On the Security of Theoretical and Realistic Quantum Key Distribution Schemes

Research Thesis

Ran Gelles
On the Security of Theoretical and Realistic Quantum Key Distribution Schemes

Research Thesis

In Partial Fulfillment of The Requirements for the Degree of Master of Science in Computer Science

Ran Gelles

Submitted to the Senate of the Technion – Israel Institute of Technology
Elul 5768, Haifa, September 2008
We have a habit in writing articles published in scientific journals to make the work as finished as possible, to cover up all the tracks, to not worry about the blind alleys or describe how you had the wrong idea first, and so on. So there isn’t any place to publish, in a dignified manner, what you actually did in order to get to do the work.

Richard P. Faynman

The research thesis was done under the supervision of Assoc. Prof. Tal Mor in the Computer Science Department.

I would like to thank my advisor, Assoc. Prof. Tal Mor, for expecting me not less than the best, and demanding me to excel. I would like to address a special thanks to Assoc. Prof. Michel Boyer for many fruitful discussions, suggestions and comments.

I would like also to thank Dan Kenigsberg, Yossi Weinstein, Yuval Elias, Matty Katz and Eli Biham. All were very keen to help in whatever needed, whether it is a mathematical assistance, \LaTeX{} help or a small-talk recess. The Internet should be thanked as well, for the very same reason...

Finally, I would like to thank my family, just for being my family.
Contents

List Of Figures vi

List Of Tables vii

Abstract 1

1 Introduction 3

1.1 Quantum Information Processing Essentials 3
1.1.1 Qubits and systems 3
1.1.2 Operations 4
1.1.3 Measurements 5
1.2 The Fock Space 5
1.2.1 Fock states 5
1.2.2 A photonic “qubit” 6
1.3 Key Distribution 7
1.3.1 Methods for secure key distribution 7
1.3.2 Modern (classical) key-distribution protocols 8
1.3.3 Quantum key-distribution protocols 9
1.4 Attacks on Quantum Key Distribution 11
1.5 Security Proofs 13
1.5.1 Working assumptions 13
1.5.2 Security proofs criteria 13
1.5.3 Known security proofs 14
1.6 Structure of Dissertation 15

2 Quantum Space Attacks 17

2.1 Introduction 17
2.2 Preliminaries 18
2.2.1 Properties of Hilbert spaces 18
2.2.2 Hilbert-state notations for Fock-states 20
## 2.3 The Quantum Space of the Protocol
- 2.3.1 Alice’s realistic space
- 2.3.2 Extension of Alice’s space
- 2.3.3 Bob’s space
- 2.3.4 The quantum space of the protocol

## 2.4 The Quantum Space Attack
- 2.4.1 Eavesdropping on the quantum space of the protocol
- 2.4.2 The QSoP is the effective attack space

## 2.5 A QSA Example

## 2.6 Known QKD Attacks as QSAs
- 2.6.1 The photon number splitting attack [21]
- 2.6.2 The tagging attack (based on [38])
- 2.6.3 The Trojan-pony attack [38, 45]
- 2.6.4 The fake-state attack (based on [56, 55])

## 2.7 Concluding Remarks

## 3 Analysis of Interferometric QKD Schemes

### 3.1 Introduction

### 3.2 Model of the Equipment Used
- 3.2.1 Beam splitter
- 3.2.2 Phase shifter
- 3.2.3 Evolution of a single mode in an interferometer
- 3.2.4 Evolution of two modes in an interferometer
- 3.2.5 Detectors and Measurement

### 3.3 Description of Interferometric-based QKD Schemes
- 3.3.1 Variant A: The BB84 protocol with $x$ and $y$ bases
- 3.3.2 Variant B: Protocols that uses the $z$-basis
- 3.3.3 Variant C: “Unified” implementation for the $z$-basis

### 3.4 Robustness of Protocols: Definition and Discussion
- 3.4.1 The robustness definitions
- 3.4.2 The relations between errors and losses
- 3.4.3 Conditions for zero-error attacks

### 3.5 Robustness Proof of Interferometric BB84
- 3.5.1 Robustness proof of Variant A against a limited adversary
- 3.5.2 Robustness proof of Variant B against a limited adversary
- 3.5.3 Robustness of Variant A against a more realistic Eve

### 3.6 Robustness Analysis of Variant C
- 3.6.1 Robustness proof for Variant C1 against a limited adversary
3.6.2 The “Reversed-Space Attack”: A complete non robustness proof for
Variant C2 ................................................. 62
3.7 Conclusion .................................................. 64

4 Security of BB84 against Collective Attacks 65
4.1 Introduction ................................................. 65
4.1.1 Notations ................................................. 65
4.1.2 The BB84 protocol ....................................... 66
4.2 Description of Eve’s Attack and its Properties ............ 67
4.2.1 Eve’s attack ............................................ 67
4.2.2 Extending the attack to multiple qubits ................. 68
4.2.3 The probability of error .................................. 68
4.2.4 The probability of error in the conjugate basis .......... 68
4.2.5 Flat attacks ............................................. 69
4.2.6 A purification ........................................... 71
4.3 Security Proof of BB84 against collective attacks ........ 71
4.3.1 Notations and distinguishability .......................... 71
4.3.2 Representing states for bitstrings ......................... 72
4.3.3 Case of a one-bit key .................................... 73
4.3.4 Calculating and bounding the trace norm for one bit: the Biham
basis. ......................................................... 74
4.3.5 Bounding Eve’s accessible information .................... 78
4.3.6 Proof of security ........................................ 80
4.3.7 Reliability ............................................... 81
4.4 Conclusion .................................................. 81

5 Quantum Key Distribution with Classical Bob 83
5.1 Introduction ................................................. 83
5.2 Security and Robustness .................................... 84
5.3 Mock Protocol and its Complete Nonrobustness ........... 85
5.4 Two Semi-Quantum Key Distribution Protocols .......... 86
5.4.1 Protocol 1: Based on randomizing the returned qubits .. 87
5.4.2 Protocol 2: Based on returning all the qubits ............ 88
5.4.3 The classical step ....................................... 89
5.5 Proofs of Robustness ....................................... 89
5.5.1 Complete robustness of Protocol 2 ......................... 89
5.5.2 Partial robustness of Protocol 1 ......................... 93
5.5.3 Properties of Protocol 1’ ................................ 100
5.5.4 Complete robustness of Protocol 1’ ....................... 102
List of Figures

2.1 The photon number probability distribution for a source with $\alpha = 0.1$  
2.2 Bob’s setup: a rotating mirror (RM) chooses the appropriate detectors 
    according to the desired basis. The left side plots the detectors efficiency 
    of the $x$ and $z$ measurement setup, with respect to time. The efficiencies 
    do not fully overlap which allows times that are measured only by a single 
    chosen basis  
3.1 An interferometer built out of two symmetric beam splitters, and a $\phi$ phase 
    shifter placed on the long arm of the interferometer.  
3.2 A symmetric beam-splitter. Two input modes (1) and (2) and two output 
    modes (3) and (4).  
3.3 Evolution in time of a single mode in an interferometer  
3.4 Evolution in time of two modes in an interferometer  
3.5 Bob’s Laboratory setup for the $x$ and $y$ bases. (a) Alice’s qubit; (b) ancilla 
    modes each in a vacuum state; (c), (d) beam-splitters; (e) phase shifter $P_\phi$ 
    is set to $\phi = 0$ for the $x$ basis or to $\phi = \pi/2$ for for the $y$ basis; (f) Bob’s 
    detectors measure time $t_1$.  
3.6 Bob’s Laboratory setup for the $z$ basis.  
5.1 (a) Eve’s maximum (over all attacks) information on the INFO string vs. the 
    allowed disturbance on the bits tested by Alice and Bob, in a completely ro- 
    bust (solid line), partly robust (dashed), and completely nonrobust (densely 
    dotted) protocol. (b) Robustness should not be confused with security; 
    Eve’s maximum information on the final key vs. allowed disturbance in a 
    secure protocol; such a protocol could be completely or partly robust.
List of Tables

3.1 Eve’s un-normalized states according the state sent by Alice . . . . . . . 63
5.1 Bit usage summary . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 88
Abstract

Quantum information processing is a relatively new computer-science field dealing with “quantum-protocols” and “quantum-computers” that are based on quantum mechanics laws. The quantum computer extends the regular computing models (e.g. the classical Turing Machine) by allowing the computer to perform any physically valid operation (e.g., performing any unitary transformation on its inputs and registers, performing any measurement as defined by the postulates of the quantum mechanics, etc.). New quantum protocols and algorithms, that enjoy the advantage of this quantum power, were defined as a result of this new model.

In 1984, Bennett and Brassard invented the BB84 Quantum Key Distribution (QKD) protocol [7], a new method of agreeing on a secret key using quantum systems. Their new concept led to many other QKD schemes. The security of those QKD schemes has been investigated by many researchers. Security proofs of the BB84 protocol were obtained, against the collective attack, and against the most general attack — the joint attack. In addition, robustness proofs were obtained for protocols that are more complicated than the ideal BB84. Robustness is usually weaker than full security, but is more simple to achieve. This research focuses on the broad field of QKD security, from several different, yet related, points of view.

Theoretical QKD protocols commonly rely on the use of qubits (quantum bits). In reality, however, due to practical limitations, the legitimate users are forced to employ a larger quantum (Hilbert) space, say a quhexit (quantum six-dimensional) space [21], or even a much larger quantum Hilbert space. Various attacks exploit these limitations. Although security can still be proved in some very special cases, a general framework that considers such realistic QKD protocols, as well as attacks on such protocols, is still missing.

We describe a general method of attacking realistic QKD protocols, which we call the ‘quantum-space attack’. The description is based on assessing the enlarged quantum space actually used by a protocol, the ‘quantum space of the protocol’. We show that this space is the effective space needed for attacking a protocol, hence this is the space needed for a general security analysis of the protocol. Analyzing a larger space will only add complexity.
to the analysis, while analyzing a smaller space might miss possible attacks.

The new method of analyzing the security of practical QKD scheme via the enlarged quantum space of the protocol, is demonstrated for schemes in which the qubits are implemented by photons. This demonstration is highly relevant since many of the practical QKD systems nowadays are implemented via photons. Photonic QKD schemes are commonly implemented using a device named interferometer. The structure of such an interferometer inevitably causes the enlargement of the quantum space in use (for instance, by adding vacuum ancillas). This enlargement exposes the protocols to new kinds of attacks that have not yet been analyzed.

We consider several QKD protocols that are implemented using interferometers. We analyze the enlarged space actually in use and define the requirements for their robustness. While we prove that the common interferometric protocol implementation is robust against simple attacks, we also demonstrate the difficulty of proving its robustness against stronger attacks. We finally present an interferometric-QKD implementation variant that is found to be non robust and therefore totally insecure.

The ultimate goal of QKD is to have practical protocols that are proven secure. A full security proof means security against the most general quantum space attack, namely, the joint attack performed onto the quantum space of the protocol. As providing such a proof is very difficult (maybe even impossible), it is important to analyze less general security results such as security against the collective attack and robustness against the joint attack.

Here we also improve the non-optimal security proof of ideal BB84 against the collective attack (for theoretical QKD) [11] to the standards of the joint attack. We prove an exponential advantage relative to the bound reached in [11] for the collective attack. This is done by using the powerful tools developed in [10] for proving security against the joint attack. Nevertheless, our proof is maintained simple since it deals with collective attacks and not with joint attacks. This simple proof might be useful for future analysis of other quantum cryptographic protocols, or of more realistic models of QKD schemes.

The last topic of this research regards the QKD scheme in which Alice is “quantum” yet Bob is “classical”, as recently published by Boyer, Kenigsberg and Mor [18, 19, 49]. Here we analyze two protocols with this constraint, and prove their robustness: we show that any adversary attempt to obtain information (even a tiny amount of information), necessarily induces some errors that the legitimate users could notice. The first protocol is the one presented in [19], with an improved robustness proof, that is applicable to other scheme configurations, such as sending the qubits one by one. The second protocol is based on the one presented in [18], yet we extend and generalize it, remove several of its limitations, and prove its robustness.
Chapter 1

Introduction

Quantum information processing (QIP), a computer-science field based on quantum mechanics is a true breakthrough, generalizing computer capabilities, as we understand them today. This field introduces us with new efficient algorithms for problems that are considered hard to solve using classical computers, such as factoring large numbers or searching un-sorted databases. Quantum computers are a real threat to classical cryptography: faster searching quantum-algorithms can bruteforce symmetric-encryption systems in order to find their keys, while efficient factoring quantum-algorithms are capable of breaking encryption systems (and other types of security-systems) based on public key technology.

However, QIP also contributes cryptographic tools [86]. New quantum-cryptography algorithms and protocols based on the idea that quantum information cannot be duplicated, are defined and researched. In 1984, Bennett and Brassard invented the BB84 quantum key distribution protocol [7], which gave a new method of agreeing on a secret key using “the quantum power” in order to achieve security in the sense of information theory (as opposed to ‘computational security’, which could be broken by a powerful enough enemy, who has unlimited computation power). This innovative protocol has actually initiated a new field: the quantum cryptography.

1.1 Quantum Information Processing Essentials

In order to explore the capability of quantum algorithms and protocols, we must first define the rules and borderlines of the quantum world. All these are defined by the quantum mechanics theory. See [63] for a detailed explanation of Quantum information processing theory.

1.1.1 Qubits and systems

The basic element of QIP is the quantum substitute of the classical bit — the qubit. While the classical bit can be in one of two possible states (0 and 1), the qubit can be in one of the states $|0\rangle$ and $|1\rangle$ as well as any superposition of those states. Mathematically, a qubit
can be defined as a unit vector $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ over the two-dimensional Hilbert space $\mathcal{H}_2$ [67, Chapter II]. The states

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

span a basis of $\mathcal{H}_2$ which is commonly referred to as the computational basis. One can define an $n$-qubits state $|\Psi\rangle = |\psi_1\rangle \otimes \ldots \otimes |\psi_n\rangle$ over the space

$$\mathcal{H}_2^\otimes n \triangleq \mathcal{H}_2 \otimes \mathcal{H}_2 \ldots \otimes \mathcal{H}_2,$$

where the state of the $i$-th qubit is $|\psi_i\rangle$.

There is no restriction on using a two-dimensional Hilbert space in order to represent a quantum system. A generalization of the above qubit, is the qudit defined as a unit vector over a $d$-dimensional Hilbert Space $\mathcal{H}_d$. We denote with $\mathcal{H}$ a general Hilbert space with a finite or an infinite dimension.

If a given system is in state $|\psi_i\rangle$ with probability $p_i$, we can describe the system using a density matrix

$$\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i|.$$ (1.1)

It follows that a system in a state $|\psi\rangle$ can be described as $\rho = |\psi\rangle \langle \psi|$. This notation is more convenient in several cases.

### 1.1.2 Operations

Quantum Mechanics defines the way to manipulate states. The state $|\psi\rangle$ can be transformed into the state $U|\psi\rangle$ for any unitary transformation $U$. A transformation $U$ is said to be unitary if

$$U^\dagger U = UU^\dagger = I.$$ (1.2)

A unitary $U$ defines an isomorphism on the Hilbert space, having the inverse transformation $U^\dagger$. Such transformation can be considered as “rotating” the state in the space by a fixed rotation, i.e. it does not change the state norm $\|\psi\| = \|U|\psi\|$, and it does not change the relations (i.e. the overlap [63]) of any two transformed states,

$$\langle U\phi|U\psi \rangle = \langle \phi|U^\dagger U|\psi \rangle = \langle \phi|I|\psi \rangle = \langle \phi|\psi \rangle.$$ (1.3)

Thus, $U$ is merely a basis change. Let $\{|\phi_i\rangle\}$ be an orthonormal basis of $\mathcal{H}$. The set $\{|\varphi_i\rangle = U|\phi_i\rangle\}$ is an orthonormal basis as well, and $U$ can be considered as changing the basis from $|\phi_i\rangle$ to $|\varphi_i\rangle$, and can be written as $U = \sum_i |\varphi_i\rangle \langle \phi_i|$. 
1.1.3 Measurements

Quantum Mechanics defines measurements of observables. An observable \( A \) is an Hermitian operator, satisfying \( A^\dagger = A \). Any Hermitian operator \( A \) can be diagonalized with respect to some orthonormal basis of the space \( \mathcal{H} \) it is defined upon [63, Theorem 2.1]. Therefore the operator \( A \) can be written as

\[
A = \sum_i \lambda_i |\phi_i\rangle \langle \phi_i|
\]  

(1.4)

where \( |\phi_i\rangle \) is the diagonalizing orthonormal basis. Measuring the state \( |\psi\rangle \) using the observable \( A \) results with the eigenvalue \( \lambda_i \) with probability \( p_i = |\langle \phi_i|\psi\rangle|^2 \).

Let us explicitly define measurements of several specific cases. Given a Hilbert space \( \mathcal{H} \) with an orthonormal basis \( |\phi_i\rangle \) for \( i = 1 \ldots \text{dim} \mathcal{H} \), a complete measurement of the state \( |\psi\rangle = \sum_i \alpha_i |\phi_i\rangle \) yields the output \( i \) with probability \( p_i = |\alpha_i|^2 = |\langle \phi_i|\psi\rangle|^2 \). [This corresponds to having an observable \( A \) with eigenvalues \( \lambda_i = i \) corresponding to the eigenstates \( |\phi_i\rangle \)].

The measurement process can be defined via a set of \( M = \text{dim} \mathcal{H} \) positive Hermitian operators \( E_i \) satisfying \( \sum_i E_i = I \), and the condition \( E_i E_j = E_i \delta_{ij} \), namely, \( (E_i)^2 = E_i \) and \( E_i E_j = 0 \) for \( i \neq j \). Such operators are called orthonormal projection operators. Measuring the state \( |\psi\rangle \) results with the output \( i \) with probability \( p_i = \langle \psi|E_i|\psi\rangle \). For a general state described by the density matrix \( \rho \), the probability of measuring \( i \) is given by \( p_i = \text{tr} (E_i \rho) \).

A more general description of measurement is the Positive Operator Valued Measure (POVM) [65, 63]. A POVM is defined via a set of \( M \) positive operators \( E_i \) satisfying \( \sum_i E_i = I \). Note that \( M \) can be different from \( \text{dim} \mathcal{H} \), and the conditions \( (E_i)^2 = E_i \) and \( E_i E_j = 0 \) (for \( i \neq j \)), need not be satisfied. This description is equivalent to enlarging the quantum system to a higher dimension \( D \), performing a projection measurement which gives \( D \) outcomes and potentially uniting several outcome to a single outcome, so that the final number of outcomes is \( M \).

1.2 The Fock Space

1.2.1 Fock states

Since most of the practical QKD experiments and products are done using photons, in this section we introduce some notations and concepts relevant to the photonic world, specifically, the Fock-Space\(^1\) notations for describing photonic quantum spaces. For clarity, a description of the Fock space and Fock notations can be found in various quantum optics books, e.g. [84, 73, 33].
states written using the Fock notation are denoted with an ‘$F$’ superscript, e.g. $|0\rangle^F$, $|3\rangle^F$ and $|0,3,1\rangle^F$.

A photon can not be treated as a quantum system in a straightforward way. For instance, unlike dust particles or grains of sand, photons are indistinguishable particles, meaning that when a couple of photons are interacting, one cannot define the evolution of the specific particle, but rather describe the whole system.

Let us examine a cavity, for instance. It can contain photons of specific wavelengths ($\lambda_1$, $\lambda_2$, etc.) and the energy of a photon of wavelength $\lambda$ is directly proportional to $1/\lambda$. While one cannot distinguish between photons, one can distinguish between different wavelengths. Therefore, it is convenient to define distinguishable “photonic modes”, such that each wavelength corresponds to a specific mode (so a mode inside a cavity can be denoted by its wavelength), and then count the number of photons in each mode. If a single photon in a specific mode carries some unit of energy, then $n$ such photons of the same wavelength carry $n$ times that energy. If the cavity is at its ground (minimal) energy level, we say that there are “no photons” in the cavity and denote the state as $|0\rangle^F$ — the vacuum state. The convention is to denote only those modes that are potentially populated, so if we can find $n$ photons in one mode, and no photons in any other mode, we write, $|n\rangle^F$. If two modes are populated by $n_a$ and $n_b$ photons, and all other modes are surely empty, we write $|n_a,n_b\rangle^F$ (or $|m,n\rangle^F_{ab}$). When there is no danger of confusion, and the number of photons per mode is small (smaller than ten), we just write $|mn\rangle^F$ for $m$ photons in one mode and $n$ in the other. In addition to its wavelength, a photon also has a property called polarization, and a basis for that property is, for instance, the horizontal and vertical polarizations. Thus, two modes (in a cavity) can also have the same energy, but different polarizations.

Outside a cavity photons travel with the speed of light, say from Alice to Bob, yet modes can still be described, e.g., by using “pulses” of light [13]. The modes can then be distinguished by different directions of the light beams (or by different paths), or by the timing of the pulses (these modes are denoted by non-overlapping times), or by the (orthogonal) polarizations of the photons.

### 1.2.2 A photonic “qubit”

A proper description of a photonic qubit is commonly based on using two modes ‘a’ and ‘b’ which are populated by exactly a single photon, namely, a photon in mode $a$, so the state is $|10\rangle^F_{ab}$, or a photon in mode $b$, so the state is $|01\rangle^F_{ab}$. A general qubit can be described as the normalized superposition

$$|\phi\rangle = \alpha_0|10\rangle^F_{ab} + \alpha_1|01\rangle^F_{ab}.$$  \hspace{1cm} (1.5)
a single photon, and can be populated by any number of photons. An orthonormal basis of this space is \{|n⟩\}_a with \(n \geq 0\), so that the quantum space is infinitely large (i.e. has an infinite, countable, dimension), and is denoted \(H_\infty\). Theoretically, a general state in this space can be written as the normalized superposition \(\sum_{n=0}^{\infty} c_n |n⟩\)_a, with \(\sum_n |c_n|^2 = 1\), \(c_n \in \mathbb{C}\). Similarly, one can define a quantum space that consists of two photonic modes. The computation basis states in this space are of the form \(|n_a, n_b⟩\)_F, with \(n_a, n_b \geq 0\), and a general state is of the form

\[
|\phi⟩ = \sum_{n_a, n_b=0}^{\infty} c_{n_a, n_b} |n_a, n_b⟩_F
\]  

with \(\sum_{n_a, n_b=0}^{\infty} |c_{n_a, n_b}|^2 = 1\), \(c_{n_a, n_b} \in \mathbb{C}\).

Using exactly two photons in two different (and orthogonal) modes assists in clarifying the difference between photons and dust particles (or grains of sand): when we consider two qubits, we get four possible orthogonal states, e.g. \(|00⟩\), \(|01⟩\), \(|10⟩\) and \(|11⟩\). However, due to the indistinguishability of the photons, only 3 different states can exist when having exactly two photons: \(|20⟩_ab\), \(|02⟩_ab\) and \(|11⟩_ab\). The last state has one photon in mode ‘a’ and another photon in ‘b’, however, exchanging the photons is meaningless since one can never tell one photon from another.

### 1.3 Key Distribution

In order to obtain privacy and security, a mutual secret must be shared between all the parties involved. This secret is usually named the key. The key is the foundation for each and every cryptographic protocol: Encryption, Authentication, Digital Signature, etc. Once the key is exposed, the legitimate users (usually known as ‘Alice’ and ‘Bob’) are subject to the deeds of their evil opponent (‘Eve’) who can decrypt and read their messages, impersonate them or digitally sign contracts on their behalf.

It is proven that for a message to be encrypted in a secure way (in the sense of information theory), one needs a key as long as the message [74]. Therefore there is a great need in key distribution algorithms that have a high key-rate, and are information-theoretically secure.

#### 1.3.1 Methods for secure key distribution

How can Alice and Bob obtain the same secret without letting anyone else know it? If Alice and Bob live in the same city, they can arrange a weekly meeting in which Alice can pass Bob a CD with the keys of the next week. But what can they do if Alice lives in Israel while Bob lives in Bangladesh?!

They still have several solutions:
• **Using a trusted third party.** Alice and Bob can be helped by David. David is Bob’s best friend who happens to be Alice’s brother. Luckily, David is a steward in El-Al, and flies to Bangladesh at least once a month. Both Alice and Bob trust David, therefore he can be used as a “Trusted Third Party” who distributes the keys.

• **Using a small pre-obtained secret.** Unfortunately, Most of the Alices have no steward brother, so a different solution must be reached. Let us say Bob and Alice already share a small secret key ($K_{key}$) (from the last visit of Bob in Israel). Alice and Bob can use $K_{key}$ in order to encrypt the weekly key ($K_{week}$) and send it over the Net$^2$. On the next week they can use $K_{key}$ again to agree on $K_{next-week}$, or they can use $K_{week}$ to encrypt $K_{next-week}$.

  Question: If Alice and Bob already share a key, why can’t they use this key as the key for all their cryptographic protocols? The Answer is that the more one uses a key, the less the key is secure. Therefore one would like to change one’s key once in a period, to maintain its secrecy.

• **Using Public Key Cryptography.** Yet, Alice might wish to have a secure conversation with someone she met on the Internet, who never reached Israel. Therefore we need a protocol which allows agreeing on a secret key, for two users that share no previous secret, never met before and can communicate only over insecure channels (e-mail, ICQ, IRC, etc.). The obtained key must be secret so that anyone but the authorized users would have no information about the key. **Is this possible?**

### 1.3.2 Modern (classical) key-distribution protocols

In 1976, W. Diffie and M. Hellman published a novel solution to the Key Agreement problem [25]. Their article, named in the promising name ‘New Directions in Cryptography’, indeed opened a way to a field today referred as **Public Key Cryptography**. The Diffie-Hellman Key Agreement$^3$ protocol, allows two users, that have never met before and share no common secret, to agree on a secret key using only a classical insecure channel.

The Diffie-Hellman Key Agreement protocol suffers from one main weakness: it is exposed to an attack called **Man in the middle Attack**. An eavesdropper can impersonate a legitimate user, and run the protocol separately with Alice (who thinks it is Bob on the other side) and separately with Bob (who assumes Alice is on the other side). In that way, Alice-Eve end the protocol with a secret key $K_{AE}$ and Eve-Bob share $K_{EB}$. Every message sent by Alice to Bob (encrypted with $K_{AE}$) is decrypted by Eve, read, encrypted...

---

$^2$This method is known to be used by the German army in WW2, for distributing the *Enigma* cryptosystem key.

$^3$This protocol is sometimes called Key-Exchange protocol. One should pay attention that no key is exchanged or distributed by this protocol, but a new key, agreed on both sides, is generated.
with $K_{EB}$ and sent to Bob. Alice and Bob have all the reasons to believe that they talk with one another, but in fact they have no security.

This flaw can be solved, for instance, using an authenticated channel, given that Alice and Bob share a small secret data in advance.

The security of the protocol is based on the hardness of the discrete-logarithm problem (DLOG [59]), i.e. the amount of time needed to find $k$, given $(g^k \mod p)$, for some prime $p$ and a number $g \in \{1 \ldots p - 1\}$ which is a generator\(^4\). No polynomial-time algorithm that solves the DLOG problem is known, and the problem is assumed to be an NP-problem which requires exponential time to be solved\(^5\). Therefore, Diffie-Hellman is *Computationally Secure*, implying that an adversary with unlimited computing power is able to break the protocol (search all the $\alpha$’s in $\{1 \ldots p - 1\}$ until one finds $\alpha$ such that $g^\alpha \equiv g^k \mod p$). Nevertheless, the security of the Diffie-Hellman protocol is considered pretty safe, relative to the available technology of our time.

Considering an opponent with quantum computing abilities might undermine the security of classical protocols, as they are considered today. Quantum search algorithms (such as [39]), shorten the search duration of an unsorted database from the $O(N)$ classical complexity into quantum-$O(\sqrt{N})$ complexity. Other quantum algorithms (such as [75]) prove the existence of polynomial time algorithms for the DLOG problem, and for the factoring problem (used to break the RSA cryptosystem), whose best known classical algorithm, the Number Field Sieve, has a running-time complexity of $O\left(e^{1.9223(\ln n)^{1/3}(\ln \ln n)^{2/3}}\right)$.

### 1.3.3 Quantum key-distribution protocols

Quantum mechanics introduces various alternative cryptographic protocols [86], in which *Information-theoretical Security* is assumed, rather than the *Computational Security*, which is proved in most of the classical protocols. The main principle standing behind all of these protocols, is using a quantum channel in order to transmit random bits between Alice and Bob. Quantum mechanics laws ensure us that while the bases used to encode those random bits are unknown, any eavesdropping inevitably causes transmission disruptions. This principle is commonly known as the “Information Vs. Disturbance” principle [31, 29, 11, 20, 10]). Once Alice and Bob identify channel disruptions, they know with high probability that eavesdropping has occurred, and abort the protocol.

We distinguish two families of QKD protocols. The first family uses individual qubits and relies on the no-cloning theorem (this family is sometimes called “Prepare and Measure” protocol) while the second family is based on entangled qubits and their properties (usually named “EPR-based” protocols, due to the use of Bell-states (EPR-pairs) [63, 4]. $g$ is called a generator if for every $\alpha \in \{1 \ldots p - 1\}$ there exist $\beta$ such that $g^\beta = \alpha \mod p$.

\(^5\)The most efficient algorithm known for DLOG is Gorodn93 [37], based on the Number-Field-Sieve which runs in complexity of $O\left(e^{(\log p)^{1/3}(\log \log p)^{2/3}}\right)$.

---

1.3. KEY DISTRIBUTION
The BB84 Protocol. The first to use this ability in order to obtain important cryptographic protocols were C. Bennett and G. Brassard [7]. In their article they proposed a key agreement protocol known as BB84. Alice uses two conjugate bases (usually, the $z$ and $x$ bases) in order to send Bob states in one of the following four possibilities:

\[
\begin{align*}
|0_z\rangle &= |0\rangle \\
|1_z\rangle &= |1\rangle \\
|0_x\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \equiv |+\rangle \\
|1_x\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \equiv |−\rangle
\end{align*}
\]  

(1.7)

where $|0_z\rangle$ and $|0_x\rangle$ are used to encode the bit-value 0, and $|1_z\rangle$ and $|1_x\rangle$ are used to encode the bit-value 1. Bob receives each qubit and measures it using a randomly chosen basis ($z$ or $x$). After measuring all the qubits, Alice announces the bases she has used. Qubits that were measured with an incorrect basis are discarded. The rest of the qubits become a string known as the *sifted key*. A portion of the sifted key qubits (usually named the *test string*) is then published and compared by Alice and Bob. This is done in order to estimate the rate of errors created during the transmission. If the error rate is higher than a predetermined threshold, the protocol aborts. Otherwise, the test string is removed from the sifted key and the protocol continues. The next stage is to perform Error Correction (EC) on the remaining sifted bits in order to correct any possible error caused by the channel (or by an eavesdropper). During this stage Alice and Bob may exchange some public data. They continue with a Privacy Amplification (PA) stage, to eliminate any partial information Eve might have on the sifted key (due to eavesdropping or due to the EC data sent publicly). This stage results with the *final key*, which is shorter than the sifted key and is supposed to be more secure.

The B92 Protocol. In 1992 C. Bennett proposed a new protocol [6] suggesting the use of only two states, instead of four. For example, to encode the bit-value 0 Alice sends $|0_z\rangle$ while for the bit-value 1 she sends $|0_x\rangle$. Bob measures the qubits in the same way he does in BB84 protocol, yet his interpretation is different; measuring $|0_z\rangle$ or $|0_x\rangle$ yields inconclusive measurement (a *loss*), since both Alice’s states might cause them. On the other hand, if Bob measures $|1_z\rangle$ (or respectively $|1_x\rangle$) he is sure that the state sent by Alice is *not* $|0_z\rangle$, since $\langle 0_z|1_z\rangle = 0$, so Alice’s state must have been $|0_x\rangle$ (or respectively, $|0_z\rangle$). The rest of the protocol continues as BB84 — Alice and Bob estimate the error rate, perform EC and PA and achieve the final key.

The Six-State Protocol. A further development achieved in 1998 by D. Bruß [22] suggesting to use three conjugate bases, i.e. sending one of the six states $|0_z\rangle$, $|1_z\rangle$, $|0_x\rangle$, $|1_x\rangle$, $|0_y\rangle$, $|1_y\rangle$. In this case Alice uses 2 random bases, usually the $z$ and $x$ bases, and Bob measures each qubit using a randomly chosen basis, usually the $z$ or $x$ basis. After measuring all the qubits, Alice announces the bases she has used. Qubits that were measured with an incorrect basis are discarded. The rest of the qubits become a string known as the *sifted key*. A portion of the sifted key qubits (usually named the *test string*) is then published and compared by Alice and Bob. This is done in order to estimate the rate of errors created during the transmission. If the error rate is higher than a predetermined threshold, the protocol aborts. Otherwise, the test string is removed from the sifted key and the protocol continues. The next stage is to perform Error Correction (EC) on the remaining sifted bits in order to correct any possible error caused by the channel (or by an eavesdropper). During this stage Alice and Bob may exchange some public data. They continue with a Privacy Amplification (PA) stage, to eliminate any partial information Eve might have on the sifted key (due to eavesdropping or due to the EC data sent publicly). This stage results with the *final key*, which is shorter than the sifted key and is supposed to be more secure.
1.4. ATTACKS ON QUANTUM KEY DISTRIBUTION

\(|1_x\rangle, |0_y\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \equiv |+i\rangle \) and \(|1_y\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) \equiv |-i\rangle\). The six-state protocol is proved to be more secure than BB84, yet it achieves a much lower key-rate.

The Mor98 Protocol. In 1998, T. Mor suggested that a QKD protocol needs not be basis-symmetric [60]. Specifically, only one basis can be used to transfer encoded bits, while the other basis is needed only to prevent eavesdropping. A protocol using this fact was defined using only three states, \(|0_z\rangle, |1_z\rangle\) used to encode 0 and 1 respectively, and \(|0_x\rangle\) used to verify the absence of an eavesdropper. The Mor98 Protocol proceeds as the BB84 protocol, except that all the \(x\)-basis qubits (as well as some of the \(z\)-basis qubits) are used as test bits. The final key is achieved from the remaining \(z\)-qubits. This protocol’s method is generalized to be the Classical-Bob Protocol [18, 19], described below in Chapter 5.

The SARG Protocol. Another variant was suggested in 2004 By Scarani et al. [72], in order to avoid a new kind of security flaws the Photon-Number Splitting attack [21]. This Protocol uses the four BB84 states, however, the bit is encoded by the basis, e.g. \(|0_z\rangle\) and \(|1_z\rangle\) to encode 0, and \(|0_x\rangle\) and \(|1_x\rangle\) to encode 1. Alice does not publish the basis she actually used, but instead, she tells Bob whether her state is one of \(\{|0_z\rangle, |0_x\rangle\}\) or of \(\{|1_z\rangle, |1_x\rangle\}\). For instance, assume Bob knows the state is of the first set. If he measures \(|0_z\rangle\) or \(|0_x\rangle\) the result is inconclusive, yet if he measures \(|1_z\rangle\) or \(|1_x\rangle\) he knows that the basis used by Alice is not his chosen basis, and thus he knows the value of the encoded bit.

1.4 Attacks on Quantum Key Distribution

Eve’s aim is to get information about the resulted key without being detected. In order to get this information Eve must interfere with the qubits transmission between Alice and Bob. By doing this, she is forced to cause errors which might lead to her detection. Eve’s attacks can be classified into several classes:

Measure/Resend. In this attack, the qubits generated by Alice never reach Bob — they are intercepted by Eve who can measure them (or just block them). Eve then prepares and sends new qubits to Bob. These qubits can be generated according to Eve’s measurement or be randomly picked. They can be independent qubits, or entangled with Eve’s state. This is the most simple individual-particle attack, since Eve measures the qubits during the protocol.

Translucent Attack. In this individual particle attack [28, 30], Eve adds an ancillary system \(|0_E\rangle\) to each qubit transmission and performs a unitary transformation on the
system

\[ |0\rangle_E|i\rangle \rightarrow \sum_{i,j \in \{0,1\}} |E_{i,j}\rangle_E |j\rangle. \]  

(1.8)

Eve keeps her ancilla for later measurement and sends Bob the rest of the system. A correlated form of this attack can be achieved if Eve chooses her unitary according to the ancillas of the previous transmissions. The C-Not attack is an example of translucent attack in which Eve tries to “replicate” Alice’s qubits before delivering them to Bob, using a C-Not gate,

\[
CNot = \begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0
\end{pmatrix}.
\]  

(1.9)

The C-Not gate operation (in the computational basis, i.e. the z-basis) is inverting the second qubit (the ‘target’) whenever the first qubit (the ‘control’) is 1, see as well [63, Section 1.3]. Eve places her ancilla as the target and uses the qubit of Alice as the control. The effect of using C-Not gate on the transmitted qubits is the following: if Alice used the \( z \)-basis, Eve’s ancilla becomes a copy of that qubit,

\[
|0\rangle_E |0\rangle_x \rightarrow |0\rangle_E |0\rangle, \quad |0\rangle_E |1\rangle \rightarrow |1\rangle_E |1\rangle.
\]  

(1.10)

However, if Alice used the \( x \) basis, the C-Not gate entangles the qubit with Eve’s ancilla:

\[
|0\rangle_E |0\rangle_x \rightarrow (|0\rangle_E |0\rangle + |1\rangle_E |1\rangle)/\sqrt{2}, \quad |0\rangle_E |1\rangle_x \rightarrow (|0\rangle_E |0\rangle - |1\rangle_E |1\rangle)/\sqrt{2}.
\]  

(1.11)

Measuring any of the qubits (in any basis) gives a random result. These kind of states are known as \( EPR-pairs \) or \( Bell-states \) \([27]\), \([63, \text{Section 2.6}]\).

**Collective Attack.** In the collective attack \([12, 11]\) Eve attaches a probe to each qubit sent by Alice, and performs a unitary operation on them. She then sends Bob the qubit, and save the probes in her memory. Eve collects all the probes, waits until the protocol ends and measures all the probes together. Eve does not measure her probes immediately because she can measure them in a better way after she acquires the classical information of the protocol which is sent over the insecure channel (e.g. the bases used, the bits of error-correction, etc.)

**Joint Attack.** The joint\(^6\) attack is the most general attack (therefore — the most powerful) that can be made. Eve receives all the qubits that are sent to Bob, and performs

\(^6\) Also known as the Coherent attack.
a unitary operation on all the qubits and probes altogether,

\[ |0\rangle_E |i\rangle \rightarrow \sum_{i,j \in \{0,1\}^n} |E_{i,j}\rangle_E |j\rangle. \tag{1.13} \]

Note that the same ancilla is used to attack all the qubits. Next, Eve sends the qubits to Bob, waits until she learns all the classical information of the protocol and only then measures her probes.

1.5 Security Proofs

1.5.1 Working assumptions

In order to define the security of a protocol, we begin with our working assumptions:

- Alice and Bob have labs that are perfectly secure.

- They share a classical channel, authenticated but not private. Therefore, all the information on this channel can be heard by Eve, but she cannot change it, block it or send her own information, impersonating a legal user\(^7\).

- Eve cannot delay the qubits sent to Bob for too long. She can let them through unchanged, block them or perform unitary operation on them. If the qubits are sent one by one, she must return Alice the qubit, before Alice sends the next one.

1.5.2 Security proofs criteria

QKD security proofs differ in many ways, especially in their methods and results. When we consider a security analysis we should pay attention to the following criteria:

- Which kind of attack the eavesdropper is allowed to perform: individual, collective or joint attack.

- The specific scheme used: BB84, B92, etc. A security proof can suit more than one scheme.

- The methods used are the most obvious and important difference between the different analyses. The tools being used are wide and different: Shannon Entropy or Rényi Entropy; Indistinguishability of Eve’s density matrices or the fidelity between Alice’s and Bob’s density matrices to a fixed state density matrix; Using purification or not, using CSS Quantum Error Correction Codes [23] or not, etc.

\(^7\)This can be achieved by digitally signing messages. Therefore, we assume that Alice and Bob already share a small secret key used for authentication, using the BB84 protocol in order to achieve larger key. Thus, the protocol is in fact a key expansion protocol.
The security proof might be restricted due to assumptions on the users system setups, for example, assuming the users have quantum computers or a quantum memory.

The bounds on the information leakage can be exponentially small or polynomially small (although both might be called negligible..) The bounds can be well-defined for a given set of parameters, or can be only asymptotic.

Another difference is the threshold of acceptable error that each proof achieves. As said, this parameter tells us when the QKD security is compromised due to eavesdropping. Theoretically, the error rate should be 0% in the absence of eavesdropping, whereas a simple C-Not attack that compromises the privacy of the key, causes an error rate of 25%. Currently, the exact maximal error-rate threshold for secure QKD, is unknown.

1.5.3 Known security proofs

One can compare the different analyses according the above criteria.

Kind of Attack: Security against individual-attacks can be found in [77, 54]. The Collective Attack is considered in [12, 11, 51]. The Joint Attack is studied in [52, 76, 9, 57, 4, 68, 10].

QKD scheme: The BB84 Protocol is studied by [57, 11, 10, 51]. A security proof for the six-state protocol can be found in [22]. Papers [51, 24] prove the security of the above schemes as well as the B92 protocol; Paper [76] starts with the EPR-scheme but finally reaches a security proof for the BB84 by using some reductions. In the same manner [81] reduces the proof for the B92 protocol. The EPR-scheme is studied by [52]. Security proofs of practical realizations of QKD schemes can be found in [44, 38, 46, 2]. These proofs regard several deviations from the theoretical protocol caused by errors, devices imperfections, etc.

Information Bounds: The information Eve gets on the key is proven to be exponentially small in [11, 10], which results in a definite bound for a given set of security parameters. Papers [52, 76] show that asymptotically the mutual information of Eve and the key is exponentially small. No definite number is given in these proofs.

Error-Rate Thresholds: Proof [11] achieves a very loose threshold for the collective attack, namely, less than 2%. Proof [10] improves the threshold for the joint attack and reaches an asymptotic error-rate threshold of 7.56%, which is obtained by [57] as well. Proof [76] achieves a threshold of less than 11%. The threshold achieved by [51] is 12.4%; it also states that the BB84 is insecure if the error rate exceeds 14.12%.

Methods, tools and assumptions: The approach of [11] as well as [10], is to analyze the information Eve might achieve, by using a purification of the mixed state Eve has. The main method of the proof is to show that Eve can hardly distinguish between the state she holds when Alice’s final-key bit is ‘0’, from the state she holds given that Alice’s key
1.6. STRUCTURE OF DISSERTATION

is ‘1’. It should be stated that [10] uses symmetrization of the attack.

The method used by [52, 76] is to bound the fidelity of Alice and Bob state with one of the Bell-states, showing that high fidelity implies low mutual information between Eve and the key. In order to achieve high fidelity an entanglement distillation process is used. It should be mentioned that [52] assumes having a quantum computer (due to considering the EPR-scheme and the entanglement distillation), while [76] extends the proof by several reductions in order to apply the proof to the BB84 scheme, and eliminate the need of a quantum computer. Some of those reductions make use of the CSS error correction codes family, inspired by the requirements of the error correction codes used in [57].

The last method, which is used by [51], describes a general QKD-scheme as a two-stages protocol that consists of a quantum bit transfer stage and a classical processing stage. It symmetrizes the density matrices in order to achieve a QKD-scheme that can be used for both the BB84, B92 and the EPR-pair schemes. The proof makes use of classical noisy channels in order to intentionally induce errors to the key, and then uses the smooth Rényi entropy ([70]) to bound the information.

1.6 Structure of Dissertation

This dissertation is build out of several subjects within the main topic of QKD protocols and their security. Chapter 2 begins with the Quantum-Space Attack (QSA), a new general framework that allows the analysis of practical implementations of QKD schemes. We find that many implementations deviate from the theoretical protocol, in a way that causes the enlargement of the spaces in use. We define the effective space needed for attacking the protocol and prove there is no use in attacking a larger space. We show that any currently known attack on practical schemes is merely a specific case of the general attack on this space — the Quantum-Space Attack.

In Chapter 3 we analyze a specific realizations of uni-directional prepare & measure QKD schemes (BB84, six-state, etc.), implemented using interferometer. We show an evidence for the security of such implementations by proving their robustness (which is a weaker property than security). We conclude this part with a successful attack on a specific variant. This attack is in fact a QSA, therefore a demonstration for the QSA power is given.

Chapter 4 deals with theoretical collective attacks on the BB84 QKD scheme. Here we improve the bound presented in [11] for the collective attack. We derive a bound on Eve’s information using the methods of [10]. Although our bound does not exceed the bound obtained in [10] for the joint atack, we yield with a shorter and simper analysis of the collective attack, without the need of tedious manipulation, such as the symmetrization done in [10].
We then continue in Chapter 5 with a new QKD protocol, in which only one party is quantum, and the other may be classical. This protocol is an enhancement of the Mor98 Protocol [60] discussed above. We define several variants to this semi-quantum protocol, prove their robustness and discuss their properties.

We Conclude this research in Chapter 6.
Chapter 2

Quantum Space Attacks

2.1 Introduction

During the recent years, many security analyses were published [87, 57, 9, 76, 10, 51] which proved the information-theoretical security of the BB84 scheme against the most general attack by an unlimited adversary (who has full control of the quantum channel). These security proofs are limited as they always consider a theoretical QKD that uses perfect qubits. Although these security proofs do take errors into account, and the protocols use error correction and privacy amplification (to compensate for these errors and for reducing any partial knowledge that Eve might have), in general, they avoid security issues that arise from the implementation of qubits in the real world.

A pivotal paper by Brassard, Lütkenhaus, Mor, and Sanders [21] presented the “Photon Number Splitting (PNS) attack” and exposed a security flaw in experimental and practical QKD: one must take into account the fact that Alice does not generate perfect qubits (2 basis-states of a single photon), but, instead, generates states that reside in an enlarged Hilbert space (we call it “quantum space” here), of six dimensions. The reason for that discrepancy in the size of the used quantum space is that each electromagnetic pulse that Alice generates contains (in addition to the two dimensions spanned by the single-photon states) also a vacuum state and three 2-photon states, and these are extremely useful to the eavesdropper. That paper proved that, in contrast to what was assumed in previous papers, Eve can make use of the enlarged space, and get a lot of information on the secret key, sometimes even full information, without inducing any noise. Many attacks on practical protocols then followed (e.g., [44, 45, 38, 62, 56, 34]), based on extensions of the quantum spaces, exploring various additional security flaws; other papers [44, 72, 85] suggested possible ways to overcome such attacks. On the one hand, several security proofs, considering specific imperfections, were given for the BB84 protocol [38, 46]. Yet on the other hand, it is generally impossible now to prove the security of a practical protocol, since a general framework that considers such realistic QKD protocols, and the possible attacks on such protocols, is still missing. The work of Acín et al. [2] makes a
substantial step in that direction. However, besides of the fact that it is fixed to a specific protocol, it ignores the possibility of losses (or measurement that are interpreted as losses) which we found important for having security analysis.

In this chapter we show that the PNS attack, and actually all attacks directed at the channel, are various special cases of a general attack that we define here, the Quantum-Space Attack (QSA). The QSA generalizes existing attacks and also offers novel attacks. The QSA is based on the fact that the “qubits” manipulated in the QKD protocol actually reside in a larger Hilbert space, and this enlarged space can be assessed. Although this enlarged space is at times not fully accessible to the legitimate users, they can still analyze it, and learn what a fully powerful eavesdropper can do.

We show that an eavesdropper’s best attack can be done by attacking a space with the dimension of this “quantum space of the protocol”. This restricts the security analysis to much a smaller space, which might be easier to analyze. We focus on schemes in which the quantum communication is uni-directional, namely, from Alice’s laboratory (lab) to Bob’s lab. We consider an adversary that can attack all the quantum states that come out of Alice’s lab, and all the quantum states that go into Bob’s lab. We do not allow the adversary to input data into Alice’s lab nor to read data from Bob’s lab, except for the classical data that Bob sends as part of the standard protocol.

This Chapter is based on [16].

2.2 Preliminaries

2.2.1 Properties of Hilbert spaces

We begin with several properties of Hilbert Spaces required to our analyses. Most of the following Lemmas are proven in [67, Section II] or in [43, Chapters 6,8]. Throughout this section, $V$ is a subspace of $\mathcal{H}$. Unless specifically mentioned, $V$ is closed, i.e. is a Hilbert Space. All the projectors $P$ are linear, bounded and Hermitian, i.e. $P^2 = P = P^\dagger$.

**Definition 2.1** For any vector subspace $V \subseteq \mathcal{H}$, its *orthogonal complement* $V^\perp$ is the subspace defined by

$$V^\perp = \{ \phi \in \mathcal{H} \mid \langle \phi | v \rangle = 0, \forall v \in V \} \quad (2.1)$$

which is closed [43, Theorem 6.12].

**Lemma 2.2** For any closed subspace $V$ of $\mathcal{H}$,

i. $V \cap V^\perp = \{0\}$

ii. $\mathcal{H} = V + V^\perp$
2.2. PRELIMINARIES

Proof Property (i) follows immediately from the definition of $V^\perp$, and from the fact that the only element $v \in V$ of which $\langle v|v \rangle = 0$ is the zero element, $v = 0$. The second property is proven in [67, Theorem II.3].

Lemma 2.3 For any subspace $V$ of $\mathcal{H}$ (closed or not) $V^\perp\perp = \overline{V}$, the closure of $V$.

Proof We first show that $V^\perp = V^\perp$. Let $x \in V^\perp$. For every $z \in V$ there exists an converging Cauchy series $\{z_n\} \in V$ such that $\lim_n z_n = z$. Since the inner product is continues [43, Theorem 6.10] and $\langle z_n|x \rangle = 0$ for every $n$ we get

$$\langle z|x \rangle = \lim_n \langle z_n|x \rangle = \lim_n (z_n|x) = 0. \quad (2.2)$$

$x$ is orthogonal to every element in $V$ and thus $V^\perp \subset V^\perp$. The other direction is trivial. Finally, using property (ii) of Lemma 2.2 we get

$$V^\perp\perp = \overline{V}.$$

Definition 2.4 For any operator $A : \mathcal{H}_1 \to \mathcal{H}_2$, its kernel, denoted $\text{Ker} A$ is

$$\text{Ker} A = \{ \phi \in \mathcal{H}_1 \mid A(\phi) = 0 \}. \quad (2.4)$$

It is a closed subspace of $\mathcal{H}_1$.

Definition 2.5 For any operator $A : \mathcal{H}_1 \to \mathcal{H}_2$, its range, denoted $\text{Ran} A$ is

$$\text{Ran} A = \{ A(\phi) \mid \phi \in \mathcal{H}_1 \}. \quad (2.5)$$

The range of an operator is not closed in general.

Lemma 2.6 For any operator $A : \mathcal{H} \to \mathcal{H}$,

$$(\text{Ran} A)^\perp = \text{Ker} A^\dagger \text{ and thus } \overline{\text{Ran} A} = (\text{Ker} A^\dagger)^\perp. \quad (2.6)$$

See [67, Page. 58].

Lemma 2.7 If $P$ is a Hermitian projector, then $\text{Ran} P$ is a closed subspace of $\mathcal{H}$,

$$(\text{Ran} P)^\perp = \text{Ker} P, \quad (2.7)$$

$P$ acts like 0 on $(\text{Ran} P)^\perp$ and like the identity on $\text{Ran} P$. See [67, Page. 187].

Lemma 2.8 For any closed $V, W \subseteq M$,

$$(V + W)^\perp = V^\perp \cap W^\perp \text{ and } (V \cap W)^\perp = V^\perp + W^\perp. \quad (2.8)$$
Proof If $\phi \in (V+W)\perp$, then $\phi$ must be orthogonal to both $V$ and $W$ and thus $(V+W)\perp \subseteq V\perp \cap W\perp$. Conversely, if $\phi$ is orthogonal to all $v \in V$ and $w \in W$, it is orthogonal to all $v+w$ and thus to $V+W$. The second part of the lemma follows from the fact that $V\perp\perp = V$ for all (closed) $V$. 

Lemma 2.9 If $P$ is a positive operator on $\mathcal{H}$, then

$$P|\phi\rangle = 0 \text{ if and only if } \langle \phi|P|\phi\rangle = 0. \quad (2.9)$$

Proof We need only show that $\langle \phi|P|\phi\rangle = 0$ implies $P|\phi\rangle = 0$. There exists $A$ such that $P = A^\dagger A$, see [67, Pages 195–196]; from $\langle \phi|A^\dagger A|\phi\rangle = \|A|\phi\|$ we deduce $A|\phi\rangle = 0$ and thus $P|\phi\rangle = A^\dagger A|\phi\rangle = 0$. 

Lemma 2.10 If $P_1$ and $P_2$ are positive (and thus Hermitian),

$$\text{Ker}(P_1 + P_2) = (\text{Ker}P_1) \cap (\text{Ker}P_2) \quad \text{and} \quad \text{Ran}(P_1 + P_2) = \text{Ran}P_1 + \text{Ran}P_2. \quad (2.10)$$

Proof $P_1 + P_2$ is positive and

$$\phi \in \text{Ker}(P_1 + P_2)$$

$$\iff \langle \phi|P_1 + P_2|\phi\rangle = 0$$

$$\iff \langle \phi|P_1|\phi\rangle + \langle \phi|P_2|\phi\rangle = 0$$

$$\iff P_1|\phi\rangle = 0 \land P_2|\phi\rangle = 0.$$

Finally, using Lemma 2.7,

$$\text{Ran}(P_1 + P_2) = \text{Ker}(P_1 + P_2)\perp$$

and by Lemma 2.8 we get

$$(\text{Ker}P_1 \cap \text{Ker}P_2)\perp = (\text{Ker}P_1)\perp + (\text{Ker}P_2)\perp = \text{Ran}P_1 + \text{Ran}P_2.$$

2.2.2 Hilbert-state notations for Fock-states

In this chapter we use the familiar Hilbert-state notations to describe systems and protocols. Yet, many of the protocols we mention and analyze are originally described using the Fock-states notations. Here we provide a useful translation between Fock states to Hilbert.
2.2. PRELIMINARIES

Writing the state of photons (or any other bosons) using Hilbert-state must conserve a symmetry property — their state must be unchanged when any two of them are interchanged. For \( w = w_1 \ldots w_n \in \{0, 1, \ldots, k - 1\}^n \), Let

\[
S_n |w\rangle = \frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} |w_{\sigma(1)} \ldots w_{\sigma(n)}\rangle
\]

(2.11)

where \( \mathfrak{S}_n \) is all the permutations of \( \{1, \ldots, n\} \). An element \( |\phi\rangle \in \mathcal{H}^\otimes_k \) is called a “symmetric tensor” of order \( n \) over \( \mathcal{H}_k \) if

\[
S_n |\phi\rangle = |\phi\rangle
\]

(2.12)

where the space of symmetric tensors of order \( n \) is \( S_n (\mathcal{H}^\otimes_k) \).

The symmetric tensors Hilbert space matching a Fock space with \( k \) modes can be written as

\[
\mathcal{F}_s (\mathcal{H}_k) = \bigoplus_{n=0}^{\infty} S_n (\mathcal{H}^\otimes_k).
\]

(2.13)

The \( \bigoplus \) sign stands for a direct sum, see [67, page 53].

The \( k \)-mode state \(|n_0 \ldots n_{k-1}\rangle^F\) can be written using the Hilbert-state notations as the normalized state \( |\phi\rangle \in \mathcal{H}^\otimes_0^{n_0 + \ldots + n_{k-1}} \) which is an equal superposition of all permutations of \( n_0 \) zeros, \( n_1 \) ones, \( n_2 \) twos, etc.; the states \(|n_0 \ldots n_{k-1}\rangle^F\) for \( n_0 + \ldots + n_{k-1} = n \) are thus symmetric and it is easy to see that they form an orthonormal basis for the symmetric states of \( n \) photons. The state \(|00 \ldots 0\rangle^F\) corresponds to no zeros, no ones, etc. It thus corresponds to what is called the “empty string” (the string of length 0) and is denoted \( \epsilon \). We shall denote \(|\epsilon\rangle\) the state \(|00 \ldots 0\rangle^F\), which corresponds to a loss. For any \(|\phi\rangle\),

\[
|\phi\rangle^\otimes_0 \triangleq |\epsilon\rangle,
\]

(2.14)

and for any Hilbert space \( \mathcal{H} \),

\[
\mathcal{H}^\otimes_0 \triangleq \{|\epsilon\rangle\}.
\]

(2.15)

For example, the Hilbert space of \( n \leq 2 \) photons with \( k = 2 \) modes is

\[
\chi^6 \triangleq S_0 (\mathcal{H}^\otimes_2) + S_1 (\mathcal{H}^\otimes_2) + S_2 (\mathcal{H}^\otimes_2)
\]

(2.16)

where the possible Hilbert states are:

\[
|\phi\rangle = \begin{cases} 
|\epsilon\rangle & n = 0, \text{ matching } |00\rangle^F; \\
|0\rangle, |1\rangle & n = 1, \text{ matching } |10\rangle^F, |01\rangle^F; \\
|00\rangle, |11\rangle, \frac{|01\rangle + |10\rangle}{\sqrt{2}} & n = 2, \text{ matching } |20\rangle^F, |02\rangle^F, |11\rangle^F.
\end{cases}
\]

(2.17)

or a superposition of these states. For another example, the space of an exactly single photon (\( n = 1 \)) with \( k = 3 \) possible modes is therefore \( S_1 (\mathcal{H}^\otimes_3) \) with basis states \(|0\rangle, |1\rangle, |2\rangle \) corresponding to \(|100\rangle^F, |010\rangle^F, |001\rangle^F \) respectively.
CHAPTER 2. QUANTUM SPACE ATTACKS

2.3 The Quantum Space of the Protocol

The Quantum Space Attack (QSA) is the most general attack on the quantum channel that connects Alice to Bob. It can be applied to any realistic QKD protocol, yet here we focus on uni-directional schemes using qubits. We need to have a proper model of the protocol in order to understand the Hilbert space that an unlimited Eve can attack. We start with a model of a practical “qubit”, continue with understanding the spaces used by Alice and Bob, and end by defining the relevant space, the Quantum Space of the Protocol (QSoP), used by Eve to attack the protocol. Attacks on the QSoP are what we call Quantum-Space Attacks.

2.3.1 Alice’s realistic space

In many QKD protocols, Alice sends Bob qubits, namely, states of a two dimensional quantum spaces ($\mathcal{H}_2$), as described in Section 1.1. A realistic view should take into account any possible deviation from theory, caused by Alice’s equipment. For example, Alice might encode the qubit via a polarized photon: $|0_z\rangle$ via a photon polarized horizontally, and $|1_z\rangle$ polarized vertically. This can be written using the Fock notations\footnote{We remind that we use $|\cdot\rangle_F$ to denote the Fock states, as described in Section 1.2.} as $|n_hn_v\rangle^F$ where $n_h$ ($n_v$) represents the number of horizontal (vertical) photons, then

$$
|0_z\rangle \equiv |10\rangle_F \quad \text{and} \quad |1_z\rangle \equiv |01\rangle_F.
$$

When Alice’s photon is lost within her equipment\footnote{The same holds for the case where the photon is lost during the transmission.} we consider that case as if Alice has sent the state $|0,0\rangle^F$, so her realistic space becomes $\mathcal{H}_3$:

Alice might send multiple photon pulses, which might result in a much larger (and even infinite) $\mathcal{H}_A$. A realistic model of a photon source is of a coherent pulse. Given any qubit state $|\phi\rangle \in \mathcal{H}_2$, Let the state $|\phi\rangle \otimes^n$ represent $n$ identical copies of that state in a symmetric state. For a complex number, we define the coherent state

$$
|\alpha\rangle = e^{-|\alpha|^2 2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |\phi\rangle^\otimes^n,
$$

which represent a superposition of having 0 particles with amplitude $e^{-|\alpha|^2 2}$, one particle in state $|\phi\rangle$ with amplitude $e^{-|\alpha|^2 2} \alpha$, two particles in state $|\phi\rangle$ with amplitude $\frac{1}{\sqrt{2}} e^{-|\alpha|^2 2} \alpha^2$ and so on (a Poissonian distribution). As the number of photons increases the probability decreases, so it is common to neglect the higher orders. Experimentalists commonly use a “weak” coherent state (such that $|\alpha| \ll 1$) and then terms with $n \geq 3$ can usually be neglected. When the phase $\text{arg}(\alpha)$ is unknown, the coherent state is equivalent to a classical mixture of Fock states with different number of photons [46], i.e., Alice can be
2.3. THE QUANTUM SPACE OF THE PROTOCOL

Figure 2.1: The photon number probability distribution for a source with $\alpha = 0.1$

considered as sending a pulse with $n$ photons with probability $e^{||\alpha||^2} \frac{\alpha^{2n}}{n!}$. Neglecting pulses with more than 2 photons causes the appropriate realistic quantum space of Alice, $\mathcal{H}_A$, to become a quhexit: the six-dimensional space $\chi^6$ described above (2.16). The Photon Number Splitting (PNS) attack demonstrated in Section 2.6.1, is based on attacking this 6 dimensional space.

It may be that Alice’s realistic space is even larger, due to extra modes that are sent through the channel, and are not meant to be part of the protocol. These extra modes might severely compromise the security of the protocol, since they might carry some vital information about the protocol. A specific QSA based on that flaw is the “tagging attack” discussed in Section 2.6.2.

**Definition 2.11 Alice’s realistic space, $\mathcal{H}_A$,** is the minimal space containing the actual quantum states sent by Alice to Bob during the QKD protocol. It is the space spanned by the states sent by Alice during the protocol.

During the BB84 protocol, Alice sends qubits in two fixed conjugate bases. Theoretically, Alice randomly chooses a basis and a bit value and then sends the chosen bit encoded in the appropriate chosen basis as a state in $\mathcal{H}_2$ (e.g. $|0_z\rangle, |1_z\rangle, |0_x\rangle$, and $|1_x\rangle$). To a better approximation, the states sent by Alice are four different states $|\psi_i\rangle_A$ ($i = 1, 2, 3, 4$) in her realistic space $\mathcal{H}_A$, spanned by these four states. This space $\mathcal{H}_A$ is of dimension $|\mathcal{H}_A|$, commonly between 2 and 4, but possibly much higher, as described above.
It is important to notice that $\mathcal{H}^A$ is merely a subspace of an enlarged space $M^A$, determined by the underlying physics of the equipment in use. For instance, when Alice sends a qubit (encoded as two modes), using a weak coherent state, her realistic space, $\mathcal{H}^A$, is embedded in (i.e. is a subspace of) $M^A = \bigoplus_{n=0}^{\infty} S_n (\mathcal{H}_2 \otimes n)$, which dimension is infinite.

### 2.3.2 Extension of Alice’s space

Bob commonly receives one of several possible states $|\psi_i\rangle_A$ sent by Alice, and measures it. The most general measurement Bob can perform is to add an ancilla, perform a unitary transformation on the joint system, perform a complete measurement, and potentially “forget” some of the outcomes. This entire process can be described in a compact way by using a POVM, due to Neumark theorem. However, once Alice’s space is larger than $\mathcal{H}_2$, the extra dimensions provided by Alice could be used by Bob for his measurement, instead of adding an ancilla. Interestingly, by his measurement Bob might be extending the space vulnerable to Eve’s attack well beyond $\mathcal{H}^A$. This is possible since in many cases the realistic space, $\mathcal{H}^A$, is embedded inside a larger space $M^A$.

Due to the presence of an eavesdropper, Bob’s choice whether to add an ancilla or to use the extended space $M^A$ is vital for security analysis. In the first case the ancilla is added by Bob, inside his lab, while in the second it is controlled by Alice, transferred through the quantum channel and exposed to Eve’s deeds. Eve might attack the extended space $M^A$, and thus have a different effect on Bob.

For example, suppose Alice sends two non-orthogonal states of a qubit, $\theta_0 = (\cos \theta \sin \theta)$ and $\theta_1 = (-\cos \theta \sin \theta)$, with a fixed and known angle $0 \leq \theta \leq 45^\circ$. Bob would like to distinguish between them, while allowing inconclusive results sometimes, but no errors [64]. Bob can add the ancilla $|0\rangle_{Anc} \equiv (1 \ 0)_{Anc}$ and perform the following transformation $U$:

\[
|0\rangle_{Anc} \otimes \begin{pmatrix} \cos \theta \\ \pm \sin \theta \\ 0 \end{pmatrix} \xrightarrow{U} \begin{pmatrix} \sin \theta \\ \pm \sin \theta \\ \sqrt{\cos 2\theta} \end{pmatrix} = \sqrt{2} \sin \theta |0\rangle_{Anc} \otimes \left( 1/\sqrt{2} \pm 1/\sqrt{2} \right) + \sqrt{\cos 2\theta} |1\rangle_{Anc} \otimes \left( 1 \ 0 \right) \tag{2.20}
\]

where $|1\rangle_{Anc} \equiv (0 \ 1)_{Anc}$. This operation leads to a conclusive result with probability $2 \sin^2 \theta$ (when the measured ancilla is $|0\rangle_{Anc}$), and inconclusive result otherwise. It is simple to see that the same measurement can be done, without the use of an ancilla, if the states

---

3By the term “forget” we mean that Bob’s detection is unable to distinguish between several measured states.
2.3. THE QUANTUM SPACE OF THE PROTOCOL

θ₀ and θ₁ are embedded at Alice’s lab in a larger space \( M^A \), e.g. \( M^A = \mathcal{H}_3 \). Using Bob’s transformation

\[
\begin{pmatrix}
\cos \theta \\
\pm \sin \theta \\
0
\end{pmatrix} \xrightarrow{U} \begin{pmatrix}
\sin \theta \\
\pm \sin \sqrt{\cos 2\theta}
\end{pmatrix}.
\]

(2.21)

In the general case, the space \( M^A \) may be very large, even infinite.

2.3.3 Bob’s space

Let us formulate the spaces involved in the protocol, as described above. Assume Alice uses the space \( \mathcal{H}^A \) according to Definition 2.11, which is embedded in a (potentially larger) space \( M^A \). Ideally, Bob would like to measure just the states \( |\psi⟩_A ∈ \mathcal{H}^A \) sent by Alice, but in practice he usually cannot do so. Each one of Alice’s states \( |\psi⟩_A \) is regarded by Bob’s measurement as some state \( |\psi⟩_M ∈ M^A \). The space which is spanned by these states contains all the information about Alice’s states.

More important, Bob might be measuring a subspace of \( M^A \) which Alice’s states do not span. For instance, examine the case where Bob uses detectors to measure the Fock states \( |10⟩_F \) and \( |01⟩_F \). Bob is usually able to distinguish a loss (the state \( |00⟩_F \)) or an error (e.g. \( |11⟩_F \), one horizontal photon and one vertical photon), from the two desired states, but he cannot distinguish between other states containing multiple photons. This means that Bob measures a much larger subspace of the entire space \( M^A \), but (inevitably) interprets outcomes outside \( \mathcal{H}^A \) as legitimate states; e.g. the states \( |20⟩_F, |30⟩_F \), etc. are (mistakenly) interpreted as \( |10⟩_F \).

We assume that the implemented scheme defines \( J \) setups that can be used by Bob for measuring the different bases; each setup \( j = 1 \ldots J - 1 \) is modeled by the POVM \( \{O^B_j\} \), performed on the space \( M \). We assume \( M^A ⊆ M \), without loss of generality\(^4\). Generally, a specific setup consists of adding an ancilla \( |0⟩_B' \) followed by a unitary transformation \( U_{B_j} : M ⊗ \mathcal{H}^B → M ⊗ \mathcal{H}^B' \), followed by a measurement. The unitary transformation is determined by the equipment used by Bob (e.g. beam splitters, phase shifters, etc., when the protocol is implemented using photons). This whole setup can be modeled as a single POVM on \( M \) due to the following Proposition:

**Proposition 2.12** Given \( \mathcal{H}^B' \), a unitary \( U : M ⊗ \mathcal{H}^B' → M ⊗ \mathcal{H}^B' \) and an arbitrary projective measurement \( P_k \) on \( M ⊗ \mathcal{H}^B' \), there is a POVM \( \{O_k\} \) on \( M \) such that \( \text{tr} [O_k |φ⟩⟨φ|] \) is the probability of measuring \( k \) when \( |0⟩_B' \) is attached to \( |φ⟩ ∈ M \), \( U \) is applied to \( |φ⟩|0⟩_B' \) and system \( M ⊗ \mathcal{H}^B' \) is measured using the projection \( \{P_k\} \).

**Proof** For \( |φ⟩ ∈ M \), let

\[
U_k |φ⟩ = P_k (U (|φ⟩|0⟩_B')).
\]

(2.22)

\(^4\)An equivalent way is to define Bob’s measurement on \( M^B \), and letting \( M = M^A + M^B \).
Clearly \( U_k : \mathcal{M} \rightarrow \mathcal{M} \otimes \mathcal{H}_{B'} \) is linear. Moreover, the probability of measuring \( k \) equals to

\[
\|U_k|\phi\rangle\|^2 = \langle \phi|U_k^\dagger U_k|\phi\rangle = \text{tr}\left[U_k^\dagger U_k|\phi\rangle\langle \phi|\right]
\]

(2.23)

where \( U_k^\dagger U_k : \mathcal{M} \rightarrow \mathcal{M} \). Take \( O_k = U_k^\dagger U_k \).

\[\begin{align*}
\end{align*}\]

Once performing a measurement in setup \( j \), Bob ends with an outcome \( k \), out of the possible outcomes for this measurement \( K_j \). It is important to define how Bob interprets this outcome and distinguishes valid outcomes (that imply some fixed value\(^5\)) from values that imply a loss. We assume that any POVM used by Bob may give one distinguished output loss that may correspond to a loss (or to any invalid state, that is not counted as an error).

Definition 2.13 For any POVM \( \{O^{B_j}_k\}_{k \in K_j} \) on a space \( \mathcal{M} \), define Bob’s Measured Space of setup \( j = 0 \ldots J - 1 \) to be

\[
\mathcal{H}^{B_j} = \sum_{k \in K_j - \{\text{loss}\}} \overline{\text{Ran} O^{B_j}_k}(\mathcal{M}),
\]

i.e., the sum of the closure space of \( \text{Ran} O^{B_j}_k \) for all valid outcomes \( k \).

It is interesting to mention that \( \mathcal{H}^{B_j} \) is the orthogonal complement of the eigenspace of \( O_{\text{loss}}^{B_j} \) corresponding to eigenvalue 1.

Proposition 2.14

\[
\mathcal{H}^{B_j} = (I - O_{\text{loss}}^{B_j})(\mathcal{M}) = \left\{ |\phi\rangle \in \mathcal{M} \mid O_{\text{loss}}^{B_j}|\phi\rangle = |\phi\rangle \right\}^\perp.
\]

Proof By the POVM definition, \( \sum_{k \neq \text{loss}} O^{B_j}_k = I - O_{\text{loss}}^{B_j} \) and the first equality follows from Lemma 2.10, i.e. the closure of the image of a sum of positive operators equals the sum of the closure of their images. The second equality follows from Lemma 2.7, i.e. \( \text{Ran} A = (\text{Ker} A)^\perp \) when \( A \) is Hermitian, with \( A = I - O_{\text{loss}}^{B_j} \).

\[
\text{Ker} A = \left\{ |\phi\rangle \in \mathcal{M} \mid |\phi\rangle - O_{\text{loss}}^{B_j}|\phi\rangle = 0 \right\}
\]

\[= \left\{ |\phi\rangle \in \mathcal{M} \mid O_{\text{loss}}^{B_j}|\phi\rangle = |\phi\rangle \right\}.
\]

\[\_\_\]

\(^5\)Pay attention that an error is considered here as a valid outcome, yet it is interpreted as an error.
2.3.4 The quantum space of the protocol

The “quantum space of the protocol” (QSoP) is in fact Alice’s extended space, taking into consideration its extensions due to Bob’s measurements. The security analysis of a protocol depends on the space $\mathcal{H}^B$ defined below.

**Definition 2.15** Bob’s effective space $\mathcal{H}^B$ is the Hilbert space defined by

$$\mathcal{H}^B = \sum_{j=0}^{J-1} \mathcal{H}^{B_j}. \quad (2.24)$$

Usually, $\mathcal{H}^A \subseteq \mathcal{H}^B$, yet those two spaces are not necessarily equal. This enlargement, caused by Bob’s equipment and measurement, is the foundation of the QSA. For instance, using photons, the ideal space $\mathcal{H}^A$ is a two-dimensional space consists of two modes with 2 basis states, while $\mathcal{H}^B$ could be an infinite-dimensional space allowing any number of photons in each mode, see several examples in Section 2.6.

The QSoP is the effective space relevant for Eve’s attack: it is the smallest Hilbert space containing both Alice’s realistic space and Bob’s effective space. Formally,

**Definition 2.16** The Quantum Space of the Protocol, $\mathcal{H}^P \subseteq M$, is the Hilbert space defined by

$$\mathcal{H}^P = \mathcal{H}^A + \mathcal{H}^B. \quad (2.25)$$

If Alice’s realistic space is fully measured by Bob’s detection process, then $\mathcal{H}^A$ is a subspace of $\mathcal{H}^B$, hence $\mathcal{H}^P = \mathcal{H}^B$. Yet, in some cases, $\mathcal{H}^A$ contains information that is considered by Bob as invalid or not measured at all, so that $\mathcal{H}^A \not\subseteq \mathcal{H}^B$. Yet, the states sent by Alice may give Eve a lot of information, so the QSoP must consist of $\mathcal{H}^A$ as well. See example in Section 2.6.2.

2.4 The Quantum Space Attack

2.4.1 Eavesdropping on the quantum space of the protocol

While Section 1.4 described Eve’s methods of attacking a theoretical QKD scheme, we now redefine Eve’s attack to regard the QSoP defined above. By replacing the theoretical qubit space $\mathcal{H}_2$ by Alice’s realistic space $\mathcal{H}^A$, and by defining Eve’s attack on the entire space of the protocol $\mathcal{H}^P$, we can generalize each of the known attacks on theoretical QKD to a “quantum space attack” (QSA). We can easily define now Eve’s most general individual-transmission QSA on a realistic “qubit”, which generalizes the individual-particle attack earlier described. Eve prepares an ancilla in a state $|0\rangle_E$, and attaches it to Alice’s state, but actually her ancilla is now attached to the entire QSoP. Eve performs a unitary transformation $U_E$ on the joint state. If Eve’s attack is only on $\mathcal{H}^A$, we write the resulting
transformation on any basis state $|i\rangle_A$ of $\mathcal{H}^A$, as $|0\rangle_E|i\rangle_A \rightarrow \sum_j |E_{ij}\rangle_E |j\rangle_A$, when the sum is over the dimension of $\mathcal{H}^A$. The most general individual-transmission QSA is based on a translucent QSA on the QSoP,

$$|0\rangle_E|i\rangle_P \rightarrow \sum_j |E_{ij}\rangle_E |j\rangle_P,$$

(2.26)

when the sum is over the dimension of $\mathcal{H}^P$. The subsystem in $\mathcal{H}^P$ is then sent to Bob while the rest (the subsystem $\mathcal{H}^E$) is kept by Eve. We write the transformation of any basis state $|i\rangle_P$ of $\mathcal{H}^P$, but note that it is sufficient to define the transformation of the different states in $\mathcal{H}^A$, namely for all states of the form $|i\rangle_A$, since other states of $\mathcal{H}^P$ are never sent by Alice, and their transformation can be arbitrarily defined (as long as $\mathcal{U}_E$ is kept unitary). Any such $\mathcal{U}_E$ has the same properties, specifically, the same error-rate imposed on the protocol and the same information available to Eve.

Attacks that are more general than the individual transmission QSA, as the collective QSA and the joint QSA, can now be defined accordingly. In the most general collective QSA, Eve performs the above translucent QSA on many (say, $n$) realistic “qubits” (potentially a different attack on each one, if she likes), waits till she gets all the data regarding the generation of the final key, and then she measures her ancillas altogether. The most general attack that Eve could perform on the channel is to attack all those realistic “qubits” transmitted from Alice to Bob, using one large ancilla. This is the “joint QSA”. The attack’s unitary transformation is written as before, but with $i$ a string of $n$ digits rather than a single digit (digits of the relevant dimension of $\mathcal{H}^P$), and so is $j$,

$$|0\rangle_E|i\rangle_P \otimes \cdots \otimes |0\rangle_E|i\rangle_P \rightarrow \sum_{j=0}^{(|\mathcal{H}^P|)^n-1} |E_{ij}\rangle_E |j\rangle_P \otimes \cdots \otimes |E_{ij}\rangle_E |j\rangle_P.$$

(2.27)

As before, Eve measures the ancilla, after learning all classical information, to obtain the optimal information on the final key or the final secret. As before, it is sufficient to define the transformation on the different input states of $(\mathcal{H}^A)^\otimes n$.

### 2.4.2 The QSoP is the effective attack space

In this section we show that Eve’s best attack is on the states in $\mathcal{H}^P$. In the case where $\mathcal{H}^P = M$, this result is trivial. Otherwise, $\mathcal{H}^P \subset M$ (and thus $\mathcal{H}^B \subset M$) and there exists some state $|\phi_0\rangle \in M$ such that $|\phi_0\rangle \in (\mathcal{H}^B)^\perp$. For any such $|\phi_0\rangle \in (\mathcal{H}^B)^\perp$, let us denote

$$\mathcal{H}^B_{\phi_0} = \mathcal{H}^B + \text{Span}\{|\phi_0\rangle\} \subseteq M.$$  

(2.28)

The sum is “direct” $(\mathcal{H}^B \cap \text{Span}\{\phi_0\} = \{0\})$ and for any two such states $\phi_0$ and $\phi_1$, $\mathcal{H}^B_{\phi_0}$ and $\mathcal{H}^B_{\phi_1}$ are isomorphic, with dimension dim$(\mathcal{H}^B) + 1$. Now let

$$\mathcal{H}^P_{\phi_0} = \mathcal{H}^A + \mathcal{H}^B_{\phi_0}.$$  

(2.29)
If $\mathcal{H}^A$ is not a subspace of $\mathcal{H}^B$, then there exists $\phi_0 \in \mathcal{H}^A$ such that $\phi_0 \not\in (\mathcal{H}^B)^\perp$ and for such $\phi_0$, we get $\mathcal{H}^P_{\phi_0} = \mathcal{H}^P$. Else, $\dim \mathcal{H}^P_{\phi_0} = \dim \mathcal{H}^P + 1$. We now show that in order to analyze the security of a protocol, we need only consider attacks on any particular $\mathcal{H}^P_{\phi_0}$.

**Proposition 2.17** For any $k \neq \text{loss}$, any $|\phi\rangle \in (\mathcal{H}^B)^\perp$, and for any $\rho \in \{|\phi\rangle \langle \phi|, |\psi\rangle \langle \phi|, |\phi\rangle \langle \psi|\}$,

$$\text{tr} \left[ O^B_{k\rho} \right] = 0.$$

**Proof** If $|\phi\rangle$ is orthogonal to $\mathcal{H}^B$ then it must be orthogonal to $\mathcal{H}^B_j$ and in particular to $O^B_{k\rho}(M) = \text{Ran} O^B_{k\rho}$ for any $k \neq \text{loss}$, i.e. $|\phi\rangle \in (\text{Ran} O^B_{k\rho})$. Therefore, $|\phi\rangle \in \text{Ker} O^B_{k\rho}$, so $O^B_{k\rho}|\phi\rangle = 0$, and for $\rho = |\phi\rangle \langle \phi|$ we get

$$\text{tr} \left[ O^B_{k\rho} \right] = 0.$$

For $\rho' = |\phi\rangle \langle \psi|$, $\text{tr} \left[ O^B_{k\rho'} \right] = \langle \psi| O^B_{k\rho} |\phi\rangle = 0$, and similarly for $\rho'' = |\psi\rangle \langle \phi|$, $\text{tr} \left[ O^B_{k\rho''} \right] = \langle \phi| O^B_{k\rho} |\psi\rangle = \langle \psi| (O^B_{k\rho})^\dagger |\phi\rangle = 0$. 

The above proposition means that the probability that Bob’s outcome of measuring any state of the form $|\phi\rangle \langle \phi|, |\psi\rangle \langle \phi|$ or $|\psi\rangle \langle \phi|$ with $\phi \in (\mathcal{H}^B)^\perp$ is the outcome loss with probability 1.

**Corollary 2.18** For any $|\phi\rangle \in (\mathcal{H}^B)^\perp$,

$$O^B_{\text{loss}}|\phi\rangle = |\phi\rangle. \quad (2.30)$$

We now show that any attack on the largest possible relevant space $M$, can be reduced to an attack in which Eve sends Bob states which are in a smaller space $\mathcal{H}^P_{\phi_0}$.

**Theorem 2.19** Let $\mathcal{U} : \mathcal{H}_E \otimes M \rightarrow \mathcal{H}_E \otimes M$ be Eve’s Attack on a protocol. For any $\phi_0 \in (\mathcal{H}^B)^\perp$ there is an attack $\mathcal{V} : \mathcal{H}_{E}^P \otimes \mathcal{H}^P_{\phi_0} \rightarrow \mathcal{X}_E \otimes \mathcal{H}^P_{\phi_0}$ that causes the same error rate as $\mathcal{U}$, where $\mathcal{H}_{E}^P = \mathcal{H}_E \otimes (\mathcal{H}^B)^\perp$, and with which Eve gets at least as much information as with $\mathcal{U}$.

**Proof** Let $|\psi\rangle$ be a basis of $\mathcal{H}^B$, and $|\phi\rangle$ a basis of $(\mathcal{H}^B)^\perp$ so that together they define a basis of $M$.

$$\mathcal{U}|0\rangle_E|\psi\rangle_A = \sum_{\psi} |E_{i\psi}\rangle |\psi\rangle + \sum_{\phi} |E_{i\phi}\rangle |\phi\rangle. \quad (2.31)$$
CHAPTER 2. QUANTUM SPACE ATTACKS

The density matrix of this state is given by

$$\rho = \sum_{\psi} |E_{iw}\rangle \langle \psi| + \sum_{\psi} |E_{iw}\rangle \langle \psi| + \sum_{\phi} |E_{iw}\rangle \langle \phi| + \sum_{\phi} |E_{iw}\rangle \langle \phi|$$

$$= \sum_{\psi} |E_{iw}\rangle \langle \psi| + \sum_{\phi} |E_{iw}\rangle \langle \phi| = \sum_{\psi} |E_{iw}\rangle \langle \psi| + \sum_{\phi} |E_{iw}\rangle \langle \phi|$$

(2.32)

Let $|e\rangle$ be a basis of Eve’s probe space. Tracing Eve’s probes out of the system is defined by

$$\rho_{Bob} = \sum_{e} \langle e| \rho| e\rangle.$$  

(2.33)

If for instance we let, $|E_{iw}\rangle = \sum_{e} \alpha_{e,iw}|e\rangle$, (and similarly for $|E_{iw}\rangle$, etc.), it is easy to see that

$$\sum_{e} \langle e| (|E_{iw}\rangle \langle E_{iw}|) |e\rangle = \sum_{e} \alpha_{e,iw} \bar{\alpha}_{e,iw} = \langle E_{iw}| E_{iw}\rangle,$$

thus Bob’s state obtained after tracing-out Eve, is

$$\rho_{Bob} = \sum_{\psi,\psi'} \langle E_{iw}| E_{iw}\rangle \langle \psi'| \psi\rangle + \sum_{\psi,\phi} \langle E_{iw}| E_{iw}\rangle \langle \phi| \psi\rangle + \sum_{\psi,\phi'} \langle E_{iw}| E_{iw}\rangle \langle \psi| \phi\rangle + \sum_{\phi,\phi'} \langle E_{iw}| E_{iw}\rangle \langle \phi| \phi\rangle.$$  

(2.34)

Using Proposition 2.17, we get that the probability that Bob obtains output $k \neq \text{loss}$ is

$$\text{tr} \left[ O_{k}^{B_{i}} \rho_{Bob} \right] = \sum_{\psi,\psi'} \langle E_{iw}| E_{iw}\rangle \text{tr} \left[ O_{k}^{B_{i}} \langle \psi'| \psi\rangle \right].$$  

(2.35)

We now define an equivalent attack that uses states in $H_{\phi_{0}}^{E}$. Without changing the notation, we simply add an ancilla in Eve’s hands, in a state $|\phi_{0}\rangle_{E}$, where $|\phi_{0}\rangle$ is some arbitrary state of $(H^{B})^\perp$,

$$U(0)_{E} |\phi_{0}\rangle_{E} |i\rangle_{A} = \sum_{\psi} |E_{iw}\rangle |\phi_{0}\rangle_{E} |\psi\rangle + \sum_{\phi} |E_{iw}\rangle |\phi_{0}\rangle_{E} |\phi\rangle.$$  

(2.36)

We now let Eve perform the following swap:

$$S(|\phi_{0}\rangle_{E} |\psi\rangle) = |\phi_{0}\rangle_{E} |\psi\rangle \quad \text{(no swap) for any} \ |\psi\rangle, \ \text{a basis state of} \ H^{B}, \ \text{and}$$

$$S(|\phi_{0}\rangle_{E} |\phi\rangle) = |\phi\rangle_{E} |\phi_{0}\rangle \quad \text{for any} \ |\phi\rangle, \ \text{a basis state of} \ (H^{B})^\perp.$$  

(2.37)

Since both $U$ and $S$ preserve orthogonality, so does their composition $S = S \circ U$, and

$$\mathcal{U} |0\rangle_{E} |\phi_{0}\rangle_{E} |i\rangle_{A} = \sum_{\psi} |E_{iw}\rangle |\phi_{0}\rangle_{E} |\psi\rangle + \sum_{\phi} |E_{iw}\rangle |\phi_{0}\rangle_{E} |\phi\rangle.$$  

(2.38)

extends to a unitary map$^6$ $\mathcal{U} : H_{E}^{A} \otimes (H^{A} + H_{\phi_{0}}^{B}) \rightarrow H_{E}^{A} \otimes (H^{A} + H_{\phi_{0}}^{B}).$

$^6$The Hilbert space on which $\mathcal{U}$ acts must contain all the vectors $|0\rangle_{E} |\phi_{0}\rangle_{E} |i\rangle_{A}$ as well as all the right-hand side members of (2.38).
Bob’s state, after tracing out Eve’s probes becomes
\[
\rho’_{Bob} = \sum_{\psi'} \langle E_{i\psi'}|E_{i\psi'}\rangle|\psi'\rangle\langle\psi'| + \sum_{\psi} \langle E_{i\phi_0}|E_{i\psi}\rangle|\psi\rangle\langle\phi_0| + \sum_{\psi} \langle E_{i\phi}|E_{i\phi_0}\rangle|\phi_0\rangle\langle\phi| + \sum_{\phi} \langle E_{i\phi}|E_{i\phi}\rangle|\phi_0\rangle\langle\phi_0|.
\] (2.39)
and we obtain exactly the same probability for measuring \(k \neq \text{loss}\) as in attack (2.31). Of course, the probability of obtaining output \(\text{loss}\) is equal to 1 minus the sum of the probabilities of obtaining \(k \neq \text{loss}\) and this means that the probabilities of all output in \(K_j\) are the same for both attacks and all setups \(j\), and consequently both attacks have exactly the same output distributions (and thus also the same error rate) for all of Bob’s measurements. Given Bob’s measurement procedure, both attacks are completely indistinguishable.

We now prove that Eve’s information can in no way be decreased by her new attack described by Equation (2.38); indeed, the very same final state is obtained with the following sequence of events:

1. Eve uses the attack \(U\) given by (2.31).
2. Bob changes his measurement procedure, creating himself a new ancilla in state \(|\phi_0\rangle_B\) and performing himself the swap used in Equation (2.37).
3. Bob then measures his state (which is in \(H^P_{\phi_0}\)), and

Clearly Bob’s measurement procedure can have no influence on Eve’s information. Moreover, being given Bob’s new probe, Eve’s information may only increase. As a consequence, Eve cannot be disadvantaged in any way with the attack described by (2.38). In addition, since \(H^A \subseteq H^P\) the attack is defined for every state sent by Alice. As said, the transformation of states outside \(H^A\) can be arbitrarily defined without any effect on the properties of the attack. Therefore the equivalent attack on \(H^P_{\phi_0}\) does not reduce Eve’s information, although it is not defined on the states that are outside \(H^P_{\phi_0}\) (but in \(M\)). As a conclusion, for any attack on \(M\), there is an attack on \(H^P_{\phi_0}\) that gives at least as much information to Eve and consequently Eve loses nothing in attacking \(H^P_{\phi_0}\) instead of \(M\).

**Theorem 2.20 (Main Theorem)** Eve’s most powerful attack can be done by attacking Alice’s states, and sending Bob states in \(H^P\).

**Proof** Let us just use the notations of the previous proof. Eve’s attack \(\mathcal{W}\) can be modified again by adding a single qubit probe as follows:
\[
\mathcal{W}^P|0\rangle_E|\phi_0\rangle_E|0\rangle_A = \sum_{\psi} \langle E_{i\psi}|\phi_0\rangle_E|0\rangle|\psi\rangle + \sum_{\phi} \langle E_{i\phi}|\phi\rangle_E|1\rangle|\phi_0\rangle.
\] (2.40)
CHAPTER 2. QUANTUM SPACE ATTACKS

If we trace-out Eve’s probes, the resulting state $\rho_{Bob}^P$ is given by
\[
\rho_{Bob}^P = \sum_{\psi,\psi'} \langle E_{i\psi} | E_{i\psi'} | \psi \rangle \langle \psi | + \sum_{\phi} \langle E_{i\phi} | E_{i\phi} | \phi \rangle \langle \phi |.
\]
(2.41)

Following Proposition 2.17, one can verify that
\[
\operatorname{tr} \left[ O_{Bj}^k \rho_{Bob}^P \right] = \operatorname{tr} \left[ O_{Bj}^k \rho_{Bob} \right]
\]
for every setup $j$ and output $k$; and the attack $\mathcal{A}^P$ thus preserves all of Bob’s probabilities of outputs.

We now show that the new attack does not reduce Eve’s information. As in Theorem 2.19, the map $\mathcal{A}^P$ can be interpreted as the attack $\mathcal{A}$ for which Bob would use the probe $|0\rangle$ instead of Eve, for some “pre-measurement” using the transformation
\[
|0\rangle \langle \psi | \rightarrow |0\rangle \langle \psi |
\]
for $|\psi\rangle \in \mathcal{H}^P$ and
\[
|0\rangle \langle \phi | \rightarrow |1\rangle \langle \phi |
\]
for $|\phi\rangle \in (\mathcal{H}^P)^\perp$, and giving the probe back to Eve. Bob’s measurement procedure can in no way affect Eve’s information, and Eve’s attack is equivalent to learning that Bob measured $|0\rangle$ or $|1\rangle$ which can in no way reduce her information.

We now notice that every time Bob measures $|1\rangle$ he could just abort the transmission, since the corresponding measurement on $|\phi_0\rangle$ with any of the measurements $\{O_{Bj}^k\}$ gives loss with probability 1. This is fully equivalent to Eve blocking the transmission (and thus forcing Bob outcome to loss), when measuring $|1\rangle$. The new attack is thus equivalent to the following scheme that uses $\mathcal{A}^P$:

1. Eve attack the protocol using $\mathcal{A}^P$.
2. Eve measures the single qubit probe.
3. Eve Blocks the transmission if she measures $|1\rangle$.
4. Otherwise, she sends Bob the subsystem in $\mathcal{H}^P$ and keeps her ancilla for later measurement.

This completes the proof.

2.5 A QSA Example

In this section we demonstrate the power of the QSA by giving a specific example. The given example matches a variant of a common BB84 scheme implemented with phase-encoded photons [82, 42], when restricting the transmissions up to a single photon per pulse. We give here an abstract attack without an extensive discussion of its realization, since our main focus is the QSA. In Chapter 3 we discuss the realization of such a scheme using interferometer and two (limited) detectors.
2.5. A QSA EXAMPLE

The protocol. We give a description of a single-photon BB84 with interferometer using the Hilbert-state notations. Assume Alice and Bob perform the following BB84 variant: Alice sends one of the four BB84 states \(|0\rangle, |1\rangle, |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |−\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\) along with an additional state \(|\epsilon\rangle\), which is considered as a loss. Alice’s space is the three-dimensional space \(H^A = H_3\). The space Alice uses is embedded in a larger space \(M = H_\infty\) with basis states \(|\epsilon\rangle, |n\rangle\), \(n = −\infty \ldots \infty\).

In order to measure the incoming state, Bob adds an ancilla which lays in \(H^{B'} = H_2\) and performs the following transformation (used for both the \(x\) and the \(z\) bases):

\[
\mathcal{U}(|\epsilon\rangle_A|0\rangle_{B'}) = |\epsilon\rangle_{AB'}, \quad \text{(2.43)}
\]

\[
\mathcal{U}(|n\rangle_A|0\rangle_{B'}) = \frac{1}{2}(|n0\rangle - (n + 1)|0\rangle + i|n1\rangle + i(n + 1)|1\rangle). \quad \text{ (2.44)}
\]

Linearly, we get

\[
\mathcal{U}|+0\rangle = \frac{1}{\sqrt{8}}(|00\rangle - |20\rangle + i|01\rangle + 2i|11\rangle + i|21\rangle), \quad \text{(2.45)}
\]

\[
\mathcal{U}|−0\rangle = \frac{1}{\sqrt{8}}(|00\rangle - 2|10\rangle + |20\rangle + i|01\rangle - i|21\rangle). \quad \text{(2.46)}
\]

Bob measures as follows: for the \(x\)-basis he uses the orthonormal projectors \(OP^x_+ = |11\rangle\langle11|, \quad OP^x_- = |10\rangle\langle10|\) and \(OP^x_{\text{loss}} = I - OP^x_+ - OP^x_-\), indicating measurement of \(|+\rangle\), \(|−\rangle\) and a loss respectively. For the \(z\)-basis the measurement operators take the form \(OP^z_0 = |01\rangle\langle01|, \quad P^z_1 = |20\rangle\langle20|\) and \(OP^z_{\text{loss}} = I - OP^z_0 - P^z_1\), indicating measurement of \(|0\rangle, |1\rangle\) and a loss respectively.

The QSoP. We follow Definitions (2.13)-(2.16) to analyze the optimal span of Eve’s attack. We begin with defining Bob’s measured spaces. Following Proposition 2.12, we need to find the equivalent POVM on \(M\) which is inferred by Bob’s measurement procedure. From direct calculations of Equation (2.22) we get

\[
U_0|\epsilon\rangle = |01\rangle\langle01|\epsilon\rangle = 0 \quad \quad U_1|\epsilon\rangle = |20\rangle\langle20|\epsilon\rangle = 0
\]

\[
U_0|n\rangle = \begin{cases} 
\frac{1}{2}i|01\rangle & \text{for } n = 0 \text{ and } n = -1 \\
0 & \text{otherwise}
\end{cases} \quad \quad U_1|n\rangle = \begin{cases} 
\frac{1}{2}|20\rangle & \text{for } n = 2 \\
\frac{1}{2}|20\rangle & \text{for } n = 1 \\
0 & \text{otherwise}
\end{cases}
\]

Which defines \(U_0\) and \(U_1\) as

\[
U_0 = \frac{1}{2}i|01\rangle\langle-1| + \frac{1}{2}2|01\rangle\langle0|, \quad \text{(2.47)}
\]

\[
U_1 = -\frac{1}{2}|20\rangle\langle1| + \frac{1}{2}|20\rangle\langle2|.
\]

Now

\[
U_0 = -\frac{1}{2}i|−1\rangle\langle01| - \frac{1}{2}i|0\rangle\langle01|, \quad \text{and} \quad U_1 = -\frac{1}{2}|1\rangle\langle20| + \frac{1}{2}|2\rangle\langle20|
\]
and consequently the POVM for the \(z\)-basis is defined by
\[
O_0^z = U_0^† U_0 = \frac{1}{4} [ \langle -1 | -1 \rangle \langle 0 | + \langle 0 | -1 \rangle + \langle 0 | 0 \rangle ],
\]
\[
O_1^z = U_1^† U_1 = \frac{1}{4} [ \langle 1 | 1 \rangle - \langle 1 | 2 \rangle - \langle 2 | 1 \rangle + \langle 2 | 2 \rangle ],
\]
\[
O_{\text{loss}}^z = I - O_0^z - O_1^z.
\]

Similarly, for the \(x\) basis, Bob performs the above \(U\) followed by the measurement with \(OP_x^z = \{|11\rangle\langle 11|\}\) and \(OP_x^z = \{|10\rangle\langle 10|\}\) as valid outcomes.
\[
U_+ |e\rangle = |11\rangle\langle 11|e0\rangle = 0 \quad \quad \quad \quad U_- |e\rangle = |10\rangle\langle 10|e0\rangle = 0
\]
\[
U_+ |n\rangle = \begin{cases} \frac{1}{2} |11\rangle & \text{for } n = 0 \text{ and } n = 1 \\ 0 & \text{otherwise} \end{cases} \quad \quad \quad \quad U_- |n\rangle = \begin{cases} \frac{1}{2} |20\rangle & \text{for } n = 0 \\ 0 & \text{otherwise} \end{cases}
\]
so that
\[
U_+ = \frac{1}{2} i |11\rangle \langle 0 | + \frac{1}{2} |11\rangle \langle 1 | \\
U_- = -\frac{1}{2} |10\rangle \langle 0 | + \frac{1}{2} |10\rangle \langle 1 |
\]
\[
U_+^† = -\frac{1}{2} i |0\rangle \langle 11 | - \frac{1}{2} |1\rangle \langle 11 | \\
U_-^† = -\frac{1}{2} |0\rangle \langle 10 | + \frac{1}{2} |1\rangle \langle 10 |
\]
so the equivalent POVM on \(M\) for the \(x\) basis measurement is
\[
O_+^x = U_+^† U_+ = \frac{1}{4} [ |0\rangle \langle 0 | + |0\rangle \langle 1 | + |1\rangle \langle 0 | + |1\rangle \langle 1 | ],
\]
\[
O_-^x = U_-^† U_- = \frac{1}{4} [ |0\rangle \langle 0 | - |0\rangle \langle 1 | - |1\rangle \langle 0 | + |1\rangle \langle 1 | ],
\]
\[
O_{\text{loss}}^x = I - O_+^x - O_-^x.
\]

Thus according to Definition 2.15, the effective space of Bob, \(\mathcal{H}_B = \mathcal{H}_B^0 + \mathcal{H}_B^1\), is spanned by \(|\{-1\}, |0\}, |1\}, |2\}\rangle\). The QSoP \(\mathcal{H}_P\), is given by Definition 2.16, and is spanned by \(|\{-1\}, |0\}, |1\}, |2\}, |e\}\rangle\}

**The Attack.** Eve performs the following attack (on states in \(\mathcal{H}_A \subseteq M\)):
\[
U_E |0\rangle_E |0\rangle_A = \frac{1}{2} |E_0\rangle \langle -1 | \langle 0 | + \frac{1}{2} |E_2\rangle \langle 0 | \langle 0 | + \frac{1}{2} |E_3\rangle \langle 1 | \langle 0 | + \frac{1}{2} |E_3\rangle \langle 1 | \langle 0 |
\]
\[
U_E |0\rangle_E |1\rangle_A = \frac{1}{2} |E_3\rangle \langle -1 | \langle 0 | \langle 0 | + \frac{1}{2} |E_2\rangle \langle 1 | \langle 0 | - \frac{1}{2} |E_1\rangle \langle 2 |
\]
\[
U_E |0\rangle_E |e\rangle_A = |E_e\rangle \langle e | \langle e |
\]

One can easily check that this attack gives Eve full information of the transmitted key, while inducing no errors at all. In this case the attack is on a space of dimension \(\text{dim}(\mathcal{H}_P)\) instead of \(\text{dim}(\mathcal{H}_P) + 1\), since Eve is able to cause a loss using the state \(|e\rangle \in \mathcal{H}_P\). Again, we refer the reader to Section 3.6.2 which shows that the above is a successful attack on a specific implementation variant of the BB84 protocol.
2.6 Known QKD Attacks as QSAs

All of the known attacks on practical QKD schemes can be considered as special cases of the Quantum-Space Attacks. In this section we show a description of several such attacks using QSA terms. For each and every attack we briefly describe the specific protocol used, the quantum space of the protocol, and a realization of the attack as a QSA.

2.6.1 The photon number splitting attack [21]

The Protocol. Consider a BB84 protocol, where Alice uses a “weak pulse” laser to send photons in two modes corresponding to the vertical and horizontal polarizations when using the $z$ basis (the diagonal polarizations then relate to using the $x$ basis). Bob uses a device called a Pockels cell to rotate the polarization (by $45^\circ$) for measuring the $x$ basis, or performs no rotation if measuring the $z$ basis. The measurement of the state is then done using two detectors and a “polarization beam splitter” that passes the first mode to one detector and the second mode to the other detector (for a survey of polarization-based QKD experiments, see [35, 26]).

The Quantum Space of the Protocol. Every pulse sent by Alice is in one of four states, where each is a mixture of the six orthogonal basis states of $H_A = \chi_6$, as described in Section 2.3.1. Bob uses two setups, $U_{B_z} = I$ for the $z$ basis, and $U_{B_x} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$ for the $x$ basis.

The detectors used by Bob cannot distinguish between modes having a single photon and multiple photons (see Section 3.2.5). Each one of his two detectors measures the basis elements $\{|b^n\rangle\}$ for $b = \{0,1\}$ and $n \geq 0$, where Bob interprets the states $\{|b^n\rangle\}$ with $n > 1$ as measuring the state $|b\rangle$, i.e. his POVM can be defined as

$$P_0 = \sum_{n=1}^{\infty} |0^n\rangle\langle 0^n|, \quad P_1 = \sum_{n=1}^{\infty} |1^n\rangle\langle 1^n|, \quad P_{\text{loss}} = |\epsilon\rangle\langle \epsilon|.$$ (2.53)

Any other outcome is considered as an error. Bob’s effective space $H_B = M$ is the infinite space. In this case, the QSoP $H^P$ is equal to $H_B = M$. Note that even if Bob was ideal ($H_B = H_A$), the QSoP would not be $H_2$ but $\chi_6$, which would allow the PNS attack.

The Attack. Eve measures the number of photons in the pulse, using non-demolition measurement. If she finds that the number of photons is $\leq 1$, she blocks the pulse and generates a loss. In the case she finds that the pulse consists of $2$ photons, she splits one photon out of the pulse and sends it to Bob, keeping the other photon until the bases are revealed, thus getting full information of the key-bit. Eve sends the eavesdropped qubits to Bob via a lossless channel so that Bob will not notice the enhanced loss-rate. As is

$^7$Let $b^n = bbb\ldots b$, i.e. the string of length $n$ whose each digit is $b$. 

Technion - Computer Science Department - M.Sc. Thesis  MSC-2009-03 - 2009
common in experimental QKD, Bob is willing to accept a high loss-rate (he does not count losses as errors), since most of Alice’s pulses are empty.

2.6.2 The tagging attack (based on [38])

The Protocol. Consider a BB84 realization in which Alice sends, without any intention or knowledge, an enlarged state rather than a qubit. This state contains, besides the information qubit, a tag giving Eve some information about the bit. The tag can, for example, tell Eve the basis being used by Alice. For a potentially realistic example, let the tag be an additional qutrit indicating if Alice used the $x$-basis, or the $z$-basis, or whether the basis is unknown: due to a fault in her equipment, whenever Alice switches basis, a single photon comes out of her lab prior to her information-carrier pulse, revealing the new basis chosen by Alice, encoded by the states $|2\rangle_{\text{tag}}$ and $|3\rangle_{\text{tag}}$, for instance, whereas there is no basis change, what comes out prior to the information qubit is just the vacuum state $|\epsilon\rangle_{\text{tag}}$.

The Quantum Space of the Protocol. In this example, Alice’s space, $\mathcal{H}^A \subset S_1(\mathcal{H}_2^{(1)}) + S_2(\mathcal{H}_4^{(2)})$, is spanned by $\{|0\rangle, |1\rangle, S_2(|0\rangle|2\rangle), S_2(|0\rangle|3\rangle), S_2(|1\rangle|2\rangle), S_2(|1\rangle|3\rangle\}$. Bob, unaware of the enlarged space used by Alice, expects and measures only the information-photon, so if the tag contains a photon, Bob measurement indicates an un-synchronized transmission (a photon that came too early) and consider the transmission as a loss. For any setup $j$, assume Bob measures $H_2$ (spanned by $|0\rangle$ and $|1\rangle$) using the projection $P^j_k$. The imposed POVM (on $M$) can be defined as $O^j_k = P^j_k$ and $O^j_{\text{loss}} = I - \sum_k P^j_k$. Thus, Bob’s effective space $\mathcal{H}^B$, is (at most) the 2-dimensional subspace $\mathcal{H}_2$ spanned by $|0\rangle$ and $|1\rangle$.

However, the tag, although not in Bob’s effective space, is of a much use to Eve, and indeed, following Definition 2.16, the QSoP is defined to be $\mathcal{H}^P = \mathcal{H}^A$.

The Attack. Eve uses the tag in order to retrieve information about the qubit without inducing error (e.g. via cloning the information qubit in the proper basis). The attack is then an intercept-resend QSA. Surprisingly, by using the tag, Eve decreases the expected loss rate since all the transmissions to Bob become valid, once the tag is omitted. We mention that this attack is very similar to side-channel attacks of classic cryptosystems.\footnote{This is since the tag is actually another channel that reveals information, which is equivalent to classical side-channels such as power consumption or EM radiation, that give extra information as a side-effect of the specific implementation.}

A Short Summary. It can be seen that the PNS attack described above is actually a special case of the tagging attack, where the tag in this case is in fact another copy of the transmitted qubit. This copy is kept by Eve until the bases are revealed, then it can be measured so that the key-bit value is exposed with certainty. Both these QSA attacks are based on the fact that Alice’s (realistic) space is larger than the theoretical one.
in the PNS example, the QSoP is further extended due to Bob’s measurement, the attack is not based on that extension but on the fact that $\mathcal{H}^A$ is larger than $\mathcal{H}_2$. In the following attacks Bob’s measurements cause the enlargement of the QSoP, allowing Eve to exploit the larger QSoP for her attack.

### 2.6.3 The Trojan-pony attack [38, 45]

In Trojan-pony attacks Eve modifies the state sent to Bob in a way that gives her information. In contrast to a “Trojan-horse” that goes in-and-out of Bob’s lab, the “pony” only goes in, therefore, it is not considered an attack on the lab, but only on the channel. We present here an interesting example [38].

#### The Protocol

Assume a polarization-encoded BB84 protocol, in which Alice is ideal, namely, sending perfect qubits ($\mathcal{H}^A = \mathcal{H}_2$). However, Bob uses realistic threshold detectors that suffer from losses and dark counts, and that cannot distinguish between one photon and $k$ photons for $1 < k < L$. In order to be able to “prove” security for a longer distance of transmission, Bob wants to keep the error-rate low despite of the increase of dark counts’ impact with the distance [21]. Therefore, Bob assumes that Eve has no control over dark counts, and whenever both his detectors click, Alice and Bob agree to consider it as a loss since it is outside of Eve’s control (i.e. the QSoP is falsely considered to be $\mathcal{H}_2$). Namely, they assume that an error occurs only when Bob measures in the right basis, and only one detector clicks, (which is the detector corresponding to the wrong bit-value).

#### The Quantum Space of the Protocol

Same as in Section 2.6.1, Bob’s effective space $\mathcal{H}^B$, as well as the QSoP $\mathcal{H}^P$, are merely the spaces describing two modes (say, with up to $L$ photons), $\bigoplus_{n=0}^{L} S_n (\mathcal{H}_2^\otimes n)$. Bob’s detectors cannot distinguish between receiving a single-photon pulse from a multi-photon pulse, so his measurement can be described by the following three outputs: “$\{10\} \equiv$ detector-1 clicks”, “$\{01\} \equiv$ detector-2 clicks”, and else it is $\{00\}$, a “loss”. formally, these three possible results are written as:

$$
\begin{align*}
\mathcal{P}_{\{10\}} \equiv & \sum_{k=1}^{L-1} |0^k\rangle\langle 0^k|, \\
\mathcal{P}_{\{01\}} \equiv & \sum_{k=1}^{L-1} |1^k\rangle\langle 1^k|, \\
\mathcal{P}_{\text{loss}} = & \mathcal{P}_{\{00\}} \equiv I - \mathcal{P}_{\{0\}} - \mathcal{P}_{\{1\}}.
\end{align*}
$$

#### The Attack

Eve’s attack is the following: (a) Randomly choose a basis (b) Measure the arriving qubit in that specific chosen basis (c) Send Bob $m$-photons identical to the measured qubit, where $m \gg 1$. Obviously, when Eve chooses the same basis as Alice and Bob then Bob measures the exact value sent by Alice, and Eve gets full information. Otherwise, both of his detectors click, implying a “loss”, except for a negligible probability, $\approx 2^{-(m+1)}$, thus Eve induces almost no errors. The main observation of this measure-resend QSA is that treating a count of more than a single photon as a loss, rather than as an error, is usually not justified. A second conclusion is that letting Bob use counters instead of threshold detectors (to distinguish a single photon from multiple photons), together with treating any count of more than one photon as an error, could be vital for proving security against QSA. The price is that dark counts put severe restrictions on
the distance to which communication can still be considered secure, as already suggested in [21].

2.6.4 The fake-state attack (based on [56, 55])

The Protocol. In this example, we examine a polarization encoded BB84 realization, with an ideal Alice ($\mathcal{H}^A = \mathcal{H}_2$). This time Bob’s detectors are imperfect so that their detection windows do not fully overlap, meaning that there exist times in which one detector is blocked (has a low efficiency), while the other detector is still regularly active (see Figure 2.2). Thus, if Eve can control the precise timing of the pulse, she can control whether or not the photon is detected. The setup consists of four detectors and a rotating mirror (since Bob does not want to spend money on a Pockels cell (polarization rotator), he actually uses 2 fixed different setups). Using the rotating mirror Bob sends the photon into the $z$ basis detection setup or into the $x$ basis detection setup. Suppose the two detection setups use slightly different detectors, or slightly different delay lines, or slightly different shutters, and Eve is aware of this (possibly from past attacks on the system). For simplicity, we model the non-overlapping detection windows as two additional pairs of modes, one slightly prior to Alice’s intended mode (the pulse), and one right after it.

The Quantum Space of the Protocol. The original qubit is sent in a specific time $t_0$ (namely, $\mathcal{H}^A = \mathcal{H}_2 = S_1(\mathcal{H}_2)$). The setup for the $z$ basis is a set of two detectors and a polarized beam splitter, separating the horizontal and the vertical modes to the detectors, where the setup for the $x$ basis separates the diagonal modes to a set of two

![Figure 2.2: Bob’s setup: a rotating mirror (RM) chooses the appropriate detectors according to the desired basis. The left side plots the detectors efficiency of the $x$ and $z$ measurement setup, with respect to time. The efficiencies do not fully overlap which allows times that are measured only by a single chosen basis](image)
(different) detectors. Let the detectors for one basis, say \( z \), be able to measure a pulse arriving at \( t_0 \) or \( t_1 \), while the detectors for the other basis (\( x \)) measure pulses arriving at \( t_{-1} \) or \( t_0 \). This implies that \( M \) has 6 possible orthogonal modes (instead of 2), i.e. it is the space \( \bigoplus_n S_0(\mathcal{H}_6^{\otimes n}) \); we restrict the analysis for the case of at most one photon, therefore \( M = S_0(\mathcal{H}_6^{\otimes 0}) + S_1(\mathcal{H}_6^{\otimes 1}) \). Denote \(|0\rangle, |1\rangle \) the horizontal, vertical photon at time \( t_0 \); \(|2\rangle, |3\rangle \) at time \( t_{-1} \); and \(|4\rangle, |5\rangle \) at time \( t_1 \). Using these notations, Alice’s space \( \mathcal{H}^A \) is redefined as a 2-dimensional subspace of \( M \) in which the time-modes \( t_{-1} \) and \( t_1 \) contain no photons; i.e. the subspace spanned by \( \{ |0\rangle, |1\rangle \} \).

Following Definition 2.13, let us define Bob’s POVM for the different setups. For the \( z \) basis he uses

\[
P_0^z = |0\rangle\langle 0| + |4\rangle\langle 4|; \quad P_1^z = |1\rangle\langle 1| + |5\rangle\langle 5|; \quad P_{\text{loss}}^z = |\epsilon\rangle\langle \epsilon| + |2\rangle\langle 2| + |3\rangle\langle 3|. \tag{2.54}
\]

Define

\[
|+\rangle_{t_0} = (|0\rangle + |1\rangle)/\sqrt{2}, \quad |+\rangle_{t_{-1}} = (|2\rangle + |3\rangle)/\sqrt{2}
\]

and similarly

\[
|\rangle_{t_0} = (|0\rangle - |1\rangle)/\sqrt{2}, \quad |\rangle_{t_{-1}} = (|2\rangle - |3\rangle)/\sqrt{2}. \tag{2.56}
\]

Bob’s POVM for the \( x \) basis is

\[
P_0^x = |+\rangle_{t_0}\langle +| + |+\rangle_{t_{-1}}\langle +|; \quad P_1^x = |\rangle_{t_0}\langle -| + |-\rangle_{t_{-1}}\langle -|; \quad P_{\text{loss}}^x = |\epsilon\rangle\langle \epsilon| + |4\rangle\langle 4| + |5\rangle\langle 5|. \tag{2.57}
\]

The resulting measured subspaces are \( \mathcal{H}^{B_z} \) spanned by \( \{ |0\rangle, |1\rangle, |4\rangle, |5\rangle \} \) and \( \mathcal{H}^{B_x} \) which is spanned by \( \{ |0\rangle, |1\rangle, |2\rangle, |3\rangle \} \). Thus the effective space, as well as the QSoP is the subspace of \( M \) containing exactly one photon, \( S_1(\mathcal{H}_6^{\otimes 1}) \).

**The Attack.** Eve exploits the larger space by sending “fake” states using the external times \( (t_{-1} \) and \( t_1 \)). Eve randomly chooses a basis, measures the qubit sent by Alice, and sends Bob the same polarization state she found, but at \( t_{-1} \) if she used the \( x \) basis, or at \( t_1 \) if she used the \( z \) basis. Since no ancilla is kept by Eve, this is an intercept-resend QSA.

Bob will get the same result as Eve if he uses the same basis, or a loss otherwise. The mathematical description of the attack is as follows: Eve’s measure-resend attack is described as measuring Alice’s qubit in the \( x \) basis, creating a new copy of the measured qubit, and performing the transformation \( (|0\rangle \rightarrow E_x |2\rangle); (|1\rangle \rightarrow E_x |3\rangle) \) or as performing a measurement in the \( z \) basis, and performing the transformation \( (|0\rangle \rightarrow E_z |4\rangle); (|1\rangle \rightarrow E_z |5\rangle) \) on the generated copy.

**A short summary** We see that Eve can “force” a desired value (or a loss) on Bob, thus gaining all the information while inducing no errors (but increasing the loss rate). Bob can use a shutter to block the channel during the time a transmission is not expected.
Yet, such a shutter could generate a similar problem in the frequency domain. This attack is actually a special case of the Trojan-pony attack, in which the imperfections of Bob’s detectors allow Eve to send states that will be un-noticed unless Bob’s measurement basis is identical to Eve’s encoding basis.

2.7 Concluding Remarks

The main conclusion of this chapter is that the quantum space which is attacked by Eve in realistic protocols can be assessed, given a proper understanding of the experimental limitations. The QSA formalism defines the space which is relevant for the attack. No advantage is given by attacking a larger space, yet attacking a smaller space (such as the theoretical space of a protocol) might restrict the power of the eavesdropper. This understanding is vital for security analyses of practical QKD schemes.

It is claimed that the QSoP presented above is the most general space for Eve that attacks the channel. Yet, in defining this space, we used the POVM method that actually hides the details of the measurement performed by Bob. In other words, If Eve knows the exact procedure of Bob’s measurement (rather than the imposed POVM), can she better attack the Protocol? We have proved that the QSoP is the effective attack space, therefore even if Eve has a better knowledge of Bob’s action, she has no advantage in attacking states that are orthogonal to the QSoP defined above. On the other hand, we know that any state that in the QSoP might either (a) be informative to Eve or (b) affects Bob measurement. The QSoP never defines Eve’s best attack; in order to compose her best attack, Eve might use only a sub-space of the QSoP. Therefore, knowing the exact measurement process performed by Bob might help Eve to compose a better QSA, yet she will always attack a subspace which is contained in or equal to the QSoP defined above. It is possible that Eve will use a different subspace of the QSoP for any given implementation of Bob’s equipment.

We would like to emphasize several issues:

1. When analyzing specific attacks, or when trying to obtain a limited security result, it is always legitimate to restrict the analysis to the relevant (smaller) subspace of the QSoP, for simplicity, e.g., to $\mathcal{H}^A$, or to $\mathcal{H}^B$, etc.

2. Any bi-directional protocol will have a much more complicated QSoP, thus it might be extremely difficult to analyze any type of QSA (even the simplest ones) on such protocols. This remark is especially important since bi-directional protocols play a very important role in QKD, since they appear in many interesting protocols such as the plug-and-play [61], the ping-pong [14], and the classical Bob [18, 19] protocols. Specifically they provided (via the plug-and-play) the only commercial QKD so far [88, 89].
3. It is well known that the collective or joint attack is only finished after Eve gets all the quantum and classical information, since she delays her measurements till then [12, 11, 9, 57, 10]; if she expects more information, she better wait and attack the final secret rather than the final key; it is important to notice that if the key will be used to encode quantum information (say, qubits) then the quantum-space of the protocol will require a modification, potentially a major one; It is interesting to study if this new notion of QSoP has an influence on analysis of such usage of the key as done (for the ideal qubits) in [5, 69].
Interferometry, like surfing, is a search for the perfect wave. But physicists don’t have to paddle around and wait.  

K. A. Goldberg

Chapter 3

Analysis of Interferometric QKD Schemes

3.1 Introduction

In this chapter, we analyze and discuss the security of QKD protocols implemented using photons as the quantum carrier. As shown in the previous chapter, the implementation of QKD protocols often causes the emergence of new security holes, and such implementations requires a thorough analysis in order to be proven secure.

A common implementation of the BB84 QKD protocol [7] is a phase-encoded, time-multiplexed scheme. This implementation uses photons as the quantum carriers, where the information bit is encoded as the phase difference between two superpositioned pulses [82, 42, 36].

Many of nowadays QKD protocols are implemented using interferometers for producing phase-encoded photons and detecting them (See detailed description in section 3.2). An interferometer (usually, a Mach-Zender interferometer) is used in many different variants of QKD protocols, such as the Differential Phase Shift QKD (DPS-QKD) [47, 79, 80], that extends the above time-multiplexing scheme by encoding the information bit as a phase shift of three superpositioned pulses (instead of two). Another variant, used in many experiments [61, 78] and products [88, 89] is the Plug & Play protocol in which the signal is originated by Bob, sent over to Alice (who modulates its phase), and then sent back to be measured by Bob.

Proving security of a given protocol is not a simple task. Although the theoretical BB84 protocol has been proven secure against the most powerful attack [76, 57, 10], the proof does not apply to realistic variants [21]. Some security analyses have been published [54, 83] dealing only with special cases: a specific protocol variant (DPSQKD, Plug&Play, etc.) or a specific eavesdropping method (individual attack, collective attack, etc.). In addition, recent analyses have considered the security of protocols realized by imperfect equipment, such as faulty sources and detectors [58, 38, 46]. These proofs usually
apply to a restricted protocol (e.g. having a perfect photon source or a basis-independent measurement), since the specific realization of a protocol has a great influence on its security.

In the following sections we present analysis of interferometric based QKD schemes. We design a novel type of attack, the reversed-space attack. It is based on looking not on what Alice sends, but on what Bob measures. In view of this new attack, we discuss several variants of the time-multiplexing BB84 and six-state schemes, proving robustness of several variants, while showing another variant that is completely nonrobust and therefore insecure. Other protocols (Plug&Play, Classical-Bob [19], etc.) might be more prone to such attacks, due to their bi-directional nature. However, this analysis is yet to be done.

This Chapter is based on [32].

3.2 Model of the Equipment Used

Let us describe a mathematical model of the equipment used in the protocol: the interferometer. An interferometer (Figure 3.1) is built out of two beam splitters (BS) with one short path and one long path, and a controlled phase shifter $P_{\phi}$, that is placed on the long arm of the interferometer. A pulse of light, entering the interferometer at time $t_0^\prime$, travels through the short arm of the interferometer in $T_{\text{short}}$ seconds, and through the long arm in $T_{\text{short}} + \Delta T$ seconds. The pulse exiting the interferometer is composed of a superposition of (time-bins) modes $t_0 \equiv t_0^\prime + T_{\text{short}}$ and $t_1 \equiv t_0 + \Delta T$.

3.2.1 Beam splitter

Each beam splitter (Figure 3.2) has two input arms (modes 1, 2) and two output arms (modes 3, 4). Each photon entering the beam splitter is transmitted/ reflected with probability of 50%; The transmitted part keeps the same phase as the incoming photon, while
3.2. MODEL OF THE EQUIPMENT USED

Figure 3.2: A symmetric beam-splitter. Two input modes (1) and (2) and two output modes (3) and (4).

the reflected part gets an extra phase of $e^{i\pi/2}$. Thus, for a single photon state, the transformation is of the form

$$\alpha|10\rangle_{1,2} + \beta|01\rangle_{1,2} \rightarrow \frac{\alpha + i\beta}{\sqrt{2}}|10\rangle_{3,4} + \frac{i\alpha + \beta}{\sqrt{2}}|01\rangle_{3,4}.$$ (3.1)

It is important to notice that when a single mode (carrying a single photon) enters a beam splitter from one arm, and nothing (namely, vacuum) enters the other arm, there are still two output modes, which means that the other (vacuum) entry must be considered as an additional mode (an ancilla carrying no photons).

3.2.2 Phase shifter

The controlled phase shifter $P_\phi$ performs a phase shift of a given phase $\phi$, and can be written as

$$P_\phi(|n\rangle^F) = e^{i\phi}|n\rangle^F.$$ (3.2)

Bob controls the phase according to his specific measurement basis. For instance, usually for performing a measurement in the $x$ basis Bob sets $\phi = 0$, and when he measures the $y$ basis he sets $\phi = \pi/2$, see Section 3.3.1.

3.2.3 Evolution of a single mode in an interferometer

When a single mode, carrying one or more photons, enters the interferometer, three ancillas, each in a vacuum state, are added by the interferometer: the mode entering the interferometer at time $t'_0$, yields two modes at time $t_0$ (due to traveling through the short arm) and two modes at time $t_1$. These four output modes are: times $t_0$, $t_1$ in the ‘s’

---

1See [33] for further information.
(straight) arm of the interferometer, and times \( t_0, t_1 \) in the ‘d’ (down) arm of the interferometer. A basis state in this Fock space is then \( |n_{s_0}, n_{s_1}, n_{d_0}, n_{d_1}\rangle^F \). In the case of a single mode carrying a single photon in the Fock space whose basis states are \( |1\rangle^F, |2\rangle^F, \ldots \), the transformation (with the additional three empty ancillas) is \( |1\rangle^F_{t_0'} |000\rangle^F \rightarrow (|1000\rangle^F - |0100\rangle^F + i|0010\rangle^F + i|0001\rangle^F) /2 \). Note that a pulse which is sent at a different time (say, \( t_1' \), or \( t_{-1}' \), etc.) results in the same output state, but with appropriate delays, e.g., a pulse entering the interferometer at time \( t_1' \) results in the Fock space whose basis states are \( |n_{s_1}, n_{s_2}, n_{d_1}, n_{d_2}\rangle^F \).

A detailed description of this evolution is shown in Figure 3.3. The evolution in time of a single photon pulse through the interferometer (with \( \phi = 0 \)) satisfies

\[
|1000\rangle^F_{1,1',2,3'} \rightarrow \frac{1}{2} (|1000\rangle^F - |0100\rangle^F + i|0010\rangle^F + i|0001\rangle^F)_{5,7,4,6},
\]

where the output state \( |n_{s_0}, n_{s_1}, n_{d_0}, n_{d_1}\rangle^F \) corresponds modes (5), (7), (4) and (6) respectively.

### 3.2.4 Evolution of two modes in an interferometer

We are now ready to consider two input modes, \( t_0' \) and \( t_1' \), that enter the interferometer one after the other, with exactly the same time difference \( \Delta T \) as the length difference of the interferometer arms. As a result of this precise timing, these two modes are transformed into a superposition of six possible modes (instead of eight modes) at the outputs, due to interference at the second beam splitter. Four (vacuum state) ancillas are added during the process and the resulting six modes are \( t_0, t_1, t_2 \) in the ‘s’ arm and in the ‘d’ arm of the interferometer. A basis state in this Fock space is then \( |n_{s_0}, n_{s_1}, n_{s_2}, n_{d_0}, n_{d_1}, n_{d_2}\rangle^F \), and a general state is a superposition of those states. The evolution in time of two modes through the interferometer (with \( \phi = 0 \)), is described in Figure 3.4, and satisfies

\[
(\alpha |1\rangle^F_{11} |0\rangle^F_{12} + \beta |0\rangle^F_{11} |1\rangle^F_{12}) |0000\rangle^F_{1',2',3',4'} \rightarrow
\frac{1}{2} (100000\rangle^F + \frac{\beta - \alpha}{2} |010000\rangle^F - \frac{\beta}{2} |001000\rangle^F + \frac{i\alpha}{2} |000100\rangle^F +
\frac{i(\alpha + \beta)}{2} |000010\rangle^F + \frac{i\beta}{2} |000001\rangle^F)_{8,10,12,7,9,11}
\]

(3.4)

where the output state \( |n_{s_0}, n_{s_1}, n_{s_2}, n_{d_0}, n_{d_1}, n_{d_2}\rangle^F \) corresponds modes (8), (10), (12), (7), (9) and (11) respectively.

Theoretically Alice sends pulses with exactly one photon, yielding in a superposition of the following six states (that we denote for simplicity by)

\[
|000000\rangle^F \equiv |s_0\rangle, |010000\rangle^F \equiv |s_1\rangle, |001000\rangle^F \equiv |s_2\rangle,
|000100\rangle^F \equiv |d_0\rangle, |000010\rangle^F \equiv |d_1\rangle, |000001\rangle^F \equiv |d_2\rangle,
\]

and (3.5)

\[
|000000\rangle^V \equiv |V\rangle \text{ the vacuum state.}
\]
3.2. MODEL OF THE EQUIPMENT USED

Pulse (1) is about to enter the interferometer. A vacuum ancilla (1’) is added in the input of the first beam splitter, $BS_1$.

Pulses (1) and (1’) interfere in the first beam splitter ($BS_1$) and yield a superposition of (2) and (3) in the short and long arms of the interferometer, respectively, $|1⟩^f_1|0⟩^f_1 \xrightarrow{BS_1} (|1⟩^f_2|0⟩^f_3 + i|0⟩^f_2|1⟩^f_3)/\sqrt{2}$. Pulse (2) is about to enter the second beam splitter ($BS_2$) so a vacuum ancilla is added (2’).

Pulses (4) and (5) are created by pulses (2) and (2’), $\frac{1}{\sqrt{2}}|0⟩^f_2|1⟩^f_2 \xrightarrow{BS_2} (i|1⟩^f_4|0⟩^f_5 + |0⟩^f_4|1⟩^f_5)/2$. Pulse (3) is about to enter the second beam-splitter so a vacuum ancilla is added (3’).

Pulses (6) and (7) are created by the interference of (3) and (3’), $\frac{1}{\sqrt{2}}|1⟩^f_3|0⟩^f_3 \xrightarrow{BS_2} (i|1⟩^f_6|0⟩^f_7 - |0⟩^f_6|1⟩^f_7)/2$.

Figure 3.3: Evolution in time of a single mode in an interferometer
A general single-photon qubit \((\alpha|10}_F + \beta|01}_F\) is sent to Bob in two modes (2) and (1), respectively. Bob adds a vacuum ancillas (1’) that will interfere with mode (1) in the first beam splitter \((BS_1)\).

Pulses (1) and (1’) interfere and yield pulses (3) and (4) in the short arm and the long arm respectively, \(\alpha|1}_F|0}_F + \beta|0}_F|1}_F\). Pulse (3) is about to enter \(BS_2\), so a vacuum ancilla (3’) is added. Pulse (2) is about to enter \(BS_1\) so a vacuum ancilla (2’) is added. [The order of these last two events does not matter.]

Pulses (7) and (8) are created by the interference of (3) and (3’) \(\frac{\alpha}{\sqrt{2}}|0}_F^3|1}_F^3 + \frac{\beta}{\sqrt{2}}|0}_F^3|1}_F^3\). Pulses (5) and (6) are created by the interference of (2) and (2’) in \(BS_1\) \(\beta|1}_F^2|0}_F^2 + \alpha|0}_F^2|1}_F^2\).

Pulses (9) and (10) are created by the interference of (4) and (5) in the second beam-splitter \(\frac{\alpha}{\sqrt{2}}|1}_F^4|0}_F^4 + \frac{\beta}{\sqrt{2}}|0}_F^4|1}_F^4\). Pulse (6) is about to enter \(BS_2\) so a vacuum ancilla is added (6’).

Pulses (11) and (12) are created by the interference of (6) and (6’) in \(BS_2\) \(\frac{i\alpha}{\sqrt{2}}|1}_F^6|0}_F^6 + \frac{i\beta}{\sqrt{2}}|1}_F^6|0}_F^6\).
Bob is able to set the phase shifter placed in the long arm of the interferometer to a desired phase $e^{i\phi}$, so that the complete interferometer transformation of a single photon basis state is described by

$$
\begin{align*}
|00\rangle_{0000}^F &\rightarrow |V\rangle, \\
|10\rangle_{0000}^F &\rightarrow \frac{1}{2} \left( |s_0\rangle - e^{i\phi}|s_1\rangle + i|d_0\rangle + ie^{i\phi}|d_1\rangle \right), \\
|01\rangle_{0000}^F &\rightarrow \frac{1}{2} \left( |s_1\rangle - e^{i\phi}|s_2\rangle + i|d_1\rangle + ie^{i\phi}|d_2\rangle \right),
\end{align*}
$$

where $|0000\rangle^F_B$ is the added ancillas.

In Appendix A we derive the transformation for a general pulse in an interferometer.

### 3.2.5 Detectors and Measurement

Bob’s ideal measurement of the $K$-mode Fock state $|n_1, n_2, \ldots, n_K\rangle^F$ is commonly assumed to be limited to a complete measurement that yields the number of photons occupying the different modes, i.e. the numbers $n_1$ to $n_K$. However, a realistic Bob usually performs an *incomplete measurement*, in which some modes might not be measured, and in some modes he cannot detect the exact number of photons.

For instance, Bob might measure a mode using a *threshold detector* and only determine whether the mode is empty (the number of photons is zero) or non-empty (the number of photons is $\geq 1$), i.e. for measuring the $i$-th mode Bob uses the projection

$$
P_i = \sum_{n_i=1}^{\infty} |n_1, n_2, \ldots, n_K\rangle^F \langle n_1, n_2, \ldots, n_K|,
$$

where $n_j = 0$ for $j \neq i$. A better measurement allows him to distinguish the exact number of photons populating the mode, using a *counter* which is a *photon-number-resolving* detector [50, 1, 40].

Bob can measure other specific properties of the state in addition to the number of photons populating each mode, using (for instance) beam splitters, phase shifters and mirrors [66]. For example, let us assume that Bob wants to distinguish the state $(|10\rangle^F + |01\rangle^F)/\sqrt{2}$ from $(|10\rangle^F - |01\rangle^F)/\sqrt{2}$, where the different modes are the different paths of the photon. Bob can use a phase shift of $e^{i\pi/2}$ on the path represented by the first mode (i.e. $|10\rangle^F \rightarrow i|10\rangle^F$), and then place a symmetric beam splitter to reach $|10\rangle^F$ or $|01\rangle^F$ respectively at the outputs of the beam splitter (up to a general phase). These last two states can then be distinguished by a simple (complete) measurement as described above.
CHAPTER 3. ANALYSIS OF INTERFEROMETRIC QKD SCHEMES

3.3 Description of Interferometric-based QKD Schemes

In this section, we introduce several variants of “Prepare & Measure” QKD schemes implemented using interferometers.

3.3.1 Variant A: The BB84 protocol with x and y bases

In this variant (Figure 3.5), Alice and Bob use bases $x$ and $y$ for transmitting qubits. Alice encodes her state as a single photon pulse superpositioned in modes $t_0$ and $t_1'$. Let $|0\rangle \equiv |0\rangle_{t_0 t_1'}$ and $|1\rangle \equiv |01\rangle_{t_0 t_1'}$. Alice, using the $x$ and $y$ bases, sends one of the states

$$|0_x\rangle_A \equiv \left( |0\rangle_{t_0 t_1'} + |01\rangle_{t_0 t_1'} \right)/\sqrt{2}$$

$$|0_y\rangle_A \equiv \left( |0\rangle_{t_0 t_1'} + i|01\rangle_{t_0 t_1'} \right)/\sqrt{2} \quad (3.8)$$

$$|1_x\rangle_A \equiv \left( |0\rangle_{t_0 t_1'} - |01\rangle_{t_0 t_1'} \right)/\sqrt{2}$$

$$|1_y\rangle_A \equiv \left( |0\rangle_{t_0 t_1'} - i|01\rangle_{t_0 t_1'} \right)/\sqrt{2} \quad (3.9)$$

which evolve in the interferometer$^2$ as

$$|0_x\rangle_A \xrightarrow{\phi=0} (|s_0\rangle - |s_2\rangle + i|d_0\rangle + 2i|d_1\rangle + i|d_2\rangle) / \sqrt{8}$$

$$|1_x\rangle_A \xrightarrow{\phi=\pi/2} (|s_0\rangle - 2|s_1\rangle + |s_2\rangle + i|d_0\rangle - i|d_2\rangle) / \sqrt{8} \quad (3.10)$$

$$|0_y\rangle_A \xrightarrow{\phi=\pi/2} (|s_0\rangle - |s_2\rangle + i|d_0\rangle - 2|d_1\rangle - i|d_2\rangle) / \sqrt{8}$$

$$|1_y\rangle_A \xrightarrow{\phi=\pi/2} (|s_0\rangle - 2i|s_1\rangle - |s_2\rangle + i|d_0\rangle + i|d_2\rangle) / \sqrt{8}$$

Bob opens his detectors at time $t_1$ in both arms. A click in the “down” direction ($|d_1\rangle$, for the single photon scheme) means that the bit-value 0 was measured, while a click in the “straight” direction ($|s_1\rangle$) means 1. The other modes are commonly considered as a loss (they are not measured) since they do not reveal the value of the original qubit. This scheme implies an intrinsic loss rate of 50%.

3.3.2 Variant B: Protocols that uses the $z$-basis

However, for various possible reasons, one might want to work with the $z$ basis; for instance, an equipment-related reason such as avoiding the need for a controlled phase shift; or in order to perform the 6-state QKD protocol [22], in which Alice sends a qubit using the $x$, $y$ and $z$ bases at random; or in order to perform “QKD with classical Bob” ([19], Chapter 5) in which Bob uses only the $z$-basis, and either performs measurements in that basis or returns the qubits (unchanged) to Alice (who can measure in either one of the bases).

We now describe a setup that Bob can employ in order to measure the $z$ basis, i.e. the states $|0_z\rangle = |0\rangle_{t_0 t_1'}$ and $|1_z\rangle = |01\rangle_{t_0 t_1'}$. This can be done by removing the beam splitters and measuring the pulses after the appropriate delay $T_{short}$, so that the measurement of $|0_z\rangle$ ($|1_z\rangle$) is done by opening a detector at time $t_0$ ($t_1$); see Figure 3.6.

$^2$The phase shift is set by Bob according to the appropriate basis.
3.3. DESCRIPTION OF INTERFEROMETRIC-BASED QKD SCHEMES

Figure 3.5: Bob’s Laboratory setup for the $x$ and $y$ bases. (a) Alice’s qubit; (b) ancilla modes each in a vacuum state; (c), (d) beam-splitters; (e) phase shifter $P_{\phi}$ is set to $\phi = 0$ for the $x$ basis or to $\phi = \pi/2$ for the $y$ basis; (f) Bob’s detectors measure time $t_1$.

Figure 3.6: Bob’s Laboratory setup for the $z$ basis.
CHAPTER 3. ANALYSIS OF INTERFEROMETRIC QKD SCHEMES

Bob’s transformation $U_{Bz}$ is then the identity operator and can be defined as $|0_z\rangle \rightarrow |s_0\rangle$ and $|1_z\rangle \rightarrow |s_1\rangle$, where the other modes are not relevant for this measurement. Instead, we use here the mode $|d_1\rangle \equiv |000010\rangle_F$ to replace more intuitive $|s_0\rangle \equiv |100000\rangle_F$, namely,

$$|0_z\rangle \xrightarrow{U_{Bz}} |d_1\rangle \quad ; \quad |1_z\rangle \xrightarrow{U_{Bz}} |s_1\rangle \quad (3.11)$$

in order to be consistent with the modes representing the bit values 0 and 1 when the $x$ or $y$ setups are used. This can be justified by placing and removing a mirror (replacing BS1), such that the pulse entering the lab at time $t'_0$ is reflected to $d_1$, while the pulse at $t'_1$ continues right to $s_1$. As opposed to the setups for measuring the $x$ and $y$ bases, this configuration has no intrinsic loss rate.

We denote the BB84 protocol that uses $x$ and $z$ bases by alternating the setups (adding and removing beam-splitters and mirrors as needed), as $xz$-BB84 (Variant B1). In the same manner, a six-state protocol using the above setup will be denoted as $xyz$-six-state scheme (Variant B2).

This is the place to mention that the above scheme is unbalanced since the $x$ basis has an intrinsic loss rate of $50\%$, while the $z$ basis has no intrinsic loss rate. In order to compensate for this bias and reach a balanced protocol, Alice should change the probability of sending a qubit in the $z$ basis to $1/3$ (and $2/3$ for the $x$ basis). By doing this, there is an equal probability for a sifted bit to be originated by the $x$ (or $z$) basis. This applies to the $y$ basis as well. For instance, in order to balance the $xyz$-six-state scheme, Alice should send $2/5$ of the qubits in the $x$-basis, $2/5$ in the $y$ basis and $1/5$ in the $z$ basis.

3.3.3 Variant C: “Unified” implementation for the $z$-basis

Our last variant deals with a BB84 protocol that uses the $z$ and $x$ bases, over the same interferometric setup. Bob uses the setup $U_{Bz}$ for measuring both the bases in the following manner: in order to perform a measurement in the $x$ basis, he opens his two detectors at time-bin $t_1$, so that he measures the states $|s_1\rangle$ and $|d_1\rangle$; in order to perform a measurement in the $z$ basis, he measures $|s_0\rangle, |d_0\rangle$ for the bit-value ‘0’ and $|s_2\rangle, |d_2\rangle$ for ‘1’ (see Equations (3.6) and (3.10)). We denote this scheme as $xz$-BB84-unified (Variant C1). It is interesting to mention that in this variant Bob measures more than 2 modes, i.e. his measured space is not a qubit but a larger space. This requires using the tools of Chapter 2 in order to correctly analyze the security of this scheme.

It may well be that, Bob wants to open his detector only to a single detection slot. This may be done in order to achieve a higher bit-rate, or may be forced due to technological limitations (or due to Bob’s financial limitations) that restrict opening the detectors for more than a single detection window per pulse. This issue is usually relevant in telecommunication wave light (IR spectrum) technology.
A scheme that deals with this limitation bounds Bob to measure only a single time-bin in each detector. For instance, let Bob measure the $x$ basis as before (at time $t_1$), and measure the $z$ basis opening the $d$-arm detector at time $t_0$ (to measure $|0_z\rangle$) and the $s$ arm detector at time $t_2$ (to measure $|1_z\rangle$). We denote this last case as Variant C2.

### 3.4 Robustness of Protocols: Definition and Discussion

#### 3.4.1 The robustness definitions

The criterion of robustness is used in latest security analyses of QKD protocols. It is used in SARG [72] dealing with the PNS attack [21] and in the BBM protocol [8] using entangled particles, dealing with any attack. In this chapter we use the definition of [19] to prove (or to disprove) robustness of several QKD implementations. A protocol is said to be completely robust if nonzero information acquired by Eve implies nonzero probability that the legitimate participants find errors in the bits tested by the protocol. A protocol is said to be completely nonrobust if Eve can acquire the entire information transmitted in the protocol, without inducing any errors on the bits tested by the protocol. See full definition of robustness and discussion in Section 5.2.

#### 3.4.2 The relations between errors and losses

In all nowadays QKD schemes the obtained security is related to the measured error-rate. Security proofs [76, 57, 10] determine the maximal error rate (attributed to Eve’s attack) that keeps Eve’s knowledge negligible. Yet, there is a distinction between errors and losses. If Bob considers each loss as a random bit obtained from Alice, he adds an error with probability half, and thus increases the error-rate. If this was the case, many of the practical QKD scheme could not be proven secure, due to the high loss rate (above 99%, using WCP, and lossy channel).

Allowing losses (without defining allowed loss-rate) might allow Eve to perform useful attacks that result with losses yet with no errors, and keep avoided from being detected [21, 56]. In such cases, one might be able to define a loss-rate threshold such that for higher loss-rate the protocol is completely nonrobust, while for lower loss-rate the protocol is partly robust, and might lead to the generation of a secure final key. In addition to natural losses, Bob might mistakenly interpret some measurements as a loss. For instance, Bob might ignore pulses with multiple photons since he assumes Alice is ideal and falsely assumes that a measurement of multiple photons must be due to detectors fault (black count) rather than the action of an adversary. This misinterpretation might as well cause a severe security problems (as discussed in Section 2.6.3 which is based on [38]).
3.4.3 Conditions for zero-error attacks

In order to prove robustness, we formulate the conditions on Eve’s attacks that imply a zero error rate. Once these conditions are defined, it is possible to specify the set of all Eve’s zero-error attacks, and examine the maximal information obtained by using those attacks.

Let Alice’s basis elements be denoted \(|i\rangle_A\) with \(i \in \{0, 1\}\). Eve adds an ancilla in the state \(|\tilde{E}\rangle\) (in a dimension of her desire) and attacks the system by using a unitary transformation \(U_E\):

\[
|0\rangle_E|i\rangle_A \xrightarrow{U_E} \sum_k \epsilon_{i,k} |E_{i,k}\rangle_E |k\rangle_P
\]

(3.12)

where the subsystem \(P\) is sent over to Bob and the subsystem \(E\) remains in Eve’s hands to be measured afterwards. We index the basis states of subsystem \(P\) by \(|k\rangle_P\). Obviously, the case in which \(P = A\) is now merely a special case, while in the more general case Eve might send Bob a system with different dimensions than \(\mathcal{H}^A\), having a different number of modes and photons. The subsystem \(E\) can similarly be different from the subsystem \(\tilde{E}\) she initially added, and both can be of any dimension as long as the dimension of the entire system is kept, \(|\mathcal{H}^E|\mathcal{H}^A| = |\mathcal{H}^E|\mathcal{H}^P|\). Let a general qubit state sent by Alice be

\[
|\psi\rangle_A = \sum_i \alpha_i |i\rangle
\]

(3.13)

with \(\sum_i |\alpha_i|^2 = 1\). Using these notations we write Eve’s attack (on a general qubit state sent by Alice),

\[
U_E(\sum_i \alpha_i |0\rangle_E |i\rangle_A) = \sum_{i,k} \alpha_i \epsilon_{i,k} |E_{i,k}\rangle_E |k\rangle_P.
\]

(3.14)

In order to perform a most general measurement, Bob manipulates the state sent by Alice. For instance, Bob might add an ancillary system \(B'\), whose space is denoted by \(\mathcal{H}^{B'}\), and perform his measurement on the joint space \(\mathcal{H}^A \otimes \mathcal{H}^{B'}\). We model Bob’s equipment as adding the ancilla\(^3\) \(|0\rangle_{B'}\), performing a unitary transformation \(U_B\) on \(|\psi\rangle_A |0\rangle_{B'}\), and then measuring his system in the computation basis\(^4\). Note that \(U_B\) must be defined differently depending on Bob’s measurement basis, since Bob may have different equipment for each basis he measures. For the \(z\) basis and \(x\) basis setups we get:

\[
|i\rangle_A |0\rangle_{B'} \xrightarrow{U_B} \sum_j \beta_{i,j} |j\rangle_{AB'} \quad ; \quad |i\rangle_A |0\rangle_{B'} \xrightarrow{U_B} \sum_j \beta_{i,j}^* |j\rangle_{AB'}.
\]

(3.15)

\(^3\)Without loss of generality, we assume that Bob uses the same ancilla \(|0\rangle_{B'}\) for all of his setups. This can always be justified, e.g., by using a sufficiently large ancilla, such that the different setups potentially use different subsystems of that ancilla.

\(^4\)Alternatively, one can describe Bob’s added ancilla, his unitary transformation, and his measurement using the so-called POVM (generalized measurements) notations [65, 63].
The relevant $\beta$'s are determined by the specific setup used by Bob and $|j\rangle_B$ are Bob's basis states in the computation basis, the set of states that span the space $\mathcal{H}^A \otimes \mathcal{H}^{B'}$. It should be noted that Bob's transformation $U_B$ is defined by his equipment on the space entering his lab. The space $\mathcal{H}^A$ used by Alice, and the space $\mathcal{H}^P$ used by Eve are merely subspaces of that space, so $U_B$ is well-defined for these spaces. While a fully powerful Eve knows Alice's and Bob's protocol spaces, and their equipment limitations, they might not be aware to the fact that $A$ is replaced by $P$. The above formulas (3.15) are immediately generalized to this case, simply by replacing the subscript $A$ by the subscript $P$, and by enlarging the computational basis in Bob’s hands so that it spans the space $\mathcal{H}^B = \mathcal{H}^P \otimes \mathcal{H}^{B'}$. For a given $\alpha_i$’s chosen by Alice, a given attack, and a given choice of transformation $U_B$, the final state $|\Psi_{BE}\rangle$ (held by Bob and Eve), can be written as

$$
|\Psi_{BE}\rangle = \sum_{i,k} \alpha_i \epsilon_{i,k} |E_{i,k}\rangle_B U_B(|k\rangle_P |0\rangle_B')
$$

$$
= \sum_{i,k,j} \alpha_i \epsilon_{i,k} \beta_{k,j} |E_{i,k}\rangle_E |j\rangle_B.
$$

(3.16)

There is a great deal of importance regarding the way Bob interprets his measurement outcome. The basis states $|j\rangle$ can be classified into sets according to Bob’s interpretation. Some of them are interpreted as “Alice sent the bit 0”, others are interpreted as “Alice sent the bit 1”. Let us denote these two sets by $J_0$ and $J_1$ respectively. In case Alice sent the bit 0 (say, encoded using the $z$ basis) while Bob measured an outcome $j$ which corresponds to a state in the set $J_1$ (or vice versa), there is an error, and this error will contribute to the error-rate if this bit is tested. Formally, if Alice encoded a bit $b$ in some way, while Bob’s outcome $j$ corresponds to a state (say, $|j\rangle$) which is interpreted as the opposite value $\bar{b}$, we say that $|j\rangle \in J_{err}$, even if the bit is not tested.

Yet, in the real world, there may be some outcomes that are not interpreted as a valid measurement. Those outcomes can be divided into two groups: (a) outcomes that interpreted by Bob as a loss — a failed transmission that is not considered as an error (e.g. a vacuum state when Alice is ideal), because they naturally occur even when no eavesdropper interferes. These outcomes are denote as the set $J_{loss}$, (b) invalid-erroneous outcomes, $J_{invalid}$, that can never occur if the quantum system sent by Alice reaches Bob intact. It is Bob’s choice of interpretation that determines whether a specific outcome is considered a loss or an invalid result. Once such an outcome increases the error rate it is in $J_{invalid}$ and otherwise it is in $J_{loss}$.

For the BB84 protocol, in order to examine the robustness we must find the attacks that induce no errors and no invalid outcomes. In mathematical terms, attacks in which for any $|j'\rangle \in J_{err}$ and for any $|j'\rangle \in J_{invalid}$, the overlap of the state $|\Psi_{BE}\rangle$ with any state

---

5Notice that this space is nothing more than the space $M$ discussed in Chapter 2.
\( |j'\rangle \) is zero. Using Equation (3.16) we see that Eve’s attack causes no errors if and only if 
\[ \langle j' | \sum_{i,k,j} \alpha_i \epsilon_{i,k} \beta_{k,j} | E_{i,k} \rangle_E | j \rangle_B \] = 0, for any \( j' \in J_{\text{err}} \) and for any \( j' \in J_{\text{invalid}} \).

**Corollary 3.1** Eve’s attack causes no errors if and only if, for every state \( |\psi\rangle_A \) (described in (3.13)) that is sent by Alice,
\[ \sum_{i,k} \alpha_i \epsilon_{i,k} \beta_{k,j} | E_{i,k} \rangle_E = 0, \] (3.17)
for any \( j \in J_{\text{err}} \) and for any \( j \in J_{\text{invalid}} \) (corresponding to the specific state \( |\psi\rangle_A \)).

Given a scheme, the error rate is determined exclusively by the attack \( \mathcal{U}_E \), performed by Eve.

**Definition 3.2** Let \( \mathcal{U}_{\text{zero}} \) be the set of attacks \( \mathcal{U}_E \), that cause no errors (in all the possible setups of the protocol).

Robustness for a given protocol’s implementation is achieved if \( \mathcal{U}_{\text{zero}} \) consist of only those attacks that give Eve no information. Note that the intersection of the zero-error attacks for the \( x \)-setup and for the \( z \)-setup determines \( \mathcal{U}_{\text{zero}} \) (and the robustness) of the BB84 protocol with \( x \) and \( z \).

### 3.5 Robustness Proof of Interferometric BB84

In this section we use the above method to demonstrate a robustness proof of a phase-encoded QKD implementation (Variant A and Variant B) against a degenerate Eve who is limited in the number of photons sent at each pulse.

**3.5.1 Robustness proof of Variant A against a limited adversary**

Following Definition 5.1 we prove the \( xy \)-BB84 implementation presented in Section 3.3.1 to be completely robust against a single-photon limited Eve. We begin by defining the set of zero errors attack \( \mathcal{U}_{\text{zero}} \) for this scheme. We then prove that any eavesdropping attempt that gives Eve some information must cause an error-probability larger than zero.

Once the protocol is limited to using a single-photon pulses, we need to focus only on the sub-space containing the vacuum state and the single-photon states, \( |V\rangle \), \( |s_0\rangle \), \( |s_1\rangle \), \( |s_2\rangle \), \( |d_0\rangle \), \( |d_1\rangle \) and \( |d_2\rangle \) as defined above. The analysis must consider the space Bob actually measures, \( \mathcal{H}_B \), and the states (sent by Alice or Eve) that can affect his measurement. Any state orthogonal to \( \mathcal{H}_B \) does not affect Bob’s measurement: it yields a loss with certainty, and does not influence our analysis.

As mentioned above, Bob opens his detectors only at time \( t_1 \), thus measuring only \( |V\rangle \), \( |s_1\rangle \) and \( |d_1\rangle \). Eve could potentially send states that result in Fock terms such as
that Equation (3.17) yields the condition we obtain of 3.15 to rewrite Equation (3.6) (while ignoring the vacuum state). Using a matrix form, 3.5. ROBUSTNESS PROOF OF INTERFEROMETRIC BB84

Moreover, when threshold detectors are used, which is the common situation in experiment and practice, Bob cannot distinguish the event of detecting multiple photons in the same mode. For example, the states $|010000\rangle^P$ and $|020000\rangle^P$ both trigger the $s$-detector at time $t_1$. This is also true for states such as $|121000\rangle^P$ and $|262102\rangle^P$, since Bob detects only at time $t_1$. Bob might use a counter instead. A realistic counter could (in a very ideal scenario) let Bob perfectly distinguish a single photon from the vacuum state and also from multiple photons. In such a case, a multiple-photon state should be considered as an error, or else, the analysis of Eve’s attack will become extremely cumbersome.

The measurement performed by Bob is described (for both the $x$ and the $y$ bases) by the set $J_0 = \{|d_1\}\}; J_1 = \{|s_1\}\}; J_{\text{loss}} = I - J_0 - J_1 = \{|V\}\}; and $J_{\text{invalid}} = \{\}$. where the set $I = \{|V\}, |s_1\}, |d_1\}\}$ represents the computation basis of the space measured by Bob, $\mathcal{H}^B$, and the minus stands for set difference. Eve might send the photon at any desired time-bin. However, it will only affect Bob if sent at time-bins $t'_0$ or $t'_1$. A single-photon pulse that is sent at a different time-bin is orthogonal to $\mathcal{H}^B$ and thus has no effect on the robustness analysis. Eve has no advantage in attacking a larger space than the one used by Alice\footnote{In other words the QSoP of this scheme is spanned by $\{|10\rangle^y_{t'_1}, |01\rangle^y_{t'_1}\}$.}, thus $\mathcal{H}^P = \mathcal{H}^A$.

We use Corollary 3.1 to define Eve’s attacks that cause no errors at all. For this specific protocol, $U_{\text{zero}}$ consists of the attacks that fulfill (3.17) in four cases, matching the four BB84 states sent by Alice. Bob’s setup (i.e. the constants $\beta_{k,j}$) is determined by the basis he measures; for the $x$ basis Bob sets $\phi = 0$, and we shall use $\beta^{MU}_k$ and for the $y$ basis Bob sets $\phi = \pi/2$ and we use $\beta^{MY}_k$. If we index the single-photon basis states (of $\mathcal{H}^P$) entering Bob’s lab $\{|10\rangle^y_P, |01\rangle^y_P\}$ as $|k\rangle$ with $k = \{0,1\}$ respectively, then we can use the notations of 3.15 to rewrite Equation (3.6) (while ignoring the vacuum state). Using a matrix form, we obtain

\[
\begin{align*}
\beta^{MU}_{k=0,1, j=\{s_0,s_1,s_2,d_0,d_1,d_2\}} &= \frac{1}{2} \begin{pmatrix} 1 & -1 & 0 & i & i & 0 \\ 0 & 1 & -1 & 0 & i & i \end{pmatrix} \quad (3.18) \\
\beta^{MY}_{k=0,1, j=\{s_0,s_1,s_2,d_0,d_1,d_2\}} &= \frac{1}{2} \begin{pmatrix} 1 & -i & 0 & i & -1 & 0 \\ 0 & 1 & -i & 0 & i & -1 \end{pmatrix} \quad (3.19)
\end{align*}
\]

Consider the case where Alice sends $|0_x\rangle$, i.e. $\alpha_0 = \alpha_1 = \frac{1}{\sqrt{2}}$. In this case $J_{\text{err}} = \{|s_1\}\}$, so that Equation (3.17) yields the condition

\[
-\frac{1}{2\sqrt{2}}(\epsilon_{0,0}|E_{0,0}\rangle_E + \epsilon_{1,0}|E_{1,0}\rangle_E) + \frac{1}{2\sqrt{2}}(\epsilon_{0,1}|E_{0,1}\rangle_E + \epsilon_{1,1}|E_{1,1}\rangle_E) = 0. \quad (3.20)
\]
In the same way, we achieve the following conditions for the other three BB84 states sent by Alice $|1_x\rangle$, $|0_y\rangle$ and $|1_y\rangle$, adjusting the constants accordingly (e.g. when Alice sends $|1_y\rangle$ we use $\alpha_0 = \frac{1}{\sqrt{2}}$, $\alpha_1 = -\frac{1}{\sqrt{2}}$, $J_{err} = J_{0_y} = \{|d_1\}\}$ and $\beta_{k,i,j}^{U_E}$):

$$\frac{i}{2\sqrt{2}}(\epsilon_{0,0} |E_{0,0}\rangle_E - \epsilon_{1,0} |E_{1,0}\rangle_E) + \frac{i}{2\sqrt{2}}(\epsilon_{0,1} |E_{0,1}\rangle_E - \epsilon_{1,1} |E_{1,1}\rangle_E) = 0 \quad (3.21)$$

$$-\frac{i}{2\sqrt{2}}(\epsilon_{0,0} |E_{0,0}\rangle_E + i\epsilon_{1,0} |E_{1,0}\rangle_E) + \frac{1}{2\sqrt{2}}(\epsilon_{0,1} |E_{0,1}\rangle_E + i\epsilon_{1,1} |E_{1,1}\rangle_E) = 0 \quad (3.22)$$

$$-\frac{1}{2\sqrt{2}}(\epsilon_{0,0} |E_{0,0}\rangle_E - i\epsilon_{1,0} |E_{1,0}\rangle_E) + \frac{i}{2\sqrt{2}}(\epsilon_{0,1} |E_{0,1}\rangle_E - i\epsilon_{1,1} |E_{1,1}\rangle_E) = 0 \quad (3.23)$$

having the solution

$$\epsilon_{0,0} |E_{0,0}\rangle_E = \epsilon_{1,1} |E_{1,1}\rangle_E \quad \text{and} \quad \epsilon_{1,0} |E_{1,0}\rangle_E = \epsilon_{0,1} |E_{0,1}\rangle_E = 0 \quad (3.24)$$

This means that $U_{\text{zero}}$ consists of attacks of the form

$$|0\rangle_E |0\rangle_z \xrightarrow{U_E} p|\phi\rangle_E |0\rangle_P + \sqrt{(1-p)^2}|\psi_0\rangle_E |V\rangle_P \quad (3.25)$$

$$|0\rangle_E |1\rangle_z \xrightarrow{U_E} p|\phi\rangle_E |1\rangle_P + \sqrt{(1-p)^2}|\psi_1\rangle_E |V\rangle_P \quad (3.26)$$

which is the blocking attack for $p < 1$, and the identity attack for $p = 1$. We can see that Eve gains information about Alice’s state only when the vacuum state is transmitted to Bob (thus blocking the photon from reaching Bob and causing a loss). In this case Eve gains no information about the key and the protocol is completely robust according to Definition 5.1.

### 3.5.2 Robustness proof of Variant B against a limited adversary

It is rather straightforward to extend the robustness proof of the $xz$-BB84 scheme to Variant B. We start with Variant B1: the sets measured by Bob when using the $z$ basis are $J_0 = \{|d_1\}\}$, $J_1 = \{|s_1\}\}$, $J_{\text{loss}} = I - J_0 - J_1$ and $J_{\text{invalid}} = \{|\rangle\}$ as above. Since the setup for the $z$ basis is different, we need to define $\beta_{k,j}$ using (3.11) for this case:

$$\beta_{k=\{0,1\},j=\{s_0,s_1,s_2,d_0,d_1,d_2\}}^{U_E} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}. \quad (3.27)$$

It follows immediately from (3.17) that any attack $U_E$ that leads to a zero error rate must satisfy

$$\epsilon_{0,1} = \epsilon_{1,0} = 0. \quad (3.28)$$

The set $U_{\text{zero}}$ consists of attacks fulfilling these requirements as well as requirements (3.20) and (3.21) of the $x$-basis. As before, $U_{\text{zero}}$ consists of only the blocking attack (Equations (3.25) and (3.26)). Variant B1 is robust, under the limitations of single photon pulses.
3.5. ROBUSTNESS PROOF OF INTERFEROMETRIC BB84

It is easy to check that exactly the same result holds when using the \( y \)-basis instead of the \( x \)-basis, i.e., using requirements (3.22) and (3.23). Therefore a BB84 scheme in which the \( y \) basis is used instead of the \( x \) basis (i.e. \( yz \)-BB84) is also robust.

Combining the above result with the result of the previous subsection immediately yields that the \( xyz \)-six-state scheme (Variant B2) is robust as well, under the same assumptions.

3.5.3 Robustness of Variant A against a more realistic Eve

In the following section we show that the \( xy \)-BB84 scheme is robust against a more powerful Eve that is allowed to use 2-photon pulses. Although we believe that the protocol is robust against the most powerful Eve (i.e. Eve that is not limited in the number of photons used), our proof is not scalable to the general case. In order to show that the protocol is robust against a 2-photon limited Eve we need to define the interferometer transformation, IT, for 2 photons. This is done (for an arbitrary number of photons) in Appendix A. We start with several Propositions.

**Proposition 3.3** States with \( n_1 \) photons, can not have a destructive interference with states occupied by \( n_2 \neq n_1 \) photons.

**Proof** Since \( \langle m_1, m_2, \ldots, m_k | m'_1, m'_2, \ldots, m'_k \rangle = \prod_{i=1..k} \delta_{m_i m'_i} \), we see that any different number of photons (in any mode) makes a zero overlap therefore such states can not cancel each other. When we apply any transformation on a state with \( n_1 \) photons, the transformed state is a superposition of elements, each with \( n_1 \) photons, that can not cancel any element of the \( n_2 \)-photon transformed states. In other words, examine the interference of two states \( \psi_{n_1} \) and \( \psi_{n_2} \) with \( n_1 \) and \( n_2 \) photons respectively; if we let \( IT|\psi_{n_1}\rangle = \sum_i \alpha_i |i_{n_1}\rangle \) and \( IT|\psi_{n_2}\rangle = \sum_j \beta_j |j_{n_2}\rangle \) then for every \( i, j \) we get \( \langle i_{n_1}|j_{n_2}\rangle = 0 \). □

As a corollary to the above, if a superposition of two (basis) states, \( |\psi_1\rangle \) and \( |\psi_2\rangle \), having a different number of photons, enters an interferometer IT as defined in (A.5), we can analyze each one of the elements separately. Causing no errors in this case is equivalent to a zero overlap between any state in \( J_{\text{err}} \cup J_{\text{invalid}} \) and IT\( |\psi_1\rangle \) or IT\( |\psi_2\rangle \).
Proposition 3.4 If a pulse with exactly 2 photons, enters an interferometer its transformation is:

\[
U_{IT}(|2\rangle^F) = \frac{1}{4} \left[ (|200000\rangle^F + \sqrt{2}i|100100\rangle^F - |000200\rangle^F \\
+ e^{i\phi}(-\sqrt{2}|110000\rangle^F + \sqrt{2}i|010100\rangle^F - \sqrt{2}|000110\rangle^F) \\
+ e^{i2\phi}(|020000\rangle^F - \sqrt{2}i|010010\rangle^F - |000020\rangle^F) \right]
\]

(3.29)

\[
U_{IT}(|11\rangle^F |t'_0 |t'_1) = \frac{1}{4} \left[ (|110000\rangle^F + i|100010\rangle^F + i|010100\rangle^F - |000110\rangle^F \\
+ e^{i\phi}(-\sqrt{2}|020000\rangle^F - \sqrt{2}|000020\rangle^F - |101000\rangle^F) \\
+ i|100010\rangle^F - i|001100\rangle^F - |000101\rangle^F \\
+ e^{i2\phi}(|011000\rangle^F - i|010010\rangle^F - |000011\rangle^F) \right]
\]

(3.30)

over the basis \(|n_{s0}, n_{s1}, n_{s2}, n_{d0}, n_{d1}, n_{d2}\rangle^F\).

Proof This follows immediately from Proposition A.1.

Theorem 3.5 Variant A is robust against an attack that is limited to having up to 2-photon in each transmission

Proof By Section 3.5.1 we know that the \(xy\)-BB84 scheme is robust if Eve is limited to states in which the number of photons is \(n \leq 1\). Due to Proposition 3.3, we need to prove only the case where Eve uses states with exactly \(n = 2\) photons. This will be proven by direct calculation.

We divide the proof to three parts, according to the number of photons occupying modes \(t'_0\) and \(t'_1\) in the state that is sent to Bob:

1. There are 0 photons in modes \(t'_0\) and \(t'_1\): For instance, Eve sends the state \(|11\rangle^F |t'_0 t'_1\rangle^F\) or \(|20\rangle^F |t'_0 t'_5\rangle^F\). These kind of states always cause a loss since they never reach Bob’s detectors at time \(t_1\). Eve can send a superposition of any such states, and Bob can not distinguish them from the case that the state \(|V\rangle\) was sent. These state are in \(J_{loss}\) and do not affect the error rate nor the robust proof.

2. There is a single photon in modes \(t'_0\) and \(t'_1\): For instance, Eve sends \(|11\rangle^F |t'_0 t'_3\rangle^F\). This case is not the same as sending a single photon, but since the second photon never interfere at time \(t_1\) in Bob’s lab, we can consider this case as giving Eve the second photon, instead of sending it to Bob. Thus, we can use the robust proof for a single photon of Section 3.5.1 to deal with this case as well.

3. Both photons are in modes \(t'_0\) and \(t'_1\), or a superposition that has (at least) one such element.
3.6. ROBUSTNESS ANALYSIS OF VARIANT C

Assume Eve sends Bob a 2-photon state of the form $|\psi_{\alpha,\beta,\gamma}\rangle = \alpha|20\rangle_{t_0't_1'} + \beta|11\rangle_{t_0't_1'} + \gamma|02\rangle_{t_0't_1'}$. We show that if Eve causes no errors, Corollary 3.1 restricts the state sent by Eve, to be a multiple-photon version of the state expected by Bob. E.g. if Bob expects $|0_x\rangle$, the only 2-photon state that causes no errors is $|0_x\rangle^{\otimes 2} = (\langle 20 |_{t_0't_1'} + \sqrt{2}\langle 11 |_{t_0't_1'} + |02\rangle_{t_0't_1'})/2$ (or a superposition of this state, and states that always cause a loss such as $|11\rangle_{t_0't_1'}$, as explained in case (1) above).

We demonstrate the above only for the case of $|0_x\rangle$; other cases can be achieved in a similar way. We set the interferometer for the $x$ basis, i.e. $\phi = 0$. By Proposition A.1 we see that $\{|20\rangle_{t_0't_1'}, |11\rangle_{t_0't_1'}, |02\rangle_{t_0't_1'}\}$ are the only 2-photon basis states that have a non-zero overlap with $|0000\rangle^F$. Any other 2-photon basis state has no effect on this element. A zero overlap of $|$IT$\rangle|\psi_{\alpha,\beta,\gamma}\rangle$ with this erroneous state (when Bob expects $|0_x\rangle$, and $\phi = 0$) implies $\alpha - \sqrt{2}\beta + \gamma = 0$.

Notice that $|010010\rangle^F \in J_{\text{invalid}}$, since it causes a click in both detectors, which imply an inconclusive result (that must be interpreted as an error, since Alice’s states are assumed to contain only a single photon). Since for $\phi = 0$ we get $\langle 010010 |_{\text{IT}}^F |20\rangle_{t_0't_1'} = -\langle 010010 |_{\text{IT}}^F |02\rangle_{t_0't_1'}$ and $\langle 010010 |_{\text{IT}}^F |11\rangle_{t_0't_1'} = 0$, canceling this invalid element in the interference of $|\psi_{\alpha,\beta,\gamma}\rangle$ and satisfying Equation (3.17), requires $\alpha = \gamma$. Again, no other 2-photon states interfere in a way that effects the element $|010010\rangle^F$, therefore we must have $\beta = \sqrt{2}\alpha = \sqrt{2}\gamma$. One can easily verify that $\frac{1}{2}|\psi_{\alpha=1,\beta=\sqrt{2}\gamma=1}\rangle = |0_x\rangle^{\otimes 2}$ causes no error if Bob expects $|0_x\rangle$, i.e. Bob’s detector of $s_1$ never clicks in that case.

We end the proof by saying that Eve who is limited to use exactly 2-photons can avoid being detected by Bob only if she can generate (and send Bob) a perfect 2- photon copy of the state sent by Alice. Due to the no-cloning theorem, this is not possible, and Eve essentially introduces errors in the process. It follows that this scheme is robust against an eavesdropper that is limited to use up to 2-photons.

3.6 Robustness Analysis of Variant C

In this variant, Bob measures different time-bins than $t_1$, explicitly, $t_0$ and $t_2$. Eve can affect Bob’s measurement of those modes by sending pulses at times $t_1'$ and $t_2'$. Using the above notations, $\mathcal{H}^P$ (which is the QSoP of this scheme), becomes a 4-mode space where the pulse sent over to Bob is a superposition of time-bins $t_1'$ to $t_2'$. A state in $\mathcal{H}^P$ is of the form $|n_{t_1'}n_{t_0'}n_{t_1}n_{t_2}'\rangle^F$.

3.6.1 Robustness proof for Variant C1 against a limited adversary

Again, we limit a single-photon pulses. The set $I$ is redefined for this limited variant to be $\{|V\rangle, |s_0\rangle, |s_1\rangle, |s_2\rangle, |d_0\rangle, |d_1\rangle, |d_2\rangle\}$. Let us describe the requirements for the robustness of the $xz$-BB84-unified scheme. When Bob measures the $x$ basis, he uses the same setup as
the $xy$-BB84 scheme. Therefore, he is constrained by requirements (3.20)-(3.21). When Bob measures the $z$ basis he uses the following set: $J_0 = \{|d_0\}, |s_0\} \}; J_1 = \{|d_2\}, |s_2\} \}; J_{invalid} = \{\}$, due to the single-photon assumption; and $J_{loss} = I - J_0 - J_1$. We assume that Eve (as well as any natural noise) is constrained to generating superpositions of single photon pulses, and (as said before) only those pulses sent to Bob at times $t'_0$ to $t'_2$ affect Bob’s measurements. We index the single-photon basis states \{\ket{1000}_P, \ket{0100}_P, \ket{0010}_P, \ket{0001}_P\} of $H_P$ as $|k\>$ with $k = -1, 0, 1, 2$ respectively. Bob’s transformation must be extended to those time-bins as well\(^7\), so that

$$
\beta^H_{k = \{-1,0,1,2\}, j = \{s_0,s_1,s_2,d_0,d_1,d_2\}} = \frac{1}{2} \begin{pmatrix}
-1 & 0 & 0 & i & 0 & 0 \\
1 & -1 & 0 & i & 0 & 0 \\
0 & 1 & -1 & 0 & i & 0 \\
0 & 0 & 1 & 0 & 0 & i
\end{pmatrix}.
$$

(3.31)

Following Corollary 3.1, an attack $U_E$ that causes zero error rate, must satisfy

$$
i\epsilon_{0,1}|E_{0,1}\> + i\epsilon_{0,2}|E_{0,2}\> = 0 \quad -\epsilon_{0,1}|E_{0,1}\> + \epsilon_{0,2}|E_{0,2}\> = 0
$$

(3.32)

matching the case which Alice sends $|0_z\>$, i.e. $\alpha_0 = 1$, $\alpha_1 = 0$, and $J_{err} = \{|d_2\}, |s_2\}$, and

$$
i\epsilon_{1,-1}|E_{1,-1}\> + i\epsilon_{1,0}|E_{1,0}\> = 0 \quad -\epsilon_{1,-1}|E_{1,-1}\> + \epsilon_{1,0}|E_{1,0}\> = 0
$$

(3.33)

matching the case which Alice sends $|1_z\>$, i.e. $\alpha_0 = 0$, $\alpha_1 = 1$, and $J_{err} = \{|d_0\}, |s_0\}$. Therefore, the requirements for Eve’s attack not to cause any error, if Alice and Bob use the $z$-basis, are $\epsilon_{0,1} = \epsilon_{0,2} = 0$ and $\epsilon_{1,-1} = \epsilon_{1,0} = 0$. The above equations along with equations (3.20) and (3.21), form a set with the solution (3.24), so that the only possible attack is the blocking attack (3.25), (3.26).

3.6.2 The “Reversed-Space Attack”: A complete non robustness proof for Variant C2

Variant C2, although easy to implement, provides no robustness and is found to be insecure. Using the tools presented above we find $U_{zero}$ to consists attacks that are capable of revealing the information in its entirety to Eve. It should be noted that these attacks are individual-attacks in which Eve uses only a single photon. Limiting Eve to a single photon pulse simplifies the analysis and is sufficient for exhibiting negative results. This attack demonstrates the risks of using practical realizations without performing an extensive security analysis regarding the specific setup in use.

\(^7\)Other states, such as $|1000\>_P$ and $|0001\>_P$ are transformed by the interferometer into modes which are not measured by Bob, such as $|s_3\>$ or $|d_{-1}\>$. Since those state have no contribution to Bob’s error rate, they are omitted here and do not appear in the matrix $\beta$. 

---

\[
\begin{pmatrix}
-1 & 0 & 0 & i & 0 & 0 \\
1 & -1 & 0 & i & 0 & 0 \\
0 & 1 & -1 & 0 & i & 0 \\
0 & 0 & 1 & 0 & 0 & i
\end{pmatrix}
\]
3.6. ROBUSTNESS ANALYSIS OF VARIANT C

Bob performs a basis dependent measurement. For the $x$-basis he measures in the same way presented in Section 3.5.1, while for the $z$-basis he uses the following set: $J_0 = \{|d_0\rangle\}; J_1 = \{|s_2\rangle\}; J_{\text{loss}} = I - J_0 - J_1$; The set $J_{\text{invalid}}$ is empty due to the assumption of using a single-photon states only.

As in the previous section we define Eve’s attacks that cause no error using Corollary 3.1. An attack that induces no errors must satisfy the requirements given by Equation (3.17). The requirements for the $x$-basis, Equation (3.24), remain as presented in Section 3.5.1, while the requirements for the $z$-basis are

$$-\epsilon_{0,1}|E_{0,1}\rangle + \epsilon_{0,2}|E_{0,2}\rangle = 0 \quad \text{when Alice sends } |0_z\rangle \quad (3.34)$$

$$i\epsilon_{1,-1}|E_{1,-1}\rangle + i\epsilon_{1,0}|E_{1,0}\rangle = 0 \quad \text{when Alice sends } |1_z\rangle. \quad (3.35)$$

Thus, the family of Eve’s attacks that cause no errors, is of the following form (avoiding the vacuum state)

$$|0\rangle_E|0_z\rangle \xrightarrow{U_E}$$

$$\epsilon_1|E_1\rangle_E|1000\rangle^p_E + \epsilon_2|E_2\rangle_E|0100\rangle^p_E + \epsilon_3|E_3\rangle_E|0010\rangle^p_E + \epsilon_4|E_4\rangle_E|0001\rangle^p_E \quad (3.36)$$

$$|0\rangle_E|1_z\rangle \xrightarrow{U_E}$$

$$(-\epsilon_3)|E_3\rangle_E|1000\rangle^p_E + \epsilon_3|E_3\rangle_E|0100\rangle^p_E + \epsilon_2|E_2\rangle_E|0010\rangle^p_E + \epsilon_4|E_4\rangle_E|0001\rangle^p_E \quad (3.37)$$

satisfying normalization conditions $|\epsilon_1|^2 + |\epsilon_2|^2 + 2|\epsilon_3|^2 = |\epsilon_4|^2 + |\epsilon_2|^2 + 2|\epsilon_3|^2 = 1$. Define the variable $r$ as the bit value measured by Bob (restricted to the case where Bob and Alice use the same basis, and no loss has occurred). After Bob’s measurement with outcome $r$,

<table>
<thead>
<tr>
<th>Alice State</th>
<th>Eve’s State / $r = 0$</th>
<th>Eve’s State / $r = 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$</td>
<td>0_z\rangle_A$</td>
<td>$\epsilon_1</td>
</tr>
<tr>
<td>$</td>
<td>1_z\rangle_A$</td>
<td>$-\epsilon_3</td>
</tr>
<tr>
<td>$</td>
<td>0_x\rangle_A$</td>
<td>$\epsilon_3</td>
</tr>
<tr>
<td>$</td>
<td>1_x\rangle_A$</td>
<td>$-\epsilon_3</td>
</tr>
</tbody>
</table>

Table 3.1: Eve’s un-normalized states according the state sent by Alice

Eve holds a state as described in Table 3.1. Eve can acquire full information about the original state, for instance by setting $\epsilon_i = 0.5$, $|E_1\rangle = |E_4\rangle$ and letting $|E_i\rangle_E$ be orthogonal for $i = 1, 2, 3$. Therefore, this scheme is completely nonrobust according to Definition 5.1, and therefore insecure.
3.7 Conclusion

We have formulated the conditions for a specific interferometric QKD scheme to be robust, showing a thin evidence for the security of common BB84 implementations, as well as a complete nonrobustness proof for a specific single-photon BB84 implementation variant against individual-particle attack, the reversed-space attack.

The presented analysis is limited due to several assumptions taken: (a) we do not allow the use of a general multiple-photon pulses; (b) we do not consider the use of coherent states; (c) we analyze only one-way protocols (BB84 and six-states); (c) Eve is restricted to collective attacks; (e) we prove only robustness and not full security. A full security analysis, that is not based on (one or more of) the assumptions prescribed above is left for further research.

We conclude that a security analysis of a QKD realization must be done according to the specific equipment in use. A security proof of a theoretical protocol has relevance only when the setup considered is proven to realize the theory in an exact manner. Yet, any realization deviates from theory in a certain way that should be taken into consideration in the security analysis. This conclusion is crucial when considering “off-the-shelf” products, claiming to bring QKD protocols with “proven security”.
Chapter 4

Security of BB84 against Collective Attacks

4.1 Introduction

In this chapter we discuss the security of the BB84 protocol against the collective attack — a subclass of the joint attacks (which are the most powerful theoretic attacks). This subclass is conjectured to be as informative to Eve as the joint attack [11, 51]. In addition, the collective attack is simpler than the joint attack, and might be more relevant for practical setups of QKD. Such protocols are very complicated to analyze, and often lack a security proof against the most general attack.

We improve the analysis of the BB84 scheme against all collective attacks, that is done in [11]. Our proof uses methods that are used in [10] for the joint attack, in order to achieve an optimized bound for the collective attack. The analysis shown in [11] bounds the information in a non-optimal way which adds a factor of $2^r$ to the information bound, where $r$ is the amount of error-correction bits revealed during the protocol. In addition, a factor of $2^m$ is added to the information bound for an $m$-key bit. Our analysis spares those factors and thus has an exponential advantage over [11]. We result with the same information bound that is derived in [10] for the joint attack. In addition, we improve the error-rate obtained in [11] to 7.56%, the same error-rate obtained by [10]. This Chapter is based on [17].

4.1.1 Notations

Let $\mathcal{H}_2$ be a 2-dimensional Hilbert space with standard basis $|0\rangle$, $|1\rangle$ and let $|0^1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|1^1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. It is clear that $|0^1\rangle$, $|1^1\rangle$ is an orthonormal basis. The unitary map $H$ such that $H|0\rangle = |0^1\rangle$ and $H|1\rangle = |1^1\rangle$ is called the Hadamard transformation. One checks easily that $H|0^1\rangle = |0\rangle$ and $H|1^1\rangle = |1\rangle$ i.e.

\[\text{If } |0^0\rangle = |0\rangle_z \text{ and } |1^0\rangle = |1\rangle_z \text{ is the standard basis, then } |0^1\rangle = |0\rangle_z \text{ and } |1^1\rangle = |1\rangle_z.\]
$H^2 = I$. Those bases are used for measurements; measuring a state represented as the density matrix $\rho$ in the $b$ basis returns output 0 with probability $\langle 0^b | \rho | 0^b \rangle$ and 1 with probability $\langle 1^b | \rho | 1^b \rangle$. Thus if the state $|0^b\rangle$ (or $|1^b\rangle$) is measured in the $b$ basis, it results with output 0 (1) with certainty. Yet, when $|0^b\rangle$ or $|1^b\rangle$ is measured in the $\overline{b} = 1 - b$ basis, the output is random, i.e. 0 with probability $\frac{1}{2}$ and 1 with probability $\frac{1}{2}$. This is the principle underlying the BB84 quantum key distribution protocol [7].

In order to send a bitstring $i = i_1 \ldots i_m$ to Bob, Alice first draws randomly a bitstring $b = b_1 \ldots b_m$ and then sends the state $|i^b\rangle = |i_1^b\rangle \ldots |i_m^b\rangle = H^b|i\rangle$ where $H^b = H^{b_1} \otimes \ldots \otimes H^{b_m}$ and $|i\rangle = |i_1 \ldots i_m\rangle$. Once they possess the same bitstring $i$, they agree on some key that is a function of $i$, or in some protocols, a quantum function of $|i^b\rangle$. If this function is the parity of $i$ it seems rather clear that an eavesdropper gets exponentially small information on the key as $m$ increases. Such a property still holds if Alice and Bob use a noisy channel and exchange publicly data for error correction. Getting explicit bounds on the information Eve can access if her attack is collective (i.e. qubitwise) is the aim of this chapter.

### 4.1.2 The BB84 protocol

Let us describe again the BB84 scheme, this time with the specific notations used in this chapter.

1. Alice and Bob agree on a linear error-correction code $C$ with parity check matrix $P^T_C$. They as well agree on a linear key-generation function (represented by the matrix $P^T_K$). Those matrices can be publicly known beforehand or they can be determined during the protocol and sent over the classical channel.

2. Alice randomly chooses $2n$-bit strings $\mathbf{i}, \mathbf{b} \in \mathbb{F}_2^{2n}$. Alice encodes the state $|\mathbf{i}^\mathbf{b}\rangle = |i_1^b\rangle \ldots |i_2n^b\rangle$ and sends it to Bob over the quantum channel, one qubit at a time. Each time Bob receives a qubit he informs Alice, who sends him the next qubit.

3. Alice randomly chooses $n$-bits that will be used to detect eavesdropping. This is done by choosing $\mathbf{s} \in \mathbb{F}_2^n$ such that $|\mathbf{s}| = n$. Alice publicly sends Bob $\mathbf{b}$ and $\mathbf{s}$.

4. Bob applies $H^\mathbf{b}$ to his state. If there is no noise and no eavesdropping, he gets exactly the state $|\mathbf{i}\rangle$ sent by Alice.

5. For each $j \in [1 \ldots 2n]$ such that $s_j = 0$, Bob measures his $j$-th qubit. Bob and Alice compare these bits; if more than $np_a$ bits mismatch, the protocol is aborted. The fixed protocol parameter $p_a$ is actually the ratio of allowed bit-flips of the testing bits.

---

2We denote $\mathbb{F}_2$ the two element field with elements $\{0, 1\}$ which is also denoted $GF(2)$ or $\mathbb{Z}_2$. 

---

Technion - Computer Science Department - M.Sc. Thesis MSC-2009-03 - 2009
4.2. DESCRIPTION OF EVE’S ATTACK AND ITS PROPERTIES

6. Bob measures the remaining \( n \) qubits in the standard basis. The result is denoted \( x_B \) and named the raw key\(^3\).

7. Alice sends Bob the error-correction information \( \xi = x_A P_C^T \). Bob uses \( \xi \) to correct his string \( x_B \). From this point we assume Alice and Bob share the same string \( x \). The string \( \xi \) is called the syndrome of the string \( x \) (with regard to \( P_C^T \)).

8. Alice and Bob compute the key \( k = x P_K^T \).

4.2 Description of Eve’s Attack and its Properties

4.2.1 Eve’s attack

To each qubit \( |i^b_j\rangle \ (j \in [1 \ldots 2n]) \) sent by Alice, Eve attaches a probe that we assume to be in the pure state \( |0^E_j\rangle \) and then applies a unitary transformation \( U_j \) to the composite system \( |0^E_j\rangle |i^b_j\rangle \). Eve keeps her probe in a quantum memory for subsequent measurement and sends Bob his part of the system. Thus, for each qubit there is a particular Hilbert probe space, and a particular \( U_j \). We now concentrate the analysis on a fixed qubit and drop momentarily the subindex \( j \); the global effect of Eve’s action on this particular qubit can be described by the equations

\[
U|0^E\rangle|0^b\rangle = |E_{00}^b\rangle|0^b\rangle + |E_{01}^b\rangle|1^b\rangle = |\phi_0^b\rangle \\
U|0^E\rangle|1^b\rangle = |E_{10}^b\rangle|0^b\rangle + |E_{11}^b\rangle|1^b\rangle = |\phi_1^b\rangle
\]

where \( |E_{00}^b\rangle, |E_{01}^b\rangle, |E_{10}^b\rangle \) and \( |E_{11}^b\rangle \) are vectors (“non normalized states”) in Eve’s Hilbert probe space corresponding to this particular qubit. Since \( U \) is unitary, \( |\phi_0^b\rangle \) and \( |\phi_1^b\rangle \) are of norm 1 and orthogonal. This means that

\[
\langle E_{00}^b|E_{00}^b\rangle + \langle E_{01}^b|E_{01}^b\rangle = 1 \quad \langle E_{10}^b|E_{10}^b\rangle + \langle E_{11}^b|E_{11}^b\rangle = 1 \\
\langle E_{00}^b|E_{10}^b\rangle + \langle E_{01}^b|E_{11}^b\rangle = 0 \quad \langle E_{10}^b|E_{00}^b\rangle + \langle E_{11}^b|E_{01}^b\rangle = 0
\]

It should be noted that for any two (normalized) orthogonal states \( |\phi_0^b\rangle \) and \( |\phi_1^b\rangle \) in the Eve+Bob space, there is always a unitary transformation \( U' \) such that \( U'|0^E\rangle|0^b\rangle = |\phi_0^b\rangle \) and \( U'|0^E\rangle|1^b\rangle = |\phi_1^b\rangle \). All we need in order to have a unitary transformation corresponding to some attack is vectors (non normalized states) \( |E_{ij}^b\rangle \) in Eve’s Hilbert probe space associated to that qubit satisfying Equations (4.3) and (4.4).

\(^3\)We differ the string that Bob measured, \( x_B \), from the string actually sent by Alice, \( x_A \). Those strings differ due to errors and eavesdropping. The difference string of those strings, \( c_s = x_A \oplus x_B \) and the difference of the \( n \)-bit strings used for the error-rate testing, \( c_s \), are used for the security proof (Section 4.3.6).
4.2.2 Extending the attack to multiple qubits

For each qubit $j \in [1 \ldots 2n]$, Eve applies the unitary $U_j$ on the space $H^E_j \otimes H_2$ where $H^E_j$ is her probe space and $H_2$ the qubit space. Eve’s state for each qubit then corresponds to the states $|E^b_{00}\rangle_j$, $|E^b_{01}\rangle_j$, $|E^b_{10}\rangle_j$, $|E^b_{11}\rangle_j$ in $H^E_j$. Eve’s view if the $b_j$ basis was used is obtained by tracing out Bob from the states $|\phi^b_{ij}\rangle_j$ and $|\phi^b_i\rangle_j$. We thus obtain

\begin{align}
(\rho^b_{ij})_j &= |E^b_{00}\rangle_j \langle E^b_{00}| + |E^b_{01}\rangle_j \langle E^b_{01}|, \\
(\rho^b_i)_j &= |E^b_{10}\rangle_j \langle E^b_{10}| + |E^b_{11}\rangle_j \langle E^b_{11}|. 
\end{align}

If Alice sends the string $i$ using bases $b$, then Eve’s global state is the tensor product of all those states $(\rho^b_{ij})_j$ for which $s_j = 1$. The set $\{j \mid s_j = 1\}$ has $n$ elements; let us denote it $\{j_1, \ldots, j_n\}$, so that $s_{j_l} = 1$ for $1 \leq l \leq n$. The string $x = i_s$ selected by the indices $j$ for which $s_j = 1$ is by definition $i_s = i_{j_1} \ldots i_{j_n}$ so that $x_l = i_{j_l}$ for $1 \leq l \leq n$. Similarly, we denote $b_s$ the $n$-bit string $b_{j_1} \ldots b_{j_n}$. Eve’s global state corresponding to $s, b$ and $x$ can now be written

\begin{equation}
\rho^b_{xs} = (\rho^b_{ij_1})_{j_1} \otimes \cdots \otimes (\rho^b_{ij_n})_{j_n} = \bigotimes_{l=1}^n (\rho^b_{i_{j_l}})_{j_l}. 
\end{equation}

If we let $b' = b_s$, and drop the index for the density matrices of individual qubits, we get

\begin{equation}
\rho^b_{xs} = \rho^b_{x} = \rho^b_{x_1} \otimes \cdots \otimes \rho^b_{x_n} = \bigotimes_{l=1}^n \rho^b_{i_{j_l}}. 
\end{equation}

It is the state $\rho^b_{xs}$ or in fact a mixture of such states that Eve measures collectively to guess the key once $b, s$ and the information for error correction is known to her.

4.2.3 The probability of error

Assuming a qubit was attacked by $U$ as defined on Equations (4.1) and (4.2), an error occurs if Alice sent 0 and Bob measured 1 or if Alice sent 1 and Bob measured 0. Let $k$ be the value measured by Bob and $i$ the value sent by Alice, for a specific qubit in the $b$ basis. The probability of Bob measuring an error is given by

\[ p(k = 1 \mid i = 0)p(i = 0) + p(k = 0 \mid i = 1)p(i = 1) = \langle E^b_{01}|E^b_{01}\rangle_{1/2} + \langle E^b_{10}|E^b_{10}\rangle_{1/2}, \]

and we denote

\[ p^b_{k} \triangleq \frac{1}{2} \left[ \langle E^b_{01}|E^b_{01}\rangle + \langle E^b_{10}|E^b_{10}\rangle \right]. \]

4.2.4 The probability of error in the conjugate basis

We are now interested in $p^b_{\bar{k}}$ where $\bar{b} = 1 - b$ (i.e. $\bar{s} = 1$ and $\bar{x} = 0$) corresponds to the conjugate basis of the $b$ basis. Working in the conjugate basis means that Eve has
performed the attack as defined in Equation (4.1) and (4.2) for qubits in basis $b$, but Alice and Bob choose to work with the $\bar{b}$ basis. Using Equation (4.9), this probability of error for this situation is given by $\frac{1}{2} \left[ \langle E_{00}^b | E_{01}^b \rangle + \langle E_{10}^b | E_{11}^b \rangle \right]$. Using the fact that

$$|0\rangle^\bar{b} = \frac{1}{\sqrt{2}} [ |0^b \rangle + |1^b \rangle], \quad |1\rangle^\bar{b} = \frac{1}{\sqrt{2}} [ |0^b \rangle - |1^b \rangle]$$

and using the linearity of $U$, we deduce from Equations (4.1) and (4.2)

$$U|0^E\rangle|0^\bar{b}\rangle = \frac{1}{\sqrt{2}} \left[ (|E_{00}^b\rangle + |E_{10}^b\rangle) |0^b\rangle + \frac{1}{\sqrt{2}} \left( |E_{01}^b\rangle + |E_{11}^b\rangle \right) |1^b\rangle, \quad \tag{4.10} \right.$$

$$U|0^E\rangle|1^\bar{b}\rangle = \frac{1}{\sqrt{2}} \left[ (|E_{00}^b\rangle - |E_{10}^b\rangle) |0^b\rangle + \frac{1}{\sqrt{2}} \left( |E_{01}^b\rangle - |E_{11}^b\rangle \right) |1^b\rangle. \quad \tag{4.11} \right.$$

Now, replacing $|0^b\rangle$ and $|1^b\rangle$ on the right-hand sides with their values in terms of $|0^\bar{b}\rangle$ and $|1^\bar{b}\rangle$ i.e. $|0^b\rangle = \frac{1}{\sqrt{2}} [ |0^\bar{b}\rangle + |1^\bar{b}\rangle]$ and $|1^b\rangle = \frac{1}{\sqrt{2}} [ |0^\bar{b}\rangle - |1^\bar{b}\rangle]$ we obtain

$$U|0^E\rangle|0^\bar{b}\rangle = \frac{1}{2} \left[ |E_{00}^b\rangle + |E_{10}^b\rangle + |E_{01}^b\rangle + |E_{11}^b\rangle \right] |0^\bar{b}\rangle$$

$$+ \frac{1}{2} \left[ \left( |E_{00}^b\rangle - |E_{11}^b\rangle \right) + \left( |E_{10}^b\rangle - |E_{01}^b\rangle \right) \right] |1^\bar{b}\rangle, \quad \tag{4.12} \right.$$

$$U|0^E\rangle|1^\bar{b}\rangle = \frac{1}{2} \left[ \left( |E_{00}^b\rangle - |E_{11}^b\rangle \right) - \left( |E_{10}^b\rangle - |E_{01}^b\rangle \right) \right] |0^\bar{b}\rangle$$

$$+ \frac{1}{2} \left[ |E_{00}^b\rangle - |E_{11}^b\rangle - |E_{01}^b\rangle + |E_{10}^b\rangle \right] |1^\bar{b}\rangle. \quad \tag{4.13} \right.$$

where the terms for $|E_{01}^b\rangle$ and $|E_{10}^b\rangle$ are parenthesized so that we can easily see that

$$p^\bar{e} = \frac{1}{2} \left[ \langle E_{01}^b | E_{01}^b \rangle + \langle E_{10}^b | E_{10}^b \rangle \right]$$

$$= \frac{1}{4} \left[ \langle E_{00}^b | E_{11}^b \rangle \langle E_{00}^b | E_{11}^b \rangle + \langle E_{10}^b | E_{10}^b \rangle \langle E_{10}^b | E_{10}^b \rangle \right].$$

If we expand this result by using the identities $\langle \phi | \psi \rangle = \overline{\langle \psi | \phi \rangle}$ and $z + \overline{z} = 2 \text{Re}(z)$ for $z \in \mathbb{C}$ and using Equalities (4.3) and (4.4) we get

$$p^\bar{e} = \frac{1}{4} \left[ 2 - \langle E_{00}^b | E_{11}^b \rangle - \langle E_{01}^b | E_{01}^b \rangle - \langle E_{01}^b | E_{00}^b \rangle - \langle E_{10}^b | E_{10}^b \rangle \right],$$

$$p^\bar{e} = \frac{1}{2} \left[ 1 - \text{Re} \left( \langle E_{00}^b | E_{11}^b \rangle + \langle E_{01}^b | E_{01}^b \rangle \right) \right]. \quad \tag{4.14} \right.$$

**4.2.5 Flat attacks**

**Proposition 4.1** Let $U$ be such that

$$\langle E_{00}^b | E_{11}^b \rangle + \langle E_{01}^b | E_{10}^b \rangle = e^{i\theta} r \quad \tag{4.15}$$

for $r \in \mathbb{R}_+$. Then there is an attack $U'$ with same $\rho_0$, $\rho_1$ and also same $p^b_e$ as $U$ and for which

$$\langle E_{00}^b | E_{11}^b \rangle + \langle E_{01}^b | E_{10}^b \rangle = r. \quad \tag{4.16}$$
CHAPTER 4. SECURITY OF BB84 AGAINST COLLECTIVE ATTACKS

Proof Let $U'$ be such that

\begin{align*}
U'|0\rangle|0^b\rangle &= |E_{00}^b\rangle|0^b\rangle + |E_{01}^b\rangle|1^b\rangle = |\phi_0^b\rangle, \\
U'|0\rangle|1^b\rangle &= e^{-i\theta}|E_{10}^b\rangle|0^b\rangle + e^{-i\theta}|E_{11}^b\rangle|1^b\rangle = |\phi_1^b\rangle.
\end{align*}

(4.17) (4.18)

There is such a $U'$ because Equations (4.3) and (4.4) are satisfied for these new coefficients. Moreover, with this new attack, $\rho_0^b$ and $\rho_1^b$ are left unchanged as can be seen from Equations (4.5) and (4.6). In the same way, the right hand side of Equation (4.9) is also clearly left unchanged and so $p_e^b$ is left unchanged. Finally

\begin{align*}
\langle E_{00}^b | E_{11}^b \rangle + \langle E_{01}^b | E_{10}^b \rangle &= \langle E_{00}^b | e^{-i\theta} E_{11}^b \rangle + \langle E_{01}^b | e^{-i\theta} E_{10}^b \rangle \\
&= e^{-i\theta} e^{i\theta} r \\
&= r.
\end{align*}

(4.19)

This new attack thus provides the same “view” $\rho_0^b$, $\rho_1^b$ to Eve, and the same probability of being detected if the $b$ basis is used. However, from Equation (4.14) we see that the new attack reduces $p_e^b$ to the minimum value (4.14) can take, because $\text{Re}(z) \leq |z|$ for any $z \in \mathbb{C}$. This means that with this new attack, Eve’s probability of being detected had the other basis been chosen can only decrease. This attack is thus better for Eve, since she needs to take into account all possible bases used by Alice. Such an attack will be said to be “flat”. In the more general case of bitstrings, since Eve’s view comes from the tensor product of density matrices on individual qubits, flat attacks on all qubits does not change Eve’s global view, nor the probability of error in the $b$ basis. A flat attack will thus be flat for each qubit. In a flat attack (one qubit case), there exists $r \in \mathbb{R}_+$ such that

\begin{align*}
\langle E_{00}^b | E_{11}^b \rangle + \langle E_{01}^b | E_{10}^b \rangle &= r, \\
p_e^b &= \frac{1}{2}(1 - r).
\end{align*}

(4.19) (4.20)

A short summary: we consider two possible cases for a specific qubit sent by Alice to Bob that is attacked by Eve with a flat unitary transformation $U$:

1. Alice and Bob use the $b$ basis. Eve’s attack causes a bit-flip with probability $p_e^b = \frac{1}{2} \left[ \langle E_{01}^b | E_{01}^b \rangle + \langle E_{10}^b | E_{10}^b \rangle \right]$.  

2. Alice and Bob use the $\overline{b}$ basis. Eve’s attack causes a bit-flip with probability $p_e^{\overline{b}} = \frac{1}{2} \left[ 1 - (\langle E_{00}^b | E_{11}^b \rangle + \langle E_{01}^b | E_{10}^b \rangle) \right]$.
4.2.6 A purification

We now assume the attack is flat, i.e. it satisfies Equations (4.3), (4.4) and (4.19) and also, as a result, Equation (4.20). Let us now define $|\psi_0^b\rangle$ and $|\psi_1^b\rangle$ as

$$|\psi_0^b\rangle = |E_{00}^b\rangle|0\rangle + |E_{01}^b\rangle|1\rangle$$

$$|\psi_1^b\rangle = |E_{11}^b\rangle|0\rangle + |E_{10}^b\rangle|1\rangle$$

where the states $|0\rangle$ and $|1\rangle$ live in some Hilbert space that need not correspond to any physical reality (they are useful mathematical entities), are normalized and orthogonal. If we trace out this Hilbert space from the state $|\psi_0^b\rangle\langle\psi_0^b|$ we get $\rho_0$ defined in (4.5); in the same way, if we trace out this Hilbert space from the state $|\psi_1^b\rangle\langle\psi_1^b|$ we get $\rho_1$ defined in (4.6). The states $|\psi_0^b\rangle$ and $|\psi_1^b\rangle$ are thus lift-ups of $\rho_0$ and $\rho_1$. Since they are also pure, they are said to be purifications of $\rho_0$ and $\rho_1$. Moreover they are normalized and their overlap is

$$\langle\psi_0^b|\psi_1^b\rangle = \langle E_{00}^b|E_{11}^b\rangle + \langle E_{01}^b|E_{10}^b\rangle = r.$$  

This establishes a direct relation between the overlap of $|\psi_0^b\rangle$ and $|\psi_1^b\rangle$ and the probability of error $p_e$. Since the overlap $r$ is real and positive, with $0 \leq r \leq 1$, there is an angle $\alpha$ such that

$$\cos(2\alpha) = r = \langle\psi_0^b|\psi_1^b\rangle$$

$$0 \leq \alpha \leq \pi/4$$

As a consequence, we get

$$p_e = \frac{1}{2}[1 - \cos(2\alpha)] = \sin^2(\alpha),$$

$$\sin(\alpha) = (p_e)^{1/2}.$$  

Since $\langle\psi_0^b|\psi_1^b\rangle$ is real, it is equal to $\langle\psi_1^b|\psi_0^b\rangle$ and consequently the states $|\psi_0^b\rangle + |\psi_1^b\rangle$ and $|\psi_0^b\rangle - |\psi_1^b\rangle$ are orthogonal and their norms are $\sqrt{2 + 2\cos(2\alpha)} = 2\cos(\alpha)$ and $\sqrt{2 - 2\cos(2\alpha)} = 2\sin(\alpha)$ respectively. We thus let

$$|0_H^b\rangle = \frac{1}{2\cos(\alpha)}(|\psi_0^b\rangle + |\psi_1^b\rangle),$$

$$|1_H^b\rangle = \frac{1}{2\sin(\alpha)}(|\psi_0^b\rangle - |\psi_1^b\rangle).$$

In this basis, we can re-write the purification, for $x \in \{0, 1\}$, as

$$|\psi_x^b\rangle = \cos(\alpha)|0_H^b\rangle + (-1)^x \sin(\alpha)|1_H^b\rangle.$$  

(4.22)

4.3 Security Proof of BB84 against collective attacks

4.3.1 Notations and distinguishability

Parity strings for the code and the key

Bitstrings of length $n$ will be identified with elements of the $n$ dimensional $\mathbb{F}_2$-vector space $\mathbb{F}_2^n$ and vector addition will be denoted $+$ or $\oplus$; it corresponds to component-wise sum
modulo 2 and thus to the exclusive-or of the corresponding bitstrings. We assume a given basis of \(\mathbb{F}_2^n\), \(\{v_1, \ldots, v_n\}\). The vectors \(v_1, \ldots, v_r\) are used as the rows of \(P_C\), the parity check matrix for the error correcting code; the vectors \(v_{r+1}, \ldots, v_{r+m}\) are used as the rows of a matrix \(P_K\) such that if \(x\) is the string sent by Alice, then the \(m\)-bit key is \(k = xP_K^T\).

For any \(r'\) we denote \(V_{r'}\) the span of \(\{v_1, \ldots, v_{r'}\}\) and \(V_{c_r}\) the span of \(\{v_{r'+1}, \ldots, v_n\}\); it is clear that \(V_{r'} + V_{c_r} = \mathbb{F}_2^n\). Moreover, if we let \(v, w \in V_{r'}\) and \(v', w' \in V_{c_r}\), then

\[
v + v' = w + w' \implies v = w \text{ and } v' = w'.
\]

This property is normally summarized by saying that \(\mathbb{F}_2^n\) is the direct sum of \(V_{r'}\) and \(V_{c_r}\), i.e., \(V_{r'} + V_{c_r} = \mathbb{F}_2^n\) and \(V_{r'} \cap V_{c_r} = \{0\}\). See Appendix C for several definitions and notation of Coding Theory, used in the sections below.

**A security parameter**

Let

\[
d_{r,m} \triangleq \min_{r \leq r' < r + m} d_H(v_{r'+1}, V_{r'}) = \min_{r \leq r' < r + m} d_{r', 1}.
\]

This will be used as a security parameter.

**The Shannon distinguishability**

We shall use \(SD(\alpha, \beta)\) as it defined in [11] to denote the Shannon Distinguishability between the state (or density matrix) \(\alpha\) to the state (or density matrix) \(\beta\). Consider the following protocol: A chooses ‘0’ or ‘1’, randomly with equal probability. If A chooses ‘0’, he sends the state \(\alpha\) over to B. Otherwise, he sends \(\beta\). \(SD(\alpha, \beta)\) is by definition B’s accessible information i.e. the maximum mutual information between A’s encoded bit and B’s measurement of the state he received. Notice that when \(\alpha\) and \(\beta\) are orthogonal (thus they form a basis), B can always distinguish between them, and has information of exactly 1 bit about A’s choosen bit. On the other hand, If \(\alpha = \beta\), B can never distinguish between these states, and he has 0 bits of information. Some important properties of the \(SD\) quantity are given by the following lemma:

**Lemma 4.2**

(a) If \(\tilde{\rho}_x\) is a lift-up of \(\rho_x\) (where \(x \in \{0, 1\}\), then \(SD(\rho_0, \rho_1) \leq SD(\tilde{\rho}_0, \tilde{\rho}_1)\);

(b) The Shannon Distinguishability of two states can be bounded by half the Trace Norm of their difference: \(SD(\rho_0, \rho_1) \leq \frac{1}{2} \text{tr} |\rho_0 - \rho_1|\)

**Proof**

These inequalities are proven in [11, 10].

**4.3.2 Representing states for bitstrings**

Let \(s\) be a fixed string of length \(2n\) with a ‘1’ in positions \(j_1, \ldots, j_n\) corresponding to the \(n\) information bits. Given the basis string \(b' = b'_1 \ldots b'_n = b_{j_1} \ldots b_{j_n}\) and \(x = x_1 \ldots x_n = \)
\[ i_{j_1} \ldots i_{j_n} \] we define the state \(|\psi_X^{b'}\rangle = \bigotimes_{l=1}^{n} |\psi_{2l}^{b'}\rangle\). Using Equation (4.2.2), we write the state as
\[
|\psi_X^{b'}\rangle = \bigotimes_{l=1}^{n} [\cos(\alpha_l) |0_l\rangle + (-1)^{x_l} \sin(\alpha_l) |1_l\rangle],
\] (4.24)
where \(|0_l\rangle\) and \(|1_l\rangle\) represent the vectors \(|0_{2l}^{b'}\rangle\) and \(|1_{2l}^{b'}\rangle\) corresponding to the attack \(U_{j_l}\) on the \(j_l\)-th qubit (the \(l\)-th information qubit). If for \(c = c_1 \ldots c_n \in \{0,1\}^n\) we define
\[
d_c = d_1^c \ldots d_n^c
\]
denoted by \(d_c\), then
\[
|\psi_X^{b'}\rangle = \sum_{c \in \{0,1\}^n} d_c(-1)^{x_c} |c\rangle
\] (4.25)
where \(|c\rangle\) stands for \(|(c_1)_1 \ldots (c_n)_n\rangle\); for instance if \(c = 0100\) then \(|c\rangle = |0_1\rangle|1_2\rangle|0_3\rangle|0_4\rangle\) with \(|0_i\rangle\) and \(|1_i\rangle\) as defined above. In the square value \(d_c^2\) of \(d_c\), the factors can be interpreted as probabilities. Indeed, from Equation (4.21) we deduce
\[
d_c^2 = \begin{cases} 
\cos^2(\alpha_l) = \overline{q_l^c} & \text{if } c_l = 0 \\
\sin^2(\alpha_l) = \overline{p_l^c} & \text{if } c_l = 1
\end{cases}
\] (4.26)
where \(\overline{p_l^c}\) is the probability of an error on the \(l\)-th information qubit (on qubit \(j_l\)) if measurement is made in the conjugate basis and \(\overline{q_l^c} = 1 - \overline{p_l^c}\) is the probability of no error on the \(l\)-th information qubit if measurement is made in the conjugate basis. This means that \(d_c^2\) is the probability of having exactly the error string \(c\) if for every information qubit, measurement is made in the other basis. If we represent by \(C_I\) the random variable corresponding to the error in Bob’s measurement of the information bits, and by \(B_I\) the random variable giving the basis string chosen by Alice then we can write, for \(c \in \{0,1\}^n\), \(b \in \{0,1\}^{2n}\) and \(s \in \{0,1\}^{2n}\) such that \(|s\rangle = n\),
\[
d_c^2 = P[C_I = c | B_I = \overline{B}_s, s]
\] (4.26.3)
where \(\overline{B}_s = \overline{b'} = \overline{b}_1 \ldots \overline{b}_{n'}\). This probability is not conditional on the syndrome \(\xi\); all possible errors are taken into account here, even with values of \(x\) inconsistent with \(\xi\).

### 4.3.3 Case of a one-bit key

We begin with proving the security of a 1-bit key, and then extend our proof to an arbitrary \(m\)-bit length key. This case corresponds to \(m = 1\) and the key (when not discarded) is \(x \cdot r_{r+1}\) where \(x\) is the string sent by Alice (that is, \(P_K\) has only one row, which equals \(v_{r+1}\)). Let \(\xi = xP_K^T\) be the \(r\) bit syndrome announced publicly by Alice and let us denote...
\( \hat{\rho}_0 \) and \( \hat{\rho}_1 \) Eve’s states corresponding to key 0 and key 1 respectively. Those states are obtained by normalizing the operators\(^4\)

\[
\rho_k = \sum_{x} |x \rangle \langle x|^{P_T^C} = \xi
\]

and, since \( \text{tr}(\rho_0) = \text{tr}(\rho_1) = 2^{n-r-1} \), \( \hat{\rho}_0 \) and \( \hat{\rho}_1 \) are equally likely and

\[
\hat{\rho}_k = \frac{1}{2^{n-r-1}} \sum_{x} \rho_k^{\mathbf{x}}
\]

Changing the attack to a flat one, does not change \( \rho_k^{\mathbf{x}} \), and therefore does not change \( \hat{\rho}_k \). Moreover, since \( |\psi^{\mathbf{x}}_{b}\rangle\langle\psi^{\mathbf{x}}_{b}| \) as defined in Equation (4.22) is a purification of \( \rho_k^{\mathbf{x}} \), it follows that

\[
\hat{\rho}_k = \frac{1}{2^{n-r-1}} \sum_{x} |\psi^{\mathbf{x}}_{b}\rangle\langle\psi^{\mathbf{x}}_{b}|\]

is a purification of \( \hat{\rho}_k \). According to Lemma 4.2, Eve’s information \( SD(\hat{\rho}_0, \hat{\rho}_1) \) on the key satisfies the following inequality

\[
SD(\hat{\rho}_0, \hat{\rho}_1) \leq \frac{1}{2} \text{tr} |\hat{\rho}_0 - \hat{\rho}_1|.
\]

4.3.4 Calculating and bounding the trace norm for one bit: the Biham basis.

We now wish to bound \( \frac{1}{2} \text{tr} |\hat{\rho}_0 - \hat{\rho}_1| \) matching the specific attack performed by Eve. Since \( V_r + V^c_r = \mathbb{F}_2^n \) and \( V_r \cap V^c_r = \{0\} \), we can simplify equation (4.25)

\[
|\psi^{\mathbf{x}}_{b}\rangle = \sum_{v \in V_r^c} (-1)^{\mathbf{x} \cdot v} \sum_{v' \in V_r} (-1)^{\mathbf{v} \cdot v'} d_{v \oplus v'} |v \oplus v'|.
\]

Let \( i_\xi \) be a fixed \( n \)-bits string that is in the same code coset of \( C \) as \( \mathbf{x} \), having the same syndrome \( \xi \), i.e. \( i_\xi \cdot P_T^C = \xi \). Being in the same coset means that the difference string \( \mathbf{x} - i_\xi \) is a codeword. It follows that for every string in the dual code \( v' \in C^\perp = V_r \) we get \( v'(\mathbf{x} - i_\xi) = 0 \) so that \( v' \mathbf{x} = v' i_\xi \) and we can write

\[
|\psi^{\mathbf{x}}_{b}\rangle = \sum_{v \in V_r^c} (-1)^{\mathbf{x} \cdot v} \sum_{v' \in V_r} (-1)^{i_\xi \cdot v'} d_{v \oplus v'} |v \oplus v'|.
\]

\(^4\) State \( \rho_k^{\mathbf{x}} \) is defined by Equations (4.8) and (4.7).
4.3. SECURITY PROOF OF BB84 AGAINST COLLECTIVE ATTACKS

Define the Biham basis

\[ |\eta_v\rangle = \sum_{v' \in V_r} (-1)^{i \cdot v'} d_{v \oplus v'} |v \oplus v'\rangle, \]  

(4.30)

to conclude with

\[ |\psi^{b'}_x\rangle = \sum_{v \in V^e_r} (-1)^{x \cdot v} |\eta_v\rangle. \]  

(4.31)

**Lemma 4.3** The non normalized states \( |\eta_v\rangle \) for \( v \in V^e_r \) are orthogonal.

**Proof**

\[
\langle \eta_{v_1} | \eta_{v_2} \rangle = \sum_{v'_1 \in V_r} (-1)^{i \cdot v'_1 \cdot d_{v \oplus v'} (v_1 \oplus v')_1} \sum_{v'_2 \in V_r} (-1)^{i \cdot v'_2 \cdot d_{v \oplus v'} (v_2 \oplus v')_2}.
\]

If \( (v_1 \oplus v'_1 |v_2 \oplus v'_2) \neq 0 \), then \( v_1 \oplus v'_1 = v_2 \oplus v'_2 \) which, by Equation (4.23), implies \( v_1 = v_2 \) (and \( v'_1 = v'_2 \)).

The \( |\eta_v\rangle \) thus provide an orthogonal (but not orthonormal) basis with which we can simply represent \( |\psi^{b'}_x\rangle \), as shown in Equation (4.31).

Using Equation (4.28) we get

\[
\tilde{\rho}_0 - \tilde{\rho}_1 = \frac{1}{2^{n-r-1}} \sum_{x \cdot P^T_C = \xi} |\psi^{b'}_x\rangle \langle \psi^{b'}_x| - \frac{1}{2^{n-r-1}} \sum_{x \cdot P^T_C = \xi} \langle \psi^{b'}_x| \langle \psi^{b'}_x|. \]

The set of elements \( \{x | x \cdot P^T_C = \xi\} \) can be written as the code coset that consists the string \( i_\xi \), namely, \( \{c \oplus i_\xi | c \in C\} \), where for every different element \( c \), the string \( c \oplus i_\xi \) represents a different possible \( x \). Moreover, the final key bit \( k \) can be written as \( (c \oplus i_\xi) \cdot v_{r+1} \), which gives us, using Equation (4.31)

\[
\tilde{\rho}_0 - \tilde{\rho}_1 = \frac{1}{2^{n-r-1}} \sum_{c \in C} (-1)^{(c \oplus i_\xi) \cdot v_{r+1} + 1} |\psi^{b'}_{c \oplus i_\xi}\rangle \langle \psi^{b'}_{c \oplus i_\xi}|.
\]

Re-arranging the elements produces

\[
\tilde{\rho}_0 - \tilde{\rho}_1 = \frac{1}{2^{n-r-1}} \sum_{m, m' \in V^e_r} (-1)^{(m \oplus m' \oplus v_{r+1}) \cdot i_\xi} \left( \sum_{c \in C} (-1)^{(m \oplus m' \oplus v_{r+1}) \cdot c} \right) |\eta_m\rangle \langle \eta_{m'}|. \]  

(4.32)

**Lemma 4.4** For every Linear Code \( C \),

\[
\sum_{c \in C} (-1)^{c \cdot w} = \begin{cases} |C| & w \in C^\perp, \\
0 & else.
\end{cases}
\]
CHAPTER 4. SECURITY OF BB84 AGAINST COLLECTIVE ATTACKS

Proof If \( w \in C^\perp \) then \( c \cdot w = 0 \) for every \( c \in C \) by the definition of \( C^\perp \). Otherwise, let \( \{ \beta_1 \ldots \beta_k \} \) be a basis of \( C \). Every codeword \( c \in C \) can be written as a linear combination (over \( F_2^n \)) of the basis elements \( c = \alpha_1 \beta_1 \oplus \ldots \oplus \alpha_k \beta_k \), where \( \alpha_i \in \{0, 1\} \). Define \( \alpha = \alpha_1 \ldots \alpha_k \), every \( \alpha \in F_2^k \) corresponds to a different \( c \in C \), i.e. it is an isomorphism. Let \( t_i \in \{0, 1\} \) be \( \beta_i \cdot w \), and \( t = t_1 \ldots t_k \), then

\[
\sum_{c \in C} (-1)^{c \cdot w} = \sum_{\alpha \in F_2^k} (-1)^{(\alpha_1 \beta_1 \oplus \ldots \oplus \alpha_k \beta_k) \cdot w}
= \sum_{\alpha \in F_2^k} (-1)^{\alpha_1 t_1 \oplus \ldots \oplus \alpha_k t_k}
= \sum_{\alpha \in F_2^k} (-1)^{\alpha \cdot t} = 0
\]

\( t \) is nonzero since \( w \notin C^\perp \).

We can use Lemma 4.4 to discard most of the elements of \( \tilde{\rho}_0 - \tilde{\rho}_1 \), for the parenthesized element of (4.32) is zero unless \( (m \oplus m' \oplus v_{r+1}) \in C^\perp = V_r \) this happens only when \( m \oplus m' \oplus v_{r+1} = 0 \), since \( m, m', v_{r+1} \in V_r^c \) (and so is their sum), and since \( V_r \cap V_r^c = \{0\} \). This means that only when \( m' = m \oplus v_{r+1} \) the parenthesized element equals \( |C| = 2^{n-r} \).

\[
\tilde{\rho}_0 - \tilde{\rho}_1 = 2 \sum_{m \in V_r^c} (-1)^{(m \oplus (m \oplus v_{r+1}) \oplus v_{r+1})} |\eta_m\rangle \langle \eta_m \oplus v_{r+1}|
= 2 \sum_{m \in V_r^c} |\eta_m\rangle \langle \eta_m \oplus v_{r+1}|
\]

and we conclude that

\[
\frac{1}{2} \text{tr} |\tilde{\rho}_0 - \tilde{\rho}_1| = \text{tr} \sum_{m \in V_r^c} |\eta_m\rangle \langle \eta_m \oplus v_{r+1}|
\]

By Lemma 4.3, \( \langle \eta_m | \eta_n \rangle = 0 \) if \( m \neq n \) with \( m, n \in V_r^c \). If we let \( \langle \eta_m | \eta_n \rangle = d_{m,n}^2 \) we get, \( \sum_{m \in V_r^c} d_{m,n}^2 = 1 \) by Equation (4.31). Let us rewrite the \( |\eta_m\rangle \) for \( m \in V_r^c \) as \( |\eta_m\rangle = d_{m,n} |\tilde{\eta}_m\rangle \) with \( \langle \tilde{\eta}_m | \tilde{\eta}_n \rangle = \delta_{m,n} \) for \( m, n \in V_r^c \). It is known that for any operator \( A \), \( |A| = \sqrt{A^\dagger A} \) and...
4.3. SECURITY PROOF OF BB84 AGAINST COLLECTIVE ATTACKS

Thus\(^5\)
\[
\text{tr} \left| \sum_{m \in V_c} |\eta_m\rangle \langle \eta_{m \oplus v_{r+1}}| \right| = \text{tr} \sqrt{\sum_{m \in V_c} |\eta_m\rangle \langle \eta_{m \oplus v_{r+1}}| \sum_{m' \in V_c} |\eta_{m' \oplus v_{r+1}}\rangle \langle \eta_{m'}|}
\]
\[
= \text{tr} \sqrt{\sum_{m,m' \in V_c} |\eta_m\rangle \langle \eta_{m \oplus v_{r+1}}| \langle \eta_{m'}|}
\]
\[
= \text{tr} \sqrt{\sum_{m \in V_c} d_{\eta_m \oplus v_{r+1}}^2 d_{\eta_m} \langle \eta_m|}
\]
\[
= \sum_{m \in V_c} d_{\eta_m \oplus v_{r+1}} d_{\eta_m}
\]
(4.33)

where the last equation follows directly from the spectral decomposition that figures under the square root. Using the fact that \(V_c = V_{r+1} \cup (v_{r+1} + V_{r+1}')\) and that this union is disjoint, we deduce
\[
\frac{1}{2} \text{tr} |\hat{\rho}_0 - \hat{\rho}_1| = 2 \sum_{m \in V_{r+1}'} d_{\eta_m} d_{\eta_m \oplus v_{r+1}}.
\]
(4.34)

In order to bound this result we use the following Lemma,

**Lemma 4.5** Let \(I\) be any set, \(s : I \to I\) be such that \(s^2 = 1_I\) and \(p_i \geq 0\) with \(\sum_{i \in I} p_i \leq 1\). Let \(I' \subseteq I\) and \(E \subseteq I\) such that \(I' \cap s(I') = \emptyset\) and \(I' \subseteq E \cup s(E)\); then
\[
\sum_{i \in I'} \sqrt{p_i} p_{s(i)} \leq \sqrt{\sum_{i \in E} p_i}.
\]

**Proof** For \(i \in I'\), if \(i \notin E\) let \(h(i) = s(i) \in E\) and \(h(s(i)) = i\), else let \(h(i) = i \in E\) and \(h(s(i)) = s(i)\). This function is well defined because \(i\) and \(s(i)\) cannot be both in \(I'\). Moreover \(h(h(i)) = i\) and \(h\) is thus 1–1 on \(I'\).
\[
\sum_{i \in I'} \sqrt{p_i} p_{s(i)} = \sum_{i \in I'} \frac{\sqrt{p_{h(i)}}}{\sqrt{P_{s(h(i))}}} \leq \sqrt{\sum_{i \in I'} p_{h(i)}} \sqrt{\sum_{i \in I'} P_{s(h(i))}} \leq \sqrt{\sum_{i \in E} p_i}
\]
the first inequality being justified by Schwartz inequality.

Let \(I = V_c\), \(I' = V_{r+1}'\), \(s(m) = m + v_{r+1}\); clearly \(I' \cap s(I') = \emptyset\) and \(s^2 = 1_I\). Let also \(E = \{m \in I \mid d_H(m, V_r) \geq d_{r,1}/2\}\) where \(d_{r,1}\) was defined as the smallest Hamming distance between \(v_{r+1}\) and the elements of \(V_r\). For the lemma to apply, we need to show that \(I' \subseteq E \cup s(E)\). If \(m \in I'\) was such that \(m \notin E\) and \(m \notin s(E)\) then \(s(m) \notin E\), \(d_H(m, V_r) < d_{r,1}/2\) and \(d_H(m + v_{r+1}, V_r) < d_{r,1}/2\); this implies \(d_H(v_{r+1}, V_r) < d_{r,1}\),

\(^5\)Here \(A\) is Hermitian, therefore \(|A| = \sqrt{AA^\dagger}|\).
CHAPTER 4. SECURITY OF BB84 AGAINST COLLECTIVE ATTACKS

contrary to the definition of \( d_{r,1} \). Moreover, if \( c = m + v' \) for \( m \in E \) and \( v' \in V_r \) then \(|c| \geq d_{r,1}/2 \). Consequently, letting \( p_m = d_{\eta_m}^2 \) for \( m \in I \),

\[
\left( \frac{1}{2} \text{tr} |\tilde{\rho}_0 - \tilde{\rho}_1| \right)^2 = 4 \left( \sum_{m \in V_r} d_{\eta_m} d_{\eta_m \oplus v_{r+1}} \right)^2 \quad \text{By (4.34)}
\]

\[
\leq 4 \left( \sum_{m \in E} d_{\eta_m}^2 \right)^2 \quad \text{By Lemma 4.5}
\]

\[
= 4 \sum_{m \in V_r} \sum_{v' \in V_r} d_{m \oplus v'}^2 = 4 \sum_{|c| \geq d_{r,1}/2} d_{c}^2.
\]

Using Lemma 4.2, we get

\[
SD(\tilde{\rho}_0, \tilde{\rho}_1) \leq \frac{1}{2} \text{tr} |\tilde{\rho}_0 - \tilde{\rho}_1| \leq 2 \sqrt{\sum_{|c| \geq d_{r,1}/2} d_{c}^2}. \quad (4.35)
\]

Note that this result is identical to the tight bound derived in [10, Lemma 4.5 (Eq. D.8)]. This result is much better than the loose bound [10, Lemma D.2 (Eq. D.3)] which is based on the methods of [11]. Using Equation (4.26) we get

\[
SD(\tilde{\rho}_0, \tilde{\rho}_1) \leq 2 \sqrt{P \left[ |C_I| \geq d_{r,1}/2 \mid B_I = \overline{B}, s \right]} \quad (4.36)
\]

4.3.5 Bounding Eve's accessible information

We now rewrite more carefully inequality (4.36) so as to be able to take into account all the parameters that were fixed and that we will now let vary. The syndrome \( \xi \) gives Eve some information about \( x \) and her information also depends on the characteristic string \( s \) for the information bits and on the 2n-bitstring corresponding to the bases \( b \) used by Alice. We will also use the following notations: the 2n-bitstring sent by Alice is \( i^A \), and the string measured by Bob is \( i^B \); those strings contain information bits selected by \( s \), namely \( i_s^A \) and \( i_s^B \) and test bits \( \overline{i_s^A} \) and \( \overline{i_s^B} \). The 2n-bit error string \( c \) is \( i^A + i^B \), the exclusive OR of the string sent by Alice and of the one measured by Bob; the corresponding error on the information bits is \( c_s \) and the error on the test bits is \( c_s \). The random variable corresponding to \( c_s \) and \( c_s \) will be denoted \( C_I \) and \( C_T \) respectively; they depend on \( b \) and \( s \). For any fixed attack \( U = U_1 \otimes \ldots \otimes U_{2n} \), Eve’s information depends only on \( b_s \), \( s \) and \( \xi \) but we will use the full string \( b \) as arguments in order to lighten the notation. In particular the n-bit string \( \overline{b} = \overline{b}_s \) that appears on the right-hand side of Equation (4.36) corresponds to the information part of the 2n-bitstring \( b + s \), the 2n-bitstring obtained from \( b \) by flipping the bits where \( s \) is 1. With those notations, Equations (4.26) and (4.36) rewrite

\[
d_{c_s}^2 = P[C_I = c_s \mid b + s, s] \quad SD(\tilde{\rho}_0, \tilde{\rho}_1) \leq 2 \sqrt{P \left[ |C_I| \geq d_{r,1}/2 \mid b + s, s \right]}
\]
where the information bits of $C_I$ are determined by $s$ and the $2n$ basis bitstring is $b + s$.

**Corollary 4.6** For a 1-bit key $k$,

$$I(K; E \mid b, s, \xi, c_s) \leq 2 \sqrt{P \left( |C_I| \geq \frac{d_{r,1}}{2} \right) \mid b + s, s}$$

(4.37)

where $K$ is the random variable giving as output key $k$ and $E$ is the random variable corresponding to the outputs of Eve’s (optimal) measurement.

**Proof** This follows from the fact that $SD(\hat{\rho}_0, \hat{\rho}_1)$ is Eve’s accessible information on $k$ if she holds $\hat{\rho}_k$ given by Equation (4.27). These states correspond to Eve’s state when Alice encodes the key-bit $k$ assuming that Eve learns $\xi$, $b$ and $s$. Eve’s information also depends in principle on $c_s$ but since her attack on a qubit is independent of the other qubits, the bits of $c_s$ have no influence on her state.

**Proposition 4.7** For an $m$-bit key $k$,

$$I(K; E \mid b, s, \xi, c_s) \leq 2^m \sqrt{P \left( |C_I| \geq \frac{d_{r,m}}{2} \right) \mid b + s, s}$$

(4.38)

**Proof** This follows by applying the chain rule for mutual information. Details of the proof can be found in [10].

The value we want to bound is Eve’s expected information, where we consider that she gets 0 bits of information when the test fails. The test passes if $|C_T| / n \leq p_a$. If we let

$$I_{(p_a)}(K; E \mid b, s, \xi, c_s) = \begin{cases} I(K; E \mid b, s, \xi, c_s) & \text{if } \frac{|c_s|}{n} \leq p_a \\ 0 & \text{otherwise} \end{cases}$$

(4.39)

then the accessible information to bound, denoted

$$\langle I_{Eve}^{(p_a)} \rangle = \sum_{b, s, \xi, c_s} I_{(p_a)}(K; E \mid b, s, \xi, c_s)p(b, s, \xi, c_s).$$

(4.40)

**Theorem 4.8**

$$\langle I_{Eve}^{(p_a)} \rangle \leq 2^m \sqrt{P \left( \left| \frac{C_I}{n} \right| \geq \frac{d_{r,m}}{2n} \right) \land \left( \left| \frac{C_T}{n} \right| \leq p_a \right)}$$

(4.41)

where $\left| \frac{C_T}{n} \right|$ is the random variable corresponding to the error rate on the test bits and $\left| \frac{C_I}{n} \right|$ is the random variable corresponding to the error rate on the information bits.

---

6The notation in [10] is $\langle I_{Eve}^{(p_a)} \rangle$, the value $p_a$ being fixed.
**Proof** The function $x^2$ is convex, i.e. $(\sum_i p_i x_i)^2 \leq \sum_i p_i x_i^2$ for $p_i \geq 0$, $\sum_i p_i = 1$. We apply this to the square $\langle I_{Eve}^{(p_a)} \rangle^2$ of the information we want to bound.

\[
\langle I_{Eve}^{(p_a)} \rangle^2 = \left[ \sum_{b,s,\xi,c_b} I_{Eve}^{(p_a)}(K; E | b, s, \xi, c_b)p(b, s, \xi, c_b) \right]^2 \quad \text{by (4.40)}
\]

\[
\leq \sum_{b,s,\xi,c_b} I_{Eve}^{(p_a)}(K; E | b, s, \xi, c_b)p(b, s, \xi, c_b) \quad \text{by convexity of } x^2
\]

\[
\leq \sum_{|\xi| \leq p_a, b, s, \xi} I^2(K; E | b, s, \xi, c_b)p(c_b, b, s, \xi) \quad \text{by (4.39)}
\]

\[
\leq 4m^2 \sum_{|\xi| \leq p_a, b, s, \xi} P \left[ \left| C_I \right| \geq \frac{d_{r,m}}{2} \right] | c_s, b+s, s \right) p(c_s, b, s, \xi) \quad \text{by (4.38)}.
\]

Once $s$ and $b$ are given, the information bits are not dependent on the test bits, $P[C_I = c_I | b+s, s] = P[C_I = c_I | c_s, b+s, s]$.

\[
\langle I_{Eve}^{(p_a)} \rangle^2 \leq 4m^2 \sum_{|\xi| \leq p_a, b, s} P \left[ \left| C_I \right| \geq \frac{d_{r,m}}{2} \right] \left| c_s, b+s, s \right] p(c_s, b, s).
\]

Since the test bits are unaffected by replacing the basis of the information bits:

\[
p(c_s, b, s) = p(c_s | b, s)p(b, s) = p(c_s | b+s, s)p(b, s) = p(c_s | b+s, s)p(b+s, s) = p(c_s, b+s, s) \quad (4.42)
\]

and since the probability $p(b, s)$ is equal for all $b$ and $s$ (those strings being chosen completely randomly by Alice, with the condition that $|s| = n$), we conclude with

\[
\langle I_{Eve}^{(p_a)} \rangle^2 \leq 4m^2 P \left[ \left| C_I \right| \geq \frac{d_{r,m}}{2} \right] \wedge \left( \frac{|C_T|}{n} \leq p_a \right) \quad (4.43)
\]

**4.3.6 Proof of security**

Following the point of view of [10] we choose a code such that $\frac{d_{r,m}}{2n} > p_a + \epsilon$ for some $\epsilon$; the right-hand side of Equation (4.41) is then less than $P \left[ \left( \frac{|C_I|}{n} > p_a + \epsilon \right) \wedge \left( \frac{|C_T|}{n} \leq p_a \right) \right]$ which itself is exponentially small in $n$. For each particular string $c_1 \ldots c_{2n}$ corresponding to a measurement of all qubits in some admissible basis we can apply Hoeffding’s sampling (Theorem B.1). Let $\bar{X} = \frac{|C_I|}{T}$ be the average of the sample corresponding to erroneous information bits; let $\mu = \frac{|\hat{C}_I|+|\hat{C}_T|}{2n}$ be the expectancy of the portion of erroneous bits out of the full population. $\frac{|\hat{C}_T|}{n} \leq p_a$ is equivalent to $2\mu - \bar{X} \leq p_a$, or equivalently,
4.4. CONCLUSION

to $X - \mu \geq \mu - p_a$. For the population $c_1, \ldots, c_{2n}$ the conditions $\left(\frac{|C_I|}{n} > p_a + \epsilon\right)$ and $\left(\frac{|C_T|}{n} \leq p_a\right)$ then rewrite to

$$\left(\bar{X} - \mu > \epsilon + p_a - \mu\right) \land \left(\bar{X} - \mu \geq \mu - p_a\right)$$
(4.44)

which implies $2(\bar{X} - \mu) > \epsilon$ and using Hoeffding’s theorem

$$P \left[\left(\frac{|C_I|}{n} > p_a + \epsilon\right) \land \left(\frac{|C_T|}{n} \leq p_a\right)\right] \leq P \left[\bar{X} - \mu > \frac{\epsilon}{2}\right] \leq e^{-\frac{1}{2}n\epsilon^2}.$$

The above discussion gives the following

**Theorem 4.9** Let us be given $\delta > 0$, $R > 0$ and, for infinitely many values of $n$, a family $\{v_1^n, \ldots, v_{r+mn}^n\}$ of linearly independent vectors in $\mathbb{F}_2^n$ such that $\delta \leq \frac{d_{r+mn}}{n}$ and $\frac{mn}{n} \leq R$. Then for any $p_a > 0$ and $\epsilon_{sec} > 0$ such that $p_a + \epsilon_{sec} \leq \frac{\delta}{2}$, Eve’s accessible information satisfies the following bound

$$\langle I^{(p_a)}_{\text{Eve}} \rangle \leq 2R ne^{-\frac{1}{2}n\epsilon_{sec}^2}. \quad (4.45)$$

All we need to guarantee security is a set of vectors $\{v_1^n, \ldots, v_{r+mn}^n\}$ satisfying the conditions of the theorem. Such families were proven to exist in [10].

4.3.7 Reliability

For the key to be reliable, we need to be sure that the error rate on the information bits is less than the maximal rate that the error correcting code can handle. The maximum number of errors for our code will be fixed to $n(p_a + \epsilon_{rel})$. For the code to be reliable with exponentially small probability of failure, we need

$$P \left[\left(\frac{|C_I|}{n} > p_a + \epsilon_{rel}\right) \land \left(\frac{|C_T|}{n} \leq p_a\right)\right] \leq e^{-\frac{1}{2}n\epsilon_{rel}^2}.$$

For any fixed set of used bits, the test bits and the information bits is a random partition with two subsets of size $n$ and the argument used in the previous section applies here too.

4.4 Conclusion

We presented a direct security analysis, using the method of “Information Vs disturbance” [31, 29, 11, 20, 10], giving explicit bound to the information acquired by Eve, given the error she causes. We optimized the result of [11] for the collective attack by a factor of $2^r2^m$, where $r$ is the amount of error correction bits revealed during the protocol, and $m$ is the obtained key length.
The security proof results with a definite and explicit bound of the information about the key that is accessible to Eve. The same equations achieved in this paper, are also achieved by [10] for the joint attack. This result leads to an asymptotic error-rate threshold of 7.56\%\(^7\), the same asymptotic result obtained for the joint attack in [57, 10]. Finally, we proved that a BB84 protocol, performed under the assumptions taken in this analysis (regarding error correction codes) is feasible, i.e. it is possible to find error-correction codes that fail only with exponentially small probability.

Although our proof is based on the methods presented in [10], the proof is maintained simple and short. This allows using a powerful security analysis methods against the collective attacks, for those theoretical and practical protocols that become too complicated for joint-attack security analysis, for instance [60, 53, 19]. We hope this research opens a path for having better bounds for the more simple case of the collective attack.

\(^7\)We refer the reader to section 5 of [10] for detailed results and further discussion
Chapter 5

Quantum Key Distribution with Classical Bob

5.1 Introduction

Processing information using quantum two-level systems (qubits), instead of classical bits, has lead to many surprising results such as the teleportation of unknown quantum states and quantum algorithms that are exponentially faster than their known classical counterpart. Given a quantum computer, Shor’s factoring algorithm would render completely insecure currently used encryption protocols but, as a countermeasure, quantum information processing has also given us quantum cryptography which was originated by Wiesner [86]. As presented in Section 1.3.3, quantum key distribution was invented by Bennett and Brassard (BB84) [7], to provide a new type of solution to one of the most important cryptographic problems: the transmission of secret messages. A key distributed via quantum cryptography techniques can be secure even against an eavesdropper with unlimited computing power, and its security is unaffected in the future.

In the well-known BB84 protocol as well as in all other suggested protocols, both Alice and Bob perform quantum operations on their qubits (or on their quantum systems). Here we present, protocols in which one party is fully classical. The receiver (Bob) is limited to classical operations on the communicated qubits: measurement in the classical \{0,1\} basis, reflecting the qubit undisturbed, reordering qubits, and resending a qubit, after its measurement, in a state (|0⟩ or |1⟩) determined by the result of the measurement. We term these protocols “QKD protocols with classical Bob”.

The concept of using a classical Bob was firstly published in [18, 19], which introduced a semi-quantum QKD protocol and proved its robustness. Here we present an enhancement of the robustness proof of [19], dealing correctly with the case in which the bits are sent one by another. Another semi-quantum QKD protocol was suggested in [18, 49], based on randomization. This protocol was proven robust as well. This second variant has several disadvantages, for instance, the Hamming weight of the resulting key is fixed (otherwise the
CHAPTER 5. QUANTUM KEY DISTRIBUTION WITH CLASSICAL BOB

Hamming weight can be learnt by Eve, making the protocol only partially robust. Due to the fixed Hamming weight, the entropy of the $n$-bit obtained key is $\approx n - 0.5 \log_2(n) - O(1)$. Here we suggest an improvement to the randomization protocol allowing the key to have a wide range of possible Hamming weights, and an entropy exponentially close to $n$. We prove this new protocol to be completely robust.

This chapter is based on [15].

5.2 Security and Robustness

A conventional measure of security is the information Eve can obtain on the final key, and a security proof usually calculates (or puts bounds on) this information. As presented in Section 1.4, various attacks on QKD have been analyzed, from the special cases such as the intercept-resend attacks and the individual particle attacks, to stronger attacks which use quantum gates and quantum memory and are usually aimed directly against the final key. The strongest (most general) attacks allowed by quantum mechanics are called joint attacks. These attacks are aimed to learn something about the final (secret) key directly, by using a probe through which all qubits pass, and by measuring the probe after all classical information becomes public. Security against all joint attacks is considered as “unconditional security”.

The security of BB84 against all joint attacks was proven in [57, 9, 76, 10, 4] via various techniques. An important step in studying security is a proof of robustness; see for instance [8] for robustness proof of the entanglement-based protocol, and [72, 3] for a proof of robustness against the photon-number-splitting attack. Robustness of a protocol means that any adversarial attempt to learn some information necessarily induces some disturbance. It is a special case (in zero noise) of the more general “information versus disturbance” measure which provides explicit bound on the information available to Eve as a function of the induced error. Robustness also generalizes the no-cloning theorem: while the no-cloning theorem states that a state cannot be cloned, robustness means that any attempt to make an imprint of a state (even an extremely weak imprint) necessarily disturbs the quantum state.

Definition 5.1 A protocol is said to be completely robust if nonzero information acquired by Eve on the INFO string implies nonzero probability that the legitimate participants find errors on the bits tested by the protocol. A protocol is said to be completely nonrobust if Eve can acquire the INFO string without inducing any error on the bits tested by the protocol. A protocol is said to be partly robust if Eve can acquire some limited information on the INFO string without inducing any error on the bits tested by the protocol.

Proving robustness of ideal protocol against any attack is easier than proving security.
5.3. MOCK PROTOCOL AND ITS COMPLETE NONROBUSTNESS

For complicated protocols or practical implementations, it is common that robustness is proved while the security is left as an open question.

It is important to mention that partially robust protocols could still be secure yet completely nonrobust protocols are automatically proven insecure. See also Figure 5.1. As one example, BB84 is fully robust when qubits are used by Alice and Bob but it is only partly robust if photon pulses are used and sometimes two-photon pulses are sent. The well known two-state protocol [6] is not fully robust even if perfect qubits are used, if realistic channel losses are taken into account. Such partly robust protocols can still lead to a secure final key if enough bits are sacrificed for privacy amplification. On the other hand, such partly robust protocols can become completely nonrobust (and therefore totally insecure) if the loss rate is sufficiently high.

![Figure 5.1](image-url) Figure 5.1: (a) Eve’s maximum (over all attacks) information on the INFO string vs. the allowed disturbance on the bits tested by Alice and Bob, in a completely robust (solid line), partly robust (dashed), and completely nonrobust (densely dotted) protocol. (b) Robustness should not be confused with security; Eve’s maximum information on the final key vs. allowed disturbance in a secure protocol; such a protocol could be completely or partly robust.

5.3 Mock Protocol and its Complete Nonrobustness

Consider the following mock protocol: Alice flips a coin to decide whether to send a random bit in the computational basis $\{|0\rangle, |1\rangle\}$ (“Z”), or in the Hadamard basis $\{|+\rangle, |-\rangle\}$ (“X”). Bob flips a coin to decide whether to measure Alice’s qubit in the computational basis (to “sift” it) or to reflect it back (“CTRL”), without causing any modification to the information carrier. In case Alice chose Z and Bob decided to SIFT, i.e. to measure in the Z basis, they share a random bit that we call SIFT or sifted bit (that may, or may not, be confidential). In case Bob chose CTRL, Alice can check if the qubit returned unchanged, by measuring it in the basis she sent it. In case Bob chose to SIFT and Alice chose the
X basis, they discard that bit. The idea that just one basis, the Z-basis, is sufficient for the key generation (while the other basis is used for finding the actions of an adversary) appeared already in [60]. The above iteration is repeated for a predefined number of times. At the end of the quantum part of the protocol Alice and Bob share, with high probability, a considerable amount of sifted bits (also known as the sifted key). In order to make sure that Eve cannot gain much information by measuring (and resending) all qubits in the Z basis, Alice can check whether they have a low-enough level of discrepancy on the X-basis ctrl bits. In order to make sure that their sifted key is reliable, Alice and Bob must sacrifice a random subset of the sifted bits, which we denote as test bits, and remain with a string of bits which we call info bits (info and test are common in QKD, e.g., in BB84 as previously described).

By comparing the value of the test bits, Alice and Bob can estimate the error rate on the info bits. If the error rate on the info bits is sufficiently small, they can then use an appropriate Error Correction Code (ECC) in order to correct the errors. If the error rate on the X-basis ctrl bits is sufficiently small, Alice and Bob can bound Eve’s information, and can then use an appropriate Privacy Amplification (PA) in order to obtain any desired level of privacy.

At first glance, this protocol may look like a nice way to transfer a secret bit from quantum Alice to classical Bob: It is probably resistant to opaque (intercept-resend) attacks. However, it is completely non-robust; Eve could learn all bits of the info string using a trivial attack that induces no error on the bits tested by Alice and Bob (the test and ctrl bits). She would not measure the incoming qubit, but rather perform a cNOT from it into a $|0^E\rangle$ ancilla\(^1\). If Alice chose Z and Bob decides to sift (i.e. measures in the Z-basis), she measures her ancilla and obtains an exact copy of their common bit, thus inducing no error on test bits and learning the info string. If, however, Bob decides on ctrl, i.e. reflects the qubit, Eve would do another cNOT from the returning qubit into her ancilla. This would reset her ancilla, erase the interaction she performed, and induce no error on ctrl bits, thus removing any chance of her being caught. In the following Section we present two protocols which overcome this problem via two different methods.

### 5.4 Two Semi-Quantum Key Distribution Protocols

The following two protocols remedy the above weakness by not letting Eve know which is a sift qubit (that can be safely measured in the computational basis) and which is a ctrl qubit (that should be returned to Alice unchanged). Both protocols are aimed at creating an n-bit info string to be used as the seed for an l-bit shared secret key.

\(^1\)By the term “cNot from A into B” we mean that A is the control qubit and B is the target, as is commonly called; we prefer to use the term “control qubit” in a different meaning in this chapter.
5.4. TWO SEMI-QUANTUM KEY DISTRIBUTION PROTOCOLS

5.4.1 Protocol 1: Based on randomizing the returned qubits

Two versions are presented: Protocol 1 is not quite robust; it depends on a single parameter $\delta > 0$; Protocol 1’, with an additional parameter $\epsilon \leq 1$ such that $0 \leq \epsilon < \delta$ and with Step 7’ replacing Step 7, is completely robust.

Let $n$, the desired length of the info string, be an even integer and let $\delta > 0$ be some fixed parameter.

1. Alice sends $N = \lceil 8n(1 + \delta) \rceil$ qubits. For each of the qubits she randomly selects whether to send it in the computational basis ($Z$) or the Hadamard basis ($X$). In each basis she sends random bits.

2. For each qubit arriving, Bob randomly chooses whether to measure it in the $Z$ basis (to sift it), or to reflect it (ctrl). Bob reorders randomly the reflected qubits so that no one, neither Alice nor Eve, could tell which of them were reflected.

3. Alice collects the reflected qubits in a quantum memory $^2$.

4. Alice publishes which were her $Z$ bits. Bob publishes which were his ctrl qubits, and in which order they were reflected; Alice then measures all the returned ctrl qubits in the basis she prepared them.

It is expected that for approximately $N/4$ bits, Alice used the $Z$ basis and Bob chose to sift (these are the sift bits, which form the sifted key); for approximately $N/4$ bits, Alice used the $Z$ basis and Bob chose ctrl (we refer to these bits as $Z$-ctrl), and for approximately $N/4$ bits, Alice used the $X$ basis and Bob chose ctrl (we refer to these bits as $X$-ctrl). In the rest of the bits, Bob expects a uniform distribution. Cf. Table 5.1.

5. Alice checks the error-rate on the ctrl bits and if either the $X$ error-rate or the $Z$ error-rate is higher than some predefined threshold $P_{\text{ctrl}}$ the protocol aborts.

6. Alice chooses at random $n$ sift bits to be test bits. She publishes which are the chosen bits. Bob publishes the value of these test bits. Alice checks the error-rate on the test bits and if it is higher than some predefined threshold $P_{\text{test}}$ the protocol aborts. Else, let $v$ be the string of the remaining sift bits.

7. Alice and Bob select the first $n$ bits in $v$ to be used as info bits.

Unfortunately, Protocol 1 is not robust: we will show how Eve can count the number of “0”s and “1”s measured by Bob (i.e. the Hamming weight of the measured string) without being detectable and can get about $0.3$ bits of information on the info string, independent of its length (and prove she can not do better).

$^2$Quantum memory is not strictly required, since instead of it (with a certain penalty to the protocol rate) Alice can measure each reflected qubit in a random basis.
CHAPTER 5. QUANTUM KEY DISTRIBUTION WITH CLASSICAL BOB

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>Name</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Z</td>
<td>SIFT</td>
<td>SIFT</td>
<td>A pool for n INFO and n TEST bits</td>
</tr>
<tr>
<td>X</td>
<td>SIFT</td>
<td></td>
<td>Bob could expect a uniform distribution</td>
</tr>
<tr>
<td>Z</td>
<td>CTRL</td>
<td>Z-CTRL</td>
<td>Alice expects her values unchanged</td>
</tr>
<tr>
<td>X</td>
<td>CTRL</td>
<td>X-CTRL</td>
<td>Alice expects her values unchanged</td>
</tr>
</tbody>
</table>

Table 5.1: Bit usage summary

To make sure Eve can not use statistics of occurrence of “0”s and “1”s in the INFO string, Protocol 1’ will fix in advance a subset of \( \{0, 1\}^n \) to be used for the \( n \)-bit INFO strings. A new parameter \( \epsilon \leq 1 \) such that \( 0 \leq \epsilon < \delta \) is introduced and the set of INFO strings is

\[
I_{n,\epsilon} = \left\{ y \in \{0, 1\}^n \text{ s.t. } \left| \frac{|y|}{n} - \frac{1}{2} \right| \leq \frac{\epsilon}{2} \right\}
\]  

\[\text{(5.1)}\]

where \( |y| \) denotes the Hamming weight of \( y \). When \( \epsilon = 0 \), \( I_{n,0} \) is the set of \( n \)-bit strings with Hamming weight \( n/2 \); for \( \epsilon = 1 \) (which can happen if \( \delta > 1 \)), \( I_{n,\epsilon} = \{0, 1\}^n \). We will prove that when \( \epsilon > 0 \), the information carried by a random \( y \in I_{n,\epsilon} \) is exponentially close to \( n \) bits (in the parameter \( n \)). In that case, the set \( I_{n,\epsilon} \) is a “good set” of INFO strings. When \( \epsilon = 0 \), \( I_{n,0} \) has entropy of the order \( n - 0.5 \log_2(n) \) bits.

As for robustness, it is obtained by replacing Step 7 by Step 7’:

\[\text{7’} \quad \text{(a)} \quad \text{Alice chooses a substring } x \text{ of } v \text{ of length } 2h \text{ with } h \text{ zeros and } h \text{ ones, where } h = \left\lfloor (1 + \epsilon)n/2 \right\rfloor; \text{ if she can’t choose such a string, the protocol aborts.} \]

\[\text{(b)} \quad \text{Alice randomly chooses } y \in I_{n,\epsilon} \]

\[\text{(c)} \quad \text{Alice randomly chooses a list of distinct indices } q_1 \ldots q_n \text{ such that } x_{q_1} \ldots x_{q_n} = y. \]

\[\text{(d)} \quad \text{Alice publicly announces } q_1 \ldots q_n; \text{ Bob thus learns that } v_{q_1} \ldots v_{q_n} \text{ is the INFO string.} \]

We will show that the protocol aborts with exponentially small probability and leaks no information to Eve as long as she is undetectable.

5.4.2 Protocol 2: Based on returning all the qubits

Our second (and improved) protocol does not require Bob to randomize all the qubits as in Step 2. Instead, Bob either measures and resends the qubit (SIFTS it) or reflects it (CTRL). Furthermore, Alice does not need to delay the measurement of the returning qubits until Step 4, because immediately in Step 3 she knows in which basis to measure.
The protocol is essentially the same as the previous one, with steps 1 to 7, but with steps 2, 3 and 4 modified to correspond to the new simplified sifting procedure; the modified steps are:

2. For each qubit arriving, Bob randomly chooses whether to measure and resend it in the same state he found (to sift it) or to reflect it (CTRL). Again, no one, neither Alice nor Eve, can tell which of the qubits were reflected.

3. Alice measures each qubit in the basis she sent it.

4. Alice publishes which were her $Z$ bits and Bob publishes which ones he chose to sift.

5.4.3 The classical step

The full protocol for the generation of the final key comprises the above “quantum” protocol, plus the “classical” step:

8. Alice publishes ECC & PA data, from which she and Bob extract the $l$-bit final key from the info string.

5.5 Proofs of Robustness

We first show that Eve cannot obtain information on info bits in Protocol 2 without being detectable. We then bound the information Eve can get with Protocol 1 without inducing errors on test and ctrl bits and finally prove the complete robustness of Protocol 1'.

5.5.1 Complete robustness of Protocol 2

Modeling the protocol

Each time the protocol is executed, Alice sends to Bob a state $|\phi\rangle$ which is a tensor product of $N$ qubits, each of which is either $|+\rangle$, $|−\rangle$, $|0\rangle$ or $|1\rangle$: those qubits are indexed from 1 to $N$. Each of those qubits is either measured by Bob in the standard basis and resent as it was measured or simply reflected. We denote $m$ the set of bit positions measured
by Bob; this is a subset of \([1 \ldots N]\) that we represent by an increasing list of \(r\) integer positions \(m_1 \ldots m_r\) corresponding to Bob measuring the \(r\) qubits with index \(m_1, \ldots, m_r\).

For \(i \in \{0,1\}^N\), we denote
\[
i_m = i_{m_1}i_{m_2} \cdots i_{m_r},
\]
the substring of \(i\) of length \(r\) selected by the positions in \(m\); of course \(|i_m\rangle = |i_{m_1}i_{m_2} \cdots i_{m_r}\rangle\).

In the protocol, it is assumed that Bob has no quantum register; he measures the qubits as they come in. The physics would however be exactly the same if Bob used a quantum register of \(r\) qubits initialized in state \(|0^B\rangle = |0^r\rangle\) (\(r\) qubits equal to 0), applied the unitary transform defined by
\[
M_m|i\rangle|0^B\rangle = |i\rangle|i_m\rangle
\]
for \(i \in \{0,1\}^N\), sent back \(|i\rangle\) to Alice and postponed his measurement to be performed on that quantum register \(|i_m\rangle\); the qubits indexed by \(m\) in \(|i\rangle\) are thus automatically both measured and resent, and those not in \(m\) simply reflected; the \(k\)th qubit sent by Alice is a SIFT bit if \(k \in m\) and is either \(|0\rangle\) or \(|1\rangle\); it is a CTRL bit if \(k \not\in m\). This physically equivalent modified protocol simplifies the analysis and we shall thus model Bob’s measurement and resending, or reflection, with \(M_m\). In most cases, Bob’s measurement will be performed bitwise; for each \(k\) in \(m\) we will denote \(M_k\) the unitary that performs an exclusive or between \(k\)-th qubit in \(i\) and on the corresponding qubit \(j_k\) in Bob’s probe i.e. \(M_k|i_k\rangle|j_k\rangle = |i_k\rangle|j_k \oplus i_k\rangle\). It follows that
\[
M_m = M_{m_r} \ldots M_{m_2}M_{m_1}.
\]

Eve’s attack

The special case where all qubits go from Alice to Bob before coming back, which happens if they are sent in parallel or if Alice and Bob are far enough, was analyzed in [19]. Eve’s most general attack is then comprised of two unitaries: \(U_E\) attacking qubits as they go from Alice to Bob and \(U_F\) as they go back from Bob to Alice, where \(U_E\) and \(U_F\) share a common probe space with initial state \(|0^E\rangle\). The shared probe allows Eve to make the attack on the returning qubits depend on knowledge acquired by \(U_E\) (if Eve does not take advantage of that fact, then the “shared probe” can simply be the composite system comprised of two independent probes). Any attack where Eve would make \(U_F\) depend on a measurement made after applying \(U_E\) can be implemented by a unitaries \(U_E\) and \(U_F\) with controlled gates so as to postpone measurements; since we are giving Eve all the power of quantum mechanics, the difficulty of building such a circuit is of no concern. Eve can use at will a general-purpose quantum computer.

---

\(^3\)If \(|j\rangle_B\) is Bob’s register with \(j \in \{0,1\}^r\), then \(M_m|i\rangle|j\rangle_B = |i\rangle|i_m \oplus j\rangle_B\) where \(\oplus\) denotes a bitwise exclusive or.
The following (more general attack) is possible if Alice and Bob are close enough and Bob is expecting qubits in a sequence. Since Eve has access to a quantum memory, she can wait till she gets all qubits $|\phi\rangle$ sent by Alice before proceeding. Once she got them all, the most general attack she can perform applies a unitary transform to $|0^E\rangle|\phi\rangle$, sends the first qubit to Bob, waits till it comes back from Bob to then repeat the same procedure (with a possibly different unitary each time) for each qubit in a sequence. When Eve has attacked all qubits forth and back, she sends them back to Alice (one by one if needed).

More formally let $\mathcal{H}_P = \bigotimes_{k=1}^N \mathcal{H}_k$ be the space of the protocol, where each $\mathcal{H}_k$ is the two dimensional Hilbert space corresponding to the $k$-th qubit and let $\mathcal{H}_E$ be Eve’s probe space; once Eve holds $|\phi\rangle$ she applies a unitary $U_1$ on $|0^E\rangle|\phi\rangle$ and sends Bob qubit 1 (corresponding to $\mathcal{H}_1$). For each qubit $k$ from 1 to $N-1$, when Eve receives qubit $k$ back from Bob, she applies $U_{k+1}$ on $\mathcal{H}_E \otimes \mathcal{H}_P$ and then sends qubit $k+1$ to Bob. When Eve receives qubit $N$ from Bob, she applies $U_{N+1}$ on $\mathcal{H}_E \otimes \mathcal{H}_P$, sends the $N$ qubits to Alice and keeps her probe. Eve’s attack is thus characterized by a sequence $\{U_k\}_{1 \leq k \leq N+1}$ of unitary transforms on $\mathcal{H}_E \otimes \mathcal{H}_P$.

The attack in [19] where Eve applies $U_E$ to all qubits, sends them to Bob, and applies $U_F$ on their way back corresponds to the attack where $U_1 = U_E$, $U_2 = \ldots = U_N = I$ and $U_{N+1} = U_F$ i.e. Eve uses $U_E$ on all qubits when she receives them, does nothing till she got all qubits back and then applies $U_F$.

Another protocol, whose robustness can be proved with the methods of [19] and which is rapidly mentioned in its conclusion requires each qubit to be sent individually, Alice sending each qubit only when she received the previous one from Bob. Eve also uses a global probe initialized to $|0^E\rangle$ but she if forced to attack qubits individually. For each qubit $k$ from 1 to $N$, Eve applies a unitary $U_E^{(k)}$ acting on $\mathcal{H}_E$ and $\mathcal{H}_k$ before sending it to Bob and applies a unitary $U_F^{(k)}$ acting on the same spaces on the way back\footnote{The transforms $U_E^{(k)}$ and $U_F^{(k)}$ act on $\mathcal{H}_E \otimes \ldots \otimes \mathcal{H}_k \otimes \ldots$ and leave $\mathcal{H}_i$ fixed for $i \neq k$.}. The robustness of the individual-qubit protocol follows immediately from the robustness of Protocol 2 under the limited class of attacks where $U_1 = U_E^{(1)}$, $U_k = U_E^{(k)}U_F^{(k-1)}$ for $1 \leq k < N$ and $U_{N+1} = U_F^{(N)}$ (and qubits are returned all together to Alice).

The final global state

Delaying all measurements allows considering the global state of the Eve+Alice+Bob system before all actual measurements; Eve’s and Bob’s actions are described by unitary transforms. The initial state is $|0^E\rangle|\phi\rangle|0^B\rangle$; Eve’s unitary transforms $U_1$, $\ldots$, $U_{N+1}$ act on the first two Hilbert spaces whilst Bob’s measurements $M_k$ performed when he receives qubit $k$ with $k \in m$ act on the last two spaces. For instance, if $N = 4$ and $m = 13$, then the final global state of the system is $U_2U_4M_3U_3U_2M_4U_4|0^E\rangle|i\rangle|0^B\rangle$ where measurement
$M_1$ on qubit 1 occurs immediately after Eve applies $U_1$ and measurement $M_3$ on qubit 3 occurs immediately after Eve applies $U_3$.

The attacks $\{U_k\}_{1 \leq k \leq N+1}$ we are interested in are only those for which Eve is completely undetectable. Such attacks put strong restrictions on the global evolution of the system. In what follows, when we say that an attack induces no error on $\text{ctrl}$ and $\text{test}$, we mean that for any choice of $\text{ctrl}$ and $\text{test}$ bits whose probability of occurrence according to Protocol 2 is not 0, the probability that Eve’s attack induces an error on them is 0.

**Proposition 5.2** If the attack $\{U_k\}_{1 \leq k \leq N+1}$ induces no error on $\text{test}$ and $\text{ctrl}$ bits, and if Alice sent state $|i\rangle$ with $i \in \{0,1\}^N$, then there is a state $|F_i\rangle \in \mathcal{H}_E$ such that, for all $m$, the final global state of the system after applying $U_{N+1}$ is

$$|F_i\rangle|i\rangle|i_m\rangle \quad (5.4)$$

**Proof** The final global state of the system can always be written as $\sum_{j,j'}|E_{ijj'}\rangle|j\rangle|j'\rangle$ where $|j\rangle$ is the standard basis of $\mathcal{H}_P$ and $|j'\rangle$ of Bob’s probe space; If the protocol induces no errors on $\text{test}$ bits, it must be so that for all $m$, $|E_{ijj'}\rangle = 0$ for $j' \neq i_m$ and thus the final global state must be $\sum_j|E_{ij(i_m)}\rangle|j\rangle|i_m\rangle$. Moreover, if there is no error on $\text{ctrl}$ bits, then the probability for Alice to measure any $|j\rangle$ that is not $|i\rangle$ must be zero. She can indeed choose any qubit not in $m$ as a $Z-\text{ctrl}$ bit; she also checks all the qubits measured by Bob, which must also coincide with those she sent since $i \in \{0,1\}^N$. Consequently $|E_{ij(i_m)}\rangle = 0$ if $j \neq i$ and the final state must be $|E_{ii(i_m)}\rangle|i\rangle|i_m\rangle$.

We now prove that $|E_{ii(i_m)}\rangle$ does not depend on $i_m$. Let $Z$ be the linear map defined by $Z|e\rangle|j\rangle|j'\rangle = |e\rangle|j\rangle|0^B\rangle$ i.e. $Z$ is the linear map on Bob’s probe space that maps its standard basis states on the state $|0^B\rangle$. It is clear that $ZU_k = U_kZ$ and $ZM_k = Z$ for all $k$. If we look at the particular case where $N = 4$ and $m = 13$, i.e. Bob measures qubits 1 and 3, this implies that

$$ZU_5U_4M_3U_3U_2M_1U_1|0^E\rangle|i\rangle|0^B\rangle = U_5U_4U_3U_2U_1Z|0^E\rangle|i\rangle|0^B\rangle$$

$$= U_5U_4U_3U_2U_1|0^E\rangle|i\rangle|0^B\rangle. \quad (5.5)$$

Applying $Z$ to the final state just gives the final state obtained if $m$ is empty. If we apply $Z$ to $|E_{ii(i_m)}\rangle|i\rangle|i_m\rangle$ we get $|E_{ii(i_m)}\rangle|i\rangle|0^B\rangle$ and this state must be equal to the final global state when $m$ is empty. This implies that for all values of $m$, the states $|E_{ii(i_m)}\rangle$ must be the same; we call them $|F_i\rangle$ and this gives $|F_i\rangle|i\rangle|i_m\rangle$ as the final global state.

We now show that if Eve’s attack is undetectable by Alice and Bob, then Eve’s final state $|F_i\rangle$ is independent of the string $i \in \{0,1\}^N$. More precisely...
5.5. PROOFS OF ROBUSTNESS

Proposition 5.3 If \( \{U_k\}_{1 \leq k \leq N+1} \) is an attack on Protocol 2 that induces no error on TEST and CTRL bits, then for all \( i, i' \in \{0, 1\}^N \)
\[
i, i' \in \{0, 1\}^N \implies |F_i⟩ = |F′_{i'}⟩
\]

Proof For any index \( k \), let Alice’s \( k \)-th qubit be in state \( |+⟩ \), and all the other qubits be prepared in the Z-basis. Alice’s state can be written \( \frac{1}{\sqrt{2}}[|i⟩ + |i'⟩] \) where \( i, i' \in \{0, 1\}^N \), \( i_k = 0, i'_k = 1 \), and \( i_t = i'_t \) for \( t \neq k \). Let Bob choose \( m \) s.t. \( k \neq m \); such an \( m \) exists because \( N \geq 2 \) and then \( i_m = i'_m \). By the previous proposition and linearity, the final global state is \( \frac{1}{\sqrt{2}}[|F_i⟩|i⟩ + |F′_{i'}⟩|i'⟩]|i_m⟩ \); since we are interested only in Alice’s \( k \)-th qubit, we trace-out all the other qubits in Alice and Bob’s hands and get the state
\[
\frac{1}{\sqrt{2}}[|F_i⟩|0⟩ + |F′_{i'}⟩|1⟩];
\]
if \( |0⟩ \) and \( |1⟩ \) are replaced by their values in term of \( |+⟩ \) and \( |−⟩ \), this rewrites \( \frac{1}{2}[|F_i⟩ + |F′_{i'}⟩]|+⟩ + \frac{1}{2}[|F_i⟩ − |F′_{i'}⟩]|−⟩ \) and since the probability that Alice measures \( |−⟩ \) must be 0, \( \frac{1}{2}[|F_i⟩ − |F′_{i'}⟩] = 0 \) i.e. \( |F_i⟩ = |F′_{i'}⟩ \). The above holds for any \( l \); any bit in \( i \) can be flipped without affecting \( |F_i⟩ \) and thus \( |F_i⟩ \) is the same for all \( i \in \{0, 1\}^N \).

Theorem 5.4 For any attack \( \{U_k\}_{1 \leq k \leq N+1} \) on Protocol 2 that induces no error on TEST and CTRL bits, Eve’s final state is independent of the state \( |φ⟩ \) sent by Alice, and Eve has thus no information on the INFO string.

Proof By Proposition 5.3, there is a state \( F_{\text{final}} \) of Eve’s probe space s.t. for all \( i \in \{0, 1\}^N \), Eve’s final state \( |F_i⟩ = |F_{\text{final}}⟩ \). By Proposition 5.2, for all \( i \in \{0, 1\}^N \) and all \( m \), the final state after applying \( U_{N+1} \) if Alice sends \( |i⟩ \) is thus \( |F_{\text{final}}⟩|i⟩|i_m⟩ \). For all superpositions \( |φ⟩ = \sum_i c_i|i⟩ \) that Alice may send, and all \( m \), the final state of the Eve+Alice+Bob system after applying \( U_{N+1} \) is consequently
\[
|F_{\text{final}}⟩ \sum_i c_i|i⟩|i_m⟩;
\]

Eve’s probe state \( |F_{\text{final}}⟩ \) is independent of \( i_m \) and therefore of the SIFT bits and INFO bits — if Eve is to be undetectable.

The above theorem means that Protocol 2 is completely robust.

5.5.2 Partial robustness of Protocol 1

Modeling the protocol

The states \( |φ⟩ \) sent by Alice are still products of \( N \) qubits each of which is either \( |+⟩, |−⟩ \), \( |0⟩ \) or \( |1⟩ \). In Step 2 of the protocol, Bob either measures a qubit, or reflects it; moreover,
he reorders randomly the reflected qubits; let \( r \) be the number of reflected qubits and let \( s = s_1 s_2 \ldots s_r \) be the list of those \( r \) randomly ordered bit positions. For instance, if \( r = 4 \), and Bob reflects qubits 8, 1, 5 and 4 in that order then \( s = 8154 \) (examples will use positions from 1 to 9 to avoid comma separated lists). The list of non-reflected bits is indexed by the complement \( \bar{s} \) and will always be listed in ascending order; if \( N = 9 \) and \( s = 8154 \) then \( \bar{s} = 23679 \). Bob’s measurement can still be postponed, but this time, since Bob keeps the qubits selected by \( \bar{s} \) without sending a copy, there is no need to copy. For all string \( s \) we still denote \( i_s = i_{s_1} \ldots i_{s_r} \) the list of bits selected by \( s \) in the order specified by \( s \); Bob’s operation is then captured by

\[
U'_s|i⟩ = |i_s⟩|\bar{i}_s⟩
\]

(5.9)

where \( |i_s⟩ \) is the state reflected to Alice, and \( |\bar{i}_s⟩ \) the state (to be) measured by Bob. With \( N = 9 \) and \( s = 8154 \), and if Alice sent \( |i_1 \ldots i_9⟩ \) with \( i_1, \ldots, i_9 \in \{0, 1\} \), the state reflected is \( |i_8 i_1 i_5 i_4⟩ \) and the state to be measured \( |i_2 i_3 i_6 i_7 i_9⟩ \). Of course, Alice can compare \( i_s \) with what she actually sent only when \( s \) is known and consequently keeps \( |i_s⟩ \) in quantum memory. With these notations, qubit \( k \) is CTRL if \( k \in s \) and it is SIFT if it is either \( |0⟩ \) or \( |1⟩ \) and \( k \notin s \).

**Eve’s attack**

Eve’s most general attack is still comprised of two unitaries: \( U_E \) and \( U_F \) sharing a common probe space; \( U_E \) is applied on \( |0^E⟩ \) and \( |φ⟩ \) and attacks qubits as they go from Alice to Bob; \( U_F \) is applied on Eve’s probe and \( |i_s⟩ \) as those bits go back from Bob to Alice; one slightly annoying problem is that the dimension of the space on which \( U_F \) acts is not fixed; it depends on the size of \( s \), i.e. the number of bits reflected by Bob; there is thus one unitary \( U_F \) for each \( r > 0 \).

**The global final state**

Since Bob uses no probe space, the global state after Eve applies \( U_E \) is simply \( U_E |0^E⟩|φ⟩ \); then Bob applies \( U'_s \) to his part of the system, which corresponds to the global unitary \( I_E \otimes U'_s \) where \( I_E \) is the identity on Eve’s probe space. Then \( U_F \) is applied only on Eve’s probe and \( |i_s⟩ \); if we denote \( I_\bar{s} \) the identity on the system left in Bob’s hands, given by the qubits selected by \( \bar{s} \), the final global state is then

\[
[U_F \otimes I_\bar{s}] [I_E \otimes U'_s |U_E |0^E⟩|φ⟩].
\]

(5.10)

**Proposition 5.5** If \( (U_E, U_F) \) is an attack on Protocol 1 such that \( U_E \) induces no error on test bits then there are states \( |E_i⟩ \) in Eve’s probe space such that for all \( i \in \{0, 1\}^N \)

\[
U_E |0^E⟩|i⟩ = |E_i⟩|i⟩.
\]

(5.11)
5.5. PROOFS OF ROBUSTNESS

If moreover $U_F$ induces no error on CTRL bits, then there are states $|F_{s,i}\rangle$ of Eve’s probe space such that for all $i \in \{0,1\}^N$, and all sequence $s$ of distinct elements of $[1,\ldots,N]$,

$$U_F|E_i\rangle|i_s\rangle = |F_{s,i}\rangle|i_s\rangle. \tag{5.12}$$

**Proof** $U_E|0^E\rangle|i\rangle$ can be expanded as $\sum_j |E_{ij}\rangle|j\rangle$ and since for any $k$ there must be a $0$ probability of getting $j_k$ different from $i_k$ (there is a non zero probability that Bob chooses bit $k$ as a test bit), $|E_{ij}\rangle = 0$ for $j \neq i$ and thus Equation (5.11) holds with $|E_i\rangle = |E_{ii}\rangle$.

In Step 4, Bob publishes the bit positions $s$ and, for Eve’s attack to be unnoticeable by Alice, the state held by Alice after $U_F$ is applied to $|E_i\rangle|i_s\rangle$ needs to be equal to $|i_s\rangle$.

By Hilbert-Schmidt, this implies that the bipartite state $U_F|E_i\rangle|i_s\rangle$ must be of the form $|F\rangle|i_s\rangle$. The pure state $|F\rangle$ depends here on $i$, both through $|E_i\rangle$ and $i_s$, and also on the string $s$ chosen to select the reflected qubits, i.e. $|F\rangle$ is a function $i$ and $s$ and will be written $|F_{s,i}\rangle$, giving Equation (5.12).

When the attack $(U_E, U_F)$ induces no error on TEST and CTRL bits then, using Equations (5.10), (5.11) and (5.12),

$$[U_F \otimes I_B][I_E \otimes U'_E]U_E|0^E\rangle|i\rangle = |F_{s,i}\rangle|i_s\rangle|i_z\rangle. \tag{5.13}$$

One can no longer expect Eve’s final state $|F_{s,i}\rangle$ after Alice sent state $|i\rangle$ and Bob reflected the qubits specified by $s$ to be constant, as is shown in the following example:

**Example 5.6** Let Eve’s probe space be of dimension $N + 1$ with basis states $|0\rangle, \ldots, |N\rangle$.

Eve’s initial state is $|0\rangle$. Let $U_E|0\rangle|i\rangle = ||i||i\rangle$ and $U_F|h\rangle|j\rangle = |h - |j||j\rangle$. This means that $U_E$ puts in the probe the Hamming weight $h = |i|$ of the string $i \in \{0,1\}^N$ if Alice sends state $|i\rangle$, and $U_F$ subtracts from the probe the Hamming weight of the string $|j\rangle$ returned by Bob. In particular $|F_{s,i}\rangle = ||i - |s|| = ||i_z||$. For $U_F$ to be defined on all basis states assume the difference is modulo $N + 1$. Bob can clearly detect no error on TEST bits. Moreover, if Alice sends $|\phi\rangle = \sum_i c_i|i\rangle$, the final state is $\sum_i c_i ||i_z|||i_z\rangle|i_z\rangle$ and, once Bob has measured $|i_z\rangle$, Eve’s probe $||i_z||$ factors out and the resulting state in Alice’s hands is the same as if Eve had applied neither $U_E$ nor $U_F$, i.e. the final state had been $\sum_i c_i|0||i_z\rangle|i_z\rangle$; no error can thus be detected on CTRL bits.

Example 5.6 shows that Eve can learn the Hamming weight $|i_z|$ of the string measured by Bob and stay completely invisible to Alice and Bob, i.e. induce no error on TEST and CTRL bits. Therefore, in order to make Protocol 1 robust, the choice of the INFO bits must be done in a more careful way.

But first, we need to show that Eve can learn at most the Hamming weight of $i_z$; this is a consequence of Equation (5.18) below, which is derived from a sequence of lemmas. The first lemma states that all the bits in $i$ whose index are in $s$ can be flipped without
changing \( |F_{s,i}⟩ \); in Protocol 2, this was true for all qubits in \( i \), but then, all the qubits were returned. In Protocol 1, only the qubits in \( s \) are returned to Alice; the following lemma shows that for a fixed \( s \), Eve’s state depends only on the bits kept by Bob.

**Lemma 5.7** For any attack \((U_E, U_F)\) on Protocol 1 that induces no error on test and ctrl bits, if \( |E_i⟩ \) and \( |F_{s,i}⟩ \) are given by Equations (5.11) and (5.12) then

\[
i_s = i'_s \implies |F_{s,i}⟩ = |F_{s,i'}⟩
\]  

**(Proof)** The result is trivial if \( s \) is empty. If not, we follow the steps of the proof of Proposition 5.3 and prove this bitwise; let \( k \) be an index in \( s \), and \( i \) and \( i' \) be such that \( i_k = 0 \) and \( i'_k = 1 \), all other bits being the same. Assume w.l.g that \( k \) is the first element of \( s \) i.e. \( s = ks' \) and thus \( i_s = i_k i_{s'} \). If Alice sends the state \( \frac{1}{\sqrt{2}} \{ |i⟩ + |i'⟩ \} \) i.e. the \( k \)th qubit sent by Alice is \( |+⟩ \) and all the other qubits are prepared in the \( Z \)-basis, with bit values according to \( i \), then by linearity and Equation (5.13) the final state of the Eve+Alice+Bob system is \( \frac{1}{\sqrt{2}} \{ |F_{s,i}⟩|0⟩ + |F_{s,i'}⟩|1⟩ \} |i_s⟩|i_{s'}⟩ \); if we trace out all the qubits in \( s' \) and \( s \) to keep only Eve’s probe and qubit \( k \) in Alice’s hands, we get the state

\[
\frac{1}{\sqrt{2}} \{ |F_{s,i}⟩|0⟩ + |F_{s,i'}⟩|1⟩ \};
\]  

writing \( |0⟩ \) and \( |1⟩ \) in terms of \( |+⟩ \) and \( |−⟩ \) and considering only those terms in the resulting state that contain \( |−⟩ \) gives \( \frac{1}{2} \{ |F_{s,i}⟩ − |F_{s,i'}⟩ \} |−⟩ \); and since the probability that Alice measures \( |−⟩ \) as the \( k \)th qubit must be 0 (because \( k \in s \)), \( |F_{s,i}⟩ − |F_{s,i'}⟩ = 0 \) i.e. \( |F_{s,i}⟩ = |F_{s,i'}⟩ \).

The following lemma simply expresses the fact that, when Alice sends \( |i⟩ \) and Bob reflects the qubits with indices in \( s \) then Eve’s final state depends only on \( |i⟩ \) and the state reflected by Bob.

**Lemma 5.8** For any attack \((U_E, U_F)\) on Protocol 1 that induces no error on test and ctrl bits, if \( |E_i⟩ \) and \( |F_{s,i}⟩ \) are given by Equations (5.11) and (5.12) then for all \( i \), \( s \) and \( s' \),

\[
i_s = i_{s'} \implies |F_{s,i}⟩ = |F_{s',i}⟩
\]  

**(Proof)** If \( i_s = i_{s'} \) then \( U_E|E_i⟩|i_s⟩ = U_F|E_i⟩|i_{s'}⟩ \) and thus \( |F_{s,i}⟩|i_s⟩ = |F_{s',i}⟩|i_{s'}⟩ \).

When Equation (5.16) is used, we are using the fact that when Eve sees a qubit \( |0⟩ \) (resp. a qubit \( |1⟩ \)) coming back from Bob, then she cannot tell to what qubit \( |0⟩ \) (resp. \( |1⟩ \)) sent by Alice this qubit corresponds provided of course more than one \( |0⟩ \) (resp. \( |1⟩ \)) had been sent by Alice. The preceding lemmas can be used to show that, if Eve induces no error on test and ctrl bits, then Eve’s intermediate state \( |E_i⟩ \) just after \( U_E \) is applied stays invariant when the bits in \( i \) are permuted; let us first look at an example.
5.5. PROOFS OF ROBUSTNESS

Example 5.9 Let \( N = 4 \) and \( r = 2 \) and let us see that \( |E_{1011}| = |E_{0111}| \) i.e. Eve’s state after the attack \( U_F \) on the qubits from Alice to Bob is the same whether Alice sends state \( |1011\rangle \) or \( |0111\rangle \). By Equation (5.14), \( |F_{14,1011}| = |F_{14,0011}| \) which is Eve’s final state when Bob reflects bits 1 and 4 and Alice sends either \( |1011\rangle \) or \( |0111\rangle \). Similarly \( |F_{24,0111}| = |F_{24,0011}| \). We now use Equation (5.16) to get \( |F_{14,0011}| = |F_{24,0011}| \) (Eve cannot tell if the returning \( |0\rangle \) is bit 1 or bit 2); those identities imply \( |F_{14,1011}| = |F_{24,0111}| \). We now go back to the definition of \( F \); \( |F_{14,1011}| \) is Eve’s final state if Alice sent \( |1011\rangle \) and Bob reflected the bits 1 and 4 and from Equation (5.12) we get \( U_F|E_{1011}\rangle|11\rangle = |F_{14,1011}\rangle|11\rangle \) (bits 14 being 11). Similarly \( U_F|E_{0111}\rangle|11\rangle = |F_{24,0111}\rangle|11\rangle \) and since the r.h.s. members are equal and \( U_F \) is unitary, \( |E_{0111}| = |E_{1011}| \).

Following the lines of Example 5.9, we prove the following lemma.

Lemma 5.10 For any attack \((U_E, U_F)\) on Protocol 1 that induces no error on CTRL and TEST bits, if \( |E_i\rangle \) and \( |F_{s,i}\rangle \) are given by Equations (5.11) and (5.12) then for all \( i, i' \in \{0, 1\}^N \)

\[
|i| = |i'| \implies |E_i\rangle = |E_{i'}\rangle \tag{5.17}
\]

Proof Equation (5.17) means that \( |E_i\rangle \) depends only on the number of “0”s and “1”s in \( i \), not on their positions. We need only show that any two (distinct) bits in \( i \) can be swapped without affecting \( |E_i\rangle \) and, wlg, \( |E_{0110}\rangle = |E_{1001}\rangle \) for any \( i'' \in \{0, 1\}^{N-25} \). Let \( s' \) be any sequence of distinct elements of \([3..N] \); \( |F_{s',i,1001}\rangle = |F_{s',0001}\rangle \) and \( |F_{s',0110}\rangle = |F_{s',0010}\rangle \) by Equation (5.14); also \( |F_{s',0001}\rangle = |F_{s',0110}\rangle \) by Equation (5.16) and thus \( |F_{s',1001}\rangle = |F_{s',1010}\rangle \). Using Equation (5.12),

\[
U_F|E_{1001}\rangle|1i_{s'}\rangle = |F_{s',1001}\rangle|1i_{s'}\rangle \quad (i = 10i''; s = 1s')
\]

\[
U_F|E_{0110}\rangle|1i_{s'}\rangle = |F_{s',0110}\rangle|1i_{s'}\rangle \quad (i = 01i''; s = 2s')
\]

and, since \( i_{s'} \) is the same for \( i = 01i'' \) and \( i = 10i'' \) and \( |F_{s',1001}\rangle = |F_{s',0110}\rangle \) the r.h.s. are equal and so \( |E_{1001}\rangle = |E_{0110}\rangle \).

Example 5.11 Lemma 5.7 allows replacing all bits indexed by \( s \) by 0 without changing \( |F_{s,i}\rangle \). This means for example that if \( i = 1010 \) and \( s = 34 \), then \( |F_{s,i}\rangle = |F_{34,1010}\rangle = |F_{34,1000}\rangle \); similarly if \( i' = 0101 \) and \( s' = 12 \), then \( |F_{s',i'}\rangle = |F_{12,0101}\rangle = |F_{12,0001}\rangle \). This means that \( |F_{s,i}\rangle \) depends only on the bits not indexed by \( s \), i.e. the bits indexed by \( \bar{s} \). Here \( i_1 = 10 \) and \( i_{s'} = 01 \); those two strings have the same Hamming weight. Let us see that they give the same final state for Eve. By Equation (5.12) \( U_F|E_{0001}\rangle|00\rangle = |F_{12,0001}\rangle|00\rangle \) (Bob reflects bits 12) and \( U_F|E_{1000}\rangle|00\rangle = |F_{34,1000}\rangle|00\rangle \) (Bob reflects bits 34). We know from Lemma 5.10 that \( |E_{0001}\rangle = |E_{1000}\rangle \); this implies \( |F_{12,0001}\rangle = |F_{34,1000}\rangle \) and thus \( |F_{s,i}\rangle = |F_{s',i'}\rangle \).

\(^5\)If \( n \geq 1 \) then \( N = [8n(1 + \delta)] \geq 8 \) and \( N - 2 \geq 1 \).
Example 5.11 provides the intuition behind the proof of the next proposition that is for Protocol 1 what Proposition 5.3 is for Protocol 2.

**Proposition 5.12** If \((U_E, U_F)\) is an attack on Protocol 1 that induces no error on TEST and CTRL bits, and if \(|E_t\rangle\) and \(|F_{s,i}\rangle\) are given by Equations (5.11) and (5.12) then for all \(s\) and \(s'\) of the same length \(r \geq 0\), and all \(i, i' \in \{0, 1\}^N\),

\[
|i_s\rangle = |i'_{s'}\rangle \implies |F_{s,i}\rangle = |F_{s',i'}\rangle
\]  
(5.18)

**Proof** Let \(j\) and \(j'\) be defined by \(j_s = j'_{s'} = 0^r\), \(j_s = i_s\) and \(j'_{s'} = i'_{s'}\). Then \(|F_{s,i}\rangle = |F_{s,j}\rangle\) and \(|F_{s',i'}\rangle = |F_{s',j'}\rangle\) by Equation (5.14). Since \(|j'\rangle = |j\rangle\), \(|E_j\rangle = |E_j\rangle\) by Equation (5.17); by Equation (5.12), \(U_F|E_j\rangle|j_s\rangle = |F_{s,j}\rangle|j_s\rangle\) and \(U_F|E_j\rangle|j'_{s'}\rangle = |F_{s',j'}\rangle|j'_{s'}\rangle\) and thus, since \(|j_s\rangle = |j'_{s'}\rangle = 0^r\), \(|F_{s,j}\rangle = |F_{s',j'}\rangle\).

Equation (5.18) can be rewritten \(|F_{s,i}\rangle = |F_{i|s}\rangle\) representing Eve’s final state when the Hamming weight of the string measured by Bob is \(|i_s\rangle\).

**Theorem 5.13** With any attack on Protocol 1 that induces no error on TEST and CTRL bits, the eavesdropper can learn at most the number of “0”s and “1”s measured by Bob and Eve’s final state can be written \(|F_{i|s}\rangle\).

**Proof** Let \((U_E, U_F)\) be an arbitrary attack that induces no error on TEST and CTRL bits. If Alice sent any superposition \(|\phi\rangle = \sum_{i \in \{0, 1\}^N} c_i |i\rangle\) and Bob returned the bits selected by \(s\), then using linearity and Equation (5.13) with \(|F_{s,i}\rangle = |F_{i|s}\rangle\) for all \(i\) gives

\[
\sum_i c_i |F_{i|s}\rangle |i_s\rangle |i_s\rangle
\]  
(5.19)

as the state describing the final Eve+Alice+Bob system. Once Bob measures \(|i_s\rangle\) the state is projected onto a state where \(|F_{i|s}\rangle\) factors out and Eve is thus left with a state that depends only on the Hamming weight \(|i_s\rangle\) of the string measured by Bob and thus can learn at most that Hamming weight. Since she knows the length of \(s\), this means she can learn at most the number of “0”s and “1”s measured by Bob.

**Information leaked by Protocol 1**

As shown in Example 5.6, Eve can indeed learn the Hamming weight of the string measured by Bob. This is why the mock protocol of Section 5.3 failed. There was only one SIFT bit and no permutation could ever hide its value.

From Equation (5.19) one also sees that the probability of Bob measuring \(i_s\) is unaffected by Eve’s attack, just because the norm of \(|F_{i|s}\rangle\) is 1 (this is a normalized state); Eve’s attack has no effect at all on Bob’s statistics. The SIFT bits are equal to the random
5.5. PROOFS OF ROBUSTNESS

Z-bits chosen by Alice; the X bits measured by Bob are also random bits, as they would be without Eve’s attack.

From the string of \( N - r \) bits (whose indices are in \( \bar{s} \)) measured by Bob, about half the bits are discarded because Alice sent the corresponding qubit in the X-basis. The bits left are the sift bits; \( n \) of them are used as test bits, the others serve as a pool selecting the info bits. Eve’s knowledge of \( |i_s| \) provides indirect knowledge on the statistics of occurrence of “0”s and “1”s in the info bits and the protocol would nevertheless not be robust if the info string was obtained by picking randomly \( n \) bits from the sift bits not used as test bits (or the first \( n \) ones available as in Protocol 2). We now give an asymptotic bound on Eve’s accessible information.

**Theorem 5.14** For any attack on Protocol 1 that induces no error on test and ctrl bits, Eve’s information on the info string is asymptotically less than \( 0.293 + O(n^{-1}) \) bits.

**Proof** Let \( N - r = kn \) be the number of bits measured by Bob; it is expected that \( k = 4(1 + \delta) \); those bits are all random but Eve knows their Hamming weight. Also known are the indices of the sift bits, of the info bits, as well as the indices and values of the test bits. Eve thus knows the Hamming weight \( W \) of the \( kn - n \) remaining random bits that are not test; \( W \) is distributed binomially, with \( kn - n \) trials and probability \( 1/2 \) of success. The entropy of a binomial distribution with \( n \) trials and probability \( p \) of success is \( 1/2 \log_2(2\pi e p(1-p)n) + O(1/n) \) where \( O(1/n) \) is the error \(^6\); the entropy \( H(W) \) is thus

\[
H(W) = \frac{1}{2} \log_2 \left( \frac{1}{2} \pi e (k - 1)n \right) + O \left( \frac{1}{n} \right). \tag{5.20}
\]

For any particular \( n \)-bit info string \( x \), the entropy of \( W \) given \( x \) is the entropy of the a binomial distribution with \( kn - 2n \) trials (for the \( kn - 2n \) remaining random bits) and is thus

\[
H(W | x) = \frac{1}{2} \log_2 \left( \frac{1}{2} \pi e (k - 2)n \right) + O \left( \frac{1}{n} \right). \tag{5.21}
\]

The bits of the info string are random bits chosen by Alice and the strings \( x \) are thus equally likely; this implies \( H(W | X) = H(W | x) \). The information Eve gains on \( X \) when \( W \) is known is \( H(X) - H(X | W) \). It is a basic fact from information theory that \( H(X) - H(X | W) = H(W) - H(W | X) \) and Eve’s information is thus

\[
H(W) - H(W | X) = \frac{1}{2} \log_2 \frac{k - 1}{k - 2} + O \left( \frac{1}{n} \right)
= \frac{1}{2} \log_2 \left( 1 + \frac{1}{k - 2} \right) + O \left( \frac{1}{n} \right), \tag{5.22}
\]

\(^6\)When \( n \) is large, the binomial \( B(n, p) \) is well approximated by a normal with variance \( \sigma^2 = np(1-p) \), whose entropy is \( \log_2(\sqrt{2\pi e}) = \log_2(\sqrt{2\pi e}(1-p)n) \). With a factor of \( \log_2(n) \), this rewrites \( \frac{1}{2} \log n + \frac{1}{2} + \log \sqrt{2\pi(1-p)} \) as in [48] where is proven a result implying the error is of order \( \frac{1}{n} \). A simple computer program shows that for \( p = 0.5 \) and \( n = 20 \) the error is already less than \( 3.4 \times 10^{-1} \).
For \( k \geq 4 \) the leak is less than \( 0.293 + O(n^{-1}) \) bits of information. The probability that \( k < 4 \) is exponentially small; even if Eve then gets full information, the expected number of bits she gets is of order \( 0.293 + O(n^{-1}) \).

5.5.3 Properties of Protocol 1′

The information contained in the info string

Alice randomly chooses \( y \in I_{n,\epsilon} \) to send as the info string. The information contained in \( y \) is thus the entropy of a uniform distribution on \( I_{n,\epsilon} \).

**Proposition 5.15** If \( \epsilon > 0 \), the entropy of the uniform distribution on \( I_{n,\epsilon} \) is exponentially close to \( n \) (its distance to \( n \) is of order \( e^{-\Omega(n)} \)).

**Proof** For any integer \( N > 0 \), the entropy of the uniform distribution on a set of \( N \) elements is \( \log_2(N) \). We are thus looking for a lower bound on \( \log_2(|I_{n,\epsilon}|) \).

Let \( Y = (Y_1, \ldots, Y_n) \) be a uniformly distributed random variable on \( \{0, 1\}^n \); the \( Y_i \) are independent Bernoulli’s with probability \( p = 1/2 \). Let \( \overline{Y} = \sum_{i=1}^n Y_i/n \); the expectancy \( E[\overline{Y}] \) is \( 1/2 \). Note that \( \overline{Y} \) is the Hamming weight of the string \( |Y| \) divided by \( n \) (i.e. normalized). Using this random variable we can bound the probability for a string to be outside the set \( I_{n,\epsilon} \), i.e. the set of strings with (normalized) Hamming weight different from 0.5 by more than \( \epsilon/2 \),

\[
|n - \log_2(|I_{n,\epsilon}|)| = -\log_2 \left( \frac{|I_{n,\epsilon}|}{2^n} \right) = \log_2 \left( P \left[ \left| \overline{Y} - \frac{1}{2} \right| \leq \frac{\epsilon}{2} \right] \right) = -\log_2 \left( 1 - P \left[ \left| \overline{Y} - \frac{1}{2} \right| > \frac{\epsilon}{2} \right] \right).
\]

(5.23)

By Hoeffding’s inequality (Theorem B.1)

\[
P \left[ \left| \overline{Y} - \frac{1}{2} \right| > \frac{\epsilon}{2} \right] \leq \exp \left( -\frac{\epsilon^2}{2} n \right)
\]

and thus

\[
n - \log_2(|I_{n,\epsilon}|) \leq -\frac{1}{\ln(2)} \ln \left( 1 - 2 \exp \left( -\frac{\epsilon^2}{2} n \right) \right).
\]

For \( 0 < x < 0.5 \), it is easy to verify that \( -\ln(1 - x) \leq 3x/2 \); thus, for \( n \) large enough (e.g. \( n > \ln(16)/\epsilon^2 \)),

\[
n - \log_2(|I_{n,\epsilon}|) \leq \frac{3}{\ln 2} \exp \left( -\frac{\epsilon^2}{2} n \right).
\]

(5.24)
5.5. PROOFS OF ROBUSTNESS

We now deal with the specific case in which $\epsilon = 0$. This yields a string with balanced Hamming weight, as done in [49].

**Proposition 5.16** For $\epsilon = 0$, the entropy of the uniform distribution on $I_{n,0}$ is asymptotically equal to $n - 0.5 \log_2(n) - 0.5(\log_2(\pi) - 1)$

**Proof** The set $I_{n,0}$ has $\binom{n}{n/2}$ possible strings. Stirling’s formula gives

$$\lim_{n \to \infty} \frac{n}{n/2} \sqrt{\frac{2n}{\pi n/2}} = 1.$$ 

We get the result by taking the log of the denominator.

Thus, by choosing $\epsilon > 0$, we avoid asymptotically losing more than $0.5 \log_2(n)$ bits of information.

**Probability of aborting Protocol 1′**

The protocol aborts if there are less than $h$ zeros or $h$ ones left in the sift string after $n$ test bits have been chosen, where $h = \lfloor (1 + \epsilon)n/2 \rfloor$. We prove that this occurs with a probability that decreases exponentially with $n$.

**Proposition 5.17** For any $0 \leq \epsilon < \delta$ and $\epsilon \leq 1$ fixed by the protocol, the probability that it aborts is exponentially small.

**Proof** We begin with showing that, besides an exponential probability, the number of sift bits is bigger than $N/4$. We follow by showing that this is enough for having at least $h$ zeros and ones, except for exponential probability. Let $\delta'$ be a real number s.t. $\epsilon < \delta' < \delta$. Let $N = \lceil 8n(1 + \delta) \rceil$. For $i \leq i \leq N$, let $X_i = 1$ if the qubit $i$ is sift and $X_i = 0$ otherwise. The variables $X_i$ are clearly independent; their distribution is a Bernoulli with $p = 0.25$, as shown in Table 5.1. The random variable $S$ giving the number of sift bits is $S = \sum_{i=1}^{N} X_i$. Denote $\overline{X} = S/N$; it is clear that $E[\overline{X}] = 1/4$, and we can bound $P[S \leq N/4]$ using Hoeffding (Theorem B.1),

$$P[S \leq 2n(1 + \delta')] \leq P \left[ \overline{X} \leq \frac{1 + \delta'}{4(1 + \delta)} \right]$$

$$\leq P \left[ \overline{X} - \frac{1}{4} \leq -\frac{\delta - \delta'}{4(1 + \delta)} \right]$$

$$\leq \exp \left( -\frac{1}{8} \left( \frac{\delta - \delta'}{1 + \delta} \right)^2 n \right)$$

and thus

$$P[S > 2n(1 + \delta')] \geq 1 - e^{-k_1 n} \quad (5.25)$$
for \( k_1 = 1/8 \frac{|(\delta' - \delta)/(1 + \delta)|^2}{.}

For each \( S > 2n(1 + \delta') \), the \( S \) bits are distributed uniformly. After \( n \) test bits are chosen, the remaining \( S - n > 2n(1 + \delta') - n = n(1 + 2\delta') \) bits are still uniformly distributed. The protocol succeeds every time there are at least \( h \) zeros and \( h \) ones after the \( n \) test bits are chosen, and in addition there are more than \( 2n(1 + \delta') \) sift bits. As a consequence, the probability of success is larger than or equal to the probability that \( S > 2n(1 + \delta') \) times the probability that the \( S - n \) remaining bits contain at least \( h \) zeros and \( h \) ones, given that \( S > 2n(1 + \delta') \). Let \( V \) be the length of the string \( v \), i.e. \( V = S - n > n(1 + 2\delta') \). Let’s index the bits in \( v \) from 1 to \( V \), let \( Z_i = 1 \) if bit \( i \) is 0 and \( Z_i = 0 \) otherwise, let \( Z = \sum_{i=1}^{V} Z_i \) and let \( \overline{Z} = Z/V \); \( Z \) is thus the number of bits equal to 0 in \( v \); the \( Z_i \) are Bernoulli’s with \( p = 1/2 \) and are independent. Let us denote \( P_V \) the probability conditional to that particular value of \( V \). The probability that there are strictly less than \( h \) zeros in \( v \) is bounded by

\[
P_V[Z < h] \leq P_V[Z \leq (1 + \epsilon)n/2]
\]

\[(5.26)\]

where \( \delta' > \epsilon \) by hypothesis and again, by Hoeffding (Theorem B.1), the probability that there not enough zeros when \( S > 2n(1 + \delta') \) is bounded by

\[
\exp \left( -\frac{1}{2} \frac{(2\delta' - \epsilon)^2}{1 + 2\delta'} n \right)
\]

and the probability that there are at least \( h \) zeros and \( h \) ones when \( S > 2n(1 + \delta') \) is larger than or equal to \( 1 - 2e^{-k_2n} \) with \( k_2 = \frac{1}{2} (2\delta' - \epsilon)^2 \). As a consequence, the probability that the protocol succeeds is at least

\[
(1 - e^{-k_1n})(1 - 2e^{-k_2n}) = 1 - e^{-k_1n} - 2e^{-k_2n} + 2e^{-(k_1+k_2)n}
\]

which is more than \( 1 - 3e^{-kn} \) with \( k = \min\{k_1, k_2\} \). It is exponentially close to 1 with \( n \).

\[\blacksquare\]

5.5.4 Complete robustness of Protocol 1’

The assumption is that Eve’s attack is undetectable, and we want to show that she gets no information on the INFO string. During the execution of the protocol, Eve learns which are the test bits, she learns their values, she learns the number of bits measured by Bob
and, more importantly, her attack allows her to know their Hamming weight. We group all those data in the multivariate random variable $R$ of which the details will be irrelevant; $r$ will be a particular set of data. The execution of the protocol also gives Eve the set of indices $q$ such that $v_q = y$. What we want to show is that

$$I(Y; Q, R) = 0$$

i.e. the mutual information between the info string $y$ and what Eve knows, namely $(q, r)$, is zero.

**Probabilistic setup**

By Theorem 5.13, if Eve is unnoticeable, her final state may depend only on $|i_F|$ where $F = \bar{s}$ is the set of indices measured by Bob. Eve’s final state does not depend on $y$ either. That implies that

$$|i_F| = |i'_F| \implies p(i \mid y, r) = p(i' \mid y, r);$$

meaning that for any two possible strings $i, i'$, as long as $|i_F| = |i'_F|$ Eve’s information $r$ can not help her differentiate them, and thus they have an equal probability to be chosen by Alice.

For $h = \lfloor (1 + \epsilon)n/2 \rfloor$, Alice chooses $2^h$ indices in $F$ that are info bits and not test bits, say $E$, and such that $i_E$ is balanced, i.e. $|i_E| = h$. For any such set $E$, let $E_h$ be the strings $x$ indexed by $E$ such that $|x| = h$.

**Lemma 5.18** For any $x, x' \in E_h$,

$$p(x \mid y, r) = p(x' \mid y, r) = \frac{1}{|E_h|} = \frac{h!^2}{(2^h)!}. \quad (5.31)$$

**Proof** To simplify notations, and without loss of generality, assume that $E = \{1, \ldots, 2^h\}$ and $F = \{1, \ldots, |F|\}$ and thus $p(x \mid y, r) = \sum_{xv'} p(xv' \mid y, r)$ where $v$ are all bitstrings with indices in $\{2^h + 1, \ldots, |F|\}$ and $v'$ are those with indices in $\{|F| + 1, \ldots, N\}$; similarly $p(x' \mid y, r) = \sum_{xv'} p(x'v' \mid y, r)$; if we let $i = xv'$ and $i' = x'v'$ then $xv = i_F$, $x'v = i'_F$ and

$$|i_F| = |xv| = |x| + |v| = |x'| + |v| = |x'v| = |i'_F|$$

and thus, by Equation (5.30), $p(i \mid y, r) = p(i' \mid y, r)$ and the two sums are equal. ■

**Combinatorial lemmas**

Given a set $E$ and $k \leq |E|$, we denote $\mathcal{P}(E, k)$ the set of permutations of $k$ elements in $E$, i.e. the set of strings $q_1 \ldots q_k$ of $k$ distinct elements in $E$\footnote{For simplifying the notations, bits keep their indices even when they appear in substrings.};

$$|\mathcal{P}(E, k)| = \frac{|E|!}{(|E| - k)!}. \quad (5.33)$$
CHAPTER 5. QUANTUM KEY DISTRIBUTION WITH CLASSICAL BOB

From now on, $\epsilon$ such that $0 \leq \epsilon \leq 1$, $\epsilon < \delta$ will be fixed, as well as $h = \lfloor (1 + \epsilon)n/2 \rfloor$ and $E$, a set of $2h$ indices of sift bits that are not test bits. For $y \in I_{n,\epsilon}$ and $x \in E_h$ we let

$$Q(x, y) = \{q \in \mathcal{P}(E, n) \mid x_q = y\}.$$  \hspace{1cm} (5.34)

**Lemma 5.19** For all $y \in I_{n,\epsilon}$ and $x \in E_h$ the number of elements $|Q(x, y)|$ of $Q(x, y)$ is

$$|Q(x, y)| = \frac{h!}{(h - n + |y|)! \times (h - |y|)!}.$$  \hspace{1cm} (5.35)

**Proof** A string $y \in \{0, 1\}^n$ is in $I_{n,\epsilon}$ if and only if is contains at most $h$ zeros and $h$ ones. Let $E_0 = \{i \in E \mid x_i = 0\}$ and $E_1 = \{i \in E \mid x_i = 1\}$; $|E_0| = h$ and $|E_1| = h$ and the permutations $q$ such that $x_q = y$ are in $1-1$ correspondence with the elements of

$$\mathcal{P}(E_0, n - |y|) \times \mathcal{P}(E_1, |y|)$$

corresponding to the $n - |y|$ indices giving a 0 in $y$ and the $|y|$ indices giving a 1 in $y$. The result follows from Equation (5.33). \hfill \blacksquare

**Lemma 5.20** For all $q \in \mathcal{P}(E, n)$ and $y \in I_{n,\epsilon}$

$$|\{x \in E_h \mid q \in Q(x, y)\}| = \binom{2h - n}{h - |y|}.$$  \hspace{1cm} (5.36)

**Proof** A string $x \in E_h$ is such that $q \in Q(x, y)$ if and only if it satisfies $x_q = y$; this means that $x_{q_1} = y_1, \ldots, x_{q_n} = y_n$ (bits indexed by $q$ are fixed), the others are arbitrary provided there is a total of $h$ bits equal to 0 and $h$ bits equal to 1; the desired strings are thus obtained by filling the $2h - n$ bit positions whose indices are not in the list $q$ with $h - |y|$ bits equal to 1 (and the others equal to 0); there are $\binom{2h - n}{h - |y|}$ such strings. \hfill \blacksquare

Formula (5.36) can be rewritten

$$|\{x \in E_h \mid x_q = y\}| = \frac{(2h - n)!}{(h - n + |y|)! (h - |y|)!}.$$  \hspace{1cm} (5.37)

**Proof of robustness**

We want to show that $q$ leaks no information on $y \in I_{n,\epsilon}$. For any fixed $x \in E_h$ and $y \in I_{n,\epsilon}$, the probability that Alice sends $q$ is $1/|Q(x, y)|$ if $q \in Q(x, y)$, 0 otherwise, independently of any value of $r$:

$$p(q \mid x, y, r) = \begin{cases} 1/|Q(x, y)| & \text{if } x_q = y \\ 0 & \text{otherwise} \end{cases}$$  \hspace{1cm} (5.38)
Lemma 5.21 For all values of \( r \), all \( y \in I_{n,\epsilon} \) and all \( q \in \mathcal{P}(E,n) \)

\[
p(q \mid y, r) = \frac{(2h - n)!}{(2h)!}.
\] (5.39)

**Proof**

\[
p(q \mid y, r) = \sum_{x \in E_h} p(q \mid x, y, r)p(x \mid y, r)
\]

\[
= \sum_{x \in E_h \mid x_q = y} \frac{1}{|Q(x, y)|} \frac{(h)!^2}{(2h)!}
= \sum_{x \in X_m \mid x_q = y} \frac{(h - n + \vert y \vert)!(h - \vert y \vert)!}{(2h)!}
= \frac{(2h - n)!(h - n + \vert y \vert)!(h - \vert y \vert)!}{(2h)!}
= \frac{(2h - n)!}{(2h)!}
\] (5.40)

where the second equality is due to Equations (5.31) and (5.38), and the third and forth equalities are given by Equations (5.35) and (5.37).

**Theorem 5.22** For all protocol choices of \( \epsilon \) and \( \delta \) such that \( 0 \leq \epsilon \leq 1 \) and \( \epsilon < \delta \), the protocol is completely robust, i.e. if Eve is undetectable by the legitimate parties, then \( I(Y; Q, R) = 0 \).

**Proof** The parameters \( n \) and \( \epsilon \) are constants of the protocol; they are fixed before all random choices of Alice or Bob, and all measurements. So is the value \( h = \lfloor (1 + \epsilon)n/2 \rfloor \). The right-hand side of Equation (5.39) is thus a constant and Lemma 5.21 implies that the random variables \( Q \) and \( (Y, R) \) are independent: \( p(q, y, r) = p(q)p(y, r) \); the variables \( Y \) and \( R \) must also be independent, because Alice chooses \( y \) randomly, independently of everything else: \( p(y, r) = p(y)p(r) \). This implies that \( p(q, y, r) = p(q)p(y)p(r) \), all the variables are independent, and \( Y \) is independent of \( (Q, R) \) and \( I(Y, (Q, R)) = 0 \).

5.6 Conclusion

We presented two protocols for QKD with one party who performs only classical operations: measure a qubit in the classical \( \{0, 1\} \) basis, let the qubit pass undisturbed back to its sender, randomize the order of several qubits, or resend a qubit after its measurement. We proved the robustness of these protocols; this provides intuition why we believe they are secure.

---

8From Equation (5.33), we see that \( P(q \mid y, r) = 1/|\mathcal{P}(E,n)| \) which is the probability of a random \( n \)-permutation of \( |E| = 2h \) elements.
The protocols and analysis presented in this chapter differ from the original protocol \([18, 49]\) in several ways: (1) Protocol 1$'$ is generalized so that the Hamming weight of the obtained key is not fixed. Protocol 1$'$ of \([18]\) is merely a specific case of our protocol; (2) The entropy of the obtained key is exponentially close to \(n\); (3) The improved Protocol 1$'$ is proven to be completely robust; (4) Protocol 2 is shown to be robust in an improved way, allowing Alice and Bob to send the qubits one by one or all together.

Note that in this work we assumed perfect qubits. We leave the examination of our protocol against PNS and other implementation-dependent attacks to future research.
Chapter 6

Summary

In this research we investigated several aspects of QKD security, dealing with both theoretical and practical schemes.

We provided a formal definition of the space relevant for attacking a practical QKD scheme. Our definition takes into consideration the actual (physical) implementation of the scheme. The Quantum Space of the Protocol (QSoP) is proven to be the effective attack space — the most general attack on a practical scheme can be performed by attacking only the QSoP. As a consequence, future security analyses can be limited to the QSoP, which might make them much simpler. Furthermore, these analyses better take into consideration the entire QSoP or else might miss possible attacks (and maybe vital ones) on the protocol.

We provided several examples for the use of the tools of the QSoP in order to perform a security analysis. We showed that many of nowadays attacks on the channel are merely specific cases of the attack on the QSoP — the Quantum Space Attack (QSA). Moreover, we extensively researched photonic schemes that use interferometers, discussing their QSoP and the possible attacks on this QSoP. We used our new tools to provide a new attack on a specific interferometric variant, the reversed-space attack. This attack exploits the enlargement of the QSoP in order to acquire full information on the key. It is important to mention that such attacks are impossible if one limits the analysis to the theoretical two-dimensional space. Additionally, we proved that the most common interferometric implementation is robust against a limited QSA, and gave a thin hint that it is robust even against more powerful QSAs.

Our analysis covered several other theoretical aspects of QKD security as well. We used sophisticated method in order to achieve an exponentially improved bound on the maximal information that an adversary might have when attacking BB84 with a collective attack. Since this bound was already proven for the joint attack (which is more general than the collective attack), our analysis is new only in the methods used and not in the result of the information bound. Thus, our main achievement in respect to the collective attack, is obtaining a simple security analysis. Our analysis reaches a specific information bound
that has an exponential advantage over other analyses of the same simplicity magnitude. Moreover, we reach an improved error-threshold (again, similar to the threshold obtained for the joint attack). We hope that this method would lead to security proofs of many other protocols, that currently lack a security proof due to its complexity.

A first step for obtaining a complete security proof is having a robustness proof of a protocol, showing that an adversary is forced to induce errors if he learns any private information of the protocol. In this research we continued the analysis of the QKD with classical Bob, where one user is limited to doing only classical operations. We improved the randomization-based protocol so it would produce a key with entropy exponentially close to \( n \) (the length of the obtained key). We proved this improved randomization-based protocol to be completely robust. Furthermore, we slightly improved the robustness proof of another variant of semi-quantum protocol, so it would fit to sequential transmission of the qubits. As in the original protocol, our proof is limited to using perfect qubits. The usage of the QSoP methods, and the derivation of a security proof (or a robustness proof) against the most general QSA is left for further work.
Appendix A

General Transformation of Interferometer

In this appendix we derive the transformation of the interferometer, in order to have a scalable method for analyzing multiple-photon pulses in an interferometers. In order to derive this transformation, we need to understand the physical basis of the devices used. This is done using the annihilation and creation operators presented below. See any quantum-optics textbook [84, 73, 33] for a full description of these two operators and devices.

A.1 Creation and annihilation operators

Important operators defined on Fock states are the creation and annihilation operators, $\hat{a}^\dagger$ and $\hat{a}$. These operators raise and lower the photon number of the specific mode they act upon in the following manner:

$$\hat{a}^\dagger |n\rangle^F = \sqrt{n+1} |n+1\rangle^F \quad \text{and} \quad \hat{a} |n\rangle^F = \sqrt{n} |n-1\rangle^F. \quad (A.1)$$

For instance, given a Fock state of two modes, $\updownarrow$ and $\leftrightarrow$, we get $\hat{a}^\dagger \updownarrow |5\rangle^F = \sqrt{6} |6\rangle^F$, and $\hat{a} \leftrightarrow |5\rangle^F = 0$. The exact (physical) meaning of these operators extends the scope of this dissertation.

A.2 The Beam Splitter

The transformation of a beam splitter (Figure 3.2) can easily be written in the Schrödinger picture using the creation and annihilation operators of the different modes. The input and output modes, are related by

$$\hat{a}_1^\dagger = \frac{1}{\sqrt{2}} (\hat{a}_3^\dagger + i\hat{a}_4^\dagger); \quad \hat{a}_2^\dagger = \frac{1}{\sqrt{2}} (i\hat{a}_3^\dagger + \hat{a}_4^\dagger), \quad (A.2)$$

so that the transformation can be described for any number of photons,

\[ |nm \rangle_F = \frac{1}{\sqrt{n!} \sqrt{m!}} \left( \frac{\hat{a}_1^\dagger}{\sqrt{2}} \right)^n \left( \frac{\hat{a}_2^\dagger + i \hat{a}_4^\dagger}{\sqrt{2}} \right)^m |00 \rangle_{1,2}, \]

(A.3)

### A.3 The Phase Shift

The phase shift can be written as

\[ \hat{a}_{\text{out}}^\dagger = e^{i\phi} \hat{a}_{\text{in}}^\dagger \]  

(A.4)

### A.4 General Interferometer Transformation

Denote the interferometer transformation with IT. The transformation can be described as the composition of two beam splitters, a phase shift \( P^l_\phi \) on the long arm and a delay of \( \Delta T \) seconds on the long arm. The transformation can be described by

\[ \text{IT} = \text{BS} \cdot P^l_\phi \cdot \delta^l_{\Delta T} \cdot \text{BS}_1 \]  

(A.5)

where \( \delta^l_{\Delta T} \) is the delay (on the long arm only).

**Proposition A.1** Let \( |\psi\rangle = |n_j n_{j+1} n_{j+2} \ldots \rangle_F \) be a state such that for each \( j \) the mode \( n_j \) is a time-bin mode, sent at time \( t_j \), such that \( t_j - t_{j-1} = \Delta T \). The transformation of \( |\psi\rangle \) through an interferometer is

\[ \text{IT}|\psi\rangle = \frac{1}{N} \prod_j \left( \hat{a}_s^\dagger_{s_j} + i \hat{a}_d^\dagger_{d_j} - e^{i\phi} \hat{a}_s^\dagger_{s_{j+1}} + i e^{i\phi} \hat{a}_d^\dagger_{d_{j+1}} \right)^{n_j} |000 \ldots \rangle_F, \]

(A.6)

written in the Schrödinger picture (up to a global normalization).

**Proof** Let the output modes of the first beam-splitter, \( \text{BS}1 \), be named \( \text{short} \) and \( \text{long} \), corresponding to the short and long arms of the interferometer. We add a time index to each mode (e.g. \( \text{short}_j \)) to distinguish the different time-modes. It should be noticed that since the delay of the long arm is explicit, the interference that occurs in \( \text{BS}2 \) corresponding to time \( t_j \), is between the input modes \( \text{short}_j \) and \( \text{long}_j \) (rather than \( \text{long}_{j+1} \)). Using
Equations (A.2) and (A.4) we get

\[ \text{IT} |\psi\rangle = B S_2 \cdot P_{\phi} \cdot \delta_T \cdot B S_1 |n_j n_{j+1} n_{j+2} \ldots \rangle^p \]  
(A.7)

\[ \frac{1}{N_1} B S_2 \cdot P_{\phi} \cdot \delta_T \prod_j (\hat{a}_{\text{short}_j}^\dagger + i \hat{a}_{\text{long}_j}^\dagger)^{n_j} |000 \ldots \rangle^p \]  
(A.8)

\[ \frac{1}{N_2} B S_2 \cdot P_{\phi} \prod_j (\hat{a}_{\text{short}_j}^\dagger + i \hat{a}_{\text{long}_j+1}^\dagger)^{n_j} |000 \ldots \rangle^p \]  
(A.9)

\[ \frac{1}{N_2} B S_2 \cdot \prod_j (\hat{a}_{\text{short}_j}^\dagger + ie^{i\phi} \hat{a}_{\text{long}_j+1}^\dagger)^{n_j} |000 \ldots \rangle^p \]  
(A.10)

\[ \frac{1}{N_3} \prod_j \left( \hat{a}_{s_j}^\dagger + i \hat{a}_{d_j}^\dagger + e^{i\phi} \hat{a}_{s_{j+1}}^\dagger + i \hat{a}_{d_{j+1}}^\dagger \right)^{n_j} |000 \ldots \rangle^p, \]  
(A.11)

which gives us the desired result.
Appendix B

Hoeffding’s theorem

Theorem B.1 (Hoeffding 1963) Let $X_1, ..., X_n$ be either

1. independent random variables, with finite first and second moments, such that $a_i \leq X_i \leq b_i$ for $1 \leq i \leq n$.

2. or a random sample of size $n$ without replacement taken from a population $c_1, ..., c_N$ such that $a_i \leq c_i \leq b_i$, for $1 \leq i \leq N$.

Let $\overline{X} = (X_1 + ... + X_n)/n$ and $\mu = E[\overline{X}]$, then for any $\epsilon > 0$

$$P \left[ \overline{X} - \mu \geq \epsilon \right] \leq e^{-2n^2 \epsilon^2 / \sum_{i=1}^{n} (b_i-a_i)^2},$$

and in the same way (by symmetry)

$$P \left[ \overline{X} - \mu \leq -\epsilon \right] \leq e^{-2n^2 \epsilon^2 / \sum_{i=1}^{n} (b_i-a_i)^2}.$$

In case (2), $\mu = 1/N \sum_{i=1}^{N} c_i$, i.e. the expectancy of a sample mean is equal to the population mean. The theorem can be found in [41].
Appendix C

Coding Theory Essentials

In this appendix we survey several basic definitions of coding theory. For a textbook see [71].

Error-correction codes are used in order to transfer information over a noisy channel. Each information word is coded into a longer redundant ‘code-word’ in such a manner that the information can be retrieved even when few bits of the codeword are received with errors due to channel disturbance.

A Linear Code is a code whose codewords form a linear vector space over some field. The code is usually defined by a generator matrix, $G_{k \times n}$, whose rows form a basis of the code. The coding process is simply multiplying the $k$-bits information word $u$ with $G$, receiving an $n$-bits codeword $c = uG$.

**Definition C.1** A linear code $C$ of length $n$ over the field $F$, is a subspace of $F^n$.

The decoding is done by searching the information word $u'$ that gives the nearest codeword to $\hat{c}$, the received codeword, according to a specific distance function $d$. In other words, decryption is finding $u'$ s.t. $d(u'G, \hat{c})$ is minimal. The distance function is usually a metric named ‘Hamming distance’ which is defined as the number of bits that differ between two words: $d_{\text{Hamming}}(x, y) = \sum_i x_i \oplus y_i$.

A relatively simple way to decode is the syndrome decoding method. Every code can be defined by a parity checking matrix $H$, whose rows are orthogonal to the code space, i.e. $HG^\top = 0$. Therefore, every codeword gives 0 once multiplied in $H$

$$Hc^\top = HG^\top u^\top = 0.$$ 

Every string $x$ in $\{0, 1\}^n$ which is not a codeword gives a non-zero result $s = Hx^\top \neq 0$ which is called the syndrome. When the number of errors is small enough, knowing the syndrome is the same as knowing exactly which bits are erroneous (i.e. error in specific bits gives the same syndrome, regardless of the information word. This is due to the code

---

1 Due to errors, $\hat{c}$ might differ from $c$. 

113

Technion - Computer Science Department - M.Sc. Thesis MSC-2009-03 - 2009
linearity:
\[ Hx^\top = H(c + e)^\top = (Hc + He)^\top = 0 + s \]
where \( e \) is all-zeros except for those bits that were inverted by the channel\(^2\).

**Definition C.2** An *Affine Code* is a non-linear code, defined as \( C_b = \{c + b \mid c \in C, b \notin C\} \)
Where \( C \) is a linear code and \( b \) is fixed.

Encoding an Affine code can be done using \( C \)'s generator matrix,
\[ u \mapsto uG + b. \]

The obtained code is not a subspace of \( F^n \), but rather a coset of the subspace \( C \). Every code word in \( C_b \) has the same syndrome \( Hb^\top \).

**Definition C.3** Let \( C \) be a linear code. The *dual code* of \( C \), denoted \( C^\perp \), is the subspace
\[ C^\perp = \{x \in F^n \mid x \cdot c^\top = 0, \text{ for all } c \in C\}. \]

The dual code is a linear code itself, and \( C^{\perp \perp} = C \). The generator of the dual code \( C^\perp \), is the parity check matrix of the code \( C \).

---

\(^2\)All the computations in this section are over GF(2).
Bibliography


בטיהות פרוטוקולים الحلפת מחתרת קרואטיה

tוארתים ומעשיים

רות גלס
בתיחות פרוטוקולים החלפת מחפים קואונטיים

תאורטיים ומפעליים

חובר על מחקר

פטנס מיליאר חלק של הדרישות לכתב לתואר
ועמרת ממ슷ים במדעי המחשב

רות גלים

רות גלים - מכון טכנולוגיה לישראל
אטלד המחשה - חפה - ספטמבר 2008
תרודה

mutex בתרודה לתוך' על מזר או שנותה אתרי מעבר או מסירים. תכיפה ממוקדת ולא פחתת
מ])-> תרודה לתוך' (ברמוד יגוז או תרים חתך פחת עגימיו), על התרדנה תרודה
ותרה התרדנה הת넖ה האסראتعليم. ככ שתרדנה לתוך' מזפש בדיאלי על עזרה רורה.
דרדרות הפרימ. התרדנה הת tjejer.
תרודה תרכוב שולטת על דרך זכרי או זכרי וונישטי. יסיק וונישטי. יוב אליאס. מוזיפ כ. אויל
בינח. כלזו ויהו נפגש צוור כל מז שרק היה נודש. לרובו עריך מבוגרים. עוזה ב.
לשת. ככ שתרודה על ככ שיאישור אמין על לקות הפרה ככלה מזיני פנס, שחלותה בשיתוף
מסודרות כלילה גжить. איי מזרה לדיי אやはり. והאיסובז בודיק.
לימים. איי מזרה לדיי אやはり. על זרכוד הפרשה שתה-רה מעש slideshow.
תקציר

במסתчки שנעות בין 80% לש…the computer science department of the Technion, the thesis is dedicated to theoretical computer science and information theory.

The thesis focuses on quantum cryptography, specifically on the development of quantum key distribution (QKD) protocols and their security analysis.

The thesis introduces new protocols that improve upon existing QKD protocols, and analyzes their security against various attacks.

The main contributions of the thesis include:

- A new QKD protocol that achieves higher security compared to previous protocols.
- A security analysis of the new protocol using computational and information-theoretic methods.
- A comparison between the new protocol and existing ones in terms of security and efficiency.

The thesis concludes with a discussion of the practical implications of the new protocol and its potential applications in real-world scenarios.

The work is based on extensive research and collaboration with leading experts in the field of quantum cryptography.

The thesis is a valuable contribution to the field of quantum cryptography and can be used as a reference for researchers and students interested in the topic.
 eventName:

logdest, logds, logdsh, logdsht, logdshst, logdshtst

Breakdown of client number 1 and the different server groups.

Technion - Computer Science Department - M.Sc. Thesis 2009-03 - 2009
נשייתנש détail המחבר והינו פרוטוקולים "חיובי-קורטזיאיס" בתוכן אלא ויש לו קורא: 

ג'ירש. אכ לב רב חליפיס. כ Mariners מפעלי-היחידה לכסיס חיהם להב יוצאים (בשם הרחב). פרוטוקולים שמהז זה הרצ להבצבה על ידי מיר. קייזברנד מער ב-197. פרוטוקול זה מניח
על פרוטוקול שפה על-ידי מער ב-1983, ראשAIR מער מער אל בת מצוות הקסם חידי מעד כולם המפרק CNC בعقل פייטס סמסטריס ובריקNESS חידי. המפרק הר שת הגעה שחיאופטריס
של פרוטוקולים כל: בראשה ובו שולח חיה ואצל חלים מפרקבייס היאברה חסדה שלא
אקריאי (על פפיס שולח חיה) אך יוסף ילקית מחзыים שCreatedBy כנף חיה. הבסיס שאנון כיס החיה. דיר ש tor לא מסוגל
فاعש עקבי מכסינים לכסים חידי: משלicroڞ לב מזרד מגר הקורטזיאיס בכסים החיה. ומוחרמד

אליס קריביטא מסقرب החיה לצג שמיד.

ואנ מתפעים Coil הריס מפעלים של הצטנוקול זראך. בריכי המפעלי מרס helt מנהלת
אשר קיימים פרוטוקולים המקודים חותם סדרת האילים על המפעלים של פרוטוקול ממוקס
(lbalanced string) אנ מצוות בו הפרוטוקל המפרוע יוני סדרת להפסד ומקומיים. והמקומיים המפרוע
תנו סטטיסטיות של המפעלים המתקדמים, ומפרוע אנ מצוות בוquier גודל המפעלים המתקדמים
n, וארא. המטריית של המפעלים שתודפות אקטיבו-איליאי ל-1.

כומ. כל פציתים לפיו הפרוטוקל וה RCS של הפרוטוקל גודיל מפרעת המפרוע וחיות
ככלית צורה, המתראת גם למפרק קפה על-ידי המפרוע מבקה. ממטרהו במ Earl
ולא בין מוניטיר אונ הקורטזיאיס חוזי לערור שדר.