_1, \ldots, s_n, S_A)$ is prepared in advance in an arbitrary way, and distributed to the players, where P_i gets string s_i, and Alice gets s_A. This allows for arbitrary correlations between any pair of players, or any subset of players. Again we emphasize that it is completely unclear how to produce this general type of correlations in practice, but we do consider this most general scenario to make the claim as strong as possible, which also means as interesting as possible.

To be consistent with Definition 0.2, a *local* protocol between P_a and Alice is a pair of functions E, D where $e = E(m, s_a)$ is the ciphertext produced by P_a and $D = D(s_A, e)$ is Alice's decoding strategy. We assume, as in Section 1.2, that all players can hear all messages, but the transmission does not carry information about its source. We define:

Definition 2.1. *A protocol is:*

- α*-correct if* $\Pr_{m,\overline{s},a}\ [D(s_A, e) = m] > \alpha$.
- β*-private if for every* $a \in \{1, \ldots, n\}$*, and all adversaries* P_j^*, $\Pr_{m,\overline{s}}\ [\ \exists_{j \neq a}\ P_j^*(s_j, e) = m] < \beta$*, with* P_a *being the active player.*
- γ*-symmetric if for every adversary* A^*, $\Pr_{m,\overline{s},a}\ [A^*(s_A, e) = a] < \gamma$.

Note that the definitions given here are deliberately much weaker compared to the definitions we used in Section 1.2. Privacy and symmetry, e.g., are defined only with respect to a single player adversary and not a collusion of adversaries as in Section 1.2, and breach of the symmetry requires

the adversary to exactly know the identity of the sender of a message; any situation other than *complete* information is not considered a breach of symmetry by the adversary.

We deliberately take the weakest possible definitions whenever it is possible, to make the result as strong as it can get. We show that even with all these weakened definitions there is no classical protocol for the problem.

2.3.2 Statement of the result and idea of the proof

Theorem 2.2. *There is no classical protocol which is local, α-correct, β-private and γ-symmetric, for any α, β, γ satisfying together $\beta < \frac{1}{4} - (1-\alpha)$ and $1 - 4(1-\alpha) > \frac{1}{2} + 2\gamma$.*

In particular, for example, no local classical protocol can be, say, 0.95-correct, 0.3-private and 0.1-anonymous.

The intuition why any classical protocol cannot have good parameters α, β, γ is quite simple. Suppose we do have a protocol with good correctness, so that Alice has a good chance of decoding the message m from the ciphertext e. She then may try to learn who sent her the message by simply going over the list of all players and searching for the one who is likely to send m given that the resulting ciphertext is e. Since we also assume that the protocol has good symmetry, this possibility must be ruled out. It must be, then, that in Alice's point of view with good probability more than one player might produce the same transcript e if they were to send the same m. But this gives rise to an attack on the privacy of the protocol - players other than the one who sent the message might try to find m. This is done by player P simply picking the message m that is the most likely one to be sent by himself given that the ciphertext is e and given the information he shares with Alice. At least one of the non active players will succeed in guessing m this way (with good probability). But since we also assume good privacy, we must conclude that this kind of attack can not work, which implies that there is more than one likely message. But now we arrived at a contradiction to the good correctness of the protocol - if P, maybe in some different time, does try to send some message to Alice, and the resulting transcript is e, then Alice has no good way to decode the correct message!

We now give the details.

2.3.3 Proof of Theorem 2.2

Let M, E, S_i, S_A be the random variables corresponding to the message, the encryption and secrets of the players. Let I be a random variable denoting the active player $i \in [1..n]$. We let V_A

denote Alice's view of the protocol (which means the information that is available to her), i.e., $V_A = (E, S_A)$, and for every i $V_i = (E, S_i)$ is P_i's view of the protocol. Since Alice's view V_A includes information about all of the V_is, we define random variables Z_is, which correspond to the net mutual information that V_A has with each V_i separately. To be more specific, we denote by $Z_i(V_A)$ the random variable describing the mutual information that Alice has with the player P_i's secret string S_i (Z_i is a function of V_A and also of V_i, because both Alice and P_i know Z_i). Z_i can be thought of as a description of the posterior probability distribution on the possible values of S_i given V_A.

For every view $V_a = v$ Alice can form a matrix $M(v)$ of size $n \times M$, where $M(v)_{i,m} = \Pr(M = m, I = i \mid V_A = v)$. Alice's decoding given her view v, is the value m such that $p_m = \sum_i M_{i,m}$ is largest. Alice's guess of the identity of the sender is the i such that $q_i = \sum_m M_{i,m}$ is largest. For every v and $M = M(v)$ let $m = m(v)$ be the most probable decoding. We have,

- Except for probability one fourth (over $V = v$) $\sum_i M_{i,m} \geq 1 - 4(1 - \alpha)$, for otherwise Alice decodes incorrectly with probability at least $1 - \alpha$.

- Except for probability one fourth, for every i we have $q_i \leq 4\gamma$, for otherwise Alice correctly guesses the sender with overall success probability γ , and,

- We soon prove Claim 2.3, that if $\beta < \frac{1}{4} - (1 - \alpha)$ then except for probability one fourth, there is at most one i such that the i'th row $M_{i,m'}$ is maximized at $M_{i,m}$ (again, m is Alice's decoding of v and $M = M(v)$).

Together, this implies that for at least one fourth of the views, all events above apply. In this case we have $p_m = \sum_i M_{i,m} \geq 1 - 4(1 - \alpha)$. Let k be the unique value such that $M_{k,m} = \max_{m'} M_{k,m'}$. Notice that $q_i = \sum_{m'} M_{i,m'}$, and for $i \neq k$, $M_{i,m}$ is at most $q_i/2$. We have, $\sum_{i \neq k} M_{i,m} \leq \sum_{i \neq k} \frac{q_i}{2} = \frac{1-q_k}{2}$. We therefore conclude,

$$\begin{aligned} p_m = \sum_i M_{i,m} &\leq M_{k,m} + \sum_{i \neq k} M_{i,m} \\ &\leq \Pr(I = k | V = v) + \sum_{i \neq k} \frac{q_i}{2} \\ &\leq q_k + \frac{1 - q_k}{2} = \frac{1 + q_k}{2} \leq \frac{1}{2} + 2\gamma. \end{aligned}$$

Altogether, if $\beta < \frac{1}{4} - (1-\alpha)$ then with probability at least one fourth $1-4(1-\alpha) \leq p_m \leq \frac{1}{2}+2\gamma$, and thus no protocol can satisfy together $\beta < \frac{1}{4} - (1-\alpha)$ and $1-4(1-\alpha) > \frac{1}{2} + 2\gamma$.

Thus, all that is left is showing Claim 2.3:

Claim 2.3. *If $\beta < \frac{1}{4} - (1-\alpha)$ then except for probability one fourth on the views V_A, there is at most one i such that $M_{i,m} = \max_{m'} M_{i,m'}$.*

Proof. $M_{i,m'} = \Pr(M = m', I = i \mid V_A = v) = \Pr(I = i | V_A = v) \cdot \Pr(M = m' | I = i, A_v = v)$ and thus the proportion between M_{i,m_1} and M_{i,m_2} is the proportion between $\Pr(M = m_1 | I = i, A_v = v)$ and $\Pr(M = m_2 | I = i, A_v = v)$. Also notice that $\Pr(M = m' | I = i, A_v = v) = \Pr(M = m' \mid I = i, Z_i(V_A) = z_i)$. This is because given that $I = i$ the message does not depend on information known to Alice and not known to the ith player P_i. Also, since Z_i can be computed from V_i, P_i can look for the most probable value m' that maximizes $\Pr(M = m' \mid I = i, Z_i = z_i)$.

It follows that if with probability one fourth over the views, there is another i whose row maximizes at m, then with probability $\frac{1}{4}$ there is another player that decodes as Alice does, and except for probability $1-\alpha$ he is right. Thus, altogether, with probability $\frac{1}{4} - (1-\alpha) > \beta$ privacy is violated. □

2.4 A classical information theoretic anonymous network

2.4.1 A non-local symmetric classical protocol

In Section 2.3 we showed that a classical local information theoretic secure protocol cannot exist. We now present a classical protocol for information theoretic privacy and symmetry, which is *non-local*. This means that you have to rely on cooperation of other (possibly adversarial) players to deliver your message.

The protocol is based on the idea of the DC-network protocol [29], with a modification due to [39].

We assume each pair of players P_i, P_j share a secret $s_{i,j}$, and each player P_j shares a secret $s_{A,j}$ with Alice (we do not concern ourselves here with how secrets are distributed - either the players met in private beforehand, or they use quantum key distribution for this matter). Note that $\sum_{i,j} s_{i,j} = 0$ because every secret is counted twice. A message m is picked by the active player P_a. For every $j \neq a$ P_j sends $e_j = s_{A,j} \oplus \sum_{i \neq j} s_{i,j}$ to Alice. The active player P_a sends $e_a = m \oplus s_{A,a} \oplus \sum_{i \neq a} s_{i,a}$. Alice decodes the message by XORing together all the pieces she has received, and then XORing the result with $\sum_i s_{A,i}$.

The protocol is easily seen to be correct, private and symmetric (even against collusions) in an information theoretic sense.

2.4.2 A network

To extend the non local protocol of Section 2.4.1 to the treatment of network anonymity, we assume that a large supply of the above secrets was prepared in advance. The solution works in cycles. At each cycle there is a unique predetermined player who is supposed to receive a message at this cycle. The order of recipients is fixed and known to everybody in the network. To send a message to player P the protocol of Section 2.4.1 is used. If no-one wishes to send P a message then this results in P receiving a message containing all zeros. On the other hand, there are various approaches to resolve the problem of collisions of messages being sent to P on his turn. One such approach is, for instance, to use a code such that the codewords are linearly independent. This way the receiver will know that a collision appened, when he receives a message which is not a codeword. He can then announce the occurence of such an event publicly. The senders can then resend their messages after a randomly chosen time delay (note, however, that this requires waiting at least additional n cycles per each attempt).

The number of round required per message delivery in this solution is, thus, linear in the number of players, and the same is true for the communication cost per message.

Part III

Quantum Private Keys

Chapter 3

Quantum key distribution

It is already known [61] that quantum computers can be used to break some of the best classical public key cryptosystems. Fortunately, however, some of the basic principles of quantum mechanics, like that non commuting observables cannot be simultaneously measured, and that general quantum information cannot be copied, enable a different type of secure cryptography. These principles can be exploited to provide unconditionally secure distribution of private information, a process we call *quantum key distribution (QKD)*. This, in turn, is enough to allow unconditionally secure communication via a classical procedure called 'private key' encryption.

The first quantum key distribution protocol was proposed by Bennett and Brassard in 1984 [16]. This simple protocol, which we also describe in this chapter, was followed by numerous other variants and protocols over the years, all following the same principle ideas from quantum information theory. The idea and general structure of most of protocols is described in Section 3.2. A few protocols, including the original protocol of [16], are presented in Section 3.3.

3.1 One time pad encryption

Private key cryptography is a much older form of cryptography than the modern commonly used public key cryptography. In a private key cryptosystem, if Alice wishes to send a secure message to Bob then she must have an *encoding key* with which she can encrypt her message. Bob, on the other hand, must have a matching *decoding key* with which he decrypts the message sent by Alice. The *one time pad* (vernam cipher) is a simple example private key cryptosystem, in which the encryption and decryption keys are identical. Alice and Bob begin with a shared n bit secret key (usually binary) string. To encode an n bit message Alice XORs the message and key together,

bitwise. To decode, Bob XORs the ciphertext obtained from Alice with the key, to restore the cleartext. For example, the ciphertext that results from XORing together the message 11010 with the key 00111 is 11101.

$$\begin{array}{r} 11010 \\ \oplus \\ \underline{00111} \\ 11101 \end{array}$$

The security of this scheme is unconditional: if the private key is truly secret, an eavesdropper who listens to the data communicated from Alice to Bob gets zero information with the actual message, no matter how computationally powerful he is. However, it can only be regarded secure if the key is the same bit length as the actual message, and if the key is only used once. To be able to send a longer message, or a new message, Alice and Bob need a fresh set of secret bits. Thus the main difficulty with one time pads is secure distribution of key bits. If Alice and Bob are far apart then classical information theory tells us that secret information cannot be distributed, because any data transferred over an unsecure communication channel is fully available to the eavesdropper Eve, who can safely copy the information without the risk of being detected by Alice and Bob. The only way to agree on a private key is by meeting in private, or using a trusted third party to deliver the secret data. This important limitation is the major reason why private key cryptography is less suitable for general use, where a lot of secret communications is required and the communicating parties are far apart. The use of quantum information, via a procedure called quantum key distribution, allows us to overcome this difficulty in distributing secret data, and thus makes private key encryption more applicable for practical use.

3.2 Generic quantum key distribution

The protocols for quantum key distribution generally have the following structure, which consists of four stages - *quantum* stage, *parameter estimation*, *information reconciliation* and *privacy amplification*. The first stage is the only stage that is 'quantum' - the other three are purely classical, and use the classical authenticated channel to communicate. The classical stages can be carried out with one way communications from Alice to Bob. Protocols with two way communications are also considered in the literature (e.g. [37]), but they are less simple.

3.2.1 The quantum stage

In the first stage Alice picks the random bits for the key, encodes them on some set of non orthogonal quantum states, and sends them to Bob through a quantum public channel. Eve may interact with the quantum signals on transition from Alice to Bob. After receiving the quantum signals, Bob performs some measurements on them, from which he deduces some classical bit string. Alice and Bob perform some sifting on the bit locations, which is mainly affected by Bob's choice of measurement bases, and which leaves them with a subset of the original bits. Bob's string might be very different from Alice's because, as noted before, Eve's interaction can cause disturbance to the states.

3.2.2 Parameter estimation

The parameter estimation stage of the quantum key distribution protocol is aimed at estimating the error rate caused by eavesdropping activity during the quantum communications. The estimated error rate is then used to place an upper bound on the eavesdropper's information. Alice randomly selects a fraction (usually a half) of the total number of bits to serve as test bits. These bit locations will be later discarded, because their bit values are revealed to Eve during the test. Alice and Bob publish and compare the values of their bits in the selected locations, counting the number of disagreements. From this number they deduce an upper bound on the error rate of the other (untested) bits. It can be shown (see [52], Exercise 12.27) that for n-bit strings (with large enough n), with probability $1-e^{-O(\epsilon^2 n)}$ the fraction of disagreements in the untested bits is within distance ϵ from their fraction in the tested bits.

If the error rate is greater than some predetermined value, Alice and Bob announce the abortion of the protocol. This threshold value is determined so that if the test passes, it is still possible to extract after information reconciliation and privacy amplification a secret key of the desired length from the remaining untested bits. Of course this value must be greater than the amount of expected noise introduced by the channel, or otherwise the protocol will almost always be aborted (for convenience and simplicity, they attribute all the errors to Eve, even though some error may be a consequence of the noise in the channel, rather than of eavesdropping activity).

3.2.3 Information reconciliation

Information reconciliation is a classical procedure, conducted over the classical public channel, which reconciles errors between Alice's bit string and Bob's bit string. This procedure with high

probability results in Alice and Bob sharing identical bit strings at the end of it, and such that the additional information leaked to Eve during the process is very small.

The procedure involves Alice choosing some random subsets of bit locations, computing the sequence of parities of the bits in the specified locations of each subset, and sending the results to Bob together with the subset specifications. According to the correlation between Alice and Bob's strings, as estimated in the parameter estimation stage, if the number of parity checks is big enough it contains enough information for Bob to correct the errors in his string with high probability. For more on information reconciliation see [13, 20].

This procedure gives Eve additional knowledge. However (see [26]), this increase can be bounded below such that there still is enough room for privacy amplification to work, with high probability.

3.2.4 Privacy amplification

Privacy amplification was first introduced by Bennett, Brassard and Robert [15]. After the information reconciliation stage Alice and Bob share a key, with which Eve has partial mutual information that is upper bounded by some value known to Alice and Bob. Privacy amplification is a classical procedure, conducted over the classical public channel, which reduces Eve's mutual information with the resulting bit string to any desired level. The length of the resulting (final) key depends on the amount of knowledge of Eve after the information reconciliation stage.

Suppose after information reconciliation Alice and Bob share an n bit string x, and Eve's knowledge about x is described by a random variable Y. The basic method for privacy amplification uses a class $\mathcal{H}$ of *universal hash functions*, which maps n-bit strings to $(m < n)$-bit strings. For any distinct $x_1, x_2 \in \{0,1\}^n$, if h is a random member of $\mathcal{H}$ then the probability that $h(x_1) = h(x_2)$ is at most $\frac{1}{2^m}$.

Alice picks a random $h \in \mathcal{H}$, and sends h to Bob over the classical public channel. The final key is $h(x)$. It can be shown ([14]) that when m is chosen small enough, Eve has almost full expected uncertainty about the final key (even though she knows the publicly announced random choice of the hash function h !).

3.3 Some protocols

In this section we present the original BB84 protocol (named after its inventors Bennett and Brassard in 1984), and three variants of it.

The BB84 protocol

First stage: Alice begins with two random classical bit strings a and b, each having $(4+\delta)n$ bits. Alice encodes each bit of the string a on one qubit. The qubit is prepared in one of two conjugate bases $\{|0\rangle, |1\rangle\}$ and $\left\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\}$, depending on the corresponding bit in the string b; in case it is 0 she uses the former basis, and in the other case she uses the latter. If the encoded bit of a is 0 it is encoded by either the state $|0\rangle$ or the state $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, depending which of the bases was chosen. If the encoded bit is 1 it is encoded by either $|1\rangle$ or $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$. The $(4+\delta)n$ qubits are then sent one by one to Bob.

Bob receives all the qubits, announces this fact, and measures each qubit in a random basis from $\{|0\rangle, |1\rangle\}$ and $\left\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\}$.

After Bob announces reception of the qubits, Alice announces the string b. Alice and Bob discard any bits which Bob measured in a different basis than prepared by Alice. With high probability they are left with at least $2n$ bits (if not, they abort the protocol and start again). They keep $2n$ bits.

Second stage: Alice and Bob perform testing on half of the bits. Alice selects a subset of n bits out of the $2n$ bits for parameter estimation, and announces her selection. She also announces the values of the bits of a in the specified locations. Bob compares these values to the outcomes of his measurements; if too many of the values disagree he announces the abortion of the protocol.

Third stage: Alice and Bob perform information reconciliation on the remaining n bits.

Fourth stage: Alice and Bob perform privacy amplification, after which they are left with m bits as their private key.

The BB84 protocol has very appealing properties in addition to its nice symmetric structure. The protocol only requires that Alice can prepare four simple one-qubit states, and that Bob can measure in one of two orthogonal bases. No ability to store quantum states, nor to manipulate qubits, is required. This makes the protocol more easy to implement than protocols that use a more complex structure, such as protocols that use entangled states and protocols that require Bob to have a quantum memory or to have an ability to perform unitary operations.

The B92 protocol

The B92 protocol, named after its inventor Bennett in 1992 [12], is a simplified version of BB84, in which only two states are used, instead of the four states used in BB84.

Consider two nonorthogonal quantum states of one qubit $|\alpha_0\rangle$ and $|\alpha_1\rangle$. To encode data bit 0 Alice sends $|\alpha_0\rangle$ to Bob, and to encode 1 she sends $|\alpha_1\rangle$. Bob chooses randomly to measure in one of two Von Neumann measurements. The first measurement consists of the vectors $\{|\alpha_0\rangle, |\alpha_0^+\rangle\}$, where $|\alpha_0^+\rangle$ is orthogonal to $|\alpha_0\rangle$. Similarly, the second measurement is given by $\{|\alpha_1\rangle, |\alpha_1^+\rangle\}$, with $|\alpha_1^+\rangle$ orthogonal to $|\alpha_1\rangle$. Bob announces acceptance if he obtains outcomes corresponding to $|\alpha_0^+\rangle$ or $|\alpha_1^+\rangle$, otherwise both parties discard the values that they recorded. Bob jots down the value 0/1 if he obtains $|\alpha_0\rangle/|\alpha_1\rangle$.

Note that in the case of perfect transmission the strings of Alice and Bob, conditioned upon acceptance, are identical and randomly distributed.

Parameter estimation, information reconciliation and privacy amplification are the same as in the BB84 protocol.

The six state protocol

The six state protocol is similar to the BB84 protocol, but makes use of a third basis on either Alice and Bob's side. The additional basis is $\left\{\frac{|0\rangle+i|1\rangle}{\sqrt{2}}, \frac{|0\rangle-i|1\rangle}{\sqrt{2}}\right\}$, which together with the two other bases of BB84 forms a complete set of MUB (see Section 4.1.3). Thus, this protocol admits higher symmetry than the BB84 protocol.

The 4MUB protocol

Quantum key distribution protocols are not restricted to two level systems. The straightforward generalization of the six state protocol to a three level system is the 4MUB protocol. It uses a complete set of MUB in a three dimensional Hilbert space. One such complete set is described in Section 4.1.3. The private key generated with this protocol is a string of *trits* rather than bits. Parameter estimation, information reconciliation and privacy amplification are generalized to trits in a straightforward way.

3.4 Attack models

Assuming that Alice's source, as well as Bob's detector, are perfect, the most general and powerful attack that can be carried out by the adversary Eve is a *coherent* attack. In a coherent attack Eve stores and manipulates large blocks of the transmitted quantum signals. She may append to the quantum states an arbitrary ancillary system of her choice and let the two systems interact in a controlled manner. She may then send the (possibly disrupted) signals on to Bob while keeping the ancilla for later inspection. After Alice and Bob reveal additional information, such as the bases they chose, and such as data leaked during information reconciliation and privacy amplification, Eve can measure her ancilla, with the choice of measurement depending on that additional information.

Less powerful and more restricted attacks are *individual* attacks and *collective* attacks, which have also been discussed in the literature. These attacks are easier to analyze than coherent attacks.

Individual attacks are the case where Eve is restricted to interacting with each of the signal systems sent by Alice separately (the signals are qubits in some protocols, but can also be higher dimensional quantum systems). For each of the signal systems Eve can attach an auxiliary system and apply some fixed unitary operation. Eve can then measure each of these systems individually before Alice and Bob start with the classical processing. This means that her measurement does not depend on further information that is revealed during classical communications.

Collective attacks are defined similarly to individual attacks, except that Eve can delay her measurement to the very end of the protocol. Moreover, she can measure all her auxiliary systems jointly.

3.5 Security and efficiency

A quantum key distribution protocol has an input – the n random bits of Alice, and an output – k bits of shared key. Eavesdropping activity, and also channel noise, cause disturbance to the quantum signals, which are the quantum states of the physical entities transmitted from Alice to Bob. This disturbance causes bit errors in the measurement results of Bob.

Definition 3.1. *The* error rate *in the system is the amount of bit errors per transmitted quantum signal. That is, the probability, averaged over the transmitted quantum systems, that Bob's measurement yields a wrong result, assuming that Alice and Bob use the same measurement bases.*

Alice and Bob get an estimate of the error rate during the testing stage of the protocol. When the estimate error rate is above a certain threshold value no key can be extracted, and they abort

the protocol.

Definition 3.2. *The* key-rate *of a protocol is the ratio* $r := \lim_{n\to\infty} \frac{k}{n}$*, which is a function of the error rate.*

Security of a protocol means that at the end of it Alice and Bob share a (essentially random) string of $k > 0$ bits, which is identical for both of them, and which has a limited amount of mutual information available to an eavesdropper.

To be more precise, we say that a protocol is ϵ-*secure* if the state describing the key of Alice and Bob, together with the adversary's quantum system, is ϵ-close to a state where the adversary's system is completely independent of the key.

Definition 3.3 (Security of QKD)**.** *Let* S *be the set of all possible secret keys,* s*, and let* $|\psi_{A,B,E}\rangle$ *be the pure state of the complete system of Alice, Bob and Eve after the protocol terminates. Then the protocol is* ϵ*-secure if there exist a state* $|\psi_E\rangle$ *of Eve's system such that*

$$\left\| |\psi_{A,B,E}\rangle - \sum_{s\in S} \frac{1}{\sqrt{|S|}} |s\rangle|s\rangle|\psi_E\rangle \right\|_{\mathrm{tr}} \leq \epsilon.$$

This definition leads to the so-called *universally composable* security, which implies that the key can safely be used in any arbitrary context [11, 10, 58].

Definition 3.3 does not take into account the *efficiency* of the protocol, which is the asymptotic behavior of the key rate r as a function of the error rate and, in particular, the maximal amount of error rate that is tolerable, i.e for which the key rate is still positive.

The security of QKD protocols against various possible eavesdropping attacks was discussed extensively over the years. Proving the security of BB84 against individual attacks was easier than for coherent attacks. It was not until 1998 that a general proof, unlimited to any specific type of attack, was presented for the BB84 protocol by Mayers [48]. Another general proof, published around that same time, is due to Biham, Boyer, Brassard, van de Graaf and Mor [18]. Unlike these two proofs, which are quite complicated, there is a simple proof given by Lo and Chau [45]. However, this proof is for a variant of the BB84 protocol which unlike the original BB84 requires that the communicating parties have the ability to perform certain quantum computations rather than just having the ability to prepare and to measure certain one qubit states, as in the original BB84. It is usually more difficult to prove the security of protocols like BB84, which requires only very simple 'prepare and measure' capabilities of Alice and Bob, than protocols that use quantum

computers or entanglement. In principle one can say that 'the simpler the protocol the harder the proof'.

In the year 2000 Preskill and Shor [62] gave another proof of the security of the BB84 protocol against general attacks. Their proof is based on the following observations:

1. Instead of preparing a system in a certain state and then sending it to Bob, Alice can equivalently prepare an entangled state, send half of it to Bob, and later measure her subsystem. In doing so, she effectively prepares Bob's system at a distance.

2. Alice and Bob can perform entanglement distillation. At the end of it their joint system is in a pure, maximally entangled state, which implies that their measurement results are perfectly correlated, and completely non accessible to Eve.

3. Certain entanglement distillation protocols are mathematically equivalent to CSS codes [27], and these codes have the property that bit errors and phase errors can be corrected separately. Since the final key is classical, only bit errors has to be corrected. This is a purely classical task - no quantum storage or quantum computation are required.

Applying a series of simple reduction steps, they showed that BB84 has the same level of security as a simple protocol based on a CSS quantum error correcting code.

The proof of Preskill and Shor is the most simple and elegant proof that was ever given to the security of the BB84 protocol. Their proof technique was subsequently extended by Tamaki et. al. [64] to the B92 protocol.

The maximum tolerable error rate of the underlying CSS code was used to give a lower bound on the maximal tolerable error rate of the corresponding QKD protocol. In the case of BB84 it was estimated that up to 11% error rate is acceptable. In the case of B92 the estimate was 4.8%.

A different proof technique, covering a large class of QKD protocols including BB84, B92 and the six state protocol, was devised by Kraus et. al. in 2003 [57]. Like the proof of Preskill and Shor, they use the equivalence to an entanglement based protocol. This proof shows that for a generic one-way QKD protocol (with structure similar to BB84) it suffices to consider collective attacks in order to derive lower bounds on the secret key rate, even when the adversary Eve actually applies a coherent attack. They also demonstrate that the lower bounds can sometimes be improved if Alice adds some random noise to her classical data, before the information reconciliation stage of the protocol. Using this method they get 12.4% tolerable error rate for BB84, 5.6% for B92 and 14.1% for the six state protocol.

Yet more recent results [63, 43] stretch the bounds for BB84 and the 6-state protocols to 12.92% and 14.59%, respectively. Both improvements come from the application of degenerate block coding.

[57] also derive upper bounds on the key rate of these protocols. The upper bound for BB84 is 14.6% and for the six state protocol it is 16.23%.

An advantage of the approach of [57] over other proofs is that it can easily be extended to protocols that use d-level quantum systems with d larger than 2.

We comment that a *two way* version of any one way QKD protocol exists, which usually has improved key rate. Two way QKD protocols are those that allow two way, instead of one way, classical communication between Alice and Bob during the information reconciliation and privacy amplification stages of the protocol. [37] show that the two way version of the BB84 protocol has 18.9% tolerable error rate, and that the six state protocol has 21.1% tolerable error rate.

Chapter 4

Biphoton quantum key distribution with single-photon operations

We show in this chapter that there are one-way quantum key distribution protocols, based on three level systems (using biphotons), which have a very simple implementation, and yet admit higher key rates than the best two-level protocols. A protocol is considered to have a simple implementation if it employs only computational basis states, and states which can be produced from computational basis states using only the set of quantum operators allowed in two-level protocols (i.e. protocols that use qubits). The detailed definition of the term "simple implementation", as well as the derivation of this set of operations, and the construction of the protocols, will be given shortly (after some necessary preliminaries). A more succinct version of the results can also be found in [21].

4.1 Preliminaries

4.1.1 Fock space representation

The Fock space is a Hilbert space used to describe quantum states with a variable or unknown number of particles.

Let $\{|\psi_i\rangle\}$ be a basis for the Hilbert space of a single particle. To denote the state of a system with n_0 particles in state $|\psi_0\rangle$, n_1 particles in state $|\psi_1\rangle$, ... , n_k particles in state $|\psi_k\rangle$, it is convenient to use the notation

$$|n_0, n_1, \ldots, n_k\rangle. \tag{4.1}$$

By the Pauli exclusion principle no two fermions can be in the same quantum state, and thus in the case of fermionic particles each n_i takes the value 0 or 1. For bosonic particles n_i may take any integer value $0, 1, 2, \ldots$

The states of the form (4.1) are a basis for the Fock space, and are called *Fock states*. The most general pure state in Fock space is the linear superposition of Fock states.

The special case where there are no particles in the system is denoted $|0, \ldots, 0\rangle$, and is called *the vacuum state*. The vacuum state is a conceptual state - no actual wave function describes it. But for notational purposes, it is defined as being a normalized state, and also orthogonal to all other states of the form (4.1).

4.1.2 Creation and annihilation operators

Creation and annihilation operators are defined with respect to a prescribed basis $\{|\psi_i\rangle\}$ for the space of a single particle. Upon acting on a Fock state they respectively remove and add a particle, in the ascribed quantum state. They are denoted $a^\dagger_{\psi_i}$ and a_{ψ_i} respectively, with ψ_i referring to the quantum basis state $|\psi_i\rangle$ in which the particle is removed or added.

When acting on the vacuum state they produce

$$a^\dagger|0\rangle = |1\rangle \tag{4.2}$$

$$a|0\rangle = 0 \quad , \tag{4.3}$$

and in general

$$a^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle \tag{4.4}$$

$$a|n\rangle = \sqrt{n}|n-1\rangle \quad . \tag{4.5}$$

4.1.3 Mutually unbiased bases

Let $B_1 = \{|\alpha_1\rangle, \ldots, |\alpha_d\rangle\}$ and $B_2 = \{|\beta_1\rangle, \ldots, |\beta_d\rangle\}$ be two orthonormal bases in the space of d dimensional quantum states. B_1 and B_2 are said to be *mutually unbiased bases (MUB)* if for every i, j $|\langle\alpha_i|\beta_j\rangle| = 1/\sqrt{d}$. A set of orthonormal bases in d dimensional Hilbert space is a set of MUB, if each pair of bases from the set are MUB.

Mutually unbiased bases have an important role in determining the state of a finite dimensional quantum system, as was first indicated by Ivanovic [40]. He proved the existence of such bases when

the dimension d is a prime, by an explicit construction. Later Wootters and Fields [67] showed, again by explicit construction, the existence of MUB for prime power dimensions and proved that for any dimension d there can be at most $d+1$ MUB. However the existence of MUB for other composite dimensions which are not a prime power is still an open problem.

The concept of mutually unbiased bases has also found useful applications in quantum cryptography - they play a key role in designing quantum key distribution schemes. If a quantum system is prepared in a state which belongs to one of the bases, and then measured by an adversary in another basis, then the adversary gets no information about the state of the system; moreover, it causes maximal disturbance to the state, i.e., now a measurement in the correct basis gives the correct result with probability only $1/d$. This connection is also discussed in Section 3.

The simplest example of a complete set of MUB is the three bases in the space of two dimensional states,

$$\begin{aligned}
&\{|0\rangle, |1\rangle\} \\
&\left\{\frac{|0\rangle + |1\rangle}{\sqrt{2}}, \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right\} \\
&\left\{\frac{|0\rangle + i|1\rangle}{\sqrt{2}}, \frac{|0\rangle - i|1\rangle}{\sqrt{2}}\right\}.
\end{aligned}$$

In three dimensions, a complete set of four MUB can be constructed as follows: One basis can be chosen to be $\{|0\rangle, |1\rangle, |2\rangle\}$. Another basis is obtained by a discrete Fourier transform,

$$\left\{\frac{|0\rangle + |1\rangle + |2\rangle}{\sqrt{3}}, \frac{|0\rangle + e^{i2\pi/3}|1\rangle + e^{-i2\pi/3}|2\rangle}{\sqrt{3}}, \frac{|0\rangle + e^{-i2\pi/3}|1\rangle + e^{i2\pi/3}|2\rangle}{\sqrt{3}}\right\}.$$

The two other bases can be taken as

$$\left\{\frac{e^{i2\pi/3}|0\rangle + |1\rangle + |2\rangle}{\sqrt{3}}, \frac{|0\rangle + e^{i2\pi/3}|1\rangle + |2\rangle}{\sqrt{3}}, \frac{|0\rangle + |1\rangle + e^{i2\pi/3}|2\rangle}{\sqrt{3}}\right\}$$

and

$$\left\{\frac{e^{-i2\pi/3}|0\rangle + |1\rangle + |2\rangle}{\sqrt{3}}, \frac{|0\rangle + e^{-i2\pi/3}|1\rangle + |2\rangle}{\sqrt{3}}, \frac{|0\rangle + |1\rangle + e^{-i2\pi/3}|2\rangle}{\sqrt{3}}\right\}.$$

4.1.4 Poincare sphere

The Poincare sphere is a unit radius sphere in the three dimensional real space. It provides a convenient way of representing polarized light and predicting how any given retarder will change

the polarization form. There is a one to one (up to global phase) correspondence between pure states of a polarized photon and points on the sphere. The upper pole of the sphere, denoted H, represents horizontal linear polarization, which corresponds to the state vector $|0\rangle$. The lower pole, V, represents vertical linear polarization, $|1\rangle$. A point on the sphere, associated with a pure state $|\psi\rangle$, can be represented using polar coordinates by the axial and azimuthal angles θ and ϕ, respectively. Equivalently, in the state space representation, $|\psi\rangle$ is obtained by applying the unitary transformation

$$U(\theta,\phi) = \begin{pmatrix} \cos\theta/2 & -e^{-i\phi}\sin\theta/2 \\ e^{i\phi}\sin\theta/2 & \cos\theta/2 \end{pmatrix} \tag{4.6}$$

to the state $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, i.e. $|\psi\rangle = \begin{pmatrix} \cos\theta/2 \\ e^{i\phi}\sin\theta/2 \end{pmatrix}$.

The point P on the equator of the sphere, in the direction of the x axis, represents linear polarization $|+\rangle \equiv 1/\sqrt{2}(|0\rangle + |1\rangle)$, and the diametrically opposite point, M, represents $|-\rangle \equiv 1/\sqrt{2}(|0\rangle - |1\rangle)$. Right circular polarization, R, is represented by the point on the equator in the direction of the y axis, and corresponds to the state vector $1/\sqrt{2}(|0\rangle + i|1\rangle)$, while the diametrically opposite point, L, represents left circular polarization, and corresponds to $1/\sqrt{2}(|0\rangle - i|1\rangle)$.

We can also think of the points on the poincare sphere as representing the unitaries $U(\theta,\phi)$, in which case the upper pole corresponds to the identity operator.

In the language of creation operators $U(\theta,\phi)$ acts as

$$a_H^\dagger \overset{U(\theta,\phi)}{\rightarrow} \cos\frac{\theta}{2}a_H^\dagger + e^{i\phi}\sin\frac{\theta}{2}a_V^\dagger \tag{4.7}$$

$$a_V^\dagger \overset{U(\theta,\phi)}{\rightarrow} -e^{-i\phi}\sin\frac{\theta}{2}a_H^\dagger + \cos\frac{\theta}{2}a_V^\dagger, \tag{4.8}$$

where $a_H^\dagger$ and $a_V^\dagger$ are the creation operators with respect to linear horizontally and vertically polarized photons, respectively.

4.1.5 Maximally entangled states and the depolarizing channel for qutrits

Let $w = e^{2i\pi/3}$, and let

$$R = \begin{pmatrix} 1 & 0 & 0 \\ 0 & w & 0 \\ 0 & 0 & w^2 \end{pmatrix} \quad \textit{and} \quad T = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}. \tag{4.9}$$

We define a set of nine unitary matrices $S = \left\{R^a T^b,\ 0 \le a, b \le 2\right\}$, which are a natural generalization of the Pauli matrices

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},\ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

to the space of qutrits, as they have similar properties. In particular they form an orthogonal basis to the space of 3×3 matrices.

Similar to the construction of the Bell basis of qubits, we construct an orthogonal basis of maximally entangled states of pairs of qutrits as follows. We take

$$|\phi_{0,0}\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle), \tag{4.10}$$

and for $0 \le a, b \le 2$ we define

$$|\phi_{a,b}\rangle = R^a T^b \otimes I |\phi_{0,0}\rangle. \tag{4.11}$$

The result is a basis of maximally entangled states, composed of the following 9 states:

$$|\phi_0\rangle = R^0 T^0 |\phi_{0,0}\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle) \tag{4.12}$$

$$|\phi_1\rangle = R^0 T^1 |\phi_{0,0}\rangle = \frac{1}{\sqrt{3}}(|20\rangle + |01\rangle + |12\rangle) \tag{4.13}$$

$$|\phi_2\rangle = R^0 T^2 |\phi_{0,0}\rangle = \frac{1}{\sqrt{3}}(|10\rangle + |21\rangle + |02\rangle) \tag{4.14}$$

$$|\phi_3\rangle = R^1 T^0 |\phi_{0,0}\rangle = \frac{1}{\sqrt{3}}(|00\rangle + w|11\rangle + w^2|22\rangle) \tag{4.15}$$

$$|\phi_4\rangle = R^1 T^1 |\phi_{0,0}\rangle = \frac{1}{\sqrt{3}}(w^2|20\rangle + |01\rangle + w|12\rangle) \tag{4.16}$$

$$|\phi_5\rangle = R^1 T^2 |\phi_{0,0}\rangle = \frac{1}{\sqrt{3}}(w|10\rangle + w^2|21\rangle + |02\rangle) \tag{4.17}$$

$$|\phi_6\rangle = R^2 T^0 |\phi_{0,0}\rangle = \frac{1}{\sqrt{3}}(|00\rangle + w^2|11\rangle + w|22\rangle) \tag{4.18}$$

$$|\phi_7\rangle = R^2 T^1 |\phi_{0,0}\rangle = \frac{1}{\sqrt{3}}(w|20\rangle + |01\rangle + w^2|12\rangle) \tag{4.19}$$

$$|\phi_8\rangle = R^2 T^2 |\phi_{0,0}\rangle = \frac{1}{\sqrt{3}}(w^2|10\rangle + w|21\rangle + |02\rangle) \tag{4.20}$$

For density operators ρ on $\mathbb{C}^3 \otimes \mathbb{C}^3$ we define the operation

$$\Lambda(\rho) = \frac{1}{9} \sum_{a,b} (R^a T^b \otimes R^{2a} T^b) \rho (R^a T^b \otimes R^{2a} T^b)^\dagger. \tag{4.21}$$

The map Λ operates on ρ as a depolarizing channel, i.e. $\Lambda(\rho)$ is diagonal in the basis $\{|\phi_{a,b}\rangle\}$. In this basis the diagonal elements of $\Lambda(\rho)$ are the same as those of ρ. To see why this is true notice that for all a, a', b, b'

$$\Lambda(R^a T^b \otimes R^{a'} T^{b'}) = \delta_{2a,a'} \delta_{b,b'},$$

and also that for all a, a', b, b' $|\phi_{a',b'}\rangle$ is an eigenstate of $R^a T^b \otimes R^{2a} T^b$.

4.2 Cryptography with biphotons and single-photon operations

The measurement basis for the space of 3-state quantum systems is $\{|0\rangle, |1\rangle, |2\rangle\}$. If the space is realized using biphotons, and if our measurement is set to detect horizontal and vertical linear polarizations then, using Fock representation, this basis is $\{|0,2\rangle, |1,1\rangle, |2,0\rangle\}$, where $|2,0\rangle$ and $|0,2\rangle$ stand for two photons in horizontal and vertical polarizations, respectively, while $|1,1\rangle$ stands for one photon in each polarization. These basis states can equivalently be written in the form

$$\begin{aligned} |2,0\rangle &= \frac{1}{\sqrt{2}} (a_H^\dagger)^2 |0,0\rangle \\ |1,1\rangle &= a_H^\dagger a_V^\dagger |0,0\rangle \\ |0,2\rangle &= \frac{1}{\sqrt{2}} (a_V^\dagger)^2 |0,0\rangle, \end{aligned}$$

where $|0,0\rangle$ is the vacuum state and $a_H^\dagger$ and $a_V^\dagger$ are creation operators with respect to H and V linear polarizations.

We define the set of "single-photon operator states", SPO, as containing all quantum states of a biphoton, that can be produced from the measurement basis states via single photon operations only, i.e. operations of the type (4.6) acting simultaneously on both photons of a biphoton. Using the creation operator notation the basis states transform under single-photon operators according

to (4.7) and (4.8), i.e.

$$\begin{aligned}
|2,0\rangle &\rightarrow \cos^2\frac{\theta}{2}|2,0\rangle + \frac{1}{\sqrt{2}}e^{i\phi}\sin\theta|1,1\rangle + e^{2i\phi}\sin^2\frac{\theta}{2}|0,2\rangle \\
|1,1\rangle &\rightarrow -\frac{1}{\sqrt{2}}e^{-i\phi}\sin\theta|2,0\rangle + \cos\theta|1,1\rangle + \frac{1}{\sqrt{2}}e^{i\phi}\sin\theta|0,2\rangle \\
|0,2\rangle &\rightarrow e^{2i\phi}\sin^2\frac{\theta}{2}|2,0\rangle - \frac{1}{\sqrt{2}}e^{-i\phi}\sin\theta|1,1\rangle + \cos^2\frac{\theta}{2}|0,2\rangle,
\end{aligned}$$

which imply that the single-photon operators, when applied to the state of a biphoton, have the general form

$$W(\theta,\phi) = \begin{pmatrix} \cos^2\frac{\theta}{2} & -\frac{1}{\sqrt{2}}e^{-i\phi}\sin\theta & e^{2i\phi}\sin^2\frac{\theta}{2} \\ \frac{1}{\sqrt{2}}e^{i\phi}\sin\theta & \cos\theta & -\frac{1}{\sqrt{2}}e^{-i\phi}\sin\theta \\ e^{2i\phi}\sin^2\frac{\theta}{2} & \frac{1}{\sqrt{2}}e^{i\phi}\sin\theta & \cos^2\frac{\theta}{2} \end{pmatrix}. \tag{4.22}$$

The question we ask is what quantum key distribution protocols can be designed using only SPO states, and what level of security can they provide.

4.2.1 Geometric structure

According to (4.22), each point on the unit sphere in $\mathbb{R}^3$, determined by θ, ϕ, corresponds to a unitary operator $W(\theta,\phi)$. Depending on which quantum state $|\psi_0\rangle$ we choose to associate with the upper pole of the sphere, this correspondence also defines a matching between points on the sphere and state vectors of a biphoton, according to $|\psi(\theta,\phi)\rangle = W(\theta,\phi)|\psi_0\rangle$.

If we take $|\psi_0\rangle = |0\rangle$ (which is $|2,0\rangle$ in Fock notation) we get $|\psi(\pi,0)\rangle = |2\rangle$, i.e. $|2\rangle$ is at the lower pole of the sphere. It is also easy to see that $|1\rangle$ cannot be obtained from $|0\rangle$ or $|2\rangle$ using any single photon operator $W(\theta,\phi)$. This implies that a sphere that contains $|0\rangle$ and a sphere that contains $|1\rangle$ do not intersect.

We conclude that the set SPO can be described as the union of two distinct spheres - the sphere with upper pole $|0\rangle$ (henceforth denoted the *0-sphere*) and the sphere with upper pole $|1\rangle$ (the *1-sphere*).

The following important observation about the 0-sphere and 1-sphere can be seen directly from (4.22):

Observation 4.1. *The fidelity of two quantum states, which are represented by two points on the sphere with angle α between them, is*

1. *In the case of the* 0*-sphere it is* $\cos^4\frac{\alpha}{2}$. *In particular, for $\alpha = \pi$ the states are orthogonal.*

2. *In the case of the* 1*-sphere it is* $\cos^2\alpha$*. In particular, for* $\alpha = \pi$ *the states are identical (up to global phase), and for* $\alpha = \pi/2$ *the states are orthogonal.*

One can verify the first part of Observation 4.1 by multiplying together the first column of the matrix W in (4.22), with two different values of θ and ϕ, because the first column describes the quantum state that corresponds to the angles θ and ϕ in the case when the upper pole of the sphere is $|0\rangle$ (i.e. the 0-sphere). The second part can be derived in a similar way from the middle column of W.

This shows that there is a lot of redundancy in the 1-sphere, and actually a hemisphere is sufficient to represent all quantum states associated with that sphere.

4.2.2 Protocols for quantum key distribution

We consider here protocols with one way information reconciliation and privacy amplification. The quantum stage of the protocol is specified by the quantum states used by Alice and Bob to encode logical values $0, 1, 2$.

For the following, we assume that Alice uses m different encodings, with index $j \in J := \{1, \ldots, m\}$. For each $j \in J$, $|\phi_j^0\rangle, |\phi_j^1\rangle, |\phi_j^2\rangle$ denote orthogonal states used to encode logical values $0, 1$ and 2, respectively.

In the first step of the protocol, Alice randomly chooses n trits $x_1, \ldots x_n$, and sends n qutrits prepared in the states $|\phi_{j_1}^{x_1}\rangle, \ldots, |\phi_{j_n}^{x_n}\rangle$ to Bob.

As in the qubit BB84 protocol, the measurements are peformed for each qutrit pair in a random basis from the set of bases from which Alice select to prepare the state of the qutrit pair. The classical post processing part is also similar to BB84.

There are plenty of ways to define interesting encodings using states from SPO, from which we choose to describe two simple ones here. But first, notice the following remarks, which are direct consequences of Observation 4.1:

1. Every two opposite points on the 0-sphere represent orthogonal states of a qutrit, but there are no *triple* of points on the 0-sphere which are mutually orthogonal. This is simply because opposite points on the sphere come in pairs, not triples...

2. Think of the 0-sphere and the 1-(hemi)sphere as having a common center (with the x, y, z axes coincide). Then the intersection of any ray through the common center, with the sphere and the hemisphere, defines a triple of mutually orthogonal states, two of which belong to the

0-sphere and one to the 1-hemisphere. To see why the point from the 1-sphere is orthogonal to the points from the 0-sphere one should fix θ and ϕ, and multiply together the first column and second column of the matrix W (4.22), to see that they are orthogonal. This way one also verifies that such a ray is the only way to define an orthogonal basis composed of points from *both* spheres (i.e some points from the 0-sphere and some from the 1-sphere). The only other way to get an orthogonal basis is to take all three points from the 1-sphere.

3. On the 1-hemisphere, no two orthogonal bases are mutually unbiased. To see why this is true, fix 3 orthogonal (i.e.angle $\pi/2$ between them) points on the hemisphere, which by Observation 4.1 correspond to an orthonormal basis. One can verify now that there are exactly 4 points on the hemisphere with equal projections ($\frac{1}{\sqrt{3}}$) on all of the three basis states, and no two of these 4 points are orthogonal.

4. Take any two rays according to Remark 2. Then the corresponding two orthogonal bases are *not* mutually unbiased. This is true because take two opposite points on the 0-sphere, then according to Observation 4.1 there is no third point on this sphere with projection $\frac{1}{\sqrt{3}}$ on both of these two points.

5. Pairs of mutually unbiased bases can be found on the union of the 0-sphere and the 1-hemisphere. According to Remarks 1 - 4, they can only be of the form of one ray (two points on 0-sphere and one point on 1-sphere) and one basis whose three components are all taken from the 1-sphere. One such example is described in Section 4.2.2. A consequence is that no *three* mutually unbiased bases exist, on the union of the two spheres.

Based on these remarks, we describe the following two protocols - the *umbrella protocol* and the *three rays* protocol, which are simple and have a nice symmetric structure.

The umbrella protocol

The umbrella protocol consists of two mutually unbiased bases. One basis is the measurement basis,

$$\{|0\rangle, |1\rangle, |2\rangle\},$$

two points of which belongs to the 0-sphere and one to the 1-sphere. This basis corresponds to a vertical ray - the z axis.

The other basis is $\{|\tilde{0}\rangle, |\tilde{1}\rangle, |\tilde{2}\rangle\}$, with

$$|\tilde{0}\rangle = \frac{1}{\sqrt{3}}(-|0\rangle + |1\rangle + |2\rangle), \tag{4.23}$$

$$|\tilde{1}\rangle = \frac{1}{\sqrt{3}}(-w^2|0\rangle + |1\rangle + w|2\rangle), \tag{4.24}$$

$$|\tilde{2}\rangle = \frac{1}{\sqrt{3}}(-w|0\rangle + 1|1\rangle + w^2|2\rangle), \tag{4.25}$$

and where $w = e^{2i\pi/3}$.

Note that all three points of the second basis belong to the 1-sphere. The corresponding points on the sphere have $(\theta = \arctan\sqrt{2}, \phi = 0), (\theta = \arctan\sqrt{2}, \phi = 2\pi/3), (\theta = \arctan\sqrt{2}, \phi = 4\pi/3)$, respectively. Altogether there are four points on the 1-sphere and two points on the 0-sphere.

Figure 4.1: The umbrella protocol

The three rays protocol

The three rays protocol consists of three bases, which correspond to the three rays defined by the x,y and z axes. Thus it has nine points altogether - six points on the 0-sphere and three points on the 1-sphere.

The z axis contributes the measurement basis, $\{|0\rangle, |1\rangle, |2\rangle\}$. The x and y axes contribute the bases $\{|\tilde{0}\rangle, |\tilde{1}\rangle, |\tilde{2}\rangle\}$ and $\{|0'\rangle, |1'\rangle, |2'\rangle\}$, respectively, with

$$|\tilde{0}\rangle = \frac{1}{2}|0\rangle + \sqrt{\frac{1}{2}}|1\rangle + \frac{1}{2}|2\rangle, \tag{4.26}$$

$$|\tilde{1}\rangle = -\sqrt{\frac{1}{2}}|0\rangle + \sqrt{\frac{1}{2}}|2\rangle, \tag{4.27}$$

$$|\tilde{2}\rangle = \frac{1}{2}|0\rangle - \sqrt{\frac{1}{2}}|1\rangle + \frac{1}{2}|2\rangle, \tag{4.28}$$

and

$$|0'\rangle = \frac{1}{2}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle - \frac{1}{2}|2\rangle, \tag{4.29}$$

$$|1'\rangle = \frac{i}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|2\rangle, \tag{4.30}$$

$$|2'\rangle = \frac{1}{2}|0\rangle - \frac{i}{\sqrt{2}}|1\rangle - \frac{1}{2}|2\rangle. \tag{4.31}$$

Figure 4.2: The three-rays protocol

4.2.3 Security

In this section we prove the security of the umbrella protocol against coherent attacks, which is actually the first proof of *any* qutrit protocol against coherent attacks ever given. In particular, we derive a lower bound on the secret key rate, r, as a function of the error rate found in the parameter estimation stage. The result is summarized in Figure 4.3, where the lower bound on the key rate of the umbrella protocol is compared to the qubit six state protocol and the qutrit 4MUB protocols (both mentioned in Section 3.3). In particular, it is shown that the maximum tolerable error rate of the umbrella protocol is at least 17.7%, compared to a known upper bound of 16.3% for the six-state protocol.

For the simplicity of the proof, instead of analyzing the umbrella protocol directly we analyze another protocol involving two mutually unbiased bases. This other protocol consists of the first two out of the four bases of the 4MUB protocol listed in Section 4.1.3. We call this protocol the *Fourier* protocol, as it involves the measurement basis together with a basis rotated by a discrete Fourier transform,

$$F = \begin{pmatrix} 1 & 1 & 1 \\ 1 & w & w^2 \\ 1 & w^2 & w \end{pmatrix}. \tag{4.32}$$

We note that the Fourier protocol and the umbrella protocol have the same key rate. To see why this is true notice that they are related via a unitary transformation,

$$U = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}. \tag{4.33}$$

Now, if the umbrella protocol had inferior security compared to the Fourier protocol, Eve could take advantage of this to increase her chances to break the Fourier protocol. She could locally rotate the states sent from Alice to Bob in the Fourier protocol, with the unitary U (4.33). The effect of U on the states of the standard basis is merely a renaming (permuting the logical values 0,1 and 2), and an overall phase (which has no physical meaning). The effect of U on the states of the Fourier basis is to replace them with the states of the second basis of the umbrella protocol. Eve could behave as if the protocol that Alice and Bob use is the umbrella protocol, instead of the real Fourier protocol. Later, when Alice publicly reveals the bases she used in each coordinate, Eve can reinterprate her results according to the Fourier protocol. Since we know that Eve cannot

gain any benefit from this kind of attack (because the Fourier protocol has proved security), we conclude that the umbrella protocol has at least the same security as the Fourier protocol. The same logic shows that they actually have *exactly* the same level of security, thus only one of them needs to be analyzed to get the parameters of them both.

To derive a lower bound on the key rate of the Fourier protocol we use the technique from [57], applied to qutrits instead of qubits.

Every QKD protocol can be viewed as an entanglement based protocol, in which Alice performs a measurement to determine the values of the random bits that correspond to her choices of logical values either before or after she sends half of the system to Bob. Both cases are, of course, mathematically equivalent. An entanglement based version of the Fourier protocol consists of Alice preparing a sequence of pairs of qutrits, each pair in the maximally entangled state $|\phi_{0,0}\rangle$ (defined in Equation (4.10)). Alice sends one qutrit of each entangled pair to Bob. For parameter estimation, Alice randomly chooses to apply either $F^\dagger$ (from Eq. 4.32), or the identity operator, to her qutrit, and measures it in the measurement basis. Note that this is equivalent to randomly choosing to measure in either the measurement basis, or the Fourier rotated basis. Bob, independently, applies either F (not $F^\dagger$), or the identity operator, and measures his qutrit in the measurement basis. Note that F is the result of swapping the 2nd and 3rd columns of $F^\dagger$, thus having Bob measure in the basis F rather than $F^\dagger$ is equivalent up to renaming of the logical values 1 and 2 at the end of the protocol. Parameter estimation takes into account only the cases where both used the same basis. An error is recorded if their measurement results are inconsistent.

The main result of [57] is a formula connecting the key rate r (Definition 3.2), to the properties of the set of quantum states that correspond to the possible *collective* attacks for which the resulting error rate is Q (Definition 3.1). We extended the result of [57] to deal with three level rather than two level quantum systems. The extension of [57] to three level systems uses entropies measured in trits instead of bits. Other than this difference, the formula of [57] has the same structure with trits (and any higher level system) as it has with bits. The resulting extension to trits is Eq. (4.34).

$$r(Q) \geq \inf_{\sigma_{AB} \in \Gamma_Q} \left(S_3(X|E) - H_3(X|Y) \right). \tag{4.34}$$

In this equation σ_{AB} is a density matrix describing the joint state of two qutrits, one held by Alice and one by Bob, after the qutrit of Bob has been interacted with by Eve's system. Q is the amount of error introduced by Eve, and/or channel noise (Definition 3.1). It is the expected fraction of coordinates (trit locations) in which the logical values of Alice and Bob disagree, assuming they

always use the same measurement bases. In other words, error probability Q means that when Alice and Bob measure σ_{AB} with the measurement specified by the protocol, the probability for an error (i.e. different outcomes for Alice and Bob) is Q.

The infimum in (4.34) is taken over all density matrices σ_{AB} which, upon measurement, have expected error probability Q. In (4.34) X and Y are Alice and Bob's classical strings right after the quantum stage of the protocol, and S_3 and H_3 denote von Neumann and Shannon entropies, in trits, respectively. $S_3(X|E)$ denotes the entropy of X, conditioned on Eve's initial information, i.e., $S_3(X|E) := S_3(\sigma_{XE}) - S_3(\sigma_E)$. The state σ_{XE} is obtained from σ_{AB} by taking a purification σ_{ABE} of the state $\sigma_{AB}^{diag} := \Lambda(\sigma_{AB})$ (with Λ being the operation defined in (4.21). $\Lambda(\sigma_{AB})$ is, as noted in Section 4.1.5, diagonal in the maximally entangled basis (4.11)), and applying the measurement of Alice in the computational basis. Similarly, Y is the outcome of Bob's measurement in the computational basis, applied to the second subsystem of σ_{ABE}.

It is also shown in [57] that additional post processing by Alice, applied to her string X before the parameter estimation stage, can increase the key rate. To account for this improvement here, we consider post processing in the form of random noise added by Alice to each of her key trits independently. To be more specific, we consider here the case where for some $0 \leq q \leq 1$, for each of her logical trits in X Alice with probability $1 - q$ keeps it unchanged, while with probability q she flips it to a random one of the other possible trit values. The state σ_{AB} is the state of Alice and Bob after Eve interacted, but before Alice and Bob measure. Now Alice measures and gets X, and Bob measures and gets Y. At this point, Alice perturbes her X with some noise q. Notice, therefore, that except for X, also Γ_Q depends (indirectly) on q, because now the errors on Bob's side are with respect to the new X.

To account for this additional random noise added by Alice, the right hand side of Equation (4.34) should be maximized with respect to Alice's noise parameter q. Thus it becomes

$$r(Q) \geq \sup_q \left(\inf_{\sigma_{AB} \in \Gamma_Q} (S_3(X|E) - H_3(X|Y)) \right). \tag{4.35}$$

In this new equation the entropies are with respect to the perturbed X of Alice. As (4.35) involves a minimization over the set Γ_Q of two-qutrit states, the lower bound on the secret key rate only depends on the set of possible *collective attacks* (see Section 3.4). On the other hand, it holds against any arbitrary *coherent attack*.

To explicitly evaluate (4.35) for a specific protocol, we need to characterize the set Γ_Q. More precisely, we need to compute a set of constraints for the diagonal elements, $\lambda_0, \ldots, \lambda_8$, in the basis

(4.11), of $\sigma_{AB} \in \Gamma_Q$, because these diagonal elements, as we will shortly see, determine the error rate Q on one hand, and the entropies that appear in the right hand side of Eq. (4.35), on the other hand.

In the entanglement based version of the Fourier protocol, Alice and Bob measure the state σ_{AB} in the measurement basis with probability $\frac{1}{2}$, and with probability $\frac{1}{2}$ they measure it with respect to the Fourier basis. This is equivalent to always measuring the state

$$\mathcal{D}(\sigma_{AB}) = \frac{1}{2}\sigma_{AB} + \frac{1}{2}(F^\dagger \otimes F)\sigma_{AB}(F \otimes F^\dagger) \tag{4.36}$$

with respect to the measurement basis.

In the basis (4.11), the operator $F^\dagger \otimes F$, appearing in $\mathcal{D}$, has the form

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \tag{4.37}$$

i.e. it is a permutation matrix in this basis. Hence, $\mathcal{D}$ is an equally weighted combination of the identity operator, and the permutation operator (4.37).

To explicitly evaluate the r.h.s. of Equation 4.35, we first show that for every fixed q, the right hand side of Equation 4.35 remains the same if Γ_Q is replaced by the set of symmetrized states $\Lambda(\Gamma_Q)$. We split the proof of this fact into two claims:

Claim 4.2. *For any σ_{AB} in Γ_Q, the entropies $S_3(X|E)$ and $H_3(X|Y)$ are equal to those resulting from $\Lambda(\Gamma_Q)$ rather than from Γ_Q.*

Proof. The entropies appearing in (4.35) are all derived from the state σ_{ABE}, which is obtained from the operator Λ applied to σ_{AB}. Recall the definition and properties of Λ, described in section 4.1.5. Λ acts as a depolarizing channel, which means that in the basis (4.11) all the off-diagonal elements of a density matrix are eliminated, while leaving the diagonal elements unchanged. It is

thus clear that $\Lambda^2 = \Lambda$ (erasing the off-diagonal elements twice is the same as erasing them just once) and, hence, the entropies appearing in (4.35) would not be affected by this substitution. □

Claim 4.3. *The error rate Q in σ_{AB} is equal to the error rate that would have resulted if we were to substitute $\Lambda(\sigma_{AB})$ in place of σ_{AB}.*

Proof. To see this fact we first notice that if Alice and Bob apply Λ to their classical strings (i.e. after the measurement, and after the additional noise q) X and Y, this would not change the error amount in them. This may become clear by inspecting the effect of Λ on all possible pairs of trits (i, j), where $i, j = 0, \ldots, 2$. This way one can verify that by the definition Λ is a mixture of combinations of (global) phase shifts and trit-value changes, that take an error-free pair (X_i, Y_i) to a mixture of error free pairs, and an erroneous pair to a mixture of erroneous pairs. Since we only refer to a single measurement basis (namely the standard basis), the same statistics of errors would be obtained if we were to apply Λ *before* the measurement in the standard basis rather than afterwards. Secondly, we notice that Λ commutes with $\mathcal{D}$. The easiest way to see this is to think of Λ as an operator that erases all the off-diagonal elements (in the basis (4.11)), and think of $\mathcal{D}$ as a combination of the identity, with a permutation of the diagonal elements. It now becomes clear that it doesn't matter whether one first permutes the diagonal elements and then erase the off-diagonals, or vice versa - the result is the same. Therefore, we conclude that if we apply Λ before both the measurement in the standard basis and the application of $\mathcal{D}$, this would also not change the error rate. □

Following these two claims, we see that we can, w.l.o.g, consider the symmetrization $\Lambda(\sigma_{AB})$, instead of σ_{AB}, in (4.35).

To simplify the analysis even further, we consider another symmetrization, namely the one achieved by applying $\mathcal{D}$ to $\Lambda(\sigma_{AB})$. The resulting state is $\mathcal{D}(\Lambda(\sigma_{AB}))$, which is also equal to $\Lambda(\mathcal{D}(\sigma_{AB}))$ because, as already mentioned, Λ and $\mathcal{D}$ commute. To justify the additional symmetrization $\mathcal{D}$ we refer to the following two claims, that for every fixed q:

Claim 4.4. *For any $\Lambda(\sigma_{AB})$ in $\Lambda(\Gamma_Q)$, the expression $S_3(X|E) - H_3(X|Y)$ is equal or greater than the corresponding expression resulting from the substitution of $\mathcal{D}(\Lambda(\sigma_{AB}))$ instead of $\Lambda(\sigma_{AB})$.*

Proof. The proof consists of two steps - first show that $S_3(X|E)$ can only decrease by the substitution, then show that $H_3(X|Y)$ can only increase.

To show that $S_3(X|E)$ can only decrease by the substitution we recall that $\mathcal{D}$ is composed of a random application of either the identity operator, or $F^\dagger \otimes F$. Both of these two operators are

unitary and therefore, in both of these two possible applications individually (i.e. either in case the identity, or $F^\dagger \otimes F$, is applied with certainty) the term $S_3(X|E)$ is the same. Since in (4.35) Eve is given the purification of $\mathcal{D}(\Lambda(\sigma_{AB}))$, she is in particular given the choice of projecting the state of the complete system of ABE onto a single specific one of the two possibilities, leaving her with at most the same amount of uncertainty about X (Note that not for every purification, a qubit which purifies the classical probabilistic choice made in $\mathcal{D}$ is easy to identify. However, it is easy to construct one such purification: purify $\Lambda(\sigma_A B)$, and then consider the natural quantum version of the classical probabilistic process involved in constructing the state $\mathcal{D}(\Lambda(\sigma_A B))$ from $\Lambda(\sigma_A B)$. This last step involves an extra qubit which carries the choice of the basis in which the measurement is applied. One can move from any purification to this particular one by a unitary transformation on Eve's side, and this does not change the entropy.).

To show that $H_3(X|Y)$ can only increase by the substitution we recall that the state $\Lambda(\sigma_{AB})$ is diagonal in the basis (4.11), and that the states in this basis are maximally entangled, which means that for a specific such maximally entangled state the outcome of Alice's measurement is completely determined by Bob's outcome. The uncertainty $H_3(X|Y)$ is thus only dependent of the distribution $\lambda_0, \ldots, \lambda_8$ and on the independent random noise q. Since $F^\dagger \otimes F$ is simply a permutation in the basis (4.11), then whether we apply $F^\dagger \otimes F$ or the identity, the singular values $\lambda_0, \ldots, \lambda_8$ are the same. We may conclude, then, that in the symmetrization $\mathcal{D}(\Lambda(\sigma_{AB}))$, if we gave Bob the knowledge of which of $F^\dagger \otimes F$ or the identity was applied, his uncertainty $H_3(X|Y)$ would have been just the same as in the case $\Lambda(\Gamma_Q)$. However, since we deny him of this information, $H_3(X|Y)$ can only be higher. □

Claim 4.5. *The error rate Q in $\Lambda(\sigma_{AB})$ is equal to the error rate that would have resulted if we were to substitute $\mathcal{D}(\Lambda(\sigma_{AB}))$ in place of $\Lambda(\sigma_{AB})$.*

Proof. From the definition of $\mathcal{D}$ (Equation 4.36) it may be easily verified that $\mathcal{D}^2 = \mathcal{D}$ (notice that $F^2 = I$). This shows that applying $\mathcal{D}$ twice, once as symmetrization and once as part of the parameter estimation phase of the protocol, does not affect the error rate Q. □

Claims 4.2,4.3,4.4,4.5, together, show that if we restrict ourselves to the (combined) symmetrization $\Lambda(\mathcal{D}(\sigma_{AB}))$, the lower bound on the key rate thus achieved, via the use of (4.35), is a lower bound also with respect to the original, before symmetrizations, Umbrella protocol.

The state $\Lambda(\mathcal{D}(\sigma_{AB}))$ is diagonal in the basis (4.11). Observe (directly from the permutation

(4.37)) that the diagonal elements $\lambda_0, \ldots, \lambda_8$ satisfy

$$\lambda_1 = \lambda_6 \tag{4.38}$$

$$\lambda_2 = \lambda_3 \tag{4.39}$$

$$\lambda_4 = \lambda_5. \tag{4.40}$$

These equations are derived using the definition of the permutation (4.37), and of $\mathcal{D}$, because when $\mathcal{D}$ is applied to the state $\mathcal{D}(\Lambda(\sigma_A B))$, it averages the first and sixth diagonal elements, and also the second and third, and the fourth and fifth.

We can, thus, write

$$\lambda_1 + \lambda_2 + \lambda_4 + \lambda_5 + \lambda_7 + \lambda_8 = \lambda_3 + \lambda_4 + \lambda_5 + \lambda_6 + \lambda_7 + \lambda_8. \tag{4.41}$$

Consider now the parameter estimation phase, in which Alice and Bob choose randomly to measure in either the measurement basis or the Fourier rotated basis. If we examine each of the basis states of the basis (4.11), we see that the outcome of a measurement in the measurement basis $\{|0\rangle, |1\rangle, |2\rangle\}$, applied to such basis state, is a pair (i, j), with probability either $\frac{1}{3}$ or 0, depending on the coefficients in the specific basis state. The cases when $i \neq j$ contribute to the error count of Alice and Bob, while the cases $i = j$ are recorded as error-free. The states (4.12),(4.15),(4.18) have no error in them, i.e. the possible measurement results are $(0,0), (1,1), (2,2)$. Similarly, with respect to the Fourier basis, the error-free states are (4.12),(4.13),(4.14), because the Fourier rotation $F^\dagger \otimes F$ exchanges the state (4.12) with itself, (4.13) with (4.18), and (4.14) with (4.15) (see Euqaiton 4.37).

The overall error probability of the protocol, Q, is determined by the diagonal elements $\lambda_0, \ldots, \lambda_8$, which are the coefficients of the different basis states of the basis (4.11) in the matrix $\Lambda(\mathcal{D}(\sigma_{AB}))$. The error probability when measuring with respect to the measurement basis is $\lambda_1 + \lambda_2 + \lambda_4 + \lambda_5 + \lambda_7 + \lambda_8$, and the error probability when measuring with respect to the Fourier basis is $\lambda_3 + \lambda_4 + \lambda_5 + \lambda_6 + \lambda_7 + \lambda_8$. Altogether the error probability in the state $\Lambda(\mathcal{D}(\sigma_{AB}))$ is $\frac{1}{2}(\lambda_1 + \lambda_2 + \lambda_4 + \lambda_5 + \lambda_7 + \lambda_8) + \frac{1}{2}(\lambda_3 + \lambda_4 + \lambda_5 + \lambda_6 + \lambda_7 + \lambda_8)$. Using Equation 4.41 we arrive at the following

constraints about the coefficients $\lambda_0, \ldots, \lambda_8$:

$$\begin{aligned} \lambda_0, \ldots, \lambda_8 &\geq 0 && (4.42) \\ \lambda_0 + \ldots + \lambda_8 &= 1 && (4.43) \\ \lambda_1 + \lambda_2 + \lambda_4 + \lambda_5 + \lambda_7 + \lambda_8 &= Q && (4.44) \\ \lambda_3 + \lambda_4 + \lambda_5 + \lambda_6 + \lambda_7 + \lambda_8 &= Q. && (4.45) \end{aligned}$$

The first two constraints are due to the fact that σ_{AB} is a density matrix, and thus have non-negative eigenvalues that sum to 1. The third and fourth constraints are the contributions of the two measurement bases (i.e the standard basis and the Fourier basis) to the total error probability Q.

These constraints form a convex domain, over which we shall optimize the expression in 4.35. We note here that the optimum is actually obtained at the point that corresponds to maximum symmetry, i.e.

$$\begin{aligned} \lambda_0 &= 1 - Q && (4.46) \\ \lambda_1 = \lambda_2 = \lambda_3 = \lambda_4 = \lambda_5 = \lambda_6 = \lambda_7 = \lambda_8 &= Q/6. && (4.47) \end{aligned}$$

Therefore, one need not solve an optimization problem, but rather solve the problem analytically (namely substitute the symmetric σ_{AB} into 4.35), because the domain for optimization is reduced to consist of a single point. Here, however, we do not want to justify equation 4.47. Hence, we shall now proceed with the general plan of deriving a convex optimization problem and solving it numerically.

In order to evaluate the entropies occurring in expression (4.35), we need to consider a purification $|\psi\rangle_{ABE}$ of the diagonalization $\Lambda(\mathcal{D}(\sigma_{AB}))$. A convenient way to express this purification would be to use the basis states (4.11). With this basis we have

$$|\psi\rangle_{ABE} := \sum_{i=0}^{8} \sqrt{\lambda_i} |\phi_i\rangle_{AB} \otimes |\nu_i\rangle_E, \tag{4.48}$$

where $|\phi_0\rangle_{AB}, \ldots, |\phi_8\rangle_{AB}$ denote the (maximally entangled) states of the basis (4.11) in Alice and Bob's joint system, and where $|\nu_0\rangle_E, \ldots, |\nu_8\rangle_E$ are some mutually orthogonal states in Eve's system. If Alice and Bob measure their system with respect to the measurement basis, and obtain results x and y, respectively, then the state of Eve's system is given by the (unnormalized) vectors $|\theta^{xy}\rangle$,

where

$$|\theta^{00}\rangle = \frac{1}{\sqrt{3}}(\sqrt{\lambda_0}|\nu_0\rangle + \sqrt{\lambda_3}|\nu_3\rangle + \sqrt{\lambda_6}|\nu_6\rangle) \quad (4.49)$$

$$|\theta^{01}\rangle = \frac{1}{\sqrt{3}}(\sqrt{\lambda_2}|\nu_2\rangle + \sqrt{\lambda_5}|\nu_5\rangle + \sqrt{\lambda_8}|\nu_8\rangle) \quad (4.50)$$

$$|\theta^{02}\rangle = \frac{1}{\sqrt{3}}(\sqrt{\lambda_1}|\nu_1\rangle + \sqrt{\lambda_4}|\nu_4\rangle + \sqrt{\lambda_7}|\nu_7\rangle) \quad (4.51)$$

$$|\theta^{10}\rangle = \frac{1}{\sqrt{3}}(\sqrt{\lambda_1}|\nu_1\rangle + w\sqrt{\lambda_4}|\nu_4\rangle + w^2\sqrt{\lambda_7}|\nu_7\rangle) \quad (4.52)$$

$$|\theta^{11}\rangle = \frac{1}{\sqrt{3}}(\sqrt{\lambda_0}|\nu_0\rangle + w\sqrt{\lambda_3}|\nu_3\rangle + w^2\sqrt{\lambda_6}|\nu_6\rangle) \quad (4.53)$$

$$|\theta^{12}\rangle = \frac{1}{\sqrt{3}}(\sqrt{\lambda_2}|\nu_2\rangle + w\sqrt{\lambda_5}|\nu_5\rangle + w^2\sqrt{\lambda_8}|\nu_8\rangle) \quad (4.54)$$

$$|\theta^{20}\rangle = \frac{1}{\sqrt{3}}(\sqrt{\lambda_2}|\nu_2\rangle + w^2\sqrt{\lambda_5}|\nu_5\rangle + w\sqrt{\lambda_8}|\nu_8\rangle) \quad (4.55)$$

$$|\theta^{21}\rangle = \frac{1}{\sqrt{3}}(\sqrt{\lambda_1}|\nu_1\rangle + w^2\sqrt{\lambda_4}|\nu_4\rangle + w\sqrt{\lambda_7}|\nu_7\rangle) \quad (4.56)$$

$$|\theta^{22}\rangle = \frac{1}{\sqrt{3}}(\sqrt{\lambda_0}|\nu_0\rangle + w^2\sqrt{\lambda_3}|\nu_3\rangle + w\sqrt{\lambda_6}|\nu_6\rangle). \quad (4.57)$$

After the measurement, the (normalized) state of the system is $\sum_{x,y}|x\rangle_A|y\rangle_B|\theta^{xy}\rangle_E$. Eve's density matrix can be expressed in the form $\sigma_E = \frac{1}{3}\sigma_E^0 + \frac{1}{3}\sigma_E^1 + \frac{1}{3}\sigma_E^2$, where $\sigma_E^0, \sigma_E^1, \sigma_E^2$ correspond to the case where Alice measures $0, 1, 2$, respectively. Explicitly they are

$$\sigma_E^0 = 3|\theta^{00}\rangle\langle\theta^{00}| + 3|\theta^{01}\rangle\langle\theta^{01}| + 3|\theta^{02}\rangle\langle\theta^{02}| \quad (4.58)$$

$$\sigma_E^1 = 3|\theta^{10}\rangle\langle\theta^{10}| + 3|\theta^{11}\rangle\langle\theta^{11}| + 3|\theta^{12}\rangle\langle\theta^{12}| \quad (4.59)$$

$$\sigma_E^2 = 3|\theta^{20}\rangle\langle\theta^{20}| + 3|\theta^{21}\rangle\langle\theta^{21}| + 3|\theta^{22}\rangle\langle\theta^{22}|. \quad (4.60)$$

We can rewrite the expression in (4.35) in the form

$$S_3(X|E) - H_3(X|Y) = S_3(X) + S_3(E|X) - S_3(E) - H_3(X|Y). \quad (4.61)$$

Clearly $S_3(X) = 1$, because each of Alice's trits is completely random.

It can be verified that $S_3(E) = -\sum \lambda_i \log_3 \lambda_i$, because the register E is a purification of AB, and thus its state has the same entropy as the state of AB, which has diagonal elements $\lambda_0, \ldots, \lambda_8$.

To evaluate $H_3(X|Y)$ we first note that $H_3(X|Y)$ depends only on the error amounts Q and q,

in the following way:

$$
\begin{aligned}
& H_3(X|Y) && (4.62)\\
& \leq \; -((1-q)(1-Q)+Qq/2)\log_3((1-q)(1-Q)+Qq/2) && (4.63)\\
& - \; 2((1-q)Q/2+(1-Q)q/2+Qq/4)\log_3((1-q)Q/2+(1-Q)q/2+Qq/4). && (4.64)
\end{aligned}
$$

To understand this inequality we note that given the result of Bob's measurement of a specific coordinate of Y, his uncertainty of the outcome of Alice for the same coordinate depends on whether there was an error caused by Eve (this happens with probability Q) or an error caused by Alice (with probability q), or both, or there was no error at all. Given a specific value for Bob's outcome, 0,1 or 2, the probability for Alice to have the same value is $\Pr(\textit{same value}) = (1-q)(1-Q)+Qq/2$, because it can happen either in the case of no error at all, or in the case when there are two errors cancelling each other. The probability to get any one of the other two possible logical values in Alice's coordinate is, in the worst case as far as Bob is concerned, i.e assuming that the two possibilities for an error are equally likely, $1/2(1-\Pr(\textit{same value}))$. This expression equals $(1-q)Q/2+(1-Q)q/2+Qq/4$. The reason why the case of equally likely errors is an upper bound on $H_3(X|Y)$ is that the closer the distribution $\Pr(X|Y)$ to uniform, the higher its entropy.

We can also express $S(E|X)$ as

$$
\begin{aligned}
& S(E|X) = && (4.65)\\
& = \; \frac{1}{3}S((1-q)\sigma_E^0+\frac{1}{2}q\sigma_E^1+\frac{1}{2}q\sigma_E^2) && (4.66)\\
& + \; \frac{1}{3}S(\frac{1}{2}q\sigma_E^0+(1-q)\sigma_E^1+\frac{1}{2}q\sigma_E^2) && (4.67)\\
& + \; \frac{1}{3}S(\frac{1}{2}q\sigma_E^0+\frac{1}{2}q\sigma_E^1+(1-q)\sigma_E^2). && (4.68)
\end{aligned}
$$

To understand this equality notice that given a specific value for Alice's coordinte, say 0, the state of Eve is a mixture of the state that correspond to no error, i.e. σ_E^0, with probability $1-q$, and the states that correstpond to an error, i.e. σ_E^1 and σ_E^2, with equal probabilities $q/2$. Similarly, for logical values 1 and 2 we get $\frac{1}{2}q\sigma_E^0+(1-q)\sigma_E^1+\frac{1}{2}q\sigma_E^2$ and $\frac{1}{2}q\sigma_E^0+\frac{1}{2}q\sigma_E^1+(1-q)\sigma_E^2$, respectively.

Therefore, to evaluate $S(E|X)$ we need to compute the entropies of each of the three density matrices appearing in the expression for $S(E|X)$. For example, the matrix $(1-q)\sigma_E^0+\frac{1}{2}q\sigma_E^1+\frac{1}{2}q\sigma_E^2$ has the form (when expressed in the basis $\{|\nu_i\rangle\}$)

$$\begin{pmatrix}
\lambda_1 & 0 & 0 & z\sqrt{\lambda_1\lambda_4} & 0 & 0 & z\sqrt{\lambda_1\lambda_7} & 0 & 0 \\
0 & \lambda_2 & 0 & 0 & z\sqrt{\lambda_2\lambda_5} & 0 & 0 & z\sqrt{\lambda_2\lambda_8} & 0 \\
0 & 0 & \lambda_3 & 0 & 0 & z\sqrt{\lambda_3\lambda_6} & 0 & 0 & z\sqrt{\lambda_3\lambda_9} \\
z\sqrt{\lambda_1\lambda_4} & 0 & 0 & \lambda_4 & 0 & 0 & z\sqrt{\lambda_4\lambda_7} & 0 & 0 \\
0 & z\sqrt{\lambda_2\lambda_5} & 0 & 0 & \lambda_5 & 0 & 0 & z\sqrt{\lambda_5\lambda_8} & 0 \\
0 & 0 & z\sqrt{\lambda_3\lambda_6} & 0 & 0 & \lambda_6 & 0 & 0 & z\sqrt{\lambda_6\lambda_9} \\
z\sqrt{\lambda_1\lambda_7} & 0 & 0 & z\sqrt{\lambda_4\lambda_7} & 0 & 0 & \lambda_7 & 0 & 0 \\
0 & z\sqrt{\lambda_2\lambda_8} & 0 & 0 & z\sqrt{\lambda_5\lambda_8} & 0 & 0 & \lambda_8 & 0 \\
0 & 0 & z\sqrt{\lambda_3\lambda_9} & 0 & 0 & z\sqrt{\lambda_6\lambda_9} & 0 & 0 & \lambda_9
\end{pmatrix},$$

where we substitute $z = 1 - 3q/2$. The other two have similar structure, and all three have the same set of eigenvalues, and thus same entropy to all three of them. Software tools (such as the cvxopt library [1] of the Python programming language) can be employed to find the eigenvalues, and in particular the entropy.

Together with the constraints (4.42) to (4.45) we obtain a convex optimization problem which can be solved numerically. We used the cvxopt library [1] of the Python programming language to solve this optimization problem.

The analysis of the 4MUB protocol follows the same lines as the Fourier protocol. The protocol uses four bases, and so the expression for the symmetrization $\mathcal{D}$ (Eq. 4.36) has now four terms in it. Denote by F_1, F_2, F_3 the unitary transformations taking the standard basis to the second, third and fourth bases of the 4MUB (Section 4.1.3), respectively. In analogy to Equation (4.36) we now have

$$\begin{aligned}
\mathcal{D}(\sigma_{AB}) = & && (4.69)\\
&= \frac{1}{4}\sigma_{AB} + \frac{1}{4}(F_1^\dagger \otimes F_1)\sigma_{AB}(F_1 \otimes F_1^\dagger) && (4.70)\\
&+ \frac{1}{4}(F_2 \otimes F_3)\sigma_{AB}(F_2^\dagger \otimes F_3^\dagger) + \frac{1}{4}(F_3 \otimes F_2)\sigma_{AB}(F_3^\dagger \otimes F_2^\dagger). && (4.71)
\end{aligned}$$

At the parameter estimation phase of the protocol Alice and Bob decide randomly which of the four possible measurements to apply. This is equivalent to an application of the operator $\mathcal{D}$ followed by a measurement in the standard basis. One can verify that the states that contribute to the error counts in each of the four possible measurements are:

(4.13) , (4.14) , (4.16) , (4.17) , (4.19) , (4.20) in the case of $I \otimes I$,
(4.15) , (4.16) , (4.17) , (4.18) , (4.19) , (4.20) in the case of $F_1^\dagger \otimes F_1$,
(4.13) , (4.14) , (4.15) , (4.17) , (4.18) , (4.19) in the case of $F_3 \otimes F_4$ and
(4.13) , (4.14) , (4.15) , (4.16) , (4.18) , (4.20) in the case of $F_4 \otimes F_3$.

The effect of the symmetrization $\mathcal{D}$ is to symmetrize the error probability with respect to each of the bases of the protocol. This means that in each of the measurement bases (four bases in the case of the 4MUB protocol, and two bases in the case of the Umbrella protocol) separately the error is the same, and equals Q.

Thus, with analogy to Equation (4.41) we get after symmetrization with $\mathcal{D}$

$$\lambda_1 + \lambda_2 + \lambda_4 + \lambda_5 + \lambda_7 + \lambda_8 = \tag{4.72}$$
$$\lambda_3 + \lambda_4 + \lambda_5 + \lambda_6 + \lambda_7 + \lambda_8 = \tag{4.73}$$
$$\lambda_1 + \lambda_2 + \lambda_3 + \lambda_5 + \lambda_6 + \lambda_7 = \tag{4.74}$$
$$\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 + \lambda_6 + \lambda_8. \tag{4.75}$$

The total error probability, as estimated with the parameter estimation phase of the protocol, is therefore

$$\begin{aligned}
&\frac{1}{4}(\lambda_1 + \lambda_2 + \lambda_4 + \lambda_5 + \lambda_7 + \lambda_8) \quad + \\
&\frac{1}{4}(\lambda_3 + \lambda_4 + \lambda_5 + \lambda_6 + \lambda_7 + \lambda_8) \quad + \\
&\frac{1}{4}(\lambda_1 + \lambda_2 + \lambda_3 + \lambda_5 + \lambda_6 + \lambda_7) \quad + \\
&\frac{1}{4}(\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 + \lambda_6 + \lambda_8) \quad .
\end{aligned}$$

As a result we arrive at four constraints, two of which already existed in the analysis of the Fourier porotcol. The two additional constraints contributed by the two additional bases of the four mutually unbiased bases are

$$\lambda_1 + \lambda_5 + \lambda_6 + \lambda_2 + \lambda_3 + \lambda_7 = Q \tag{4.76}$$
$$\lambda_2 + \lambda_4 + \lambda_6 + \lambda_1 + \lambda_3 + \lambda_8 = Q. \tag{4.77}$$

To see why $\mathcal{D}$ symmetrizes (equalizes) of the errors in the different bases, we note that as with the operator $F_1^\dagger \otimes F_1$ (4.37), each of the other two operators appearing in (4.69) (excluding the

identity operator), $F_2 \otimes F_3$ and $F_3 \otimes F_2$, is a permutation operator in the basis (4.11). Examining these permutations, with analogy to (4.39),(4.40),(4.40), we see that each of the diagonal elements of the state $\mathcal{D}(\Lambda(\sigma_{AB}))$, which is diagonal in the basis (4.11), is a sum of four diagonal elements of $\Lambda(\sigma_{AB})$. One can verify that the diagonal elements of $\mathcal{D}(\Lambda(\sigma_{AB}))$, $\lambda_0, \ldots, \lambda_8$, satisfy Equations (4.72),...,(4.74).

We saw that each measurement basis has a different set of λs that cause errors, and this is why we get a total of 4 constraints; just like with the Fourier protocol, each basis contributes one constraint to our set of constraints.

The results of our analysis are summarized in Figure 4.3. It shows the key rate, as a function of the error rate, in the case of three different protocols: the six-state protocol (lower curve), the umbrella protocol (middle curve) and the 4MUB protocol (upper curve). For each of these protocols the figure shows the critical value of error-rate, i.e. the amount of error above which the key-rate goes below zero. This critical value is 14.1% for the six-state protocol, 17.7% for the umbrella protocol and 21.1% for the 4MUB protocol. A lower bound on the critical value for the BB84 protocol is also known [57], to be 12.4%.

Figure 4.3: Lower bounds on the secret-key rate of the six-state protocol (3x2), the Umbrella protocol (2x3) and the 4MUB protocol (4x3), as a function of the error Q induced by Eve. The dashed lines represent the results without introducing of additional error by Alice. The full lines show the improved results obtained with the introduction of additional error.

Part IV

Conclusions and Open Questions

Quantum public keys.

Quantum public key cryptography is far from being fully explored. The notion of a quantum public key was shown useful in a few settings, like digital signatures and like network anonymity, and it is likely that other potential uses for cryptography will be discovered with time.

In this thesis I presented three protocols for quantum public key encryption - the random access code protocol, the modified random access code protocol, and the oblivious rotations protocol. These protocols can be used for secure communication. The protocols are secure from an information theoretic point of view, unlike the classical public key counterpart. They also have the important property of symmetry (which means that a public key is indeed *public*).

Each of the protocols starts with a session for distribution of the quantum public keys. Unlike common classical public key schemes, some information might leak to an eavesdropper who interacts with the quantum keys during the distribution session. Another possible flaw which does not exist in the classical counterpart, is the ability of the dealer to create non-identical copies of the key. This in some circumstances enables him to later apply various quantum cheating strategies. To deal with these two threats I described a generic testing phase, which consists of many repetitions of the original key distribution session, where most of the keys generated this way are used for testing, and at the end only one of them is kept for real use. It might very well be possible that there is a more efficient way for testing than the way described here, and this point is left for further research.

Unlike common quantum (private) key distribution protocols, which are very simple, and which are implementable using nowaday's technology, the quantum public key protocols are much more complex. They require quantum computational ability, and sometimes even the ability to maintain a large system in an entangled state for a long period of time. It is an interesting open question whether there is a more simple way to do quantum public key cryptography.

A quantum public key is a one time pad. This seems to be unavoidable because of the way it is used for encryption. Either it is measured and thus the coherence is lost, or the quantum system is manipulated and then sent back to the dealer. In either case, due to the no-cloning principle, the key can be used only once. This is a major disadvantage compared to a classical public key.

Another disadvantage of the quantum version of a public key is that the key must be at least as long as the cleartext. It is an open question whether it is possible to have a shorter key, and

still get information theoretic security.

In this thesis I only discussed public key schemes with unconditional security. It would be interesting to define quantum schemes which are computationally secure, with various assumptions on the computational power of the adversary. This, of course, will require a better knowledge of quantum complexity - a field which is still at its infancy.

The subject of network anonymity is brought in this thesis as a natural use of quantum public keys. I showed how to use quantum public keys to construct an anonymous network with information theoretic privacy and anonymity. The construction is efficient - it requires only polylogarithmic rounds per message delivery, and only polylogarithmic communication per message, in a model where the adversary controls an arbitrary fraction of the communication links in the network. It remains an open question to determine the relation of key length and message length for one of the protocols presented in this thesis - the MRAC protocol. It also remains as an open question to determine the optimal general relation of key length to message length in an arbitrary quantum public key scheme.

I also describe a classical construction of a network with information theoretic privacy and anonymity, which is based on an improvement of Yuval Ishai to the idea of a DC-network by David Chaum. However, this construction is inefficient. It is a very interesting open problem to decide whether or not there is an efficient classical solution with an information theoretic security.

The solution given here for the anonymous network problem is in the model of the *active* adversary, who can initiate his own messages, but cannot delete or alter messages initiated by others. The question of an anonymous network against a malicious adversary is still a very interesting open problem, awaiting resolution in both the computational and information theoretic settings.

Quantum private keys.

Quantum key distribution is one of the prominent achievements of quantum cryptography. Private key distribution is one of the simplest tasks in quantum information processing; efficient QKD can be done with nowaday's technology. For example, to realize qubits with photons, one only needs a

photon source and a photodetector to perform a QKD protocol such as BB84.

In this thesis I demonstrate that with essentially the same technological requirements one can perform QKD with qutrits instead of qubits. Moreover, if qutrits are realized with bi-photons I present such a simple protocol, which can tolerate an error rate up to at least 17.7%, compared, for example, to an upper bound of 14.6% on the maximal error rate that the BB84 protocol tolerates, and to an upper bound of 16.3% for the six-state protocol [57].

The optimum error rate of a protocol is the maximum probability that Alice and Bob get disagreeing results in one coordinate of the raw key (averaged over all the coordinates), for which the key rate is still positive. When a quantum channel is used to communicate bi-photons it is reasonable to expect that the induced error rate would be different than in the case of single photons. It remains an open question to determine the exact relation of the error rate induced by the same channel, when it is used to communicate qutrits compared to qubits. In this respect we can remark that, on one hand, clearly bi-photons are expected to be more susceptible to noise than single photons. On the other hand we should take into consideration that usually the quantum channel noise, and the noise operators describing that noise, are limited to single photon operations. This may suggest that the induced error rate in the case of bi-photons can be the same as with single photons. In addition to that, if an error occurs to both photons of a bi-photon, then only one error is effectively counted. Moreover, an error in the channel can sometimes leave the state of a bi-photon unchanged; for example, if both photons in the Fock state $|11\rangle$ (i.e. one photon in vertical linear polarization and one in horizontal linear polarization) undergo a bit flip type error, the state remains $|11\rangle$.

An interesting direction for further research would be to extend the results presented in this thesis to dimensions higher than 3. In particular it would be interesting to find a complete theory of QKD with d-level systems, for general d, implemented with d-photons, with a restriction to single photon operations.

In this thesis I consider eavesdropping attacks on the communication channels, when the apparatus of Alice and Bob are assumed to be perfect (see [50]). Another interesting direction for further research is to see what happens to bi-photons QKD protocols, and to d-level systems in general, when more general eavesdropping attacks are considered. These can be of the form of *splitting* attacks (i.e when the eavesdropper tries to exploit the tendency of a laser to sometimes emit

pairs of polarized photons instead of one [60]), *trojan horse* attacks (i.e. when Alice's apparatus is prepared by Eve, or biased in some way known only to Eve [34]), etc. .

Bibliography

[1] http://abel.ee.ucla.edu/cvxopt.

[2] Masayuki Abe and Fumitaka Hoshino. Remarks on mix-network based on permutation networks. *Lecture Notes in Computer Science*, 1992:317–324, 2001.

[3] Dorit Aharonov, Amnon Ta-Shma, Umesh V. Vazirani, and Andrew C. Yao. Quantum bit escrow. In ACM, editor, *Proceedings of the thirty second annual ACM Symposium on Theory of Computing: Portland, Oregon, May 21–23, [2000]*, pages 705–714, 2000.

[4] Andris Ambainis, Ashwin Nayak, Ammon Ta-Shma, and Umesh Vazirani. Dense quantum coding and a lower bound for 1-way quantum automata. In ACM, editor, *Proceedings of the thirty-first annual ACM Symposium on Theory of Computing: Atlanta, Georgia, May 1–4, 1999*, pages 376–383, New York, NY, USA, 1999. ACM Press.

[5] D. Beaver, S. Micali, and P. Rogaway. The round complexity of secure protocols. In *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing*, pages 503–513, 1990.

[6] Donald Beaver. Multiparty protocols tolerating half faulty processors. In G. Brassard, editor, *Advances in Cryptology-CRYPTO '89*, volume 435 of Lecture Notes in Computer Science, pages 560–572. IACR, Springer Verlag, 1990, 20–24 August 1989.

[7] H. Bechmann-Pasquinucci and N. Gisin. *Phys. Rev. A*, 59:4238, 1999.

[8] H. Bechmann-Pasquinucci and A. Peres. Quantum cryptography with 3-state systems. *Physical review letters*, 85(15):3313, 2000.

[9] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing*, pages 1–10, May 2–4 1988.

[10] M. Ben-Or, M. Horodecki, D. Leung, D. Mayers, and J. Oppenheim. The universal composable security of quantum key distribution, 2004. arXive e-print quant-ph/0409078.

[11] M. Ben-Or and D. Mayers. General security definition and composability for quantum and classical protocols, 2004. arXive e-print quant-ph/0409062.

[12] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Physical review letters*, 68(21):3121–3124, 1992.

[13] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5(1):3–28, 1992.

[14] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41:1915–1923, 1995.

[15] C. H. Bennett, G. Brassard, and J. M. Robert. Privacy amplification by public discussion. *SIAM Journal on Computing*, 17:210–229, 1988.

[16] Charles .H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computer Systems and Signal Processing, Bangalore India*, pages 175–179, 1984. http://www.research.ibm.com/people/b/bennetc/bennettc198469790513.pdf.

[17] Ron Berman, Amos Fiat, and Amnon Ta-Shma. Provable unlinkability against traffic analysis. http://www.cs.tau.ac.il/~amnon/Papers/BFT.fc04.ps. To appear in the 8th International Conference on Financial cryptography (FC-04), 2004.

[18] E. Biham, M. Boyer, G. Brassard, J. van de Graaf, and T. Mor. Security of quantum key distribution against all collective attacks, 1998. arXive e-print quant-ph/9801022.

[19] P. Oscar Boykin. Information security and quantum mechanics: Security of quantum protocols, 2002. arXiv:0210194.

[20] G. Brassard and L. Salvail. Secret-key reconciliation by public discussions. In T. Helleseth, editor, *Lecture Notes in Computer Science: Advances in Cryptology – EUROCRYPT'93*, volume 765, pages 410–423. Springer Verlag, 1994.

[21] I. Bregman, D. Aharonov, M. Ben-Or, and H.S. Eisenberg. Simple and secure quantum key distribution with biphotons. arXive e-print quant-ph/0709.3804v2.

[22] D. Bruss. *Physical review letters*, 81:3018, 1998.

[23] H. Buhrman, M. Christandl, P. Hayden, H-K. Lo, and S. Wehner. On the (im)possibility of quantum string commitment, 2005. arXive e-print quant-ph/0504078.

[24] H. Buhrman, R. Cleve, J. Watrous, and R. De-Wolf. Quantum fingerprinting . *Phys. Rev. Lett. 87*, page 167902, 2001.

[25] A.V. Burlakov, L.A. Krivitskiy, S.P. Kulik, G.A. Maslennikov, and M.V. Chekhova. Measurement of qutrits, 1996. arXive e-print quant-ph/0207096.

[26] C. Cachin and U. M. Maurer. Linking information reconciliation and privacy amplification. *Journal of Cryptology*, 10:97–110, 1997.

[27] A. R. Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54:1098, 1996.

[28] David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Thesis (M.S. in Computer Science), University of California, Berkeley, Berkeley, CA, USA, June 1979.

[29] David Chaum. The Dining Cryptographers Problem: Unconditional sender and recipient untraceability. *Journal of Cryptology*, 1(1):65–75, 1988.

[30] David Chaum, Claude Crepeau, and Ivan Damgård. Multiparty unconditional secure protocols. In *Proceedings of the 20th Annual Symposium on Theory of Computing (STOC)*, pages 11–19, Chicago, IL USA, May 1988. ACM Press.

[31] Hannes Federrath, editor. *Designing Privacy Enhancing Technologies, International Workshop on Design Issues in Anonymity and Unobservability, Berkeley, CA, USA, July 25-26, 2000, Proceedings*, volume 2009 of *Lecture Notes in Computer Science*. Springer, 2001.

[32] C.A. Fuchs and J. van de Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Transactions on Information Theory*, 45(4):1216–1227, 1999.

[33] Joseph Fitzsimons Sebastien Gambs Alain Tapp Gilles Brassard, Anne Broadbent. Anonymous quantum communication, 2007. arXiv:0706.2356.

[34] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy. Trojan horse attacks on quantum key distribution systems. *arXiv:quant-ph/0507063*, 2005.

[35] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game or a completeness theorem for protocols with honest majority. In *Proceedings of the 19th Annual ACM Symposium on Theory of Computing*, pages 218–229, 1987.

[36] Daniel Gottesman and Isaac Chuang. Quantum digital signatures, 2001. http://www.citebase.org/abstract?id=oai:arXiv.org:quant-ph/0105032.

[37] Daniel Gottesman and Hoi-Kwong Lo. Proof of security of quantum key distribution with two-way classical communications. *IEEE Transactions on Information Theory*, 49:457–475, 2003.

[38] John C. Howell, Antia Lamas-Linares, and Dik Bouwmeester. Experimental violation of a spin-1 bell inequality using maximally entangled four-photon states. *Phys. Rev. Lett.*, 88(3):030401, Jan 2002.

[39] Yuval Ishai, 2004. private communications.

[40] I. D. Ivanovic. Geometrical description of quantum state determination. *Journal of Physics A*, 14(12):3241–3245, 1981.

[41] R. Jozsa. Fidelity for mixed quantum states. *Journal of Modern Optics*, 41(12):2315–2323, 1994.

[42] A. Kent. Quantum bit string commitment. *Phys. Rev. Lett. 90*, page 237901, 2003.

[43] Oliver Kern and Joseph M. Renes. Improved one-way rates for bb84 and 6-state protocols, 2007. arXiv:0712.1494v1.

[44] Hoi-Kwong Lo and H. F. Chau. Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica D*, 120:177–187, 1998. see also quant-ph/9711065.

[45] Hoi-Kwong Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283:2050–2056, 1999.

[46] A. Mair, A. Vaziri, G. Weihs, , and A. Zeilinger. Entanglement of the orbital angular momentum states of photons. *Nature*, 412:313 – 316, Jul 2001.

[47] Stephanie Wehner Matthias Christandl. Quantum anonymous transmissions, 2004. arXiv:0409201.

[48] D. Mayers. Unconditional security in quantum cryptography, 1998. arXive e-print quant-ph/9802025.

[49] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical review letters*, 78:3414–3417, 1997.

[50] Dominic Mayers and Andrew Yao. Quantum cryptography with imperfect apparatus. *arXiv:quant-ph/9809039*, 1998.

[51] Ashwin Nayak. Optimal lower bounds for quantum automata and random access codes. In IEEE, editor, *40th Annual Symposium on Foundations of Computer Science*, pages 369–376, 1999.

[52] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge, 2000.

[53] T. Rabin and M. Ben-Or. Verifiable secret sharing and multiparty protocols with honest majority. In *Proceedings of the 21st Annual ACM Symposium on Theory of Computing*, pages 73–85, 1989.

[54] Charles Rackoff and Daniel R. Simon. Cryptographic defense against traffic analysis. In *Proceedings of the Twenty-Fifth Annual ACM Symposium on the Theory of Computing*, pages 672–681, San Diego, California, 16–18 May 1993.

[55] Jean-François Raymond. Traffic analysis: Protocols, attacks, design issues, and open problems. *Lecture Notes in Computer Science*, 2009:10–29, 2001.

[56] Michael K. Reiter and Aviel D. Rubin. Crowds: anonymity for Web transactions. *ACM Transactions on Information and System Security*, 1(1):66–92, November 1998.

[57] R. Renner, N. Gisin, and B. Kraus. Lower and upper bounds on the secret key rate for qkd protocols using one–way classical communication. *Physical review letters*, 95:080501, 2003.

[58] R. Renner and R. Konig. Universally composable privacy amplification against quantum adversaries, 2004. arXive e-print quant-ph/0403133v2.

[59] R. Rivest, A. Shamir, and L. Adlemen. A method for obtaining digital signatures and public-key cryptosystems. *Comm. Assoc. Comput. Mach. 21*, pages 120–126, 1978.

[60] V. Scarani, A. Acin, G. Ribordy, and N. Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulses implementations. *Physical review letters*, 92:057901, 2004.

[61] Peter Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comp. 26*, 5:1484–1509, 1997.

[62] Peter W. Shor and John Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441–444, 2000. Comment: 5 pages, Latex, minor changes to improve clarity and fix typos.

[63] Graeme Smith, Joseph M. Renes, and John A. Smolin. Better codes for bb84 with one-way post-processing, 2006. arXiv:quant-ph/0607018v1.

[64] Kiyoshi Tamaki, Masato Koashi, and Nobuyuki Imoto. Unconditionally secure key distribution based on two nonorthogonal states. *Physical review letters*, 90:167904, 2003.

[65] W. Tittel and G. Weihs. Photonic entanglement for fundamental tests and quantum communication. *Quantum Inf. Comput.*, 1(2):3–56, 2001.

[66] A. Uhlmann. The 'transition probability' in the state space of a $*$-algebra. *Reports on Mathematical Physics*, 9:273–279, 1976.

[67] W. K. Wootters and B. D. Fields. Optimal statedetermination by mutually unbiased measurements. *Annals of Physics*, 192(2):363–381, 1989.

[68] Marek Zukowski, Anton Zeilinger, and Michael A. Horne. Realizable higher-dimensional two-particle entanglements via multiport beam splitters. *Phys. Rev. A*, 55(4):2564–2579, Apr 1997.