

A COMPARISON BETWEEN PREPARE-AND-MEASURE AND ENTANGLEMENT-BASED PROTOCOLS

A Thesis

presented to

the Faculty of Natural and Applied Sciences

at Notre Dame University-Louaize

In Partial Fulfillment

of the Requirements for the Degree

Master of Science in Computer Science

by

FIRAS FRANÇOIS EL-JERDY

JULY 2022

© COPYRIGHT

By

Firas Francois El-Jerdy

2022


All Rights Reserved Notre Dame University - Louaize


Notre Dame University - Louaize
Faculty of Natural and Applied Sciences
Department of Computer Science

We hereby approve the thesis of

Firas Francois El-Jerdy

Candidate for the degree of Master of Science in Computer Science


Dr. Marie Khair Supervisor, Chair


Dr. Hoda Maalouf Committee Member

Declaration

I declare that this piece of work is my own and was completed for the partial fulfillment of the MSc of Computer Science at Notre Dame University - Louaize and has not been previously submitted as a dissertation or thesis to any national or international institution. I was acquainted with the academic ethics and research guidelines of Notre Dame University - Louaize and accept all ownership and authorship over this piece of work.

Acknowledgments

Words cannot describe the immense gratitude I hold for professor and chair Dr. Maalouf for her unending patience, rock-solid academic/ethical values, and continuous assistance throughout the writing of this piece of work. I would also like to thank Notre Dame University and the Faculty of Natural and Applied Science for providing me with a unique opportunity to pursue my master's degree and helping shape my career in academics.

I am also grateful to the professors whom I had the honor to meet during the program, which not only provided me with invaluable lessons and knowledge from the field but fueled my thirst for lifelong learning, which influenced my attitude towards life.

Finally, I would be remiss in not mentioning my support from my parents and siblings, Jad, Rawad, and Stephanie, for their belief that kept my spirits and motivation high throughout this process. A thank you should also go out to baby Jude for bringing a constant supply of joy and love into our lives.

Thank you,

Firas El-Jerdy

Table of Contents

| | |
|-----------------------------|------|
| Acknowledgments | v |
| Table of Contents | vi |
| List of Figures | viii |
| List of Abbreviations | ix |
| Abstract..... | x |

Chapter 1: Basics of key distribution..... 11

| | |
|------------------------------------------------|----|
| 1.1 Introduction to the General Problem | 11 |
| 1.2 Polarization of photons | 15 |
| 1.3 An introduction to the BB84 protocol | 16 |

Chapter 2: Quantum systems 18

| | |
|--------------------------------------------------------------------|----|
| 2.1 Introducing quantum systems | 18 |
| 2.2 The preparation stage of a QKD | 19 |
| 2.3 Overview of a quantum channel in a QKD | 20 |
| 2.3.1 Conveying quantum channels with the Kraus decomposition..... | 22 |
| 2.3.2 The unary-evolution channel | 23 |
| 2.3.3 The amplitude damping channel..... | 23 |
| 2.4 The measurement channel | 25 |

Chapter 3: Composite systems..... 26

| | |
|----------------------------------------------|----|
| 3.1 Introduction to composite systems | 26 |
| 3.2 Overview of the Hilbert space | 28 |
| 3.2.1 An example of a composite system | 29 |
| 3.3 Entanglement | 29 |
| 3.4 The Schmidt Decomposition | 30 |
| 3.5 Entanglement for mixed states | 31 |
| 3.6 Partial trace | 31 |
| 3.7 Classical-quantum ensembles..... | 32 |
| 3.8 Evolution of composite systems | 33 |
| 3.9 The no-cloning theorem..... | 35 |

Chapter 4: Prepare-and-measure Vs Entanglement..... 37

| | |
|-----------------------------------------------------------------------------------------------|----|
| 4.1 Introduction | 37 |
| 4.2 Prepare-and-measure | 38 |
| 4.2.1 Sifting step in a prepare-and-measure protocol | 39 |
| 4.2.2 Intercept and resend strategy | 40 |
| 4.3 The six-state protocol | 42 |
| 4.4 The SARG04 protocol | 43 |
| 4.5 Entanglement-based protocols..... | 46 |
| 4.6 The Ekert protocol | 47 |
| 4.6.1 Measurement operations | 47 |
| 4.6.2 The CHSH inequality in the classical case | 49 |
| 4.6.3 Steps of the Ekert protocol..... | 49 |
| 4.7 Entanglement-based BB84 protocol..... | 50 |
| 4.8 Connection between prepare and measure protocols and entanglement-based protocols..... | 53 |
| 4.9 Conclusion | 55 |

| | |
|---------------------------|-----------|
| Bibliography | 56 |
|---------------------------|-----------|

List of Figures

| | |
|------------------------------------------------------------------------|----|
| Figure 1.1 Normal distribution of letters in the English alphabet..... | 12 |
| Figure 1.2 One Time Pad scheme | 12 |
| Figure 1.3 Ideal key generator scheme | 14 |
| Figure 1.4 Polarization filter in the rectilinear basis | 15 |
| Figure 1.5 BB84 distribution protocol | 16 |
| Figure 1.6 Stages of the BB84 protocol..... | 17 |
| Figure 2.1 Stages of a quantum key distribution protocol | 18 |
| Figure 2.2 A quantum channel..... | 21 |
| Figure 2.3 An amplitude damping channel | 24 |
| Figure 3.1 Quantum experiment A..... | 26 |
| Figure 3.2 Quantum experiment B..... | 27 |
| Figure 3.3 A system containing experiments A and B..... | 27 |
| Figure 3.4 A quantum system that maps from system A to system B | 33 |
| Figure 3.5 Evolution on the subsystem A and B..... | 34 |
| Figure 3.6 The no-cloning theorem..... | 35 |
| Figure 4.1 Basic structure of a Prepare-and-measure protocol | 38 |
| Figure 4.2 A detailed overview of the steps in the BB84 protocol | 41 |
| Figure 4.3 A quantum system that maps from system A to system B | 43 |
| Figure 4.4 A basic PNS attack on a protocol | 44 |
| Figure 4.5 General scheme of an entanglement-based protocol | 46 |
| Figure 4.6 Bloch sphere of Alice's measurement operations | 48 |
| Figure 4.7 Bloch sphere of Bob's measurement operations | 48 |

List of Abbreviations

| Abbreviation | Term |
|---------------------|----------------------------------|
| A | Alice |
| B | Bob |
| C | Cyphertext |
| CHSH | Causer-Horne-Shimony-Holt |
| CSS | Calderbank-Shor-Steane |
| E | Eve |
| PNS | Photon Number Splitting |
| POVM | Positive Operator-Valued Measure |
| TLS | Transport Layer Protocol |

Abstract

Quantum key distribution uses special purpose hardware and quantum mechanics to distribute cryptographic keys in a system for its usage in a classical symmetric key scheme for encryption and decryption. There are two appeals for going to such length of creating special hardware and utilizing quantum mechanics to distribute keys over parties. First, detecting eavesdropping on communication due to the fundamental properties of photons governed by quantum mechanics. Second, offering a solution to the byproduct effect of quantum computers breaking the most common asymmetric schemes (Transport Layer Protocol). In this research paper, prepare-and-measure and entanglement-based protocols are compared on an implementation level to understand the various components and the context in which they are utilized.

Keywords: Quantum Key Distribution Protocols, Quantum Computers, Quantum Information Theory, Prepare-and-measure protocols, Entanglement-based protocols, Quantum Security, Quantum Mechanics, Calderbank-Shor-Steane, Causer-Horne-Shimony-Holt.

Chapter 1: Basics of key distribution

1.1 Introduction to the General Problem

Cryptography is a topic that has played a role in history leading back to the ancient Greeks. The Roman Empire and its modern republic used a cipher to encrypt and decrypt their messages, especially in conflict with warring nations. Enemies failed to intercept crucial messages from Rome sent to the frontline commanders. One such ingenious idea in its time was the Caesar-cypher. The plain alphabet $\{a, b, c, \dots, z\}$ would be offset by a predetermined number of letters in either the left or the right direction. Traditionally, the Caesar-cypher was offset 3 letters to the right. Hence, the cypher alphabet became $\{d, e, f, \dots, c\}$.

Suppose we want to send a message using this encryption scheme. A plain message that looks something like *MEET ME NEXT TO TREE* would translate to cyphertext of *PHHW PH QHAW WR WVHH*. This produces an unreadable sequence of letters that seems arbitrary to human readers. The sender and the receiver know the action in which the plaintext is encrypted. However, even if the message looks random at first, there are mathematical ways where it could easily decrypt. In every language, the letters are not equally distributed in frequency. For example, the letters E and T are the most used in the English alphabet. [1]

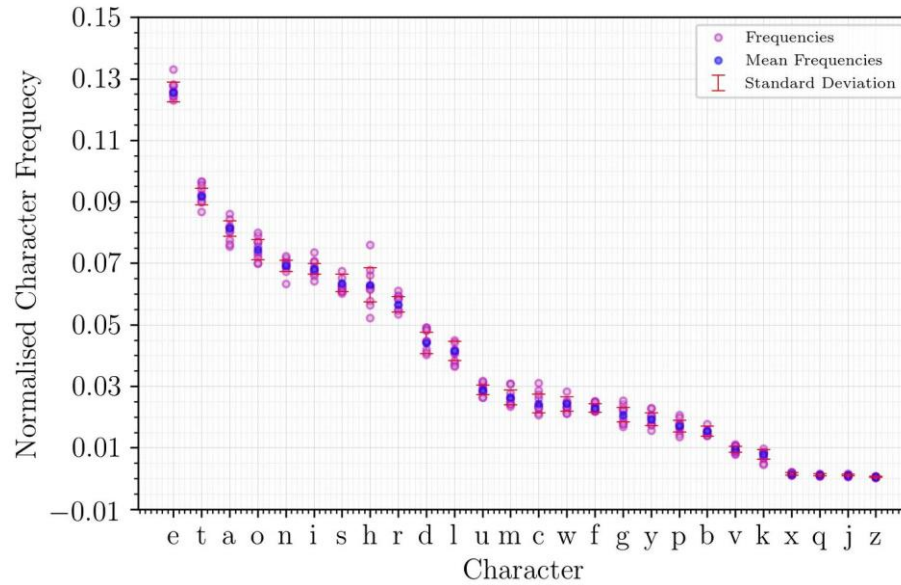


Figure 1.1 Normal distribution of letters in the English alphabet

In the above text, the letter E has been used six times and T four times. The sentence is a typical English-written text. Frequency analysis would quickly decrypt the cipher text. It gets faster with longer plaintexts since a more typical combination of letters forms [2]. Fortunately, there are provably secure encryption schemes. One such scheme is the One Time Pad (OTP).

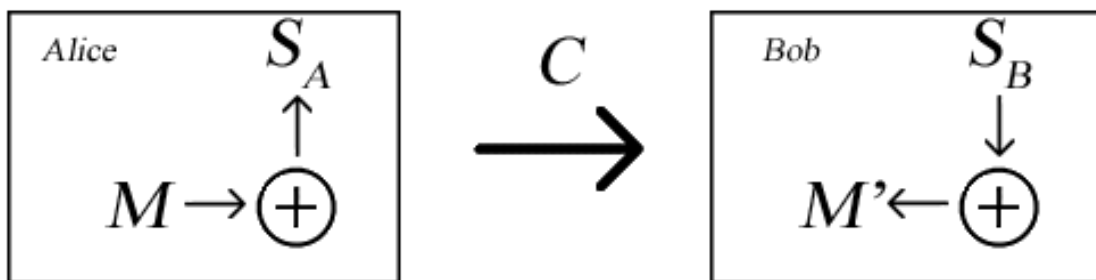


Figure 1.2 One Time Pad scheme

Every instance where we have a system with a sender and a receiver, we denote them respectively by Alice and Bob. M is the message we want to transmit, S_A and S_B are the keys that are held by both Alice and Bob. C is the cyphertext that Alice is sending. A message is generally a long string of bits.

1. Encryption: Alice encrypts the message M using her key S_A : $C = M \oplus S_A$ by performing binary addition, meaning if two different bits were added together, it would result in the bit 1. Similar bits added together yield the bit 0.
2. Transmission: Alice sends the cyphertext C to Bob over a public channel. Any eavesdropper can listen in on it and read the cyphertext.
3. Decryption: Bob receives the message and decrypts using his key S_B : $C = M' \oplus S_B$.

At the end, it is provable that the message Bob receives M' , is in fact equal to M .

$$M' = M: M'_i = (S_B)_i \oplus C_i = M_i \oplus (S_A)_i \oplus (S_B)_i = M_i$$

Say Alice wants to send a message $M: 0\ 1\ 1\ 0\ 1\ 0\ 0$ to Bob. She encrypts this using the key $S_A: 1\ 0\ 1\ 1\ 1\ 0\ 1$. This results in a cyphertext $C: 1\ 1\ 0\ 1\ 0\ 0\ 1$. Assuming Bob has the same key, performing binary addition will recover the plaintext. This protocol is information-theoretically secure because the key cannot be obtained from the cyphertext. The key is also random, the same length as the plaintext and is never reused wholly or partially. The limitation is agreeing on the key, Alice and Bob cannot just meet up and exchange it. They would need a more formal approach for exchanging keys [3].

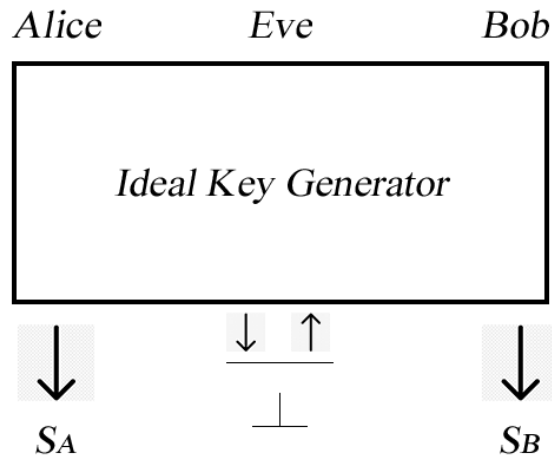


Figure 1.3 Ideal key generator scheme

An Ideal Key Generator is conceived and can output S_A for Alice and S_B for Bob, but aborts if it detects an eavesdropper Eve tampering with the process. The outputted key from the Ideal Key Generator should have:

1. Correctness: The probability that Alice and Bob's keys differ but the protocol does not is small $\Pr[S_A \neq S_B] \leq \epsilon$ where ϵ is a predetermined small constant. If the keys are very different, then the protocol should recognize and abort.
2. Close to a perfect key:
 - a. Eve does not have any knowledge of the key.
 - b. The individual key bits are uncorrelated.

How do we create keys for Alice and Bob that fulfill their requirements? It is where quantum key distribution protocols play a significant role. [4]

1.2 Polarization of photons

Encrypting bits into quantum states is the building block for any quantum key distribution protocol. We have two different bases in which we can encode and decode in. The rectilinear bases: $\leftrightarrow \updownarrow$ and the diagonal bases: $\nearrow \swarrow \searrow \nwarrow$. We can use the polarization of photons to encrypt bits into quantum states. Consider linear polarization the oscillation of the photon occurring in a one-directional plane. Given one basis, we can distinguish between the different basis states by using polarization filters.

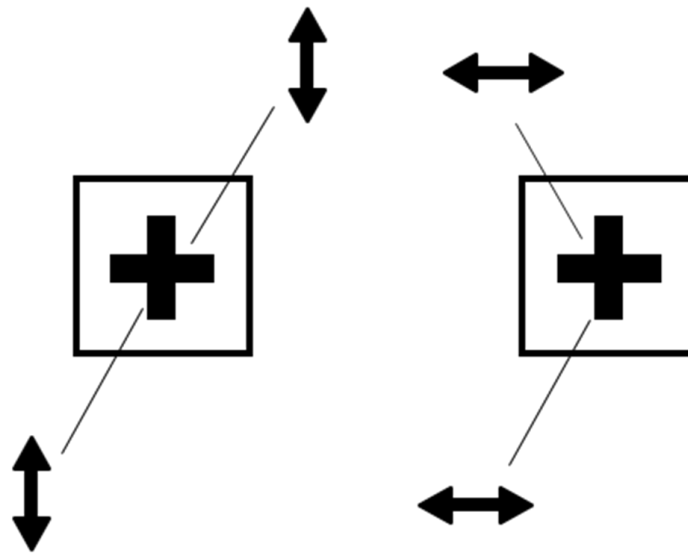


Figure 1.4 Polarization filter in the rectilinear basis

A vertically polarized photon that passes through the filter would be deflected to the right, whereas a horizontal photon would deflect to the left. If a photon encoded in the diagonal basis is sent through a rectilinear polarization filter, the state of the photon changes; therefore, the

polarization of the photon is now either horizontal or vertical in an equal probability. All the information about the previous polarization is now lost [5].

1.3 An introduction to the BB84 protocol

Based on the diagonal and rectilinear basis, we choose for the bits 0 and 1 a polarized state.

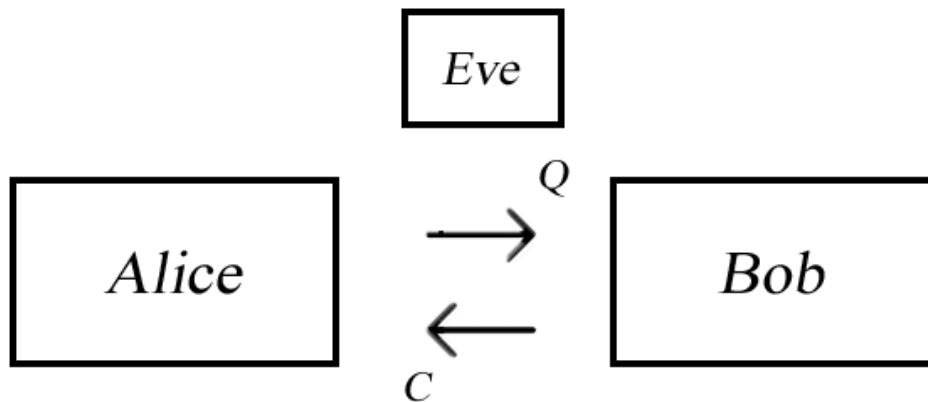


Figure 1.5 BB84 distribution protocol

Alice and Bob want to communicate and create a secret key that can be used in the one-time pad encryption scheme. Alice and Bob now have access to a quantum channel where they exchange quantum states. A classical channel is also available to send back and forth classical messages. Eve has access to the quantum channel and can manipulate the sent states. Eve can also listen in on the classical channel but cannot change the messages [6].

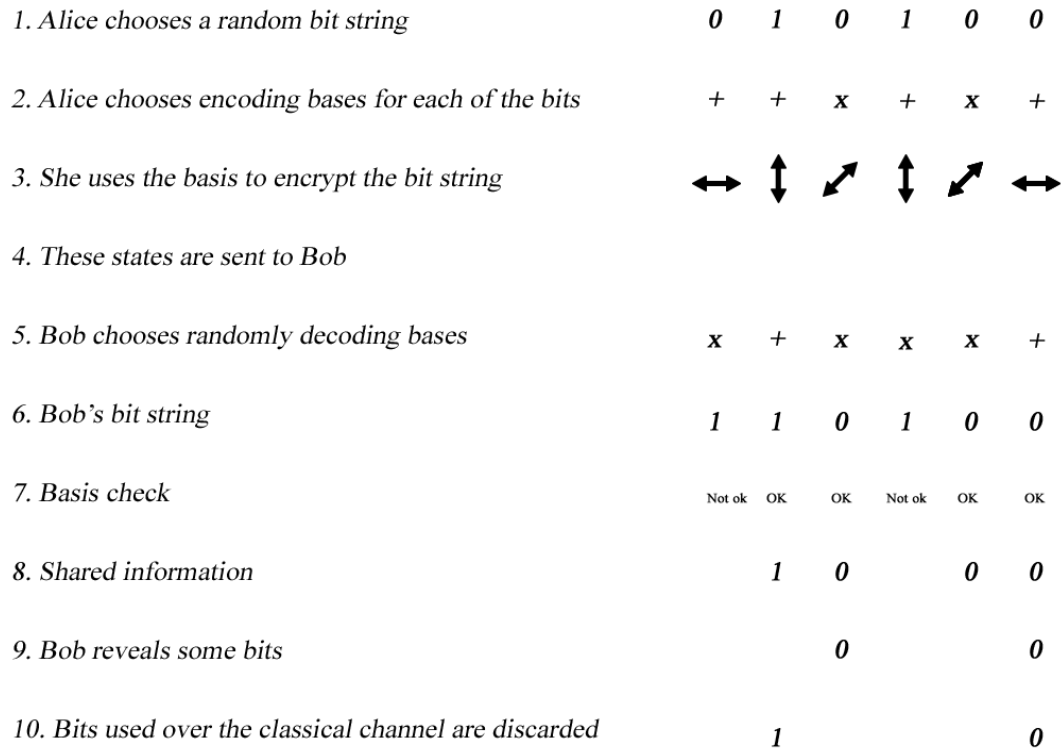


Figure 1.6 Stages of the BB84 protocol

Chapter 2: Quantum systems

2.1 Introducing quantum systems

In this section, we want to develop a mathematical description of the physical systems and processes that appear in a quantum key distribution protocol. The BB84 protocol where Alice prepares the states and sends them to Bob, then Bob measures them. A quantum key distribution protocol usually has three different steps or quantum stages.

The process stratifies into three different stages that are 1. The preparation stage involves Alice preparing the states she wants to send to Bob, 2. Channel stage: This is where Alice physically sends the states to Bob, 3. Measurement stage: Bob receives the states and derives a classical outcome x .

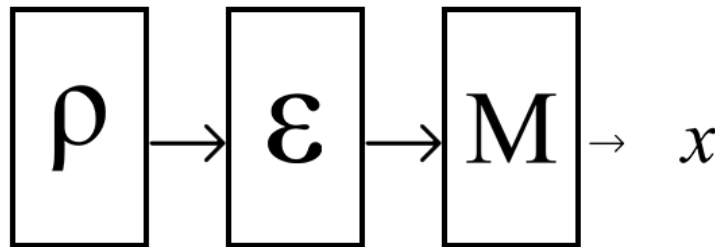


Figure 2.1 Stages of a quantum key distribution protocol

The channel stage is all the things that happen between the preparation and the measurement stage, and this includes all types of attacks that Eve can perform and all the losses and noise that might occur from a non-ideal environment. [7]

2.2 The preparation stage of a QKD

A density operator can be used to describe the preparation stage $\rho \in B(H)$. B is an operator that maps from the Hilbert space into the Hilbert space. The density operator has the following properties:

Normalized $Tr(\rho) = 1$

Hermitian $\rho^\dagger = \rho$, where the Hermitian conjugate is equal to the density operator itself.

Positive semi-definite $\langle \theta | \rho | \theta \rangle \geq 0$

A density operator is an ensemble of pure states and mixed states $\{\rho_i |\psi_i\rangle\}_{i=1, \dots, d}$. An ensemble that specifies all the distributed possible pure states with a probability distribution. For every possible pure state, a probability ρ_i is assigned. The density operator ρ sum is

$$\sum_{i=1}^d \rho_i |\psi_i\rangle\langle\psi_i|$$

Assume ρ_3 is the only state where it is a pure state or $\rho_3 = 1$ and the others are equal to 0.

$\rho_3 = 1, \rho_i = 0 \forall i \neq 3$. The density operator therefore is just $\rho_{pure} = |\psi_3\rangle\langle\psi_3|$. This equation

has a sum of one term which makes it a pure state.

A qubit, as we have already discussed, is when a polarized photon encodes into a physical system. However, mathematically we can assume that $|0\rangle$ is a horizontally polarized state and $|1\rangle$ is a vertically polarized state. A general qubit state would then be a linear combination of zero and one vectors $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with α, β being complex numbers \mathbb{C} . α, β are not however probabilities with which 0 and 1 vectors occur, but they are the probability amplitudes $|\alpha|^2 + |\beta|^2 = 1$. We can write out the basis vector 0 and 1 as $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. This is also the rectilinear basis in BB84. We can have multiple choices for the basis of the qubit state space. The Hadamard basis, unlike the computational basis, can be denoted with $|+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, $|-\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$. The Hadamard basis is an orthogonal basis for the qubit state space, or the diagonal polarization in the BB84 protocol. The preparation stage is described by a density operator. [7]

2.3 Overview of a quantum channel in a QKD

This stage includes all the things that happen after the preparation stage, or in other words, everything that happens between Alice sending the prepared states and Bob receiving them. Mathematically the quantum channel is a linear, completely positive, trace preserving map $\epsilon: \beta(H_A) \rightarrow \beta(H_B)$. It is a map that goes from the operator from the first Hilbert space H_A to the operator of the second Hilbert space H_B . A quantum channel is a linear map, meaning that $E(\alpha\rho_A + \beta\sigma_A) = \alpha E(\rho_A) + \beta E(\sigma_A)$ for $\rho_A, \sigma_A \in \beta(H_A)$, $\alpha, \beta \in \mathbb{C}$.

This equation fulfills for every choice of density operator possible for coefficients alpha and beta. If we apply the quantum channel to a state, it should be the same as applying the quantum

channel to the individual states and build a linear combination. A quantum channel is a positive map. For map $E(\rho_A)$ to be the positive semidefinite for all positive semi-definite $\rho_A \in \beta(H_A)$. For every choice of ρ_A we can make, the map applied to this state has to be a semidefinite operator.

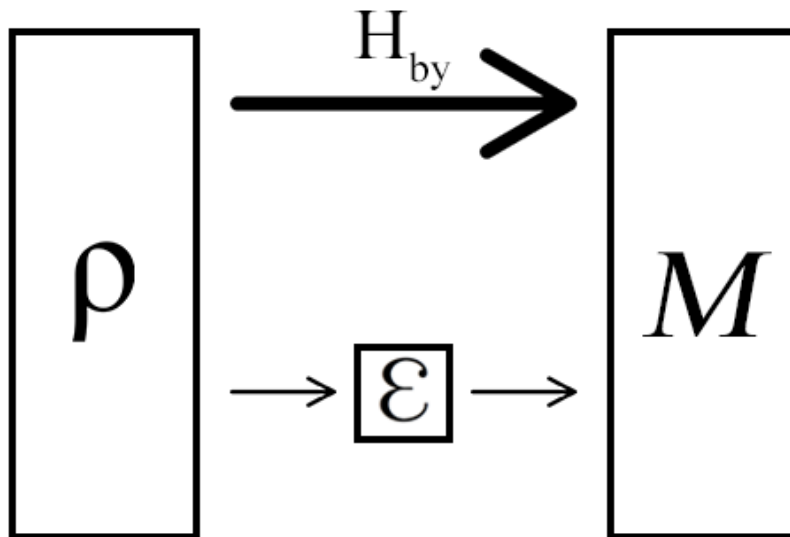


Figure 2.2 A quantum channel

Assume we have state ρ , we apply the channel ϵ at parts of ρ . Nothing is happening in the other part of the state, the sent state evolves freely without being attacked

and is a bystander. Applying the map ϵ to the H_{by} yields as a positive map, which makes the quantum channel completely positive.

$$E \otimes id_n: \beta(H_A) \otimes (C^n) \rightarrow \beta(H_A) \otimes \beta(C^n)$$

is positive for all $n \in \mathbb{N}$. The tensor product of the map E and the identity of the Hilbert space of the bystander id_n , then the tensor product map should be positive for all choices of n regardless of the size of the Hilbert space.

A quantum channel is a trace preserving and the quantum state doesn't change

$$Tr(\rho_A) = Tr(E(\rho_A)) \forall \rho_A \in \beta(H).$$

The trace of the quantum state inputted into the channel is equal to the quantum state that we got as an output, all this are true for all ρ_A within the operator of H_A .

In conclusion, a quantum state is always mapped to another quantum state through a quantum channel. A quantum state always results in a quantum state [8].

2.3.1 Conveying quantum channels with the Kraus decomposition

We can mathematically convey and write these quantum channels with the Kraus decomposition. Suppose we have a channel that is a linear, completely positive trace-preserving map as previously stated, it can always find operators such that we can write the map as a sum of these operators applied to the state we have put in. Operators k_j

are mapped from the Hilbert space H_A to H_B and at most d operators to describe the quantum channel, where d is the product of the dimensions of the Hilbert space.

Kraus decomposition for a channel $E: \beta(H_A) \rightarrow \beta(H_B): E(\rho_A) = \sum_{j=1}^d k_j \rho_A k_j^\dagger$, where

$k_j: H_A \rightarrow H_B \forall j \in \{1, \dots, d\}$ with $d \leq \dim(H_A)\dim(H_B)$ and $\sum_{j=1}^d k_j^\dagger k_j = I_A$. The

summation of all the k_j operators and k_j^\dagger together yields the identity of the Hilbert space H_A .

A Kraus decomposition for the map can always be derived if it is linearly completely positive trace preserving. If a map possesses a Kraus decomposition, then it is provable that it is a linearly positive trace preserving map [7].

2.3.2 The unary-evolution channel

One such channel is the unary evolution u . It is a closed system that has only one Kraus operator. We have one unary that we denote with U that is applied to the state to get a resulting state. [7]

$$\rho' = U\rho U^\dagger \equiv u(\rho)$$

Unitary evolutions are reversible, finding the inverse of the unitary evolution by taking the dagger of the map.

$$(u^\dagger \cdot u)(\rho) = U^\dagger U \rho U U^\dagger = \rho$$

While $U^\dagger U = I$.

2.3.3 The amplitude damping channel

An example of an open channel can be described as a two-level system. It is an atom with a ground state 0 and an excited state 1. The amplitude damping channel models the decay of the atom. If the atom is in an excited state, it goes to the decaying state with

probability of γ where $0 \leq \gamma \leq 1$. The atom will stay in its excited state with probability of $1 - \gamma$. If the atom is already in a grounded state, it will stay grounded with the probability of 1.

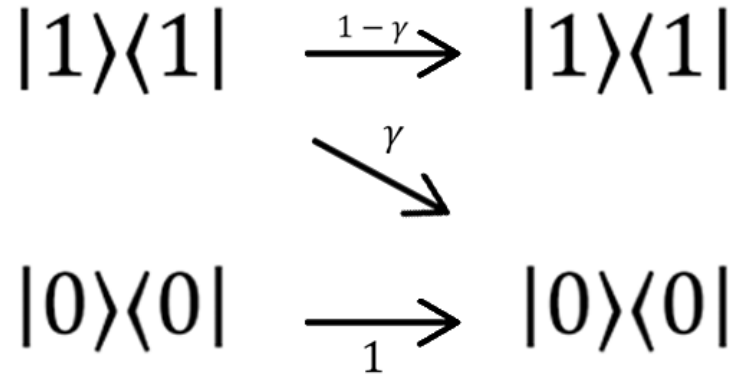


Figure 2.3 An amplitude damping channel

This type of channel has two Kraus operators:

$$k_1 = \sqrt{\gamma}|0\rangle\langle 1| \rightarrow k_1|1\rangle\langle 1|k_1^\dagger = \gamma|0\rangle\langle 0|$$

$$k_2 = |0\rangle\langle 0| + \sqrt{1-\gamma}|1\rangle\langle 1|$$

In k_1 , applying it to the excited state will yield the ground state with the factor of γ . It models the decay of the excited state to the ground state with probability γ . A second operator is needed because $k_1^\dagger k_1 \neq I$. If the sum of $k_1^\dagger k_1$ and $k_2^\dagger k_2$ is calculated, the identity $I = k_1^\dagger k_1 + k_2^\dagger k_2 = I$ can be derived. [9]

2.4 The measurement channel

This stage is where the quantum state is received and measured to deduce a classical outcome.

Measurement is described as a Positive Operator-Valued Measure. For a finite outcome set X ,

a POVM is a collection M of operators M_x that fulfill: $\forall_x \in X: M_x \geq 0, \sum_{x \in X} M_x = I$.

Probability of getting an outcome $x \in X: \rho_\rho(x) = \text{Tr}(\rho M_x)$. For a pure state $|\psi\rangle$ that

simplifies to $\langle \psi | M_x | \psi \rangle$. The expectation value of a POVM of all the outcomes, this can be

done by taking sum of all the outcomes in the outcome set multiplied by the trace of $\rho(M_x)$.

$$\sum_{x \in X} x \text{Tr}(\rho M_x). [10]$$

Chapter 3: Composite systems

3.1 Introduction to composite systems

In this section, we will be discussing composite systems mathematically. We will also look at the entanglement quantum phenomena and briefly discuss the no-cloning theorem and why we cannot clone arbitrary quantum states. As shown before, the following section describes a general quantum experiment.

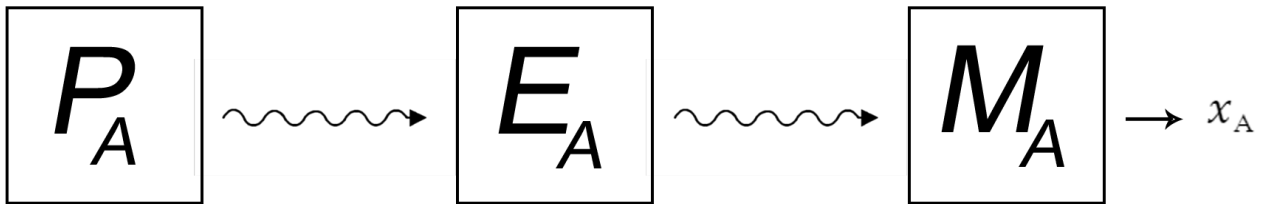


Figure 3.1 Quantum experiment A

Suppose Alice conducts this experiment. Alice prepares a quantum state P_A , sends it through a quantum channel E_A and finally measures the state with a measurement M_A to deduce a classical outcome. We can assume that Bob is doing the same by preparing quantum states P_A sending them through E_A channel and measuring the state M_A .

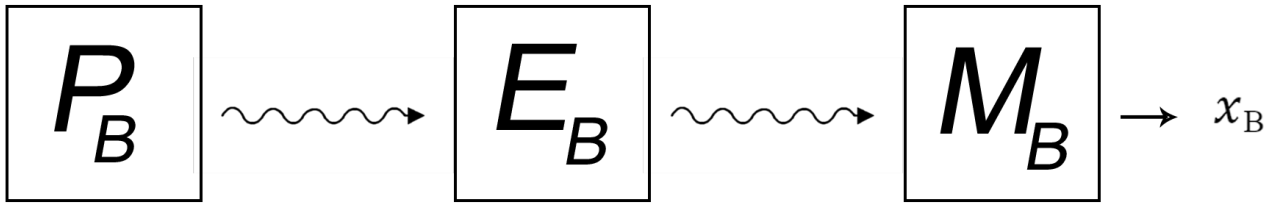


Figure 3.2 Quantum experiment B

These are two completely independent quantum experiments that do not influence each other.

We can still view this as one system where two individual quantum experiments occur. We can also describe it as tensor products of quantum states.

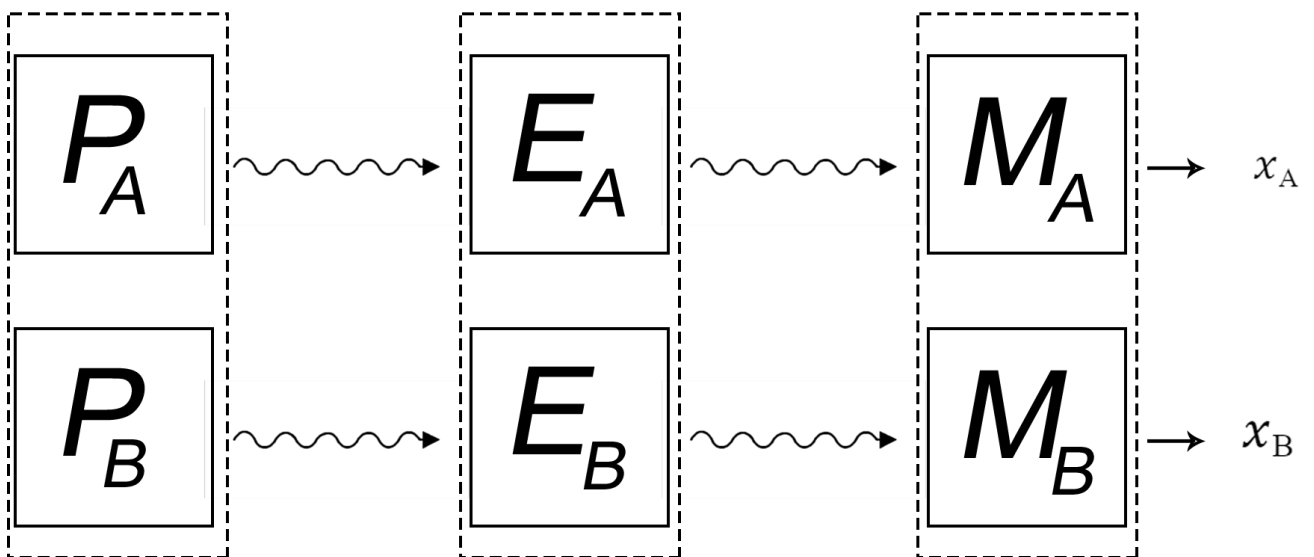


Figure 3.3 A system containing experiments A and B

The state of the composite systems is $P_A \times P_B$. The quantum channel is $E_A \times E_B$ and the measurement is the tensor product of $M_A \times M_B$. Composite system can be two different quantum experiments viewed as one. [11]

3.2 Overview of the Hilbert space

We specify an underlying Hilbert space whenever we have a quantum system. In this section, we will introduce bipartite systems, or a system with two different parties, like in the case of Alice and Bob. The Hilbert space is a tensor product of two Hilbert spaces $H_A \times H_B$. A system could be multiple parties as well, which yields a tensor product of multiple Hilbert spaces. The concepts in this section apply to multipartite Hilbert spaces unless shown otherwise. A Hilbert space is a vector space $|Z\rangle \in H$ of complex numbers C . A Hilbert space has scalar products $\langle x|y\rangle$. We can define an orthogonal basis of a Hilbert space H as a family of vectors $\{x_i\}_i$ with $\langle x_i|x_i\rangle = 1$, $\langle x_i|x_j\rangle = 0$ where $i \neq j$.

The basis of the Hilbert space is described as $H_A: \{|e_i\rangle\}$, $H_B: \{|f_i\rangle\}$.

The bases of the subsystems construct a basis of the tensor product of the Hilbert space. $H_A \times H_B: \{|e_i\rangle \times |f_j\rangle\}$. This leads directly to a formula of the dimensions of the Hilbert space $\dim(H_A \times H_B) = \dim(H_A) \dim(H_B)$. We take every combination of basis states of the tensor product. The dimension of the tensor product Hilbert space just becomes the product of the dimensions of the subsystem of Hilbert spaces. [12]

Notation:

$$|e\rangle \otimes |f\rangle = |e\rangle|f\rangle = |ef\rangle$$

$$|e\rangle_A \otimes |f\rangle_B = |e\rangle_A|f\rangle_B = |ef\rangle_{AB}$$

Mixed states:

$$\rho_A \in \beta(H_A), \rho_B \in \beta(H_B)$$

$$\rho_A \otimes \rho_B \in \beta(H_A \otimes H_B)$$

3.2.1 An example of a composite system

We can define the basis of one-qubit space: $\{|0\rangle, |1\rangle\}$ where $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

A one-qubit space has the computational basis as the only basis we can choose. If we have a system of two qubits, we can assign a computational basis to each subsystem, and the basis of composite Hilbert space is given by the tensor product of the one-qubit bases.

We describe the basis the two-qubit space as $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. We take every combination of the zeroes and ones to get the basis of the two-qubit space, resulting in a four basis states which fits perfectly with the dimension formula shown in section 3.2. We already have the vectoral presentation of the basis for the one-qubit space and now we can take the algebraic tensor product to get the presentation of the two-qubit states

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \times \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} (1)(1) \\ (0)(0) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Given the spaces, a general two-qubit state is a linear combination of these four basis states.

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \sigma|11\rangle = \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \sigma \end{pmatrix} \text{ with } |\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\sigma|^2 = 1. [13]$$

3.3 Entanglement

Assume we have a tensor product of the zero states. One state is present in Alice's system and the other in Bob's. This is a composite state, and we can safely announce that Alice's and Bob's qubit are in state zero.

$$|\phi\rangle^+ = \frac{1}{\sqrt{2}}|10\rangle_A \times |10\rangle_B + |1\rangle_A \times |1\rangle_B$$

The following quantum state is in the composite Hilbert state. It is in a super-positional state, meaning we have the tensor product of zero states in both Alice and Bob's qubits with a tensor product of one state added. This raises the uncertainty about the state of Alice's and Bob's qubit.

Entanglement is a pure bipartite state meaning $|\Psi\rangle_{AB}$ is entangled if it cannot be written as a product state $|\psi\rangle_A \times |\psi\rangle_B$ for any choice of states $|\psi\rangle_A$ and $|\psi\rangle_B$. If there are no states $|\psi\rangle_A$ and $|\psi\rangle_B$ such as the tensor products of these states give the state $|\psi\rangle$, then $|\psi\rangle$ is an entangled state. To prove if a state is a pure bipartite state and to figure out if the state is entangled, we use the Schmidt decomposition theorem. [14]

3.4 The Schmidt Decomposition

We always write a pure bipartite state $|\psi\rangle_{AB}$ as $|\psi\rangle_{AB} = \sum_{i=1}^d \lambda_i |e_i\rangle_A \times |f_i\rangle_B$ with $\lambda_i > 0$ and $\sum_i \lambda_i^2 = 1$, $d < \min\{\dim(H_A), \dim(H_B)\}$. Suppose Alice has a qubit, a two-dimensional system. Bob possesses a large system, then we can always find a subspace in Bob's system such that the Schmidt decomposition only includes the subspace of Bob's

system. The Schmidt decomposition also shows if the state is entangled when $d > 1$. If the state $|\psi\rangle$ is an entangled state, then d is always greater than one. Therefore, by taking the Schmidt decomposition and calculating the Schmidt rank, we can figure out if the state is entangled or a product state.

Going back to the previous example

$$|\phi\rangle^+ = \frac{1}{\sqrt{2}}|10\rangle_A \times |10\rangle_B + |1\rangle_A \times |1\rangle_B \Rightarrow \lambda_1 = \frac{1}{2}, \lambda_2 = \frac{1}{2}, d = 2$$

Therefore, the state $|\phi^+\rangle_{AB}$ is entangled. The Schmidt decomposition is applicable to pure bipartite states. [15]

3.5 Entanglement for mixed states

A bipartite state ρ_{AB} is called separable if and only if it can be written as:

$$\rho_{AB} = \sum_x \rho_x \sigma_A^x \otimes \eta_B^x$$

For a probability distribution ρ_x and states $\sigma_A^x \in \beta(H_A)$ and $\eta_B^x \in \beta(H_B)$. Otherwise, ρ_{AB} is called entangled. Meaning, if we could write this bipartite state as the summation, it is separable, otherwise it is entangled. [16]

3.6 Partial trace

We can conclude from the previous example that $|\phi^+\rangle_{AB}$ is an entangled state. A local density operator can calculate the state of Alice's system. Let ρ_{AB} be a bipartite density operator and $\{|e_i\rangle_B\}$ a basis for H_B is then $Tr_B(\rho_{AB}) = \sum_i (I_A \otimes \beta\langle e_i|) \rho_{AB} (I_A \otimes |e_i\rangle_B)$ or $Tr_B(\rho_{AB}) = \sum_i \beta\langle e_i| \rho_{AB} |e_i\rangle_B$. We use the partial trace to calculate the local density operator of state $|\phi^+\rangle_{AB}$.

We need a basis for Bob's system. $|\phi^+\rangle_{AB}$ is a state in a two qubits Hilbert space, we already have an understanding that the basis for the one-qubit Hilbert space is the computational basis. Therefore, we can use the computational basis to calculate the partial trace:

$$\begin{aligned}
\rho_A &= \text{Tr}_B(|\phi^+\rangle_{AB}\langle\phi^+|) \\
&= \frac{1}{2} (\langle 0|_B(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)(\langle 0|_A\langle 0| + \langle 1|_A\langle 1|)|0\rangle_B \\
&\quad + (\langle 1|_B(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)(\langle 0|_A\langle 0|_B + \langle 1|_A\langle 1|_B)|1\rangle_B) \\
&= \frac{1}{2} (|0\rangle_A\langle 0| + |1\rangle_A\langle 1|) \\
&= \Pi_A
\end{aligned}$$

We can see that there are only two terms which are non-zero. Combining the one state with the zero leads to a scalar product of 0. We get a maximally mixed state Π_A . Both basis states of the system appear with equal probability. We cannot gain information from the state because all the possible basis states are equally provable. The same calculation can be applied to Bob's system, tracing out Alice's system yields a maximally mixed state of Bob's system. This does not mean the state $|\phi^+\rangle_{AB}$ can be written as a tensor product of $\Pi_A \otimes \Pi_B$.

$$|\phi^+\rangle_{AB}\langle\phi^+| \neq \Pi_A \otimes \Pi_B$$

The local density operator for Alice and Bob describes the situation in their experiments but tracing out one part of the system leads to a complete loss of all the information. Therefore, it cannot be describing this entangled state by looking at the local density operator. [17]

3.7 Classical-quantum ensembles

One of the subsystems is a classical system with a Hilbert space $H_A \otimes H_Z$.

An ensemble: $\{\rho_\zeta, \rho_A^\zeta \otimes |\zeta\rangle_Z\langle\zeta|\}_{\zeta \in Z}$

Density operator: $\rho_{AZ} = \sum_{\zeta \in Z} \rho_\zeta \rho_A^\zeta \otimes |\zeta\rangle_Z\langle\zeta|$

The corresponding ensemble to this system is an ensemble where the states are tensor products of density matrices ρ_A with an index ζ and classical values ζ that are encoded into quantum states. These tensor product states are then distributed by a probability distribution ρ_ζ . Before, we had an ensemble of pure states, now the state ρ_A in the ensemble derives from another ensemble. Essentially, it is an ensemble of ensembles. The density operator is a sum over all the classical values. [18]

3.8 Evolution of composite systems

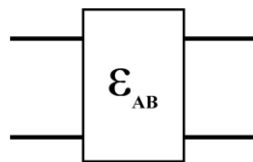


Figure 3.4 A quantum system that maps from system A to system B

Just like we defined in the previous section, a quantum channel is a linear, completely positive, trace-preserving map $\epsilon_{AB}: \beta(H_A \otimes H_B) \rightarrow \beta(H'_A \otimes H'_B)$. The only difference that the map, maps between tensor products of Hilbert spaces. The properties still held even if the Hilbert spaces are tensor products.

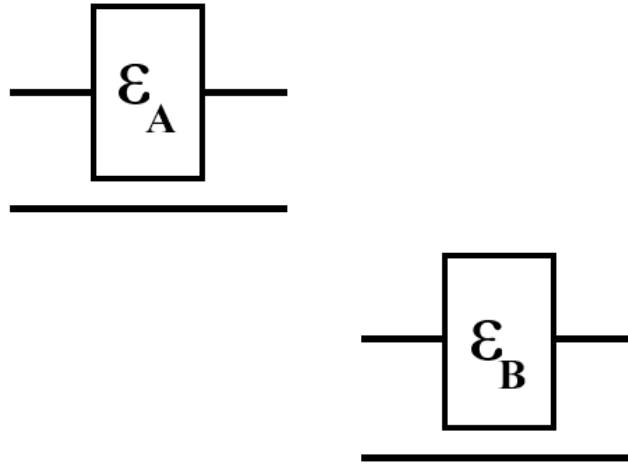


Figure 3.5 Evolution on the subsystem A and B

A particular case of the evolution of composite systems is when the evolution takes place on one subsystem and the other subsystems, the identity evolution is applied. An example of such evolution is the partial trace or the discarding channel, which means that the quantum channel on the B system is the partial trace and the evolution on the A system is the identity.

[13]

Partial trace: $\epsilon_B = Tr_B$

$$Tr_B(\rho_{AB}) = (I_A \otimes Tr_B)(\rho_{AB}) = \sum_i (I_A \otimes \langle e_i |) \rho_{AB} (I_A \otimes | e_i \rangle_B)$$

Kraus operator: $\{I_A \otimes \langle e_i |_B\}$

3.9 The no-cloning theorem

A composite system appears in the no-cloning theorem where it deals with perfectly copying unknown quantum states. Suppose we want to build a machine which is a unitary u that takes $|\psi\rangle$ pure state as an input and outputs two perfect copies of $|\psi\rangle$.

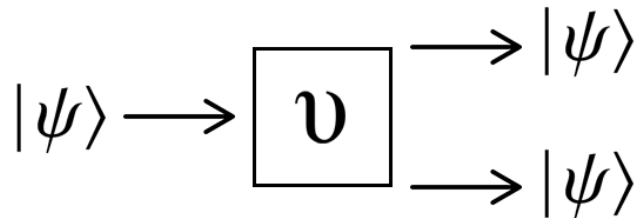


Figure 3.6 The no-cloning theorem

Fortunately for quantum key distribution protocols, building such a machine is not realistically feasible. That is because Eve could use this machine to copy the entirety of the states Alice is sending, then proceed to send one to Bob and hold on to it. Alice and Bob would not be aware of the process. This machine is not realistic due to the linear nature of quantum mechanics.

Proof.

General qubit state: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Consider a general qubit $|0\rangle$ and $|1\rangle$. Passing $|\psi\rangle$ as a parameter into the u no-cloning machine entails the following.

$$\begin{aligned}
v|\psi\rangle|0\rangle &= |\psi\rangle|\psi\rangle \\
&= (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle) \\
&= \alpha^2|0\rangle|0\rangle + \alpha\beta|0\rangle|1\rangle + \beta\alpha|1\rangle|0\rangle + \beta^2|1\rangle|1\rangle
\end{aligned}$$

We can calculate this using the linear combination given for $|\psi\rangle$.

$$\begin{aligned}
v|\psi\rangle|0\rangle &= v(\alpha|0\rangle + \beta|1\rangle)|0\rangle \\
&= \alpha v|0\rangle|0\rangle + \beta v|1\rangle|0\rangle \\
&= \alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle
\end{aligned}$$

Because v is a linear map, we can calculate the linear combination applied to the basis state $|0\rangle$ and $|1\rangle$.

$$\begin{aligned}
&\alpha^2|0\rangle|0\rangle + \alpha\beta|0\rangle|1\rangle + \beta\alpha|1\rangle|0\rangle + \beta^2|1\rangle|1\rangle \\
&\neq \alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle
\end{aligned}$$

These two expressions are not equal. However, they are equal only when $\alpha = 1, \beta = 0$ or $\alpha = 0, \beta = 1$. Meaning we can always copy classical states. [19]

Chapter 4: Prepare-and-measure Vs Entanglement

4.1 Introduction

The goal of quantum key distribution protocols is to establish a secret key between two different parties, Alice, and Bob, which is used to encrypt then and decrypt shared messages. A quantum key distribution scheme can be split into two parts: quantum transmission and classical post-processing. Quantum transmission is where quantum states are sent back and forth between the parties. Depending on the protocol, this phase might be utilized to measure quantum states or have an independent source distributing them. At the end of this phase, Alice and Bob will possess a classical bit string that is not identical but partially correlated and partially secured. The classical post-processing phase consists of Alice and Bob taking their bit strings deduced from the quantum transmission phase to form an actual key. Errors are corrected to make a more reliable and usable key for a secure line of communication. We can subdivide the quantum transmission stage into two stages: the prepare-and-measure and entanglement stage.

In prepare and measure, quantum states are prepared, sent, and then measured. Whereas entanglement schemes do not require Alice to prepare and send states to Bob, Alice and Bob possess entangled pairs of qubits. The method in which they obtain these pairs is irrelevant as it is from a friendly third-party source or a

potential aggressor. In this section, we will discuss the prepare and measure protocols and draw comparisons to the entangled protocols.

4.2 Prepare-and-measure

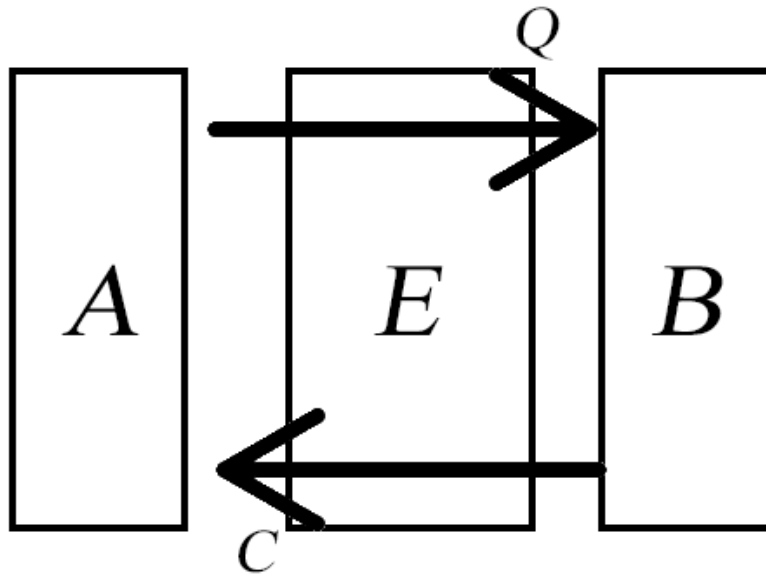


Figure 4.1 Basic structure of a Prepare-and-measure protocol

We have already discussed the BB84 protocol in the previous section, which possesses the same structure shown in the above figure. The structure is as follows; there are two parties, Alice, and Bob, which want to establish a secret key. The use of a quantum channel to allow the flow of qubits. We use a classical channel to send messages. Eve can interact with quantum states if it respects the rules of quantum mechanics. The BB84 protocol is an excellent example of a prepare and measure protocol. Introduced in 1984 by Bennet and Brassard, it begins with Alice choosing two random bit strings:

$$a = (a_1, a_2, \dots, a_n)$$

$$b = (b_1, b_2, \dots, b_n)$$

a is the key bit string and b is the basis bit: $0 = C$, $1 = H$. Both bit strings contain $4n$ bits.

String a includes the actual key. String b determines in which basis the key bit will be

encoded. If the bit is 0, the computational basis is used, whereas for the Hadamard basis the

bit is 1. These two strings are used to prepare states $|\psi_{00}\rangle_A = |0\rangle$, $|\psi_{10}\rangle_A = |1\rangle$, $|\psi_{01}\rangle_A =$

$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|\psi_{11}\rangle_A = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. If both bits are, then Alice encodes the 0 into the

computational basis, so on and so forth. The prepared states are sent to Bob, where these

states endure noise and loss from non-ideal hardware and/or acts of eavesdropping. However,

consider an ideal scenario where these errors do not occur. Bob receives the states

$E(|\psi\rangle_A \langle\psi|)$, where $|\psi\rangle_A = \sum_{i=1}^{4n} |\psi_{a_i b_i}\rangle_A \otimes |\psi_{a_{i+1} b_{i+1}}\rangle_A$. Bob proceeds to measure in order

to receive his own bit string $a' = (a'_1, a'_2, \dots, a'_{4n})$ which is the analog of Alice's string a . $b' =$

$(b'_1, b'_2, \dots, b'_{4n})$ denotes the basis Bob has chosen to measure with. Alice and Bob now both

hold two bit-strings a' and a for the key bit, and bit string b' and b where the chosen basis is

stored.

4.2.1 Sifting step in a prepare-and-measure protocol

The sifting step comes next where parties compare the basis they choose:

1. Alice declares the bit string b . Alice cannot declare her basis if Bob did not announce that he has received them. This is to deter Eve from figuring out the basis Alice has measured.

2. Bob declares the bits where it differs from Alice's bit string, $b \neq b'$ this is where Bob has chosen different basis than Alice. In this case, Bob's calculations yield a completely different result.
3. Alice and Bob discard pairs $\{a_i, a'_i\}$ for which $b_i \neq b'_i$. They discard the pairs in the key bit string where the basis bit strings differ.

At the end of the sifting process, Alice, and Bob now both possess a string a and a' of length $2n$. This is because the probability of Bob choosing the correct basis is 50%.

In the classical post-processing phase the following steps are performed:

1. Parameter estimation: The amount of information that could potentially be obtained from Eve is deduced.
2. Error correction: The generated key strings are correlated but not identical, error corrections are applied to mitigate this effect.
3. Privacy amplification: It is a decisive step to attempt to minimize Eve's knowledge on the key. The less knowledgeable Eve is, the more the key is secure.

4.2.2 Intercept and resend strategy

1. Eve obtains a total of $4n$ qubits from Alice. She must successfully guess which basis Alice has chosen.
2. Eve randomly selects the basis either in the computational or the Hadamard basis. In all $2n$ cases, Eve guesses correctly. The bits are then correlated with Alice's bits.

3. Eve transmits the prepared qubits to Bob.
4. Bob measures the qubits in his own randomly chosen basis.
5. Sifting step is applied, where Alice and Bob perform a comparison of basis and find string a and a' of length $2n$.

In the final bit strings, they get after performing the sifting step, both parties choose the same bases, but Eve's differ. In n cases, Alice and Bob chose the exact same bases. Therefore, Bob got a random outcome because Eve's result was random. In half of the cases, this means that Bob got the correct result. $n/2$ or 25% errors in the sifted keys have been detected. Such high percentage causes the protocol to be aborted.

| | | | | | | | | | | |
|----------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|
| Key bit a | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 |
| Alice basis b | C | C | H | C | C | H | H | C | H | H |
| Alice's state | $ \psi_{00}\rangle$ | $ \psi_{10}\rangle$ | $ \psi_{11}\rangle$ | $ \psi_{10}\rangle$ | $ \psi_{00}\rangle$ | $ \psi_{01}\rangle$ | $ \psi_{11}\rangle$ | $ \psi_{10}\rangle$ | $ \psi_{11}\rangle$ | $ \psi_{01}\rangle$ |
| Eve's basis | H | C | C | H | C | H | C | H | C | H |
| Eve's state | $ \psi_{10}\rangle$ | $ \psi_{10}\rangle$ | $ \psi_{11}\rangle$ | $ \psi_{01}\rangle$ | $ \psi_{00}\rangle$ | $ \psi_{01}\rangle$ | $ \psi_{10}\rangle$ | $ \psi_{11}\rangle$ | $ \psi_{10}\rangle$ | $ \psi_{01}\rangle$ |
| Bob's basis | H | C | H | H | C | C | H | C | H | C |
| Bob's result | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 |
| Sifting step | ✗ | ✓ | ✓ | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ | ✗ |
| Key bit | | 1 | 0 | | 0 | | 1 | 1 | 0 | |
| Parameter estimation | | | ✗ | | | | ✓ | ✓ | | |

Figure 4.2 A detailed overview of the steps in the BB84 protocol

Alice and Bob calculate the estimate in which Eve has produced. They can conclude that in $1/3$ of the cases Eve had introduced an error. The protocol is thus aborted. [21]

4.3 The six-state protocol

The six-state protocol is like the BB84 protocol in all the steps except for one main difference. The BB84 protocol uses the computational and the Hadamard basis, while the six-state introduces the third basis y . The states are:

$$|\psi_{y^+}\rangle = \frac{1}{2} \begin{pmatrix} 1 \\ i \end{pmatrix}$$

$$|\psi_{y^-}\rangle = \frac{1}{2} \begin{pmatrix} 1 \\ -i \end{pmatrix}$$

The massive advantage of the six-state protocol over the BB84 protocol is that it has more possibilities for the state. In the BB84, the computational and Hadamard measurements span a plane in the Bloch sphere, while a third added state spans the entirety of the Bloch sphere, yielding more possibilities for states.

In the sifting step, parties must discard more bits because the probability that Bob has chosen the wrong basis is $2/3$, instead of the $1/2$ in the BB84. Eve would have less knowledge about which basis she should use to measure the state in. This introduces more errors into Alice's and Bob's key bit during the error estimation step. This security analysis of both protocols shows that the six-state protocol lets us generate a higher secret key rate. [21]

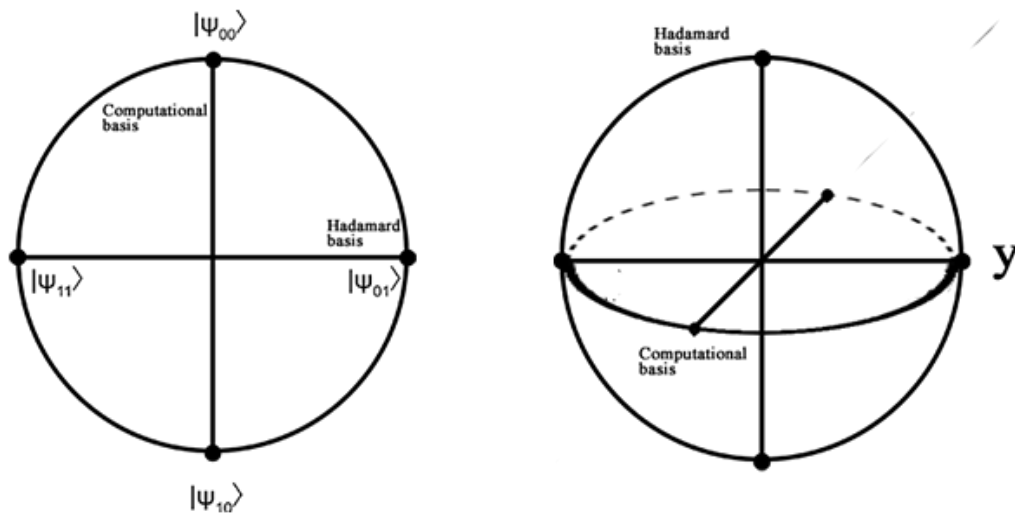


Figure 4.3 A quantum system that maps from system A to system B

4.4 The SARG04 protocol

The SARG04 protocol is specifically tailored to be secure against a specific attack, the Photon Number Splitting attack or PNS. The PNS attack targets the implementation part of the protocol. An ideal single-photon source is needed in the polarization of photons where the states are being prepared.

These ideal single-photon sources do not exist. In experimentation, a weak laser pulse is generally used to encode qubits. A certain percentage of the weak laser pulsations do not always contain photons; ideally, one weak laser pulse should contain only one single photon.

In certain instances, a pulse might contain two or more photons. [22]

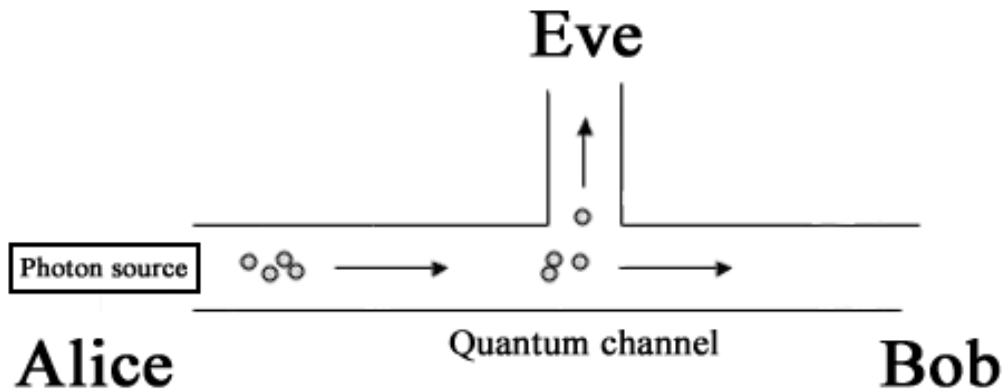


Figure 4.4 A basic PNS attack on a protocol

In figure 4.4, Eve performs an attack to eavesdrop on the quantum channel. Since the pulse contains more than one photon, then the key-bit is shared between them. Eve can simply store one of these photons in her quantum memory. In this case, Bob still receives part of the photons initially sent and announces that he had received them without recognizing that Eve had performed an attack. This is dangerous because when Alice announces her basis for encoding, Eve now can use the correct one to measure her stored photon and calculate a perfectly correlated bit value. In all the cases where a pulse contains more than one photon, Eve can gain perfect knowledge about the key. It is difficult for Alice and Bob to detect invasive attacks of that magnitude because no error had been introduced in the measured and sent photons. The SARG04 protocol is advantageous for mitigating this attack type but weak against other types of attacks. The protocol has a different sifting process than the BB84 and the six-state protocol. The sifting process in the SARG04 protocol:

1. Alice's state is $|\psi_{00}\rangle$.

2. After Bob measures the state received, he announces the pair $\{|\psi_{00}\rangle, |\psi_{01}\rangle\}$. It is crucial that one of the states present in the pair is the actual state Alice sent, and the other one is a state of the other basis. Alice notes 0 as the secret key bit, 0 being the state she has prepared in the computational and sent. The secret key bit determined by the bases she has used for the encoding.
3. Bob deduces his measurement and decides whether the bit is valid or invalid. It is valid if Bob can differentiate between the two candidate states.
 - a. Suppose Bob has chosen the computational basis. He gets $|\psi_{00}\rangle$. However, this result is also possible if the transmitted state had been $|\psi_{01}\rangle$. That is because Alice could have sent the state $|\psi_{01}\rangle$ and Bob would have measured in the computational basis, yielding an equal probability of receiving the state $|\psi_{00}\rangle$ or the state $|\psi_{10}\rangle$, both candidate states. Therefore, it cannot be concluded which state Alice has sent, invalidating the bit.
 - b. Suppose Bob had chosen the Hadamard basis to measure the bit with. In this case, Bob would get a random result $|\psi_{01}\rangle$ or $|\psi_{11}\rangle$. If the outcome is $|\psi_{01}\rangle$, the bit is rendered invalid because it is consistent with both candidate states. If the state Alice had sent was $|\psi_{01}\rangle$ then this state would have been the outcome of Bob's measurement in the Hadamard basis. If Bob's outcome is $|\psi_{11}\rangle$, then the bit is valid because this can only occur if the state Alice has sent is $|\psi_{00}\rangle$. In the other case, if Alice sent $|\psi_{01}\rangle$ and Bob measures in the Hadamard basis then the only possible result is $|\psi_{01}\rangle$. From the outcome $|\psi_{11}\rangle$, Bob knows Alice must have sent state $|\psi_{00}\rangle$ and the secret key bit is 0.

The sifting process is much more complex than in the BB84 protocol. Alice and Bob must discard more qubits because, in SARG04, more bits would be invalid. The advantage is that Alice never has to announce the basis used for the encoding. This can aid in the Photon Number Splitting, as Eve stored photon could never conclude on which basis it has to measure. [23]

4.5 Entanglement-based protocols

A quantum key distribution is divided into a quantum transmission phase and a classical post-processing phase. A quantum transmission can occur either through a prepare and measure protocol or an entanglement-based one.

The idea of an entanglement-based protocol, as opposed to a prepare and measure protocol, is to have access to a source that distributes quantum states to Alice and Bob; it can belong to a friendly third-party provider Charlie. It can also be controlled by Eve directly; this is the worst-case scenario that is assumed in every eavesdropping scenario, just like in the prepare and measure protocols where Eve is assumed to listen in on the communication. [24]

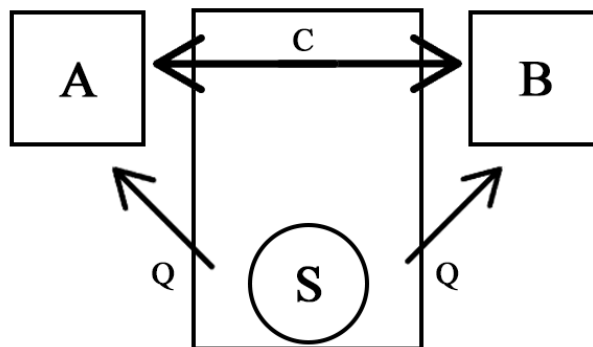


Figure 4.5 General scheme of an entanglement-based protocol

4.6 The Ekert protocol

It was created by Arthur Ekert in 1991 and utilized maximally entangled states to generate keys. The source distributes maximally entangled states to Alice and Bob. If Alice and Bob prove that the states are indeed maximally entangled, they can prove that Eve has no information on the state.

$$|\psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle_{AB} + |10\rangle_{AB})$$

Due to the monogamy of entanglement, if two parties share maximally entangled states, a third party cannot have entanglement with the same state. The shape of the system shared across Alice, Bob and Eve always follows a dynamic where Alice and Bob share a maximally entangled state, and Eve possesses a product state with both. Eve tampering with the state results in a non-maximally entangled state. The problem thus falls upon detecting the percentage of Eve's interaction with the state [24]

4.6.1 Measurement operations

We specify the measurement operation Alice can perform:

$$A_1 = Z$$

$$A_2 = X$$

$$A_3 = \frac{1}{\sqrt{2}}(Z + X)$$

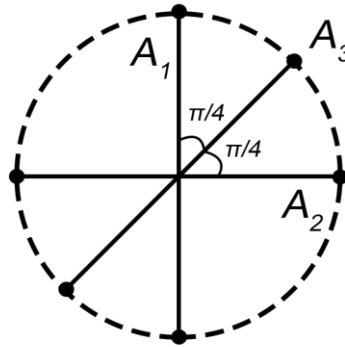


Figure 4.6 Bloch sphere of Alice's measurement operations

The operations that Bob can perform:

$$B_1 = Z$$

$$B_2 = \frac{1}{\sqrt{2}}(Z - X)$$

$$B_3 = \frac{1}{\sqrt{2}}(Z + X)$$

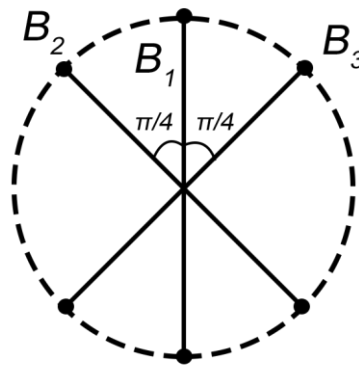


Figure 4.7 Bloch sphere of Bob's measurement operations

Note that $A_1 = B_1 = Z$, $A_3 = B_3 = \frac{1}{\sqrt{2}}(Z + X)$. Using these pairs of measurements generates a key (A_1, B_3) , (A_1, B_2) , (A_2, B_3) , (A_2, B_2) . [24]

4.6.2 The CHSH inequality in the classical case

The inequality can be derived for classical random variables: A_1, A_2, B_3, B_2 . These notations are used for the measurement direction, however, assume they are classical random variables now. All these random variables can take realizations $+1, -1$ with equal probability:

$$A_1(B_3 + B_2) + A_2(B_3 - B_2) = \pm 2$$

By calculating the above term, the answer yields -2 or $+2$. We can take the expectation value and absolute value; the statement would always be less or equal to 2. Since the expectation value is a linear operation, we can put it amongst products of itself:

$$S := |\langle A_1 B_3 \rangle + \langle A_1 B_2 \rangle + \langle A_2 B_3 \rangle - \langle A_2 B_2 \rangle| \leq 2$$

The expectation value in the case where the realizations are all equally probable is defined by

$$A_i^v = \text{realizations of r.v } A_i. \langle A_i B_j \rangle = \frac{1}{N} \sum_v A_i^v B_j^v.$$

At the end, the resulting inequality S is the CHSH inequality, where it is always less or equal to 2 in the classical case. [26]

4.6.3 Steps of the Ekert protocol

1. Alice and Bob distribute several $|\psi^-\rangle_{AB}$ states between them. Alice and Bob might be the distributors, or this job could be given to a friendly third party. We assume this role is given to Eve as a worst-case scenario analysis.

2. Foreach state, Alice and Bob randomly choose a measurement from the sets $\{A_i\}$ and $\{B_i\}$.
3. Alice and Bob announce the base they chose foreach of the measurements. The result of the pairs (A_1, B_1) and (A_3, B_3) form the sifted key. The key is sifted, because in the prepare and measure protocols, where Alice announces the basis and Bob compares it to his basis choice, the bits are discarded where they chose different basis states, they use the results with the same basis for the sifted key, but they don't discard the other results and use them for testing.
4. The results for the pair (A_1, B_3) , (A_1, B_2) , (A_2, B_3) , and (A_2, B_2) are used to check the CHSH inequality.
5. If the results of the S value are higher than 2, Alice and Bob continue to perform error corrections and privacy amplification, with the of turning the partially correlated bit string into a secure key that can be used in cryptography. [25]

4.7 Entanglement-based BB84 protocol

The idea of the entanglement based BB84 protocol is closely like the prepare and measure

BB84. Alice and Bob want to distribute several maximally entangled states between them so

it can be used for key generation between them. In this case, they want to distribute m pairs of

$|\phi^+\rangle$ states defined by:

$$|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$$

Because, if they are certain they have the state, which is maximally entangled, they can simply measure it and choose the result for the key generation. The difficult is the distribution of these perfectly maximally entangle states. A quantum error correction code, Calderbank-Shor-Steane code, is used for error correction. We will not get into the details of the code but assume have access to two classical error correction codes C_1 and C_2 that can both correct t errors. Both C_1 and C_2 are used to construct a quantum error correction code that encodes m qubits into n qubits and that can correct up to t errors.

Steps for the entanglement based BB84 protocol:

First, we define the Hadamard transformation:

$$H: |0\rangle \rightarrow |+\rangle$$

$$H: |1\rangle \rightarrow |-\rangle$$

$$H: |+\rangle \rightarrow |0\rangle$$

$$H: |-\rangle \rightarrow |1\rangle$$

1. Alice creates $2n$ qubit pairs, where each qubit is in the $|\phi^+\rangle^{\otimes 2n}$ state.
2. Alice randomly selects n qubits that will later be used to estimate the errors in the qubit pairs. This is to gauge the damage done to the $|\phi^+\rangle$ state.
3. Alice selects a random classical bit string b of length $2n$. If the b_i is 1, she applies the Hadamard transformation to her half of the corresponding qubit pair. A Hadamard transformation maps between the computational basis and the Hadamard basis and vice versa.
4. She then sends the other half of all qubit pairs to Bob.

5. Alice announces the string b , which stores which qubit she has applied the Hadamard transformation to, and she also announces the positions of the check qubits.
6. Bob proceeds to apply a Hadamard transformation to those qubits for which the corresponding bit value is 1, $b_i = 1$. This procedure of applying Hadamard transformation is equal to preparing a qubit in the Hadamard basis on Bob's side and then measuring it in the Hadamard basis.
7. Alice and Bob measure the checked qubits in the computational basis $\{|0\rangle, |1\rangle\}$ to estimate the error rate. If more than t errors occur, they abort the protocol. Remember that the quantum error correction code they have used can correct up to t errors in qubits. Therefore, if the checked qubits have more errors, then it is very likely that in the qubits used for key generation has more than t errors. Even if the checked qubits have less than t errors, it is possible that there a more than t errors in the key qubits, and then the quantum error correction procedure fails. However, this scenario is highly improbable.
8. If the number of errors is below t , Alice and Bob use the CSS code built from the error correction codes C_1 and C_2 to correct the errors in the n remaining bits and obtain m copies of $|\phi^+\rangle$ defined by $|\phi^+\rangle^{\otimes m}$. The CSS was able to encode m qubits into n qubits while correcting t errors, so Alice and Bob end up with m of the $|\phi^+\rangle$ state.
9. Since they are now sure that they share a maximally entangled state, they can measure the state $|\phi^+\rangle^{\otimes m}$ in the computational basis to obtain the shared secret key.

4.8 Connection between prepare and measure protocols and entanglement-based protocols

This section's objective is to show that an entangled-based protocol can replicate the statistics we have in a prepare and measure protocol.

Prepare and measure:

1. Remember that in a prepare and measure protocol, Alice randomly chooses bit sequence x_1, \dots, x_n where these bits are a realization of a classical random variable X with some probability distribution $p_X(x)$.
2. Alice encodes them into quantum states $|\phi_{x_1}\rangle, \dots, |\phi_{x_n}\rangle$ and sends them to Bob.
3. Bob's role in the prepare and measure protocol is to receive and measure the states sent from Alice.

However, there is an alternative way to get the same result from an entanglement-based protocol:

1. Alice begins by preparing the bipartite entangled state $|\Phi\rangle_{AB} = \sum_x \sqrt{p_x(x)} |x\rangle_A \otimes |\phi_x\rangle_B$ where $\{|x\rangle_A\}$ is an orthonormal basis for Alice's system.
2. Alice sends the second half of the state to Bob.
3. Alice measures the state she kept with respect to the basis $\{|x\rangle_A\}$.

We want to show that this entangled procedure yields similar statistics as the prepare-and-measure protocol.

Proof:

From Alice's side the probability of obtaining outcome y . In the prepare and measure protocol this is given by $p_x(y)$, the probability distribution of the classical random variable.

In the entangled based version, we can also calculate this probability

$$P(y) = \Phi(|y\rangle\langle y| \otimes I)|\Phi\rangle$$

$$= \sum_{x,x'} \sqrt{p_x(x)} \sqrt{p_x(x')} \langle x|y\rangle \langle y|x'\rangle \langle \phi_x|\phi_{x'}\rangle = p_x(y)$$

If we put in the calculation of the phi state, we get the square root of probabilities and two data functions

$$\langle x|y\rangle \equiv \sigma_{x,y}$$

$$\langle y|x'\rangle \equiv \sigma_{y,x'}$$

Resulting at the end, in the probability of y , which is the same in the prepare-and-measure protocol.

From Bob's side, it is interesting in which state he receives it if Alice's bit is y . In the prepare-and-measure protocol it is defined by $|\phi_y\rangle$. In the entangled-based protocol we can calculate the state

$$\frac{(|y\rangle\langle y| \otimes I)|\Phi\rangle}{\sqrt{P(y)}}$$

We apply the measurement to phi and normalize it with a square root of the probability of y .

If we plug in the definition of phi, we get the following:

$$\frac{(|y\rangle\langle y| \otimes I)|\Phi\rangle}{\sqrt{P(y)}} = \frac{1}{\sqrt{P_X(y)}} \sum_x \sqrt{P_X(x)} |y\rangle\langle y|x\rangle \otimes |\phi_x\rangle =$$

$$\frac{1}{\sqrt{P_X(y)}} \sqrt{P_X(y)} |y\rangle \otimes |\phi_y\rangle = |y\rangle \otimes |\phi_y\rangle$$

In the end, we take the state y on Alice's side and apply it as a tensor to the state $|\phi_y\rangle$ from Bob's side. Alice has obtained the state outcome y and Bob gets the state $|\phi_y\rangle$, which is like the prepare-and-measure protocol.

4.9 Conclusion

To conclude, we can obtain similar statistics either with a prepare-and-measure or an entangled-based one. However, it is never that easy in practice since it is not a trivial task for Alice to create a quantum state described earlier. We also have the error introduced, such as noise in the channel when she distributes the state to Bob. We can mathematically achieve the same statistics in both descriptions.

Bibliography

- [1] Mohammed, Abdalbasit & Varol, Nurhayat. (2019). A Review Paper on Cryptography. 1-6. [10.1109/ISDFS.2019.8757514](https://doi.org/10.1109/ISDFS.2019.8757514).
- [2] Luciano, D., & Prichett, G.D. (1987). Cryptology: From Caesar Ciphers to Public-key Cryptosystems. *College Mathematics Journal*, 18, 2-17.
- [3] Singh, B., Athithan, G., & Pillai, R. (2021). On extensions of the one-time-pad. *IACR Cryptol. ePrint Arch.*, 2021, 298.
- [4] Key generator. (n.d.). *SpringerReference*. https://doi.org/10.1007/springerreference_17200
- [5] Baym, G. (2018). Photon polarization. *Lectures on Quantum Mechanics*, 1–37. <https://doi.org/10.1201/9780429499265-1>
- [6] Bennett, C. H., & Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560, 7–11. <https://doi.org/10.1016/j.tcs.2014.05.025>
- [7] Cholevo, A. S. (2019). Quantum systems, channels, information a mathematical introduction. De Gruyter.
- [8] State Evolution and trace-preserving completely positive maps. (n.d.). *Quantum Information*, 117–143. https://doi.org/10.1007/3-540-30266-2_6
- [9] Khatri, S., Sharma, K., & Wilde, M. M. (2020). Information-theoretic aspects of the generalized amplitude-damping channel. *Physical Review A*, 102(1). <https://doi.org/10.1103/physreva.102.012401>
- [10] Wilde, M. M. (2013). Quantum Entropy Inequalities. In *Quantum Information theory*. essay, Cambridge University Press.
- [11] Composite systems. (n.d.). *Entangled Systems*, 115–142. <https://doi.org/10.1002/9783527619153.ch7>
- [12] Cohen, D. W. (1989). An introduction to hilbert space and Quantum logic. *Problem Books in Mathematics*. <https://doi.org/10.1007/978-1-4613-8841-8>
- [13] Wilde, M. (2017). Evolution of Composite Systems. In *Quantum Information theory*. essay, Cambridge University Press.
- [14] Barnett, S. M. (2017). Introduction to quantum information. *Oxford Scholarship Online*. <https://doi.org/10.1093/oso/9780198768609.003.0001>
- [15] The density operator, entangled states, the Schmidt decomposition, and the von neumann entropy. (2004). *Introductory Quantum Optics*, 294–303. <https://doi.org/10.1017/cbo9780511791239.012>

- [16] Al-Qasimi, A., & Eberly, J. H. (2018). Polarization and entanglement in mixed classical states. *Frontiers in Optics / Laser Science*. <https://doi.org/10.1364/fio.2018.jw4a.38>
- [17] Trace and partial trace. (2018). *Problems and Solutions in Quantum Computing and Quantum Information*, 461–468. https://doi.org/10.1142/9789813238411_0021
- [18] The classical ensembles. (2022). *Classical and Quantum Statistical Physics*, 17–39. <https://doi.org/10.1017/9781108952002.005>
- [19] The classical ensembles. (2022). *Classical and Quantum Statistical Physics*, 17–39. <https://doi.org/10.1017/9781108952002.005>
- [20] Bae, J. (2020). Measurement protection in prepare-and-measure quantum key distribution. *Quantum Communications and Quantum Imaging XVIII*. <https://doi.org/10.1117/12.2566250>
- [21] Senekane, M., Mafu, M., & Petruccione, F. (2015). Six-state symmetric quantum key distribution protocol. *Journal of Quantum Information Science*, 05(02), 33–40. <https://doi.org/10.4236/jqis.2015.52005>
- [22] Kronberg, D. A., & Molotkov, S. N. (2009). Robustness of quantum cryptography: Sarg04 key-distribution protocol. *Laser Physics*, 19(4), 884–893. <https://doi.org/10.1134/s1054660x09040495>
- [23] Gaidash, A. A., Egorov, V. I., & Gleim, A. V. (2016). Revealing of photon-number splitting attack on quantum key distribution system by photon-number resolving devices. *Journal of Physics: Conference Series*, 735, 012072. <https://doi.org/10.1088/1742-6596/735/1/012072>
- [24] Braunstein, S. L., & Pati, A. K. (2003). Introduction to entanglement-based protocols. *Quantum Information with Continuous Variables*, 59–66. https://doi.org/10.1007/978-94-015-1258-9_7
- [25] Quantum key distribution, 1984; Bennett, Brassard 1991; Ekert. (n.d.). *SpringerReference*. https://doi.org/10.1007/springerreference_57835
- [26] Khrennikov, A. (2012). Quantum probabilities and violation of CHSH-inequality from classical random signals and threshold type detection scheme. *Progress of Theoretical Physics*, 128(1), 31–58. <https://doi.org/10.1143/ptp.128.31>
- [27] Sharma, A., Ojha, V., & Lenka, S. K. (2010). Security of entanglement based version of BB84 protocol for Quantum Cryptography. *2010 3rd International Conference on Computer Science and Information Technology*. <https://doi.org/10.1109/iccsit.2010.5564133>