



Norwegian University of
Science and Technology

Understanding complementarity-based security proofs of quantum key distribution with imperfect sources

Jan Gulla

Master of Science in Physics and Mathematics

Submission date: June 2017

Supervisor: Jan Myrheim, IFY

Co-supervisor: Johannes Skaar, Institutt for elektroniske systemer

Norwegian University of Science and Technology
Department of Physics

Understanding complementarity-based security proofs of
quantum key distribution with imperfect sources

Jan Gulla

June 18, 2017

Abstract

We present a study of modern security proofs of quantum key distribution based on complementarity. This is a quantum communication protocol allowing for provable, unconditional security, although there is still a gap between theoretical analyses and real, operational systems. We focus on a recent argument by Koashi, which enables the treatment of individual, basis-dependent imperfections in the source. A detailed review is given based partly on an alternate derivation, with the goal of providing a more accessible approach to utilizing the strength of the complementarity-based proof. Some subtleties in the argument are then pointed out, particularly regarding the requirement of perfectly independent states in the random sampling. A numerical approach is implemented to simulate arbitrary protocols in order to investigate the necessity of this requirement. For independent states, the results provide strong evidence in support of the established security bounds. We then focus on imperfect sources with basis-independent correlations, which reveals concrete counterexamples to the security claims, even in the operational regime. This increases the understanding of why security relies critically on perfect independence of the states. We also predict the possibility of attacking real-world devices as the results show a necessary, although not sufficient, condition for exploiting small, but finite basis-independent correlations in an imperfect source. Furthermore, we argue that analyzing such systems and finding capable attack operations is difficult to achieve by analytic methods; instead we develop further numerical techniques for sampling the parameter space of source states and attack operations in a computationally efficient manner. These parameters are then iteratively improved using a hybrid uniform search and genetic optimization routine. The numerical methods prove to be effective in both uncovering sources that are prone to correlation attacks as well as constructing explicit attack operations for a given system.

Sammendrag

Vi studerer moderne sikkerhetsbevis av kvantenøkkedistribusjon (quantum key distribution) basert på et argument om komplementaritet. Dette er en kvantemekanisk kommunikasjonsprotokoll som muliggjør beviselig, ubetinget sikkerhet, men hvor nåværende teoretiske modeller imidlertid fremdeles ikke fullt kan beskrive operative systemer. Vi fokuserer på et nylig argument fra Koashi, som gjør det mulig å analysere kilder med individuelle, basis-avhengige feil. Beviset gis en detaljert gjennomgang, delvis basert på en alternativ utledning, med et mål om å gjøre styrken til komplementaritetsbeviset mer tilgjengelig. Vi påpeker deretter noen subtile konsekvenser av sikkerhetsargumentet, spesielt med tanke på kravet om perfekt uavhengighet mellom tilstandene i den tilfeldige utvalgsprøven. For å undersøke nødvendigheten til dette kravet implementerer vi en numerisk metode for å simulere vilkårlige protokoller innen kvantekommunikasjon. For uavhengige tilstander viser resultatene utmerket overensstemmelse med etablerte sikkerhetsgrenser. Vi fokuserer deretter på basis-uavhengig korrelerte kilder med feil, hvor vi finner konkrete eksempler på svikt i sikkerheten selv for realistiske parametere. Dette bidrar til en økt forståelse for hvorfor sikkerheten er kritisk avhengig av tilstander som er perfekt uavhengige. Vi foreslår også muligheten for et angrep mot realistiske system, da resultatene viser en nødvendig, skjønt ikke tilstrekkelig, betingelse for å utnytte små, men endelige basis-uavhengige korrelasjoner i kilder med feil. Å bruke rene analytiske metoder for å analysere slike system og finne kapable angrepsoperasjoner viser seg imidlertid å være vanskelig. Vi utvikler derfor numeriske teknikker for å effektivt gjøre tilfeldig samplinger av parameterområde for kildetilstander og angrepsoperasjoner. Disse parameterne forbedres deretter iterativt ved hjelp av en kombinasjon av uniformt søk og en genetisk optimeringsrutine. De numeriske metodene vises å være effektive for å kartlegge hvilke kilder som er utsatt for korrelasjonsangrep, samt å konstruere eksplisitte angrep mot konkrete system.

Preface

This work represents the Master's thesis for a degree in Applied Physics at the Norwegian University of Science and Technology (NTNU). Parts of the introduction, Chapter 2, Chapter 3 and Section 4.1 were written during the fall of 2016 as the report for a project preparing for the thesis. The research and work in the rest of the document was done during 20 weeks in the spring of 2017.

I would like to thank my advisor Professor Johannes Skaar at the Department of Electronic Systems, NTNU for the opportunity to do this work as well as invaluable feedback during the year. I would also like to thank my supervisor at the Department of Physics, NTNU, Professor Jan Myrheim.

The code used in the numerical investigation is implemented in MATLAB, Fortran and / or C++ as indicated. Source code and raw data is available upon request at jangu@stud.ntnu.no or jangu11a93@gmail.com.

Contents

Preface	vii
List of figures	xiii
List of tables	xv
Nomenclature and notation	xvii
1 Introduction	1
1.1 The cryptographic problem	2
1.1.1 Setup	2
1.1.2 Security criteria	3
1.1.3 Security classes	3
1.1.4 Vernam one-time pad	4
1.1.5 Limits of cryptography	4
1.2 Background	5
1.2.1 Classical cryptography	5
1.2.2 Quantum cryptography	7
1.3 Motivation	7
1.3.1 Social importance	8
1.3.2 Importance to the field	9
1.3.3 Personal motivation	10
1.4 Structure of this document	10
2 Fundamentals	13
2.1 Quantum mechanics	13
2.1.1 Postulates	13
2.1.2 Physical consequences	15
2.1.3 The qubit	16
2.1.4 Interpreting uncertainty	17
2.2 Quantum computation	18
2.2.1 Bloch sphere	18
2.2.2 Operators	19
2.2.3 Measurement	19
2.2.4 Density operators	21
2.2.5 Composite systems and entanglement	24
2.2.6 Quantum circuits	27
2.2.7 Useful theorems	30

3	Quantum information	31
3.1	Quantum operations	31
3.1.1	System-environment model	31
3.1.2	Operator-sum representation	32
3.1.3	Axioms	33
3.1.4	Operator-sum freedom	34
3.2	Distance measures	34
3.2.1	Classical distance measures	34
3.2.2	Trace distance	35
3.2.3	Fidelity	37
3.2.4	Distance measure equivalence	39
3.3	Information theory	39
3.3.1	Classical information	39
3.3.2	Classical multivariate entropy	41
3.3.3	Quantum information	43
3.3.4	Quantum multi-state entropy	45
3.3.5	Encoding classical information	46
3.3.6	The Holevo bound	47
4	Quantum cryptography	49
4.1	Quantum key distribution	50
4.1.1	Setup and goals	50
4.1.2	Assumptions	51
4.1.3	Proving security	52
4.1.4	The modern security definition	52
4.1.5	BB84	53
4.2	Security proof	56
4.2.1	Idea	56
4.2.2	Principles	57
4.2.3	Formal protocol	58
4.2.4	Equivalent entanglement protocol	60
4.2.5	Proof of the main theorem	63
4.2.6	Asymptotic limit	67
5	Source imperfections	69
5.1	Protocol	69
5.1.1	General source	70
5.1.2	Koashi's source condition	70
5.1.3	Revised source condition	71
5.1.4	Entanglement protocol	72
5.2	Error estimation	73
5.2.1	Problem formulation	73
5.2.2	Koashi's theorems	75

5.2.3	Single state	76
5.2.4	Double disconnected state	76
5.2.5	Double joint state	78
5.2.6	Random sampling	79
5.2.7	Larger values of L	82
6	Numerical investigation	85
6.1	Investigation 1	85
6.1.1	Simplifying restrictions	86
6.1.2	Algorithm	86
6.1.3	Uniformly generating variables	87
6.1.4	Implementation	88
6.1.5	Results	89
6.1.6	Fixed parameter simulations	90
6.1.7	Other values of L	92
6.2	Investigation 2	94
6.2.1	Finding realistic counterexamples	94
6.2.2	Algorithm	96
6.2.3	Implementation and results	98
6.2.4	Genetic optimization	98
6.3	Investigation 3	99
6.3.1	Adjusting the algorithm	100
6.3.2	Implementation and results	101
7	Discussion	103
7.1	Validity of results	103
7.1.1	Feasibility of an explicit attack	104
7.1.2	Impact of numerical errors	105
7.1.3	Realism of result properties	106
7.1.4	Summary	107
7.2	Assumptions and impact	107
7.2.1	Understanding security for imperfect sources	107
7.2.2	Correlation attacks	108
7.3	Further work	109
8	Conclusion	111
	Bibliography	113
	Appendix A Numerical values of counterexamples	1

List of figures

1.1	Schematic diagram of the classic setup in cryptography	2
2.1	Euler diagram of properties of common quantities in quantum computation .	24
2.2	Quantum circuit for implementing a general quantum measurement	30
3.1	Quantum circuit of the defining process for a quantum operation	32
4.1	Clavis 2: commercial quantum key distribution system manufactured by ID Quantique [MLS10a].	49
4.2	Schematic diagram of the setup in quantum key distribution	50
4.3	Illustration of the key gain for an example key	56
5.1	Interpretation of the error rate in the X -basis case for $L = 4$	74
5.2	Error rate analysis model for $L = 1$	76
5.3	Error rate analysis model for $L = 2$ with a disconnected channel	77
5.4	Error rate analysis model for $L = 2$ with a joint channel	79
5.5	Example of a deployment of the protocol	80
5.6	Error rate analysis model for $L = 3$ with a joint channel	82
5.7	Error rate analysis model for $L = 4$ with a joint channel	83
6.1	Scatter plot of δ_{ph} vs. δ_x for $L = 2, M = 80\,000, F_1 = 0.99$ and $F_2 = 0.991$ from the Fortran simulation	89
6.2	Scatter plot of δ_{ph} vs. δ_x for $L = 2, M = 100\,000, F_1 = 0.99$ and $F_2 = 0.991$ from the C++ simulation	90
6.3	Scatter plot of δ_{ph} vs. δ_x for $L = 2, M = 1\,000\,000, F_1 = 0.99$ and $F_2 = 0.991$ with fixed states $ \chi_a\rangle$	91
6.4	Scatter plot of δ_{ph} vs. δ_x for $L = 2, M = 100\,000, F_1 = 0.99$ and $F_2 = 0.991$ with a fixed channel U	92
6.5	Scatter plot of δ_{ph} vs. δ_x for $L = 3, M = 1\,000\,000, F_1 = 0.99$ and $F_2 = 0.991$	93
6.6	Scatter plot of δ_{ph} vs. δ_x for $L = 1, M = 100\,000, F_1 = 0.99$ and $F_2 = 0.991$.	93
6.7	Circuit model for the definition of $\sigma_a^{(i)}$ in the improved algorithm for sampling random channels \mathcal{E}	97

List of tables

2.1	Basic quantum circuit elements.	27
2.2	Single-qubit quantum gates.	27
2.3	Multi-qubit quantum gates.	28
2.4	Additional quantum circuit elements.	29
6.1	Summary of quantitative results in Figure 6.1 - 6.6	94

Nomenclature and notation

During this work we will frequently use terms such as “classical cryptography”, “classical information” or similar. This is not referring to techniques that are old or outdated in some way, but rather techniques that are quantum mechanical in nature.

We will make reference to two types of vectors: Quantum states, which are represented by vectors on a complex Hilbert space, are given in the standard bra(c)ket notation $|\psi\rangle$. Any ordered collection of numbers in the format of a column vector are denoted by conventional vector notation \mathbf{x} . In particular this applies regardless of the number of elements x_i and their transformation properties (e.g. they may not even transform at all).

Distinguishing labeled vectors from labeled *components* of vectors is done by denoting components of a named vector \mathbf{a} by a_i , whereas a collection of vectors will be denoted \mathbf{a}_i . Denoting components of an unnamed or modified vector is done with parenthesis, e.g. $(\mathbf{a} - \mathbf{b})_i$ or $(\hat{\mathbf{k}})_i$, whereas $\hat{\mathbf{k}}_i = \mathbf{k}_i / \|\mathbf{k}_i\|$ is a vector.

In the bra(c)ket notation, we will differentiate between subscripts within and outside the bracket. Inner subscripts will label different bras / kets, such as $|\psi_n\rangle$. Outer subscripts will label the associated structure of the particular bra / ket, e.g. $|\psi\rangle_A$ symbolizes that it belongs to a particular Hilbert space \mathcal{H}_A or $|\psi\rangle_I$ indicates that its dynamics is governed by the interaction picture.

Operators are denoted by capital letters, with A, B, \dots usually representing general operators, and U, V, \dots usually representing unitary operators.

Quantum operations will be denoted in calligraphic font as $\mathcal{E}, \mathcal{F}, \dots$.

The computational basis for qubits is defined in the mathematical convention:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad (1)$$

We define σ_0 as the 2×2 identity matrix, so that $\sigma_\mu; \mu = 0, \dots, 3$ are the components of a Pauli 4-vector. The Pauli matrices will also be denoted as X, Y, Z .

Summation convention is assumed for indexed quantities unless otherwise stated. Whenever a contraction is possible but not performed should be clear for the expression.

Below is an explanation of various symbols used throughout this work.

General

\log	binary logarithm
\ln	natural logarithm
c^*	complex conjugate of c
δ_{ij}	Kronecker delta
ε_{ijk}	permutation symbol (Levi-Civita)
\mathbb{R}	set of real numbers
\mathbb{C}	set of complex numbers
$\operatorname{Re}\{c\}$	real value of c
$\operatorname{Im}\{c\}$	complex value of c
$\operatorname{Pr} E$	probability of an event E

Bra(c)ket

$ \psi\rangle$	state vector (ket)
$\langle\psi $	functional (bra) corresponding to the state vector $ \psi\rangle$
$\langle\psi \phi\rangle$	inner product between state vectors $ \psi\rangle$ and $ \phi\rangle$
$\ \psi\rangle \ $	norm of the state vector $ \psi\rangle$

Linear algebra

$\operatorname{tr}(A)$	trace of operator A
$\operatorname{supp}(A)$	support of operator A
$\operatorname{rank}(A)$	rank of operator A
$\operatorname{ran}(A)$	range of operator A
$\operatorname{ker}(A)$	kernel of operator A
$E(A)$	eigenspace of operator A

Operators

I	identity operator
σ_μ	Pauli matrix μ ; $\mu = 0, \dots, 3$
$\mathcal{L}(V)$	set of linear operators on vector space V
$\mathcal{P}(V)$	set of positive operators of unit trace (density operators) on vector space V
$U(n)$	group of $n \times n$ unitary matrices
A^\dagger	adjoint of operator A

Distance measures

$D(p_x, q_x)$	classical trace distance between distributions p_x and q_x
$F(p_x, q_x)$	classical fidelity between distributions p_x and q_x
$D(\rho, \sigma)$	quantum trace distance between states ρ and σ
$F(\rho, \sigma)$	quantum fidelity between states ρ and σ

Entropy

$h(\delta)$	binary entropy of δ
$H(X)$	classical (Shannon) entropy of distribution X
$H(X, Y)$	classical joint entropy of distributions X and Y
$H(Y X)$	classical conditional entropy of distribution Y given distribution X
$D(p q)$	classical relative entropy of distribution p_x with respect to distribution q_x
$I(X : Y)$	classical mutual information between distributions X and Y
$S(\rho)$	quantum (von Neumann) entropy of state ρ
$S(A, B)_\rho$	quantum joint entropy of state ρ_{AB}
$S(A B)_\rho$	quantum conditional entropy of the reduced state ρ_A given the reduced state ρ_B
$S(\rho \sigma)$	quantum relative entropy of state ρ with respect to the state σ
$I(A : B)_\rho$	quantum mutual information between reduced states ρ_A and ρ_B

Vectors

\mathbf{v}	vector
$\hat{\mathbf{v}}$	unit vector
\mathbf{e}_i	Cartesian unit vector in the i -direction; $i = x, y, z$

Chapter 1

Introduction

Can two parties communicating only through a channel open to the public, exchange messages with guaranteed secrecy? If so, what resources need to be established between the parties in order to achieve this? The incessant search for secure communication plays an integral part of our history and seems to be more important than ever in today's digital society. At the same time, the field of cryptography is currently undergoing a rapid, fundamental shift from classical information theory to that of quantum information. In this framework, information is inherently physical, and as such, security analyses must account for fundamental properties of physical representations, among others notably *imperfections*. Understanding the implications of device imperfections on cryptographic security in the quantum realm is only in the beginning stages, but its importance and intrinsic relevance can hardly be overstated.

This work aims to investigate some recent developments in the security analysis of quantum cryptography, specifically the BB84 protocol, with device imperfections. A detailed review of existing proofs is given and numerical procedures are developed to validate the models by performing explicit simulation of the system in question. The results support the security proofs, but point out a possibility for attacking real systems with slightly correlated imperfections.

This chapter attempts to outline the context in which this work falls under. The first section introduces the core problem which cryptography aims to address as well as some important results and terminology. The second section then gives a brief account of the historical development of classical and quantum cryptography leading up to this point. The final section presents this work: its motivation, how it relates to other works in the field and the structure of this document.

1.1 The cryptographic problem

The defining goal of a cryptographic system is to secure a transmission of information along an unsafe communication line, i.e. there is a possibility of a third party accessing any or all messages sent across the line [DK07]. Physically, this could either be realized by an unauthorized access to a private communication line or, as is typically the case, the line being fully public, e.g. when transmitting over EM signals or through the Internet. Cryptography is the study of constructing and applying protocols to such unsafe lines in a way that still renders the message secure.

This section introduces the basics principles of cryptography, including security criteria, classification of security categories and the fundamental limits of cryptography. A description of the principle and importance of the Vernam one-time pad is also given.

1.1.1 Setup

In the standard setup in cryptography [DK07], as depicted in Figure 1.1, we consider two parties: person A (Alice) and person B (Bob). Alice seeks to transmit a message, called the *plaintext*, to Bob over some communication channel. An eavesdropper (Eve) also has access to the line of communication and has some degree of control over the transmissions through it. In the case where Eve has full control over the line, she has the capacity to read, block or alter any transmission through the line, as well as sending her own messages to any of the parties.

To secure the message, Alice and Bob adopt some scheme to convert the plaintext into some (seemingly) unintelligible text, called the *ciphertext*. The process of converting from the plaintext to the ciphertext is known as *encryption* and the reverse as *decryption*. Commonly, an algorithm designed for encryption and decryption is also referred to as a *cipher*. The details of the conversion is typically governed by two parts: a set of instructions (the *algorithm*), which is universal for all messages, and a *key*, which is individual to each message [KL08]. The key is usually a sequence of random numbers that Alice or Bob generate and need to be kept hidden from any other parties.

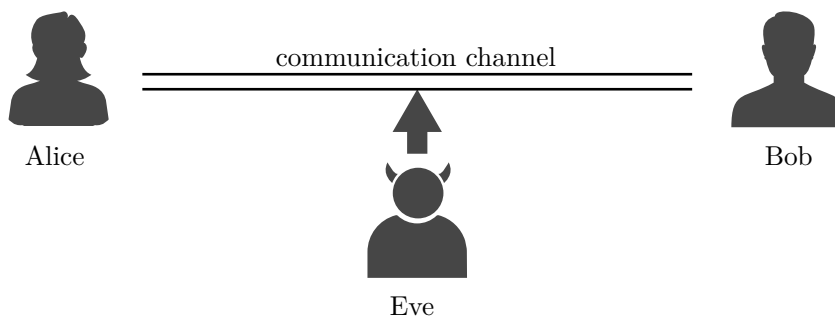


Figure 1.1: Schematic diagram of the classical setup in cryptography: person A (Alice) seeks to securely communicate a message to person B (Bob) over some channel. An eavesdropper (Eve) has access to the communication channel.

1.1.2 Security criteria

The criteria of what exactly “securing” the message entails was first formalized by Shannon in 1949 [Sha49]. The modern theory identifies 4 main goals of cryptography [DK07]:

- Confidentiality: Ensuring that the message can only be read by the intended parties, and equivalently that it is unreadable by everyone else.
- Authenticity: Allowing accurate identification of the message’s sender, such that no other party can pretend to be the original sender.
- Integrity: Preventing modifications of the message during transmission, or alternatively allowing the receiver to verify whether the received message was modified from the original.
- Non-repudiation: Providing a reliable mechanism to prove that the sender did send the message, such that the sender cannot later deny sending it.

1.1.3 Security classes

Shannon was also the first to introduce different classes of security, based on the assumptions made in the security proofs [Sha49]. Today we distinguish between *unconditional* security and *computational* security [KL08]. The latter applies to protocols that remain secure given reasonable assumptions about the attackers computing power. The former, on the other hand, promises that security holds for *any* attack, specifically against attackers with unlimited computing power. This form of security is of course attractive in its absoluteness; yet, computational security is often sufficient, e.g. when the best attacks are projected to take several thousand years of computation.

The real problem with computational security comes however from the fact that the theoretical foundation of computational hardness is so far limited. Particularly, most modern encryption schemes attain their secrecy from the computational cost of certain mathematical problems. The problem is however that it is typically not yet known exactly how difficult these underlying problems are to compute [KL08]. In addition, the whole area of computational complexity classes is not completely understood, most notably in the lack of determining whether $\mathbf{P} \neq \mathbf{NP}$. This has the consequence that the underlying mathematical problems could in principle admit an efficient solution, even when they are shown to be equally intractable as other computationally hard problems.

Note also that one interesting feature of unconditional security is that it in particular holds against even *brute-force* attacks. This term is used to describe strategies where an attacker simply searches through and tries all possible keys. Although it is typically extraordinary unlikely to guess the correct key by chance, the attacker could of course in theory do so. Unconditionally secure ciphers are however resistant to brute-force attacks, because even if the attacker does manage to guess the correct key, there is no way for the attacker to verify

this is indeed the case. Even when part of the plaintext is known on beforehand, there is no way to verify if a key was correctly guessed.

1.1.4 Vernam one-time pad

The simplest classical cipher that is known to be unconditionally secure is the Vernam one-time pad [KL08]. It consists of combining the plaintext with a truly random bits sequence of equal length, thus requiring a one-time, pre-shared key for all information being transmitted. First, the plaintext is represented in binary form as $m \in \{0, 1\}^l$, where l its length. Second, a random key k is chosen from a uniform probability distribution of bit strings over $\{1, 0\}^l$. The ciphertext c is then computed as

$$c = k \oplus m, \tag{1.1}$$

and the plaintext can similarly be recovered from the ciphertext by

$$m = k \oplus c, \tag{1.2}$$

where \oplus is the logical XOR operator.

The difficulty with distributing such massive amount of key material makes the Vernam cipher not very much used in practice.

1.1.5 Limits of cryptography

One of the fundamental insights necessary to analyze cryptographic systems is related to what it can, and what it cannot accomplish. Such fundamental limits are always present in any cryptographic system, and can in particular not be solved by quantum techniques either. One example of this is the noteworthy exception to the list of cryptographic goals, namely to guarantee delivery of the message. Another relevant example concerns an important, reoccurring concept in cryptography: how much information Alice and Bob share prior to initiating the protocol.

To fully capture all possible attacks, e.g. Eve having physical access to the line, Eve must be allowed full control over the communication channel. In particular this implies that Eve has the option to block the transmission of signals, cutting of the communication completely. As such, there is no method available to Alice and Bob to prevent this; Eve will always have to option of *jamming* the communication. Consequently, Alice and Bob must consider methods for securing their communication, *in the case that* Eve does not jam the line. This fundamental limit of cryptography is notably present also in the quantum case, where Alice and Bob need to estimate the interference by Eve.

The other limit is related to the information shared by Alice and Bob at the beginning of the protocol. As an example, establishing a secure connection to a web page never

previously visited leaves Alice and Bob with no pre-shared information. On the other hand, credit cards issued by a bank establishes a secret number shared between the user and the bank. Any information shared by communicating parties prior to the initialization of the communication protocol is labeled their *pre-shared key*. The amount of information in this key is called the *key material* and dictates what level of security Alice and Bob can achieve.

In the event of Alice and Bob having no pre-shared key, any level of secrecy is impossible. This resides in the possibility of Eve performing a perfect man-in-the-middle attack. In this scenario, Eve intercepts the connection to Bob, redirects it to herself and simply follows the details of the protocol Alice and Bob use. If there is no pre-shared key at all, then by definition Alice has no way of distinguishing Bob from Eve. No cryptographic system can overcome this limit; Alice will therefore have no way of detecting Eve's interference and the security is necessarily broken. This limit will become apparent also in the quantum case, but it is important to realize its general validity to all cryptography¹.

1.2 Background

Ever since we first started recording and storing information, there has been an accompanying need to secure it. Examples of early attempts at cryptography are found as far back as 1500 BC [Kah96]. Since then, a myriad of cryptographic techniques were developed over the centuries, starting with simple substitution ciphers and gradually spawning more sophisticated techniques. Alongside the development of new methods of securing information was the accompanying effort to break them. Thousands of years of an unflinching cryptographic arms race has blossomed into a rich field of study on its own, as well as spawning other areas of research [Gol01]. This section gives a brief overview of the history of cryptographic development.

1.2.1 Classical cryptography

In the past, attention was often directed towards inventing new, “clever” schemes for encryption [KL08]. Cryptography was then primarily an art, relying on ingenuity and creativity to come up with new, convoluted substitution codes. The security of such methods relied on keeping the operations of the encryption scheme secret and the belief that discovering and recreating it in all its detail would be too difficult. This cryptographic approach is generally known as *security through obscurity*, and has the disadvantage that weaknesses in the system can go unnoticed for a long time. Despite new, real-world cases of such security attempts resurfacing with alarming frequency, the scientific community has generally abandoned obscurity techniques in favor of Kerckhoff's Principle [DK07]; this states that a cryptographic system should remain secure if an adversary learns the full detail of the

¹See also the discussion in Section 1.2.1

system. Such systems attain their security based on the secrecy of only the key and has the advantage of the scientific community's continuous scrutiny and improvement.

Apart from increasing the efficiency of existing techniques, the theoretical foundation of cryptography remained relatively untouched up until after the end of the Second World War. A major breakthrough occurred in 1948 - 1949² however with the publication of Shannon's papers [Sha48; Sha49], initiating the era of information theory and modern cryptography (see Section 3.3.1). Shannon's key idea was evaluating the information content of a *message* in terms of its likelihood given the set of *all possible* messages that could have been selected. He then introduced "entropy" as a quantitative measure of this content, with units named the "bit". He also established the systematic classification of attacks against a cryptographic system as described in Section 1.1.3, marking the final transition of cryptography from art to science.

Shannon's work also provided definite proof that the already-known technique of the Vernam one-time pad was in fact unconditionally secure [Sha49]. As mentioned, the caveat is however that it requires a unique shared key of equal length as the message to be established between the communicating parties. This makes the one-time pad highly impractical in practice. Since Shannon's proof, the development of new cryptographic techniques has largely addressed this trade-of between security and practicality [KL08].

Today we have a suite of well-developed cryptographic techniques available. One of the most popular methods is the Advanced Encryption Standard (AES), a substitution-permutation encryption method with no known, feasible vulnerabilities [KL08]. It is an example of a symmetric-key algorithm, where a single, secret key shared by the communicating parties is used to both encrypt *and* decrypt the message. It is in a sense the modern equivalent to the traditional ciphers, where the two parties agree on a secret recipe for encryption, prior to communicating. As a contrast, there is also today a whole different *class* of cryptographic techniques labeled public-key, where the two communicating parties need not have a shared secret on beforehand. It functions by constructing *two* keys, such that finding the second key from the first is computationally trivial, whereas the other way has no known efficient solution [KL08]. Security is then provided by the fact that there exists a scheme by which a message encrypted by the second key can only be decrypted with the first.

There is a precaution to be made about the preceding claims about public-key cryptography. As remarked in Section 1.1.5, any messaging scheme in which the two parties start out with no shared secret at all, will always be vulnerable to a man-in-the-middle attack. This is simply due to the fact that sharing no initial secret information makes distinguishing the other party from an attacker impossible. In the case of public-key cryptography, this is in practice typically solved by establishing certificate authorities: centralized agencies whose public key is already known and that are contacted during the protocol in order to verify other public keys. Later, when designing quantum cryptographic protocols, we will take the different approach by making the existence of a small, shared initial secret an explicit

²[Sha49] was originally written in 1945, but declassified only in 1949 [Gol01].

requirement of the protocol.

In summary, since the work of Shannon, an incredible amount of progress has been made in both the application and theoretical understanding of cryptography. At the end of the 20th century however, one blind spot remained: the one-time pad was still the only cryptographic protocol with a strict proof of its security. In line with the discussions in Section 1.3.1, the core issue is that the modern cryptographic techniques only provide computational security.

1.2.2 Quantum cryptography

The situation was completely overturned with the discovery of quantum information, beginning a new era of cryptographic research. Following the discovery of quantum mechanics around the beginning of the 20th century, the application to information processing systems was not immediately realized. The first signs started appearing in the 1970s, with the Holevo bound [Hol73] and on the difference between classical and quantum information [Ing76]. In 1981 Feynman famously called for the construction of special “quantum computers” in order to make efficient simulations of nature [Fey82]. In 1984 Bennett and Brassard published their article [BB84], describing for the first time a complete quantum cryptographic protocol. Deutsch then introduced the theoretical construct of the “universal quantum computer” in 1985 [Deu85], and within a few years he also provided one of the first examples of a “quantum algorithm” that runs more efficiently than any classical counterpart [DJ92]. In 1994 the power of quantum computers made headlines as Shor discovered how they can be used to do integer factorization in polynomial time [Sho94].

Since then, research on quantum information has seen a massive boom. New algorithms and communication protocols for quantum systems have been developed in the past decades as the theoretical foundation of quantum information is explored. At the same time, extensive effort has been put into realizing these techniques. Through advances in NMR, optical cavities and ion traps, several quantum algorithms have been experimentally verified [NC10]. This process is however still slow, and scaling up the number of qubits in a physical device to make a large-scale quantum computer is still some time into the future.

1.3 Motivation

The motivation for this work can be understood from two perspectives. In the arena of quantum cryptography, understanding the effects of imperfections is immensely important, not only from a theoretical standpoint, but also for bridging the gap between the analytical proofs and real-world implementations. In a broader sense, the field of cryptography *in general* also underpins the information infrastructure of modern society. In a world of increasingly specialized research, it can be helpful to take a step back and assess the work’s social implications.

1.3.1 Social importance

As indicated in the previous section, the development of cryptography has played an important role in our history and science. Today, its importance also comes from the last decades explosive expansion of the use of digital networks and devices. In step with the proliferation of the Internet, an ever-growing number of our social and commercial arenas are now digital and perpetually interconnected. Cryptography stands as one of the cornerstones to these applications as it provides procedures such as access control, message confidentiality and user identification. In this way, cryptography has gone from being a tool employed by military and intelligence organizations, to being the workhorse of all our digital communication systems. Its importance does however go much deeper, and the use of pseudo-randomness, one-way functions, hashing and digital signatures clearly shows how interconnected cryptography is to our information systems.

There is however an unsettling gap between the reliance on and the theoretical foundation of modern cryptography; despite their widespread use, the most commonly deployed cryptographic protocols, such as RSA, is not strictly known to be secure. In line with the earlier discussion of security classes, modern cryptographic techniques typically aim for attaining *computational* security. The RSA algorithm fits into this paradigm nicely as it relies on the computational hardness of integer factorization, for which there is currently no known, feasible³, efficient algorithm. The existence of an efficient factoring algorithm has however never been disproved, meaning that although RSA has been extensively tested, its security currently has no formal proof. Furthermore, even if we were to successfully identify the complexity class of integer factorization, the broader problem of determining whether $\mathbf{P} \neq \mathbf{NP}$ still prevents the formal security proof. Moreover still, cryptographic protocols whose proofs rely on computational security are potentially vulnerable to advances in computational power. Although such advances are usually gradual, the discovery of Shor's algorithm is an example of precisely this worry [SP00].

Quantum information theory brings with it the promise of a solution to this obstacle. After the publication of the BB84 protocol, and its subsequent analyses and proofs, it became apparent that quantum cryptography allows for *unconditional security*. Specifically this applies to protocols of quantum key distribution (QKD), that is cryptographic techniques utilizing a public quantum communication channel in order to establish a secret key between two parties. Even when allowing for *any* attack by the eavesdropper, the proofs assert the security of QKD. This means that the protocol offers not only computational security, but remains secure against an attacker with *arbitrary* computational power. Granted, it relies on our laws of physics being correct, as well as on the actual protocol being correctly implemented (as is always the case); however, as long as these conditions are met, QKD will resist any attacks, including new mathematical algorithms for integer factoring or advances in computational power.

In this way, quantum information theory is expanding our understanding of the theoretical

³We are here referring to *classical* algorithms.

foundation of cryptography. One of its most important features however comes from the fact that it is not only attainable in theory; rather, the quantum theory provides us with the tools to exploit this power for cryptographic purposes in real life. Unlike with the construction of large-scale quantum computers, which seems unattainable for the foreseeable future, quantum cryptography can be physically realized today. In fact, there are already commercial systems available (see Section 4.1).

1.3.2 Importance to the field

There is however still a gap between the theoretical protocols with unconditional security, and actual, operational systems. The BB84 protocol makes several assumptions about the apparatus, e.g. that it leaks no information about the basis choice and that the source and detector are perfect. This is however, of course unattainable in practice; imperfections in the source and detector will always exist, even if they are very small.

The original proposal of the BB84 protocol [BB84] also provided the first proof of its security. This was however limited to certain types of attacks [SP00] and thus did not yet reveal the true power of quantum cryptography. One of the earliest proofs of *unconditional security* of BB84 was provided by [May96], which also had the additional benefit of allowing for an *uncharacterized* detector, as long as the detector's efficiency is basis-independent. It has since become a highly desirable feature of security proofs to allow for the apparatus to be uncharacterized, since it is indeed impossible to fully represent all the degrees of freedom in a real device [KP03].

One disadvantage of [May96] is however the complexity of the proof [Koa09]. An approach which is much easier to follow was given by [LC99], although it requires a quantum computer to run the protocol [SP00]. A security argument without this requirement was then given in [SP00], which provided a simple proof based on reduction to an entanglement protocol and quantum error correcting codes (QECC) [Koa09]. This proof however assumes that the imperfections of the apparatus could always be absorbed into Eve's basis-independent attack [KP03]. Finally, [KP03] combined the efforts of [SP00] and [May96] and described a complementarity-based proof allowing for uncharacterized *sources*.

Much research has later been directed towards imperfect devices, particularly looking at security when their operation is *basis-dependent*. A proof for uncharacterized sources with basis-dependent imperfections was given by [Koa06]. This also has the advantage of avoiding the use of QECC by decoupling the error correction and the privacy amplification by classical encryption techniques [Lo03]. The case of imperfections in both the source and detector was analyzed in [Got+04], although it only allowed for limited detector imperfections [MLS10b]. Recent work has been done to cover arbitrary imperfections in both the source and detector [MLS10b].

All the above proofs however are limited to imperfections that are *uncorrelated*. This means that even though the devices can be fully uncharacterized except for a few parameters, their

operation must be completely independent from earlier signals [MLS10b]. The effects of correlations on the apparatus is largely an open problem, although it is not immediately clear how such correlations can be attacked. We aim to investigate the necessity of requiring individual imperfections in the security of quantum key distribution.

1.3.3 Personal motivation

Lastly, a word about the personal motivation for this work. I consider myself incredibly lucky to be given the opportunity to work on this project. Quantum information science is truly a unique field, where my fascination for physics can be combined with the prospect of immediate applications of great social importance.

1.4 Structure of this document

This document is divided into 8 chapters. Chapter 2 and Chapter 3 is largely a review of material from [NC10]. To avoid cluttering the text, explicit references to this work have been omitted, but these chapters are to be understood as both implicitly referencing it.

Chapter 1 (this chapter) has introduced the core principles of cryptography, outlined its historical developments and presented the motivation for its study. Then an overview of other work related to this was given.

Chapter 2 introduces the fundamental concepts of quantum computation, starting from the postulates of quantum mechanics and quantum measurement. It also introduces density operators, composite systems, quantum circuits and some important theorems for analyzing quantum systems.

Chapter 3 gives a detailed account of chosen topics from quantum information theory, including the quantum operation formalism and quantum state distance measures. A comprehensive introduction to classical and quantum entropy is also provided.

Chapter 4 introduces the application of quantum communication channels for cryptographic purposes, covering quantum key distribution and the modern security definition. The definition of the BB84 protocol is then provided, before presenting a detailed review of its security proof by [Koa09].

Chapter 5 describes the formalism used to describe devices that have basis-dependent imperfections, specifically generalizing the operation of the source. It is then argued that security is still guaranteed as long as the source states are *independent*, but it is not immediately clear whether this restriction is in fact necessary.

Chapter 6 then investigates this claim by numerical procedures. Various algorithms are described and the outcomes are provided in plots or in listings in Appendix A. The results show concrete counterexamples to the previous claim, even for realistic conditions.

Chapter 7 presents an analysis of the numerical findings. First, the validity of the results is addressed, in the context of the theoretical model. Then the assumptions of the model are evaluated, motivating the interpretation of the main results. Finally, suggestions for further work is provided.

Chapter 8 concludes this document and attempts to summarize the work, its results and its consequences.

Chapter 2

Fundamentals

Before presenting topics from quantum information and then quantum cryptography, a review of the fundamentals is included. The underlying theory is that of quantum computation, which combines computer science and physics to analyze computing systems exhibiting quantum effects [NC10]. It relies heavily on results from linear algebra, which is assumed to be known at the level of operator functions and singular value decomposition in finite dimensions. Although some of the topics in this chapter are considered rudimentary, they are included here for completion and because their interpretation are crucial for the later topics.

This chapter reviews some fundamentals concepts in the theory of quantum computation, starting at the postulates of quantum mechanics, quantum operators and quantum measurement. Then the topic of density operators is introduced, together with their connection to composite quantum systems and purification. A summary of the quantum circuit model is also presented, before the chapter is concluded with a few, useful theorems about quantum systems.

2.1 Quantum mechanics

Quantum mechanics is a framework for describing the physics of the very small. It exhibits a range of counterintuitive properties such as superposition of states, inherent randomness, history creation, and non-locality. This section presents the postulates of quantum mechanics and outlines some of their immediate consequences.

2.1.1 Postulates

Quantum mechanics can be formulated in a variety of ways. We will begin with the formulation of physical postulates [NC10] that mostly assert which mathematical framework correctly represents the physical quantum reality.

Postulate 1. Any *isolated* physical system is associated with a complex, complete inner-product space (*Hilbert space*) \mathcal{H} , called the *state space*. The state of the system is completely characterized by a complex unit vector $|\psi\rangle$ in this vector space.

A system is considered isolated when it is not interacting with any other system. We will restrict ourselves to the case of \mathcal{H} being finite-dimensional, which is equivalent to the physical system having a finite number of discrete degrees of freedom.

Postulate 2. The state of an isolated quantum system evolves in time from an initial state $|\psi(t = t_0; t_0)\rangle$ to a final state $|\psi(t = t_1; t_0)\rangle$ according to

$$|\psi(t = t_1; t_0)\rangle = U(t_1, t_0) |\psi(t = t_0; t_0)\rangle, \quad (2.1)$$

where $U(t_1, t_0)$ is a unitary operator on the state space that only depends on the initial and final times.

Furthermore, if the dynamics can be described by continuous time, then the time evolution of the state $|\psi\rangle$ is governed by the *Schrödinger equation*

$$i\hbar \frac{d|\psi\rangle}{dt} = H |\psi\rangle, \quad (2.2)$$

where \hbar is the reduced Planck constant and H is known as the *Hamiltonian* of the system.

Postulate 3. A quantum measurement is characterized by a set $\{M_m, m\}$ where m labels the possible outcomes of the measurement. To each label m there is a corresponding linear operator on the state space denoted M_m called a *measurement operator*. The measurement operators must satisfy the completeness relation

$$\sum_m M_m^\dagger M_m = I. \quad (2.3)$$

A measurement on $|\psi\rangle$ produces, at random, *one* of the results m with probability

$$p(m) = \|M_m |\psi\rangle\|^2 = \langle\psi| M_m^\dagger M_m |\psi\rangle \quad (2.4)$$

and maps the state $|\psi\rangle$ to $|\psi_m\rangle$ immediately after the measurement, given by

$$|\psi_m\rangle = \frac{M_m |\psi\rangle}{\sqrt{p(m)}} = \frac{M_m |\psi\rangle}{\sqrt{\langle\psi| M_m^\dagger M_m |\psi\rangle}}. \quad (2.5)$$

It is seen from the spectral decomposition theorem that the often-used condition of quantum observables being represented by Hermitian operators is a special case of the quantum measurement postulate. Postulate 3 is however more general, describing all possible measurement

processes allowed in physics.

Postulate 4. A *composite* physical system, made out of combining distinct component systems with state spaces $\{\mathcal{H}_i\}_{i=1}^n$, is described by a composite state space \mathcal{H} constructed from the tensor product of the component systems

$$\mathcal{H} = \bigotimes_{i=1}^n \mathcal{H}_i. \quad (2.6)$$

If the component systems are all in definite states $|\psi\rangle_1, |\psi\rangle_2, \dots, |\psi\rangle_n$ respectively, the state of the composite system $|\psi\rangle$ is similarly given by the tensor product

$$|\psi\rangle = |\psi\rangle_1 \otimes |\psi\rangle_2 \otimes \dots \otimes |\psi\rangle_n. \quad (2.7)$$

The full range of implications of these postulates is contained in the mathematical properties of their various components, such as Hilbert space, unitary operators and tensor products. The basic properties of these mathematical objects are assumed known.

2.1.2 Physical consequences

Some important physical consequences can already be seen from the postulates of quantum mechanics:

- Superposition

Because the state space of quantum systems is a linear vector space, the states of the system satisfy the *superposition principle*. This means that linear combinations of valid states are also all valid states. This gives the notorious notion of quantum objects being in “two places at once”.

- Operator Linearity

Both time evolution and measurement is described by linear operators. This means that any physical operation, including quantum gates, is described by an appropriate *linear operator* on the state space.

- Reversibility

An important property of a unitary operator is its guaranteed, well-defined inverse, namely its adjoint. Since time evolution in quantum systems is described by a unitary operator, this has the consequence that any physical operation, except measurement, is in theory completely reversible. In particular it means that any quantum gate must be reversible, unlike classical logic gates.

The notable exception of measurement to this property is one of the more unsettling aspects of quantum mechanics, often treated under the term “wave function collapse”. This means that a measurement represents something fundamentally different from

time evolution, and measuring some quantity will potentially subject the system to irreversible change.

- Randomness

A quantum measurement is described by a set of outcomes and corresponding operators that predict *probabilities* for these outcomes. Yet, the action of performing a measurement has no dynamic process assigned to it. Instead the outcome is said to be selected *at random*, as if modeled by a random variable. This assertion of an intrinsic randomness in quantum mechanics can be hard to grasp, and its interpretation has bothered many minds in pursuit of understanding quantum mechanics.

An important pitfall should be avoided here: quantum processes are not random. Time evolution is not only completely deterministic, but also always reversible. Only when the system is *measured* does the randomness manifest. This paradoxical interplay between the inherent randomness of measurement and the reversible, determinism of time evolution is at the very heart of quantum mechanics [NC10].

In summary, it is seen that the stage of quantum mechanics is set in a complex vector space, its states described by vectors, its physical operations by linear operators and its measurement dynamics by random processes. The study of quantum mechanics is thus intimately tied to the study of linear vector spaces and random variables.

2.1.3 The qubit

In classical logic the basic unit of information is labeled a *bit*. It takes a single binary value, either 0 or 1. Together with the classical logic operators of conjunction, disjunction and negation, it forms a Boolean algebra. In this framework states are discrete, and operations and systems are characterized by logic tables.

In the quantum world the basic unit of information is label a *qubit*, short for quantum bit. It manifests as the state of the simplest quantum system imaginable: a state space allowing only two states $|0\rangle$ and $|1\rangle$. Although seemingly identical to the classical case, quantum systems are not characterized by logic tables, but rather a complex linear vector space. This has the pivotal consequence that the state of the system cannot only take on the two base states, but in fact any *linear combination* of them

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{2.8}$$

where α and β are arbitrary complex numbers satisfying the normalization condition $|\alpha|^2 + |\beta|^2 = 1$. Equation 2.8 is indeed the defining equation for the qubit. The state space of a qubit will typically be denoted as $\mathcal{K} \ni |\psi\rangle$.

As a short precaution, it should be noted that this is not only a funny mathematical abstraction, but can be achieved physically. Using trapped ions for instance, a state space can

be achieved that has this property, and in this way the qubit is made real.

Unlike the classical bit, it is not immediately clear how much information a qubit encodes. Since α and β are arbitrary complex constants, an *infinite* amount of information could in theory be encoded in their binary expansion. This however has the caveat that any measurement will necessarily only reveal one *classical* bit of information about the state [NC10]. Thus to determine α and β to arbitrary precision and thus recovering the infinite amount of information encoded in them would require an infinite number of measurements on an infinite number of prepared copies of the state.

This “infinite” amount of information is however somehow contained in the state as long as it is not measured. Although not directly accessible, the exact values of α and β certainly matter and have physically real consequences. This duality of the discrete and the continuous nature of quantum systems and the “hidden” information of infinite precision they encode is one of the fundamental concepts of quantum information.

2.1.4 Interpreting uncertainty

Probability typically arises in two different contexts, each with their own corresponding interpretation. In the context of repeated experiments, probabilities assigned to various outcomes are interpreted as that in the limit of a large number of trials, the relative frequency of the particular outcome approaches its assigned probability value. In the context of information theory, probabilities represent knowledge, or rather lack of knowledge, about a system. Associated with this last interpretation is the notion of *uncertainty*, understood as the lack of distinguishability between unknown, distinct possibilities.

Classically, there is no clear notion of objective uncertainty, as the laws of physics in theory completely determine any physical process. For a collection of trials however, it is possible to introduce probabilities to different possibilities. This is not to be understood as implying that there is a lack of distinguishability in any particular trial; in fact it is always completely determined. Rather, it is a mathematical tool which allows subsequent effects to be assigned probabilities, which give the expectation values of the relative frequency they will occur at in repeated trials.

Quantum mechanics introduces the concept of an intrinsic uncertainty, a lack of knowledge not by the observers, but by the state itself. A quantum state can be repeatedly prepared to give probabilistic random outcomes when measured, yet the initial state is understood as completely determined. In particular, this uncertainty is present for all (possible) observers.

When analyzing quantum systems it is frequently desirable to subject the system also to classical uncertainty, e.g. when modeling quantum noise. In these cases it is important to keep in mind the physical origin of the various uncertainties and probabilities in the model.

2.2 Quantum computation

Quantum computation is the study of physical systems exhibiting quantum effects, with states used for encoding information. This is most naturally done by constructing a physical state space consisting of a collection of qubits and analyzing operations on these through the framework of linear algebra. This section reviews basic quantities and techniques used to describe quantum computation, such as quantum operators, quantum measurement and density operators. A table of quantum circuit elements is also given. Lastly, three highly useful theorems on general measurement implementation, no-cloning and deferred measurements are stated.

The state space V_i for a single qubit is one that allows only two base states $|0\rangle_i$ and $|1\rangle_i$. In line with Postulate 4, the state space for n qubits is then formed as the tensor product of single-qubit spaces $V = \bigotimes_{i=1}^n V_i$ with corresponding basis $\{|i_1 i_2 \dots i_n\rangle\}_{i_1, i_2, \dots, i_n}$. Choosing the *computational basis* $\{|00\dots 0\rangle, |00\dots 1\rangle, \dots, |11\dots 1\rangle\}$ as convention has the consequence that states, functionals and operators can be uniquely represented by vectors and matrices.

Some useful quantum states are:

$$\left. \begin{aligned} |+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned} \right\} X\text{-basis states} \quad (2.9)$$

$$\left. \begin{aligned} |\psi_-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \\ |\psi_+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\ |\phi_-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ |\phi_+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \end{aligned} \right\} \text{Bell states} \quad (2.10)$$

2.2.1 Bloch sphere

Recall Equation 2.8 for the qubit: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, which has a total of 4 real parameters (2 complex). Considering the constraint $|\alpha|^2 + |\beta|^2 = 1$ and noting that global phase has no physical significance, the expression for the qubit can be decomposed as

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle, \quad (2.11)$$

which is characterized by only 2 cyclic parameters $\theta, \phi \in \mathbb{R}$. This allows a pleasant visualization of one qubit as a point on a spherical shell of unit radius.

2.2.2 Operators

The dimensionality of linear operators on a single qubit is $2^2 = 4$. A conventional basis for single-qubit operators is the $\{I, X, Y, Z\}$ -basis, given by

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad (2.12)$$

where X, Y, Z are known as the Pauli matrices, also denoted $\boldsymbol{\sigma} = [X, Y, Z]$. They are Hermitian and unitary but not positive, with properties

$$[\sigma_i, \sigma_j] = 2i\varepsilon_{ijk}\sigma_k \quad (2.13)$$

$$\{\sigma_i, \sigma_j\} = 0 \quad (2.14)$$

$$\sigma_i\sigma_j = \delta_{ij}I + i\varepsilon_{ijk}\sigma_k. \quad (2.15)$$

In this document, linear operators on a Hilbert space V will be denoted $\mathcal{L}(V)$.

Postulate 2 states that quantum operations on a single qubit are described by unitary operators $U \in \text{U}(2)$, which has the general matrix representation

$$U = \begin{bmatrix} a & b \\ -e^{i\theta}b^* & e^{i\theta}a^* \end{bmatrix}; \quad |a|^2 + |b|^2 = 1, \quad (2.16)$$

with $a, b \in \mathbb{C}$ and $\theta \in \mathbb{R}$. It can be decomposed as

$$\begin{aligned} U &= e^{i\alpha} \begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix} \begin{bmatrix} \cos(\frac{\gamma}{2}) & -\sin(\frac{\gamma}{2}) \\ \sin(\frac{\gamma}{2}) & \cos(\frac{\gamma}{2}) \end{bmatrix} \begin{bmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{bmatrix} \\ &= e^{i\alpha} R_Z(\beta) R_Y(\gamma) R_Z(\delta), \end{aligned} \quad (2.17)$$

for $\alpha, \beta, \gamma, \delta \in \mathbb{R}$. The operators $R_{X_i}(\theta)$ are rotations about the \hat{X}_i -axis as visualized on the Bloch sphere. This decomposition is equivalent to the concept of Euler angles.

Rotations on the Bloch sphere of an angle θ about an arbitrary $\hat{\mathbf{n}}$ -axis is generated by

$$R_{\hat{\mathbf{n}}}(\theta) = e^{-i\frac{\theta}{2}\hat{\mathbf{n}}\cdot\boldsymbol{\sigma}} = \cos\left(\frac{\theta}{2}\right)I - i\sin\left(\frac{\theta}{2}\right)\hat{\mathbf{n}}\cdot\boldsymbol{\sigma}. \quad (2.18)$$

Note that the factor $\frac{\theta}{2}$ gives the correct expression for a rotation of θ .

2.2.3 Measurement

As noted in Postulate 3, quantum measurement is described by a collection of *measurement operators* $\{M_m\}$ satisfying the completeness relation $\sum_m M_m^\dagger M_m = I$, which predict probabilities for each measurement outcome as well as the associated post-measurement state. Also note that the case of just a single measurement operator (only one possible

outcome) implies it must be unitary, and as such the measurement operators also describe any quantum operation.

If a system is left in an unknown but definite state, measurement can be used to determine in which state the system is. A measurement can always be made which will never give an incorrect value, but only in the case of distinguishing orthogonal states can the measurement be guaranteed to succeed. Non-orthogonal states cannot be perfectly distinguished by measurement, as there will always be either a non-zero probability of obtaining an incorrect value, or a non-zero probability of obtaining no value at all.

Projective measurement

A special class of measurement is known as *projective measurement*.

Definition 2.1. A projective measurement is represented by a set of *orthogonal projectors* $\{P_m\}$; $P_m P_{m'} = \delta_{m,m'} P_m$ that satisfy the completeness relation $\sum_m P_m = I$.

Alternatively, it is also described by an *observable*: a Hermitian operator M , that has spectral decomposition

$$M = \sum_m m P_m, \quad (2.19)$$

where P_m is the projector onto the eigenspace of M with eigenvalue m . Both representations are equivalent.

The probability of obtaining outcome m when measuring state $|\psi\rangle$ is then

$$p(m) = \langle \psi | P_m | \psi \rangle, \quad (2.20)$$

with post-measurement state

$$|\psi_m\rangle = \frac{P_m |\psi\rangle}{\sqrt{p(m)}}. \quad (2.21)$$

There is furthermore a convenient expression for the expectation value of the observable M , given by

$$\langle M \rangle = \sum_m m p(m) = \langle \psi | M | \psi \rangle, \quad (2.22)$$

which is sometimes misunderstood as valid for all measurement.

The concept of “measuring in basis $|m\rangle$ ”, where $\{|m\rangle\}$ is an orthonormal basis, simply refers to a projective measurement with projectors $P_m = |m\rangle \langle m|$.

Projective measurement on a single qubit can visualized as measuring along a particular axis of choice \hat{n} on the Bloch sphere. The observable for this measurement is then given by

$$M_{\hat{n}} = \hat{n} \cdot \boldsymbol{\sigma}, \quad (2.23)$$

with eigenvalues ± 1 and corresponding projectors $P_{\pm 1} = (I \pm \hat{n} \cdot \boldsymbol{\sigma})/2$.

Comparing with the general measurement operators M_m , it is seen that projective measurement corresponds to the special case of the different M_m 's being projectors as well as being orthogonal. Although projective measurement corresponds nicely to easily realizable physical measurements, there are measurement processes that can only be described by the general operators M_m .

An important difference between general and projective measurements regards the question of repeatability. When performing the same measurement repeatedly on the same system, a general measurement $\{M_m\}$ will generally give different outcomes, whereas the outcomes of a repeated projective measurement $\{P_m\}$ will always be the same.

POVM measurement

Another class of measurement is known as *POVM* (Positive Operator-Valued Measure) measurement.

Definition 2.2. A POVM measurement is described by a set $\{E_m\}$ of *positive* operators E_m , known as *POVM elements*, satisfying the completeness relation $\sum_m E_m = I$.

The probability of outcome m is then given by

$$p(m) = \langle \psi | E_m | \psi \rangle. \quad (2.24)$$

By inspection of Postulate 3 it is seen that the POVM elements can be constructed from the general measurement operators as

$$E_m = M_m^\dagger M_m. \quad (2.25)$$

By the uniqueness of the square root of a positive linear operator, the measurement operators M_m can also easily be constructed from the POVM elements. Since both representations can easily and uniquely be converted to each other it is evident that they are equivalent and can both describe any form of general physical measurement.

2.2.4 Density operators

The postulates of quantum mechanics were formulated with states represented by vectors. This is a very common starting point, as it is perhaps the most intuitive and mathematically straightforward approach. There is however an alternative formalism for representing quantum states, namely the *density operator*. It captures the notion of a quantum state in a mathematically equivalent manner as the vector formalism, but offers more powerful methods for treating probabilistic mixtures of states.

A quantum state that can be described by a vector $|\psi\rangle$ is termed a *pure state*. All states

encountered so far have been pure states. In general the exact state of a system may not be known, but rather it is known to be in *one of several possible* states $|\psi_1\rangle, |\psi_2\rangle, \dots$ with corresponding probabilities p_1, p_2, \dots . Such a probabilistic state *ensemble* is specified by a set of possible states and probabilities as $\{p_i, |\psi_i\rangle\}$ and has an associated density operator

$$\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i|. \quad (2.26)$$

Note that any pure state $|\psi\rangle$ consequently has its corresponding density operator given simply by the outer product $|\psi\rangle \langle \psi|$. As such, the density operator is able to represent any quantum state encountered so far, as well as probabilistic mixtures of these states. A quantum state whose density operator cannot be represented as an outer product is said to be *mixed*.

It is easily shown that Equation 2.26 implies two universal, important properties for any density operator ρ . First, it is a positive operator, meaning that all its eigenvalues are non-negative. Second, it has unit trace: $\text{tr}(\rho) = 1$. Moreover, any density operator corresponding to a pure state will always satisfy the condition $\text{tr}(\rho^2) = 1$, whereas a mixed state satisfies $\text{tr}(\rho^2) < 1$.

In general it is not convenient to require density operators to be defined in terms of the underlying ensemble. Equivalent to the fact that any density operator satisfies positivity and unit trace, it is easily shown that the reverse also holds. Thus, any operator satisfying these properties will necessarily correspond to a state ensemble, and hence forms a suitable requirement for the general definition of the density operator.

Definition 2.3. A density operator is a *positive* operator ρ with unit trace: $\text{tr}(\rho) = 1$.

In this document, the set of all density operators on Hilbert space V will be denoted by $\mathcal{P}(V)$.

Postulates

All the defining postulates of quantum mechanics can now be reformulated in terms of density operators. Time evolution of a closed quantum system is described by a unitary operator U which evolve the initial state ρ to a final state ρ' according to

$$\rho' = U\rho U^\dagger. \quad (2.27)$$

Quantum measurement is described by a set of measurement operators $\{M_m\}$ that satisfy the completeness relation in Equation 2.3. The probability of obtaining result m is then

$$p(m) = \text{tr}(M_m^\dagger M_m \rho), \quad (2.28)$$

with corresponding post-measurement state

$$\rho_m = \frac{M_m \rho M_m^\dagger}{p(m)} = \frac{M_m \rho M_m^\dagger}{\text{tr}(M_m^\dagger M_m \rho)}. \quad (2.29)$$

Finally, the state ρ of a composite physical system with component states $\rho_1, \rho_2, \dots, \rho_n$ is given by

$$\rho = \rho_1 \otimes \rho_2 \otimes \dots \otimes \rho_n. \quad (2.30)$$

Unitary freedom

An important property of density operators is their non-bijective mapping to the state ensembles. In fact, any given density operator can correspond to many different ensembles. The precise condition for when two different ensembles generate the same density operator turns out to rely on *unitary transformations*.

Theorem 2.4 (Density operator freedom). *The two state ensembles $\{p_i, |\psi_i\rangle\}$ and $\{q_j, |\phi_j\rangle\}$ generate the same density matrix if and only if*

$$\sqrt{p_i} |\psi_i\rangle = \sum_j u_{ij} \sqrt{q_j} |\phi_j\rangle, \quad (2.31)$$

for some unitary matrix with components u_{ij} , and whichever set of vectors is smallest has additional 0-vectors added to it to make the sets have the same number of elements.

Remark. Note that this implies that density matrices for pure states have a unique ensemble interpretation.

Figure 2.1 gives an overview of some important mathematical properties of various quantities encountered in this section.

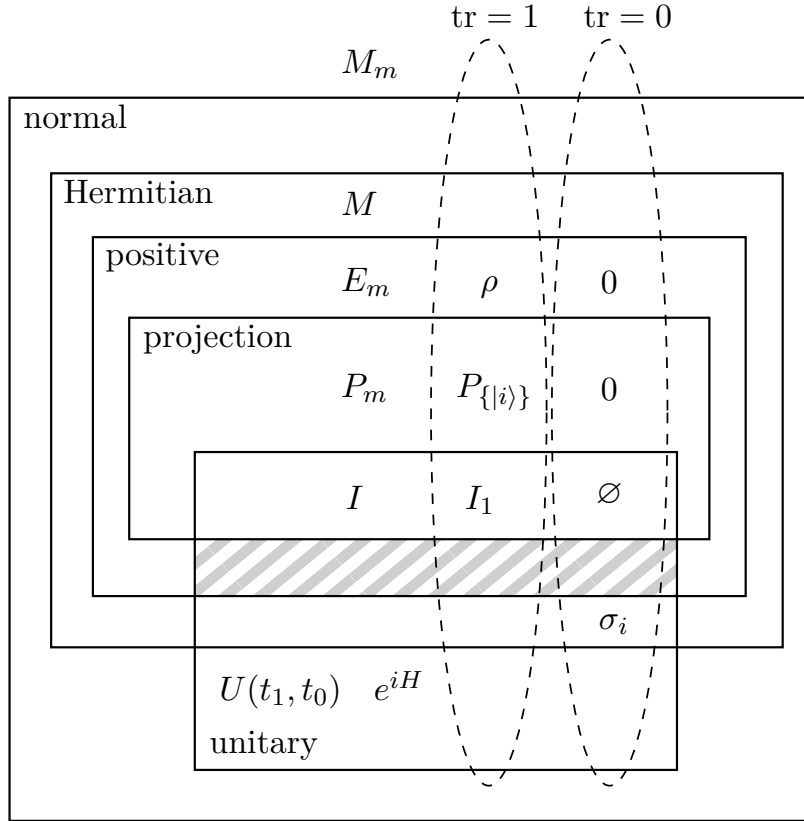


Figure 2.1: Euler diagram of properties of common quantities in quantum computation:

- M_m : measurement operator
- M : observable
- E_m : POVM element
- P_m : projective measurement operator
- $U(t_1, t_0)$: time development operator
- e^{iH} : exponentiated skew-Hermitian operator
- ρ : density matrix
- $P_{\{|i\rangle\}}$: projective measurement operator to a one-dimensional vector space
- I_1 : one-dimensional identity operator
- σ_i : Pauli matrix

2.2.5 Composite systems and entanglement

When multiple systems are put together to form a composite system, it is convenient to distinguish between the different types of states in which it can be. If the component states $|\psi\rangle_A \in V_A$ and $|\psi\rangle_B \in V_B$ are known, it is postulated in Equation 2.7 that the composite state $|\psi\rangle_{AB} \in V = V_A \otimes V_B$ is simply $|\psi\rangle_{AB} = |\psi\rangle_A \otimes |\psi\rangle_B$. However, this does not include all possible states in which the composite system can in fact be.

If $\{|e_k\rangle_A\}_{k=1}^n$ and $\{|e_l\rangle_B\}_{l=1}^m$ form bases for V_A and V_B respectively, their tensor product $\{|e_k e_l\rangle_{AB}\}_{k=1, l=1}^{k=n, l=m}$ forms a basis for the composite space V . Hence any possible state can

be expanded in this basis

$$|\psi\rangle_{AB} = \sum_{k,l} c_{kl} |e_k e_l\rangle_{AB}. \quad (2.32)$$

In general it is possible that there is no $|\psi\rangle_A \in V_A$ and $|\psi\rangle_B \in V_B$ such that $|\psi\rangle_{AB} = |\psi\rangle_A \otimes |\psi\rangle_B$. In that case $|\psi\rangle$ is known as an *entangled state*.

A mixed state of a composite Hilbert space $V = V_A \otimes V_B$ is described by a density operator $\rho^{AB} \in \mathcal{P}(V)$. If this state can be expanded as a probabilistic mixture of component states

$$\rho^{AB} = \sum_i p_i \rho_i^A \otimes \rho_i^B; \quad \sum_i p_i = 1, \quad (2.33)$$

for $p_i > 0$ and $\rho_i^A \in \mathcal{P}(V_A)$, $\rho_i^B \in \mathcal{P}(V_B)$ it is called *separable* [Hay06]. If it cannot be written in this form it is an entangled state.

Similarly, measurements on the composite space V are given by a set of operators $\{M_m\}$. If it can be expanded in terms of measurement operators M_i^A and M_i^B on only the component systems V_A and V_B respectively as

$$M_m = \sum_i M_i^A \otimes M_i^B \quad (2.34)$$

it is called separable. Otherwise it is a *collective measurement* [Hay06].

Reduced density operator

A common task when dealing with a composite system $V = V_A \otimes V_B$ is to describe the dynamics of only one part of the system, say V_A . The dynamics of V_B are not relevant in this case and may not even be known at all. Due to the non-local structure of quantum mechanics, it is however not immediately clear that such a construction is possible; the state in V_A does in general depend on processes and measurements applied to V_B if the states are initially entangled. It is nevertheless possible to find a density operator that correctly predicts the physics of only interacting with V_A , namely the *reduced density operator*

$$\rho^A = \text{tr}_B(\rho^{AB}), \quad (2.35)$$

where the partial trace is defined as a linear map such that

$$\text{tr}_B(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) \stackrel{\text{def}}{=} |a_1\rangle\langle a_2| \text{tr}(|b_1\rangle\langle b_2|). \quad (2.36)$$

The use of reduced states must however be carefully applied in order to ensure a correct description. In particular, a reduced state on one subsystem can only be used to predict probabilities on that subsystem. Formally, let $V = V_A \otimes V_B$ be a composite system in the state ρ^{AB} . Now, label any event on system V_A by A_i and any event on system V_B by B_i . Then the reduced state ρ^A can only be used to predict probabilities of the form $p(A_i)$,

and ρ^B to predict probabilities $p(B_i)$. Predicting probabilities across both systems, such as $p(A_i, B_j)$ or $p(A_i|B_j)$ cannot be done using either reduced state, but only from the total state ρ^{AB} . As the models get more complex, it is important to keep this principle in mind.

Schmidt decomposition and purification

This section is concluded with two key theorems for composite quantum systems. The first, Schmidt decomposition, provides a convenient rephrasing of Equation 2.32 with some important consequences.

Theorem 2.5 (Schmidt decomposition). *Consider a composite system $V = V_A \otimes V_B$ where V_A and V_B have the same dimensionality n . For any pure state $|\psi\rangle \in V$ there exists orthonormal bases $\{|e_i\rangle_A\}_{i=1}^n$ and $\{|e_i\rangle_B\}_{i=1}^n$ for V_A and V_B respectively, such that*

$$|\psi\rangle = \sum_{i=1}^n \lambda_i |e_i\rangle_A |e_i\rangle_B, \quad (2.37)$$

where the Schmidt coefficients λ_i satisfy $\lambda_i \geq 0$ and $\sum_i \lambda_i^2 = 1$.

The bases $\{|e_i\rangle_A\}$ and $\{|e_i\rangle_B\}$ are known as the *Schmidt bases* under $|\psi\rangle$ for V_A and V_B respectively. The number of non-zero Schmidt coefficients λ_i , known as the *Schmidt number* for $|\psi\rangle$, quantifies the entanglement $|\psi\rangle$ exhibits between the component systems. If $|\psi\rangle$ is maximally entangled, the Schmidt number equals the dimensionality of the component space.

A very useful technique related to the Schmidt decomposition is the *purification* of a mixed quantum state $\rho^A \in \mathcal{P}(V_A)$. Since ρ^A is positive, its spectral decomposition $\rho^A = \sum_i p_i |e_i\rangle_A \langle e_i|$ defines an orthonormal basis $\{|e_i\rangle_A\}$ for V_A . Introducing an ancilla system V_B with the same state space as V_A it is clear that it has the same orthonormal basis $\{|e_i\rangle_B\}$. The *purification* $|\psi\rangle_{AB}$ of ρ^A into $V_A \otimes V_B$ is then defined

$$|\psi\rangle_{AB} = \sum_i \sqrt{p_i} |e_i\rangle_A |e_i\rangle_B. \quad (2.38)$$

The usefulness of Equation 2.38 is captured in the following theorem.

Theorem 2.6 (Purification). *The reduced density operator on V_A of the purification $|\psi\rangle_{AB}$ of $\rho^A \in \mathcal{P}(V_A)$, is equal to ρ^A , i.e.*

$$\text{tr}_B(|\psi\rangle_{AB} \langle \psi|_{AB}) = \rho^A. \quad (2.39)$$

2.2.6 Quantum circuits

Quantum circuit diagrams are a frequent tool for designing and analyzing quantum processes. In this model, one qubit is represented by a single wire. Then various gates on the qubits are added left to right, according to the sequential steps of the algorithm or protocol in question. Note that fan-out, fan-in or loops are not permitted in the diagrams, as they do not correspond to anything real. Finally measurement elements are given for the qubits that produce the desired output of the algorithm.

Tables of the standard quantum circuit elements are given below.

Table 2.1: Basic quantum circuit elements.


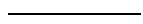
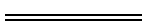
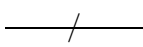
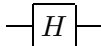
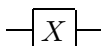
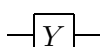
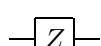

Name	Circuit element
measurement	
qubit	
classical bit	
multiple qubits	

Table 2.2: Single-qubit quantum gates.

Name	Circuit element	Matrix
Hadamard		$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Pauli-X (NOT)		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Phase (\sqrt{Z})		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$


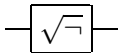
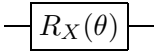
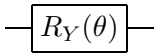
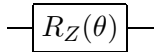

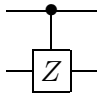
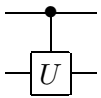



$\pi/8$ ($\sqrt[4]{Z}$)		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
$\sqrt{\text{NOT}}$ (\sqrt{X})		$\frac{1}{2} \begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix}$
X-rotation		$\begin{bmatrix} \cos(\frac{\theta}{2}) & -i \sin(\frac{\theta}{2}) \\ -i \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{bmatrix}$
Y-rotation		$\begin{bmatrix} \cos(\frac{\theta}{2}) & -\sin(\frac{\theta}{2}) \\ \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{bmatrix}$
Z-rotation		$\begin{bmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{bmatrix}$

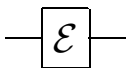
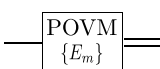
Table 2.3: Multi-qubit quantum gates.

Name	Circuit element	Matrix
CNOT (controlled- X)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
controlled- Z		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
controlled- U		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & & U \\ 0 & 0 & & \end{bmatrix}$
swap		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

Toffoli (CCNOT)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$
Fredkin (controlled-swap)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$

In addition to the conventional circuit elements, we will find it convenient to introduce a few additions. The description of some of the circuit elements are not given until later, but are included here for reference. Note also that the notation for these circuit elements has not been universally standardized and might differ from that in other works.

Table 2.4: Additional quantum circuit elements.

Name	Circuit element	Explanation
Quantum operation		Applies the quantum operation \mathcal{E} to the qubit (see Section 3.1).
POVM measurement		Performs a general POVM measurement on the qubit, given by the POVM elements $\{E_m\}$ (see Section 2.2.3).

2.2.7 Useful theorems

We conclude this chapter with a few, famous theorems. They form useful tools for analyzing all types of quantum systems, but are included here as they are most conveniently formulated in the quantum circuit formalism.

Theorem 2.7 (General measurement). *Any general measurement, described by measurement operators $\{M_m\}$, can be realized by a unitary transformation on an enlarged system, followed by a projective measurement.*

This has important consequences for the physical realization of quantum algorithms, as any general measurement can be implemented by first evolving the system together with an *ancilla* system according to some unitary operation and then performing a simple projective measurement. The ancilla system is an “extra” quantum system with the required properties and state space in question. This implementation is illustrated in Figure 2.2, where ρ denotes the initial state of the principal system, ρ_{env} denotes the initial state of the ancilla system and U denotes the total unitary operator.

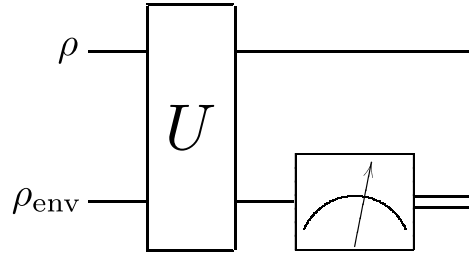


Figure 2.2: Quantum circuit for implementing a general quantum measurement: a unitary operator on an enlarged system, followed by a projective measurement.

Theorem 2.8 (Deferred measurement). *Quantum measurements can always be deferred to the end of the quantum circuit. Any classical operations, including controlled operators, that are applied to the resulting bit values can be replaced by corresponding quantum operators.*

Theorem 2.9 (No cloning). *An unknown quantum state cannot be copied. Formally, let $|\psi\rangle$ be some unknown quantum state of the principal system and $|s\rangle$ be the initial state of the target system. Then there exists no quantum operation that maps $|\psi\rangle \otimes |s\rangle \rightarrow |\psi\rangle \otimes |\psi\rangle; \forall |\psi\rangle$.*

Remark. In the case of only processing mutually orthogonal states, there does exist a quantum procedure for copying them. The previous theorem simply asserts that if one aims to construct a *single* copying machine for copying e.g. $|0\rangle$ and $|+\rangle$, this cannot be done.

Chapter 3

Quantum information

Information theory is essentially the study of the most fundamental, or most granular, pieces of information one can store or transmit. Quantum information technology (QIT) is then the application of this study to the most fundamental and granular description of the physical world. In this sense QIT describes information in its most essential form and teaches us to think physically about information and computation [NC10].

This chapter is meant to provide a detailed account of chosen topics underlying quantum cryptography. This includes the quantum operation formalism and quantum state distance measures. Then a comprehensive overview of classical as well as quantum entropy is provided. The chapter concludes with an important theorem for the transmission rate of classical information over quantum communication channels.

3.1 Quantum operations

Starting with the postulates of quantum mechanics, the above sections have developed a solid theory for describing closed quantum systems. Real systems are however rarely perfectly non-interacting with the environment, and it would be useful to be able to describe such *open* systems from a quantum mechanics perspective. This section reviews the quantum operation formalism, including the axiomatic approach and the operator-sum representation.

3.1.1 System-environment model

The procedure for describing open systems is to model its interaction with some external environment and then average over the dynamics of this environment. The system of interest is modeled by a Hilbert space Q and has some initial state $\rho \in \mathcal{P}(Q)$. It is free to interact with some other, environment system E which is in a state $\rho_{\text{env}} \in \mathcal{P}(E)$. Implicitly this assumes that the state of the total system QE is a product state $\rho \otimes \rho_{\text{env}}$, i.e. that the system is not entangled with the environment. This is a common condition satisfied for

experimental realizations, as the setup typically begins by isolating the system so that it is in fact uncorrelated with the environment. There is no restriction on the system or the environment starting in a pure state.

Creating a model for open system dynamics is relatively straight-forward by using the tools of Section 2.2.5. The evolution of the whole system-plus-environment QE follows the familiar closed system dynamics and therefore has an associated unitary time evolution operator $U \in \mathcal{L}(Q \otimes E)$. After applying the time evolution to the initial state $\rho \otimes \rho_{\text{env}}$, the density operator for the *system state*, averaged over the environment, is simply given by the partial trace. This process, as depicted in Figure 3.1, is called a *quantum operation* \mathcal{E} .

Definition 3.1. A quantum operation \mathcal{E} describes the time evolution of a open quantum system, i.e. a system interacting with an environment. \mathcal{E} maps the initial system state $\rho \in \mathcal{P}(Q)$ to $\mathcal{E}(\rho) \in \mathcal{P}(Q)$ according to

$$\mathcal{E}(\rho) = \text{tr}_{\text{env}} [U(\rho \otimes \rho_{\text{env}})U^\dagger]. \quad (3.1)$$

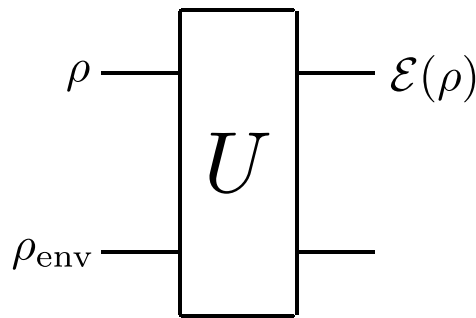


Figure 3.1: Quantum circuit of the defining process for a quantum operation: an open interaction between a system and an environment.

3.1.2 Operator-sum representation

A simple analysis of the expression in Equation 3.1 shows that any quantum operation \mathcal{E} can always be expanded as a sum of *operation elements* E_k acting only on the system Q . This is known as the *operator-sum representation*

$$\mathcal{E}(\rho) = \text{tr}_{\text{env}} [U(\rho \otimes \rho_{\text{env}})U^\dagger] \quad (3.2)$$

$$= \sum_k \langle e_k | U[\rho \otimes |e_0\rangle \langle e_0|] U^\dagger |e_k\rangle \quad (3.3)$$

$$= \sum_k E_k \rho E_k^\dagger, \quad (3.4)$$

where the vectors $\{|e_k\rangle\}$ constitute a basis for a purification of the environment, $|e_0\rangle$ is the purified initial state and E_k are any linear operators $E_k \in \mathcal{L}(Q)$ satisfying the completeness relation

$$\sum_k E_k^\dagger E_k = I. \quad (3.5)$$

It can be shown [NC10] that the maximum number of quantum operation elements necessary to describe any quantum operation on a system Q of dimensionality $\dim Q = d$ is d^2 .

This expression reveals the physical intuition behind the quantum operation formalism. The operation elements E_k can be interpreted as the general measurement operators described in Section 2.2.3. Equation 3.4 then describes a process in which a general measurement M_m is performed on the system, but the outcome m is not recorded. This is also illustrated by the difference between Figure 3.1 and Figure 2.2. This interpretation highlights how the open dynamics interaction manifests as *random noise* in the system as well as the parallels between quantum operations and classical Markov processes. It furthermore indicates that quantum operations indeed can describe all closed system dynamics, but also a whole set of processes that are not describable by closed system dynamics.

3.1.3 Axioms

A detailed analysis in [NC10] identifies three key properties of the quantum operation map \mathcal{E} from Equation 3.5, which are in turn considered axioms for the definition of quantum operations.

Axiom 3.1. Quantum operations are trace preserving, i.e. $\text{tr}(\mathcal{E}(\rho)) = 1$. Generally $\text{tr}(\mathcal{E}(\rho))$ is the probability of the process occurring, and an alternative definition which includes projective measurements on the entire system-plus-environment is possible. This alternate definition relaxes the requirement to $0 \leq \text{tr}(\mathcal{E}(\rho)) \leq 1$.

Axiom 3.2. The quantum operation map \mathcal{E} on a system Q is *convex-linear* on the density matrices, i.e.

$$\mathcal{E}\left(\sum_i p_i \rho_i\right) = \sum_i p_i \mathcal{E}(\rho_i), \quad (3.6)$$

for probabilities p_i and $\rho_i \in \mathcal{P}(Q)$.

Axiom 3.3. On a system Q , the quantum operation map \mathcal{E} for states $\rho \in \mathcal{P}(Q)$ is *completely positive*. This means that for any extra system R of arbitrary dimensionality, all positive operators $A \in \mathcal{L}(Q \otimes R)$ must remain positive, i.e. $(\mathcal{E} \otimes I)(A)$ is positive.

The analysis in [NC10] is concluded with a theorem assuring the equivalence of the operator-sum representation and the above axioms.

Theorem 3.2 (Quantum operations). *The map \mathcal{E} on Q satisfies Axiom 3.1, Axiom 3.2 and Axiom 3.3 if and only if $\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$ where the E_k 's are any linear operators on Q satisfying the completeness relation $\sum_k E_k^\dagger E_k = I$. Alternatively, if the generalized definition of \mathcal{E} is used, which includes system-plus-environment projective measurements, the condition is relaxed to $\sum_k E_k^\dagger E_k \leq I$.*

3.1.4 Operator-sum freedom

Similarly to the fact that a single density operator can correspond to a number of different pure state ensembles $\{p_i, |\psi_i\rangle\}$, there is also a freedom in the operator-sum representation. It turns out that a single underlying process $U \in \mathcal{L}(Q \otimes R)$ on the whole system-environment QR can be represented by many different sets of operator elements $\{E_k\}$. This non-uniqueness in the operator-sum representation is captured in the following theorem. The proof [NC10] is a consequence of the unitary freedom of density operators (Theorem 2.4).

Theorem 3.3 (Freedom of the operator-sum representation). *Two quantum operations \mathcal{E} and \mathcal{F} on a system Q have operator elements $\{E_i\}_{i=1}^m$ and $\{F_j\}_{j=1}^n$ respectively. Padding whichever set contains the least number of elements with zero-operators ensures that $m = n$. Then the two operations \mathcal{E} and \mathcal{F} are equal if and only if*

$$E_i = \sum_j u_{ij} F_j, \quad (3.7)$$

for some unitary matrix with elements u_{ij} .

3.2 Distance measures

Before analyzing information change in a dynamical process, it is first necessary to develop a precise procedure for measuring how “similar” two different quantum states are. Some properties, such as two equal states being the most similar, are apparent, but it is not immediately clear how to quantify the difference in general. At the same time, there is an intuitive expectation that states that produce almost the same probabilities for some measurement outcomes are indeed more “similar” than states whose outcome probabilities differ greatly. This section introduces various methods to evaluate the distance between arbitrary quantum states.

3.2.1 Classical distance measures

To motivate the quantum state distance measures, a short summary of two classical distance measures is given. Many different forms of measures are possible, both in the classical and in the quantum case, and choosing among them is simply a matter of convention. Two measures however stand out as the most popular today in quantum information science: the *trace distance* and the *fidelity*.

Classical distance measures are concerned with quantifying how different two information sources are. In accordance with Section 3.3.1, sources are understood as probability distributions. Hence, classical distance measures will be various forms of discrete “counting”

distances between probability functions.

Given two probability distributions $\{p_x\}$ and $\{q_x\}$, two common classical distance measures are:

- The *trace distance* is defined by

$$\begin{aligned} D(p_x, q_x) &= \frac{1}{2} \sum_x |p_x - q_x| \\ &= \max_S \left(\sum_{x \in S} p_x - \sum_{x \in S} q_x \right), \end{aligned} \quad (3.8)$$

where S is any subset of the index set $\{x\}$. It is also known as the L_1 metric.

The trace distance is non-negative, symmetric and satisfies the triangle identity for probability functions. Hence it is a *metric*.

- The *fidelity* is given by

$$F(p_x, q_x) = \sum_x \sqrt{p_x q_x}. \quad (3.9)$$

The fidelity is not a metric.

3.2.2 Trace distance

The classical trace distance has an intuitive generalization to the quantum case.

Definition 3.4. The *quantum trace distance* between two states $\rho, \sigma \in \mathcal{P}(Q)$ is defined

$$D(\rho, \sigma) = \frac{1}{2} \text{tr}(|\rho - \sigma|) \quad (3.10)$$

$$= \frac{1}{2} \sum_k \langle e_k | \sqrt{(\rho - \sigma)^\dagger (\rho - \sigma)} | e_k \rangle, \quad (3.11)$$

where Equation 3.11 is simply an explicit expansion of Equation 3.10 in terms of a basis $\{|e_k\rangle\}$ for Q using the standard operator function $|A| = \sqrt{A^\dagger A}$.

Remark. In the case that the two states ρ and σ commute, their quantum trace distance is simply equal to the classical trace distance between their generating probability distributions in the shared basis.

The trace distance always falls within the bound

$$0 \leq D(\rho, \sigma) \leq 1, \quad (3.12)$$

where $D(\rho, \sigma) = 0$ implies that $\rho = \sigma$, and $D(\rho, \sigma) = 1$ implies that ρ and σ are orthogonal.

Properties

The trace distance exhibits a range of convenient properties which makes it a powerful tool for analyzing quantum operations. For any two states $\rho, \sigma \in \mathcal{P}(Q)$ their trace distance satisfies the following properties

- Metric properties

The trace distance is symmetric, non-negative and satisfies the triangle inequality for density operators. Hence it is a metric.

- Unitary invariance

The trace distance is invariant under unitary transformations

$$D(U\rho U^\dagger, U\sigma U^\dagger) = D(\rho, \sigma), \quad (3.13)$$

so that time evolving the states does not alter their distance.

- Generating positive operator

The trace distance is achieved by the maximization

$$D(\rho, \sigma) = \max_P \text{tr}(P(\rho - \sigma)), \quad (3.14)$$

where P is any *positive* operator on Q such that $P \leq I$. In particular Equation 3.14 states that such an operator P must always exist, which provides a invaluable tool for evaluating distance quantities.

- POVM maximization

Analogous to the previous point, there is a close relationship between the quantum and the classical trace distance. Let $\{E_m\}$ be a POVM on Q with the probabilities for the m -th outcome $p_m = \text{tr}(\rho E_m)$ and $q_m = \text{tr}(\sigma E_m)$. Maximizing over all possible POVM's $\{E_m\}$ yields the equivalence

$$D(\rho, \sigma) = \max_{\{E_m\}} D(p_m, q_m). \quad (3.15)$$

This highlights the fact that the trace distance gives an upper bound on the distinguishability of the states by measurement.

Contractivity under quantum operations

The main theorem for the trace distance measure is a generalization from its unitary invariance to its behavior under general quantum operations, as explored in Section 3.1.

Theorem 3.5 (Contractivity of the trace distance). *For two states $\rho, \sigma \in \mathcal{P}(Q)$, let \mathcal{E} be a trace-preserving quantum operation on Q . \mathcal{E} will then be a contractive operations on the trace distance between the states, i.e.*

$$D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \leq D(\rho, \sigma). \quad (3.16)$$

This has profound applications for quantum cryptography. As noted, the trace distance provides an upper bound on the distinguishability between quantum states that any measurement can provide. In addition, as long as the state is prepared to be uncorrelated with the environment, any physical process applied to it will follow the dynamics of quantum operations, which by Theorem 3.5 cannot increase the trace distance. In particular this means that if an upper bound on the trace distance between two states is found, there is no method for any observer to distinguish the states better than this bound.

3.2.3 Fidelity

The fidelity measure has a similar quantum generalization, although the form is slightly altered to ensure it is symmetric.

Definition 3.6. The *quantum fidelity distance* between two states $\rho, \sigma \in \mathcal{P}(Q)$ is defined

$$F(\rho, \sigma) = \text{tr} \left(\sqrt{\rho^{1/2} \sigma \rho^{1/2}} \right). \quad (3.17)$$

Remark. As with the trace distance, in the case that the two states ρ and σ commute, their quantum fidelity is simply equal to the classical fidelity distance between their generating probability distributions in the shared basis.

The fidelity between a general state ρ and a pure state $|\psi\rangle\langle\psi|$ takes a particularly convenient form. Using $F(|\psi\rangle, \rho)$ as a shorthand for $F(|\psi\rangle\langle\psi|, \rho)$ it is seen that

$$F(|\psi\rangle, \rho) = \sqrt{\langle\psi|\rho|\psi\rangle}. \quad (3.18)$$

The fidelity always falls within the bound

$$0 \leq F(\rho, \sigma) \leq 1, \quad (3.19)$$

where $F(\rho, \sigma) = 1$ implies that $\rho = \sigma$, and $F(\rho, \sigma) = 0$ implies that ρ and σ have orthogonal support, i.e. they are perfectly distinguishable.

Properties

The fidelity measure exhibits some properties similar to the trace distance. However, unlike the trace distance which increases as the states become more distinguishable, the fidelity has the opposite behavior. As such, some properties of the fidelity are similar but mirrored with respect to their trace distance counterpart. Also note that the fidelity is not a metric.

For any two states $\rho, \sigma \in \mathcal{P}(Q)$ their fidelity satisfies the following properties

- Symmetry

Similarly to the trace distance, the fidelity is symmetric in its inputs, i.e.

$$F(\rho, \sigma) = F(\sigma, \rho). \quad (3.20)$$

- Unitary invariance

Similarly to the trace distance, the fidelity is invariant under unitary transformations

$$F(U\rho U^\dagger, U\sigma U^\dagger) = F(\rho, \sigma). \quad (3.21)$$

- Uhlmann's theorem

As with the trace distance, the fidelity can also be achieved by a maximization procedure. Introducing a second quantum system R as a copy of the principal system Q , then

$$F(\rho, \sigma) = \max_{|\phi\rangle} |\langle \psi | \phi \rangle|, \quad (3.22)$$

where $|\psi\rangle$ and $|\phi\rangle$ are purifications of ρ and σ into QR respectively. This is a slightly modified version of Uhlmann's theorem.

- POVM minimization

Similarly to the trace distance, there is a close relationship between the quantum and the classical fidelity measures. However, unlike the trace distance, the equivalence is achieved by minimizing over POVM operators. More precisely, let $\{E_m\}$ be a POVM on Q with the probabilities for the m -th outcome $p_m = \text{tr}(\rho E_m)$ and $q_m = \text{tr}(\sigma E_m)$. Then

$$F(\rho, \sigma) = \min_{\{E_m\}} F(p_m, q_m). \quad (3.23)$$

As with the trace distance, this highlights the fact that the fidelity gives an upper bound on the distinguishability of the states by measurement.

Monotonicity under quantum operations

The fidelity behaves in a similar way as the trace distance under quantum operations. The following theorem mirrors that of Theorem 3.5.

Theorem 3.7 (Monotonicity of fidelity). *For two states $\rho, \sigma \in \mathcal{P}(Q)$, let \mathcal{E} be a trace-preserving quantum operation on Q . \mathcal{E} will then be a monotonically increasing operation on the fidelity between the states, i.e.*

$$F(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \geq F(\rho, \sigma). \quad (3.24)$$

3.2.4 Distance measure equivalence

This section is concluded with a theorem that supports the notion that the two distance measures explored in this section are in many ways equivalent. In view of their many shared properties, especially the behavior under quantum operations, choosing between them is purely a matter of preference. They are both valuable tools for analyzing quantum channels and their security.

The following theorem substantiates the above claims and gives explicit bounds on the relation between the two distance measures

Theorem 3.8 (Distance measure equivalence). *For any two states $\rho, \sigma \in \mathcal{P}(Q)$, the trace distance $D(\rho, \sigma)$ and fidelity $F(\rho, \sigma)$ satisfy*

$$1 - F(\rho, \sigma) \leq D(\rho, \sigma) \leq \sqrt{1 - [F(\rho, \sigma)]^2}. \quad (3.25)$$

3.3 Information theory

Information theory concerns the storage and transmission messages [Sha48]. The defining goal is to reproduce some message, i.e. a sequence of characters, at another time or place than its creation. The message is always chosen among a set of possible messages, and selecting the correct message is then only possible when additional *information* is available. This section provides brief summary of common quantities in classical information theory and their quantum analogues, before presenting the Holevo bound for evaluating how much classical information can be encoded in a quantum state.

3.3.1 Classical information

Classically, information is described by probabilities, measured in *bits*. Shannon's influential paper [Sha48] on noiseless and noisy channel coding provides the mathematical framework

for describing information and gives explicit bounds for how compactly it is possible to store it as well as how efficiently it can be transmitted through a communication channel subject to noise.

Information source

A classical information source is described by a generator of random messages, or more precisely, successive stochastic characters [Sha48]. When discussing information sources we shall usually refer to a memoryless information source, where each message is an independent identically-distributed discrete random variable X . The message can be generated in discrete chunks or continuously, each with their own type of source. In line with our finite dimensionality of the state spaces, we are mostly concerned with discrete information sources, so that $X : S \rightarrow \{x\} \subset \mathbb{R}$ on a sample space S , with probability distribution $p_X : \{x\} \rightarrow [0, 1] : x \mapsto p_X(x)$ such that

$$p_X(x) = \Pr\{s \in S : X(s) = x\}. \quad (3.26)$$

The set of possible values for X is denoted $\{x\}$.

The message is then a sequence of characters from the sample space S , each distributed according to the random variable X . One fundamental question is to consider how much information is carried by an average message of this sort, given the probability distribution of X . Equivalently, using the properties of X , how much can a message be compressed on average.

Shannon entropy

The Shannon entropy $H(X)$ is a measure of the amount of information present in a message.

Definition 3.9. A discrete, memoryless information source is characterized by a random variable X with possible values $\{x\}$ and probability distribution $p_X(x)$. Then the *Shannon entropy* of the information source is given by

$$H(X) = - \sum_x p_X(x) \log p_X(x), \quad (3.27)$$

where it is implicitly assumed that indeterminate expressions of the form $0 \log 0$ are treated in accordance with the limit.

Shannon's noiseless coding theorem [Sha48] asserts that the Shannon entropy is the upper limit for lossless compression of a information source. This means that the least amount of bits per character needed to represent a message by a information source X is given by $H(X)$, establishing entropy as the measure of information rate.

Intuitively, entropy is therefore a measure of the information contained on average in a message by the source in question. More precisely, the entropy is the average information gain *after* learning the true value of the random variable X when only the possible values and the associated probability distribution was known. Alternatively, the entropy can also be interpreted as the uncertainty in the random variable *before* learning the true value.

Below is a summary of noteworthy properties of the Shannon entropy for a random variable X .

- Information is non-negative

$$H(X) \geq 0 \quad (3.28)$$

with equality only if the outcome is already certain $H(X) = 0$.

- The entropy is maximized when all outcomes are equally likely. Formally, if X is a random variable with d outcomes then

$$H(X) \leq \log d, \quad (3.29)$$

with equality if and only if X is uniformly distributed.

3.3.2 Classical multivariate entropy

For treating combinations of information sources, there is a range of other quantities related to the entropy. These expressions are highly useful for instance in describing information gain when some previous information is already available. A few of the most important quantities are surveyed below, all under the assumption of discrete, memoryless information sources.

Joint entropy

The joint entropy of two discrete random variables X and Y respectively is simply the entropy of the pair. That is, the two variables produce messages as a sequence of pairs of characters. If the joint probability distribution of X and Y is given by $p(x, y)$, the joint entropy is given by

$$H(X, Y) = - \sum_{x, y} p(x, y) \log p(x, y). \quad (3.30)$$

The joint entropy is non-negative $H(X, Y) \geq 0$, symmetric $H(X, Y) = H(Y, X)$ and is bounded by

$$\max [H(X), H(Y)] \leq H(X, Y) \leq H(X) + H(Y), \quad (3.31)$$

where the last equality holds if and only if X and Y are independent.

Conditional entropy

Conditional entropy occurs in a similar fashion when there are two random variables, but some information is already known. Given two random variables X and Y with joint probability distribution $p(x, y)$, suppose the value of X is already known to be $X = x$. The conditional entropy of Y given $X = x$ is then

$$H(Y|X = x) = - \sum_y p(y|x) \log p(y|x). \quad (3.32)$$

The conditional entropy of Y *on average* is then given as the weighted sum of conditional entropies $H(Y|X = x)$ for all values of x , i.e.

$$\begin{aligned} H(Y|X) &= - \sum_x p(x) H(Y|X = x) \\ &= - \sum_{x,y} p(x, y) \log \frac{p(x, y)}{p(x)}, \end{aligned} \quad (3.33)$$

where $p(x)$ is the marginal probability distribution $p(x) = \sum_y p(x, y)$.

Intuitively, the conditional entropy $H(Y|X)$ measures the *average* information gained by obtaining the value of Y given that the value of X is already known. Equivalently, it also measures the information needed on average to describe Y given that X is already known.

The conditional entropy satisfies the bound

$$0 \leq H(Y|X) \leq H(Y), \quad (3.34)$$

with the first equality holding if Y is completely determined by X and the second equality holding if and only if X and Y are independent. It also satisfies

$$H(Y|X) = H(X, Y) - H(X). \quad (3.35)$$

Mutual information

Mutual information measures the mutual dependence of two random variables X and Y with joint probability distribution $p(x, y)$. The mutual information between them is then given by

$$I(X : Y) = \sum_{x,y} p(x, y) \log \frac{p(x, y)}{p(x)p(y)}, \quad (3.36)$$

where $p(x)$ and $p(y)$ are the respective marginal probabilities.

Intuitively, mutual information measures how much information is gained on average about one of the variables when the value of the other is known. Equivalently, it also measure the information *saved* on average for describing X given that Y is known, compared to not knowing Y .

The mutual information is symmetric $I(X : Y) = I(Y : X)$ and satisfies the bound

$$0 \leq I(X : Y) \leq H(Y), \quad (3.37)$$

with the first equality holding if and only if X and Y are independent and the second equality holding if and only if Y is completely determined by X . It also satisfies

$$I(X : Y) = H(X) + H(Y) - H(X, Y). \quad (3.38)$$

Relative entropy

The Kullback-Leibler divergence, also known as the relative entropy, measures the information contained in a refinement from one model to a new model. Suppose a random variable X is modeled to have probability distribution $p(x)$, yet its true probability follows $q(x)$. The relative entropy of p with respect to q is then

$$D(p||q) = \sum_x p(x) \log \frac{p(x)}{q(x)}. \quad (3.39)$$

Intuitively, the relative entropy measures how much information is gained on average when revising the probability model. Equivalently, it measures the average number of extra information needed to encode samples from $p(x)$ using a code optimized for $q(x)$ instead of for $p(x)$.

The relative entropy is always non-negative $D(p||q) \geq 0$.

3.3.3 Quantum information

The classical expressions for entropy are extended to measure the information contained in quantum states. These new quantities typically involve operator functions such as $\log \rho$; $\rho \in \mathcal{P}(V)$. As long as the operator is normal, which e.g. density operators are, the operator function can be evaluated by spectral decomposition, instead of the usual series representation. More precisely, if a normal operator A has spectral decomposition $\sum_i \lambda_i |e_i\rangle \langle e_i|$, the operator function $f(A)$ takes the form $f(A) = \sum_i f(\lambda_i) |e_i\rangle \langle e_i|$. This gives expressions involving operator functions a convenient, explicit representation.

Von Neumann entropy

Analogous to the classical case, the *von Neumann entropy* quantifies the information content of a single quantum state.

Definition 3.10. The von Neumann entropy for a density operator $\rho \in \mathcal{P}(V)$ is defined

$$S(V)_\rho = S(\rho) = -\text{tr}(\rho \log \rho). \quad (3.40)$$

As a concrete example to the above discussion of operator functions, Equation 3.40 takes the explicit form

$$S(\rho) = -\sum_i \lambda_i \log \lambda_i, \quad (3.41)$$

when the density operator has spectral decomposition $\rho = \sum_i \lambda_i |e_i\rangle \langle e_i|$. This gives an intuitive motivation for the definition of quantum entropy by highlighting the parallels to the classical Shannon entropy.

The von Neumann entropy exhibits similar properties as the Shannon entropy, which has some important physical interpretations. The following properties hold for any density operator $\rho \in \mathcal{P}(V)$.

- The entropy is non-negative

$$S(\rho) \geq 0, \quad (3.42)$$

with equality if and only if the state is pure $\rho = |\psi\rangle \langle \psi|$. This provides an important illustration of the point made in Section 2.1.4. Assigning entropy as a measure of “randomness”, it is perhaps tempting to associate the quantum entropy with the intrinsic uncertainty of the quantum state, i.e. the randomness of outcomes from measuring in some basis. The entropy is however only related to the quantum state’s information content, through its generating probability distribution.

- The entropy is maximized for a completely random quantum state. Formally, if the dimensionality of the state space is $\dim V = d$ then

$$S(\rho) \leq \log d, \quad (3.43)$$

with equality if and only if the state is completely mixed $\rho = I/2$.

- The entropy is invariant under unitary transformations

$$S(U\rho U^\dagger) = S(\rho). \quad (3.44)$$

- The entropy is concave in the density operators

$$S\left(\sum_i p_i \rho_i\right) \geq \sum_i p_i S(\rho_i). \quad (3.45)$$

3.3.4 Quantum multi-state entropy

The familiar expressions for treating multivariate entropy in the classical case all have analogues to the quantum case. The relative and joint entropy carry over in a straightforward manner. The conditional entropy and mutual information find their most natural definitions by treating the properties of the classical entropy (see Section 3.3.2) as defining axioms for the quantum case.

Joint entropy

In a composite system AB , the joint entropy of a density operator $\rho^{AB} \in \mathcal{P}(A \otimes B)$ is defined

$$S(A, B)_\rho = S(\rho^{AB}) = -\text{tr}(\rho^{AB} \log \rho^{AB}). \quad (3.46)$$

Similarly to the classical case, it is symmetric $S(A, B)_\rho = S(B, A)_\rho$ and is bounded by

$$\left| S(A)_\rho - S(B)_\rho \right| \leq S(A, B)_\rho \leq S(A)_\rho + S(B)_\rho, \quad (3.47)$$

where the last equality holds if the component states are uncorrelated $\rho^{AB} = \rho^A \otimes \rho^B$.

Also note that by Schmidt decomposition (Theorem 2.5), if the composite state is pure $\rho^{AB} = |\psi\rangle\langle\psi|$ then $S(A)_\rho = S(B)_\rho$.

Conditional entropy

Given a composite state $\rho^{AB} \in \mathcal{P}(A \otimes B)$, the component states ρ^A and ρ^B are given by the reduced density operators of their respective system. The conditional entropy of ρ^A given ρ^B is then

$$S(A|B)_\rho = S(\rho^A | \rho^B) = S(A, B)_\rho - S(B)_\rho. \quad (3.48)$$

It is bounded by above by

$$S(A|B)_\rho \leq S(A)_\rho. \quad (3.49)$$

However, unlike the classical case, the conditional quantum entropy can be *negative*, i.e. $S(A|B)_\rho < 0$. This holds whenever the two component systems are in an entangled state.

Mutual information

Given a composite state $\rho^{AB} \in \mathcal{P}(A \otimes B)$ with reduced states ρ^A and ρ^B , the mutual information between the component systems is given by

$$I(A : B)_\rho = I(\rho^A : \rho^B) = S(A)_\rho + S(B)_\rho - S(A, B)_\rho. \quad (3.50)$$

It is symmetric $I(A : B)_\rho = I(B : A)_\rho$, but unlike the classical case it is bounded by

$$0 \leq I(A : B)_\rho \leq \min\{S(A)_\rho, S(B)_\rho\}, \quad (3.51)$$

where the last inequality mirrors the fact that the conditional entropy can be negative for entangled states.

Relative entropy

Given two states $\rho, \sigma \in \mathcal{P}(V)$, the relative entropy of ρ with respect to σ is then

$$S(\rho||\sigma) = \text{tr}(\rho \log \rho) - \text{tr}(\rho \log \sigma). \quad (3.52)$$

Similarly to the classical case, it is non-negative $S(\rho||\sigma) \geq 0$.

3.3.5 Encoding classical information

Finally, one of the key questions of classical and quantum information can be addressed; how can information be encoded in and extracted from quantum states. This is a big topic in quantum information, and only a few, basic results will be given here.

Analogous to the classical case, the information is stored as a sequence of characters that constitutes a message. Each character is now however not simply a number x from a distribution $\{p_x, x\}$, but rather a *quantum state* ρ_x drawn from some distribution $\{p_x, \rho_x\}$. The measure of how much information is stored in such a quantum message is given in qubits. The difference between storing information with classical numbers and quantum states resides in the lack of distinguishability between non-orthogonal quantum states.

A variety of situations can now be considered, depending on the nature of the information to be encoded in the quantum states. For instance, one may ask what rate of qubits is needed to store a sequence of quantum pure states drawn from some distribution $\{p_x, |\psi_x\rangle\}$. The answer to this turns out to be given by the von Neumann entropy $S(\rho)$ of the density operator generated by the distribution $\rho = \sum_x p_x |\psi_x\rangle \langle \psi_x|$. The focus here will however be on how the quantum message can be used to encode *classical* information.

The classical information to be encoded in a quantum message is described by the random variable X with distribution $\{p_x, x\}$. The general scheme for encoding this information is to assign one quantum state ρ_x to each classical character x . The quantum state describing the *average* encoded character is then simply the weighted sum $\sum_x p_x \rho_x$ which is immediately recognized as the density operator generated by the distribution $\rho = \sum_x p_x \rho_x$. This means that the encoding ρ does not only depend on the classical information to be stored, but also on our encoding scheme $\{\rho_x\}$. The choice of quantum states for encoding the message will generally impact its recoverability.

As a direct consequence of the no-cloning theorem, it is seen that the quantum message cannot offer an improved storage rate over classical encoding schemes, i.e.

$$H(X) \geq S(\rho), \quad (3.53)$$

where $H(X)$ is the Shannon entropy of the classical source and $S(\rho)$ is the von Neumann entropy of the encoded qubits. The equality is satisfied if and only if the states are orthogonal $\text{tr}(\rho_x \rho_y) = 0$; $x \neq y$. This formalizes the fact that quantum states cannot be used to encode classical information better than what is classically possible. Furthermore, if non-orthogonal state are used, the information rate is strictly lower as some information can no longer be recovered.

3.3.6 The Holevo bound

This section is concluded with a key theorem of quantum information, namely the Holevo bound. This result takes the previous consideration of storing classical information with quantum states to its natural conclusion. In addition to the encoding rate already explored in the previous section, the Holevo bound evaluates the actual recoverable classical information rate by considering an explicit measurement scheme.

As before, the classical information to be encoded is described by the random variable X with distribution $\{p_x, x\}$. The encoded characters of the quantum message is described by the generated density operator $\rho = \sum_x p_x \rho_x$, given our choice of encoding scheme $\{\rho_x\}$. Finally, a measurement is done on the quantum message, described by POVM elements $\{E_y\}$. The measurement outcomes y and their associated probabilities p_y generate a new, classical random variable Y with distribution $\{p_y, y\}$.

A detailed analysis in [NC10] proves a series of results regarding strong subadditivity of the von Neumann entropy, which establishes the fact that quantum operations cannot increase mutual quantum information. This in turn is the basis for proving the Holevo bound.

Theorem 3.11 (Holevo bound). *Consider a quantum message $\rho = \sum_x p_x \rho_x$ constructed from an encoding scheme $\{\rho_x\}$ and a classical source X with distribution $\{p_x, x\}$. A measurement procedure with POVM elements $\{E_y\}$ on the message then generates a random variable Y according to the distribution $p(y) = \text{tr}(E_y \rho)$. The mutual classical information between the source variable X and the measurement variable Y then satisfies*

$$I(X : Y) \leq S(\rho) - \sum_x p_x S(\rho_x). \quad (3.54)$$

In light of Equation 3.38 and Equation 3.53, it is evident that $I(X : Y) \leq S(\rho)$. Whether this bound is tight for orthogonal quantum states is however not immediately obvious, but it is at least clear that the inequality definitely becomes strict in the case of non-orthogonal states. Holevo's theorem offers an improvement on this bound.

Chapter 4

Quantum cryptography

Increased awareness about the power of quantum computers has had far-reaching consequences for the field of cryptography [All+14]. The majority of today's need for securing communication is addressed with classical cryptographic techniques, e.g. by public-key cryptography. The implementation of a large-scale quantum computer poses serious challenges to the security of these protocols [Sho94]. At the same time, the theory of quantum information reveals a completely new type of cryptographic system. Using quantum states to encode the information and exploiting the dynamics of quantum measurement, a promise of *unconditionally* secure communication is made [SP00].

This chapter is divided into two parts. First, the ideas of quantum key distribution are presented, looking specifically at the modern security definition [RK05] and the BB84 protocol [BB84]. The second part presents a detailed account of the security proof of BB84 as presented in [Koa09].

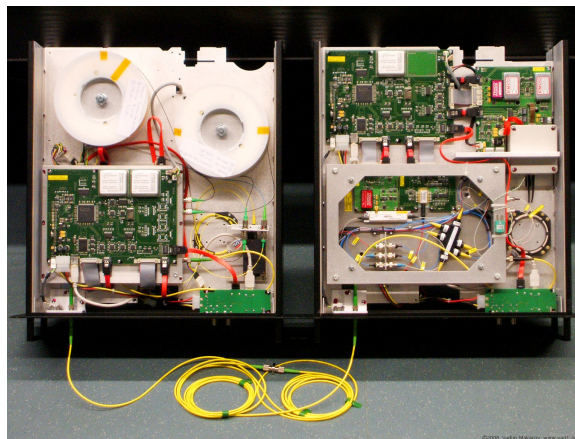


Figure 4.1: Clavis 2: commercial quantum key distribution system manufactured by ID Quantique [MLS10a].

4.1 Quantum key distribution

Quantum cryptography is the application of quantum communication channels for the purpose of secure communication. Concretely this is done by establishing some physical line of communication that is capable of sharing physical states exhibiting quantum behavior between the participants. This can for instance be done by sending polarized photons through an optical fiber [NC10]. Already there are commercial systems available by e.g. ID Quantique in Geneva, Switzerland (see Figure 4.1) and MagiQ Technologies in Massachusetts, USA.

The possibilities offered by quantum mechanics to secure communication are just beginning to be explored. In line with the study of quantum computation at large, it is evident that exploiting the advantages of quantum mechanics in the design of algorithms is not an easy task [NC10]. The known, useful quantum algorithms have largely been discovered by considering specific problems. It is therefore not unjustified to claim that the field of quantum cryptography is in an early state, with new possible techniques still awaiting discovery. In this section we will specialize to studying the so-far most established quantum cryptographic technique, namely quantum key distribution.

4.1.1 Setup and goals

Quantum key distribution (QKD) is a quantum cryptographic protocol for performing *key exchange* [NC10]. That is, it provides a mechanism for two parties to establish a shared secret key between them by use of a public (insecure) quantum communication channel. In line with the security criteria in Section 1.1.2, the QKD protocol does not offer to secure messages on its own. Rather, it provides a method for distributing key information among the parties, so that conventional symmetric-key methods, such as the one-time pad, may be deployed.

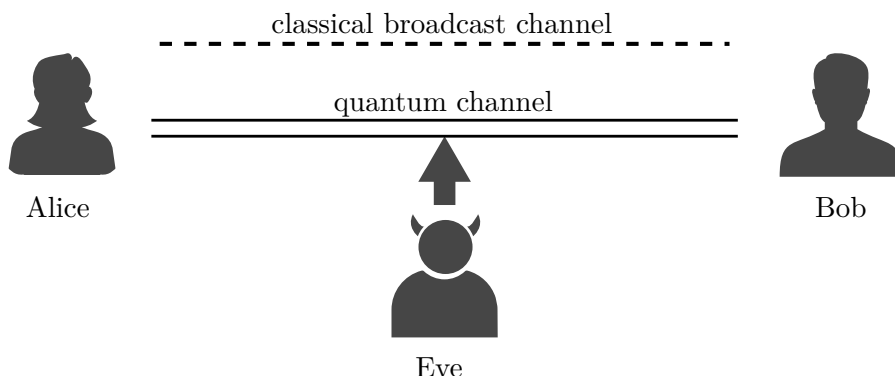


Figure 4.2: Schematic diagram of the setup in quantum key distribution: Alice and Bob communicate by the use of a quantum channel plus an authenticated, but open classical broadcast channel. An eavesdropper (Eve) has access to read both channels, but can only interfere with the quantum one.

Analogous to Section 1.1, the standard setup in QKD [All+14], as depicted in Figure 4.2,

considers two parties Alice and Bob. Their goal is to agree on a secret key that they did not share before. Available to their disposal is a quantum communication channel, which is not secure, i.e. an eavesdropper Eve has full access to control the line.

There is however an additional assumption of a public (broadcast) channel, where Alice and Bob may freely publish information. Although the broadcast channel is completely open (it offers no confidentiality), it is assumed to provide *authentication* and *integrity* of transmitted messages. This means that although Eve is free to read both channels, she can only interfere with the quantum one. That is, in this analysis Eve is not capable of faking or modifying messages sent by Alice or Bob *over the broadcast channel*.

The goal of this scheme is to establish new key material shared by Alice and Bob that they can verify is secure [All+14]. As QKD satisfies the strongest security definition of unconditional security, it in fact promises that no information at all about the key is available to any other party, except for some exponentially small probability¹. Note also that QKD makes *no* promise to succeed in establishing this key. As mentioned in Section 1.1.5 this is however not specific to QKD, but rather a general limit of cryptography; Eve is free to jam the channel and thereby making communication impossible. The goal of QKD is rather to detect any tampering that would compromise the security of the key, with absolute accuracy.

4.1.2 Assumptions

In line with the reasoning in Section 1.1.5 it is evident that in order to achieve authentication over the public channel, Alice and Bob must have a pre-shared key. Another option would be to use public-key protocols to authenticate the broadcast channel, although this decreases the security of the proof while also allowing for man-in-middle attacks. Instead, it is customary to take the different approach of making a small amount of key material pre-shared between Alice and Bob an *explicit* assumption of the protocol.

This may seem contradictory for two reasons; first, what is the purpose of the QKD protocol if Alice and Bob already share a key? The answer to this is simply: to produce a longer key. It is true that the pre-shared key may be used to achieve secrecy for a while, yet perfect security quickly consumes all the key material. QKD however stands as the only unconditionally provable method to *gain* key material over an insecure channel. In this way, an almost logarithmically small² [All+14] initial pre-shared key will allow Alice and Bob to produce arbitrary amounts of shared key material. The shared key can then be used to deploy conventional symmetric-key encryption to secure their communication. This is the true hallmark of QKD

The second question regards the actual security benefit of the protocol. As it stands,

¹“Exponentially small” here means that the probability decreases exponentially with the number of qubits transmitted through the protocol. In this way, Alice and Bob can control the failure probability and make it as small as they wish.

²Similarly, “logarithmically small” here means that the necessary minimum length of the initial pre-shared key scales only logarithmically with the length of the desired length of the final key.

classical encryption techniques are to be used for both the public channel authentication as well as for the actual encryption following successful execution of the QKD protocol. As any cryptographic system is only as secure as its weakest link, this may seem paradoxical in light of the challenges to classical encryption methods. The answer to the authentication issue comes from the fact that unlike for the case of confidentiality, there are classical schemes for authentication that consume little key material. Second, QKD allows Alice and Bob to agree on a shared, secret key of an arbitrary length. Once established, this key can then be used in any classical encryption algorithm with a security strength of their choice. In particular, Alice and Bob can choose to use the Vernam cipher (see Section 1.1.4), making the whole protocol unconditionally secure [All+14].

4.1.3 Proving security

A large number of techniques have been used to provide security proofs of QKD protocols. All proofs are based on the key property that distinguishes quantum cryptography from the classical case, namely the non-orthogonality of quantum states [All+14]. By the no-cloning theorem for general, non-orthogonal states (see Theorem 2.9), it follows that any measurement capable of obtaining information about the state will necessarily disturb it [NC10]. This has the consequence that any attempts by Eve to observe the messages on the line will necessarily produce detectable disturbances in the message. In this way, Alice and Bob can monitor the channel for interference to estimate the amount of information Eve has extracted. If the interference is below a certain threshold, they can successfully establish a shared, secure key with an information leak to other parties that is exponentially decreasing with the number of qubits transmitted.

One of the most attractive features of QKD is that it is proven to be unconditionally secure. In line with the discussion in Section 1.1.3, this is the strongest form of security possible. Compare this to the contrasting case of e.g. public-key encryption such as RSA, where the security is provided by assumption of the attackers' computational power. The goal for QKD proofs is to avoid such assumptions, so that unconditional security is only dependent on correct implementation of the system and the laws of physics [All+14].

4.1.4 The modern security definition

Early proofs of QKD were typically related to the Holevo bound [LC99] (see Section 3.3.6). These techniques aimed at establishing an upper bound on the mutual information any attacker could share with the key. It was however realized that security definitions based on mutual information were insufficient; although it allows for any measurement by Eve, it does assume that Eve in fact makes a measurement. In general this may not be the case, as Eve can apply some scheme to entangle the intercepted quantum states with her own quantum system and simply keep the quantum states. It is desirable to be able to characterize the security of the key even if no measurement has been done yet.

The modern security definition [RK05] remedies this fact. In this model, Alice and Bob deploys some key distribution protocol that establishes the shared key s^* between Alice and Bob. The key belongs to some key space $\mathcal{S} \ni s^*$ over all possible distributable keys. The joint quantum state of Alice and Bob after running the protocol is represented by $\rho_S \in \mathcal{P}(H_S)$ for some key-Hilbert space H_S . The dimensionality of H_S equals that of the key space \mathcal{S} , i.e. $\dim H_S = |\mathcal{S}|$, so there exists some probability distribution $p(s)$ such that

$$\rho_S = \sum_{s \in \mathcal{S}} p(s) |s\rangle \langle s|, \quad (4.1)$$

with $\{|s\rangle\}_{s \in \mathcal{S}}$ as an orthonormal basis for H_S . Let Eve's quantum state after running the protocol be given by $\rho_E \in \mathcal{P}(H_E)$. The final combined state ρ_{SE} for Alice, Bob and Eve then takes the form

$$\rho_{SE} = \sum_{s \in \mathcal{S}} p(s) |s\rangle \langle s| \otimes \rho_E(s), \quad (4.2)$$

where Eve may in general be correlated with the different key values.

The cryptographically ideal situation occurs when Eve's state is *equally* correlated with all possible key values $s \in \mathcal{S}$. Formally, define the ideal density operator ρ'_{SE} as

$$\rho'_{SE} = \frac{1}{|\mathcal{S}|} \left(\sum_{s \in \mathcal{S}} |s\rangle \langle s| \right) \otimes \rho_E, \quad (4.3)$$

where ρ_E is independent of s .

Definition 4.1. A key distribution protocol leaves Alice, Bob and Eve with the key state ρ_{SE} and corresponding ideal state ρ'_{SE} . The protocol is said to be ε -secure if

$$\frac{1}{2} \|\rho_{SE} - \rho'_{SE}\| \leq \varepsilon, \quad (4.4)$$

where the norm is given as $\|M\| = \text{tr}(|M|)$, so that the left-hand side of Equation 4.4 is simply the trace distance from Definition 3.4.

As seen from Chapter 3 (and also argued in [RK05]), this security definition is solid; it provides an upper bound on the distinguishability between the ideal and the actual key by any observer. This means that there is a fundamental limit to the amount of information an attacker can possibly have about the key. Also note that by the contractivity of the trace distance under quantum operations (Theorem 3.5), no further action on the state cannot be used to increase distinguishability.

4.1.5 BB84

A variety of specific QKD protocols have been proposed. One of the most common implementations is known as BB84, after its authors Bennet and Brassard [BB84]. In this protocol, Alice prepares a collection of qubits that encode the random key she wishes to

share with Bob. The qubits are then transmitted across some quantum communication channel, where Bob receives and measures them. The physical realization is typically done with sending photons through an optical fiber, with the photons' polarization states representing the qubits.

The steps of the protocol are presented below. Note in particular the importance of the public broadcast channel; whenever the algorithm calls for a “public announcement” of some information, it is to be understood that it is transmitted over the authenticated, public channel. The importance of authenticity is made explicitly clear from the algorithm: if for instance Eve could spoof Bob's acknowledgment of receipt, Alice may reveal her basis selection before any measurement has been done. This would allow Eve to measure the qubit without the risk of altering it, thus breaking the security of the protocol.

The basis states used in the protocol can for example be

$$\begin{aligned}
 |Z; 0\rangle &= |0\rangle \\
 |Z; 1\rangle &= |1\rangle \\
 |X; 0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
 |X; 1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)
 \end{aligned} \tag{4.5}$$

Protocol

The protocol is formulated in the algorithmic steps [NC10; Koa09]:

1. Alice begins with generating a random bit string \mathbf{b} of length $|\mathbf{b}| = (4 + \gamma)N$. This is the key that she aims to share with Bob by applying the protocol. She also generates another random bit string \mathbf{a} of equal length, that will determine the encoding into the qubit states.
2. For each digit k of \mathbf{a} , Alice then prepares a separate qubit in the Z or X -basis depending on the value $a_k \in \{0, 1\}$. The direction of the qubit is determined by the corresponding value of $b_k \in \{0, 1\}$. Formally, this leaves Alice with the state

$$|\psi\rangle = \bigotimes_{k=1}^{(4+\gamma)N} |\psi_{a_k b_k}\rangle; \quad \begin{cases} |\psi_{0i}\rangle = |Z; i\rangle \\ |\psi_{1i}\rangle = |X; i\rangle \end{cases} \tag{4.6}$$

3. Alice transmits $|\psi\rangle$ through the quantum communication channel. The presence of noise and the actions of Eve will generally perturb the state.
4. Bob generates his own random bit string \mathbf{a}' ; $|\mathbf{a}'| = |\mathbf{a}|$. He then performs a Z or X -basis measurement on the quantum state received through the channel according to the value of $a'_k \in \{0, 1\}$. The results are recorded as \mathbf{b}' that can take values $b'_k \in \{0, 1, \perp\}$. Here, \perp represents no result, or “vacuum”, which corresponds to Bob's detector not

making any detection. This can occur due to noise in the channel, jamming by Eve or imperfections in the instruments. Whenever Bob obtains an outcome 0 or 1 he publicly acknowledges receipt.

5. Alice and Bob then publicly announces \mathbf{a} and \mathbf{a}' .
6. Alice and Bob keep the bits where $a_k = a'_k$, i.e. when Bob did obtain an outcome 0/1 and also happened to measure in the same basis as Alice prepared the state in. Depending on the choice of γ , Alice and Bob will at this point be left with $2N$ bits, except for a failure probability ϕ . Given a reasonable rate for successful transmission over the channel³, γ can be chosen so that the failure probability ϕ is exponentially decreasing in γ [NC10].
7. Alice then randomly selects half⁴ of her bits to sacrifice for error estimation. She publicly announces the selection of these N bits.
8. Alice and Bob both publicly announce the values of their bit strings according to the selection made by Alice in the previous step. These *check bits* satisfy $a_k = a'_k$, which means that in the presence of no imperfections, noise or interference, all N of them would be equal. In practice there will however be errors, and the number of non-matching bits are labeled n_z and n_x for the Z and X -basis respectively. Since the check bits were publicly announced, Alice and Bob will agree on the number of non-matching bits.
9. After removing the N check bits, Alice and Bob are left with each their own N -bit *sifted* key, labeled $\kappa_{A,\text{sif}}$ and $\kappa_{B,\text{sif}}$ respectively. If the check bits show an error rate above a certain threshold, Alice and Bob will both declare failure and the protocol is aborted. Otherwise, if the error rate is below the threshold, Alice and Bob can proceed from their N -bit sifted keys with information reconciliation to agree on a *reconciled* key κ_{rec} . Finally, privacy amplification is used to establish the final, shared $(N - m)$ -bit key κ_{fin} .

Key gain

Authenticating all the public announcement messages consumes some of the pre-shared secret key of Alice and Bob. In addition, the last steps of reconciling errors and distilling an ε -secure key from $\kappa_{A,\text{sif}}$ and $\kappa_{B,\text{sif}}$ will also consume pre-shared key material. Security proofs of the protocol will however typically ignore the details of the authentication, as it

³There is no additional assumption about the channel being made here. For any particular BB84 protocol (that is, including the reconciliation and amplification steps), we will find a minimum transmission rate for the channel that still allows security of the protocol. Using this rate, γ is then simply chosen to make the probability $1 - \phi$ of being left with $2N$ bits as desired.

⁴Sacrificing half the qubits is a very stringent requirement; in practice, much less is typically needed to still provide the required security. Still, out of simplicity of the argument, we will here assume half the qubits are sacrificed for error estimation.

is a purely classical cryptographic problem. As such, the broadcast channel is assumed to already be authenticated.

Denoting the number of bits of pre-shared key material needed for error correction in the reconciliation step by r , the *secret key gain* G of the protocol is seen to be

$$G = N - r - m, \tag{4.7}$$

since the protocol produces a key of length $G - m$ by consuming a key of length r . As long as $G > 0$, the protocol promises to distribute more key material than it consumes in the process. This is illustrated by an example in Figure 4.3

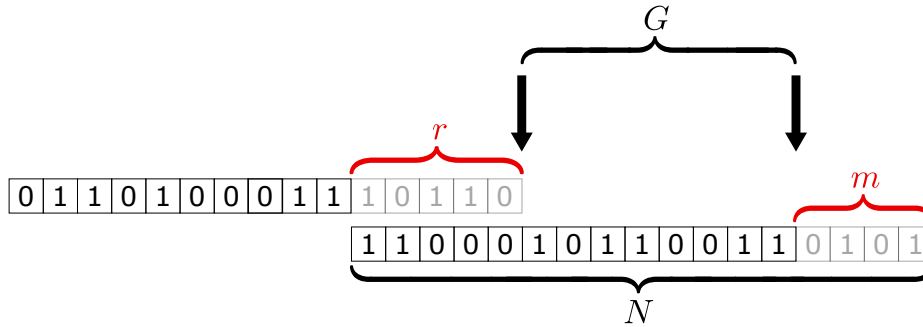


Figure 4.3: Illustration of the key gain for an example key: the gain is found by subtracting the consumed key material r and sacrificed key material m , from the established key length N .

4.2 Security proof

A modern proof of BB84 was given recently by Koashi [Koa09]. Earlier proofs typically relied on constructing specific quantum error-correcting codes (QECC) for the error correction and privacy amplification steps. In this paper however, both these objectives are accomplished by classical techniques, notably by the use of classical encryption and universal hashing. One remarkable consequence of this approach is how conveniently it can be shown to hold true for other protocols. In particular, we will later consider protocols with source imperfections, which forms the topic of the next chapter.

This section presents a detailed review of the proof in [Koa09]. This is an updated version of an original article [Koa06] which was modernized to fit the new security definition (see Section 4.1.4). We first present the idea of the proof, explain how it is structured and describe a few of the underlying principles. The subsequent parts then go through the steps of the proof.

4.2.1 Idea

The aim is to prove security of the BB84 protocol, specifically satisfying the requirements for *unconditional* security. This is achieved by making us of Definition 4.1 to show that

the protocol is ε -secure for an ε that Alice and Bob can make arbitrarily small. As argued in Section 4.1.4, this property is a sufficient conditions for satisfying the requirements unconditional security.

The proof functions by establishing a set of Hilbert spaces and accompanying measurement operators for Alice and Bob. In this language, the original BB84 protocol is converted into an equivalent entanglement-based protocol with an explicit procedure for constructing κ_{fin} by choosing a specific method for information reconciliation and privacy amplification. We will then construct a set of key assumptions relating to the protocol. The proof is conducted in 2 steps: First, it is shown that the BB84 protocol satisfies these assumptions. Second, it is the shown that *any* protocol satisfying the assumptions is consistent with Definition 4.1.

The core idea of the proof is to consider complementary measurement variables. In this line of reasoning, one of the bases, say Z , is fixed as the measurement operator for obtaining the secret key. This is the principle procedure of the *actual protocol*. Then one tries to establish a method for estimating a complementary measurement outcome X to as high degree as possible. This is then called the *virtual protocol*. The main contribution by [Koa09] is providing such a modern, elegant method for proving the security.

4.2.2 Principles

In order to prove security, it will be necessary to give Eve access to a lot of the information that Alice and Bob see. As the proof progresses, the roles of the various parties of the protocol might get hard to distinguish. It is therefore helpful to start out by consider a few, underlying principles to this style of proof. Although some will find these principles obvious, they are included mainly because the author spent some time contemplating them when trying to understand the proof himself.

The first principle relates to the meaning of the virtual protocol. It represents a different protocol to the actual one and is in fact not physically carried out at all. Rather, it represents a protocol that in principle *could* have been carried out instead. It does however have the pivotal and *only* restriction that it is allowed only as long as it is theoretically *indistinguishable* from the actual protocol *as far as Eve is concerned*. This means that any information revealed to Eve, notably including all messages on the broadcast channel, must be identical in the actual and virtual protocol. As long as this condition is met, there is however no restriction on what the virtual protocol can involve. In particular, whereas the actual protocol is bound by the operation of Alice's and Bob's physical apparatus, the virtual protocol can involve any operation that is allowed by physics.

The second principle relates to the defining features of the 3 parties of the protocol: Alice, Bob and Eve. Specifically, if Alice and Bob share most of their information and measurement results with Eve, what exactly distinguishes them from an attacker? It is tempting to define this difference in terms of knowledge about the final key, but this cannot be an assumption as it is in fact the result we are trying to prove. Looking back at the protocol

steps, it is seen that the defining distinction is knowledge about the result of Alice's and Bob's measurement in the actual protocol. Eve is granted access to all other information, particularly any additional measurements introduced through the virtual protocol as well as broadcast messages.

Lastly, it may seem paradoxical that Eve receives all this information; after all, as the proof does not function without it, can Eve not simply chose to ignore this information? The answer resides in the fact that doing so would not disprove the security. Rather, it would mean that the situation is inaccurately modeled and would give no result. The last guiding principle can then be summarized in that there is no loss of generality in making Eve try her best to estimate all the various measurements Alice and Bob do.

4.2.3 Formal protocol

Let Alice and Bob deploy some QKD protocol. Assume they have discarded some mismatching states (where Alice's and Bob's basis didn't happen to match) as well as states used for error estimation. They are left with some shared, collective quantum state $\rho_0 \in \mathcal{P}(\mathcal{H}_A \otimes \mathcal{H}_B)$, where \mathcal{H}_A and \mathcal{H}_B are Alice's and Bob's state space respectively.

Protocol 4.1 (Actual protocol).

1. Alice and Bob conduct measurements on ρ_0 on their respective state spaces \mathcal{H}_A and \mathcal{H}_B . The measurement outcomes are recorded as their respective sifted keys $\kappa_{A,\text{sif}}$ and $\kappa_{B,\text{sif}}$, with $|\kappa_{A,\text{sif}}| = |\kappa_{B,\text{sif}}| = N$. Define Alice's key as the the reconciled one⁵, i.e. $\kappa_{\text{rec}} = \kappa_{A,\text{sif}}$.
2. Then Alice sends encrypted, classical error correcting information over the public channel. This consumes r bits of their pre-shared key. Bob then agrees on the same key $\kappa_{B,\text{sif}} \mapsto \kappa_{\text{rec}}$ except for a small failure probability ζ .
3. Choose a number of bits $m \leq N$ to forfeit for privacy amplification. Alice chooses a set $\{\mathbf{v}_k\}_{k=1}^{N-m}$ of $N - m$ N -bit *linearly independent* sequences randomly from the space of N -bit binary strings $\{0, 1\}^N \ni \mathbf{v}_k$.
4. She announces this set through the broadcast channel.
5. The k th bit of the final key κ_{fin} is then defined as

$$(\kappa_{\text{fin}})_k = \kappa_{\text{rec}} \cdot \mathbf{v}_k, \tag{4.8}$$

where \cdot is the binary dot product (mod 2).

Except for the small failure probability ζ , Alice and Bob both agree on the same final key κ_{fin} . As we will see, the number of bits m used in the amplification step will determine the

⁵Note that we define κ_{rec} opposite that of [Koa09], which defines the key in terms of Bob's measurement. We will define it in terms of Alice's instead.

security ε of the protocol.

The shared state ρ_0 that Alice and Bob measure on is now completely free and can in particular be heavily correlated to some other system that Eve controls. Because of the error estimation step, there are however some promises that are placed on the error between outcomes of some measurements that Alice and Bob can do. These promises are made concrete through the security assumptions defined later. For now, we will make an *informal* definition of the error rates:

- Let δ_{bit} be the bit error rate between the measurements Alice and Bob make in Protocol 4.1; that is, it is the error rate of the measurement establishing the key.
- Let δ_{ph} be the phase error rate between the measurement by Alice and Bob that is *complementary* to that in Protocol 4.1; this is made concrete through the squash operator and the security assumptions.

As we will see later in Section 4.2.4, the protocol will be constructed so that the error rates δ_{bit} and δ_{ph} correspond to δ_z and δ_x respectively.

Squash operator

Now, define a *squash operator* Λ that relates Alice's state space to a qubit space⁶:

$$\begin{aligned} \Lambda : \mathcal{P}(\mathcal{H}_A \otimes \mathcal{H}_B) &\rightarrow \mathcal{P}(\mathcal{K}^{\otimes N} \otimes \mathcal{H}_R) \\ \rho &\mapsto \Lambda(\rho) \end{aligned} \tag{4.9}$$

where \mathcal{K} is simply a qubit space and \mathcal{H}_R is a virtual ancilla system. The function of Λ is to relate Alice's general Hilbert space \mathcal{H}_A to a space on which we can define complementary Z and X -basis measurements. As will be made explicit through the security assumptions, Λ must be chosen so that the measurement $Z^{\otimes N}$ on $\mathcal{K}^{\otimes N}$ corresponds to Alice's actual measurement on \mathcal{H}_A .

Let Z and X -basis measurements on $\mathcal{K}^{\otimes N}$ be denoted by the vector notation: $\mathbf{Z} = Z^{\otimes N}$ and $\mathbf{X} = X^{\otimes N}$. Consider the measurements:

- Let \mathbf{z} be the outcome of measuring \mathbf{Z} on $\mathcal{K}^{\otimes N}$ of the state $\Lambda(\rho_0)$.
- Let \mathbf{x} be the outcome of measuring \mathbf{X} on $\mathcal{K}^{\otimes N}$ of the state $\Lambda(\rho_0)$.
- Let $\boldsymbol{\mu}$ be the outcome of some measurement M_R on \mathcal{H}_R of the state $\Lambda(\rho_0)$.

Security assumptions

As planned the introduction (Section 4.2.1), we will construct 2 assumptions relating to Alice's and Bob's measurements. A theorem is then posed, claiming that any protocol with

⁶See footnote 5

the above-mentioned setup, that also satisfies these assumptions, is indeed *unconditionally* secure. Security of Protocol 4.1 then follows from showing it satisfies both assumptions and then proving the theorem.

Assumption 1. Assume that the application of the mapping Λ followed by the measurement \mathcal{Z} on $\mathcal{K}^{\otimes N}$ is equivalent to Alice's measurement in Protocol 4.1, that is

$$\kappa_{\text{rec}} = \kappa_{A,\text{sif}} = \mathcal{Z}. \quad (4.10)$$

Assumption 2. Apply Λ and make the measurements \mathbf{X} on $\mathcal{K}^{\otimes N}$ and M_R on \mathcal{H}_R with results \mathbf{x} and $\boldsymbol{\mu}$ respectively. Then for each $\boldsymbol{\mu}$ define a set $\{\mathbf{T}_{\boldsymbol{\mu}}\}$ of N -bit sequences $\mathbf{T}_{\boldsymbol{\mu}} \in \{0, 1\}^N$, that has cardinality $|\{\mathbf{T}_{\boldsymbol{\mu}}\}| = 2^{N\xi}$.

Assume this can be constructed so that for any possible measurement pair $(\mathbf{x}, \boldsymbol{\mu})$ that can occur, $\mathbf{x} \in \{\mathbf{T}_{\boldsymbol{\mu}}\}$ except for an exponentially small probability η .

Intuitively, it is possible to get an idea of the function of the error rates: The bit error rate δ_{bit} is connected to the key sacrifice r and the failure probability ζ . The phase error rate δ_{ph} on the other hand is connected to Assumption 2 and the failure probability η .

Main theorem

The main theorem is then stated as follows:

Theorem 4.2. *Alice and Bob apply a QKD protocol according to Protocol 4.1 so that it satisfies Assumption 1 and Assumption 2. The protocol is the ε -secure, for*

$$\varepsilon = \sqrt{\eta + 2^{-N\varepsilon_2}}, \quad (4.11)$$

where $\varepsilon_2 = m/N - h(\delta_{\text{ph}})$ and m must be chosen so that $\varepsilon_2 > 0$.

Since η decreases exponentially in N , it is clearly seen that the security parameter ε also decreases exponentially in N .

4.2.4 Equivalent entanglement protocol

Protocol 4.1 assumes a starting point of a shared quantum state ρ_0 , and that there are estimates δ_{bit} and δ_{ph} about the error rates of Alice's and Bob's subsequent measurements on this state. It does not however describe what method Alice and Bob could use to achieve this state for good values of $\delta_{\text{bit}}, \delta_{\text{ph}}$. That is the role of the BB84 protocol in Section 4.1.5.

Looking back at the BB84 protocol steps, it is seen that the starting situation of Protocol 4.1 is achieved at the beginning of the final step (step 9). The equivalence is attained by

first converting to an *entanglement protocol*: In the original protocol, Alice first randomly generates $(4 + \gamma)N$ basis and bit values \mathbf{a} and \mathbf{b} and then transmits corresponding Z and X -basis states through the channel.

Consider now instead a scheme in which Alice start out by preparing $(4 + \gamma)N$ Bell states

$$|\phi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{2}(|++\rangle + |--\rangle). \quad (4.12)$$

Alice initiates the protocol simply by transmitting *half* of each state through the channel, while keeping the other half of each state herself. *After* all the states are transmitted, Alice can then randomly generate basis values \mathbf{a} and *determine* the bit sequence \mathbf{b} from corresponding measurements on her half. By the principle of deferred measurement (Theorem 2.8), this must be equivalent to the setup in the original BB84 protocol in Section 4.1.5.

The transmitted half is of course a representation of some actual physical state⁷, and to keep the treatment general we will not assume any structure about its Hilbert space. Similarly, we do not place any restrictions on the Hilbert space of Bob's received states either, other than that he can implement some form of measurements that he labels Z and X . Alice's kept half is however only a *virtual* representation of her recorded bit values \mathbf{b} , and so it is equivalent to a perfect qubit space $\mathcal{K}^{\otimes(4+\gamma)N}$.

The deferred measurement can furthermore be considered in two steps: First the states that are sacrificed for error estimation are measured, then the rest. Although everything is measured before Alice and Bob publish their basis choices, *in theory* the error estimation data does *exist* just prior to Alice's and Bob's final measurement. In addition, since we are here considering a case where Bob's detector is completely basis-independent, we are free to disregard all the states on which Alice and Bob *later* do not pick matching bases to measure. We also discard all states where they ended up choosing the X -basis, so that we are only looking to prove security for their Z -basis key measurements. Label this state by ρ' .

In summary, we have described a new, entanglement protocol. At the end of this protocol Alice and Bob are left with a shared, unmeasured state ρ' . As argued, this is completely equivalent to the original BB84 protocol in Section 4.1.5, so that its error estimation data n_z and n_x is available. In addition, the end point ρ' of the entanglement protocol clearly satisfies the definition of ρ_0 in Protocol 4.1. We have thus shown how the BB84 protocol therefore effectively leaves Alice and Bob with the formal situation described in Protocol 4.1. Protocol 4.1 then gives a specific algorithm by which Alice and Bob carry out step 9: error reconciliation and privacy amplification.

⁷The quantum states are typically realized by polarized photonic modes in an optical fiber [NC10]

Satisfying the assumptions

It is now easy to show that applying the entanglement protocol followed by Protocol 4.1 satisfies Assumption 1 and Assumption 2. Specifically, the shared state ρ' from the entanglement protocol is defined on a shared space between Alice and Bob, but where Alice's space is a perfect qubit space: $\mathcal{H}_A = \mathcal{K}_A^{\otimes N}$. As a consequence, Assumption 1 holds trivially by letting Λ be the identity map and setting $\mathcal{K}^{\otimes N} = \mathcal{K}_A^{\otimes N}$.

Then consider the error estimation step of the protocol. As the bits sacrificed for error estimation are picked by random sampling of the whole set of bits, it follows that it forms a good estimate for the error that will be observed in the remaining bits. Specifically, from the measured error counts n_z and n_x define error rates:

$$\delta_z = n_z/N \tag{4.13a}$$

$$\delta_x = n_x/N. \tag{4.13b}$$

[NC10] shows how the probability that the *true* error rates of the yet unmeasured bits are higher than these estimates decreases exponentially in N . Furthermore, since by Assumption 1 the key is defined from the Z -basis measurement, we have in this case:

$$\delta_{\text{bit}} = \delta_z \tag{4.14a}$$

$$\delta_{\text{ph}} = \delta_x, \tag{4.14b}$$

except for a probability that is exponentially in N .

Now simply choose Bob's complementary measurement $M_R = \mathbf{X}$. From the random sampling, it is clearly seen that the error estimation guarantees the existence of the set $\{\mathbf{T}_\mu\}$, since Alice's and Bob's measurements \mathbf{x} and μ must agree up to $\delta_{\text{ph}}N$ errors. The knowledge of one of these quantities therefore leaves the other one within $2^{h(\delta_{\text{ph}})N}$ possible values, where

$$h(\delta) = -\delta \log \delta - (1 - \delta) \log(1 - \delta) \tag{4.15}$$

is the binary entropy function. Consequently, Assumption 2 is therefore satisfied for $\xi = h(\delta_{\text{ph}}) + \varepsilon_2$ for some $\varepsilon_2 > 0$. In addition, η is simply the failure probability of the error estimation mentioned above. Following the previous arguments, η will clearly decrease exponentially in N .

Similarly, the error estimation also then guarantees that Alice's and Bob's Z -basis measurements agree up to $\delta_{\text{bit}}N$ errors. Except for a small failure probability, this error is correctable by $N(h(\delta_{\text{bit}}) + \varepsilon_1)$ bits of extra information for some $\varepsilon_1 > 0$. By Assumption 1, this clearly means that in Protocol 4.1, $r = N(h(\delta_{\text{bit}}) + \varepsilon_1)$ and ζ is equal to the failure probability of the error correction. Furthermore, this failure probability is exponentially decreasing in N .

4.2.5 Proof of the main theorem

Proving security for the BB84 protocol has now been reduced to proving Theorem 4.2. Before doing so, it is however helpful to get an overview of the various quantities that govern the protocol:

1. Alice and Bob will choose 4 control parameters: N , r , m and γ .
2. Alice and Bob will then conduct *measurements* to find: n_z and n_x .
3. The protocol then guarantees the key gain G (Equation 4.7) with security ε (Equation 4.11), except for failure probabilities: ϕ , ζ and η .

Proving the success and security of the protocol in a meaningful way therefore depends on showing that Alice and Bob can choose their parameters so that:

- The protocol is ε -secure for the ε in Theorem 4.2 (so that ε is exponentially decreasing in the control parameters).
- The failure probability is as low as desired (preferably exponentially decreasing in some control parameter).
- The key gain G is in fact positive.

Out of these requirements, the failure probabilities ϕ , ζ and η have all already been shown to be exponentially decreasing in γ or N .

To prepare for the main proof, we also show a useful extension of Equation 3.22 for purifications of pure states:

Lemma 4.3. *Let $|\psi\rangle_1$ be an arbitrary pure state in some space V_1 . Then any purification $|\phi\rangle_{12}$ of $|\psi\rangle_1$ into an enlarged space $V_1 \otimes V_2$ will necessarily be of the form*

$$|\phi\rangle_{12} = |\psi\rangle_1 \otimes |\phi\rangle_2 \tag{4.16}$$

where $|\phi\rangle_2$ is some state in V_2 .

It is of course clear that the construction in Equation 4.16 means that $|\phi\rangle_{12}$ is in fact *some* purification of $|\psi\rangle_1$. This lemma however asserts the slightly stronger property that *any* purification of $|\psi\rangle_1$ can indeed be written in this form.

Proof. Using Theorem 2.5, decompose $|\phi\rangle_{12}$ in its Schmidt bases $\{|e_\lambda\rangle_1\}, \{|e_\lambda\rangle_2\}$:

$$|\phi\rangle_{12} = \sum_\lambda \lambda |e_\lambda\rangle_1 |e_\lambda\rangle_2. \tag{4.17}$$

The requirement that $|\phi\rangle_{12}$ purifies $|\psi\rangle_1$ then implies

$$\sum_{\lambda} \lambda^2 |e_{\lambda}\rangle_{11} \langle e_{\lambda}| = |\psi\rangle_{11} \langle \psi|. \quad (4.18)$$

Interpreting this as two state ensembles that should generate the same density matrix, we can invoke Theorem 2.4. Since one of the ensembles only has 1 element and because the Schmidt bases are orthonormal, this implies that

$$|e_{\lambda}\rangle_1 = e^{i\phi_{\lambda}} |\psi\rangle_1; \quad \forall \lambda, \quad (4.19)$$

for some phases ϕ_{λ} . It then immediately follows that

$$|\phi\rangle_{12} = \sum_{\lambda} \lambda e^{i\phi_{\lambda}} |\psi\rangle_1 |e_{\lambda}\rangle_2 = |\psi\rangle_1 \otimes \sum_{\lambda} \lambda e^{i\phi_{\lambda}} |e_{\lambda}\rangle_2, \quad (4.20)$$

which is the form in Equation 4.16. □

Concepts

The idea of the proof of Theorem 4.2 is as follows: Protocol 4.1 instructs Alice and Bob to conduct Z -basis measurements to establish the key. We will now however consider virtual protocols where Alice and Bob will aim to estimate the outcome, had Alice chosen to measure her qubits in the X -basis instead. In line with the discussion in Section 4.2.2, this must be done in a way that looks theoretically completely equivalent to Protocol 4.1 as far as Eve is concerned. This ensures that Eve has no method to detect or respond to which protocol Alice and Bob choose.

The trick to estimating Alice's hypothetical X -basis measurement outcome \mathbf{x} comes from the fact that it does not matter to Eve what Bob does; it cannot influence Eve's situation. Bob can therefore make a X -basis measurement himself, giving the outcome $\boldsymbol{\mu}$. If there was no eavesdropping and no imperfections, the error rate $\delta_{\mathbf{x}}$ would be 0, and so Bob would have a perfect estimate for \mathbf{x} , except for the error estimation failure probability η . This means that Alice's qubits state σ has to be nearly a pure X -basis eigenstate $|\mathbf{X}; \mathbf{x}\rangle$. For any attacker, Alice's subsequent measurement of σ in the Z -basis will then scramble her qubit state into a perfectly mixed state $I/2^N$.

Imperfections and Eve's influence will generally mean that $\delta_{\mathbf{x}} > 0$, in which case Bob's result $\boldsymbol{\mu}$ only limits Alice's measurement to $\mathbf{x} \in \{\mathbf{T}_{\boldsymbol{\mu}}\}$ from Assumption 2. Due to the distillation step, Alice is however able to make a limited X -basis measurement on her qubits. By using Bob's measurement $\boldsymbol{\mu}$ and Alice's result together, they can make a reliable estimate of Alice's hypothetical X -basis measurement. In order for this to still be indistinguishable from Protocol 4.1 for Eve, Alice's limited measurement must commute with her key measurement.

Formal proof

In order to prove Theorem 4.2, we will consider a set of virtual protocols. To conclude the proof, we will show that these protocols are all equivalent to Protocol 4.1.

Protocol 4.2 (Virtual protocol 1).

1. Apply the Λ mapping and discard \mathcal{H}_R .
2. Alice determine her key κ_{rec} from measuring \mathbf{Z} on $\mathcal{K}^{\otimes N}$.
3. Conduct steps 2 - 5 of Protocol 4.1.

Define the observable on $\mathcal{K}^{\otimes N}$ according to:

$$\sum_{\nu}(\mathbf{w}) = \sigma_{\nu}^{w_1} \otimes \sigma_{\nu}^{w_2} \otimes \cdots \otimes \sigma_{\nu}^{w_N}; \quad \nu = \{z, x\}, \quad (4.21)$$

where $\mathbf{w} = [w_1, w_2, \dots, w_N]$ is a N -bit sequence and σ_{ν} is the ν th Pauli matrix $\sigma = [X, Y, Z]$. As an example, $\sum_z([011]) = I \otimes Z \otimes Z$ and $\sum_x([11 \dots 1]) = \mathbf{X}$.

$\sum_{\nu}(\mathbf{w})$ yields measurement outcomes that are either $+1$ or -1 , thus essentially functioning as a parity operator.

Protocol 4.3 (Virtual protocol 2).

1. Apply the Λ mapping and obtain $\boldsymbol{\mu}$ by conducting measurement M_R on \mathcal{H}_R .
2. Choose a number of bits $m \leq N$ to forfeit for privacy amplification. Alice chooses a set $\{\mathbf{w}_j\}_{j=1}^m$ of m N -bit sequences randomly from the space of N -bit binary strings $\{0, 1\}^N \ni \mathbf{w}_j$.
3. Alice then chooses a set $\{\mathbf{v}_k\}_{k=1}^{N-m}$ of $N - m$ N -bit *linearly independent* sequences randomly from the space of N -bit binary strings $\{0, 1\}^{\otimes N} \ni \mathbf{v}_k$ so that

$$\mathbf{v}_k \cdot \mathbf{w}_j = 0; \quad \forall j, k = 1, \dots, N \quad (4.22)$$

where \cdot again is the binary dot product (mod 2).

4. Alice announces $\{\mathbf{v}_k\}_{k=1}^{N-m}$ through the broadcast channel.
5. Alice measures the m observables $\sum_x(\mathbf{w}_j)$, obtaining m N -bit sequences \mathbf{x}_k^* .
6. Alice then measures the $N - m$ observables $\sum_z(\mathbf{v}_k)$, recording their outcomes as the final key κ_{fin} .

By Assumption 2, prior to step 5, Bob's result $\boldsymbol{\mu}$ promises that Alice's measurement \mathbf{X} would give a result in the set $\mathbf{x} \in \{\mathbf{T}_{\boldsymbol{\mu}}\}$ if measured, except for a probability η . Knowing $\boldsymbol{\mu}$, there are therefore $2^{N\xi} = 2^{Nh(\delta_{\text{ph}})}$ candidate sequences in $\{\mathbf{T}_{\boldsymbol{\mu}}\}$. Each of the m measurements in

step 5 gives a random parity bit $\mathbf{X} \cdot \mathbf{w}_j$. Choose m in step 2 as

$$m = N(\xi + \varepsilon_2) = N(h(\delta_{\text{ph}}) + \varepsilon_2), \quad (4.23)$$

for some $\varepsilon_2 > 0$. It then follows from universal hashing techniques that the probability that 2 different sequences $\mathbf{y}_1, \mathbf{y}_2 \in \{\mathbf{T}_\mu\}$ both produce the same parity measurements in step 5 is less than $2^{N\xi}2^{-m} = 2^{-N\varepsilon_2}$.

Label Alice's qubit state at the end of step 5 by $\sigma_A \in \mathcal{P}(\mathcal{K}^{\otimes A})$. In effect, Alice and Bob together can now make a prediction \mathbf{x} about Alice's hypothetical measurement \mathbf{X} with a failure probability of $\eta' = \eta + 2^{-N\varepsilon_2}$, i.e.

$$p(\mathbf{X} = \mathbf{x})_{\sigma_A} = \text{tr}(|\mathbf{X}; \mathbf{x}\rangle_A \langle \mathbf{X}; \mathbf{x}| \sigma_A) = {}_A\langle \mathbf{X}; \mathbf{x} | \sigma_A | \mathbf{X}; \mathbf{x}\rangle_A \geq 1 - \eta', \quad (4.24)$$

which means that σ_A must be nearly the pure X -basis eigenstate $|\mathbf{X}; \mathbf{x}\rangle_A$.

Any attacker who has knowledge about the error rates, Bob's measurement $\boldsymbol{\mu}$ and Alice's measurements in step 5 will make the above estimate about Alice's qubits *before* she measures them according to step 6. Eve's state $\sigma_{AE} \in \mathcal{P}(\mathcal{K}^{\otimes N} \otimes \mathcal{H}_E)$ at the end of step 5, for some arbitrary state space \mathcal{H}_E , will therefore necessarily satisfy

$$\text{tr}_E(\sigma_{AE}) = \sigma_A. \quad (4.25)$$

Introduce a virtual ancilla system \mathcal{H}_C and let $|\psi\rangle_{AEC}$ be the purification of σ_{AE} into $\mathcal{K}^{\otimes N} \otimes \mathcal{H}_E \otimes \mathcal{H}_C$. Conservatively, let Eve control this purification [Ska08]. From Equation 4.25 it is clear that $|\psi\rangle_{AEC}$ is also a purification of σ_A . Then by Uhlmann's theorem (Equation 3.22) and Lemma 4.3, there exists an *extension* $|\phi\rangle_{EC}$ of $|\mathbf{X}; \mathbf{x}\rangle_A$, so that

$$|{}_{AEC}\langle \psi | \mathbf{X}; \mathbf{x}\rangle_A \langle \phi |_{EC}| = F(\sigma_A, |\mathbf{X}; \mathbf{x}\rangle_A) \geq \sqrt{1 - \eta'}. \quad (4.26)$$

In particular, this must hold even when $|\psi\rangle_{AEC}$ is fixed. Using the relation Equation 3.25 and the contractivity of the trace distance under partial trace, it is then seen that

$$\frac{1}{2} \|\sigma_{AE} - |\mathbf{X}; \mathbf{x}\rangle_A \langle \mathbf{X}; \mathbf{x}| \otimes \rho_E\| \leq \sqrt{1 - (1 - \eta')} = \sqrt{\eta'}, \quad (4.27)$$

where $\rho_E = \text{tr}_C(|\phi\rangle_{EC} \langle \phi|)$.

Finally, we invoke the principal difference between Alice / Bob and an attacker from Section 4.2.2: the attacker does not see the result of Alice's Z -basis measurement. As far as Eve is concerned, this measurement will thus function as a quantum operation that maps $|\mathbf{X}; \mathbf{x}\rangle_A$ to the fully mixed state

$$\rho_{\text{mix}} = \sum_{\mathbf{z} \in \{0,1\}^{N-m}} \frac{1}{2^{N-m}} |\mathbf{z}\rangle \langle \mathbf{z}|. \quad (4.28)$$

By Assumption 1, there is however a one-to-one correspondence between $|\mathbf{z}\rangle \in \mathcal{K}^{\otimes(N-m)}$

and the final key space of κ_{fin} . Thus ρ_{mix} is nothing but the cryptographically ideal state from Section 4.1.4. By the contractivity of the trace distance under quantum operations, the final state σ_{AE} clearly satisfies Equation 4.4 for $\varepsilon = \sqrt{\eta'}$.

The next step is to reduce Protocol 4.3 to Protocol 4.1. The final measurement $\sum_z(\mathbf{v}_k)$ in step 6 clearly commutes with measurement $\sum_x(\mathbf{w}_j)$ in step 5 because of Equation 4.22. Hence, step 5 has no influence on the final key and can be omitted. The final key is also independent of the measurement M_R on \mathcal{H}_R . Since step 5 is no longer needed, Alice is free to choose $\{\mathbf{v}_k\}_{k=1}^{N-m}$ freely, as long as it is linearly independent and orthogonal to a random subspace with maximal dimensionality 2^m . This is however automatically guaranteed by the original choice of $\{\mathbf{v}_k\}_{k=1}^{N-m}$ in step 3 since it cannot span more than a 2^{N-m} -dimensional subspace. Finally, the outcome of the $\sum_z(\mathbf{v}_k)$ observable can now be directly obtained by simply measuring \mathbf{Z} and using Equation 4.8.

Thus we have reduced Protocol 4.3 to Protocol 4.2. Furthermore, any measurement Bob makes on \mathcal{H}_R cannot impact Alice's measurement, and he is therefore free to omit it. Finally, by Assumption 1 Alice's measurement \mathbf{Z} on $\mathcal{K}^{\otimes N}$ is equivalent to her actual key measurement on \mathcal{H}_A . Hence we have shown the Protocol 4.2 is itself equivalent to Protocol 4.1. This concludes the proof of Theorem 4.2. \square

4.2.6 Asymptotic limit

The key gain of the protocol is

$$G = N - r - m = N(1 - h(\delta_{\text{bit}}) - h(\delta_{\text{ph}}) - \varepsilon_1 - \varepsilon_2). \quad (4.29)$$

In line with the discussion in Section 4.2.4, the failure probabilities decrease exponentially in N for fixed ε_1 and ε_2 . We now invoke the asymptotic limit $N \rightarrow \infty$: It is then possible to choose $\varepsilon_1, \varepsilon_2 \rightarrow 0$ while still guaranteeing that all failure probabilities similarly go to 0. Finally, the security parameter $\varepsilon \rightarrow 0$ as well.

In conclusion: We have shown the security of the BB84 protocol in the limit of large $N \rightarrow \infty$. This protocol then gives a the asymptotic key gain

$$G = N(1 - h(\delta_{\text{bit}}) - h(\delta_{\text{ph}})), \quad (4.30)$$

which is positive if and only if $h(\delta_{\text{bit}}) + h(\delta_{\text{ph}}) < 1$.

We have thus finally arrived at a formal error threshold from step 9 in Section 4.1.5: In the protocol, Alice and Bob measure check bits according to random sampling and determines error rates δ_{bit} and δ_{ph} . Then these values are compared with Equation 4.30; if the key gain is negative, abort the protocol and try again. Otherwise, continue with error reconciliation and privacy amplification according to Protocol 4.1, governed by r and m respectively,

where:

$$r = Nh(\delta_{\text{bit}}) \tag{4.31}$$

$$m = Nh(\delta_{\text{ph}}). \tag{4.32}$$

The resulting key gain G is then unconditionally secure.

Chapter 5

Source imperfections

In the last chapter we proved the security of the BB84 protocol [BB84]. We furthermore showed that the security in fact holds for *any* BB84-style protocol that matches the description in Protocol 4.1 and satisfies Assumption 1 and Assumption 2. The mechanism that enabled the BB84 protocol to meet these assumptions came from the random sampling in the error estimation step.

In this chapter we propose a new protocol. It consists of the same algorithmic steps as the original BB84 protocol, but describes a situation where Alice’s source is no longer perfect. This allows us to investigate the security in the case of certain imperfections in the apparatus, the importance of which was discussed in Section 1.3. The core question is reduced to determining whether it is still possible to perform error estimation in a way that satisfies the security assumptions in Section 4.2.3.

5.1 Protocol

Alice and Bob are to deploy the BB84 protocol (see Section 4.1.5) over a quantum channel. Instead of using “perfect” states $|Z; i\rangle$, $|X; i\rangle$, we are now interested in a situation where the source can have basis-dependent imperfections¹. In this section we will characterize the protocol corresponding to such imperfect sources. First, we will present the framework for characterizing general sources. The notion of “small” basis dependencies is then formulated as a precise condition on this general source in line with Koashi [Koa09]. This description is however in practice difficult to analyze, as will be pointed out. We therefore propose a slightly modified, *stricter* source description that complies with the formalism in [Koa09] and that can still describe adequately general sources.

¹The meaning of “basis-dependence” in the sense of imperfections is introduced in Section 5.1.1.

5.1.1 General source

Let the real source be characterized as follows: Given a random basis choice $a \in \{0, 1\}$ and bit choice $b \in \{0, 1\}$, the source produces the quantum state $\rho_{ab} \in \mathcal{P}(\mathcal{H}_Q)$ on some state space \mathcal{H}_Q . The basis a is chosen randomly, with no condition on the selection being uniformly random; the actual number of times the various states are selected during the protocol simply determines the failure probability of the error estimation step. The probability of selecting bit value b given basis choice a is denoted $p(b|a) = p_{ab}$, so that

$$p_{a0} + p_{a1} = 1. \quad (5.1)$$

After selecting N basis and bit values, N corresponding states $\rho_{a_i b_i}$; $i = 1, \dots, N$ are then sent through the channel, which may have imperfections as well as be tampered with by Eve.

Types of imperfections

Note also that most types of imperfections are already automatically covered by the original proof (Section 4.2). This includes for instance defects on the quantum channel or even Alice's or Bob's apparatus, *as long as* they are *basis-independent*; that is, although the defects can depend on the quantum state Alice sends through the channel, it cannot depend on Alice's and Bob's basis choices \mathbf{a} and \mathbf{a}' directly. The reason why this does not break the security proof is that these imperfections are all absorbed in the error rates $\delta_{\text{bit}}, \delta_{\text{ph}}$. If the channel or apparatus do not perform sufficiently to enable security, this will simply be reflected by a negative key gain G according to Equation 4.30.

The case of basis-dependent imperfections is however very different and is not accounted for in the proof in Section 4.2. This means that if some of the devices change their operation based on Alice's and Bob's basis choices \mathbf{a} and \mathbf{a}' , the protocol might *not be secure* even though Equation 4.30 suggest a positive key rate. The above description of a general source allows us to analyze precisely these types of imperfections on Alice's source.

5.1.2 Koashi's source condition

To analyze the security of this protocol, we construct the *basis states*

$$\rho_a = \sum_b p_{ab} \rho_{ab}. \quad (5.2)$$

Of course the security of the protocol will depend on the choices of ρ_{ab} and p_{ab} , e.g. when ρ_0 and ρ_1 are orthogonal it is entirely insecure [Koa09]. A strong claim is nevertheless made, stating that the security can be guaranteed from a single parameter $F(\rho_0, \rho_1)$, the fidelity²

²Note that unlike in [Koa09], we are using the non-squared version $F(\rho, \sigma) = \text{tr}\left(\sqrt{\rho^{1/2}\sigma\rho^{1/2}}\right)$

between ρ_0 and ρ_1 . As long as the fidelity is sufficiently high

$$F(\rho_0, \rho_1) \geq F, \quad (5.3)$$

for some F to be determined, the protocol is claimed to remain secure.

The argument for why this holds begins with a purification step. According to [Koa09], for any choice of $\rho_{ab} \in \mathcal{P}(\mathcal{H}_Q)$ and p_{ab} we can find purifications $|\chi_a\rangle \in \mathcal{H}_S \otimes \mathcal{H}_Q$ of $\rho_a \in \mathcal{P}(\mathcal{H}_Q)$ with the following properties:

1. Their inner product satisfies

$$\langle \chi_0 | \chi_1 \rangle \geq F. \quad (5.4)$$

In particular this implies $\langle \chi_0 | \chi_1 \rangle \in \mathbb{R}$.

2. There exists measurements $\{M_{a0}, M_{a1}\}$ for each basis choice a , that produce the source states with the given probabilities, i.e.

$$\text{tr}_S[(M_{ab} \otimes I_Q) |\chi_a\rangle \langle \chi_a|] = p_{ab} \rho_{ab}. \quad (5.5)$$

Note that the condition $\langle \chi_0 | \chi_1 \rangle \in \mathbb{R}$ is in fact redundant. As long as the inner product $|\langle \chi_0 | \chi_1 \rangle| \geq F$, Equation 5.4 is obtained by simply absorbing the phase difference into one of the basis states $|\chi_0\rangle, |\chi_1\rangle$. This will function as a global phase on the state and can hence not influence any measurements.

Although the first property can be achieved by by purifying according to Uhlmann's theorem (Equation 3.22), it is not clear whether this can be done while simultaneously satisfying the second property as well. [Koa09] merely states that such purifications can always be found, without proper justification. Whether this construction is actually always possible is indeed an interesting question, although it is something we will ignore for now.

5.1.3 Revised source condition

Instead we will circumvent this difficulty by simply taking the purified states as the starting point [MLS10b]. In this fashion, we define purifications $|\beta_{ab}\rangle \in \mathcal{H}_S \otimes \mathcal{H}_Q$ of the source states $\rho_{ab} \in \mathcal{P}(\mathcal{H}_Q)$. Using the condition $p_{a1} = 1 - p_{a0}$ and letting $p_a = p_{a0}$, we no longer let $|\chi_a\rangle$ denote *some* purifications of ρ_a , but instead *define* $|\chi_a\rangle \in \mathcal{K}_A \otimes \mathcal{H}_S \otimes \mathcal{H}_Q$ according to:

$$|\chi_0\rangle = \sqrt{p_0} |0\rangle |\beta_{00}\rangle + \sqrt{1 - p_0} |1\rangle |\beta_{01}\rangle \quad (5.6a)$$

$$|\chi_1\rangle = \sqrt{p_1} |+\rangle |\beta_{10}\rangle + \sqrt{1 - p_1} |-\rangle |\beta_{11}\rangle, \quad (5.6b)$$

where $|0\rangle, |1\rangle$ are some orthonormal qubit states and $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. Furthermore, \mathcal{H}_S is some arbitrary ancilla system and \mathcal{K}_A is a qubit state space corresponding to Alice's bit values.

We now substitute the fidelity condition and instead *require* that

$$F(|\chi_0\rangle, |\chi_1\rangle) = |\langle\chi_0|\chi_1\rangle| \geq F, \quad (5.7)$$

for some F to be determined.

The construction of $|\chi_a\rangle$ is chosen so as to automatically satisfy Equation 5.5. Together with Equation 5.7 it is clear that this definition satisfies the two properties (Equation 5.4 and Equation 5.5) required by [Koa09]. This explicit construction is however more restrictive, in the sense that there exists combinations of ρ_{ab} and p_{ab} such that Equation 5.3 holds while Equation 5.7 does not.

As a concrete example³ consider ρ_{ab} all pure so that $\rho_{ab} = |\beta_{ab}\rangle\langle\beta_{ab}|$. Then let $|\beta_{a0}\rangle = |0\rangle, |\beta_{a1}\rangle = |1\rangle$ and $p_{a0} = p_{a1} = 1/2; \forall a \in \{0, 1\}$. Then using the constructions Equation 5.2 and Equation 5.6 clearly gives $F(\rho_0, \rho_1) = 1$ yet $|\langle\chi_0|\chi_1\rangle| = 0$. Note that this does not disprove that it might be possible to find *some* $|\chi_a\rangle$ that satisfy the two properties (Equation 5.4 and Equation 5.5). It only shows that there are some combinations of ρ_{ab} and p_{ab} for which *this particular* construction of $|\chi_a\rangle$ is indeed definitely more restrictive than condition Equation 5.3.

The converse implication does however apply as Equation 5.7 being true necessarily means that Equation 5.3 holds as well. Thus, Equation 5.6 gives an explicit construction of states that satisfy all the necessary properties laid out by [Koa09]. Note also that the construction of ρ_a (from Equation 5.2) is not needed at all in this formalism.

5.1.4 Entanglement protocol

We can now describe an entanglement protocol for Alice and Bob: Alice picks N random basis values \mathbf{a} and prepares N corresponding states $|\chi_{a_i}\rangle \in \mathcal{K}_A \otimes \mathcal{H}_S \otimes \mathcal{H}_Q; i = 1, \dots, N$. She then transmits the \mathcal{H}_Q -part of each state, all through the channel. The \mathcal{H}_S -parts are simply discarded. Bob receives each state on the space \mathcal{H}_B . After all N states are transmitted, Alice and Bob make measurements on their respective state spaces and proceed according to the steps of the BB84 protocol in Section 4.1.5.

It is clear that this matches the description in Protocol 4.1 and the setup in Section 4.2.3. The detailed argument for this is equivalent to that in Section 4.2.4, except the error estimation. In particular, Assumption 1 is clearly satisfied since Alice's state space is again already a perfect qubit space (choose the squash operator Λ to be the identity map). Proving security for the general source in Section 5.1.1 has thus been reduced to showing that Assumption 2 is satisfied.

³This source is of course completely insecure, as the error rates would be through the roof at ~ 0.5 . It is nevertheless an allowed construction which should be addressed by the source model.

5.2 Error estimation

In the previous section we described a protocol that accurately represents the use of BB84 [BB84] in the case of basis-dependent imperfections at the Alice’s source. It was also noted that the security of this new protocol rests on proving that Assumption 2 holds. Looking back at the proof of the original BB84 protocol in Section 4.2, this assumption was met due to a result coming from the error estimation step. The key property is that it was possible to find an upper bound on the difference between Alice’s and Bob’s X -basis measurements, even when they measured the key in the Z -basis.

This section investigates how this estimation procedure functions for the imperfect source. We first formulate the requirement from Assumption 2 into a precise question about the error rates. We then present two theorems places by [Koa09] and then subsequently investigate their claim through a set of simplifying cases, which uncovers an apparent paradox. The resolution is then introduced through the requirement of fair random sampling in the protocol. Lastly, we conjecture the possibility that this assumption is in fact not needed, at least for any realistic situations.

5.2.1 Problem formulation

The error estimation follows the same argument as in Section 4.2.4. After discarding the states where Alice’s and Bob’s qubit measurements did not happen to agree, a subset of the remaining measurements are selected uniformly *randomly* for error estimation. This then places a promise on each basis’ *error rate* that is expected in the measurements of the remaining states. This means that for any collection of L copies of one of the basis states $|\chi_a\rangle^{\otimes L}$ used in the protocol, we can select one of them at random; the probability of Alice’s and Bob’s measurement in the *same* basis disagreeing, is then provided by the error estimate. It is however important to keep in mind the entirety of the protocol, i.e. all states are *transmitted jointly* through the channel, as illustrated in Figure 5.1.

For a collection of L Z -basis states $|\chi_0\rangle^{\otimes L}$ transmitted and subsequently measured in the Z -basis, the error rate is denoted δ_z . Similarly, for a X -basis collection $|\chi_1\rangle^{\otimes L}$ and X -basis measurements, the error rate is denoted δ_x . In line with the above discussion, both these quantities are known from the error estimation step. Furthermore, we will ignore the failure probability of the error estimation simply by taking the limit $N \rightarrow \infty$ (L is finite). The error rates are therefore known with *complete* accuracy.

There is however one important distinction between this protocol and that in Section 4.2.4: the error rates are now not only dependent on Alice’s and Bob’s measurement basis, but also on the basis choice of the states $|\chi_a\rangle$. Specifically, Assumption 2 rests on the ability to *fix* the key measurement to the Z -basis and then estimate the X -basis error rate δ_{ph} . Whereas δ_{bit} still equals δ_z , the error rate δ_{ph} therefore now corresponds to a X -basis measurements on a collection of Z -basis states $|\chi_0\rangle^{\otimes L}$.

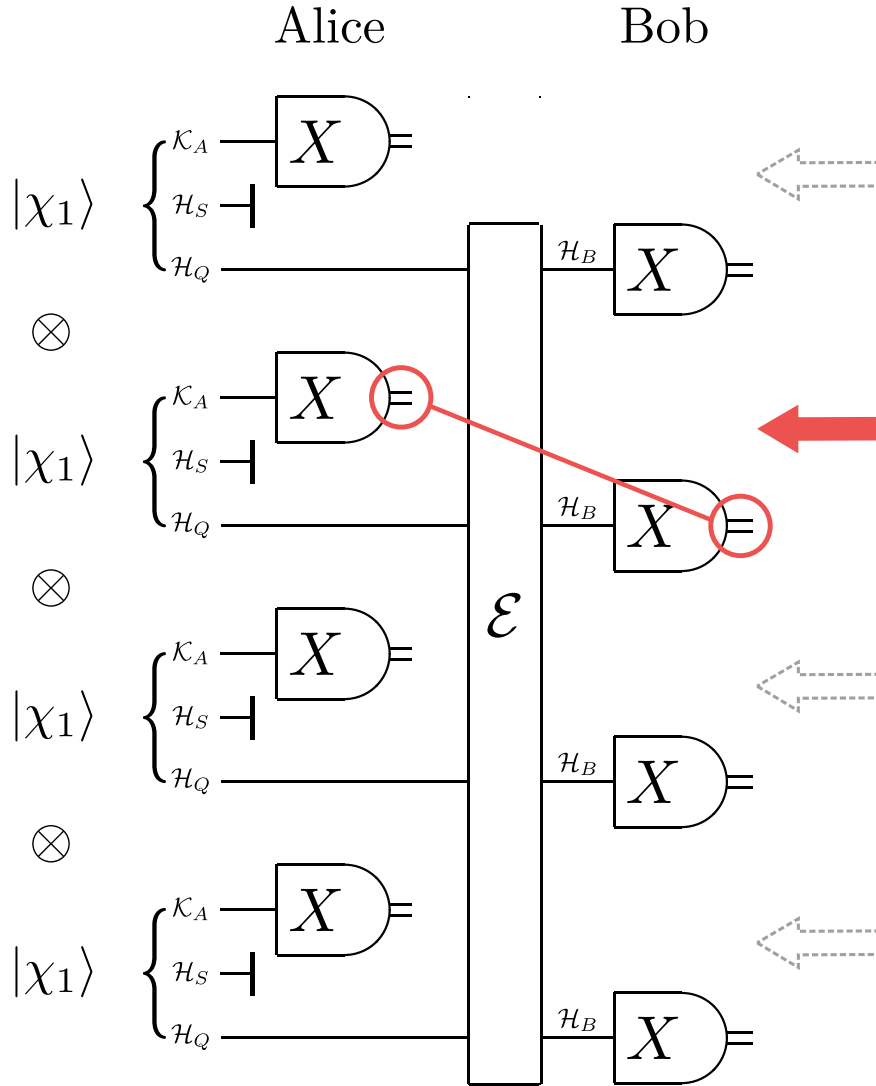


Figure 5.1: Interpretation of the error rate in the X -basis case for $L = 4$. The state $|\chi_1\rangle^{\otimes 4}$ is prepared and the individual \mathcal{H}_Q -parts jointly transmitted through the channel \mathcal{E} . One of the 4 states is then randomly selected, as represented by the solid arrow, and this pair of Alice's and Bob's X -basis measurements is compared. The error rate δ_x then gives the probability of their results being different.

Key question

If $|\chi_0\rangle = |\chi_1\rangle$ the proof would of course immediately follow, since $\delta_{\text{ph}} = \delta_x$. In the general case however, $|\chi_0\rangle \neq |\chi_1\rangle$, as long as Equation 5.7 is satisfied; the key question to investigate is then:

Question 5.1. Given two *arbitrary* states $|\chi_0\rangle, |\chi_1\rangle$ that satisfy Equation 5.7, how much can δ_{ph} and δ_x defined in Section 5.2.1 possibly differ for a given L ?

5.2.2 Koashi's theorems

[Koa09] presents an analysis of the situation proposed in Question 5.1 and suggests two methods for finding an upper bound on the phases error rate δ_{ph} . The first method follows an argument based on the entropic uncertainty relation [MU88] and is stated as:

Theorem 5.2. *In a protocol with fair random sampling and with states $|\chi_0\rangle, |\chi_1\rangle$ satisfying Equation 5.7 for some parameter F , the error rates δ_x and δ_{ph} satisfy*

$$1 - h\left(\frac{1-F}{2}\right) \leq \frac{\delta_x + \delta_{\text{ph}}}{2} h\left(\frac{\delta_x}{\delta_x + \delta_{\text{ph}}}\right) + \frac{2 - \delta_x - \delta_{\text{ph}}}{2} h\left(\frac{1 - \delta_{\text{ph}}}{2 - \delta_x - \delta_{\text{ph}}}\right) \quad (5.8)$$

independent of the parameter L .

[Koa09] argues however that this inequality is not tight and presents another, longer analysis to find a better bound. The main argument is supplied by quoting a result from an earlier paper on random sampling [TKI03], which finally gives the result:

Theorem 5.3. *In a protocol with fair random sampling and with states $|\chi_0\rangle, |\chi_1\rangle$ satisfying Equation 5.7 for some parameter F , the error rates δ_x and δ_{ph} satisfy:*

$$F \leq \sqrt{(1 - \delta_x)(1 - \delta_{\text{ph}})} + \sqrt{\delta_x \delta_{\text{ph}}} \quad (5.9)$$

independent of the parameter L .

Theorem 5.3 is a stronger claim and will form the topic of this section. Theorem 5.2 is not pursued further here, but will be revisited in Section 6.3.

Given a specific, measured δ_x , the above inequalities can be solved to obtain the maximum δ_{ph} allowed, in order to provide an upper bound on the error rate needed. This in turn allows the general source protocol from Section 5.1.4 to satisfy the assumptions for the security proof.

The theorems do however not provide a unconditional answer to Question 5.1; rather, the result is given under the additional requirement of *fair random sampling*. This will be one of the key topics of this work and will be properly introduced in Section 5.2.6. It is however important to first get an understanding of how the situation proposed in Question 5.1 functions without any additional restrictions. In the following, we therefore investigate the validity of Theorem 5.3 purely in the context of Section 5.2.1 and Figure 5.1, by considering simplifying cases.

5.2.3 Single state

For $L = 1$, as illustrated in Figure 5.2, the situation is as follows: A state $|\chi_a\rangle$ (that can be either $|\chi_0\rangle$ or $|\chi_1\rangle$) is prepared and the \mathcal{H}_Q -part sent through a quantum channel \mathcal{E} . Then X -basis measurements are done on \mathcal{K}_A and \mathcal{H}_B . δ_{ph} and δ_x are found as the probability of the two measurements disagreeing in the $a = 0$ and $a = 1$ case respectively. Question 5.1 then corresponds to asking how different these two probabilities can be.

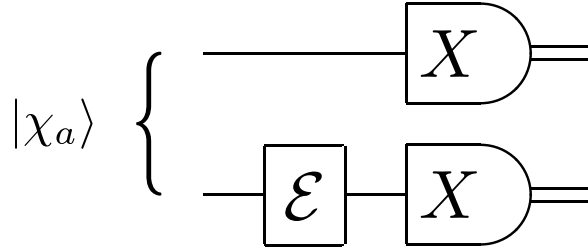


Figure 5.2: Error rate analysis model for $L = 1$. The $|\chi_a\rangle$ -state's qubit lines represents \mathcal{K}_A and \mathcal{H}_Q from the top. \mathcal{H}_S is not needed and is suppressed. \mathcal{E} represents the channel.

Theorem 5.3 is easily seen to follow from the monotonicity (Equation 3.2.3) and POVM minimization equivalence (Equation 3.23) of the fidelity measure: Confirming whether the measurements disagree can be implemented by an XOR gate on the outputs and a single measurement to determine the parity. In line with Theorem 2.8 the classical XOR can be replaced by its quantum equivalent CNOT to express the probability of disagreement as a single quantum measurement. This measurement has outcome probabilities δ_{ph} , $1 - \delta_{\text{ph}}$ in the case of $|\chi_a\rangle = |\chi_0\rangle$, and δ_x , $1 - \delta_x$ when $|\chi_a\rangle = |\chi_1\rangle$. By expressing the channel \mathcal{E} as a quantum operation on the whole state $\mathcal{F} = I \otimes \mathcal{E}$ it is seen that:

$$\begin{aligned} F(p_m, q_m) &\geq F[\mathcal{F}(|\chi_0\rangle\langle\chi_0|), \mathcal{F}(|\chi_1\rangle\langle\chi_1|)] \geq F(|\chi_0\rangle, |\chi_1\rangle) \\ &\Rightarrow \sqrt{(1 - \delta_x)(1 - \delta_{\text{ph}})} + \sqrt{\delta_x \delta_{\text{ph}}} \geq F, \end{aligned} \quad (5.10)$$

which proves Equation 5.9 for $L = 1$.

5.2.4 Double disconnected state

The second case to consider is $L = 2$. Additionally we will begin the analysis by making the restricting of the channel being disconnected, i.e. it acts as *individual* quantum operations on its input states. The situation, as illustrated in Figure 5.3, is as follows: Two copies of either $|\chi_0\rangle$ or $|\chi_1\rangle$ are created, denoted as $|\chi_a\rangle^{\otimes 2}$. The \mathcal{H}_Q -parts are then *individually* transmitted through a quantum channel \mathcal{E} each. After conducting X -basis measurements on two pairs of \mathcal{K}_A and \mathcal{K}_B , one of the two pairs is selected at random. δ_{ph} and δ_x are then found as the probability of disagreement in the measurements of the randomly selected pair, in the $a = 0$ and $a = 1$ case respectively. The question is as always how different these probabilities can be.

This situation can be analyzed in the same manner as in Section 5.2.3. There is however the

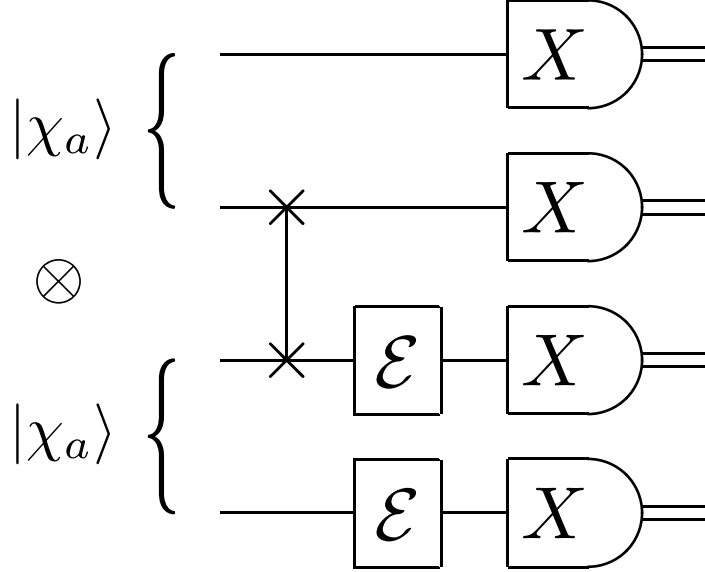


Figure 5.3: Error rate analysis model for $L = 2$ with a disconnected channel. The $|\chi_a\rangle$ -states' qubit lines represent \mathcal{K}_A and \mathcal{H}_Q , whereas \mathcal{H}_S is suppressed. \mathcal{E} are the individual channels. Initially, qubit lines 1 + 3 represent Alice's states, whereas lines 2 + 4 Bob's states. Because its convenient to separate Alice's from Bob's side, the SWAP operation is included to diagrammatically collect each party's states.

additional need for a method to calculate the probability of a random selection. Luckily, in this case of a uniformly random selection, the method is relatively trivial: For each basis choice a , let the probability of disagreeing measurements in pair k be denoted

$$p_{ak}^{\text{error}}; \quad k = 1, \dots, L; \quad a \in \{0, 1\}. \quad (5.11)$$

E.g. in this case $k \in \{1, 2\}$.

The probability of a uniformly randomly selected pair among the L pairs to disagree is then simply given by the arithmetic mean, so that δ_{ph} and δ_x are given by:

$$\delta_{\text{ph}} = \frac{1}{L} \sum_{k=1}^L p_{0k}^{\text{error}} \quad (5.12a)$$

$$\delta_x = \frac{1}{L} \sum_{k=1}^L p_{1k}^{\text{error}}, \quad (5.12b)$$

Trivial generalization

The first approach to analyze this situation is to represent the various measurements and averages as a single, total quantum measurement. Subsequently, the channel can similarly still be represented as a quantum operation. This immediately lead to the trivial generalization

of Equation 5.10 for *arbitrary* L :

$$\begin{aligned} F(|\chi_0\rangle^{\otimes L}, |\chi_1\rangle^{\otimes L}) &\geq F^L \\ \Rightarrow \sqrt{(1 - \delta_x)(1 - \delta_{\text{ph}})} + \sqrt{\delta_x \delta_{\text{ph}}} &\geq F^L \end{aligned} \quad (5.13)$$

This approach is however not very useful, since it leads to a lower bound in Equation 5.9 that *decreases in* L . The protocol relies on sending a large number of states, so that we are essentially interested in the large L limit. In that case, this would result in a property on the input states that will always be satisfied and thus providing no information about the error rate.

Remedy for the disconnected channel

In the case of a disconnected quantum channel there is however a much simpler method. As there is no interaction between the two state-and-measurement pairs, each pair can be analyzed individually. The pairs therefore both separately follow the exact same analysis as in Section 5.2.3. Since the probability of error in each state satisfies Equation 5.9, it must follow that their average satisfies the same condition. Thus the result holds for the double disconnected case.

5.2.5 Double joint state

The final case to consider is again $L = 2$, but now with a joint quantum channel. The situation is illustrated in Figure 5.4, and is identical to that of Section 5.2.4 except that the channel acts *jointly* on the two transmitted \mathcal{H}_Q -parts.

Despite being almost identical to that of Section 5.2.4, the method by which to address the problem in this case is not obvious. The first approach suggested in the previous section still suffers from the same degradation of usefulness as $L \rightarrow 0$. The second approach is however also not possible this time, since it relied on the assumption that the states do not interact.

Quite contrary, there seems to be a possibility of constructing a concrete counterexample for this situation under certain conditions. For instance, in the case that

$$|\chi_a\rangle = |+\rangle \otimes |\psi_a\rangle; \quad \forall a = 0, 1 \quad (5.14)$$

for some $|\psi_a\rangle$, the states $|\chi_0\rangle$ and $|\chi_1\rangle$ are clearly only distinguished by the part that is sent through the channel \mathcal{E} and therefore admit a POVM measurement on the joint state that can distinguish them with classical fidelity $F^2 < F$. Since Alice's measurement outcomes are fixed, Bob's POVM outcomes will therefore translate directly into error rates δ_x and δ_{ph} .

This is however an extreme situation in the sense that it can definitely never be used in an

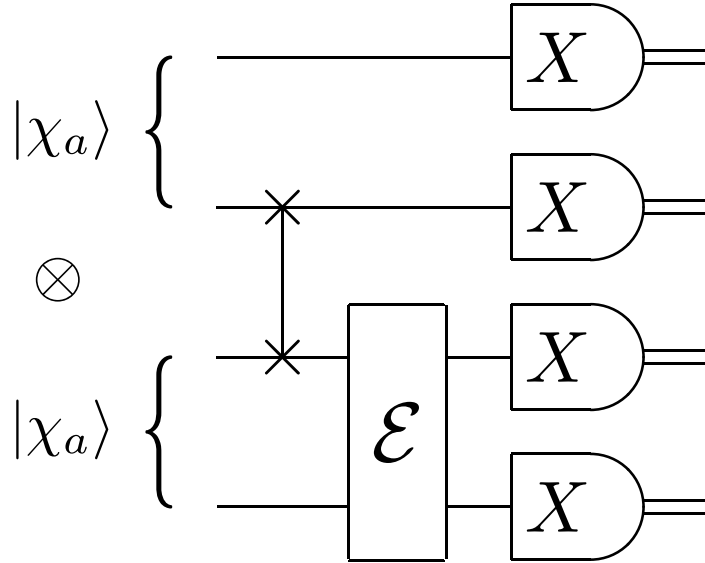


Figure 5.4: Error rate analysis model for $L = 2$ with a joint channel. The $|\chi_a\rangle$ -states' qubit lines represent \mathcal{K}_A and \mathcal{H}_Q , whereas \mathcal{H}_S is suppressed. The SWAP operations is added to make the diagram easier by collecting Alice's and Bob's measurements separately. Note the key difference from Figure 5.3 in that the channel \mathcal{E} now acts jointly on the input states.

actually functioning protocol. For realistic states $|\chi_0\rangle$ and $|\chi_1\rangle$, the situation is much more complicated: First, there are different reduced states that are sent through the channel \mathcal{E} depending on Alice's 4 measurement results. Violating Equation 5.9 then requires a channel that is able to distinguish all the 4 pairs of reduced states with classical fidelity better than F on average for the 4 state pairs. This must however simultaneously be done so that it is not simply Bob's measurement results that are distinguished at this rate, but the probability of errors between Alice and Bob's measurements. Finally, it must be constructed so that this in fact holds for error probabilities averaged also over the 2 measurement pairs.

It is therefore not clear under exactly what circumstances Equation 5.9 might hold in this case. Specifically, under any situation that could possibly exist for an functioning protocol, there is no clear answer. In fact it seems that there is no method based on general quantum operations that can capture the full interaction between the fidelity requirement on the states in Equation 5.7 and the fact that the channel only acts on Bob's half. And at the same time, considering specific cases is equally unproductive since the channel and states are otherwise uncharacterized. It is indeed not obvious how to proceed with the analysis of the validity of Equation 5.9 in this situation for realistic parameters.

5.2.6 Random sampling

In light of the discussion in Section 5.2.5, one important question is apparent: how can Theorem 5.3 hold when we have motivated a specific counterexample in the case of $L = 2$. The resolution to this paradox comes from the additional assumption stated in its description, namely that it holds for protocols with *fair random sampling*. Specifically it relates to the order that the various operations are applied and when information becomes available.

To get an idea, let us consider a concrete example of how the situation of an actual protocol looks, as depicted in Figure 5.5a. Here, Alice and Bob have chosen basis values \mathbf{a} and prepared a sequence of the corresponding states $|\chi_0\rangle / |\chi_1\rangle$ that have been sent through the channel. Focusing only on finding the error rates, we now let Alice and Bob conduct X -basis measurements on these states. It is then clear that this matches the description of Section 5.2.1, with jointly sent *collections* of states $|\chi_0\rangle^{\otimes L_0}$ and $|\chi_1\rangle^{\otimes L_1}$ giving average probabilities of a measurement error as δ_{ph} and δ_x respectively.

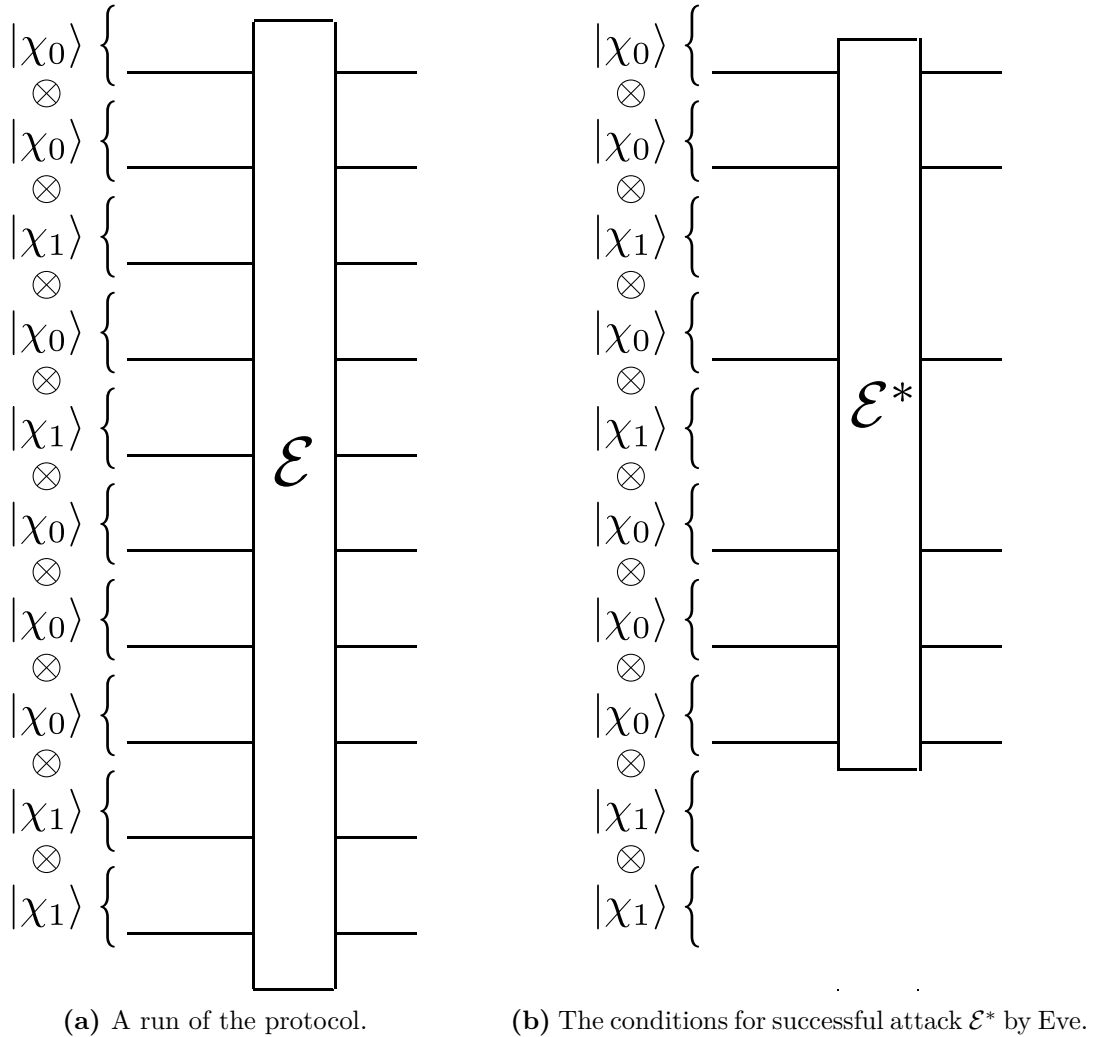


Figure 5.5: Example of a deployment of the protocol: A sequence of states $|\chi_0\rangle$ and $|\chi_1\rangle$ are prepared randomly and the \mathcal{H}_Q -part of all of them jointly sent through the channel \mathcal{E} . The other parts of $|\chi_a\rangle$ are suppressed, as well are the measurements.

Eve aims to attack these collections $|\chi_a\rangle^{\otimes L_a}$ by maximizing the error rate of the $|\chi_0\rangle$ states compared to the $|\chi_1\rangle$ states. At first it appears that there is indeed a possibility of performing such an attack in violation of Theorem 5.3: In line with section Section 5.2.5 it is possible to use a joint channel working on all the $|\chi_0\rangle$ states combined, so that the average error rate is increased more than it could if Eve had attacked only one of the $|\chi_0\rangle$ states. Since we are assuming that the operation of the source is known to Eve *before* the attack, she can use the exact values of $|\chi_0\rangle$ and $|\chi_1\rangle$ to construct an ideal attack operation \mathcal{E}^* . Eve can the

presumably deploy this on the channel, acting on the $|\chi_0\rangle$ states according to Figure 5.5b.

There is however a flaw in this analysis, again relating to the order of operations. Whereas the characterization of the source states $|\chi_a\rangle$ is made *before* the attack, revealing the information about Alice's and Bob's choice of when to send which basis is done *after* the attack. Notice on the other hand, in Figure 5.5b, that Eve's attack operation was assumed to act jointly on a collection of either $|\chi_0\rangle^{\otimes L_0}$ or $|\chi_1\rangle^{\otimes L_1}$ states. Although Eve does not need to know the order these collections of states are sent, she does in fact need to act jointly on a *collection of one state*. Concretely, in Figure 5.5b there is an implicit assumption that Eve knows exactly on which states to apply the attack operation \mathcal{E}^* .

We are now in a position to formally define the assumptions of Theorem 5.3 and Theorem 5.2. A protocol is said to exhibit *fair random sampling* when the states used for error estimation are representative for the whole protocol and consecutive basis choices a are *completely independent*, i.e. uncorrelated. In such a situation, it follows that Eve's attack is not possible, since it relies on identifying collections of one particular state. Specifically, for any one transmitted state $|\chi_a\rangle$ that Eve is looking to attack, all the preceding and following states have an *uncorrelated* probability of being $|\chi_0\rangle$ or $|\chi_1\rangle$. Thus the *average* result of such an attack is simply that where all preceding and following states are treated as mixed states of the two basis choices $|\chi_0\rangle, |\chi_1\rangle$, so that they are in particular *constant*. Consequently, Eve cannot gain anything by entangling multiple states in a joint attack. The situation therefore reduces to the disconnected case in Section 5.2.4, which informally proves Theorem 5.3 for arbitrary L .

This argument is however dependent on fair (perfect) random sampling of the basis states, which is indeed a very strict requirement. Moreover, it was indicated in Section 5.2.5 that the existence of the attack operation \mathcal{E}^* was not even obvious, at least for all interesting situations. If such an operation does in fact not exist, the security proof of Theorem 5.3 would be relieved of the stringent random sampling requirement, providing a much stronger security statement. As will be discussed in Chapter 7, this would allow providing proof for a much wider range of situations and sources, specifically when there are correlations between the states.

We would therefore like to investigate the validity of Koashi's theorem, but with the additional random sampling requirement removed. We begin by formulating the conjectures:

Conjecture 5.4. *Theorem 5.2 holds true without the requirement of fair random sampling. To reiterate:*

For arbitrary states satisfying Equation 5.7 for some parameter F , the error rates δ_x and δ_{ph} obey:

$$1 - h\left(\frac{1-F}{2}\right) \leq \frac{\delta_x + \delta_{\text{ph}}}{2} h\left(\frac{\delta_x}{\delta_x + \delta_{\text{ph}}}\right) + \frac{2 - \delta_x - \delta_{\text{ph}}}{2} h\left(\frac{1 - \delta_{\text{ph}}}{2 - \delta_x - \delta_{\text{ph}}}\right)$$

independent of the parameter L .

Conjecture 5.5. *Theorem 5.3 holds true without the requirement of fair random sampling. To reiterate:*

For arbitrary states satisfying Equation 5.7 for some parameter F , the error rates δ_x and δ_{ph} obey:

$$F \leq \sqrt{(1 - \delta_x)(1 - \delta_{\text{ph}})} + \sqrt{\delta_x \delta_{\text{ph}}}$$

independent of the parameter L .

Note that the validity of these conjectures are in itself not the point. In fact, in Section 5.2.5 we already motivated the possibility of a counterexample to Theorem 5.3; rather, as was pointed out, the case to investigate is under exactly what circumstances these conjectures hold. The difficulty is however that the traditional analytical methods do not seem to offer an efficient way to investigate the model. We therefore propose another approach: in the next chapter, we develop models and specific tools to treat the problem numerically.

5.2.7 Larger values of L

To conclude this chapter, we include for reference a couple of circuit models for the case of $L > 2$. These are not part of the analysis of Conjecture 5.5 presented in this section, but will be revisited in Section 6.1.7 and Section 6.3. From Figure 5.6 and Figure 5.7 it should be clear how the circuit generalizes for arbitrary L .

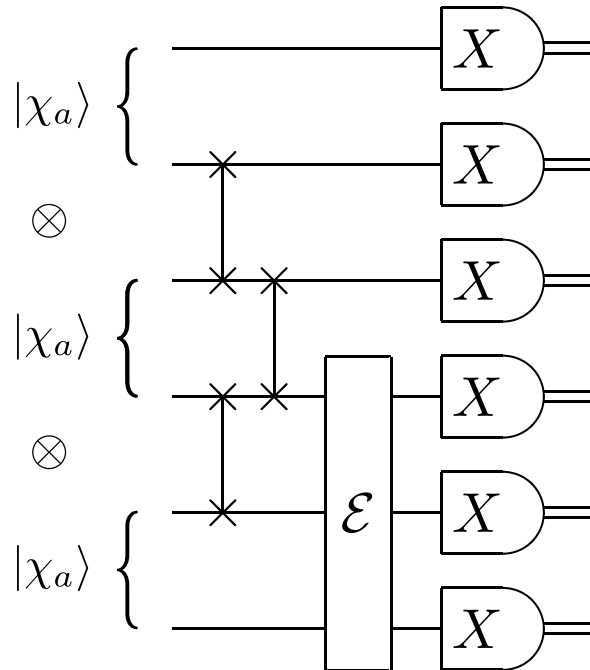


Figure 5.6: Error rate analysis model for $L = 3$ with a joint channel. The $|\chi_a\rangle$ -states' qubit lines represent \mathcal{K}_A and \mathcal{H}_Q , whereas \mathcal{H}_S is suppressed.

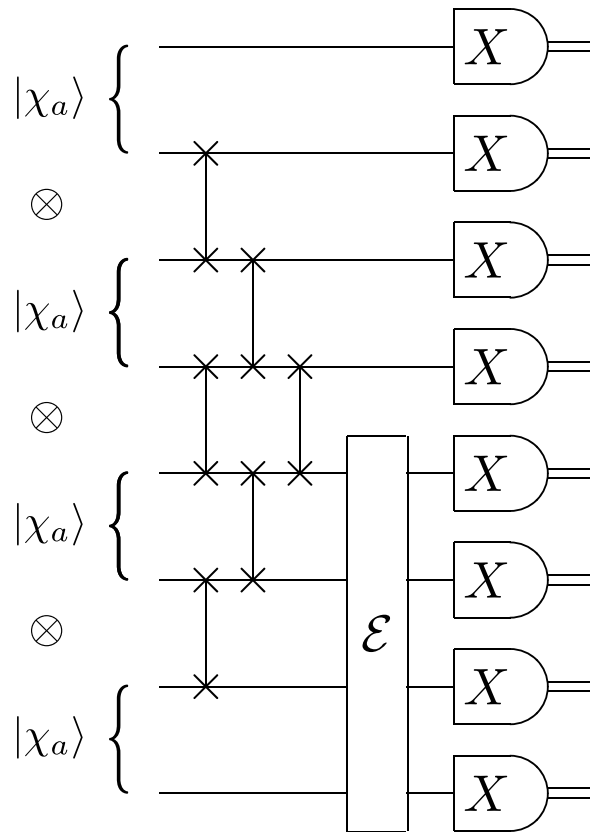


Figure 5.7: Error rate analysis model for $L = 4$ with a joint channel. The $|\chi_a\rangle$ -states' qubit lines represent \mathcal{K}_A and \mathcal{H}_Q , whereas \mathcal{H}_S is suppressed.

Chapter 6

Numerical investigation

The previous chapter investigated the impact of basis-dependent imperfections in Alice’s source when deploying the BB84 protocol [BB84]. It was further shown that the security in this case relies on Alice and Bob being able to accurately estimate the phase error rate δ_{ph} , even when it is not equal to the observable error rates δ_z and δ_x . We then presented Theorem 5.3 by Koashi [Koa09], but noted that it relied on a stringent requirement of perfect random sampling of the basis states. Finally we argued that it is not mediately clear that this assumption is in fact necessary, at least for all practical situations. This formed the basis for Conjecture 5.4 and Conjecture 5.5, which suggests that the theorem could be valid without this assumption.

This section proposes to investigate Conjecture 5.5 by doing a numerical simulation of the protocol. We furthermore specialize to the situation in Section 5.2.5, where the source states are perfectly correlated. By looking at specific examples of source states and channels, we can hopefully gain some insight into this claim and why it does or does not hold. Specifically, challenging the claim would, as always, only require a single counterexample. Although we have already motivated the existence of such a counterexample to Conjecture 5.5 in Section 5.2.5, it is instructive to begin the development of the numerical tools by investigating its validity and hopefully find concrete support for this idea. We can then tackle the question of whether counterexamples exist in the realistic regime.

6.1 Investigation 1

A procedure to do numerical tests of Conjecture 5.5 was devised, implementing the simplest case that does not hold trivially: $L = 2$. The idea is to generate random, *particular* numerical examples of all variables involved, namely the input states $|\chi_0\rangle, |\chi_1\rangle$ and the quantum channel \mathcal{E} . The states must of course be selected to still satisfy condition Equation 5.7. The various measurement probabilities can then simply be explicitly calculated by performing the action of the circuit in Figure 5.4. Finally δ_{ph} and δ_x are obtained and we can check:

Question 6.1. Do there exist combinations of states $|\chi_0\rangle, |\chi_1\rangle$ and a channel \mathcal{E} that violate Conjecture 5.5?

6.1.1 Simplifying restrictions

To facilitate the process of making a random sampling of the various variables, a few restrictions are made. Of course, if a counterexample is not found, these restrictions can then be revised and relaxed.

First, the source states ρ_{ab} are all assumed pure single-qubit states, meaning that \mathcal{H}_S is not needed. This means that the states $|\beta_{ab}\rangle$ are also all single-qubit states, and $|\chi_a\rangle$ are then 2-qubit states. Furthermore, \mathcal{H}_Q and \mathcal{H}_B are also assumed to be qubit spaces so that everything can be treated as qubits. Second, the quantum channel \mathcal{E} is assumed to simply be a unitary operation U , operating on the 2 qubits.

Lastly, the required property Equation 5.7 for the states $|\chi_a\rangle$ is also restricted from above, so that

$$F_1 \leq |\langle \chi_0 | \chi_1 \rangle| \leq F_2, \quad (6.1)$$

where $F_1 = F$ for some F we choose, and which is used in Equation 5.9. By this construction it is clear that all states generated satisfy the required property Equation 5.7. At the same time it is clear that states satisfying this property for a much greater parameter $F' \gg F_1$ will have a much smaller probability of violating Equation 5.9. We therefore choose to also bound the fidelity from above by F_2 , to maximize the probability of finding a counterexample.

Another important consideration is to ensure that the randomly generated quantities are chosen somewhat *uniformly*. This is of course no requirement, since we are only interested in finding a single, specific counterexample. Yet, if there is a strong bias for a particular set of states or channels, it may become significantly less likely to pick the ones that happen to produce the desired result. The solution chosen here is therefore to pick all variables completely uniformly at random, and then *check* if they happen to satisfy the required properties. This is of course a highly inefficient method because a very large number of trials are on average needed to find variables that are valid. Nevertheless, this approach was chosen because it has the advantage of guaranteeing a uniform sampling of the parameter space, thus making it less likely to systematically miss some choices.

6.1.2 Algorithm

Initially set a lower fidelity F_1 and upper fidelity F_2 . These values are fixed during one run, where the following steps are executed a large number of times M :

1. Pick 4 random single-qubit pure states $|\beta_{ab}\rangle$ uniformly. Pick two random probabilities p_0 and p_1 uniformly.

2. Construct $|\chi_0\rangle$ and $|\chi_1\rangle$ using Equation 5.6 and calculate their fidelity $F = |\langle\chi_0|\chi_1\rangle|$. If the fidelity happens to be within the desired range $F_1 \leq F \leq F_2$, proceed; if not, go back to step 1.
3. Pick a random 2-qubit unitary matrix U uniformly.
4. Construct the input states $|\chi_0\rangle^{\otimes 2}, |\chi_1\rangle^{\otimes 2}$. Calculate the output states $|\chi_0^{\text{out}}\rangle, |\chi_1^{\text{out}}\rangle$ that result from passing the input states through the channel, by:

$$|\chi_a^{\text{out}}\rangle = (I \otimes I \otimes U)(I \otimes \text{SWAP} \otimes I) |\chi_a\rangle^{\otimes 2}. \quad (6.2)$$

5. For each basis a , calculate the probability p_{ak}^{error} of the X -basis measurements in measurement-pair k disagreeing, as:

$$p_{ak}^{\text{error}} = \langle\chi_a^{\text{out}}| P_k |\chi_a^{\text{out}}\rangle, \quad (6.3)$$

for projective measurement operators

$$P_0 = \begin{aligned} &|+\rangle\langle+| \otimes I \otimes |-\rangle\langle-| \otimes I \\ &+ |-\rangle\langle-| \otimes I \otimes |+\rangle\langle+| \otimes I \end{aligned} \quad (6.4a)$$

$$P_1 = \begin{aligned} &I \otimes |+\rangle\langle+| \otimes I \otimes |-\rangle\langle-| \\ &+ I \otimes |-\rangle\langle-| \otimes I \otimes |+\rangle\langle+|. \end{aligned} \quad (6.4b)$$

6. Calculate the error probability of a random selection for each basis choice:

$$\delta_{\text{ph}} = \frac{1}{2}(p_{00}^{\text{error}} + p_{01}^{\text{error}}) \quad (6.5a)$$

$$\delta_x = \frac{1}{2}(p_{10}^{\text{error}} + p_{11}^{\text{error}}). \quad (6.5b)$$

7. Compute $\sqrt{(1 - \delta_x)(1 - \delta_{\text{ph}})} + \sqrt{\delta_x \delta_{\text{ph}}}$ and determine if it is in fact larger than F_1 as promised by Equation 5.9.

6.1.3 Uniformly generating variables

In line with the goal of uniformly sampling the parameter space, the algorithm makes several call for randomly generating various quantities *uniformly*. While it is clear how a random scalar number in a finite range can be uniformly sampled, it is not immediately obvious how this generalizes to the required quantities. This section provides a short description of the method by which the various quantities are randomly generated.

The single-qubit pure states $|\beta_{ab}\rangle$ are constructed from 3 real, random parameters γ, θ and ϕ , according to:

$$|\beta_{ab}\rangle = e^{i\gamma} \left(\cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle \right), \quad (6.6)$$

where γ gives the qubit a random phase while θ and ϕ characterize a random qubit by spherical coordinates of the Bloch sphere. By this reasoning, θ and ϕ are chosen to be sampled by a distribution that is uniform over the *area of the Bloch sphere*. A common method to achieve this probability distribution is to construct:

$$\gamma = 2\pi u \tag{6.7a}$$

$$\theta = 2\pi v \tag{6.7b}$$

$$\phi = \cos^{-1}(2w - 1), \tag{6.7c}$$

from real parameters u, v, w all picked randomly according to a uniform distribution on $[0, 1]$.

The 2-qubit unitary matrix U is constructed from two random, 4-by-4, real matrices A_1 and A_2 . Each matrix element is independently randomly selected from a Normal distribution $\mathcal{N}(0, 1)$. Then the two matrices are combined into a 4-by-4 random *complex* matrix $A_3 = A_1 + iA_2$. This matrix is then made into a Hermitian matrix $A_4 = (A_3 + A_3^\dagger)/2$ which is in turn used to construct the unitary matrix by $U = e^{iA_4}$.

6.1.4 Implementation

The algorithm was designed and checked using MathWorks MATLAB R2016b (win64). It was then optimized for speed by porting to 2 different computationally fast languages: one using a standard linear algebra approach and the other using a specialized framework for performing quantum simulations. Finally, the results were independently double-checked using Wolfram Mathematica 11.0.1.0 (win64).

The first method was written in Fortran2003, with the LAPACK¹ and BLAS² linear algebra software packages [And+99]. It was compiled with the GNU Fortran compiler (gfortran) on Ubuntu 16.04 LTS. The BLAS / LAPACK routines were first provided by LAPACK95³ version 3.0 and the Netlib open implementation version 3.6.0, and then using the optimized Intel MKL 2017 Update 2 for Linux⁴.

The other method was written in C++2017 using the Quantum++ quantum computing library⁵ [Ghe14], which is made specifically for simulating quantum processes. It was compiled with the GNU C++ compiler on Ubuntu 16.04 LTS.

Note that the Fortran program implemented the uniform sampling from Section 6.1.3, whereas the C++ program used pre-made sampling methods from the Quantum++ library.

¹<http://www.netlib.org/lapack/>

²<http://www.netlib.org/blas/>

³<http://www.netlib.org/lapack95/>

⁴<https://software.intel.com/en-us/mkl>

⁵<http://vsoftco.github.io/qpp/>

6.1.5 Results

The results of the Fortran and C++ simulations for $L = 2$, $F_1 = 0.99$ and $F_2 = 0.991$ are shown in Figure 6.1 and Figure 6.2 respectively.

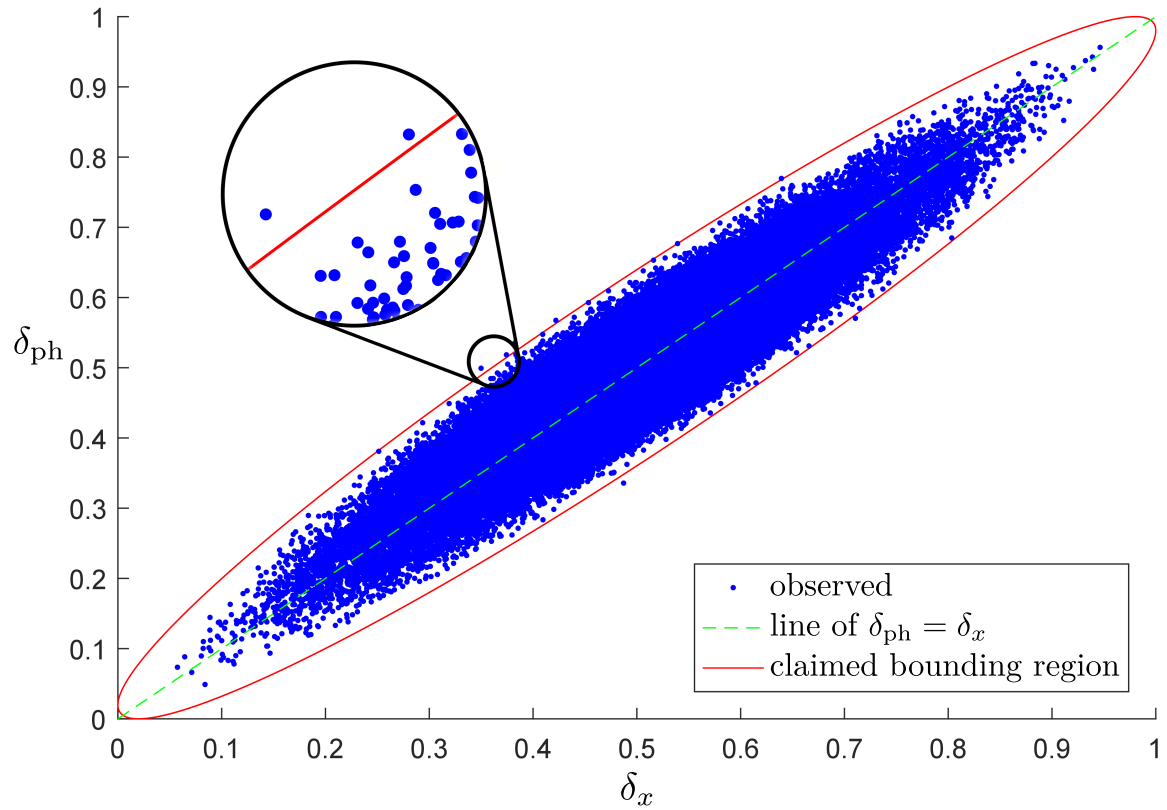


Figure 6.1: Fortran simulation: Scatter plot of δ_{ph} vs. δ_x for $L = 2$, $M = 80\,000$, $F_1 = 0.99$ and $F_2 = 0.991$. Each point is found from a single trial by the algorithm in Section 6.1.2. The dashed line is a visual aid showing where $\delta_{\text{ph}} = \delta_x$. The solid line labeled “claimed bounding region” is the extremal line for Equation 5.9 in that it encloses all combinations of δ_{ph} , δ_x for which it is satisfied. The bubble provides an closer view at a region of high interest. See also Table 6.1.

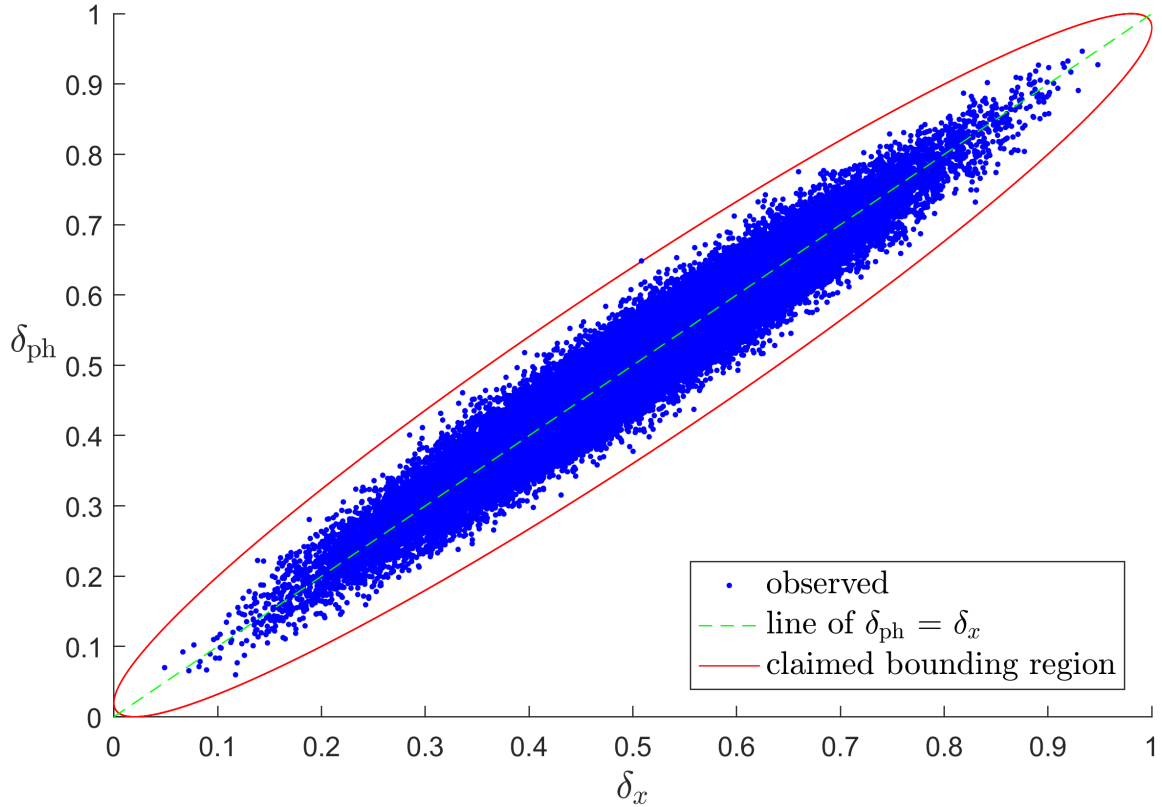


Figure 6.2: C++ simulation: Scatter plot of δ_{ph} vs. δ_x for $L = 2$, $M = 100\,000$, $F_1 = 0.99$ and $F_2 = 0.991$. Each point is found from a single trial by the algorithm in Section 6.1.2. The dashed line shows $\delta_{\text{ph}} = \delta_x$ and the solid line labeled “claimed bounding region” encloses the region of all combinations of $\delta_{\text{ph}}, \delta_x$ that satisfy Equation 5.9. See also Table 6.1.

The Fortran simulation identified 7 points among its $M = 80\,000$ total trials that were outside the valid region of $(\delta_x, \delta_{\text{ph}})$ points according to Equation 5.9. Similarly, the C++ simulation also found 1 point among its $M = 100\,000$ total trials that did not satisfy Equation 5.9. These points are *concrete* examples⁶ of states $|\chi_0\rangle, |\chi_1\rangle$ and a channel \mathcal{E} , for which Conjecture 5.5 does not hold. We have therefore provided definite proof for the answer “yes” to Question 6.1.

It is also interesting to observe that the final distribution of points in the $\delta_{\text{ph}}\text{-}\delta_x$ plane was notably different in the two simulations. The uniform sampling suggested in Section 6.1.3 clearly produced a more uniform final distribution of $(\delta_x, \delta_{\text{ph}})$ points than the built-in sampling method in the Quantum++ library. This difference is however of little importance here. The main takeaway is that two different simulation methods were both able to find examples for which Equation 5.9 was not satisfied.

6.1.6 Fixed parameter simulations

One immediate follow-up idea was to fix some of the parameters of the simulation to that of one of the counterexamples found in Section 6.1.5. Specifically, the algorithm in Section 6.1.2

⁶Concrete numerical values for one counterexample is provided in listing 1 in Appendix A.

calls for generating 2 sets of quantities: the states $|\chi_a\rangle$ and the channel matrix U . Two new simulations were conducted: First, a particular choice of states $|\chi_0\rangle^*$, $|\chi_1\rangle^*$ and matrix U^* were set to that of one of the counterexamples found in Figure 6.1. Then one simulation picked random matrices U as before, but the states were fixed $|\chi_0\rangle = |\chi_0\rangle^*$, $|\chi_1\rangle = |\chi_1\rangle^*$. The other simulation picked states $|\chi_a\rangle$ randomly as before, but the channel was fixed $U = U^*$.

Both simulations used $L = 2$, $F_1 = 0.99$ and $F_2 = 0.991$ and were run by the Fortran program. The results are shown in Figure 6.3 and Figure 6.4 respectively.

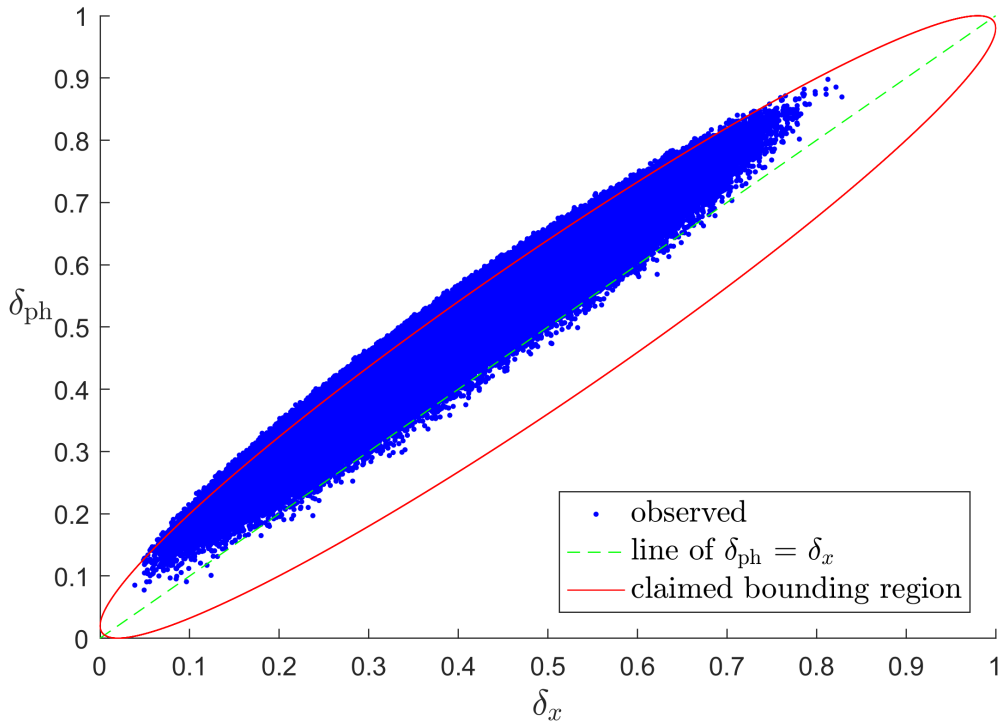


Figure 6.3: Fixed states: Scatter plot of δ_{ph} vs. δ_x for $L = 2$, $M = 1\,000\,000$, $F_1 = 0.99$ and $F_2 = 0.991$ with fixed states $|\chi_a\rangle = |\chi_a\rangle^*$. Each point is found from a single trial by the algorithm in Section 6.1.2. The dashed line shows $\delta_{\text{ph}} = \delta_x$ and the solid line labeled “claimed bounding region” encloses the region of all combinations of δ_{ph} , δ_x that satisfy Equation 5.9. See also Table 6.1.

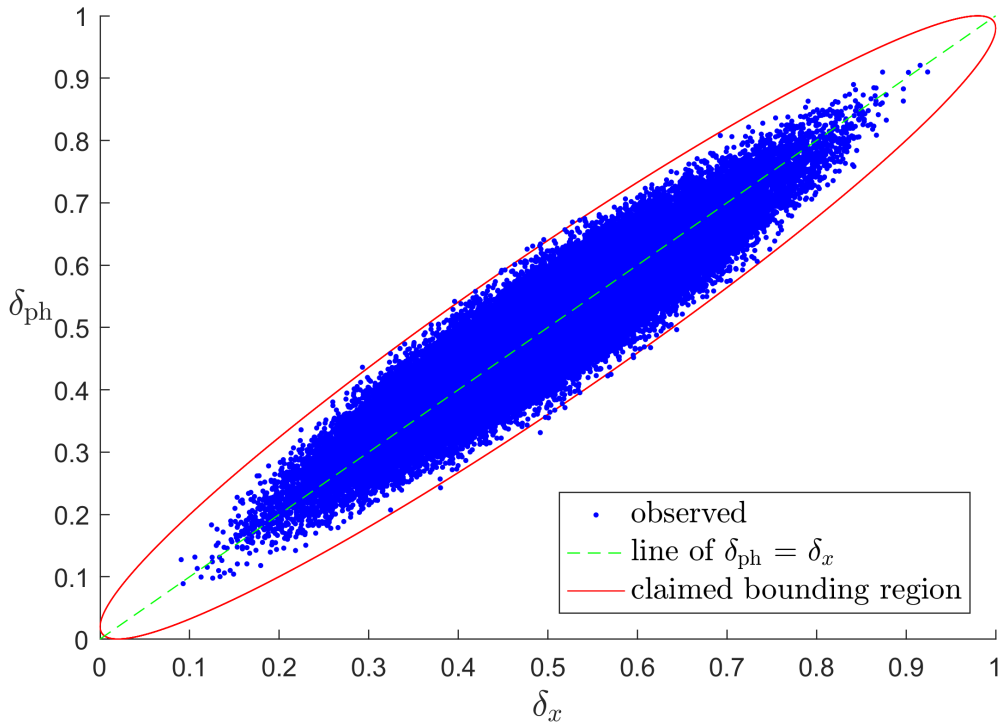


Figure 6.4: Fixed channel: Scatter plot of δ_{ph} vs. δ_x for $L = 2$, $M = 100\,000$, $F_1 = 0.99$ and $F_2 = 0.991$ with a fixed channel matrix $U = U^*$. Each point is found from a single trial by the algorithm in Section 6.1.2. The dashed line shows $\delta_{\text{ph}} = \delta_x$ and the solid line labeled “claimed bounding region” encloses the region of all combinations of $\delta_{\text{ph}}, \delta_x$ that satisfy Equation 5.9. See also Table 6.1.

Both of the new simulations identified several new counterexamples to Conjecture 5.5. Figure 6.4 shows that the simulation with a fixed channel matrix produced a slightly different distribution of $(\delta_x, \delta_{\text{ph}})$ points than the original simulation, but is overall fairly similar. Figure 6.3 on the other hand shows that fixing the state produced a notably different distribution and identified counterexamples at a much higher frequency than the original simulation. This seems to support the fact that certain states $|\chi_a\rangle$ are more prone to violating Equation 5.9 than others.

6.1.7 Other values of L

It is also interesting to see how the simulation behaves for other values of L . Specifically, simulations were conducted for the case of $L = 3$ and $L = 1$, with results shown in Figure 6.5 and Figure 6.6 respectively. Both simulations used $F_1 = 0.99$ and $F_2 = 0.991$ and were run by the Fortran program. Circuit diagrams for these situations are shown in Figure 5.2 and Figure 5.6 respectively.

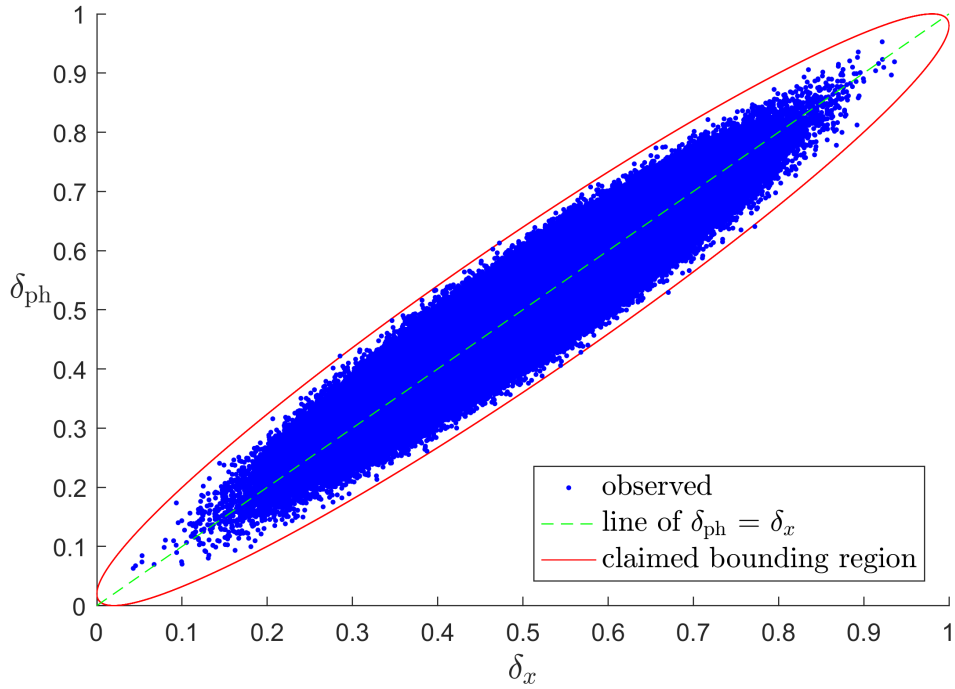


Figure 6.5: Scatter plot of δ_{ph} vs. δ_x for $L = 3, M = 1\,000\,000, F_1 = 0.99$ and $F_2 = 0.991$. Each point is found from a single trial by the algorithm in Section 6.1.2. The dashed line shows $\delta_{\text{ph}} = \delta_x$ and the solid line labeled “claimed bounding region” encloses the region of all combinations of $\delta_{\text{ph}}, \delta_x$ that satisfy Equation 5.9. See also Table 6.1.

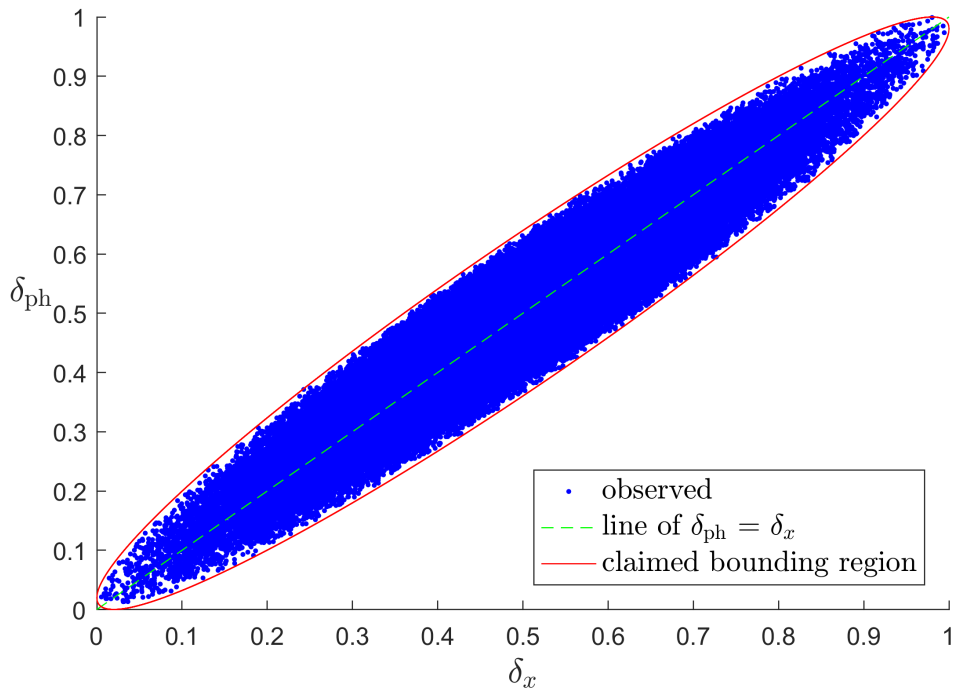


Figure 6.6: Scatter plot of δ_{ph} vs. δ_x for $L = 1, M = 100\,000, F_1 = 0.99$ and $F_2 = 0.991$. Each point is found from a single trial by the algorithm in Section 6.1.2. The dashed line shows $\delta_{\text{ph}} = \delta_x$ and the solid line labeled “claimed bounding region” encloses the region of all combinations of $\delta_{\text{ph}}, \delta_x$ that satisfy Equation 5.9. See also Table 6.1.

The results show a very good match with the theory developed in Chapter 5. Figure 6.5 illustrates that the probability of finding a counterexample by random sampling seems to *decrease* for increasing L . This is not surprising as the total parameter space increases for larger L , and so finding a point with a particular property becomes less likely. The simulation was still able to find 3 $(\delta_x, \delta_{\text{ph}})$ points out of $M = 1\,000\,000$ that do not satisfy Equation 5.9.

Additionally, Equation 5.10 showed that for $L = 1$, Equation 5.9 should in fact remain true. And this is precisely the result shown in Figure 6.6: out of the $M = 100\,000$ trials, all the observed $(\delta_x, \delta_{\text{ph}})$ points indeed satisfy Equation 5.9.

A summary of the exact number of counterexamples identified in each simulation is given in Table 6.1.

Table 6.1: Summary of quantitative results in Figure 6.1 - 6.6

Simulation type	L	Total number of trials M	Number of points violating (5.9)	Plotted in figure
Fortran, random	2	80 000	7	Figure 6.1
C++, random	2	100 000	1	Figure 6.2
Fortran, fixed state	2	1 000 000	39 343	Figure 6.3
Fortran, fixed channel	2	100 000	20	Figure 6.4
Fortran, random	3	1 000 000	3	Figure 6.5
Fortran, random	1	100 000	0	Figure 6.6

6.2 Investigation 2

The previous section presented the identification of explicit counterexamples to Conjecture 5.5. We are now in a position to evaluate the properties of the counterexamples: Are the concrete situations the examples correspond to realistic? Are there any systematic properties common to all the examples found? This section will begin by considering these questions and show that all the counterexamples found in the previous section are in fact *not* realistic. A new scheme is then proposed in order to search for examples that satisfy an additional set of properties to make them more realistic.

6.2.1 Finding realistic counterexamples

The initial reaction to the previous section is obviously to look at the actual numbers of the counterexamples. Checking the channel matrices U does not seem to reveal any trends, as may not be surprising since the number of parameters in a 4x4 complex, unitary matrix is quite large. Furthermore, U represents the action of the attacker Eve and should therefore not be restricted. Checking the states $|\beta_{ab}\rangle$ is similarly unproductive as it is hard to notice

any trends in the numbers. Furthermore, the $|\beta_{ab}\rangle$ states have already been assumed to be pure, so it is not clear if restricting them further would be interesting at this point.

There is however one trend that is immediately obvious, relating to the bit value probabilities p_0 and p_1 . Whereas p_0 seem to take on values in the range $[0, 1]$ fairly uniformly, p_1 is always very close to 0 or 1. In fact all the counterexamples produced in Section 6.1 have values of p_1 that are *outside* of the range $[0.1, 0.9]$. In step 1 of the algorithm in Section 6.1.2 the values of p_1 was chosen uniformly in $[0, 1]$, meaning that values of $p_1 \sim 0.5$ are evidently extremely unlikely to violate Equation 5.9 when performing a *uniform* parameter search. Note that this trend does however not contradict the validity of the counterexamples from Section 6.1. Conjecture 5.5 only relies on the assumption of Equation 5.7, which is indeed satisfied, and in particular it places no restrictions of p_0 and p_1 .

The problem with the extreme values of p_1 is that it represents a situation that is *easy to avoid*: p_a describes the probability of selecting bit value 0 given basis choice a . $p_1 \approx 0$ or $p_1 \approx 1$ therefore represents a situation where there is a high probability that only one of the qubit states is used for the X -basis. While this does not necessarily break security, it means that the outcome from Alice's random number generator for the bit choice is heavily skewed. All the counterexamples discovered therefore corresponds to Alice having a very poor random number generator. In addition to being something Alice can easily fix, the original proof Section 4.2 already relies inseparably on (nearly) perfect random number generators.

It is therefore interesting to know whether it is possible to construct a counterexample where $p_1 \approx 0.5$ and exactly *how close* to 0.5 it is possible to get. In particular, we may ask:

Question 6.2. Do there exist combinations of states $|\chi_0\rangle, |\chi_1\rangle$ and a channel \mathcal{E} that violate Conjecture 5.5 *and* that have realistic properties: $p_0 = 0.5, p_1 = 0.5$?

The other problematic trend in the counterexamples from Section 6.1 is that they always lead to very high error rates. As with extreme values of p_1 , note however that the validity of the counterexamples is in this case also not challenged because Conjecture 5.5 makes no assumptions about the error rates δ_x, δ_z and δ_{ph} . At the same time, high values of δ_{bit} and δ_{ph} will obviously lead to a negative key gain from Equation 4.30, meaning that Alice and Bob cannot actually run the protocol. We are therefore interested in investigating if a counterexample can exist also in the operational regime:

Question 6.3. Do there exist combinations of states $|\chi_0\rangle, |\chi_1\rangle$ and a channel \mathcal{E} that violate Conjecture 5.5 *and* that predict a positive key gain G (Equation 4.30)?

Note that there are two possible interpretations for predicting the key gain G :

1. From the measured error rates δ_z and δ_x , calculate the maximum *predicted* phase error δ_{ph}^* using the conjectured Equation 5.9. Then calculate the *predicted* minimum key gain G^* from Equation 4.30 using $\delta_{\text{bit}} = \delta_z$ and $\delta_{\text{ph}} = \delta_{\text{ph}}^*$.

2. Or from the *true* measured error rates δ_{ph} and $\delta_{\text{bit}} = \delta_z$, calculate the *true* key gain G from Equation 4.30.

In addition, as is seen from the plots in Section 6.1, the counterexamples to Conjecture 5.5 that were produced do not distinguish between a true value of δ_{ph} that is too high or too low; they only assert that there exist examples where δ_{ph} is more different from δ_x that Equation 5.9 predicts is possible. Of course examples where δ_{ph} is in fact lower than δ_x is not particularly interesting, since it simply means that the protocol is *more* secure than Conjecture 5.5 suggests.

For counterexamples to Conjecture 5.5 that also satisfy $\delta_{\text{ph}} > \delta_x$, the interpretations for Question 6.3 is however easily simplified: Since such an example would obviously have a true δ_{ph} that is higher than the maximum predicted value δ_{ph}^* , we can focus on finding counterexample according to the second interpretation (positive, *true* key gain G). Note also that if such an example can be found, constructing a new counterexample that satisfies *only* the first interpretation is relatively trivial⁷. We therefore rephrase Question 6.3 into a more restrictive version:

Question 6.4. Do there exist combinations of states $|\chi_0\rangle, |\chi_1\rangle$ and a channel \mathcal{E} that violate Conjecture 5.5 *and* satisfy $\delta_{\text{ph}} > \delta_x$ *and* that imply a positive, *true* key gain G (Equation 4.30)?

6.2.2 Algorithm

The full detail of the algorithms used to investigate Question 6.2 and Question 6.3 is too involved to be included here, and we will only give a rough sketch of its operation. The core functionality is the same as that of Section 6.1.2: Pick a lower bound F for Equation 5.7, a set of states $|\beta_{ab}\rangle$, probabilities p_a and a channel \mathcal{E} , and determine $\delta_x, \delta_{\text{ph}}$ by explicitly simulating the protocol. Also as before, we are considering $L = 2$ and pure $|\beta_{ab}\rangle$.

The new components of the algorithm regard the method by which to choose the various quantities. First of all, the probabilities are now fixed $p_a = 0.5; \forall a = 0, 1$. Second, selecting the states $|\beta_{ab}\rangle$ randomly and then *checking* whether Equation 6.1 holds is a very slow process. Instead, we now consider a more analytic approach:

1. Pick 1 of the 4 $|\beta_{ab}\rangle$ states at random and generate the *other* 3 in line with Section 6.1.3. It can then be shown that finding the last state $|\beta_k\rangle$ so that Equation 5.7 holds is always reducible to it instead satisfying

$$|c + \langle \tilde{\gamma} | \beta_k \rangle| = F, \quad (6.8)$$

for suitable choices of an *unnormalized* state $|\tilde{\gamma}\rangle$ and complex number c , that depend

⁷Given a channel \mathcal{E} , it is always trivial to make small adjustments to it so that the error rates *increase* slightly.

on the 3 other $|\beta_{ab}\rangle$ states and the probabilities p_a .

2. Determine the range of possible complex numbers z that satisfy $|z + c| = F$; if there are none, go back to step 1. Otherwise, proceed by making a random choice of z *uniformly* among the allowed values.
3. From the orthogonal subspace of $|\tilde{\gamma}\rangle$, pick a state $|\delta\rangle \in |\tilde{\gamma}\rangle^\perp$ uniformly at random. The last state can then be constructed as

$$|\beta_k\rangle = K|\delta\rangle + z\frac{|\tilde{\gamma}\rangle}{\|\tilde{\gamma}\|^2}, \quad (6.9)$$

where K is chosen so that $|\beta_k\rangle$ is normalized.

Third, we consider a new method for picking channels \mathcal{E} . The previous method where the selection is limited to unitary matrices U is clearly very restrictive. Numerous algorithms performing a uniform search among more general quantum operations \mathcal{E} were implemented and tested extensively. All of these methods were however found to be too inefficient, as a random search in such a large parameter space has a very low probability of finding anything interesting. Therefore, a new method was devised to increase the chance of finding “good” channels:

1. Begin by focusing on Alice’s X -basis measurements: Given the two states $|\chi_a\rangle$ and probabilities p_a , calculate which one of Alice’s 4 possible measurement outcomes (00, 01, 10, 11) is the most likely *averaged over* the two basis choices $|\chi_0\rangle$ and $|\chi_1\rangle$. Calculate the reduced state σ_a that Alice sends to Bob in the event of this measurement outcome, for each of the two basis choices $a = 0, 1$.
2. Pick a random 2-qubit unitary matrix U in line with Section 6.1.3 to serve as the channel \mathcal{E} . Then calculate the result of sending the state σ_a through the channel U and find the 2 corresponding reduced states $\sigma_a^{(i)}$ on the two single-qubit systems $i = 1, 2$ after the channel. This is illustrated in Figure 6.7.

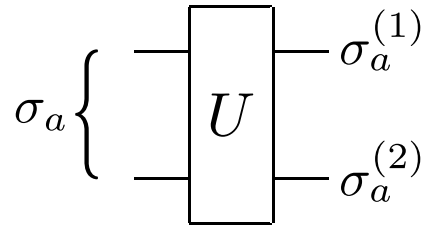


Figure 6.7: Circuit model for the definition of $\sigma_a^{(i)}$. σ_a is the reduced state Alice is most likely to send to Bob after conducting her measurement and U is the channel.

3. Calculate the fidelity between the basis choices for each subsystem: $F(\sigma_0^{(1)}, \sigma_1^{(1)})$ and $F(\sigma_0^{(2)}, \sigma_1^{(2)})$. If they are *both less* than the parameter F , continue; otherwise, return to step 1.
4. According to Equation 3.23 there now exists a POVM measurement $\{E_k^{(i)}\}$ that can

distinguish $\sigma_0^{(i)}$ from $\sigma_1^{(i)}$ better than F , on *each* of the two subsystems $i = 1, 2$.
Formally: $\exists \{E_k^{(1)}\}, \{E_k^{(2)}\}$ with measurement probabilities

$$\left. \begin{aligned} p_k^{(i)} &= \text{tr}(E_k^{(i)} \sigma_0^{(i)}) \\ q_k^{(i)} &= \text{tr}(E_k^{(i)} \sigma_1^{(i)}) \end{aligned} \right\} \forall i = 1, 2 \quad (6.10)$$

so that

$$F(p_k^{(i)}, q_k^{(i)}) < F; \quad \forall i = 1, 2. \quad (6.11)$$

5. Convert the combination of the unitary matrix U and two sets of POVM measurements $\{E_k^{(1)}\}, \{E_k^{(2)}\}$ into a single, equivalent quantum channel \mathcal{E} .

The new methods for selecting the states $|\chi_a\rangle$ and the channel \mathcal{E} have some important differences to the original algorithm of Section 6.1.2. First, due to the improved sampling of the states $|\beta_{ab}\rangle$, this new algorithm runs much faster and can thus search through more examples. Second, because of the construction of the channel \mathcal{E} from the two sets of POVM measurements, the channel is no longer limited to a unitary matrix but has instead 4 operator elements $\mathcal{E} : \{E_k\}_{k=1}^4$. The new algorithm can therefore try a much greater range of channels, while simultaneously limiting the search to the ones that are the most promising.

6.2.3 Implementation and results

The algorithm was designed and implemented in MathWorks MATLAB 2016b (win64). Because of the complexity of the algorithm and the improved run time, it was not ported to other languages.

After running for ~ 48 hours, the algorithm reported a successful discovery: It had found an example⁸ of states $|\chi_0\rangle, |\chi_1\rangle$ and a channel \mathcal{E} that did not satisfy Equation 5.9 *and* has $p_0 = p_1 = 0.5$. This provides a concrete counterexample to Conjecture 5.5 for the realistic situation of having a perfect random number generator for the bit selection! Thus we have provided definite proof for the answer “yes” to Question 6.2.

The success of the new algorithm did however not extend to Question 6.3. In fact, all the counterexamples it found had error rates δ_{bit} and δ_{ph} that were consistently ~ 0.5 , which is of course too high to give a positive key gain G .

6.2.4 Genetic optimization

To address Question 6.4, the focus was turned from a uniform search to an iterative one. The idea is to utilize some *optimization scheme* to systematically make small adjustments to the states $|\chi_a\rangle$ and channel \mathcal{E} . Given sufficient run time, the algorithm will hopefully be able to converge to an example that is consistent with all the requirements of Question 6.4.

⁸Concrete numerical values for this counterexample is provided in listing 2 in Appendix A.

The method to solve the optimization problem was chosen to be a *genetic algorithm*. The channel \mathcal{E} was fixed to consist of 4 operation elements $\{E_k\}_{k=1}^4$, which was then parametrized by a vector \mathbf{x} of 512 real numbers. The algorithm could then search for and make small variations to individuals of \mathbf{x} , which would then in turn be converted to the corresponding set $\{E_k\}_{k=1}^4$. The series of requirements in Question 6.4 were then formulated into *one* score function. This function was furthermore *continuous* in the requirements, so that the closer the properties of Question 6.4 were to being satisfied, the lower the score.

While this approach is well-suited for finding a good channel \mathcal{E} , it is not easily applied to the states $|\beta_{ab}\rangle$. The reason for this is that the highly sensitive requirement from Equation 5.7 is broken by the mutation step of the genetic approach and also not easily convertible to a linear constraint either. Instead we opted for a simpler solution: alternate between a genetic search for good channels \mathcal{E} and a uniform search for good states $|\beta_{ab}\rangle$. The latter of these searches is done by making random mutation to the states $|\beta_{ab}\rangle$ and then using the techniques from Section 6.2.2 to recalculate 1 of the states to ensure that Equation 5.7 is satisfied. The mutation is then evaluated using the *score function* developed above.

Implementation and further results

This hybrid algorithm was developed and run by MathWorks MATLAB 2016b (win64). The genetic optimization algorithm was further provided by the `ga` solver from the Global Optimization Toolbox for MATLAB. The counterexamples identified in Section 6.2.3 were then used as a *starting point* for the genetic solver.

The result from this method was a huge success! After running for another ~ 48 hours, the hybrid genetic algorithm identified an example⁹ of states $|\chi_0\rangle, |\chi_1\rangle$ and a channel \mathcal{E} with all the properties we are looking for: It does not satisfy Equation 5.9, gives error rates so that $\delta_{\text{ph}} > \delta_x$ and provides a positive, true key gain G from Equation 4.30. Furthermore, all this was achieved while *simultaneously* keeping the bit selection probabilities fixed to $p_0 = p_1 = 0.5$. This remarkable results thus provides a counterexample to Conjecture 5.5 that corresponds to both having a perfect random number generator *and* is in the operational regime of a positive key gain G .

We have thus provided definite proof that the answer to both Question 6.2 and Question 6.4 is in fact “yes”. Additionally, we have shown that there exists a situation that simultaneously satisfies the requirements for answering both these questions.

6.3 Investigation 3

The previous sections concluded with having found concrete evidence to disprove Conjecture 5.5. Furthermore, the specific counterexample was constructed to also satisfy all

⁹Concrete numerical values for this counterexample is provided in listing 2 in Appendix A.

additional properties that seem relevant. Looking back at Chapter 5, this was however not the only bound on the error rates that was suggested. We are also interested in investigating the necessity of the random sampling requirement in the other theorem from [Koa09], as stated in Conjecture 5.4. This section describes how the methods from the previous sections can be applied to investigate this claim as well.

6.3.1 Adjusting the algorithm

The first thing to check is of course whether Conjecture 5.4 still holds for the values of δ_x and δ_{ph} provided by the counterexamples to Conjecture 5.5. It turns out that it does in fact hold, which supports the earlier claim that Equation 5.8 is less strict than Equation 5.9. As before, we are therefore interested in investigating:

Question 6.5. Do there exist combinations of states $|\chi_0\rangle, |\chi_1\rangle$ and a channel \mathcal{E} that violate Conjecture 5.4?

It is possible to get an idea of why this might be the case by looking back at Equation 5.2.4. This restriction on δ_x and δ_{ph} was shown to hold for any L , but at the expense of a decreasing lower bound for increasing L . This seems to suggest that it may be possible to find larger differences between δ_x and δ_{ph} for systems with increasing L . Although the choice of simulating $L = 2$ was sufficient for investigating Conjecture 5.5, this means that this choice might in fact not allow finding counterexamples for Conjecture 5.4. Specifically, further comparison of these bounds suggests that a violation of Conjecture 5.4 cannot occur for $L < 4$.

We therefore consider the case of $L = 4$, as shown in Figure 5.7. The core idea is again to run a simulation of the protocol on this system for particular choices of F , $|\beta_{ab}\rangle$, p_a and \mathcal{E} to, and determine δ_x , δ_{ph} . The algorithm used was the same as in Section 6.2: First, a uniform search is done with the scheme for finding good states $|\beta_{ab}\rangle$ and channels \mathcal{E} from Section 6.2.2. Then, the hybrid search and genetic optimization approach from Section 6.2.4 is used to iteratively improve these parameters. Both these algorithms were of course updated to work for the case of $L = 4$. Specifically, the genetic optimization routine worked with a representation of the channel \mathcal{E} parameterized by a vector \mathbf{x} of 2048 real numbers.

As in the first investigation of Conjecture 5.5 in Section 6.1, we are initially interested in investigating the validity of Equation 5.8, without considering any additional requirements. In particular we are not limiting the search to states that satisfy $p_0 = 0.5$ and $p_1 = 0.5$ or that give a positive key gain G .

6.3.2 Implementation and results

The updated algorithm for $L = 4$ was implemented and run by MathWorks MATLAB 2016b (win64). The genetic optimization algorithm was again provided by the `ga` solver from the Global Optimization Toolbox for MATLAB.

This new method was also able to identify a counterexample¹⁰. Again a set of states $|\chi_0\rangle, |\chi_1\rangle$ and a channel \mathcal{E} was found that violated Equation 5.8. Note that this state does however *not* satisfy the additional properties of giving a positive key gain G or corresponding to a perfect random number generator for the bit values p_a . It nevertheless provides a concrete counterexample to Conjecture 5.4, thus providing proof for the answer “yes” to Question 6.5.

¹⁰Concrete numerical values for this counterexample is provided in listing 3 in Appendix A.

Chapter 7

Discussion

In Chapter 5 we presented a theory for treating basis-dependent imperfections in the source and concluded with two theorems from [Koa09]. In Section 5.2.6 it was explained how the theorems relied critically on the assumption of perfect random sampling of the basis states, if a certain attack operation could be constructed. The simplest non-trivial example of such an operation was described in Section 5.2.5, where it was further noted that it was not clear whether it in fact does exist for realistic situations. Due to the various constraints in the model, it also seems this decision problem is difficult to analyze analytically.

The previous section therefore presented a different approach in the form of a numerical investigation. The statement that the two theorems hold even without the assumption of perfect sampling was formulated in Conjecture 5.4 and Conjecture 5.5. The numerical approach was able to provide conclusive evidence against both these conjectures. In addition, the focus was turned towards Conjecture 5.5, which was in fact proven to not hold under a set of additional assumptions of a realistic system.

This chapter discusses the validity and impact of these results. Specifically, we will do this in two parts: First we will assess the *validity of the results*, given the model in Chapter 6. Second, we will look at the *validity of the assumption* in this model. Finally, a few suggestions for further work is provided.

7.1 Validity of results

The main result from Chapter 6 was to provide concrete counterexamples to Conjecture 5.4 and Conjecture 5.5. It is of course important to address the validity of these results. We will first discuss the feasibility of utilizing the results for implementing a concrete attack. Then we will ask whether applying a numerical scheme to address these issues is in fact valid, specifically looking at the impact of numerical errors. Finally, we will consider the legitimacy of the actual physical reality that are described in the results and evaluate how realistic it is.

7.1.1 Feasibility of an explicit attack

First, the counterexamples identified are supposed to represent a situation where the protocol can be attacked in a manner that breaks the security proof in Section 4.2. It is then essential to verify that an actual attack can indeed be performed, based on a single counterexample: Consider a run by the BB84 protocol with an imperfect source as described in Chapter 5 and without perfect random sampling of the basis states. In particular, we consider the situation in Chapter 6, where the source states are *perfectly correlated*. This implies that although Eve does not know the order the states $|\chi_0\rangle$ and $|\chi_1\rangle$ are transmitted, she can always identify a collection L of one particular state $|\chi_a\rangle^{\otimes L}$. L is here a parameter we can vary and that we simply set to the value of the counterexample in question.

Consider specifically a counterexample to Conjecture 5.5 for $L = 2$, describing explicit states $|\chi_0\rangle, |\chi_1\rangle$ and a channel \mathcal{E} . An actual attack of the protocol by Eve is then carried out simply by applying \mathcal{E} on every consecutive two states that Alice transmit. By the above discussion, we assume Alice chooses basis a randomly, but that every two consecutive states are of the same basis. We then take the limit $N \rightarrow \infty$ as declared in Section 5.2.1 so that there are an infinite sequence of random state pairs $|\chi_a\rangle^{\otimes 2}$ transmitted through an infinite number of attack operations \mathcal{E} .

Ignoring imperfections on the channel itself, every state pair $|\chi_a\rangle^{\otimes 2}$ produces a measurable error rate as found in the counterexample calculation. Denote this calculated value by δ_{ph}^* and δ_x^* for the case of $a = 0$ and $a = 1$ respectively. Alice and Bob proceed according to the protocol by measuring the states $|\chi_1\rangle^{\otimes 2}$ in the X basis to get a series of X -basis measurement results. The final, total error rate δ_x is found as the cumulative frequency of mismatched results, which for $N \rightarrow \infty$ will converge to the calculated value $\delta_x = \delta_x^*$.

Using this value, Alice and Bob solve Equation 5.9 to obtain the maximum possible average phase error rate δ_{ph} . The true phase error rate is however given as the cumulative frequency of mismatched outcomes of all the *hypothetical* X -basis measurements of $|\chi_0\rangle^{\otimes 2}$, that Alice and Bob of course cannot measure. These hypothetical measurements would however follow exactly the same argument as the real ones, so that the true phase error rate is convergent to the calculated value δ_{ph}^* . Finally, since the counterexample violates Equation 5.9, this means that $\delta_{\text{ph}} < \delta_{\text{ph}}^*$. Consequently, Alice and Bob will *underestimate* the true phase error rate, which breaks Assumption 2 in the security proof in Section 4.2.

It is important to note that this is not a breakdown of only the proof, i.e. the proof is regarded invalid while the protocol is actually completely secure. On the contrary, such a situation would imply that there is a possibility of Eve having more knowledge about the key than ε from its security definition. Intuitively, the mechanism for this is that Eve frequently makes a measurement that is essentially in the Z -basis, but in such a way that she measures more significantly when the state is $|\chi_0\rangle$. Such a Z -basis measurement by Eve provides information about the key that Alice and Bob establish with their own Z measurement, but at the expense of increasing the phase error rate δ_{ph} . This is however precisely the quantity

that Eve manages to make Alice and Bob underestimate, so that she is able to hide some of her key-revealing measurements.

In summary, we have shown that the existence of the counterexamples to a protocol with no random sampling of basis states can be practically used by Eve. This was done by constructing an explicit attack approach and showing that the security is indeed broken from such an attack. In particular, we showed that it is not possible to avoid this security breach by sending more states, i.e. taking the limit $N \rightarrow \infty$.

7.1.2 Impact of numerical errors

The second consideration to make about the validity of the results is regarding numerical errors. All the counterexamples to Conjecture 5.4 and Conjecture 5.5 are constructed numerically. This means that rather than having symbolic expressions for the various states and operator elements, all these quantities are instead available only as a huge list of real numbers. Consequently, all the constraints in the model, including implicit ones such that state are normalized to 1, are never exactly satisfied; rather all the constraints are valid up to some numerical accuracy. If all assumptions are in fact not exactly true, is it possible to be confident in the final result?

The argument for ruling out numerical errors consists of two parts. First, the final result is clearly robust to small changes in the input parameters. This comes from the fact that the calculation does not involve any chaotic dependencies and no discretization. The final physical results are always in the form of *probabilities* and so infinitesimal perturbations in the final results is insignificant and does not change the physics. In addition, quantum mechanics is convenient in that all these probabilities are always given exactly by an appropriate linear expression in the input parameters. This means that the final result is well-behaved in the input parameters, and specifically have a numerical accuracy that is of comparable order of magnitude as the accuracy of the input.

The second part needed to rule out numerical errors is then to look at the specific accuracy that the input parameters exhibit. The listings in Appendix A provide a breakdown of the accuracy of all the input parameters to the model. This typically includes the normalization of the states $\|\chi_a\|^2 = 1$, sum of the channel operation elements $\sum_k E_k^\dagger E_k = I$ and fidelity requirement $\langle \chi_0 | \chi_1 \rangle \geq F$. As is demonstrated in Appendix A these requirements are always accurate up to less than $\sim 10^{-13}$. The final result is typically the violation of Equation 5.9 or Equation 5.8, which is always at least valid up to an accuracy of $\sim 10^{-4}$. Together with the discussion in the previous paragraph, it is clear that the claimed results are not caused by numerical errors.

Another consideration to make regards the possibility of errors in the implementation. Although bugs in the code are hard to void completely, we have taken several steps to significantly remove their likelihood and severity. First, the algorithm was implemented and run in parallel by multiple languages and programming frameworks, with matching results (see

in particular Section 6.1.4). Second, the final counterexamples produced were exported and then independently verified using a computer algebra system, again giving the same result. Finally, a number of simulations were conducted primarily for the purpose of verifying the model, most notably in Section 6.1. For instance the correspondence between the theory of Chapter 5 and the results from the simulation for $L = 1$ (Figure 6.6) provides strong evidence supporting the correctness of the implementation.

7.1.3 Realism of result properties

The third and last consideration about the validity of the results is about their physical implications. To be clear, the question of whether the assumptions of our model are physically valid, is treated in the next section. Here, we instead deal with the physical interpretation of any *additional properties* that are present as features in the final results.

This topic was already introduced in the analysis in Section 6.2.1, where it was pointed out that it is the properties of the *source* that are crucial. The channel \mathcal{E} on the other hand represents Eve’s action, and to cover all possible attacks it is not interesting to restrict it. The source is modeled as producing a set of arbitrary states ρ_{ab} as long as it satisfies Equation 5.7 for some F that Alice and Bob control. Other than this parameters, we assume that Alice and Bob have no control over, or even knowledge about, the actual state ρ_{ab} .

Of course, in a real, operational system, Alice and Bob would typically have at least some knowledge about the states ρ_{ab} . It is however crucial to be able to allow for *some* degree of uncertainty in the source states, and a very powerful way to do this is through the established constraint in Equation 5.7. We are therefore choosing to model the source in this simple manner: Alice and Bob have no knowledge *at all* about the states ρ_{ab} *other than* that they satisfy Equation 5.7.

This consideration is important, because the counterexamples identified do not apply for any one particular set of source states that were fixed; rather contrary, we have iteratively searched for *any* set of states that satisfy the final result we sought. This is however understood as unproblematic in light of the discussion of the previous paragraph, since Alice and Bob are in fact oblivious to the actual states. One interpretation of this is allowing a two-step attack by Eve: First she prepares a source that produces certain states ρ_{ab} , but has no control over it afterwards. Alice and Bob are then given the value of F for which Equation 5.7 is satisfied. Second, Eve attacks the protocol that Alice and Bob deploy as usual. This matches the “Eve and Fred” model in [Got+04].

Lastly, we recall the discussion in Section 6.2.1 about the possible additional requirement we can place on the source, namely having perfect bit value random number generators and giving a positive key gain G . As can be seen in listing 2 in Appendix A, the final counterexample to Conjecture 5.5 found in Section 6.2 does indeed satisfy all these additional properties. The final counterexample to Conjecture 5.4 (listing 3 in Appendix A) does not however satisfy the two properties, although there does not seem to be any reason preventing

such an example, given more time to find it.

7.1.4 Summary

From all the above discussions, it is clear that given the assumptions of the model, the results are attainable in a implementable, concrete setting. First, Section 7.1.3 asserts that finding a source with the desired characteristics is indeed feasible, simply because we assume we are free to control it. Furthermore, this source is realistic and can produce a positive key gain G . Second, Section 7.1.1 describes how Eve can use the information from the counterexamples to implement an explicit attack scheme. Finally, Section 7.1.2 asserts that this situation would in fact produce the numerical results from the simulations.

7.2 Assumptions and impact

In the previous section we argued why the results from Chapter 6 are valid and implementable, *given* the assumptions in the model. Following this path, investigating the justification for and importance of these assumptions will be the focus of this section. Specifically, the idea behind Conjecture 5.4 and Conjecture 5.5 was to consider a protocol that does not necessarily have perfect random sampling of the basis states. A concrete choice of such a protocol was made by considering a source that is in fact *perfectly correlated*; that is, one particular basis state is always transmitted in a collection with a size Eve can decide. This is of course hardly realistic, but it forms a basis for understanding the effects of other levels of correlation.

The goal of evaluating the validity of the assumptions in the model is to assess the impact of the results. We will first see how the results provide new insight into the existing security proof of imperfect sources. In particular we will argue that the security is critically dependent on perfect, uncorrelated random sampling of the basis states. Second, we will use the results to make predictions about the security of actual, physical devices, which will typically always exhibit small correlations.

7.2.1 Understanding security for imperfect sources

As a start, the numerical results provide a nice verification of the theory developed in Chapter 5. The prediction that a counterexample to Conjecture 5.5 should exist was indeed confirmed by explicitly constructing it. Additionally, we also showed in Chapter 5 that a protocol with perfect sampling was in fact equivalent to our model for $L = 1$. In Section 6.1, a simulation for $L = 1$ was carried out, with results agreeing perfectly with the prediction by Theorem 5.3. Furthermore, the distribution of results as plotted in Figure 6.6 provides strong evidence that the inequality in Equation 5.9 is in fact tight.

We can also get a sense of the importance of the requirement of perfect random sampling in Theorem 5.2 and Theorem 5.3. In Section 5.2.6 we asked whether there really was a need for such a strict assumption, since it seems hard to find concrete counterexamples for any realistic conditions. This is however precisely the result of Section 6.2, where a counterexample of Conjecture 5.5 was constructed in accordance with additional realistic requirements. This supports the need for requiring perfect random sampling of the basis states in the security proof, as counterexamples have been found for correlated states.

7.2.2 Correlation attacks

A natural question to ask now is how realistic the assumption of perfect random sampling of the basis states actually is. On the other hand, the situation of the counterexamples, namely that of a perfectly correlated source, does not look realistic either. As we will see, these situations are in fact two extremes, and most realistic, functioning protocols will fall somewhere in-between.

There are many mechanisms which may cause the random sampling of the basis states to be imperfect. A straight-forward example is if the random subset of states sacrificed for error estimation is not done uniformly randomly, i.e. so that it is not representative of the whole set. This situation, together with many similar ones, however fall in a category of imperfections on the *digital part* of the protocol. Intuitively, selecting a random subset is a purely theoretical process that can be done digitally or even by hand (given a random source). The need for perfect digital systems is however a necessity throughout the proof and is not an unreasonable assumption for real-world systems. This was also precisely the argument for considering sources with $p_0 = p_1 = 0.5$, in accordance with the discussion in Section 6.2.1.

There are however other mechanisms that can cause a failure of the random basis sampling. A notable example is if there are *correlations* between the states that are used for the error estimation. In Chapter 6 we specialized to the case that Alice's source is perfectly correlated, which indeed would satisfy this situation. There are also other possibilities, such as Bob's detector having a correlated device efficiency, possibly due to some influence by Eve.

It is however important to realize how these situations are in fact different from the ones requiring imperfect digital operations. Specifically, what the mechanisms causing correlations have in common is that they are achievable also with systems where the digital processing part is perfect. First, this means that it does not contradict any assumptions in other parts of the security proof, which means we can evaluate this situation accurately using the frameworks developed in this work. Second, these mechanisms are not obviously unrealistic, since it can be caused by imperfection that are purely on the physical apparatus.

To illustrate this, consider a specific example: Alice and Bob deploy the BB84 protocol using devices where the digital processing is always *perfect*. First, Alice's source has basis-dependent imperfections in line with the model in Chapter 5 and satisfies Equation 5.7 for

some parameter F . If this was the only imperfection, Alice and Bob could use Theorem 5.3 to establish an unconditionally secure key. Now assume in addition that Alice's source states are not completely independent, but that there is a small chance of two consecutive states being equal. Formally, for every i th basis and bit choice a_i and b_i Alice makes, the source prepares the state

$$\rho'_{a_i b_i} = p_{\text{corr}} \rho_{a_{i-1} b_{i-1}} + (1 - p_{\text{corr}}) \rho_{a_i b_i}, \quad (7.1)$$

where $\rho_{a_i b_i}$ is the state the source *should* produce and p_{corr} is some probability of correlations occurring. This source model is clearly more general than the framework developed in Chapter 5, which assumed every source state is completely independent.

Assume Alice and Bob are unaware of this correlation effect on the source. Suppose furthermore that the correlation probability is small $p_{\text{corr}} \sim 0.01$. Since the digital choices a_i and b_i are perfect, this source would cause an increase in the observed error rates δ_z and δ_x . Keeping the correlation probability p_{corr} small will however mean that it is still possible that it can be used in a protocol which gives a positive key gain G . Now, since there is a small chance of correlations occurring between the source states, the assumption of perfect random sampling in Theorem 5.2 and Theorem 5.3 does no longer hold. In line with the reasoning in Section 5.2.6, this is because Eve now has an increased probability of finding collections of particular basis states $|\chi_a\rangle$. It is then possible that an attack such as the one described in Section 7.1.1 would be successful, making Alice and Bob underestimate δ_{ph} .

Of course, we have in no way demonstrated any *sufficient* evidence for that an attack on such a system would in fact be successful. We have however showed a *necessary* property, namely that if the correlations between basis-dependent source state become very large, it can indeed be attacked. Further work can then be done on investigating concrete correlated sources and how effective such a correlation attack would be.

Lastly, we note that the assumptions needed to perform this type of attack is not too unrealistic. Unlike the purely theoretic choices for basis and bit values a and b , the states ρ_{ab} are physical. As such there is some mechanical device responsible for producing these states, and its operation will typically never be *perfectly independent*. Furthermore, we have shown implementable attacks for values of L as low as $L = 2$. This is important because the probability of finding L equal states decreases very rapidly for a source with fixed correlation probability. Since the counterexamples from Chapter 6 work for low values of L , this increases the possibility of a correlation attack successfully extracting some non-negligible key material.

7.3 Further work

Given the results from Chapter 6, we propose some possible paths for further work. In line with Section 1.3, the overarching motivation for this work has been to bridge the gap between provable security and real-world devices, focusing on the effects of source imperfections. As

such, the suggestions for further explorations are directed towards this broader goal of understanding the security of quantum key distribution, building off of the results from this work.

Through this work, we have given an in-depth analysis of protocols using sources with individual, basis-dependent imperfections. In Section 7.2.1 we noted how the results from this work further strengthens the understanding of these sources, specifically through what assumptions are critical for their security. The details of this work should therefore provide a strong basis for understanding more complicated protocols that also use imperfect sources. In particular, it is possible to extend the analysis to cover individual imperfections in both the source *and* detector [MLS10b], which must then address the necessary conditions for security indicated in this work.

In addition, it is highly desirable to be able to treat imperfections in the apparatus that is not only individual. Specifically, to fully describe real-world devices, a security proof would need to account for the possibility of small, but finite correlations. We believe this work to be an important step towards understanding the effects of such situations and how they are vulnerable to joint attacks.

As a concrete example, we have investigated the validity of Equation 5.9 in the case of strong correlations on the basis states $|\chi_a\rangle$. Although we were able to find counterexamples even in realistic situations, we noted that it was highly dependent on the choice of states $|\chi_a\rangle$. This seems to suggest that there are certain choices of $|\chi_a\rangle$ for which it is extremely hard to find a concrete attack, at least for realistic conditions. As it stands, the source is only characterized by the general bound in Equation 5.7. It may however be possible to characterize the sources further, and find situations that make the security less critically dependent on the independence of the states. Such sources would evidently be more resistant to attacks, even if the states are in fact slightly correlated.

Chapter 8

Conclusion

We have presented a detailed account of modern security proofs of quantum key distribution based on complementarity. A numerical approach was implemented to investigate sources with correlated, basis-dependent imperfections. This allows us to understand the mechanism for why the security proof requires perfect random sampling of the basis states. In addition, we can make predictions about the effects of small, general correlations in the devices.

In Chapter 1 we gave an overview of cryptography and motivated the importance of unconditional security offered by quantum key distribution. We then developed the mathematical framework necessary, starting from the postulates of quantum mechanics in Chapter 2 and reaching topics from quantum information theory in Chapter 3. Chapter 4 presented the BB84 protocol and a detailed review of its security proof from [Koa09] was given. Chapter 5 then introduced a model for characterizing sources with basis-dependent imperfections and we noted that security is still guaranteed under the assumption of perfect random sampling of the basis states. Finally, we investigated the importance of this assumption in Chapter 6, where concrete examples of security failing were shown in the case of strong correlations in the source.

The modern complementarity-based security proof of [Koa09] forms a powerful basis for analyzing quantum cryptographic systems. Its arguments can however at times appear somewhat convoluted, making the reasoning hard to follow. It has been our goal to address some of these difficulties in our review by focusing on explaining the principles of the idea as well as providing detailed clarifications of some steps. We thereby hope to have constructed a single, coherent document with the full details of the proof and the major topics of necessary background material, in order to make complementarity-based proofs more accessible.

From the numerical results we have gained a solid understanding of the proof in [Koa09]. First, we have validated Theorem 5.3 numerically and found strong evidence that this bound is in fact tight. Second, we have seen how the proof is critically dependent on perfect random sampling of the basis states. This is important for applying the formalism from this proof to more complicated systems.

We also predicted the possibility of performing attacks against sources with imperfections that are slightly correlated. We specifically showed a necessary, although not sufficient, condition that would allow such a style of attack to be carried out. Furthermore, using purely analytic approaches for analyzing protocols and corresponding attacks does not seem productive. Instead, the theory and methods developed in the investigation form effective tools for constructing attack schemes numerically.

Finally, we have developed an arsenal of numerical algorithms for deploying concrete attacks against a system. Specifically, if the states $|\chi_a\rangle$ on a slightly correlated source are known, the genetic algorithm in Section 6.2.4 can be used to successively “breed” efficient attack operations. On the other hand, if we are free to also control the states $|\chi_a\rangle$ of Alice’s source, the search algorithms from Section 6.2 can look for suitable states that are prone to correlation attacks. The hybrid search and genetic algorithm can then be deployed to refine this choice and find optimal attack operations.

The numerical methods are also believed to be highly useful for investigating the behavior of general quantum systems. The exceptional speed of the Fortran routines allowed us to perform a perfectly uniform search in the space of quantum states and operations, as detailed in Section 6.1.2 and Section 6.1.3. The results from this scheme proved to map out a surprisingly uniform distribution also in the final output parameters. This method can be highly useful for evaluating, verifying or disproving claims from analytic approaches.

Bibliography

- [All+14] R. Alléaume et al. “Using quantum key distribution for cryptographic purposes: A survey”. In: *Theoretical Computer Science* 560.Part 1 (2014), pp. 62–81. arXiv: [quant-ph/0701168v3](https://arxiv.org/abs/quant-ph/0701168v3).
- [And+99] E. Anderson et al. *LAPACK Users’ Guide*. Third. Philadelphia, PA, USA: Society for Industrial and Applied Mathematics, 1999.
- [BB84] C. H. Bennett and G. Brassard. “Quantum cryptography: public key distribution and coin tossing”. In: *International Conference on Computers, Systems, and Signal Processing*. (Bangalore, India). New York, NY, USA: IEEE, 1984, pp. 175–179.
- [Deu85] D. Deutsch. “Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer”. In: *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences* 400.1818 (1985), pp. 97–117.
- [DJ92] D. Deutsch and R. Jozsa. “Rapid Solution of Problems by Quantum Computation”. In: *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences* 439.1907 (1992), pp. 553–558.
- [DK07] H. Delfs and H. Knebl. *Introduction to cryptography. Principles and applications*. Second Edition. Information Security and Cryptography. Berlin / Heidelberg, Germany: Springer, 2007.
- [Fey82] R. P. Feynman. “Simulating physics with computers”. In: *International journal of theoretical physics* 21.6 (1982), pp. 467–488.
- [Ghe14] V. Gheorghiu. “Quantum++: A C++ 11 quantum computing library”. In: *arXiv preprint* (2014). arXiv: [1412.4704](https://arxiv.org/abs/1412.4704).
- [Gol01] S. W. Golomb. “Retrospective: Claude E. Shannon (1916-2001)”. In: *Science* 292.5516 (2001), pp. 455–455.
- [Got+04] D. Gottesman et al. “Security of quantum key distribution with imperfect devices”. In: *International Symposium on Information Theory*. (Chicago, IL, USA). New York, NY, USA: IEEE, 2004, pp. 136–. arXiv: [quant-ph/0212066](https://arxiv.org/abs/quant-ph/0212066).
- [Hay06] M. Hayashi. *Quantum Information. An Introduction*. Berlin / Heidelberg, Germany: Springer, 2006.

- [Hol73] A. S. Holevo. “Bounds for the quantity of information transmitted by a quantum communication channel”. In: *Problemy Peredachi Informatsii* 9.3 (1973), pp. 3–11.
- [Ing76] R. S. Ingarden. “Quantum information theory”. In: *Reports on Mathematical Physics* 10.1 (1976), pp. 43–72.
- [Kah96] D. Kahn. *The Codebreakers. The Comprehensive History of Secret Communication from Ancient Times to the Internet*. New York, NY, USA: Scribner, 1996.
- [KL08] J. Katz and Y. Lindell. *Introduction to Modern Cryptography. Principles and Protocols*. Cryptography and network security. Boca Raton, FL, USA: Chapman & Hall/CRC, 2008.
- [Koa06] M. Koashi. “Unconditional security of quantum key distribution and the uncertainty principle”. In: *Journal of Physics: Conference Series* 36.1 (2006), p. 98.
- [Koa09] M. Koashi. “Simple security proof of quantum key distribution based on complementarity”. In: *New Journal of Physics* 11.4 (2009), p. 045018.
- [KP03] M. Koashi and J. Preskill. “Secure Quantum Key Distribution with an Uncharacterized Source”. In: *Physical Review Letters* 90 (5 2003), p. 057902.
- [LC99] H.-K. Lo and H. F. Chau. “Unconditional security of quantum key distribution over arbitrarily long distances”. In: *Science* 283.5410 (1999), pp. 2050–2056. arXiv: [quant-ph/9803006](https://arxiv.org/abs/quant-ph/9803006).
- [Lo03] H.-K. Lo. “Method for decoupling error correction from privacy amplification”. In: *New Journal of Physics* 5.1 (2003), p. 36.
- [May96] D. Mayers. “Quantum Key Distribution and String Oblivious Transfer in Noisy Channels. 16th Annual International Cryptology Conference Santa Barbara, California, USA August 18–22, 1996 Proceedings”. In: *Advances in Cryptology — CRYPTO ’96*. Berlin / Heidelberg, Germany: Springer, 1996, pp. 343–357.
- [MLS10a] V. Makarov, L. Lydersen, and J. Skaar. *Cracking commercial quantum cryptography: how we did it, in pictures*. Quantum Hacking group, NTNU. 2010. URL: <http://www.iet.ntnu.no/groups/optics/qcr/hacking-commercial-quantum-cryptography-2010/> (visited on 2017-01-03).
- [MLS10b] Ø. Marøy, L. Lydersen, and J. Skaar. “Security of quantum key distribution with arbitrary individual imperfections”. In: *Physical Review A* 82 (3 2010), p. 032337.
- [MU88] H. Maassen and J. B. M. Uffink. “Generalized entropic uncertainty relations”. In: *Physical Review Letters* 60 (12 1988), pp. 1103–1106.
- [NC10] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge, UK: Cambridge university press, 2010.

- [RK05] R. Renner and R. König. “Universally composable privacy amplification against quantum adversaries”. In: *Second Theory of Cryptography Conference*. (Cambridge, MA, USA). Lecture Notes in Computer Science. Berlin / Heidelberg, Germany: Springer, 2005, pp. 407–425. arXiv: [quant-ph/0403133](https://arxiv.org/abs/quant-ph/0403133).
- [Sha48] C. E. Shannon. “A mathematical theory of communication”. In: *Bell System Technical Journal* 27.3 (1948), pp. 379–423.
- [Sha49] C. E. Shannon. “Communication theory of secrecy systems”. In: *Bell System Technical Journal* 28.4 (1949), pp. 656–715.
- [Sho94] P. W. Shor. “Algorithms for quantum computation: discrete logarithms and factoring”. In: *35th Annual Symposium on Foundations of Computer Science*. (Santa Fe, NM, USA). Washington, DC, USA: IEEE Computer Society Press, 1994, pp. 124–134.
- [Ska08] J. Skaar. “Understanding Koashi’s BB84 security proof”. unpublished. 2008.
- [SP00] P. W. Shor and J. Preskill. “Simple proof of security of the BB84 quantum key distribution protocol”. In: *Physical Review Letters* 85.2 (2000), pp. 441–444. arXiv: [quant-ph/0003004](https://arxiv.org/abs/quant-ph/0003004).
- [TKI03] K. Tamaki, M. Koashi, and N. Imoto. “Unconditionally Secure Key Distribution Based on Two Nonorthogonal States”. In: *Physical Review Letters* 90 (16 2003), p. 167904.

Appendix A

Numerical values of counterexamples

The following pages list exported pages from Wolfram Mathematica notebooks, containing numerical values for the main counterexamples found during this work. Step-by-step calculation from the initial set of states $|\beta_{ab}\rangle$, probabilities p_a and a channel \mathcal{E} to the final error rates is also provided.

This listing contains 3 documents titled:

1. “Counterexample to $F \leq \sqrt{(1 - \delta_{\text{ph}})(1 - \delta_x)} + \sqrt{\delta_{\text{ph}}\delta_x}$ for $L = 2$, $F = 0.99$ ”
2. “Counterexample to $F \leq \sqrt{(1 - \delta_{\text{ph}})(1 - \delta_x)} + \sqrt{\delta_{\text{ph}}\delta_x}$ for $L = 2$, $F = 0.99$, $p_0 = p_1 = 0.5$ and positive true key gain G ”
3. “Counterexample to $1 - h\left(\frac{1-F}{2}\right) \leq \frac{\delta_x + \delta_{\text{ph}}}{2} h\left(\frac{\delta_x}{\delta_x + \delta_{\text{ph}}}\right) + \frac{2 - \delta_x - \delta_{\text{ph}}}{2} h\left(\frac{1 - \delta_{\text{ph}}}{2 - \delta_x - \delta_{\text{ph}}}\right)$ for $L = 4$, $F = 0.99$ ”

Counterexample to $F \leq \sqrt{(1 - \delta_{ph})(1 - \delta_x)} + \sqrt{\delta_{ph} \delta_x}$ for $L = 2, F = 0.99$

```
In[1]:= L = 2;
        F = 0.99;
```

Definitions

```
In[3]:= Kr = KroneckerProduct;
        Ct = ConjugateTranspose;
        z0 = {{1}, {0}};
        z1 = {{0}, {1}};
        x0 = 1/Sqrt[2] (z0 + z1);
        x1 = 1/Sqrt[2] (z0 - z1);
        Id[n_] = IdentityMatrix[n];
        Id2 = Id[2];
        H = 1/Sqrt[2] {{1, 1}, {1, -1}};
        X = {{0, 1}, {1, 0}};
        Y = {{0, -I}, {I, 0}};
        Z = {{1, 0}, {0, -1}};
        Swap = {{1, 0, 0, 0}, {0, 0, 1, 0}, {0, 1, 0, 0}, {0, 0, 0, 1}};
        PX0 = x0.Ct[x0];
        PX1 = x1.Ct[x1];
        PZ0 = z0.Ct[z0];
        PZ1 = z1.Ct[z1];
```

Measurement operators in Z and X-basis

```
In[20]:= mx1 = Kr[Kr[Kr[PX0, Id2], PX1], Id2] + Kr[Kr[Kr[PX1, Id2], PX0], Id2];
        mx2 = Kr[Kr[Kr[Id2, PX0], Id2], PX1] + Kr[Kr[Kr[Id2, PX1], Id2], PX0];
        mz1 = Kr[Kr[Kr[PZ0, Id2], PZ1], Id2] + Kr[Kr[Kr[PZ1, Id2], PZ0], Id2];
        mz2 = Kr[Kr[Kr[Id2, PZ0], Id2], PZ1] + Kr[Kr[Kr[Id2, PZ1], Id2], PZ0];
```

Input parameters: states $|\beta_{ab}\rangle$, probabilities p_a and channel U

```
In[24]:= beta1 = {{0.8618356164550959 - 0.483762580928078 I}, {-0.09880039297707263 - 0.11598110988797108 I}};
        beta2 = {{-0.6665350096819082 + 0.7291992606988255 I}, {0.10256568096383674 + 0.1161025415443161 I}};
        beta3 = {{0.5164651076645687 + 0.8475134050541189 I}, {0.029064465339296124 - 0.11891205856909239 I}};
        beta4 = {{0.7734313845423763 - 0.5910715952440599 I}, {-0.2211185889650996 - 0.05953849439302495 I}};
        p1 = 0.5191264537224269;
        p2 = 0.018566314843056483;
        U = {{0.21983772460001566 - 9.0854226683340200 * 10^-2 I,
              -0.43543986468904161 - 5.0518039104228987 * 10^-2 I,
              -0.26808686277683269 + 0.50278263009215185 I, -0.60517535335788764 + 0.24568025739436672 I},
            {-0.42937143562478330 + 0.38521993832169049 I, 0.58384776801563232 - 0.18016195889907693 I,
              -0.23414828312528019 + 0.26423079584145270 I, -0.13831149331924153 + 0.38747363857691564 I},
            {-0.51980033088750011 + 0.24302284988172962 I, -0.26173223727921840 - 0.12760343761743692 I,
              0.60175136339598012 + 1.4161200268333174 * 10^-2 I, -0.38983281924392071 - 0.26774286025963556 I},
            {-0.18479908247584215 + 0.49725191129456692 I, -0.32173088643741032 + 0.49619183760183927 I,
              -0.29921604469083324 + 0.31442049007687434 I, 0.33710510203418487 - 0.25853896619544364 I}};
```

Check numerical accuracy of input:

- states should be normalized $\| |\beta_{ab}\rangle \|^2 = 1$
- channel matrix should be unitary $U U^\dagger = I$

```
In[31]:= Norm[beta1] - 1
        Norm[beta2] - 1
```

```

Norm[beta3] - 1
Norm[beta4] - 1
Total[Abs[Flatten[U.Ct[U] - Id[4]]]]

```

Out[31]= 0.

Out[32]= 2.22045×10^{-16}

Out[33]= -1.11022×10^{-16}

Out[34]= 0.

Out[35]= 7.26192×10^{-15}

Construct states $|\chi_a\rangle$

```

In[36]:= chi1 = Sqrt[p1] Kr[z0, beta1] + Sqrt[1 - p1] Kr[z1, beta2];
chi2 = Sqrt[p2] Kr[x0, beta3] + Sqrt[1 - p2] Kr[x1, beta4];

```

Check accuracy of the fidelity requirement:

$$\square \langle \chi_0 | \chi_1 \rangle \geq F$$

```

In[38]:= inner = Ct[chi1].chi2
AbsArg[inner]
fid = Abs[inner[[1, 1]]]
fid - F

```

Out[38]= $\{\{0.990197 - 1.12757 \times 10^{-16} i\}\}$

Out[39]= $\{\{\{0.990197, -1.13873 \times 10^{-16}\}\}\}$

Out[40]= 0.990197

Out[41]= 0.00019722

Apply the circuit and find the final states

```

In[42]:= chit1 = Kr[Kr[Id2, Swap], Id2].Kr[chi1, chi1];
chit2 = Kr[Kr[Id2, Swap], Id2].Kr[chi2, chi2];
chif1 = Kr[Kr[Id2, Id2], U].chit1
chif2 = Kr[Kr[Id2, Id2], U].chit2

```

Out[44]= $\{\{0.0808029 - 0.140941 i\}, \{0.0256431 + 0.269577 i\}, \{-0.0561534 + 0.284176 i\}, \{0.236356 + 0.173195 i\},$
 $\{-0.0309719 + 0.144443 i\}, \{-0.102749 - 0.223455 i\}, \{-0.0321599 - 0.282936 i\}, \{-0.277291 - 0.0966652 i\},$
 $\{-0.0439533 + 0.146599 i\}, \{-0.110384 - 0.243224 i\}, \{-0.0378912 - 0.263858 i\}, \{-0.273254 - 0.0956241 i\},$
 $\{-0.00133345 - 0.138623 i\}, \{0.168259 + 0.175747 i\}, \{0.113921 + 0.236597 i\}, \{0.289396 + 0.0108238 i\}\}$

Out[45]= $\{\{0.0677397 - 0.175133 i\}, \{0.000352876 + 0.264362 i\}, \{-0.0669172 + 0.269578 i\},$
 $\{0.213681 + 0.0928234 i\}, \{-0.0186472 + 0.188144 i\}, \{-0.0701786 - 0.252168 i\},$
 $\{-0.00997922 - 0.289427 i\}, \{-0.245617 - 0.036875 i\}, \{-0.0264284 + 0.191797 i\},$
 $\{-0.0784767 - 0.263248 i\}, \{-0.0102078 - 0.276417 i\}, \{-0.242894 - 0.0369347 i\},$
 $\{-0.025442 - 0.193198 i\}, \{0.144766 + 0.230366 i\}, \{0.0893506 + 0.274574 i\}, \{0.259969 - 0.0289838 i\}\}$

Double-check the normalization of the final states

```
In[46]:= Norm[chif1] - 1  
Norm[chif2] - 1
```

```
Out[46]= -1.11022 × 10-16
```

```
Out[47]= -4.44089 × 10-16
```

Calculate the error rate for each basis a for each measurement pair

```
In[48]:= p11 = Norm[Ct[chif1].mx1.chif1];  
p12 = Norm[Ct[chif1].mx2.chif1];  
p21 = Norm[Ct[chif2].mx1.chif2];  
p22 = Norm[Ct[chif2].mx2.chif2];  
p31 = Norm[Ct[chif1].mz1.chif1];  
p32 = Norm[Ct[chif1].mz2.chif1];
```

Calculate the total error rates δ_{ph} , δ_x and δ_z

```
In[54]:= dp = 1/2 (p11 + p12)  
dx = 1/2 (p21 + p22)  
dz = 1/2 (p31 + p32)
```

```
Out[54]= 0.535572
```

```
Out[55]= 0.382661
```

```
Out[56]= 0.507851
```

Check whether the claim $F \leq \sqrt{(1 - \delta_{ph})(1 - \delta_x)} + \sqrt{\delta_{ph} \delta_x}$ in fact holds?

```
In[57]:= F  
F^L  
cfid = Sqrt[(1 - dp)(1 - dx)] + Sqrt[dp dx]  
cfid - F
```

```
Out[57]= 0.99
```

```
Out[58]= 0.9801
```

```
Out[59]= 0.988158
```

```
Out[60]= -0.00184162
```

Counterexample to $F \leq \sqrt{(1 - \delta_{ph})(1 - \delta_x)} + \sqrt{\delta_{ph} \delta_x}$ for $L = 2$, $F = 0.99$, $p_0 = p_1 = 0.5$ and positive true key gain G

```
In[1]:= L = 2;
        F = 0.99;
```

Definitions

```
In[3]:= Kr = KroneckerProduct;
        Ct = ConjugateTranspose;
        z0 = {{1}, {0}};
        z1 = {{0}, {1}};
        x0 = 1/Sqrt[2] (z0 + z1);
        x1 = 1/Sqrt[2] (z0 - z1);
        Id[n_] = IdentityMatrix[n];
        Id2 = Id[2];
        H = 1/Sqrt[2] {{1, 1}, {1, -1}};
        X = {{0, 1}, {1, 0}};
        Y = {{0, -I}, {I, 0}};
        Z = {{1, 0}, {0, -1}};
        Swap = {{1, 0, 0, 0}, {0, 0, 1, 0}, {0, 1, 0, 0}, {0, 0, 0, 1}};
        PX0 = x0.Ct[x0];
        PX1 = x1.Ct[x1];
        PZ0 = z0.Ct[z0];
        PZ1 = z1.Ct[z1];
```

Measurement operators in Z and X-basis

```
In[20]:= mx1 = Kr[Kr[Kr[PX0, Id2], PX1], Id2] + Kr[Kr[Kr[PX1, Id2], PX0], Id2];
        mx2 = Kr[Kr[Kr[Id2, PX0], Id2], PX1] + Kr[Kr[Kr[Id2, PX1], Id2], PX0];
        mz1 = Kr[Kr[Kr[PZ0, Id2], PZ1], Id2] + Kr[Kr[Kr[PZ1, Id2], PZ0], Id2];
        mz2 = Kr[Kr[Kr[Id2, PZ0], Id2], PZ1] + Kr[Kr[Kr[Id2, PZ1], Id2], PZ0];
```

Input parameters: states $|\beta_{ab}\rangle$, probabilities p_a and channel $\mathcal{E}: \{E_k\}$

```
In[24]:= beta1 = Exp[0.30673531340579263` I]
        {{-0.0241612508205372 + 0.0133612168155024 I}, {0.710348714644220 + 0.703308193786551 I}};
        beta2 = Exp[0.30673531340579263` I] {{-0.806304859246544 - 0.441572041715479 I},
        {0.221103936814983 - 0.325575882177335 I}};
        beta3 = {{-0.462870297764371 - 0.486778414449058 I}, {0.583289643889546 + 0.456695800292920 I}};
        beta4 = {{0.341029326470811 + 0.584906188898497 I}, {0.207408593957079 + 0.706091653985407 I}};
        p1 = 0.5;
        p2 = 0.5;
        E1 = {{0.00811932038439783 - 0.0151921392659071 I, 0.0842786089530878 + 0.0414746581607201 I,
        0.0739348004099622 + 0.0447387156933429 I, -0.278534286507675 + 0.395238339340388 I},
        {-0.0746073997796507 - 0.0374315044241198 I, -0.00799127660788268 + 0.00946414631517856 I,
        0.176069547170176 - 0.450842476205211 I, -0.0898810776290537 - 0.0287858574735873 I},
        {-0.0645323389821607 - 0.0421980808932271 I, 0.181407211742590 - 0.442172964852311 I,
        -0.0142584183641981 + 0.00597041682494305 I, -0.0940696074221421 - 0.0300515562643858 I},
        {-0.0911413282551480 + 0.471684544570432 I, 0.0789761733193762 - 0.00759544883522111 I,
        0.0833963135389054 - 0.0146476261083193 I, -0.0126384796020175 - 0.00750905498462820 I}};
        E2 = {{0.00905095469045945 + 0.00151630320370057 I, -0.0483670095968135 + 0.0480395720399541 I,
        -0.0435714637474110 + 0.0484255678570627 I, -0.322305764226428 - 0.288821421276326 I},
        {0.0390962036952514 - 0.0378803607930427 I, -0.0116735589815758 - 0.00851637045460712 I,
        0.375880045399247 + 0.204706535296235 I, 0.0208923521374876 - 0.0649279745746424 I},
        {0.0414291156532660 - 0.0417224038150195 I, 0.379950793413494 + 0.203250375073269 I,
        -0.00656923304239875 - 0.0111904475289894 I, 0.0288533820444241 - 0.0673739470780729 I},
```

```

{-0.411417232353784 - 0.134202489008279 I, 0.00711306628296094 + 0.0560639264673237 I,
 0.00160938309872234 + 0.0578773784251183 I, 0.0114807319664248 - 0.0115612756925726 I} };
E3 = { {-0.0123477659400021 - 0.0153427634686885 I, 0.0836828844500001 - 0.0691954494635905 I,
 0.0831232035786679 - 0.0680612611744219 I, 0.349455491105575 + 0.426353453732412 I},
{-0.0803405566524457 + 0.0543826625200902 I, 0.0105364558149468 + 0.0195792480256657 I,
-0.443005229167043 - 0.346431144131854 I, -0.0708721029008873 + 0.0781139113448472 I},
{-0.0792250228186423 + 0.0570062779412960 I, -0.445783689698328 - 0.339972408711247 I,
0.00885356310087114 + 0.0137933837517638 I, -0.0678296330095582 + 0.0847009179986621 I},
{0.500679806976024 + 0.254446632426640 I, 0.0210703263821668 - 0.0960604704959166 I,
0.0243712431410546 - 0.0927573268988079 I, -0.0173231353826995 - 0.00580217520873882 I} };
E4 = { {-0.0193954111385712 + 0.0115538108723434 I, -0.0311920207895825 - 0.0829100508398706 I,
-0.0327975455313441 - 0.0807642199470851 I, 0.395356033384337 - 0.231872709386858 I},
{0.0202970745676468 + 0.0676971109867272 I, 0.0160342046586544 - 0.00766158120635709 I,
-0.338196767161162 + 0.309442312011943 I, 0.0511229269339178 + 0.0588239413287494 I},
{0.0246342190649380 + 0.0635917252987215 I, -0.342016446138799 + 0.310737282337100 I,
0.00887258920919010 - 0.0104024047377134 I, 0.0471840398851952 + 0.0638362156144589 I},
{0.281217086716562 - 0.371793680602653 I, -0.0608762803218771 - 0.0302870131185094 I,
-0.0625046743815065 - 0.0284425715420375 I, 0.00170957016824478 + 0.0127357304426778 I} };

```

Check numerical accuracy of input:

- states should be normalized $\| |\beta_{ab}\rangle \|^2 = 1$
- channel should sum to the identity matrix $\sum_k E_k^\dagger E_k = I$

```

In[34]:= Norm[beta1] - 1
Norm[beta2] - 1
Norm[beta3] - 1
Norm[beta4] - 1
Total[Abs[Flatten[Ct[E1].E1 + Ct[E2].E2 + Ct[E3].E3 + Ct[E4].E4 - Id[4]]]]

```

Out[34]= 0.

Out[35]= -1.11022×10^{-16}

Out[36]= 2.22045×10^{-16}

Out[37]= -3.33067×10^{-16}

Out[38]= 5.41666×10^{-15}

Construct states $|\chi_a\rangle$

```

In[39]:= chi1 = Sqrt[p1] Kr[z0, beta1] + Sqrt[1 - p1] Kr[z1, beta2];
chi2 = Sqrt[p2] Kr[x0, beta3] + Sqrt[1 - p2] Kr[x1, beta4];

```

Check accuracy of the fidelity requirement:

- $\langle \chi_0 | \chi_1 \rangle \geq F$


```

In[41]:= inner = Ct[chi1].chi2
AbsArg[inner]
fid = Abs[inner[[1, 1]]]
fid - F
Out[41]= {{0.99 + 1.14492 × 10-16 i}}
Out[42]= {{{0.99, 1.15648 × 10-16}}}
Out[43]= 0.99
Out[44]= -4.44089 × 10-16

```

Apply the circuit and find the final states

```

In[45]:= chit1 = Kr[Kr[Id2, Swap], Id2].Kr[chi1, chi1];
chit2 = Kr[Kr[Id2, Swap], Id2].Kr[chi2, chi2];
rhot1 = chit1.Ct[chit1];
rhot2 = chit2.Ct[chit2];
rhof1 = Kr[Kr[Id2, Id2], E1].rhot1.Ct[Kr[Kr[Id2, Id2], E1]] +
Kr[Kr[Id2, Id2], E2].rhot1.Ct[Kr[Kr[Id2, Id2], E2]] + Kr[Kr[Id2, Id2], E3].rhot1.
Ct[Kr[Kr[Id2, Id2], E3]] + Kr[Kr[Id2, Id2], E4].rhot1.Ct[Kr[Kr[Id2, Id2], E4]];
rhof2 = Kr[Kr[Id2, Id2], E1].rhot2.Ct[Kr[Kr[Id2, Id2], E1]] +
Kr[Kr[Id2, Id2], E2].rhot2.Ct[Kr[Kr[Id2, Id2], E2]] + Kr[Kr[Id2, Id2], E3].rhot2.
Ct[Kr[Kr[Id2, Id2], E3]] + Kr[Kr[Id2, Id2], E4].rhot2.Ct[Kr[Kr[Id2, Id2], E4]];

```

Double-check the normalization of the final states

```

In[51]:= Tr[rhof1] - 1
Tr[rhof2] - 1
Out[51]= -4.44089 × 10-16 - 2.78759 × 10-18 i
Out[52]= -6.66134 × 10-16 - 2.13473 × 10-18 i

```

Calculate the error rate for each basis a for each measurement pair

```

In[53]:= p11 = Abs[Tr[mx1.rhof1]];
p12 = Abs[Tr[mx2.rhof1]];
p21 = Abs[Tr[mx1.rhof2]];
p22 = Abs[Tr[mx2.rhof2]];
p31 = Abs[Tr[mz1.rhof1]];
p32 = Abs[Tr[mz2.rhof1]];

```

Calculate the total error rates δ_{ph} , δ_x and δ_z

```

In[59]:= dp = 1/2 (p11 + p12)
dx = 1/2 (p21 + p22)
dz = 1/2 (p31 + p32)
Out[59]= 0.0967867
Out[60]= 0.0298381
Out[61]= 0.0388362

```

Check whether the claim $F \leq \sqrt{(1 - \delta_{ph})(1 - \delta_x)} + \sqrt{\delta_{ph} \delta_x}$ in fact holds

```

In[62]:= F

```

```
F ^ L
cfid = Sqrt [ (1 - dp) (1 - dx) ] + Sqrt [ dp dx]
cfid - F
```

Out[62]= 0.99

Out[63]= 0.9801

Out[64]= 0.989829

Out[65]= -0.00017123

Show that the true key gain G is positive

```
In[66]:= h[x_] = -x Log2[x] - (1 - x) Log2[1 - x];
1 - h[dz] - h[dp]
```

Out[67]= 0.304343

Counterexample to $1 - h\left(\frac{1-F}{2}\right) \leq \frac{\delta_x + \delta_{ph}}{2} h\left(\frac{\delta_x}{\delta_x + \delta_{ph}}\right) + \frac{2 - \delta_x - \delta_{ph}}{2} h\left(\frac{1 - \delta_{ph}}{2 - \delta_x - \delta_{ph}}\right)$ for $L = 4$, $F = 0.99$

```
In[1]:= L = 4;
        F = 0.99;
```

Definitions

```
In[3]:= Kr = KroneckerProduct;
        Ct = ConjugateTranspose;
        z0 = {{1}, {0}};
        z1 = {{0}, {1}};
        x0 = 1/Sqrt[2] (z0 + z1);
        x1 = 1/Sqrt[2] (z0 - z1);
        Id[n_] = IdentityMatrix[n];
        Id2 = Id[2];
        H = 1/Sqrt[2] {{1, 1}, {1, -1}};
        X = {{0, 1}, {1, 0}};
        Y = {{0, -I}, {I, 0}};
        Z = {{1, 0}, {0, -1}};
        Swap = {{1, 0, 0, 0}, {0, 0, 1, 0}, {0, 1, 0, 0}, {0, 0, 0, 1}};
        PX0 = x0.Ct[x0];
        PX1 = x1.Ct[x1];
        PZ0 = z0.Ct[z0];
        PZ1 = z1.Ct[z1];
```

Measurement operators in Z and X-basis

```
In[20]:= mx1 = Kr[Kr[Kr[Kr[Kr[Kr[Kr[PX0, Id2], Id2], Id2], PX1], Id2], Id2], Id2] +
        Kr[Kr[Kr[Kr[Kr[Kr[Kr[PX1, Id2], Id2], Id2], PX0], Id2], Id2], Id2];
        mx2 = Kr[Kr[Kr[Kr[Kr[Kr[Kr[Id2, PX0], Id2], Id2], Id2], PX1], Id2], Id2] +
        Kr[Kr[Kr[Kr[Kr[Kr[Kr[Id2, PX1], Id2], Id2], Id2], PX0], Id2], Id2];
        mx3 = Kr[Kr[Kr[Kr[Kr[Kr[Kr[Id2, Id2], PX0], Id2], Id2], Id2], PX1], Id2] +
        Kr[Kr[Kr[Kr[Kr[Kr[Kr[Id2, Id2], PX1], Id2], Id2], Id2], PX0], Id2];
        mx4 = Kr[Kr[Kr[Kr[Kr[Kr[Kr[Id2, Id2], Id2], PX0], Id2], Id2], Id2], PX1] +
        Kr[Kr[Kr[Kr[Kr[Kr[Kr[Id2, Id2], Id2], PX1], Id2], Id2], Id2], PX0];
        mz1 = Kr[Kr[Kr[Kr[Kr[Kr[Kr[PZ0, Id2], Id2], Id2], PZ1], Id2], Id2], Id2] +
        Kr[Kr[Kr[Kr[Kr[Kr[Kr[PZ1, Id2], Id2], Id2], PZ0], Id2], Id2], Id2];
        mz2 = Kr[Kr[Kr[Kr[Kr[Kr[Kr[Id2, PZ0], Id2], Id2], Id2], PZ1], Id2], Id2] +
        Kr[Kr[Kr[Kr[Kr[Kr[Kr[Id2, PZ1], Id2], Id2], Id2], PZ0], Id2], Id2];
        mz3 = Kr[Kr[Kr[Kr[Kr[Kr[Kr[Id2, Id2], PZ0], Id2], Id2], Id2], PZ1], Id2] +
        Kr[Kr[Kr[Kr[Kr[Kr[Kr[Id2, Id2], PZ1], Id2], Id2], Id2], PZ0], Id2];
        mz4 = Kr[Kr[Kr[Kr[Kr[Kr[Kr[Id2, Id2], Id2], PZ0], Id2], Id2], Id2], PZ1] +
        Kr[Kr[Kr[Kr[Kr[Kr[Kr[Id2, Id2], Id2], PZ1], Id2], Id2], Id2], PZ0];
```

Input parameters: states $|\beta_{ab}\rangle$, probabilities p_a and channel $\mathcal{E}: \{E_k\}$

```
In[28]:= beta1 = Exp[0 I] {{-0.713743960743703 + 0.229164822801698 I}, {0.410741274930708 + 0.518984245965574 I}};
        beta2 = Exp[0 I] {{-0.648898851416328 + 0.388641342980431 I}, {0.430113569420790 + 0.492839227899976 I}};
        beta3 = {{-0.624131126328058 + 0.549623846555202 I}, {0.493671347539571 + 0.254288350234134 I}};
        beta4 = {{-0.542990813613280 - 0.817756120409776 I}, {-0.135167191779458 + 0.134780318037893 I}};
        p1 = 0.485041682782097;
        p2 = 0.992239876137303;
        E1 = {{-0.0356022997661755 - 0.0481605814161666 I, -0.134924633863143 + 0.0858230860132571 I,
        0.104395296289273 + 0.126440952810266 I, -0.00525765288938560 - 0.0869306224895398 I,
        -0.0378834012501664 + 0.125694105382689 I, -0.00985715843415386 - 0.0413635089085552 I,
        0.117756939136923 - 0.171577184123959 I, -0.0126089441970748 + 0.122350890863886 I,
        0.189230411833114 - 0.103905466165478 I, 0.00580626714058966 - 0.0700401523412931 I,
```

$0.00144591029566180 + 0.0295816442460953 I, 0.141384925954945 + 0.107041481491727 I,$
 $0.0336662200372885 - 0.0315755889639548 I, 0.0563103195348770 + 0.0572010298470908 I,$
 $0.0762577889077209 - 0.199784359172350 I, -0.0131410221835931 - 0.0173563688029599 I \},$
 $\{0.0422349053948077 - 0.100989572990767 I, -0.0822669225972996 - 0.0459657610378551 I,$
 $-0.0399777121838828 + 0.0309552251088860 I, -0.0547175930718370 + 0.143501448296577 I,$
 $0.0418806229519992 + 0.0342613447177754 I, -0.00710228339049925 + 0.00440480472023064 I,$
 $0.0415737063650895 - 0.0642440266192675 I, -0.0233743984880721 - 0.0843400678382183 I,$
 $0.000730614186792031 + 0.108925965026000 I, -0.0477825107432922 - 0.0932931679509728 I,$
 $-0.0620532615676592 + 0.103083676429391 I, 0.0261546459468523 + 0.0293770674683722 I,$
 $-0.0708102395101081 + 0.0740086549427447 I, 0.0584619127508201 + 0.00861571832326477 I,$
 $-0.189278346613680 - 0.0280872920943520 I, 0.0453419640339046 - 0.0666805040060135 I \},$
 $\{0.133432793566794 - 0.0465971472071595 I, 0.106671730670846 - 0.0879247156662050 I,$
 $0.0770038437390069 + 0.0551487288680862 I, -0.00917107975319439 - 0.105841266543374 I,$
 $-0.0554914996869581 + 0.0280255817348976 I, -0.127223622706072 + 0.0986019828223026 I,$
 $-0.0897490894403357 - 0.0124909592934167 I, -0.111552908284731 + 0.100015723023371 I,$
 $-0.0268592612861987 - 0.0829298110249709 I, -0.000819365977251851 + 0.0395230025533959 I,$
 $-0.180708194266785 + 0.123850893474990 I, -0.0224086117669768 + 0.0702966965803151 I,$
 $-0.0643230582499883 - 0.166056824336622 I, -0.133055367170015 - 0.0701709152758717 I,$
 $-0.0583124982841232 - 0.0500719309021837 I, 0.106855256726398 - 0.0838532099918339 I \},$
 $\{-0.0524407655461734 - 0.0479928399596027 I, 0.0142617777585576 - 0.00556784087703798 I,$
 $-0.0336225970791011 + 0.139589261541199 I, -0.0664960403931574 - 0.0290425507611319 I,$
 $-0.0781800830932150 + 0.147311537325748 I, 0.0826708400828151 - 0.0594939144176092 I,$
 $0.0492589865522599 - 0.00259017031557809 I, 0.0402128101055225 - 0.0571481491518549 I,$
 $0.0766529541533149 + 0.0835795524068445 I, 0.198509516610352 - 0.0237992426235623 I,$
 $0.135855602559550 + 0.0731627904872573 I, -0.0302157428424118 - 0.0884710257151234 I,$
 $-0.105165755285078 + 0.0429237391667936 I, 0.0508285386604596 - 0.0634055954213215 I,$
 $0.112885282729283 + 0.0748543910981132 I, -0.189781429496724 + 0.0624884734578997 I \},$
 $\{0.162375227005844 - 0.0877197767931987 I, 0.112121714209937 + 0.0287669675538981 I,$
 $-0.0422290472490708 + 0.0396995343643532 I, -0.0976571037972037 + 0.127911541159828 I,$
 $-0.0261442671179668 - 0.0548974058962032 I, 0.0655353810766052 - 0.104168565940955 I,$
 $0.0113933278059291 + 0.0398974412743730 I, 0.00145273093754822 - 0.0619001332561941 I,$
 $-0.00295898741671115 + 0.0706359779902267 I, -0.0152158784873551 - 0.0858709836966696 I,$
 $0.0371993143762007 + 0.0442128678380876 I, -0.123459301912686 + 0.00534695572654159 I,$
 $-0.0115051897880332 + 0.155683290365974 I, -0.0686182202425213 - 0.133492961862909 I,$
 $-0.193825982064228 - 0.202733510461619 I, -0.0250516172054813 + 0.0146333466684195 I \},$
 $\{-0.0118326354823244 - 0.103210437227780 I, -0.0929851237932889 + 0.0796732678640214 I,$
 $-0.0325346629822709 + 0.0263927369384032 I, 0.0279422312762364 - 0.138822790937584 I,$
 $0.146834257833049 - 0.0851515384441984 I, -0.295483834978632 + 0.0309443975921210 I,$
 $-0.0338645090500668 + 0.273534049801456 I, 0.190579402583076 + 0.144868028690340 I,$
 $-0.142746317222374 + 0.0778751550485498 I, 0.0215680941117167 - 0.0657543955963039 I,$
 $0.113447503196014 - 0.0488397386358002 I, 0.0692065071531964 - 0.0194330171593179 I,$
 $0.0150578294327876 - 0.0456356157706755 I, -0.0461705384800383 - 0.0356755771709821 I,$
 $0.0324128103540976 + 0.0150644288513018 I, -0.0351656697054564 + 0.0797647788135806 I \},$
 $\{-0.0309360372450842 - 0.0917731365353606 I, 0.0599882767320194 + 0.109333551627723 I,$
 $0.00391755428349184 - 0.0984930991821972 I, -0.0300725658861006 - 0.139273133659748 I,$
 $-0.0309804293422657 + 0.0898626954516352 I, 0.0595216217159224 - 0.131127488118497 I,$
 $-0.165321561412382 + 0.0129206717433064 I, -0.00329835704795488 - 0.0383762056010018 I,$
 $0.0578264117902360 - 0.0287488163728043 I, -0.0294938173435989 - 0.0197097732579218 I,$
 $0.0308302057648827 - 0.110598172490386 I, 0.106735522660711 + 0.141431564252687 I,$
 $0.0203318881593314 - 0.0673468603403993 I, 0.0201444955742644 - 0.00762482444568400 I \},$
 $\{-0.0127852284606991 + 0.0132450949658167 I, -0.0827194714535339 + 0.0474403396450996 I \},$
 $\{-0.0232184510465993 + 0.0436807489654178 I, 0.146437237680789 + 0.0652236765433520 I,$
 $0.0413027933467273 + 0.0272870244055719 I, -0.0194609697779758 + 0.249657888798325 I,$
 $-0.0510092023109336 + 0.131302915201535 I, 0.141605695796902 + 0.0297560407294172 I,$
 $-0.0429714985728125 + 0.109649275116257 I, -0.0655515219336579 - 0.0882346669242513 I,$
 $-0.0149879717410151 + 0.200010714466962 I, -0.0521817645916522 - 0.0374238869738906 I,$
 $0.10447560726573 - 0.0439127466046309 I, 0.0255867240308093 - 0.00974224103324367 I,$
 $-0.162547746278772 - 0.0141691202696717 I, -0.0726416502921618 + 0.0667336442559679 I,$
 $-0.137970613487762 - 0.115901204710668 I, -0.0505913066465055 + 0.00241176673316720 I \},$
 $\{0.0822983221790220 - 0.0474518213347779 I, -0.0158901632857026 - 0.180461338437815 I,$
 $0.131501560973463 + 0.0613260263905355 I, -0.121365099133982 - 0.00974395105736305 I,$
 $0.0240057519931852 + 0.0666463168777986 I, 0.0292393031270303 - 0.181575866685715 I,$

$-0.0909154286990823 - 0.0152178344977944 I, -0.0463022553961827 + 0.0507051818628257 I,$
 $-0.0944546028013596 + 0.0926682378776882 I, 0.0701609457009481 + 0.101317763524354 I,$
 $-0.0205846608252977 + 0.139365482459972 I, -0.0917783795263319 + 0.0300222633187670 I,$
 $-0.185034415983465 + 0.0407508138649586 I, 0.0103103592066350 - 0.104792606530552 I,$
 $-0.0181467078725164 - 0.0566247644975475 I, 0.0989001992098107 - 0.0679973971476150 I \},$
 $\{-0.0863854931317873 - 0.115096994377656 I, 0.0352863123000902 - 0.0150068642262310 I,$
 $0.00341402127114774 + 0.141025799912062 I, -0.199836059456227 + 0.0143564655391287 I,$
 $-0.128474367002812 - 0.00498906151483311 I, 0.0119502242944062 + 0.0163809658309385 I,$
 $0.106596306218010 - 0.124272624615803 I, 0.00747320054542445 + 0.171645237807801 I,$
 $0.00512723643481402 + 0.0293361286983472 I, -0.245814734213528 - 0.00585001368077466 I,$
 $0.0326634259802672 + 0.0778499568501653 I, 0.0756649717107095 + 0.0203065231181358 I,$
 $0.0290077835801666 - 0.0896869568697387 I, 0.0620976938612835 + 0.0615092277562654 I,$
 $-0.0224373966456859 + 0.141771358081184 I, 0.0695247881263345 - 0.0571624542888200 I \},$
 $\{0.0848691425737881 - 0.0952733556587323 I, -0.00649448210346616 - 0.0190552671259053 I,$
 $0.0409126332535626 - 0.0483545463953764 I, -0.0524886675472393 + 0.0687756675330330 I,$
 $0.0190933561273036 - 0.0471189956326473 I, -0.130177576573764 + 0.0133158025059951 I,$
 $-0.0887377564160506 + 0.0616033446370246 I, 0.169457478388538 + 0.207859874444965 I,$
 $-0.0451460821731093 - 0.0354521201482620 I, 0.0462042289950452 - 0.114284712252094 I,$
 $-0.0932888415625769 - 0.0702704062210345 I, 0.102103391621519 + 0.128386951425360 I,$
 $0.00423112579904485 - 0.146070749295539 I, 0.0159620877571188 - 0.0975624188029686 I,$
 $-0.0517426796886379 - 0.000907212137085250 I, 0.0158340273931913 - 0.0182206421755171 I \},$
 $\{0.0679647215422411 - 0.148879082903746 I, -0.0190279207421438 + 0.0176660624307736 I,$
 $-0.0295822624112130 - 0.0622966963973286 I, 0.0267775515608015 - 0.0925270008612462 I,$
 $0.0329817370317017 + 0.0796317136519403 I, 0.0323450146899394 + 0.0448393541632969 I,$
 $-0.0444451940208512 + 0.0354578282280341 I, -0.0748857255635172 - 0.0365994521058194 I,$
 $-0.00346814407011564 + 0.0535314666287576 I, -0.0709833014932522 + 0.0908051525408860 I,$
 $-0.0578057672809273 + 0.00721397123364916 I, -0.186828754305812 - 0.0165046874494438 I,$
 $-0.0436157046729809 - 0.0910294450056731 I, -0.0428543233525811 + 0.0108756174663330 I,$
 $-0.102574242966070 - 0.0588815582764013 I, 0.0979729710863607 + 0.0467173596793684 I \},$
 $\{0.0506085109150077 - 0.106456699167290 I, -0.0684809639477499 - 0.0607844517190391 I,$
 $0.0455514116213238 + 0.0318525029436447 I, -0.0215502750138470 - 0.232739881101938 I,$
 $0.0404175210841512 - 0.0680631223481761 I, -0.0236267937207555 - 0.0527805689838223 I,$
 $0.0512114007554632 - 0.123808983597969 I, -0.0461719732438773 - 0.116055422701146 I,$
 $0.0259100466894248 + 0.0596103313784723 I, -0.0629320099189093 + 0.0967842404591232 I,$
 $0.0534623814587499 - 0.0197739988459543 I, 0.0200090949358617 + 0.166411265371757 I,$
 $-0.102509556693028 - 0.0699569474963283 I, -0.102293222630200 - 0.0362285596057876 I,$
 $0.220025325569240 + 0.104319814924145 I, -0.0419046522045051 + 0.0688864251680750 I \},$
 $\{-0.0821417344628279 + 0.00540051722990871 I, 0.0639687317498659 + 0.101012195499515 I,$
 $-0.0757588013075271 + 0.0548040722532367 I, 0.0199489724556975 - 0.130333147987155 I,$
 $0.127361342998320 + 0.0799570325425670 I, -0.0244690542197446 + 0.0396553743556133 I,$
 $-0.0341376621947945 - 0.0668824818180549 I, -0.0604241879739837 - 0.0174579343720107 I,$
 $0.00254545880388477 + 0.109886369173674 I, -0.124297593032155 + 0.00412017800015455 I,$
 $0.0795948214581361 - 0.00777444459787596 I, -0.0762886933566725 - 0.119741786610626 I,$
 $-0.0212779074117873 + 0.104922369994601 I, 0.0289018593361354 - 0.0481455224188759 I,$
 $-0.0485366008203410 + 0.0726830682241494 I, 0.00801413647471125 - 0.100556761982238 I \},$
 $\{0.0773063899147400 + 0.104500251012214 I, 0.0223841583652599 + 0.0335793303262228 I,$
 $0.241787733161477 + 0.157938501165633 I, -0.0437807140182614 - 0.0666396731794333 I,$
 $-0.0617746542635587 - 0.0144811860970574 I, 0.0261015980215754 + 0.0385168672403975 I,$
 $-0.0860853088975147 + 0.142407555796825 I, 0.155153324488739 - 0.0901406969520066 I,$
 $0.0832048397703086 + 0.0506959532717787 I, -0.0141894648774996 + 0.112301683945562 I,$
 $0.0823346961368635 - 0.140999787117142 I, -0.0908642132768906 - 0.0400764929880320 I,$
 $-0.0494550066944156 - 0.00844616512903889 I, 0.0676532983041198 - 0.0488053808738025 I,$
 $-0.0898594099522237 + 0.0212468998550593 I, -0.0160340347026941 - 0.188634214801470 I \},$
 $\{-0.101230544554414 - 0.0617340988446553 I, 0.0501030935985476 - 0.00597062146732171 I,$
 $-0.0203179124263883 + 0.0979406342041178 I, 0.0302427593387874 + 0.0285015100508219 I,$
 $0.0308887775166264 + 0.0718135156809797 I, -0.114418923300015 + 0.0497430669104828 I,$
 $0.155958008221731 - 0.110175668661981 I, -0.0189599324678679 + 0.137475900002474 I,$
 $-0.111793269628165 + 0.0785675007177127 I, 0.0158515724801182 - 0.0948903868702153 I,$
 $-0.0759500728352900 + 0.0621223910667638 I, 0.0846770722733160 - 0.0157032439814213 I,$
 $-0.109522160354693 - 0.00731165899918668 I, 0.0447348806550991 + 0.0636162528363136 I,$
 $-0.00970256946187396 + 0.0227967976029429 I, -0.159312588350274 + 0.0281906631447752 I \} \};$
 $E2 = \{0.0427070928013415 + 0.00199746620328997 I, -0.0136553278181962 - 0.113876396678592 I,$

0.18943666883529 - 0.0378067927627540 I, -0.0965217753847287 - 0.0547241298896174 I,
 0.0944119841250714 + 0.0189616487858097 I, 0.160843581172613 + 0.147701124266284 I,
 -0.0285787740965284 + 0.0174480336431249 I, -0.0221447858599124 - 0.0254604725952083 I,
 -0.120394982434197 - 0.150067613286174 I, 0.0861757378591553 + 0.0254400791495580 I,
 0.102313105175715 - 0.0236087732265817 I, -0.0586198569430925 + 0.0325313328463710 I,
 -0.101165315635613 - 0.0246289517021289 I, -0.0521721724489491 + 0.0261042811191245 I,
 0.0277104857605902 - 0.0123407609845495 I, 0.0571207315231798 + 0.111218387701244 I},
 {-0.0275575880537401 - 0.0406819393127364 I, 0.0431404304369874 - 0.133632231148488 I,
 -0.0878411072846488 + 0.0200676373143301 I, -0.196860405815917 + 0.0351611472667314 I,
 -0.0172113375995790 - 0.0930797158216488 I, -0.000378892780403069 + 0.218715263446225 I,
 0.0410798059431400 - 0.0758192813932984 I, -0.153430760216877 + 0.0637927260086311 I,
 -0.0275202651561203 - 0.0375658450299332 I, 0.0898276571711668 + 0.00602058891329832 I,
 0.0114602205332890 - 0.0529654392780474 I, 0.0418270222899041 - 0.0282099255519564 I,
 0.0254707224877161 + 0.105772487347213 I, 0.123443083936487 - 0.0932198974522128 I,
 -0.0205441113144470 + 0.0310009514608390 I, -0.0352367183053605 - 0.0596932875256350 I},
 {-0.0663617709214414 - 0.0342662919040174 I, 0.0727276007969980 - 0.0690831440755507 I,
 -0.0868090027615303 - 0.0497291823523401 I, -0.0650317716794432 + 0.0357166545206417 I,
 0.00141014567566464 - 0.0933369008656765 I, -0.108636124687108 + 0.0923417440991899 I,
 -0.0571082531346395 - 0.0351985970302235 I, 0.00243120206640560 + 0.0112249625423124 I,
 -0.0704142107501897 - 0.0140788290501322 I, -0.0855946763840041 + 0.0986045785268446 I,
 0.0225185157109198 - 0.0372132542830593 I, -0.0342955253932196 + 0.0550593576962688 I,
 -0.000549743188338151 + 0.119112631183629 I, -0.0472169758631359 + 0.119503387903446 I,
 -0.0231635147833472 + 0.0660550133168735 I, -0.0370758021111729 + 0.172069897885262 I},
 {-0.0728290756213172 - 0.0884458594043660 I, -0.0485979321729008 + 0.0195023771546775 I,
 -0.0298110528940877 - 0.0441628089004085 I, 0.129489021735484 - 0.00790280237711128 I,
 -0.0685791378083980 + 0.0774830447145142 I, 0.114037073402368 + 0.0401902328416146 I,
 0.0144132063116051 - 0.00474828509041392 I, 0.0860976164217233 - 0.106074134143853 I,
 0.0628145355536667 - 0.189640464709910 I, -0.00268508137930437 - 0.0428759589299339 I,
 -0.0639365121814929 - 0.0299800710524033 I, 0.0367387868506566 - 0.0691610562190437 I,
 0.106836301738979 - 0.0175805922435553 I, -0.152981983015143 - 0.0900129196714806 I,
 0.0333253850451061 + 0.0358687324010277 I, 0.0597136209573466 - 0.0788813235188227 I},
 {-0.0225597951364759 + 0.125400857156221 I, -0.0629831290539875 + 0.0848992186047231 I,
 -0.0321363290410211 + 0.0753503689270317 I, -0.0622971948673259 - 0.0161539545355114 I,
 0.117073127994770 - 0.198102972536623 I, -0.0669470743891973 - 0.00522300271446098 I,
 0.100762285491121 + 0.0596182391967234 I, 0.0467558529912113 - 0.0670304932203644 I,
 0.0896193735831176 - 0.140540121398204 I, -0.0855328110240963 - 0.0122917356209359 I,
 -0.124082968390902 + 0.293543939413664 I, -0.124323666322002 + 0.131874388283897 I,
 -0.0193006568933500 + 0.0558431808451670 I, 0.193357168281156 - 0.00608337974760186 I,
 -0.0734679534432348 - 0.0395218182964157 I, -0.153540808623327 + 0.0602103956206801 I},
 {-0.0633319619442652 - 0.00560560450986694 I, 0.0838030134508402 - 0.0589527099936786 I,
 -0.0318812784979467 - 0.223905428747557 I, 0.0298229219667137 - 0.00797755935443062 I,
 -0.0501732598377602 - 0.0517561126846986 I, -0.0912513261035088 + 0.00460930691108069 I,
 -0.0331698800366139 - 0.0551203974075508 I, 0.0338010088478671 + 0.0271325515432192 I,
 -0.0202306895574161 + 0.0937151037049981 I, -0.109732223550710 + 0.0468680285991969 I,
 -0.00345514077959421 - 0.0448786655115297 I, 0.0557540205528192 - 0.00159675584284907 I,
 -0.00756294836182239 + 0.0470448929095807 I, 0.0412875859959290 - 0.0156009257985674 I,
 -0.0132398823185754 - 0.00963324254055805 I, -0.0582305821263382 - 0.0602138275491020 I},
 {-0.0347556452595942 - 0.0388056508948010 I, 0.0541075705981141 - 0.0400140274118182 I,
 -0.134690851660243 - 0.0326519935100917 I, 0.0961421246692608 + 0.0613974968584806 I,
 -0.0112339450967430 - 0.110415477626212 I, -0.0571190664164929 - 0.0440754572489726 I,
 0.0212711001286028 - 0.0932201729605593 I, 0.0105979957913018 - 0.160192353399763 I,
 0.0745001800244681 - 0.0114928766135747 I, 0.0650162520409578 - 0.0151736621264183 I,
 0.0124075757788971 + 0.167955150955960 I, -0.0344168136676094 + 0.0343133295024952 I,
 -0.0379637481386471 - 0.124002161481975 I, -0.0426967667995384 + 0.0354357882195599 I,
 -0.00587189328068259 - 0.0578600242529719 I, 0.0160576329532105 + 0.0489949554514632 I},
 {-0.190809313792196 - 0.171072712300264 I, -0.177622867413939 - 0.0406157403266163 I,
 -0.0966078286554574 + 0.00281555376842845 I, 0.0641870933824552 - 0.0440630232440615 I,
 -0.130597099162118 - 0.0178318243470179 I, -0.0381604247276034 + 0.00743528451645108 I,
 -0.0421496474340534 + 0.0778786893430603 I, -0.174510212536294 - 0.0332186719902745 I,
 -0.0892025811292502 + 0.0266403229233226 I, -0.0334891680340061 + 0.147210498660982 I,
 0.0200856650238255 + 0.0806711148304596 I, -0.0980373850341237 - 0.132517882067773 I,
 -0.0188984430371617 - 0.125754187536077 I, 0.0236753635902320 + 0.0114307449545868 I,

$-0.125943662486302 - 0.00711956774032972 I, -0.0933646202814541 - 0.0129239101086959 I \},$
 $\{-0.0318956233744262 - 0.0178814369996651 I, 0.0367237040426138 - 0.0107169660412260 I,$
 $0.0371326314136259 + 0.0697855342932707 I, 0.0941501787589036 + 0.211199789277144 I,$
 $-0.0240795905373791 - 0.114390505439495 I, -0.0765998120385129 - 0.0977811412015492 I,$
 $-0.0577721421198696 + 0.0112696368298573 I, 0.0468474248560329 - 0.103754884001501 I,$
 $-0.0112607016325327 - 0.0965432631584784 I, -0.0349866410619110 + 0.0715883047266628 I,$
 $0.0850343908701594 + 0.0938175402889482 I, 0.0602227293602918 - 0.149581100440099 I,$
 $0.126389692892907 - 0.0362807679197662 I, 0.110676074060897 + 0.0143232631702621 I,$
 $0.0633558038278377 + 0.0351093578877932 I, -0.0301426417518862 - 0.136473560922521 I \},$
 $\{-0.123855801604729 + 0.0528156604202327 I, 0.0223461418783796 + 0.0198870375105474 I,$
 $0.0694809815286783 + 0.163000024193226 I, 0.0477477031224998 + 0.0197549047578833 I,$
 $0.0116429369821421 - 0.163545773514451 I, 0.0478284015767198 - 0.0210703680968135 I,$
 $-0.102359837650613 - 0.0295982143074365 I, -0.0864611031930062 + 0.0394360074454642 I,$
 $0.0470853282061236 + 0.0753129802101780 I, 0.125472727140047 + 0.0409079402337063 I,$
 $0.0578736907010033 + 0.0132148836630376 I, 0.0169473806673967 + 0.0798396525471705 I,$
 $0.0383596793521081 - 0.0120258059864372 I, -0.135463447602639 - 0.00501709310473148 I,$
 $0.0677740447051647 + 0.0985314445586576 I, 0.192190721455775 + 0.207956438921668 I \},$
 $\{-0.0355045297571870 + 0.00587555509055945 I, -0.0310102966674833 - 0.107923437283870 I,$
 $-0.0653204493488775 - 0.176538766249361 I, 0.0602423306350051 + 0.241580547492057 I,$
 $0.0413556840501175 + 0.0199206946493877 I, -0.0552622097575649 + 0.154948389170064 I,$
 $0.0286094491884775 + 0.0499377549441635 I, -0.0308599218805003 - 0.0492139577314185 I,$
 $0.0886101859871370 + 0.0436890846058536 I, 0.0300614438416452 - 0.0425505437187352 I,$
 $-0.0604904768802374 + 0.00612499088396591 I, 0.00312044023774419 + 0.0338003542854416 I,$
 $-0.113189750402949 - 0.00982839511952701 I, -0.000632977038380913 + 0.0711189834219693 I,$
 $0.152400349782771 + 0.0378852587712256 I, -0.0534173693688757 + 0.0204776032492029 I \},$
 $\{-0.0290496856751493 - 0.108517994798180 I, -0.159902644538959 - 0.0498158095263727 I,$
 $0.0466297237885898 - 0.0335631089747458 I, 0.0931384801271451 + 0.0565690839508534 I,$
 $-0.0842591670191840 - 0.0392360010304926 I, -0.129582646985868 + 0.0283863272287046 I,$
 $0.0857800083623394 - 0.0578594272673614 I, 0.0139042010531401 + 0.0241468942067818 I,$
 $0.0134646655030480 - 0.0184899648146094 I, 0.294796449130051 + 0.155587152834550 I,$
 $0.0752065739550447 - 0.0128423825425423 I, 0.0269857330763662 - 0.189734388547562 I,$
 $-0.0580087563136088 - 0.0314863734922707 I, 0.0492197928862805 - 0.0741392657077702 I,$
 $-0.250408162811038 - 0.0898722417854675 I, -0.0128451429354375 + 0.200462874335770 I \},$
 $\{-0.122874149763327 - 0.118587562680544 I, -0.0693426976260546 - 0.0396066614630267 I,$
 $0.0173451633398852 + 0.0724077807686525 I, 0.0533636400606740 - 0.114960291103813 I,$
 $-0.173814846305836 - 0.247957596918615 I, -0.0974025073085666 + 0.120568272969258 I,$
 $-0.0588686106487620 + 0.0558616236862849 I, -0.0396970062579524 + 0.00591186566645459 I,$
 $0.0946593402837961 + 0.0424412040329193 I, 0.0814577938627198 - 0.121726453120226 I,$
 $-0.0469204532190175 - 0.0596418668343561 I, -0.000262659039448696 - 0.0382092394586420 I,$
 $0.0667718441268801 + 0.0187449175593355 I, -0.0895368839283049 - 0.0248124632612007 I,$
 $-0.0176969512261311 - 0.101954529933148 I, -0.120837867678893 + 0.0475979230287344 I \},$
 $\{-0.0672723098344599 + 0.00400592107503198 I, -0.00550832218305991 - 0.0296736567433868 I,$
 $-0.0691548202555815 - 0.0511944112216329 I, 0.115348279972056 - 0.0384804350061622 I,$
 $0.0302546836052186 + 0.201242359641500 I, -0.0446863049282728 + 0.216205512379607 I,$
 $-0.0492792493636078 + 0.0609086372206984 I, 0.0386439559427433 - 0.114597877373519 I,$
 $-0.0689513179009221 - 0.104468497744728 I, 0.00153081612326186 + 0.101715564073217 I,$
 $0.0975607554358904 + 0.0602834820058265 I, 0.119975895762014 + 0.300356653215935 I,$
 $-0.0351291590440576 + 0.102909444064566 I, 0.0513475353236981 - 0.0711386679770900 I,$
 $-0.072892503332769 - 0.0501106293560428 I, 0.0679307508096297 - 0.0195266071126098 I \},$
 $\{-0.0580757540851644 + 0.0207288315441561 I, 0.0221581320155956 - 0.0201359128256242 I,$
 $0.143947894761158 + 0.0901338636652783 I, 0.0381982217091188 + 0.113216991486740 I,$
 $-0.0148131930785498 - 0.101079208577893 I, 0.0225681791319824 + 0.0712798776948631 I,$
 $-0.0216771697595883 - 0.0187041317242253 I, -0.204219207756125 + 0.102421450653747 I,$
 $-0.112971177332129 - 0.187145709861406 I, -0.0198760152829848 - 0.0671552429603085 I,$
 $-0.104893384183274 - 0.0836750226028885 I, 0.0315595727783868 - 0.0784905978156193 I,$
 $-0.0911141958871793 + 0.143297017748435 I, 0.0159570608448721 - 0.0108349235067535 I,$
 $0.0255520827921504 - 0.0299492709979035 I, -0.158661695847103 + 0.0367677713259320 I \},$
 $\{-0.0578615623842580 + 0.00883895626264980 I, 0.109880754574031 - 0.0848430473148271 I,$
 $-0.0656207450049758 + 0.00730268765745429 I, 0.00299132470992130 + 0.0544985348152020 I,$
 $0.0784796000842968 + 0.0970827948201768 I, 0.0798670986789291 + 0.0296473924850109 I,$
 $0.0569852416383010 + 0.0961894931568307 I, 0.0616572569500971 - 0.0465963247304250 I,$
 $-0.189512218598787 - 0.215187091999388 I, -0.0210410627077898 + 0.100503650287448 I,$

$-0.201672804733969 - 0.0235858180286405 I, -0.0329104663124969 - 0.0657468965639322 I,$
 $-0.0149763141308114 - 0.0603914618827541 I, 0.115080414216316 + 0.136083340542638 I,$
 $-0.0119404360174536 + 0.211517751417210 I, 0.0531219233327009 + 0.133464954288912 I \} \};$
 $E3 = \{ \{ 0.00780215921336187 + 0.125597025062786 I, 0.179726708798944 - 0.0106741438986617 I,$
 $0.0346362568293429 + 0.000606017001352628 I, 0.0409636109697248 + 0.106657766935496 I,$
 $-0.0342245460600017 - 0.0643461945891670 I, -0.0501379356717370 + 0.0267745874843861 I,$
 $0.00275152138739191 + 0.0158599332494662 I, -0.0297718520718570 + 0.0254188579910956 I,$
 $0.117675737566048 - 0.114443433528940 I, 0.116968938179482 + 0.0714358200546068 I,$
 $-0.0783338918066457 - 0.0163176077394568 I, -0.181009856066079 - 0.0154927264469934 I,$
 $-0.0979342201622306 + 0.00982941721175014 I, 0.0697709568660990 - 0.0376032119453227 I,$
 $-0.0829022966012253 + 0.0367419214707060 I, -0.168259291750650 + 0.0559363484201691 I \},$
 $\{ -0.107098643787074 - 0.0234404828584113 I, 0.0535983824907086 - 0.0378572796152177 I,$
 $0.0602140839433709 - 0.112152204442665 I, -0.00244807269479286 - 0.0582351610322442 I,$
 $-0.00379897931986207 + 0.120798735396764 I, 0.0289914673282802 - 0.0252014085460075 I,$
 $0.0214310246602251 + 0.0565650408262115 I, -0.0104000327478351 - 0.0395169259354990 I,$
 $-0.112697259693718 + 0.0120471430374815 I, -0.0385854682983284 - 0.126698946958434 I,$
 $0.152692475160329 + 0.127768064348018 I, 0.0707742886104047 - 0.0910517882296720 I,$
 $0.0487718377360340 + 0.107424684555137 I, 0.125987492330994 + 0.00914390884365969 I,$
 $0.127423128347431 - 0.0979773159603678 I, -0.0345753872397068 + 0.0224959456952508 I \},$
 $\{ -0.186597707905459 + 0.0383042527375014 I, 0.0803760597424655 - 0.0458957933892664 I,$
 $0.103203492065930 + 0.0134490159640194 I, 0.0590993854825877 - 0.0921229976893584 I,$
 $-0.0556744794819522 + 0.00255604353070844 I, 0.0676564931113238 - 0.0818359899583129 I,$
 $-0.164448270943736 + 0.0686479229436703 I, -0.0860508976441319 - 0.0913538905333515 I,$
 $-0.101120149080223 + 0.0585342493223762 I, -0.130721496402022 - 0.153391957261401 I,$
 $-0.0434678492638293 + 0.0550812349447144 I, 0.0164334080266814 + 0.0861015683736227 I,$
 $0.0897743934453811 + 0.125170304218047 I, 0.0115002533427500 + 0.121076276098078 I,$
 $0.0227496151259044 - 0.0473685212769587 I, -0.0913235270506802 + 0.173148460915557 I \},$
 $\{ -0.144400385365622 + 0.0455292746062962 I, 0.0835143978491071 + 0.0803083016016150 I,$
 $0.0159138684292971 + 0.0605284796519339 I, 0.220042126497879 + 0.140163227714092 I,$
 $0.0467592585556566 - 0.0225570528681141 I, -0.140553313945148 + 0.0935376442736031 I,$
 $-0.0583506251729244 + 0.201779766053316 I, -0.0931803769148143 + 0.125723045495750 I,$
 $-0.0593459570709512 + 0.0342092755346413 I, -0.0747007158284082 + 0.0585585649704080 I,$
 $0.0538615135387833 + 0.0121041790379349 I, -0.0487759110411561 + 0.109993293918261 I,$
 $-0.0506467698218913 + 0.0145017431418299 I, -0.0445355380050912 + 0.0720083262604985 I,$
 $0.0464842647132952 - 0.0270167284918033 I, 0.0500553241717375 - 0.00151401924284268 I \},$
 $\{ -0.101879095380653 - 0.0773160214971690 I, 0.00969643801572740 - 0.0649092486160399 I,$
 $-0.0780346782676989 + 0.0323029948841745 I, -0.0531888872798947 - 0.164001111148982 I,$
 $0.0173052428586807 - 0.0659594049648748 I, -0.00290062635463587 - 0.120596520629287 I,$
 $-0.0909050353924018 + 0.0389681950104271 I, -0.00904891079925963 + 0.0232846715314484 I,$
 $0.0133026253737984 - 0.116931796332582 I, 0.0808286915645311 + 0.0597095395322534 I,$
 $0.0136674595940158 - 0.111049444021230 I, -0.155390766703204 - 0.0652533766705261 I,$
 $-0.0246229300974509 + 0.00927358984649798 I, 0.00678880799956996 + 0.0475562356074275 I,$
 $0.125158971563388 - 0.183429289423700 I, 0.0088165477007608 + 0.104411110116639 I \},$
 $\{ 0.00395382973084593 - 0.0365038837619680 I, -0.0388630322136994 + 0.0659026318415193 I,$
 $-0.0542093560281585 - 0.106990567000099 I, -0.0660663336484616 - 0.0431309959781652 I,$
 $-0.00514962527475346 - 0.102345651621938 I, 0.179466178072364 + 0.0513145720013938 I,$
 $-0.0428124455458828 - 0.0672890657683891 I, 0.0830449480384768 + 0.0674560363662167 I,$
 $0.100141197517193 - 0.0755242637586832 I, -0.0709359240784994 + 0.143909432579792 I,$
 $-0.0397438352733541 + 0.198706518549517 I, -0.0869053671464288 + 0.0889623517038035 I,$
 $0.0629997908442413 + 0.132068702588866 I, -0.156338481987024 - 0.0685298083568892 I,$
 $-0.0144655855915948 - 0.121309001037305 I, -0.103429968752547 - 0.0217425260577845 I \},$
 $\{ -0.00847896939159094 - 0.0486376906994518 I, 0.0950608261231132 - 0.0764922210919767 I,$
 $0.0654470355225330 - 0.0182435291248992 I, -0.0518111573249211 + 0.0544696194165740 I,$
 $-0.0532862693048979 + 0.0191441604215321 I, -0.0771542807002573 + 0.184749307942011 I,$
 $-0.00227460653682622 + 0.0703468642605776 I, -0.122073156693136 + 0.0952790824144126 I,$
 $-0.106147694702930 - 0.101526530499876 I, -0.0695741350451875 + 0.0358881811704967 I,$
 $0.0790120783162531 + 0.0715042699382574 I, -0.169951840626276 - 0.0122150233324189 I,$
 $0.0969869890535405 - 0.0330702933386007 I, 0.0625404448885521 - 0.0200260897807327 I,$
 $0.0745436625605539 - 0.0967478506060529 I, -0.0848132511777276 - 0.0326521862096359 I \},$
 $\{ -0.0906004100365441 - 0.0834335967337709 I, 0.0392022508336645 + 0.0300561487381795 I,$
 $-0.00431451911998437 - 0.0408696136548836 I, -0.170175599325764 + 0.00802453992496498 I,$
 $0.00345350753742877 - 0.0979754491899369 I, -0.00198393696483374 - 0.182427609963553 I,$

0.150345955455650 + 0.0166120276278597 I, -0.00620415470096225 - 0.0219599822166352 I,
-0.120218037933278 - 0.0926444059619402 I, -0.0489137354143700 + 0.0533771689065093 I,
0.00867707024759127 - 0.0672642856846407 I, -0.00315059540469630 - 0.0292400673277478 I,
-0.106131862717526 + 0.0913804374443689 I, 0.0299922160492283 + 0.0748411242142432 I,
0.0272757809469644 - 0.0492566858658166 I, 0.0376665640518405 + 0.102119008395533 I},
{-0.150079233854565 - 0.0711698089953110 I, -0.0999857447920155 - 0.0169858419160361 I,
0.0870574309674713 + 0.0755321854386952 I, 0.0483808865252591 + 0.0633894254644047 I,
-0.00932243375006589 - 0.0670217853145282 I, -0.00295548344105067 - 0.0189969905529774 I,
-0.0535937419380551 + 0.0161723525602716 I, 0.0313335152153018 - 0.0292265175870523 I,
-0.0580705210955491 + 0.0160252188431431 I, -0.0985714424190649 + 0.0509179702756265 I,
0.0952593228900721 - 0.0484095880996789 I, 0.0579931816385817 + 0.0746843598309805 I,
-0.124824337194613 - 0.140213030020094 I, 0.0581394413956520 + 0.0349133335045702 I,
-0.0366911614914640 + 0.00294433882908822 I, 0.0646842270368554 + 0.0389534435715712 I},
{-0.0439583704723322 + 0.0822680847595609 I, 0.0184183732906530 + 0.0698820000369489 I,
0.178944625489125 - 0.0535588833609138 I, -0.00812697690842078 + 0.0967040866246202 I,
0.0969995334544103 - 0.114109069447835 I, -0.00707143267370099 + 0.0812696979704690 I,
0.00619611528936980 - 0.0236183597770987 I, -0.0860355385146407 - 0.168178442623663 I,
0.0449604527337029 + 0.142749392149769 I, -0.0277687837730870 + 0.0208537748326903 I,
-0.0553672260811285 - 0.0313977172474834 I, -0.123304585008231 + 0.101349280440644 I,
0.210129943911537 - 0.233738238515733 I, -0.0945426565012427 + 0.0835056066532204 I,
0.0168123618975840 + 0.0367543318537092 I, 0.0758113623132068 - 0.00532069148319889 I},
{-0.0291138950821840 - 0.0631710397480631 I, -0.0246984610446063 + 0.0544804342921891 I,
0.0628441979036336 - 0.0683374997564357 I, 0.0918063884812643 - 0.0526767986686226 I,
0.00818587478568174 - 0.00630677949004629 I, -0.0500049260246231 - 0.00765416539255333 I,
0.0849943657866611 - 0.0718181552648787 I, -0.0717839168643614 + 0.0105157740957712 I,
0.0143549942593599 - 0.0764134535412826 I, -0.181950752939441 + 0.0821300070531892 I,
0.137688771577244 - 0.0343095327618221 I, -0.152723089174720 + 0.0850519795362733 I,
0.00208356952934295 + 0.176734273332204 I, 0.00938241684221843 + 0.00956429654147696 I,
-0.0332893083703374 - 0.137271974254702 I, 0.0351094967730239 - 0.111760368347874 I},
{-0.148824126238421 - 0.0512835503448271 I, -0.109376669744482 - 0.136219714756081 I,
0.0616674909116822 + 0.0686740489269813 I, 0.0346387334161795 + 0.0296187884456301 I,
-0.0223354552215262 - 0.000355677381362090 I, 0.0744656576745973 - 0.0852200492567104 I,
-0.000974778381880343 + 0.0342273879662756 I, -0.0423769502525583 - 0.0758971089847378 I,
-0.0182431764416285 - 0.0265077307107618 I, -0.169187198759583 + 0.119626434686010 I,
-0.198941913732355 - 0.216762813156685 I, 0.152858993947006 + 0.236107588150737 I,
-0.0545199249169373 + 0.108744934090079 I, 0.0470012435847744 - 0.0677102456560565 I,
0.0382972923063862 - 0.0386277381006496 I, -0.0941541104691909 - 0.0343821264949737 I},
{-0.0287216275043243 + 0.0234447235894163 I, 0.0198755381733240 - 0.210472858943623 I,
0.192242511466046 - 0.0171864299251409 I, 0.0144660729959391 - 0.0153770435492014 I,
0.0752495571204231 + 0.104825749962352 I, -0.0527101220513733 + 0.0751531715670673 I,
0.0516079788793231 - 0.0413956746127303 I, -0.0416723734240148 - 0.0804251128602850 I,
-0.0237388342758246 + 0.170072995017040 I, 0.00211829405697135 - 0.0793868202929106 I,
0.0281883688922229 + 0.178109995726126 I, 0.0405040765739116 + 0.0481716461867545 I,
0.261713901590125 - 0.00660494866848526 I, -0.136040106676418 + 0.150078628738630 I,
0.0304897038169275 - 0.170968558598155 I, 0.0114394978313386 - 0.0602824692491118 I},
{-0.115355435777772 + 0.00352234357292250 I, 0.268275694587541 - 0.0668944637733256 I,
-0.135922160210879 - 0.132769481041005 I, 0.0576913166680911 - 0.203017082819597 I,
0.0624932598028262 + 0.0639347213664750 I, -0.149930150860914 - 0.0928614830040168 I,
-0.0855933015742530 + 0.0325305393890041 I, 0.0825972549704063 + 0.0215543692354673 I,
-0.0524177311644776 + 0.0238529505526697 I, 0.0209763248504215 - 0.0936433126958803 I,
0.0226461463258003 - 0.0923806461856918 I, 0.0212814814584123 + 0.0229672112942946 I,
-0.0485279546878276 + 0.0901228902586867 I, -0.0121979876220478 - 0.0318809860185512 I,
-0.0290815290743069 - 0.0519940174296223 I, 0.0682364883960001 - 0.0587702166015027 I},
{-0.164065912734665 - 0.161560785192966 I, -0.142554577287511 - 0.0321256597903332 I,
-0.0471240437704009 - 0.0296837414688255 I, 0.0466523645154574 + 0.0763543524613429 I,
-0.118295686047737 + 0.120651818550152 I, -0.0166855437828618 - 0.0742496011147917 I,
0.117278973087108 + 0.135387896186439 I, -0.0960660113595851 + 0.00170931818349255 I,
0.0853884051180384 + 0.00718522828666866 I, -0.0682424272217088 - 0.0713911545757076 I,
-0.0824909126431147 - 0.0931018996095544 I, -0.0248344249931639 + 0.117905499217360 I,
0.0387222594356634 - 0.0704135304491672 I, 0.0802562499618300 - 0.150198075426635 I,
0.142178978049137 - 0.00962190387642390 I, 0.0654173889137152 + 0.0299968727001012 I},
{-0.188254297473329 + 0.0363879591490253 I, -0.0161554977452655 + 0.175235547582104 I,

$0.0940291050844188 + 0.0117813414876744 I, -0.0720889139377294 + 0.0576582049340434 I,$
 $0.123949956523578 - 0.0371526658047407 I, -0.0226162315255483 - 0.0286054632231970 I,$
 $-0.0490197113696324 - 0.00512078159864770 I, -0.0588600441859515 - 0.0662736477389456 I,$
 $-0.0465960970112404 + 0.00472127653336636 I, 0.110926958627681 + 0.0427102140365729 I,$
 $-0.0897732632371266 - 0.0392333347812649 I, -0.0884202171794193 + 0.142380405283794 I,$
 $-0.0266554926271756 + 0.00435383898757029 I, -0.0518971313373209 + 0.000798380234311006 I,$
 $-0.0557757687506877 + 0.139827164690360 I, 0.0244761114241344 - 0.167171845474488 I \} \};$
 $E4 = \{ \{ 0.0795000728322018 + 0.0447484184526321 I, -0.0192692133810577 + 0.0148811905240262 I,$
 $0.0746564151458731 - 0.0968241738378083 I, -0.00269358100633933 - 0.0628751654459325 I,$
 $-0.163969422048475 - 0.0746273332936552 I, -0.0816003541108775 - 0.0617648178546368 I,$
 $-0.0653544843734204 - 0.128909545971246 I, -0.219587855095435 + 0.0396093455589103 I,$
 $-0.136943710075808 + 0.195840482127622 I, 0.00421490171157636 + 0.0535472599864438 I,$
 $-0.0966908433613507 - 0.0459806207868330 I, 0.00446268238748977 - 0.0724199128654455 I,$
 $-0.0478012370492700 + 0.0206537855064991 I, -0.208559174168969 + 0.0443803399581392 I,$
 $-0.0581531067004658 + 0.105486087407921 I, -0.0228855268408959 - 0.0779565209694444 I \},$
 $\{ 0.0540044628937945 + 0.111804957722509 I, -0.0121359455854117 - 0.0694088150993056 I,$
 $-0.0786887446861494 + 0.104857223588550 I, 0.153746125259613 + 0.0907766719240877 I,$
 $0.0305656127337997 + 0.0258693820873992 I, 0.0349144880000810 - 0.0177208658568375 I,$
 $-0.0252860840396036 - 0.108220902711778 I, 0.0583076374928550 + 0.127633717372041 I,$
 $-0.131745723999118 + 0.0471652212104816 I, -0.102822532650317 - 0.00116431984051417 I,$
 $-0.112802684651003 - 0.228209904466754 I, -0.0536573989691704 - 0.0521807451838925 I,$
 $-0.0617666521348647 - 0.120486987958988 I, -0.0719567745952136 + 0.0660358264237425 I,$
 $-0.0464474444908668 - 0.107187169511383 I, -0.0830595385269058 + 0.0810775467219312 I \},$
 $\{ 0.0123054578756725 + 0.192648174972105 I, -0.108719990538793 + 0.0753754288877105 I,$
 $-0.00651917382868594 - 0.0903984993356139 I, -0.188384080012626 + 0.0443373392676576 I,$
 $-0.0592972313214944 + 0.203988741026211 I, -0.159108168277374 - 0.108694752234477 I,$
 $-0.00244289940800732 - 0.0414733467992261 I, -0.0180632899279705 - 0.109620012903425 I,$
 $0.00572701462022801 + 0.0210215701001143 I, -0.0859526847687090 - 0.00155160859916560 I,$
 $0.0980508502137613 + 0.0781632196812455 I, 0.00628374639475529 + 0.0906611667170592 I,$
 $0.0117142726270456 - 0.0292674492495863 I, 0.0869737159669673 - 0.000958228737978475 I,$
 $0.0583981119337738 + 0.232087700709352 I, -0.0939575135364703 + 0.170227786750491 I \},$
 $\{ 0.149478325646879 + 0.00108675337948410 I, -0.0807357570338267 + 0.121394397540870 I,$
 $-0.0600600456825219 - 0.0769983082578559 I, 0.0129613785381449 - 0.0781265509591715 I,$
 $0.0278129362040410 + 0.0662555579166707 I, -0.0264495259985903 + 0.0374052611093846 I,$
 $0.234385397613476 - 0.0128486214255740 I, -0.271655916866670 - 0.0381617456637844 I,$
 $-0.146436785165085 - 0.0469192799412174 I, -0.0503362950562049 - 0.0754275009732876 I,$
 $-0.0209257680711970 + 0.0101203847416127 I, -0.00442382765827591 - 0.0662019993116244 I,$
 $0.0632381705320581 - 0.0190425334562865 I, 0.00425497596634966 - 0.0597957976740829 I,$
 $-0.0741410482618164 + 0.144074740627901 I, -0.0355012132471361 - 0.0384182829765770 I \},$
 $\{ 0.00640623026852716 + 0.0407104588904177 I, -0.0791175486407025 - 0.0383285132899451 I,$
 $-0.188274264441400 + 0.0203853165121955 I, 0.0552551042181374 - 0.0269640537762563 I,$
 $-0.0223261674953533 - 0.0311687067842014 I, 0.0695981924121943 - 0.0516560802180440 I,$
 $-0.292431699286730 - 0.0495918985425656 I, 0.0615202886930442 - 0.133581907101472 I,$
 $-0.112876708841408 + 0.131440830439647 I, 0.00553526048833962 - 0.0490698942618516 I,$
 $-0.0562298447250705 - 0.0526674288788655 I, 0.0104946964703073 + 0.0202679784392222 I,$
 $0.101100958361950 - 0.00417230637880710 I, 0.158966551947836 + 0.0319726704344560 I,$
 $0.0658535395021903 + 0.0211569825745591 I, -0.143395322510738 - 0.000295315579507616 I \},$
 $\{ 0.0705825281558090 + 0.145278784916051 I, -0.0123723297535809 - 0.0474360593865147 I,$
 $-0.0449176181403412 - 0.000135592808226195 I, -0.0103128307543095 - 0.0243726519766532 I,$
 $0.0250312273136634 + 0.0561770312755243 I, 0.0944107902357818 - 0.00612599491866229 I,$
 $0.0136653916671298 + 0.146729646632541 I, -0.0550217826169089 + 0.0581005799048213 I,$
 $-0.0724813460060278 + 0.136323997008479 I, -0.0599886881332731 - 0.0482923450146503 I,$
 $0.124594609445437 - 0.00729186731914102 I, -0.0184130468731811 + 0.148373736780993 I,$
 $-0.134077542879421 - 0.0272328312526994 I, -0.0457364840516161 - 0.231068729715844 I,$
 $-0.0685816817653501 - 0.0271704260250268 I, -0.234337354287606 - 0.0864305736596562 I \},$
 $\{ 0.0345367373786603 + 0.110270827147942 I, -0.0365179624647755 - 0.000652379912514619 I,$
 $-0.118849117235924 + 0.142066003990709 I, -0.0604625449693699 + 0.061097690398674 I,$
 $-0.0688593141081945 + 0.104214233668893 I, 0.163023665043850 + 0.0358418409806853 I,$
 $-0.0618029064980183 + 0.0569977304384313 I, -0.104814811752549 + 0.0643982531965018 I,$
 $-0.00700640323471009 - 0.00646959519234662 I, -0.00786447625096444 + 0.0560550766995849 I,$
 $-0.0394510798857030 - 0.0574925064912790 I, -0.0165053325124334 - 0.0126361701329233 I,$
 $0.0230526199405426 + 0.0688748363130641 I, -0.0649649489804004 + 0.223790388553482 I,$

$-0.0193439156124796 - 0.0731245413663504 I, -0.0134208401296506 - 0.0404559610359284 I \},$
 $\{0.0543009677002960 + 0.0488091997054300 I, -0.0177737363963542 - 0.0991216902592645 I,$
 $-0.158931727751434 + 0.0868597023890751 I, -0.0159534555918632 + 0.0224828389876247 I,$
 $-0.0704578743612408 - 0.00652026384285027 I, -0.0956976880470441 - 0.0800214849511969 I,$
 $0.0164054182811175 - 0.155818079786008 I, -0.00201243996649536 + 0.0699996416863253 I,$
 $0.0497629646085325 - 0.00847669036385303 I, -0.0125837538399882 - 0.125381897965109 I,$
 $-0.00205515681628149 - 0.115350528368678 I, 0.0244190030104447 + 0.0742633184021561 I,$
 $-0.120431324392587 - 0.0356503318307665 I, 0.185483859910851 - 0.0431311023880122 I,$
 $-0.103064603735721 + 0.0204226392687099 I, 0.123256108703812 - 0.00367996991152220 I \},$
 $\{0.00612276638515948 + 0.0801047774444942 I, -0.0945020078951758 + 0.160026135455441 I,$
 $-0.0263007798102686 - 0.0122010663524703 I, 0.0772228911639723 + 0.0186482375261314 I,$
 $0.00188600973514703 - 0.112604420508761 I, -0.0366929339941097 + 0.000938119341825139 I,$
 $-0.00777717657349400 - 0.235386519069397 I, 0.123711295486774 - 0.158367790126706 I,$
 $-0.123642416025431 + 0.0711498838909132 I, 0.0118507400231143 - 0.0423690568135792 I,$
 $-0.0925962227328007 - 0.0481973027311593 I, 0.0300165057636424 + 0.209483183405143 I,$
 $-0.0740223379237415 - 0.131106986306767 I, 0.0212337370597239 + 0.0396084459478583 I,$
 $0.00524645078403514 - 0.0978434475717043 I, -0.0692648583020979 - 0.00171799842675464 I \},$
 $\{0.0587370884423028 + 0.0641027941331677 I, 0.116348077483684 - 0.112108175149134 I,$
 $-0.163612862705868 + 0.239350905406250 I, 0.0285620512675876 + 0.0163659650331983 I,$
 $-0.173444880818990 + 0.157244400030262 I, -0.0855666431962139 - 0.0977046001484752 I,$
 $0.0854904744914325 - 0.0555588836512902 I, 0.00747215970308031 - 0.106203677509263 I,$
 $0.0354909403603143 - 0.0408417148971117 I, 0.117849851133672 + 0.0467464537371153 I,$
 $0.0819430398794248 - 0.0217716610515046 I, 0.0463129485831973 + 0.0880356965636211 I,$
 $0.104059838951551 + 0.0395704200272784 I, -0.122549737598526 + 0.0102216511698902 I,$
 $-0.0131132569206112 - 0.0582518128313549 I, 0.00162777026875022 - 0.210882898137395 I \},$
 $\{0.118404661713376 + 0.101029146205949 I, -0.185741451360822 + 0.0603192122208622 I,$
 $-0.0481642621780343 + 0.0317768462106182 I, 0.0686043883370303 + 0.0102842605156800 I,$
 $0.0240934584344901 + 0.0754723553046963 I, -0.182513747542422 + 0.00804282193987863 I,$
 $0.0610958442056995 - 0.0512070176131857 I, 0.0306646097955689 - 0.0596179034147353 I,$
 $-0.0366622864521520 - 0.0131565823431198 I, 0.0541686706800058 + 0.0918624130713205 I,$
 $0.0862580195502679 - 0.0142491062811612 I, -0.159293723025811 + 0.00114144823633013 I,$
 $-0.103035764039456 + 0.198216249692893 I, -0.0879365640423083 + 0.367991795782539 I,$
 $0.0348913908490944 - 0.0662904401512384 I, -0.0362392424171493 - 0.0671625594118156 I \},$
 $\{0.110644326287516 + 0.183185828906416 I, -0.0134847068225477 - 0.00147806679589516 I,$
 $0.000133448006735232 + 0.0711858019617217 I, -0.00646083565347130 + 0.00930392707794328 I,$
 $-0.138325701394728 - 0.0985399464051971 I, -0.117223936862705 - 0.0327862254082947 I,$
 $0.0567396165835630 - 0.0238935049408593 I, 0.120373016860890 - 0.00683218309660960 I,$
 $-0.0422652410047441 - 0.0368092084551697 I, -0.217892639789029 - 0.184408273642542 I,$
 $0.0870504371017148 - 0.0245625356923017 I, 0.0111627520452673 + 0.0174890613324921 I,$
 $-0.147210486446677 - 0.0464501246305870 I, -0.0889594036750902 + 0.0251867213012987 I,$
 $0.0115615925267698 - 0.00788086824548893 I, -0.150972609900257 + 0.120968799756599 I \},$
 $\{0.212842748465117 + 0.0170893236743892 I, -0.233485388285405 + 0.121654835194901 I,$
 $-0.0971321324716485 + 0.104255896607505 I, -0.0104980321270276 + 0.0746541477943407 I,$
 $0.0843790348515274 - 0.171344494792870 I, 0.0441660478493092 + 0.0628601573125766 I,$
 $-0.104101437457860 + 0.221054585832313 I, -0.0616220166655297 + 0.00621246715307825 I,$
 $-0.138407875156015 - 0.138222920901718 I, -0.00993840675619925 - 0.0224765121362198 I,$
 $0.0836662139664533 + 0.00675187704603134 I, 0.0597625948949549 + 0.0329013681543257 I,$
 $-0.0482112083479921 + 0.0238226600242938 I, -0.0869171422779413 + 0.166329860875983 I,$
 $0.0263647014269383 + 0.0715001349209339 I, 0.0774698902206913 - 0.0230197729173610 I \},$
 $\{0.0927330839602131 - 0.0128019176520678 I, -0.193668888367957 - 0.0572492936274010 I,$
 $-0.00101482991492798 - 0.0796534640499825 I, -0.0804734140857746 - 0.0683618868442422 I,$
 $-0.166304287147224 + 0.0463945690667429 I, -0.0976395732609795 + 0.0180896710277784 I,$
 $-0.0620804984037984 - 0.0230520023884767 I, 0.0493170276024386 - 0.0304091300719072 I,$
 $-0.0660407768759971 - 0.0430381352178645 I, -0.0878638206105099 - 0.00850672669529827 I,$
 $0.0107488883155386 - 0.0978542327929211 I, -0.0723989915625955 - 0.0334007904907206 I,$
 $0.0347543996085645 + 0.0379572612829092 I, 0.110476463433028 - 0.0198232568870933 I,$
 $0.184175655718814 + 0.128130684025783 I, -0.0169878873128861 - 0.0895894197138873 I \},$
 $\{0.0748178630710239 + 0.0810530095502250 I, -0.0979378731510529 + 0.0601430807494969 I,$
 $0.00370538613928538 - 0.0864695338166981 I, -0.109502887274467 - 0.00399488889378139 I,$
 $-0.179565572352388 + 0.0459238652387241 I, -0.0752932254541316 + 0.0154742337152224 I,$
 $0.0207238500447961 - 0.0803514031341186 I, 0.0225733055036028 - 0.0432214442713633 I,$
 $-0.0675629438106809 + 0.0483261529880924 I, 0.176152260141479 + 0.0407962768128008 I,$

```

-0.0586043480807911 - 0.111120458658763 I, 0.00606290911829775 - 0.000625904780262018 I,
0.0356176297635097 + 0.0112713916310856 I, 0.0331881381731597 - 0.0128065763842009 I,
0.0556333501251537 - 0.0742170335259964 I, -0.0677664994058328 + 0.0543807214511369 I},
{0.124558065292282 + 0.0609448290442719 I, -0.0490982665329477 + 0.197254069600885 I,
-0.0894101097809709 - 0.0216648761193079 I, 0.0431287137403479 + 0.0405738162077395 I,
-0.124656748594225 + 0.00586145943608328 I, -0.00699605510688242 - 0.0712165652126409 I,
-0.0356113843585667 + 0.110619022921450 I, 0.0537405662021477 + 0.160595163396734 I,
-0.0493297502039978 - 0.0986821181546958 I, -0.124960739019453 + 0.0891269724937698 I,
-0.0175717067399395 + 0.00692615509605435 I, -0.0767858828449464 + 0.0294288977674801 I,
0.172515251052156 + 0.0583827532785341 I, -0.0824707471164269 - 0.0669786511549297 I,
0.00992531210947728 + 0.0242274755433028 I, -0.0339314883521501 - 0.0890710257450848 I } };

```

Check numerical accuracy of input:

- states should be normalized $\| |\beta_{ab}\rangle \|^2 = 1$
- channel should sum to the identity matrix $\sum_k E_k^\dagger E_k = I$

```

In[38]:= Norm[beta1] - 1
Norm[beta2] - 1
Norm[beta3] - 1
Norm[beta4] - 1
Total[Abs[Flatten[Ct[E1].E1 + Ct[E2].E2 + Ct[E3].E3 + Ct[E4].E4 - Id[16]]]]
Out[38]= 6.66134 × 10-16
Out[39]= -1.11022 × 10-16
Out[40]= 0.
Out[41]= 0.
Out[42]= 7.55388 × 10-14

```

Construct states $|\chi_a\rangle$

```

In[43]:= chi1 = Sqrt[p1] Kr[z0, beta1] + Sqrt[1 - p1] Kr[z1, beta2];
chi2 = Sqrt[p2] Kr[x0, beta3] + Sqrt[1 - p2] Kr[x1, beta4];

```

Check accuracy of the fidelity requirement:

- $\langle \chi_0 | \chi_1 \rangle \geq F$

```

In[45]:= inner = Ct[chi1].chi2
AbsArg[inner]
fid = Abs[inner[[1, 1]]]
fid - F
Out[45]= {{0.935259 - 0.324639 i}}
Out[46]= {{{0.99, -0.334099}}}
Out[47]= 0.99
Out[48]= 1.11022 × 10-16

```

Apply the circuit and find the final states

```

In[49]:= chit1 = Kr[Kr[Kr[Kr[Kr[Kr[Id2, Id2], Id2], Swap], Id2], Id2], Id2].
Kr[Kr[Kr[Kr[Kr[Id2, Id2], Swap], Swap], Id2], Id2].
Kr[Kr[Kr[Kr[Id2, Swap], Swap], Swap], Id2].Kr[Kr[Kr[chi1, chi1], chi1], chi1];

```

```

chit2 = Kr[Kr[Kr[Kr[Kr[Kr[Id2, Id2], Id2], Swap], Id2], Id2], Id2].
  Kr[Kr[Kr[Kr[Kr[Id2, Id2], Swap], Swap], Id2], Id2].
  Kr[Kr[Kr[Kr[Id2, Swap], Swap], Swap], Id2].Kr[Kr[Kr[chi2, chi2], chi2], chi2];
rhot1 = chit1.Ct[chit1];
rhot2 = chit2.Ct[chit2];
rhof1 = Kr[Id[16], E1].rhot1.Ct[Kr[Id[16], E1]] + Kr[Id[16], E2].rhot1.Ct[Kr[Id[16], E2]] +
  Kr[Id[16], E3].rhot1.Ct[Kr[Id[16], E3]] + Kr[Id[16], E4].rhot1.Ct[Kr[Id[16], E4]];
rhof2 = Kr[Id[16], E1].rhot2.Ct[Kr[Id[16], E1]] + Kr[Id[16], E2].rhot2.Ct[Kr[Id[16], E2]] +
  Kr[Id[16], E3].rhot2.Ct[Kr[Id[16], E3]] + Kr[Id[16], E4].rhot2.Ct[Kr[Id[16], E4]];

```

Double-check the normalization of the final states

```

In[55]:= Tr[rhof1] - 1
Tr[rhof2] - 1
Out[55]= 2.66454 × 10-15 - 1.35209 × 10-17 i
Out[56]= 2.22045 × 10-16 + 9.83712 × 10-18 i

```

Calculate the error rate for each basis a for each measurement pair

```

In[57]:= p11 = Abs[Tr[mx1.rhof1]];
p12 = Abs[Tr[mx2.rhof1]];
p13 = Abs[Tr[mx3.rhof1]];
p14 = Abs[Tr[mx4.rhof1]];
p21 = Abs[Tr[mx1.rhof2]];
p22 = Abs[Tr[mx2.rhof2]];
p23 = Abs[Tr[mx3.rhof2]];
p24 = Abs[Tr[mx4.rhof2]];
p31 = Abs[Tr[mz1.rhof1]];
p32 = Abs[Tr[mz2.rhof1]];
p33 = Abs[Tr[mz3.rhof1]];
p34 = Abs[Tr[mz4.rhof1]];

```

Calculate the total error rates δ_{ph} , δ_x and δ_z

```

In[69]:= dp = 1 / 4 (p11 + p12 + p13 + p14)
dx = 1 / 4 (p21 + p22 + p23 + p24)
dz = 1 / 4 (p31 + p32 + p33 + p34)
Out[69]= 0.440788
Out[70]= 0.196967
Out[71]= 0.49876

```

Check whether the claim $1 - h\left(\frac{1-F}{2}\right) \leq \frac{\delta_x + \delta_{ph}}{2} h\left(\frac{\delta_x}{\delta_x + \delta_{ph}}\right) + \frac{2 - \delta_x - \delta_{ph}}{2} h\left(\frac{1 - \delta_{ph}}{2 - \delta_x - \delta_{ph}}\right)$ in fact holds

```
In[72]:= h[x_] = -x Log2[x] - (1 - x) Log2[1 - x];  
lhs = 1 - h[ $\frac{1 - F}{2}$ ];  
rhs[ddx_, ddp_] =  $\frac{ddx + ddp}{2} h\left[\frac{ddx}{ddx + ddp}\right] + \frac{2 - ddx - ddp}{2} h\left[\frac{1 - ddp}{2 - ddx - ddp}\right];$   
lhs  
rhs[dx, dp]  
rhs[dx, dp] - lhs
```

Out[75]= 0.954585

Out[76]= 0.949684

Out[77]= -0.00490171