SECURITY OF QUANTUM KEY RECYCLING

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

KAAN AKYÜZ

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
PHYSICS

SEPTEMBER 1, 2022

Approval of the thesis:

SECURITY OF QUANTUM KEY RECYCLING

submitted by **KAAN AKYÜZ** in partial fulfillment of the requirements for the degree of **Master of Science in Physics Department, Middle East Technical University** by,

Prof. Dr. Halil Kalıpçılar
Dean, Graduate School of **Natural and Applied Sciences** _____

Prof. Dr. Seçkin Kürkcüoğlu
Head of Department, **Physics** _____

Prof. Dr. Sadi Turgut
Supervisor, **Physics, METU** _____

Examining Committee Members:

Assoc. Prof. Dr. Yusuf İpekoğlu
Physics, METU _____

Prof. Dr. Sadi Turgut
Physics, METU _____

Assist. Prof. Dr. Kıvanç Uyanık
Physics, Gazi University _____

Date: 01.09.2022

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Surname: Kaan Akyüz

Signature :

ABSTRACT

SECURITY OF QUANTUM KEY RECYCLING

Akyüz, Kaan
M.S., Department of Physics
Supervisor: Prof. Dr. Sadi Turgut

September 1, 2022, 56 pages

In cryptography, unconditional security is achieved by hiding the message under a sufficiently long one-time pad, a key that is completely unknown from outside. The one-time pad is single-use-only, because the presence of an eavesdropper is undetectable in a classical channel. In contrast, an adversary is highly detectable in a quantum channel. Quantum key recycling's objective is to detect the adversary and re-use the one-time pad. The analysis of quantum key recycling is mainly concerned with the rate and the security of the transmission. By using a method called "smoothing", tight bounds on these quantities can be established. Smoothing was used in a noise tolerant quantum key recycling scheme; however, only for the asymptotic case. This thesis' primary focus is to establish more favorable bounds on the rate and security for the non-asymptotic case by using the smoothing method.

Keywords: information theory, quantum cryptography, quantum key recycling

ÖZ

KUANTUM ANAHTAR GERİ DÖNÜŞÜMÜNÜN GÜVENLİĞİ

Akyüz, Kaan
Yüksek Lisans, Fizik Bölümü
Tez Yöneticisi: Prof. Dr. Sadi Turgut

Eylül 1, 2022 , 56 sayfa

Kriptografide koşulsuz güvenlik, yeterince uzun, saklı bir "tek kullanımlık şifre" kullanılarak elde edilir. Bu şifre tek kullanımlıktır, çünkü klasik bir kanalda gizlice dinleyen birinin varlığının tespit edilememektedir. Tersine, gizli dinleyici bir kuantum kanalda tespit edilebilmektedir. Bir kuantum anahtar geri dönüşümü protokolünün amacı, gizli dinleyicinin varlığını tespit etmek ve "tek kullanımlık şifrenin" tekrar kullanılmasını sağlamaktır. Protokolün incelenmesi temel olarak iletim hızı ve güvenliği ile ilgilidir. "Smoothing" adında bir method kullanarak, iletim hızı ve güvenliği nicelikleri üzerinde sıkı sınırlar tespit etmek mümkündür. "Smoothing" daha önce bir (gürültülü) kuantum anahtar geri dönüşümü için kullanıldı; ancak sadece asimtotik durum için. Bu tezin öncelikli amacı "smoothing" methodunu kullanarak, asimtotik olmayan durumda hız ve güvenlik üzerinde daha sıkı sınırlar tespit etmektir.

Anahtar Kelimeler: bilgi teorisi, kuantum kriptografi, kuantum anahtar geri dönüşümü

ACKNOWLEDGMENTS

I would like to express my gratitude to my primary advisor Dr. Sadi Turgut for sharing his time and wisdom, and for guiding me throughout my thesis research.

I am also very grateful to Dr.Boris Škorić, for kindly and generously sharing his time, his insights, and his guidance.

Last but not least, I want to thank my family and friends for their seemingly endless support and love.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

$\mathcal{H}$	Hilbert space.
$\mathcal{S}(\mathcal{H})$	Space of density operators on $\mathcal{H}$.
$\mathcal{C}(\mathcal{S}(\mathcal{H}^A), \mathcal{S}(\mathcal{H}^B))$	Space of completely positive and trace-preserving maps from $\mathcal{S}(\mathcal{H}^A)$ to $\mathcal{S}(\mathcal{H}^B)$.
$\log$	Logarithm base 2.

CHAPTER 1

INTRODUCTION

Communication is the exchange of information, and is often intended to be private. The study of private (or secure) communication, cryptography, has a long history which dates back to the ancient Egypt, 1900 BC [1]. Contemporary "classical cryptography" studies the security of digital information in two main branches, symmetric key cryptography and public key cryptography. Symmetric key cryptography requires the use of a pre-shared "secret key". Public key cryptography does not require a pre-shared key, but it relies on the assumptions of computational hardness. To illustrate their general scheme, one example will be given for each, starting from the symmetric key cryptography. Let Alice wants to send a private message to her friend Bob. She first puts her message in a box, locks it using her key, and sends the box to Bob. After receiving the box, Bob uses his key to unlock the box and read the contents of the message. If Alice's and Bob's keys are identical, and the information to make this key is hidden from the outside world, then Alice and Bob use symmetric-key cryptography. In public key cryptography, Bob offers a public key, a key that will lock his lock. But that is an asymmetric key that only locks, it cannot open. Alice puts her message in a box and locks the box with Bob's public key and sends it to Bob. Bob takes the box and opens it with his private opening key. In a nutshell, anyone who wishes to send Bob a private message can use Bob's public key, which can only be opened by Bob's private key after it is locked. The important thing is that, in principle, Bob's opening key can be produced by an investigation of the locking key. However, this operation is very infeasible, and that ensures its safety

In classical computers and communication channels, the information is binary, and represented in binary strings. Hence, the messages and the keys are also represented

in binary strings. Encryption, refers to the mapping of a plaintext (message) to a ciphertext (encrypted message). Decryption, refers to the mapping of the ciphertext back to the plaintext. In both, mapping is done by a key. In symmetric-key cryptography the key which encrypts the message is same with the key which decrypts it, whereas in public-key cryptography, they are not. The security in symmetric-key cryptography depends on the amount of "secrecy" on the secret key, which refers to the amount of information content that is hidden from the outside. Using a secret key consumes its secrecy so it can only be used as a one-time pad once. Also, these keys cannot be used to distribute more keys for the same reason. So, if the parties are interested in "unconditional" security, they should physically meet and share keys or thrust a courier for the delivery. The security in public-key cryptography is conditional, it depends on the hardness of computing Bob's private key from Bob's public key, and the "hardness" decreases with increasing computational power, computation time, and the efficiency of the algorithm. Hence, it doesn't provide everlasting security. To exemplify, let's look at the first and still one of the most used public-key cryptography, the RSA Encryption. To reveal the private key from the public key, one should factor an integer with two large prime factors. Execution of the protocol requires multiplying large prime numbers, which can be done by the computers in polynomial time. However, the factorization runs in exponential time. Therefore, RSA can be executed by a classical computer but cannot be broken. In contrast, a quantum algorithm called "Shor's algorithm" factors integers in polynomial time on a quantum computer. The temporariness of privacy in public-key cryptography is a significant problem for organizations that do not want to risk disclosing their information in the future. On the contrary, quantum cryptography offers protocols for secret key distribution and secret key recycling (key re-using) that does not suffer from decreased security. Furthermore, these protocols have rigorous security proofs and their physical implementations are already being produced commercially.

In 1984, Charles Bennett and Gilles Brassard developed the first quantum key distribution(QKD) scheme[2], the BB84. The basic idea is sending the key information in quantum bits (qubits) rather than classical bits so that an attack on the qubits would disturb the state of the qubits. This can be detected by consuming a part of the qubits to publicly discuss if a disturbance exists. The fundamental assumption of quantum

key distribution is that the laws of quantum mechanics hold. There may be other assumptions depending on the type of the security proof such as, trusting the manufacturer of the device etc. More importantly, quantum key distribution suffers from a very small probability of failure, the probability that protocol accepts the distributed keys although the keys are not secure. In 2005, Renato Renner gave a rigorous proof on upper bounding this small probability of failure, along with new tools that have been crucial for quantum cryptography[3].

Back to 1982, two years before the invention of BB84, a scheme named quantum key recycling was given by Charles Bennett, Gilles Brassard, and Seth Breidbart [4]. This protocol gave an idea on how to re-use a secret key securely, which is not possible solely with a classical communication. The idea revolves around sending the ciphertext in quantum bits instead of classical bits. Therefore, an attack on the qubits would disturb them, which can be later detected with a classical authentication method. An attack on more qubits increases probability of disturbance along with the probability of detection. Although quantum key recycling did not receive as much attention as quantum key distribution, a quantum key recycling protocol with error tolerance established comparable rates of secure data transmission with less classical post-processing[5].

As it can be seen from both protocols, the core difference between the classical and the quantum cryptography comes from the detection of the adversarial behavior. In a classical channel, an adversary can intercept the signals and copy the information without disturbing the transmission. Therefore, parties are forced to assume that an adversary is present and copying their transmitted information. In quantum cryptography, the information inside the qubits cannot be copied/cloned and the adversary is forced to perform measurement on the qubits if she is interested in the information encoded by the qubit's state. However, without knowing the method of encoding, the adversary always takes the risk of disturbing the state. This disturbance is directly proportional to the number of qubits she measures as well as the information she obtains. By applying some methods that will be discussed in the following chapters, disturbance she makes can be corrected in both sending and receiving ends and the stolen information can be removed by a method called privacy amplification. The error correction and privacy amplification comes with very tiny probabilities of fail-

ure that can be calculated and upper bounded. The upper bound can be decreased at the cost of reducing rate of the transmission. The users can knowingly choose how much risk they wish to take against the rate they want to send the information. Classical cryptography lacks parties to remotely send secrecy with a such quantifiable security. The only remote classical transmission of secret keys can be done by computational assumptions which of course cannot provide a time invariant upper bound on the probability of failure. There is no doubt that given enough time all calculable (or decidable) problems can be calculated and hence the upper bound of failure can ultimately become unity.

CHAPTER 2

PRELIMINARIES

Quantum cryptography is built on quantum mechanics, information theory and cryptography. In this chapter the main concepts, terminology used and common techniques that will be used in this thesis will be introduced.

2.1 Quantum Mechanics

2.1.1 The Quantum State

Any closed quantum system has an associated Hilbert space $\mathcal{H}$, i.e. a complete inner-product space. The associated space of a system is called, the state space of the system. The system is completely described by a unit vector in its state space called, the state vector. If $\{|i\rangle\}_i$ is an orthonormal basis for $\mathcal{H}$, then the state vector $|\psi\rangle$ can be expanded in this basis as,

$$|\psi\rangle = \sum_i \alpha_i |i\rangle \tag{2.1}$$

where the α_i are amplitudes, which are complex numbers satisfying, $\sum_i |\alpha_i|^2 = 1$.

2.1.2 The Quantum Evolution

Time evolution of a closed quantum system is described by a unitary operation. Let $|v\rangle$ describes the state of a system at time t_0 and $|w\rangle$ at time t_1. The transformation U that describes the evolution should be unitary and should only depend on time t_0 and t_1[6].

$$|w\rangle = U |v\rangle \tag{2.2}$$

An operator U is said to be unitary if $U^\dagger U = UU^\dagger = I$. It can be shown that any unitary operator can be expanded as

$$U = \sum_i \lambda_i \left|i\right\rangle\!\left\langle i\right| \tag{2.3}$$

where $\{|i\rangle\}$ are its eigenvectors and λ_i are eigenvalues, which are complex numbers with modulus 1. Any unitary operator U maps an orthonormal to another orthonormal basis. Let, $\{|v_i\rangle\}_i$ is an orhonormal basis, if U is unitary, then for some orhonormal basis $\{|w_i\rangle\}_i$

$$U = \sum_i \left|w_i\right\rangle\!\left\langle v_i\right|. \tag{2.4}$$

2.1.3 The Quantum Measurement

General quantum measurements are described by a collection $\{M_k\}$ of measurements operators which satisfy the equation [6]

$$\sum_k M_k^\dagger M_k = I. \tag{2.5}$$

This equation corresponds to the sum of the probabilities being one. A collection $\{M_k^\dagger M_k\}$ of operators satisfying (2.5) are called positive operator valued measure (POVM) operators. The measurement operators act on the state space of the measured system. Suppose the system is in state $|\psi\rangle$ before measurement, then the probability that outcome k occurs is,

$$p_k = \left\langle\psi\right| M_k^\dagger M_k \left|\psi\right\rangle \tag{2.6}$$

and the post-measurement state of the system is,

$$\frac{M_k \left|\psi\right\rangle}{\sqrt{\left\langle\psi\right| M_k^\dagger M_k \left|\psi\right\rangle}}. \tag{2.7}$$

If one does not care about the post-measurement state but only cares about the probabilities of measurement outcomes, then one may use a set of POVMs instead of generalized measurement operators. In case, all measurement operators in a collection $\{P_k\}$ are orthogonal projectors, then the measurement is called a projective measurement. For a projective measurement, POVMs and generalized measurement operators are the same. The probability of getting outcome k is,

$$p_k = \left\langle\psi\right| P_k \left|\psi\right\rangle \tag{2.8}$$

and the post-measurement state of the system is,

$$\frac{P_k \left|\psi\right\rangle}{\sqrt{\left\langle\psi\right| P_k \left|\psi\right\rangle}}. \tag{2.9}$$

2.1.4 Entanglement

Entanglement is the inability of describing a joint state by a tensor product of individual states. If a joint state $\left|\psi_{AB}\right\rangle \in \mathcal{H}^{AB}$ can be written in the form $\left|\psi_A\right\rangle \otimes \left|\psi_B\right\rangle$ for some $\left|\psi_A\right\rangle \in \mathcal{H}^A$ and $\left|\psi_B\right\rangle \in \mathcal{H}^B$ then the state is a product state. If the state is not a product state, then it is entangled.

For two systems A and B with associated state spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, the composite system AB's state space $\mathcal{H}_{AB}$ is given by the tensor product $H_A \otimes H_B$. In other words, a generic state $\left|\psi\right\rangle$ of AB can be written as a superposition of tensor product of states of A and B as

$$\left|\psi\right\rangle = \sum_{ij} \alpha_{ij} \left|i_A\right\rangle \otimes \left|j_B\right\rangle. \tag{2.10}$$

It can be shown that, for any state $\left|\psi\right\rangle$ it is possible to find two orthonormal bases of $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively such that

$$\left|\psi\right\rangle = \sum_{i} \lambda_i \left|i_A\right\rangle \otimes \left|i_B\right\rangle \tag{2.11}$$

where, λ_i are non-negative numbers. This is called the Schmidt decomposition[6].

2.1.5 The Density Operator

In many cases, one *cannot* not certainly know which state a quantum system is in. Therefore, one is forced to assign some probabilities on some possible states. Suppose a system is in state $\left|\psi_i\right\rangle$ with probability p_i, then the set of pairs $\{\left|\psi_i\right\rangle, p_i\}_i$ is called, an ensemble of pure states. The density operator ρ associated with this ensemble is,

$$\rho = \sum_{i} p_i \left|\psi_i\right\rangle\!\left\langle\psi_i\right| \tag{2.12}$$

The density operator is the main quantity that enables us to compute all physically relevant quantities like expectation values, probabilities of measurement outcomes etc. Let's see why by investigating a measurement process. A measurement on a density

state is described by a collection of measurement operators $\{M_k\}$ which satisfies the equation $\sum_k M_k^\dagger M_k = I$. Suppose the system is in state ρ. Given the state $|\psi_i\rangle$ the conditional probability probability of measuring k is[6],

$$p_{k|i} = \langle\psi_i| M_k^\dagger M_k |\psi_i\rangle = \mathrm{tr}\Big(M_k^\dagger M_k |\psi_i\rangle\langle\psi_i|\Big) \tag{2.13}$$

and the post-measurement state is,

$$\frac{M_k |\psi_i\rangle}{\sqrt{\langle i| M_k^\dagger M_k |\psi_i\rangle}} \tag{2.14}$$

Given the state ρ, the probability of measuring k is[6],

$$p_k = \sum_i p_i p_{k|i} = \sum_i p_i \,\mathrm{tr}\Big(M_k^\dagger M_k |\psi_i\rangle\langle\psi_i|\Big) \tag{2.15}$$

$$\mathrm{tr}\left(M_k^\dagger M_k \sum_i p_i |\psi_i\rangle\langle\psi_i|\right) = \mathrm{tr}\Big(M_k^\dagger M_k \rho\Big) \tag{2.16}$$

and using the Bayes' rule the post-measurement state is,

$$\rho_k = \sum_i p_{i|k} \frac{M_k |\psi_i\rangle\langle\psi_i| M_k^\dagger}{\langle\psi_i| M_k^\dagger M_k |\psi_i\rangle} \tag{2.17}$$

$$= \sum_i p_{k|i} p_i \frac{M_k |\psi_i\rangle\langle\psi_i| M_k^\dagger}{p_k \,\mathrm{tr}\Big(|\psi_i\rangle\langle\psi_i| M_k^\dagger M_k\Big)} \tag{2.18}$$

$$= \sum_i p_i \frac{M_k |\psi_i\rangle\langle\psi_i| M_k^\dagger}{p_k} \tag{2.19}$$

$$= \frac{M_k \rho M_k^\dagger}{p_k} \tag{2.20}$$

If the outcome k is unknown, then the post-measurement state ρ' should be a mixture of ρ_k with probability p_k which is,

$$\rho' = \sum_k p_k \rho_k = \sum_k M_k \rho M_k^\dagger \tag{2.21}$$

Suppose that a system whose state is described by ensemble $\{|\psi_i\rangle, p_i\}_i$ has evolved in time according to a unitary transformation U. This means that, after the time evolution, the new ensemble is $\{U|\psi_i\rangle, p_i\}_i$, This shows that the final density operator is [6]

$$\sum_i p_i U |\psi_i\rangle\langle\psi_i| U^\dagger = U \rho U^\dagger \tag{2.22}$$

A density operator should be a non-negative operator with unit trace. An operator is non-negative if it is Hermitian and it has non-negative eigenvalues. Non-negative operators are also normal, therefore can be written in the diagonal form. Let ρ be a density operator, then there exists some orhonormal basis $\{|\psi_i\rangle\}_i$ such that [6]

$$\rho = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i| \tag{2.23}$$

where, $|\psi_i\rangle$ are the eigenvectors of ρ and $\mathrm{tr}(\rho) = \sum_i \lambda_i = 1$. A density operator is mixed state if it has more than one non-zero eigenvalues. If all of its eigenvalues are non-zero and equal to each other, it is the maximally mixed state or completely unpolarized state. If a density operator is not mixed then it is a pure state in which case it can be written as a single 1-dimensional projector as $|\psi\rangle\langle\psi|$ for some $|\psi\rangle \in \mathcal{H}$. If a density operator ρ^{AB} describes the state of a composite system AB and can be written in the form,

$$\rho^{AB} = \sum_i p_i \rho_i^A \otimes \rho_i^B \tag{2.24}$$

for some non-negative p_i and ρ_i^A ρ_i^B, then it is called a separable state. If a state is not a separable state, then it is entangled. In the rest of the thesis, the set of density operators on Hilbert space $\mathcal{H}$ will be denoted as $\mathcal{S}(\mathcal{H})$.

2.1.6 The Partial Trace

Let particle A and B interact for a period of time and have a final state represented by ρ^{AB}. If one wants to describe the state of particle A individually, one should remove particle B from the representation of their combined state. This corresponds to taking the partial trace on B,

$$\rho^A := \mathrm{tr}_B(\rho^{AB}) \tag{2.25}$$

Generally, a density state of system AB can be written as $\rho^{AB} = \sum_{ijkl} \lambda_{ijkl} |i_A\rangle\langle j_A| \otimes |k_B\rangle\langle l_B|$ where $\{|i_A\rangle\}_i$ $\{|k_B\rangle\}_k$ are orhonormal bases for A and B spaces respectively.

In that case, the partial trace is computed as,

$$\rho^A = \mathrm{tr}_B(\rho^{AB}) \tag{2.26}$$
$$= \sum_{ijkl} \lambda_{ijkl} \, |i_A\rangle\langle j_A| \otimes \mathrm{tr}(|k_B\rangle\langle l_B|) \tag{2.27}$$
$$= \sum_{ijkl} \lambda_{ijkl} \, |i_A\rangle\langle j_A| \, \langle l_B|k_B\rangle \tag{2.28}$$
$$= \sum_{ijkl} \lambda_{ijkl}\delta_{kl} \, |i_A\rangle\langle j_A| \tag{2.29}$$
$$= \sum_{ijkl} \lambda_{ijll} \, |i_A\rangle\langle j_A| \tag{2.30}$$

To illustrate how the partial trace acts on a separable state, let $\rho^{AB} = \sum_i p_i \rho_i^A \otimes \rho_i^B$.

$$\mathrm{tr}_B(\rho^{AB}) = \mathrm{tr}_B(\sum_i p_i \rho_i^A \otimes \rho_i^B) \tag{2.31}$$
$$= \sum_i p_i \, \mathrm{tr}_B(\rho_i^A \otimes \rho_i^B) \tag{2.32}$$
$$= \sum_i p_i \rho_i^A \, \mathrm{tr}\big(\rho_i^B\big) \tag{2.33}$$
$$= \sum_i p_i \rho_i^A \tag{2.34}$$
$$= \rho^A \tag{2.35}$$

2.1.7 Purification

Let an arbitrary density operator $\rho \in \mathcal{S}(\mathcal{H}^A)$, then a state $|\Psi_{AR}\rangle \in \mathcal{H}^{AR}$ that satisfies the equation $\rho = \mathrm{tr}_R(|\Psi_{AR}\rangle\langle\Psi_{AR}|)$ is called, a purification of ρ.

Note that, if a unitary operator U^R is applied on the ancilla space $\mathcal{H}^R$ of a purification, the result will also be a purification of the same state due to the cyclic property of trace.

$$\begin{aligned} & tr_R\left(I_A \otimes U_R|\Psi_{AR}\rangle\langle\Psi_{AR}|I_A \otimes U_R^+\right) \\ & = tr_R\left(I_A \otimes U_R^+ U_R|\Psi_{AR}\rangle\langle\Psi_{AR}|I_A \otimes I_R\right) \\ & = tr_R\left(|\Psi_{AR}\rangle\langle\Psi_{AR}|\right) \end{aligned} \tag{2.36}$$

2.1.8 The Classical-Quantum States

In quantum cryptography, a classical random variable X with a set of probabilities $\{p_x\}_x$ defines a classical state and is described as,

$$\rho_X = \sum_x p_x \left|x\right\rangle\!\left\langle x\right| \tag{2.37}$$

where $|x\rangle$ are orthonormal. Let the state ρ_{XE} be a classical-quantum state (cq-state) with classical part X and quantum part E, by this we mean that ρ_{XE} can be written as

$$\rho_{XE} = \sum_x p_x \left|x\right\rangle\!\left\langle x\right| \otimes \rho_x^E. \tag{2.38}$$

Note that if an adversary, Eve has subsystem E but not X, she may differentiate between ρ_x^E 's by making a measurement on E and obtain information about x.

2.1.9 The Ideal State

An ideal state is a cq-state composed of an uncoupled maximally mixed state and a quantum state,

$$\rho_{ideal} := \frac{1}{|X|} \sum_{x \in \mathcal{X}} \left|x\right\rangle\!\left\langle x\right| \otimes \rho^E. \tag{2.39}$$

Let Alice has the subspace $\mathcal{H}_X$ and Eve has the subspace $\mathcal{H}_E$. Alice performs a projective measurement on her space and obtain a value $x \in \mathcal{X}$, uniformly at random. Furthermore, Eve cannot do any measurement on her space that gives her any information about x. Hence, x is completely unknown to Eve, and this defines an ideal state for keeping x a secret.

2.1.10 The Completely Positive Trace Preserving Maps

Time evolution of open quantum systems is described by the CPTP maps. Let $\mathcal{E}$ be a map from density states in $\mathcal{S}(\mathcal{H}_A)$ to density states in $\mathcal{S}(\mathcal{H}_B)$ denoted as, $\mathcal{E} \in \mathcal{C}(\mathcal{S}(\mathcal{H}_A), \mathcal{S}(\mathcal{H}_B))$, then for any $\rho \in \mathcal{S}(\mathcal{H}^A)$ and $\sigma \in \mathcal{S}(\mathcal{H}^{AE})$, $\mathcal{E}$ should be

1) Trace preserving,

$$\mathrm{tr}\left(\mathcal{E}(\rho)\right) = \mathrm{tr}\left(\rho\right) \tag{2.40}$$

2) Convex linear,

$$\mathcal{E}\left(\sum_i p_i \rho_i\right) = \sum_i p_i \mathcal{E}\left(\rho_i\right) \tag{2.41}$$

where, $\sum_i p_i \rho_i$ is a density operator.

3) Completely positive,

$$(\mathcal{E} \otimes \mathrm{I}_E)(\sigma_{AE}) \geq 0 \tag{2.42}$$

CPTP maps may "expand, evolve and reduce" the state of the system. This behavior is shown by the Steinspring dialation.

Let $\mathcal{E} \in \mathcal{C}\left(\mathcal{S}(\mathcal{H}_A), \mathcal{S}(\mathcal{H}_B)\right)$ and $\rho \in \mathcal{S}(\mathcal{H}^A)$, then there exist an isometry V ($V^\dagger V = \mathbb{I}$) from $\mathcal{H}_A$ to $\mathcal{H}_{BR}$ such that,

$$\mathcal{E}(\rho) = \mathrm{tr}_R\left(V \rho V^\dagger\right). \tag{2.43}$$

V can be seen as an operator which makes an *isometric embedding* from $\mathcal{H}^A$ to $\mathcal{H}^B \otimes \mathcal{H}^R$, followed by a unitary operation on $\mathcal{H}^B \otimes \mathcal{H}^R$. Finally, the partial trace throws away some part of the system reducing it to a sub-system.

It can be shown that any CPTP mapping can be described by a collection $\{E_k\}$ of Kraus operators that satisfy the equation $\sum_k E_k^\dagger E_k = \mathbb{I}$. If $\mathcal{E}$ is a CPTP map, then there exists some collection of Kraus operators $\{E_k\}$ such that,

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger. \tag{2.44}$$

This is known as the operator-sum representation.

Example 2.1.1. Let a projective measurement be performed on subsystem A of a joint system AB which has an arbitrary state $\rho^{AB} \in \mathcal{S}(\mathcal{H}^{AB})$, while recording the outcomes $\{k\}_k$ in a state in system K. The measured observable M is an observable of A, and let M=$M = \sum_k k P_k$ where P_k are the projection operators to the eigensubspace associated with k. Here the measurement operators are $P_k := |k\rangle\langle k|$, the probability of measuring k is $p_k = \mathrm{tr}(P_k \otimes I\rho)$ and the corresponding post-measurement state is

$\rho_k^{AB} = \frac{1}{p_k}(P_k \otimes I)\rho(P_k \otimes I)$. Therefore, the post-measurement state without knowing the result is,

$$\rho^{KAB} = \sum_k p_k \left|k\right\rangle\!\left\langle k\right| \otimes \rho_k^{AB}. \tag{2.45}$$

A CPTP mapping $\mathcal{E}_{meas}$ from $\mathcal{S}(\mathcal{H}^{AB})$ to $\mathcal{S}(\mathcal{H}^{KAB})$ can be written in the operator-sum representation as,

$$E_k = \left|k\right\rangle \otimes P_k^A \otimes \mathbb{I}_{\mathbb{B}} \tag{2.46}$$

which satisfies the condition,

$$\begin{aligned} \sum_k E_k^\dagger E_k &= \sum_k \left\langle k|k\right\rangle P_k^A \otimes \mathbb{I}_{\mathbb{B}} \\ &= \left(\sum_k P_k^A\right) \otimes \mathbb{I}_{\mathbb{B}} \\ &= I_{AB}. \end{aligned} \tag{2.47}$$

Then,

$$\begin{aligned} \mathcal{E}_{meas}(\rho) &= \sum_k E_k^\dagger \rho^{AB} E_k \\ &= \sum_k \left|k\right\rangle\!\left\langle k\right| \otimes (P_k \otimes I_b)\rho^{AB}(P_k \otimes I_b) \\ &= \sum_k p_k \left|k\right\rangle\!\left\langle k\right| \otimes \rho_k^{AB} \\ &= \rho^{KAB}. \end{aligned} \tag{2.48}$$

It can be seen that the final state is a sum over coupled states between observed values k's and its environment states ρ_k^{AB}'s. Any measurement outcome k and the coupled environment state ρ_k^{AB} live in a space which is orthonormal to other spaces of outcomes.

2.1.11 The Trace Distance

The trace distance is a metric on the space of density operators. Let $\rho \in \mathcal{S}(\mathcal{H})$ and $\sigma \in \mathcal{S}(\mathcal{H})$, then the trace distance between ρ and σ is

$$T(\rho, \sigma) := \sup_{0 \le M \le I} \operatorname{tr}\left[M(\rho - \sigma)\right] \tag{2.49}$$

where M is a POVM operator. Or equivalently using ℓ_1 distance $\|\rho - \sigma\|_1$,

$$T(\rho, \sigma) := \frac{1}{2}\|\rho - \sigma\|_1 = \frac{1}{2}\operatorname{tr}|\rho - \sigma| = \frac{1}{2}\operatorname{tr}\sqrt{(\rho - \sigma)^2} \tag{2.50}$$

Suppose $\rho - \sigma$ is written in diagonal form as $\rho - \sigma = \sum_i \lambda_i |i\rangle\langle i|$, where $|i\rangle$ are the orthonormal eigenvectors of $\rho - \sigma$ and λ_i are its eigenvalues. The absolute value of $\rho - \sigma$ can be written as $|\rho - \sigma| = \sum_i |\lambda_i| |i\rangle\langle i|$ and its trace is $\operatorname{tr}|\rho - \sigma| = \sum_i |\lambda_i|$.

Trace distance implies the maximum probability of success in differentiating density states in a single measurement. To illustrate this, let's assume one has an equal chance of getting σ or ρ and wants to find out the state by performing a measurement. Pairs of measurement operators and outcomes (i.e. guesses) are (M,ρ) and ($I - M$, σ). Then, probability of success is,

$$p_{success} = \frac{1}{2}\operatorname{tr}(M\rho) + \frac{1}{2}\operatorname{tr}((I - M)\sigma) \tag{2.51}$$

$$= \frac{1}{2}\operatorname{tr}(\sigma) + \frac{1}{2}\operatorname{tr}(M(\rho - \sigma)) \tag{2.52}$$

$$= \frac{1}{2} + \frac{1}{2}\operatorname{tr}(M(\rho - \sigma)). \tag{2.53}$$

To maximize this probability one can maximize the second term in the left-hand side of (2.53), which corresponds to selecting an appropriate measurement operator,

$$p_{success} = \frac{1}{2} + \frac{1}{2}\sup_{0 \le M \le I} \operatorname{tr}\left[M(\rho - \sigma)\right] \tag{2.54}$$

$$= \frac{1}{2} + \frac{1}{2}T(\rho, \sigma). \tag{2.55}$$

Observe that the trace distance gives us the maximum advantage one can have in distinguishing these density states with a single measurement. In quantum cryptography, the aim is to quantify the maximum information an adversary can gain on a secret message by measuring her state. Therefore it is very important to distinguish the output state of a quantum protocol and the ideal state which is uniformly random and uncorrelated from an adversary. The upper bound of the distance between the ideal state and the output state quantifies how secure a quantum protocol is.

2.1.12 The Diamond Distance

The diamond distance gives us the distinguishing advantage between two quantum maps with equal prior probabilities of 1/2. Let $\mathcal{E}_1, \mathcal{E}_2 \in \mathcal{C}(\mathcal{S}(\mathcal{H}_A), \mathcal{S}(\mathcal{H}_B))$, then the diamond distance between $\mathcal{E}_1$ and $\mathcal{E}_2$ is

$$\|\mathcal{E}_1 - \mathcal{E}_2\|_\diamond := \sup_{\rho \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_R)} \|\mathcal{E}_1 \otimes \mathrm{I}_R(\rho) - \mathcal{E}_2 \otimes \mathrm{I}_R(\rho)\|_1 . \tag{2.56}$$

2.1.13 No-cloning Theorem

In the heart of quantum cryptography, lies the no-cloning theorem. The inability of cloning an unknown state without already knowing what the state is. Suppose operator U is defined as,

$$U : |\psi\rangle \rightarrow |\psi\rangle \otimes |\psi\rangle \,,\ \forall |\psi\rangle \in \mathcal{H} \tag{2.57}$$

Let $|\psi_1\rangle \in \mathcal{H}$ and $|\psi_2\rangle \in \mathcal{H}$, then,

$$U |\psi_1\rangle = |\psi_1\rangle \otimes |\psi_1\rangle \tag{2.58}$$

$$U |\psi_2\rangle = |\psi_2\rangle \otimes |\psi_2\rangle \tag{2.59}$$

$$\implies \langle\psi_1| U^\dagger U |\psi_2\rangle = |\langle\psi_1|\psi_2\rangle|^2 \tag{2.60}$$

U must be inner product preserving in order to describe a quantum system's time evolution. However, $|\langle\psi_1|\psi_2\rangle|^2 \neq |\langle\psi_1|\psi_2\rangle|$ unless $|\langle\psi_1|\psi_2\rangle| = 0$ or $|\langle\psi_1|\psi_2\rangle| = 1$, therefore U cannot be defined for an arbitrary $|\psi\rangle$ (2.57).

2.2 The Information Theory and Cryptography

2.2.1 Quantifying Information

In the following definitions, let X be a random variable with alphabet $\mathcal{X}$, outcomes $x \in \mathcal{X}$ and probability mass function $P_X(x)$. Similarly, let Y be a random variable with alphabet $\mathcal{Y}$, outcomes $y \in \mathcal{Y}$ and probability mass function $P_Y(y)$.

Definition 2.2.1. (Information content) The information content of outcome x is,

$$h(x) := -\log(P_X(x)) \tag{2.61}$$

Definition 2.2.2. (Shannon entropy) The entropy of X is the average information content,

$$H(X) := \mathbf{E}[h(X)] \tag{2.62}$$

$$= -\sum_x P_X(x) \log(P_X(x)) \tag{2.63}$$

where, $\mathbf{E}$ is the statistical average.

The entropy of a random variable X is the average information content of n realizations of X where n goes to infinity. The average information content of any n realizations of X asymptotically converge to the Shannon entropy.

Suppose that one will observe X once and wants to correctly guess the outcome. The best guess is the most probably outcome.

Definition 2.2.3. The minimum entropy of X is the information content of its most probable outcome,

$$\begin{aligned} \mathrm{H}_{\min}(X) &:= \min_x h(x) && (2.64)\\ &= \min_x \left[-\log P_X(x)\right] && (2.65)\\ &= -\log \max_x \left[P_X(x)\right]. && (2.66) \end{aligned}$$

In terms of minimum entropy the guessing probability is,

$$\max_x P_X(x) = 2^{-\mathrm{H}_{\min}(X)}. \tag{2.67}$$

Definition 2.2.4. The conditional entropy of X given Y is,

$$\begin{aligned} H(X|Y) &= \sum_y P_Y(y) H(X|Y=y) && (2.68)\\ &= -\sum_y P_Y(y) \sum_x P_{X|Y}(x|y) \log\big(P_{X|Y}(x|y)\big) && (2.69)\\ &= -\sum_{xy} P_Y(y) P_{X|Y}(x|y) \log\big(P_{X|Y}(x|y)\big) && (2.70)\\ &= -\sum_{xy} P_{XY}(x,y) \log\big(P_{X|Y}(x|y)\big). && (2.71) \end{aligned}$$

Definition 2.2.5 (Conditional minimum entropy)**.** The conditional minimum entropy of X given Y is,

$$H_{\min}(X|Y) = -\log\left(\sum_y \max_x (p_{X|Y}(x|y))\right). \tag{2.72}$$

2.2.2 Quantifying Quantum Information

Now, the quantum counterparts of the classical entropies will be defined.

Definition 2.2.6. (von Neumann entropy) Let $\rho \in \mathcal{S}(\mathcal{H})$, then von Neumann entropy of ρ is

$$H(\rho) := \mathrm{tr}(\rho \log \rho). \tag{2.73}$$

Example 2.2.1. Let ρ has a spectral decomposition $\sum_x p_x \left|x\right\rangle\!\left\langle x\right|$, then

$$H(\rho) = -\sum_x p_x \log p_x. \tag{2.74}$$

One can observe that the von Neumann entropy of the density operator is the counterpart of the Shannon entropy of a random variable.

Definition 2.2.7. (Min-entropy) [3] Let $\{M_m\}$ be a POVM, then

$$H_{\min}(\rho) := -\log \max_m \mathrm{tr}(\rho M_m). \tag{2.75}$$

Definition 2.2.8. (Conditional min-entropy) [3] Let $\rho^{AB} \in \mathcal{S}(H^A \otimes H^B)$, $\sigma^B \in \mathcal{S}(\mathcal{H}^B)$ then,

$$H_{\min}(\rho^{AB}|\sigma^B) := \log(\lambda) \tag{2.76}$$

such that, $\lambda \cdot I_A \otimes \sigma_B - \rho_{AB} \geq 0$.

Definition 2.2.9. (Smooth min-entropy) [3] Let $\rho^{AB} \in \mathcal{S}(H^A \otimes H^B)$, $\sigma^B \in \mathcal{S}(\mathcal{H}^B)$ then, ε-smooth min-entropy of ρ_{AB} to σ_B is,

$$H^{\varepsilon}_{\min}\left(\rho_{AB} \mid \sigma_B\right) := \sup_{\bar{\rho}_{AB}:\|\rho_{AB}-\bar{\rho}_{AB}\|_1 \leq \varepsilon} H_{\min}\left(\bar{\rho}_{AB} \mid \sigma_B\right), \tag{2.77}$$

2.2.3 The One-Time Pad

One-time pad encryption is used to provide information-theoretic security. Let Alice and Bob pre-share a key $x \in \{0,1\}^n$, i.e. a binary string of n bits. Alice wants to send a message text $m \in \{0,1\}^n$. Alice computes a ciphertext $c_1 = x \oplus m$ and send it to Bob. After receiving c_1 Bob can recover m_1 by using his key x and c_1, $c_1 \otimes x = x \oplus x \oplus m_1 = m_1$. If key x is sampled from an uniform distribution hidden from Eve, then Eve cannot gain any information about the message from the

ciphertext. *Proof.*

$$P(M = m|C = c) = \frac{P(C = c|M = m)P(M = m)}{P(C = c)} \tag{2.78}$$

$$= \frac{P(X = m \oplus c)P(M = m)}{P(C = c)} \tag{2.79}$$

$$= \frac{P(M = m)}{2^n P(X \oplus M = c)} \tag{2.80}$$

$$P(X \oplus M = c) = \sum_{xm} P(X = x)P(M = m)\delta_{m\oplus x,c} \tag{2.81}$$

$$= \frac{1}{2^n} \sum_{m} P(M = m) \sum_{x} \delta_{m\oplus x,c} = \frac{1}{2^n} \tag{2.82}$$

$$P(M = m|C = c) = P(M = m) \tag{2.83}$$

where δ is the Kronecker delta. However, Eve can store this cyphertext so if Alice and Bob use the same key x to exchange another message $m_2 \in \{0,1\}^n$ where $c_2 = m_2 \oplus x$ then Eve can perform $c_1 \oplus c_2 = m_1 \oplus m_2$. Therefore, using the same key twice leaks information ($m_1 \oplus m_2$) about the messages.

2.2.4 The Hash Function

In a general sense, the hash functions can be defined as functions that map long bit strings to shorter bit strings. Hash functions can have unique properties. A set of hash functions that shares a common property is called, *a family of hash functions*.

Definition 2.2.10 (1-universal)**.** A family of hash functions, $\mathscr{H} = \{h : \{0,1\}^n \rightarrow \{0,1\}^m\}$ where $m \leq n$ is 1-universal if $\forall x \in \{0,1\}^n$ and $\forall z \in \{0,1\}^m$,

$$P_{h\in\mathscr{H}}(h(x) = z) = \frac{1}{2^m} \tag{2.84}$$

where h is chosen from $\mathscr{H}$ uniformly at random. Note that, the only random variable here is h. For any value of x and z, when h is chosen from $\mathscr{H}$ uniformly at random, equation (2.84) holds.

Definition 2.2.11 (2-universal)**.** A family of hash functions $\mathscr{H} = \{h : \{0,1\}^n \rightarrow \{0,1\}^m\}$ where $m \leq n$, is *2-universal*, if $\forall x, \forall x' \in X, x \neq x'$, and all pairs $z, z' \in Z$,

$$P_{h\in\mathscr{H}}(h(x) = z \wedge h(x') = z')) = \frac{1}{2^{2m}} \tag{2.85}$$

where h is chosen from $\mathscr{H}$ uniformly at random. Also note that when $x = x'$, $\mathscr{H}$ satisfies (2.84) , i.e.

$$P_{h\in\mathscr{H}}(h(x) = z \wedge h(x) = z)) = P_{h\in\mathscr{H}}(h(x) = z) = \frac{1}{2^m} \tag{2.86}$$

which means that any 2-universal hash is 1-universal. An extractor function, or a randomness extractor, $\mathrm{Ext}(u, x)$ is essentially a construction over hash functions. The *seed* of the extractor $u \in U$ is defined for indexing the hash functions. For example, if $\mathscr{H} := \{h_1, h_2, h_3\}$, then the seed is $u \in \{1, 2, 3\}$ and the hash functions can be denoted as h_u. Therefore, choosing a seed uniformly at random, corresponds to choosing a hash function at random for the extractor. Finally, x denotes the input for the chosen hash function. Let $\mathrm{Ext} : (u, x) \mapsto z$, and $\mathbb{E}_u f(u) = \sum_u \frac{1}{|u|} f(u)$, then

$$\mathbb{E}_u \delta_{\mathrm{Ext}(u,x),z}\delta_{\mathrm{Ext}(u,x'),z'} = \delta_{x,x'}|Z|^{-1} + (1 - \delta_{x,x'})|Z|^{-2} \tag{2.87}$$

2.2.5 The Message Authentication Codes

A message authentication code (MAC or *a tag*) is a binary string that contains information about a larger binary string (a message). MACs are used to check the integrity of the messages. Suppose Alice and Bob pre-shares a key k which selects a hash function f_k from a family of 2-universal hash functions. Alice calculates the tag $\tau = \Gamma(m, k)$, i.e. the function denoted by Γ takes the message m and the key k and calculates $f_k(m) = \tau$. Alice sends τ along with m. Bob receives m' and τ (assumes τ remains unchanged), checks if $\Gamma(m', k) = \tau$, encodes the accept/reject result in one bit and sends to Alice. The failure probability of a MAC is $P(\tau = \Gamma(m', k)|m \neq m')$, i.e. the probability of accept when $m \neq m'$. This probability is calculated as follows.

Let binary strings, $m, m' \in \{0, 1\}^l$ represent two messages, $k \in \{0, 1\}^n$ represents a MAC key, $\tau \in \{0, 1\}^z$ represents tag and $\tau = \Gamma(m, k)$, then $\mathrm{P}(\tau = \Gamma(m', k)|m \neq m') = \frac{1}{2^z}$ [7] or equivalently,

$$\mathbb{E}_k \delta_{\Gamma(m',k),\Gamma(m,k)} = \delta_{m,m'} + (1 - \delta_{m,m'})\frac{1}{2^z}. \tag{2.88}$$

2.2.6 Syndromes

Syndromes are used as a method of error correction. An error correction refers to correcting the flipped bits of a message that is sent through a noisy channel. A given set of syndromes has an encoder function $\mathrm{Syn} : \{0,1\}^n \to \{0,1\}^\tau$ and a decoder function $\mathrm{DecSyn} : \{0,1\}^\tau \to \{0,1\}^n$. The encoder function maps a message to a syndrome, which encodes the relations (such as the checksums) of the message bits. After the message and the syndrome is sent through a noisy channel, the receiver puts the syndrome to its decoder function which checks if the relations hold and gives a bit string with the length of the message. Then, one can XOR the received (and possibly corrupted) message m' and the decoder output s to recover the original message $s \oplus m' = \hat{m}$. The decoding can fail, i.e. $\hat{m} \neq m$, if the flipped bits are more than the number of bits the syndrome can correct. However, failure of the decoding is noticed by the receiver [7].

CHAPTER 3

QUANTUM CRYPTOGRAPHY

3.1 Quantifying Security

The one-time pad is the “gold standard” in cryptography. It is the only known algorithm that can unconditionally and perfectly secure a message. However, one-time pad is also costly, a secret key can be only used once as a one time pad. Meanwhile, Alice aims to find a more sustainable method and she considers using Bob’s public-key to encrypt her messages. Nobody except Bob, has the private key that can decrypt it, but, this situation can change. In particular, Bob’s private key can be calculated from Bob’s public key, but this requires to perform calculations which are practically impossible with current technologies. However she is anxious because she thinks that with promising new technologies together with new algorithms, these problems can be solved. Therefore, her security may not hold in the future and may completely lose its value. If Alice chooses to send her messages using Bob’s public key, Eve, the malicious eavesdropper, can easily copy them without notice. Eve can then store them until she can compute Bob’s private key from his public key, and can read all the messages Alice sent to Bob. Alice looks at the probability "ε" that Eve computes Bob’s private key, and it is very small. However, "ε" grows as the technology improves.

For quantum protocols, "ε" gives the probability that after (or during) the execution of the protocol, Eve learns *some* information about the secret message. With probability "$(1 - \varepsilon)$" Eve learns *absolutely nothing*, *forever*. In other words, the ε in quantum protocols stays constant. Alice decides to use quantum cryptography, if the ε is very small and it provides fast and accurate communication.

3.2 Quantum Key Distribution

Quantum key distribution is used as an umbrella term for the key distribution protocols that utilize quantum mechanics. Unlike classical key distribution methods which rely on computational assumptions such as the hardness of factorization in RSA, security of quantum key distribution is unconditional. It is invulnerable to new decryption algorithms as well as increasing computational power. Developed in 1984 by Charles Bennett and Gilles Brassard [2], BB84 is the first scheme for implementing quantum key distribution.

3.2.1 BB84

Alice chooses binary strings $x \in \{0,1\}^n$ and $b \in \{0,1\}^n$ uniformly at random and for each x_i she encodes qubits $\left|\psi_{x_i}^{b_i}\right\rangle$ as,

$$\begin{aligned} \left|\psi_0^0\right\rangle &:= |0\rangle \ \left|\psi_0^1\right\rangle := |+\rangle \\ \left|\psi_1^0\right\rangle &:= |1\rangle \ \left|\psi_1^1\right\rangle := |-\rangle \end{aligned} \tag{3.1}$$

where $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ are the eigenvectors of Pauli-Z and Pauli-X matrices respectively. Then, Alice sends $\left|\psi_x^b\right\rangle$ to Bob.

Bob receives $\left|\psi_x^b\right\rangle$ and chooses a binary string $b' \in \{0,1\}^n$ uniformly at random. Then for all qubits in $\left|\psi_x^b\right\rangle$ he performs measurement according to the bits in the binary string b'. In particular, he measures i^{th} qubit in Z-basis if $b'_i = 0$ and X-basis if $b'_i = 1$ and obtains the bit x'_i. After measuring all qubits he obtains a binary string $x' \in \{0,1\}^n$ that is composed of x'_is. Consider that, if $b_i = b'_i$ then $x_i = x'_i$ but if $b_i \neq b'_i$, with probability one half $x'_i = 0$ and probability one half $x'_i = 0$ regardless of the value of x_i. Consequently, Alice and Bob publicly compare each b_i and b'_i to see whether they match or not, and if they match Alice and Bob keep x_i and x'_i otherwise they discard them. After that, they consume a part the binary string that they keep in order to check if there is a discrepancy. If there is discrepancy, this shows the channel is noisy and the noise may be caused by an adversary. If they decide that the error is so high that they will not be able to recover a secure key from the noisy qubits they may abort the protocol. If there is a 'tolerable' amount of unmatched bits, Alice and Bob

can use error correction protocols and correct the unmatched bits in the remaining part of the key. However, as the remaining part of the key is recovered from noisy qubits, Eve may have information on this key. In order to have perfectly secure key from a partially insecure key, Alice and Bob perform privacy amplification on their partially insecure keys. This involves applying a random hash function to their insecure keys and as a result producing a secure key with a smaller length.

Note that the crucial feature of QKD is that, the adversary Eve cannot clone the state sent by Alice due to the no-cloning theorem. To gain any information, Eve is forced to make destructive measurements on the state and forward them to Bob. Hence, Eve's existence and actions can be detected by Alice and Bob. In classical communications, Eve can simply copy the cyphertext without changing it and hence remain undetected.

3.2.2 The protocol

From a uniformly random source generating $2n$ bits, Alice generates $x, b \in \{0,1\}^n$. She encodes the bits in a classical state $|\psi\rangle$ as in (3.1), and sends the qubits to Bob. Note that the state may change while transmission so lets denote Bob's received state $|\psi'\rangle$. Bob generates n bits $b' = \{0,1\}^n$ from a uniformly random source and measures the qubit in the i^{th} location in the Pauli-Z basis if $b_i = 0$ and in Pauli-X basis if $b_i = 1$ for each $i \in \{0,1\}^n$ and records the outcomes as 0 or 1 on a binary string $x' \in \{0,1\}^n$. Then, he announces the b' to Alice, and in return, she announces the locations i where $b'_i \neq b_i$. They both throw the x and x' values corresponding those locations, and left with raw keys $r, r' \in \{0,1\}^m$.

3.2.3 Parameter estimation and error correction

Alice and Bob have to perform error correction for their raw keys in order to use them as a one-time pad, however before that they have to estimate how much noise is present in their communication. To do that, they discuss and randomly choose k bits, $k < m$, and announce them. By looking at the error rate $\delta_1 := e/k$ where e is the number of unmatched bits in k bits, they make an error estimation for the remaining raw key. Suppose that δ_1 is the error rate on the compared k bits and δ_2 is the error

rate on the remaining raw key of $m-k$ bits. Suppose that Alice and Bob decided to tolerate a maximum error rate of γ on the compared bits. If $\delta_1 \leq \gamma$, they will perform error correction on the remaining raw key that can correct for an error rate that is less than $\gamma+\nu$, where $0<\nu<1-\gamma$. Then, the probability of failure of the error correction can be written as follows,

$$P_{\mathrm{pe}}(\gamma,\nu) := P\left((\delta_1 \leq \gamma) \cap (\delta_2 \geq \gamma+\nu)\right). \tag{3.2}$$

This probability can be upper bounded based on Serfling's inequality as[8],

$$P_{\mathrm{pe}}(\gamma,\nu) \leq \exp\left(-2\nu^2 \frac{(m-k)k^2}{m(k+1)}\right). \tag{3.3}$$

3.2.4 Privacy amplification

Suppose that the error correction is successful and Alice and Bob shares the same binary string l with length $\log|l| = m-k$. But, they still don't have perfectly secure keys. The error causing measurements of Eve and the error correcting information they shared publicly, leak information about l. Hence, they should somehow map the partially secure l to another binary string $z \in \{0,1\}^t$ that is perfectly secure. $l \in \{0,1\}^{m-k}$ can be modelled as a binary string sampled from a random variable L with a non-uniform distribution given Eve's knowledge E. Eve's probability of guessing L is $2^{-H_{min}(L|E)}$. Alice and Bob cannot decrease Eve's probability of guessing l but they can map l to a smaller binary string z with length t that looks uniformly random from Eve's perspective. It should also have a similar probability of guessing, that is, 2^{-t} should be as close as possible to $2^{-H_{min}(L|E)}$. But, notice that t cannot be more than $H_{min}(L|E)$. Because the secrecy of l cannot be increased without spending another hidden information. The process of mapping non-uniformly distributed binary string to a smaller but uniformly distributed binary string is called the privacy amplification. Privacy amplification is done by using a randomness extractor (2.2.4) that takes a uniformly random seed s, and an input string l. The failure probability of privacy amplification is the probability that it fails to produce a perfectly secure z. This is given by the distance between ρ_{ZSE}, i.e. the actual state after privacy amplification and $\mu_t \otimes \rho_S \otimes \rho_E$ the ideal state where μ_t is the decoupled maximally mixed state.

This can be upper bounded in terms of smooth min-entropy 2.2.9 as [3]

$$\delta\left(\rho_{ZSE}, \mu_t \otimes \rho_S \otimes \rho_E\right) \leq \frac{1}{2}\sqrt{2^{t-H_{\min}^{\varepsilon}(L|E)_\rho}} + \varepsilon, \tag{3.4}$$

3.2.5 The Ekert91

The Ekert91 is the entanglement version of the prepare-and-share protocols[9]. Any security proof of a quantum protocol in the entanglement version also holds for the prepare-and-measure version. In the entanglement version, instead of preparing Alice and measuring Bob, Alice and Bob shares parts of a Bell state and both measure their parts in either standart basis $\{|0\rangle, |1\rangle\}$ or Hadamard basis $\{|+\rangle, |-\rangle\}$.

$$|\Phi_+\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \tag{3.5}$$

$$= \frac{1}{\sqrt{2}}\left(|{+}{+}\rangle + |{-}{-}\rangle\right) \tag{3.6}$$

If Alice and Bob measures in the same basis their outcome will match with probability 1, and if they use different basis their outcome will match with probability 1/2. Therefore, Alice or Bob may announce the bases of measurement just like in prepare and measure version, and the other side can send the locations of the matching bases (or non-matching). Remember that, the purpose of Alice and Bob is to produce and share an identical random key. In prepare and measure protocols, Alice generates random bit and encodes it with a random basis then sends it to Bob. Then Bob measures it and announce his basis, then Alice lets him know if the basis matches or not. In Ekert version, when Alice measures with a random basis, the outcome will always be uniformly random as the reduced state for both Alice and Bob is $\mathrm{I}/2$. But after Alice measures, Bob's state will collapse into whatever Alice's is, so if Bob measures with the same basis, he will get the same outcome with probability 1 and if not he will get it with probability 1/2. Note that a maximally entangled state is necessarily in a product state with the environment's state (including Eve's state). This property of entanglement is sometimes called as the monogamy of entanglement.

$$|\psi_{ABE}\rangle = |\phi_{AB}\rangle \otimes |\psi_E\rangle \tag{3.7}$$

Therefore, Alice and Bob shares an entangled pair and an adversary can have no knowledge on the measurements of Alice and Bob. The Ekert version provides a theoretical framework for the analysis of the protocols like quantum key distribution and

quantum key recycling, which may be more favorable over the prepare-and-measure version while making security proofs.

3.3 Quantum Key Recycling

Two years before the BB84, Charles H. Bennett, Gilles Brassard and Seth Breidbart, proposed the first quantum key recycling scheme in their paper "Quantum Cryptography II:How to re-use a one-time pad safely even if P=NP"[4]. Their idea was to send a quantum ciphertext instead of a classical ciphertext, so that if an adversary is present they can detect it by checking if the ciphertext is changed or not. If it's not changed, then it's safe to re-use the one-time pad. The paper was submitted to "Fifteenth Annual ACM Symposium on Theory of Computing" but got rejected. After publishing BB84, Charles H. Bennett and Gilles Brassard decided to drop their idea of key recycling, thinking that BB84 was a better idea[4]. Thirty years later, Ivan Damgård, Thomas Brochmann Pedersen and Louis Salvail picked up the idea and proposed a key recycling scheme together with a security proof, in their paper, "A Quantum Cipher with Near Optimal Key-Recycling"[10]. However, their scheme requires the honest users to use quantum computation. In 2017, Serge Fehr and Louis Salvail proposed a new scheme with a security proof, in their paper, "Quantum Authentication and Encryption with Key Recycling" which does not require quantum computers and uses BB84 qubits[11]. Their scheme is as follows.

Alice and Bob shares an authentication key k and a basis key $\theta \in \{0,1\}^n$. Alice and Bob agrees on a MAC function Γ which has the properties described in $(2.2.5)$. Alice chooses a bit string $x \in \{0,1\}^n$ uniformly at random and encodes it on BB84 qubits (3.1) by using θ. Alice produces a plaintext m then computes the tag t as $t = \Gamma(m\|x,k)$. "$\|$" stands for concatenation. Alice sends t, m through a classical channel and $|x\rangle$ through a quantum channel to Bob. Bob receives the noisy qubits, measures them in θ-basis recovers measurements x' and checks if t equals to $\Gamma(m'\|x,k)$. If it is Bob accepts, otherwise he rejects. Bob encodes result accept/reject on the bit $w \in \{0,1\}$ and sends it to Alice. In accept, they re-use θ and k. In reject, only θ will be refreshed, k will still be re-used. Notice that, if it was $\Gamma(m_i,k)$ and Eve knows the plaintexts m_i then Eve would gain information on key k. However, in our case

Eve does not know x. Therefore, in order to get information on k she has to measure the BB84 qubits. Unless Eve knows θ, she has a chance to disturb the state and get detected. So, if Bob accepts, the next round key θ', is set to θ. Otherwise, Alice and Bob selects θ' uniformly at random. Note that, as long as the input of a MAC function holds a considerable uncertainty (see [4]), k is safe to be re-used to authenticate the message. Alice generates a new, uniformly random x every round, hence, in both accept and reject cases, k can be re-used. Suppose Eve holds the system E, authors' claim is, if before the execution, $P_{guess}(\theta|E) \approx 0$ and k is uniformly random given θ and E, then after the execution, $P_{guess}(\theta'|E) \approx 0$ and k stays uniformly random given θ' and E.

3.4 Security Definition

3.4.1 The Ideal Protocol

The security of a quantum protocol is quantified by bounding its diamond distance to its "ideal version".

Definition 3.4.1 (The ideal protocol)**.** Suppose that Alice and Bob want a part of the classical information, let's say X, to remain completely hidden from the adversary Eve after the execution of the protocol. Let $\mathcal{F}$ denote the action of the ideal protocol.

$$\mathcal{F} : \rho_{input} \rightarrow \rho_{ideal} \tag{3.8}$$

where,

$$\rho_{ideal} = \frac{1}{|X|} \sum_{x \in X} |x\rangle\langle x| \otimes \rho^E \tag{3.9}$$

clearly, X is uniformly random and uncoupled from Eve's state, i.e. completely unknown from Eve's perspective.

3.4.2 The Diamond Distance

Definition 3.4.2 (The diamond distance)**.** Let $\mathcal{E}_1, \mathcal{E}_2 \in \mathrm{CPTPM}(\mathcal{S}(\mathcal{H}_A), \mathcal{S}(\mathcal{H}_B))$. Then the diamond distance between $\mathcal{E}_1$ and $\mathcal{E}_2$ is defined as,

$$\|\mathcal{E}_1 - \mathcal{E}_2\|_\diamond := \sup_{\rho \in \mathcal{S}(\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_R)} \|\mathcal{E}_1 \otimes \mathrm{I}_R(\rho) - \mathcal{E}_2 \otimes \mathrm{I}_R(\rho)\|_1 \tag{3.10}$$

Let $\mathcal{E}$ be the map induced by the real protocol and $\mathcal{F}$ be the map induced by the ideal protocol. Then, the diamond distance between $\mathcal{E}$ and $\mathcal{F}$ gives the maximum distinguishing advantage between $\mathcal{E}$ and $\mathcal{F}$ in a single execution. To illustrate, let an unknown map be either $\mathcal{F}$ or $\mathcal{E}$ with probability 1/2 and any operation or measurement on its input space and its the environment is allowed. Then, the maximum probability of correctly guessing the map, after applying it on an input state once is,

$$p_{success} = \frac{1}{2} + \frac{1}{2}\varepsilon \tag{3.11}$$

A useful interpretation of ε is; *with probability of at least* $1 - \varepsilon$*, the action of the real protocol is indistinguishable from the action of the ideal protocol.*

3.4.3 Composability

The security defined with the diamond distance is composable. This means, if single execution of the protocol is ε-secure, two consecutive execution of the protocol is at least 2ε-secure.

Proof. Let $\|\mathcal{E} - \mathcal{F}\|_\diamond \leq \varepsilon$, using triangular inequality in step (3.13) and the fact that CPTP maps do not increase trace distance [3] in step (3.14),

$$\begin{aligned} \|\mathcal{E} \circ \mathcal{E} - \mathcal{F} \circ \mathcal{F}\|_\diamond &= \|\mathcal{E} \circ (\mathcal{E} - \mathcal{F}) + (\mathcal{E} - \mathcal{F}) \circ \mathcal{F}\|_\diamond && (3.12) \\ &\leq \|\mathcal{E} \circ (\mathcal{E} - \mathcal{F})\|_\diamond + \|(\mathcal{E} - \mathcal{F}) \circ \mathcal{F}\|_\diamond && (3.13) \\ &\leq \|\mathcal{E} - \mathcal{F}\|_\diamond + \|\mathcal{E} - \mathcal{F}\|_\diamond \leq 2\varepsilon && (3.14) \end{aligned}$$

This can be clearly generalized to N executions of the protocol. Different maps that induce diamond distance can also be composed, such as parts of a quantum protocol

or subsequent rounds of different quantum protocols. *Proof.*

$$\|\mathcal{E}_2 \circ \mathcal{E}_1 - \mathcal{F} \circ \mathcal{F}\|_\diamond = \|\mathcal{E}_2 \circ (\mathcal{E}_1 - \mathcal{F}) + (\mathcal{E}_2 - \mathcal{F}) \circ \mathcal{F}\|_\diamond \tag{3.15}$$

$$\leq \|\mathcal{E}_2 \circ (\mathcal{E}_1 - \mathcal{F})\|_\diamond + \|(\mathcal{E}_2 - \mathcal{F}) \circ \mathcal{F}\|_\diamond \tag{3.16}$$

$$\leq \|\mathcal{E}_2 - \mathcal{F}\|_\diamond + \|\mathcal{E}_1 - \mathcal{F}\|_\diamond \leq \varepsilon_2 + \varepsilon_1 \tag{3.17}$$

3.4.4 Partitioning the Epsilon

The analysis of quantum key distribution involves composable quantities such as *correctness*, *secrecy* and *robustness*. Correctness refers to the probability that Alice and Bob obtain identical keys, secrecy refers to the probability that Eve is clueless about the keys that Alice and Bob obtains, robustness refers to the probability that Alice and Bob rejects and the output is discarded. To illustrate, let quantum key distribution protocol induces a CPTP map $\mathcal{E}^{QKD}_{ABE \to K_A K_B TE}$ that maps initial state of Alice, Bob and Eve in combined system ABE to key states in $K_A K_B$. Alice and Bob's public discussions are encoded in the state in T. Let $K_A, K_B \in K \cup \{\perp\}$, $K := \{0,1\}^l$ and $\{\perp\} \cap K = \emptyset$. K is the set of keys Alice and Bob accept after execution and $\{\perp\}$ is the reject set.

$$\mathcal{E}^{QKD}_{ABE \to K_A K_B TE}(|\Psi_{ABE}\rangle\langle\Psi_{ABE}|) = p_\perp |\perp\rangle\langle\perp| \otimes \rho_{TE} + (1 - p_\perp)\rho_{K_A K_B TE} \tag{3.18}$$

where,

$$\rho_{K_A K_B TE} = \sum_{k_a, k_b \in K, t \in T} p_{k_a k_b t} |k_a k_b t\rangle\langle k_a k_b t| \otimes \rho^E_{k_a k_b t} \tag{3.19}$$

Let $\mathcal{F}$ define the ideal map,

$$\mathcal{F}(|\Psi_{ABE}\rangle\langle\Psi_{ABE}|) = \mu_{K_A K_B} \otimes \rho_{TE} \tag{3.20}$$

$$\mu_{K_A K_B} = \frac{1}{2^{2l}} I \tag{3.21}$$

then, ε-security,[12]

$$\frac{1}{2}||\rho_{K_A K_B TE} - \mu_{K_A K_B} \otimes \rho_{TE}||_1 \leq \varepsilon_{secure} \tag{3.22}$$

ε-correctness,[3]

$$(1 - p_\perp) \Pr[K \neq K'] \leq \varepsilon_{\text{corr}} \tag{3.23}$$

ε-secrecy,[3]

$$(1-p_{\perp})\frac{1}{2}\left\|\rho_{K_AK_BTE}-\mu_{K_AK_B}\otimes\rho_{TE}\right\|_1\leq\varepsilon_{secr}. \tag{3.24}$$

and ε-robustness is $\varepsilon_{robust}=p_{\perp}$.

Furthermore, ε-security is upper bounded with ε-correctness and ε-secrecy as,

$$\varepsilon_{secure}\leq\varepsilon_{secr}+\varepsilon_{corr} \tag{3.25}$$

3.4.5 6-state and 8-state Encodings

In a quantum key recycling protocol, the security and the rate of the protocol may depend on the selection, and number of the bases used to encode the binary information on the qubits [13]. As seen in quantum key distribution and quantum key recycling protocols, one can encode one bit of information $g\in\{0,1\}$ in 4-states $|0\rangle,|1\rangle,|+\rangle,|-\rangle$ according to the value of g and the basis basis $b\in\{0,1\}$. These states are commonly called as the BB84 states. Another method of encoding is the *6-state encoding*. Here, the basis key for encoding one bit is $b\in\{0,1,2\}$, and a qubit $\left|\psi_g^b\right\rangle$ is defined as,

$$\left|\psi_0^0\right\rangle:=|+x\rangle\ \left|\psi_0^1\right\rangle:=|+y\rangle\ \left|\psi_0^2\right\rangle:=|+z\rangle \tag{3.26}$$

$$\left|\psi_0^0\right\rangle:=|-x\rangle\ \left|\psi_1^1\right\rangle:=|-y\rangle\ \left|\psi_2^2\right\rangle:=|-z\rangle \tag{3.27}$$

where $|\pm x\rangle|\pm y\rangle|\pm z\rangle$ denote the eigenkets of Pauli matrices $\sigma_x,\sigma_y,\sigma_z$. Finally, g can be encoded into 8-states with four bases $(u,w)\in\{0,1\}\times\{0,1\}$ [13],

$$|\psi_{uwg}\rangle:=E_{uw}|\psi_g\rangle \tag{3.28}$$

$$=(-1)^{gu}\left[(-\sqrt{i})^g\cos\frac{\alpha}{2}|g\oplus w\rangle+(-1)^u(\sqrt{i})^{1-g}\sin\frac{\alpha}{2}|\overline{g\oplus w}\rangle\right] \tag{3.29}$$

where $E_{uw}:=\sigma_{u+2w}$ and $\cos\alpha:=1/\sqrt{3}$. It has been demonstrated that 8-state encoding provides more favorable security bounds and secure transmission rates than 6-state encoding and 4-state encoding for quantum key recycling [13].

3.5 Post-selection

In the Ekert91 version of the protocol Eve prepares the initial state in $\mathcal{S}(\mathcal{H}_{ABE}^{\otimes n})$, and distribute sub-systems A and B to Alice and Bob and keeps E to herself. As a result,

the attack that Eve can make depends on the preparation of the initial state and Eve's action on her sub-system E.

Definition 3.5.1 (Eve's attacks)**.** The *general attacks* refer to the attacks without any constraints.

The *collective attacks* introduces two constraints [14],

- The initial state is of the form $\rho_{ABE} = \sigma^{\otimes n} \in \mathcal{S}(\mathcal{H}_{ABE}^{\otimes n})$.
- The measurement device on AB system is memoryless (results don't effect other measurements) and makes measurements individually. This constraint is not valid for Eve, Eve can make measurements on the combined space and hence the name *collective attacks*.

General attacks introduce many complications on the security proofs. Therefore, the protocols are commonly modeled under collective attacks and generalized to general attacks by the post-selection argument.

Let $\mathcal{E}$ be the map induced by a quantum protocol and act on $\mathcal{S}(\mathcal{H}_{AB}^{\otimes n})$. Let $\mathcal{F}$ be the map induced by the ideal version of the protocol. The post-selection argument [17] states that if $\mathcal{E}$ is invariant under the permutations of the input states, then ε'-security against general attacks implies ε-security against collective attacks.

$$\text{(General attacks) } \varepsilon' := \|\mathcal{E} - \mathcal{F}\|_\diamond \tag{3.30}$$

$$:= \max_{\rho \in \mathcal{S}\left(\mathcal{H}_R \otimes \mathcal{H}_{ABE}^{\otimes n}\right)} \|(I \otimes \mathcal{E} - I \otimes \mathcal{F})(\rho)\|_1 \tag{3.31}$$

$$\text{(Collective attacks) } \varepsilon := \max_{\sigma \in \mathcal{S}(\mathcal{H}_{ABE})} \left\|(\mathcal{E} - \mathcal{F})\left(\sigma^{\otimes n}\right)\right\|_1 \tag{3.32}$$

Post-selection argument,

$$\|\mathcal{E} - \mathcal{F}\|_\diamond \leq (n+1)^{d^2-1} \max_{\sigma \in \mathcal{S}(\mathcal{H}_{ABE})} \left\|(\mathcal{E} - \mathcal{F})\left(\sigma^{\otimes n}\right)\right\|_1 \tag{3.33}$$

$$\implies \varepsilon' \leq (n+1)^{d^2-1} \varepsilon \tag{3.34}$$

where, d denotes the dimension of Alice and Bob subspace $\mathcal{H}_{AB}$. The σ that maximizes (3.32) is a pure state of ABE system and can be written as a 1-dimensional projector,

$$\sigma := |\Psi_{ABE}\rangle\langle\Psi_{ABE}| \tag{3.35}$$

Proof. Let an arbitrary density state be expanded as $\rho = p\rho_0 + (1-p)\rho_1$, ρ_0 and ρ_1 has orhogonal support when ρ is not pure. By using linearity of CPTP maps and the triangular inequality,

$$\|\mathcal{E}(\rho) - \mathcal{F}(\rho)\|_1 \leq p\,\|\mathcal{E}(\rho_1) - \mathcal{F}(\rho_1)\|_1 + (1-p)\,\|\mathcal{E}(\rho_2) - \mathcal{F}(\rho_2)\|_1 \tag{3.36}$$

$$\leq \max\{\|\mathcal{E}(\rho_1) - \mathcal{F}(\rho_1)\|_1, \|\mathcal{E}(\rho_2) - \mathcal{F}(\rho_2)\|_1\} \tag{3.37}$$

Let π be a CPTP map that randomly permutes the n-subspaces (that are in tensor product) of the state space $\mathcal{S}(\mathcal{H}^{\otimes n})$. The CPTP map $\mathcal{E} \circ \pi$ is permutation invariant under its input states if $\mathcal{E}$ does not apply any operation depending on the action of π. Post-selection argument can be used if Alice and Bob starts the protocol by randomly selecting a permutation for their qubits and forgetting about it.

3.6 Noise Symmetrization

The noise symmetrization [3] is a mapping of the initial state that lets us write the reduced state of Alice and Bob as a mixture of pure Bell states. Let Σ be the CPTPM induced by noise symmetrization and $\sigma^{AB} := \Sigma(\mathrm{tr}_E\,\sigma)$, then

$$\sigma^{AB} = \lambda_0 \left|\Psi^-\right\rangle\!\left\langle\Psi^-\right| + \lambda_1 \left|\Phi^-\right\rangle\!\left\langle\Phi^-\right| + \lambda_2 \left|\Psi^+\right\rangle\!\left\langle\Psi^+\right| + \lambda_3 \left|\Phi^+\right\rangle\!\left\langle\Phi^+\right| \tag{3.38}$$

where $\lambda_0 + \lambda_1 + \lambda_2 + \lambda_3 = 1$, $|\Psi^-\rangle\langle\Psi^-|, |\Phi^-\rangle\langle\Phi^-|, |\Psi^+\rangle\langle\Psi^+|, |\Phi^+\rangle\langle\Phi^+|$ are the Bell states and Σ is defined as

$$\Sigma:\ \rho^{AB} \mapsto \frac{1}{4}\sum_{i=0}^{3}(\sigma_i \otimes \sigma_i)\,\mathrm{tr}_E\,\sigma(\sigma_i \otimes \sigma_i) \tag{3.39}$$

for any $\rho^{AB} \in \mathcal{S}(\mathcal{H}^{AB})$ where σ_i 's are the Pauli matrices including the identity, σ_0. $\Sigma(\rho^{AB})$ produces a density matrix diagonal in the Bell basis. Hence, if Alice and Bob publicly selects Pauli matrices, uniformly and independently at random, and apply it on their individual states, their joint state can be written as a simple convex sum over pure Bell states.

Let Alice and Bob apply the same, randomly chosen Pauli matrix to their state σ^{AB} and perform measurement in the same basis. Alice gets the bit x, Bob gets y. If the state produces $x = y$ with a probability γ, their state before the measurement should

be in the form [15],

$$\sigma^{AB} = (1 - \frac{3\gamma}{2}) \left|\Psi^-\right\rangle\!\left\langle\Psi^-\right| + \frac{\gamma}{2} \left|\Phi^-\right\rangle\!\left\langle\Phi^-\right| + \frac{\gamma}{2} \left|\Psi^+\right\rangle\!\left\langle\Psi^+\right| + \frac{\gamma}{2} \left|\Phi^+\right\rangle\!\left\langle\Phi^+\right|. \quad (3.40)$$

3.7 Purification

There is unitary freedom in the purification of σ^{AB}. In [16], the purification is written as,

$$\left|\Psi^{ABE}\right\rangle = \sqrt{1 - \frac{3}{2}\gamma} \left|\Psi^-\right\rangle \otimes |m_0\rangle + \sqrt{\frac{\gamma}{2}} \left(- \left|\Phi^-\right\rangle \otimes |m_1\rangle + i \left|\Psi^+\right\rangle \otimes |m_2\rangle + \left|\Phi^+\right\rangle \otimes |m_3\rangle\right) \quad (3.41)$$

where $\{|m_i\rangle\}_i$ is an orthonormal basis and Eve's Hilbert space can be chosen as $\mathcal{H}^E$.

3.8 Quantum key recycling with Noise

This section is intended as a summary of [5]. Alice and Bob share some secret keys beforehand and publicly agree to use some functions during the executing the protocol. Alice wants to send a plaintext m_{bare} to Bob securely without consuming any key material. Therefore in each round, Alice sends next round keys concatenated with plaintext. If the protocol succeeds, they would gain the same amount key material that they consumed. But if it fails, they consume their keys completely and next round keys would be unsecure to use and hence discarded. In both cases, plaintext is transmitted securely. Considering the odds of failing, Alice and Bob may choose to allocate some part of the plaintext to send key information. So after some number of rounds, if the protocol fails, they can consume the key material sent inside the plaintexts and continue executing the protocol. Description of the protocol is as follows. The assumptions are: Eve has no access to Alice's and Bob's devices,i.e. the information that is generated locally by Alice, and the calculations that Alice and Bob make. Eve has unbounded quantum memory and unbounded computation power. In prepare-and-measure version, Alice prepares n qubits individually, and sends them individually to Bob. In EPR version, Alice and Bob shares n pairs of EPR states and they perform their measurements individually and separately on each

pair. Furthermore, Eve prepares the initial state in EPR version. Eve may perform any measurement on her combined subspace after n rounds, i.e., $\mathcal{H}_E^{\otimes n}$. The initial state of Alice, Bob and Eve is prepared and distributed by Eve. Alice and Bob then publicly choose a permutation, uniformly at random, and apply it to their initial state. This guaranties that their protocol is permutation invariant and allows to make the post-selection argument. Then, Alice and Bob applies the same random Pauli to each of their n qubits individually (noise symmetrization). As a result, the initial state is written as a purification with one free variable which is the error rate γ. This greatly simplifies the subsequent analysis.

3.8.1 Prepare-and-measure version

3.8.2 Before execution

Alice and Bob privately share,

- a basis key $b \in \mathcal{B}^n$
- two MAC keys $k^1_{\mathrm{MAC}}, k^2_{\mathrm{MAC}} \in \{0,1\}^\lambda$
- an extractor seed $u \in \mathcal{U}$
- a one-time-pad key for protecting syndrome $k_{\text{syn}} \in \{0,1\}^a$

Alice and Bob publicly agree to use,

- a pairwise independent hash function $\mathrm{Ext} : \mathcal{U} \times \{0,1\}^n \times \mathcal{B}^n \to \{0,1\}^\ell \times \mathcal{B}^n$
- a MAC function $\Gamma : \{0,1\}^\lambda \times \{0,1\}^{n+\ell+a} \to \{0,1\}^\lambda$
- a linear error correcting code with encoder $\mathrm{Syn} : \{0,1\}^n \to \{0,1\}^a$ and decoder $\mathrm{SynDec} : \{0,1\}^a \to \{0,1\}^n$

3.8.3 During execution

Encryption

Alice, independently from Bob and Eve

- generates a uniformly random bit string $x \in \{0,1\}^n$
- generates a uniformly random key $k \in \{0,1\}^{2\lambda+a}$
- produces a plaintext $m_{bare} \in \{0,1\}^{\ell'}$ where, $\ell' := \ell - 2\lambda - a$

By using the shared key material and her generated material, Alice computes

1. $m = m_{\text{bare}} \| k$. ($m \in \{0,1\}^{\ell}$. "$\|$" denotes concatenation.)
2. $s = k_{\text{syn}} \oplus \text{Syn}(x)$
3. $z \| b' = \text{Ext}(u, x \| b)$
4. $c = m \oplus z$
5. $\tau = \Gamma\left(k^1_{\text{MAC}}, x \| c \| s\right)$

Finally, she encodes x to qubits with shared basis key b

$$|\Psi\rangle = \bigotimes_{i=1}^{n} |\psi_{b_i x_i}\rangle \tag{3.42}$$

and sends $|\Psi\rangle, s, c, \tau$ to Bob.

Decryption

Bob receives $|\Psi'\rangle, s', c', \tau'$ and

1. measures $|\Psi'\rangle$ in the b-basis and obtain $x' \in \{0,1\}^n$,
2. recovers $\hat{x} = x' \oplus \text{SynDec}\left(k_{\text{syn}} \oplus s' \oplus \text{Syn}\, x'\right)$,
3. computes $\hat{z} \| \hat{b}' = \text{Ext}(u, \hat{x} \| b)$ and $\hat{m} = c' \oplus \hat{z}$,
4. accepts if $\tau' = \Gamma\left(k^1_{\text{MAC}}, \hat{x} \, \| c' \| \mid s'\right)$ and syndrome decoding is successful. Reject otherwise.
5. Sends Accept/Reject bit w (if accepts, $w = 0$, if rejects, $w = 1$) and an authentication tag $\chi = \Gamma(k^2_{\text{MAC}}, w)$ to Alice.
6. If Accept, parse $\hat{m}$ as $\hat{m}_{\text{bare}} \| \hat{k}$, as the length of k is known.

3.8.4 After execution

- If Accept, set $b \leftarrow b'$, $(k^1_{\mathrm{MAC}} \| k^2_{\mathrm{MAC}} \| \, k_{\mathrm{syn}}) \leftarrow k$. Re-use u.
- If Reject, refresh $k^1_{\mathrm{MAC}}, k^2_{\mathrm{MAC}}, k_{\mathrm{syn}}, b, u$.

If accept, Alice and Bob send the same amount of key material they consume during the round. Basis key b, mac keys $k^1_{\mathrm{MAC}}, k^2_{\mathrm{MAC}} \in \{0,1\}^\lambda$ and syndrome one time pad $k_{\mathrm{syn}} \in \{0,1\}^a$ are replaced by the sent material, while extractor seed u is re-used. Moreover, Alice sends the plaintext m_{bare} to Bob. If reject, Alice and Bob lose $k^1_{\mathrm{MAC}}, k^2_{\mathrm{MAC}}, k_{\mathrm{syn}}, b, u$ but m_{bare} is still sent. The remaining part proves the security of this quantum key recycling protocol.

3.9 The security proof

The security proof of the protocol is done on the EPR version of the protocol. This also proves the security of the prepare-and-measure version [6]. In prepare-and-measure Alice randomly generates a $x \in \{0,1\}$, encodes x in b-basis and sends it to Bob through a noisy channel. In EPR version, Alice and Bob shares a noisy EPR pair, Alice and Bob measure the qubits in b-basis. Alice's measurement outcome is $x \in \{0,1\}$ and Bob's is $y \in \{0,1\}$. The other steps are the same in both versions. The map induced by EPR version of the protocol is,

$$\mathcal{E} = \mathcal{P} \circ \mathcal{M} \circ \mathcal{I} \circ \Sigma \circ \pi \tag{3.43}$$

Here, π randomly permutes the states as defined in 3.5, Σ randomly applies Pauli operators to each n-partite states 3.39, $\mathcal{I}$ adds the state of the basis key b in tensor product, $\mathcal{M}$ measures Alice and Bob spaces separately in basis b, $\mathcal{P}$ performs post-processing.

The protocol starts with a random permutation therefore the post-processing argument can be used and one can assume Eve prepares n identical and independent states $\sigma^{\otimes n}$.

After noise-symmetrization, $\sigma = \left|\Psi^{ABE}\right\rangle\!\left\langle\Psi^{ABE}\right|$ where

$$\left|\Psi^{ABE}\right\rangle = \sqrt{1-\frac{3}{2}\gamma}\left|\Psi^{-}\right\rangle \otimes |m_0\rangle + \sqrt{\frac{\gamma}{2}}\left(-\left|\Phi^{-}\right\rangle \otimes |m_1\rangle + i\left|\Psi^{+}\right\rangle \otimes |m_2\rangle + \left|\Phi^{+}\right\rangle \otimes |m_3\rangle\right) \quad (3.44)$$

Then Alice and Bob put their basis key in working memory, which is in a maximally mixed state.

$$\mathcal{I}(\sigma^{\otimes n}) = \mathbb{E}_b \left|b\right\rangle\!\left\langle b\right| \otimes \sigma^{\otimes n} \quad (3.45)$$

where $b \in \mathcal{B}$ and $\mathbb{E}_b(.) := \sum_b p_b(.)$, i.e. expectation over the states denoted the by subscript of $\mathbb{E}$.

Alice and Bob measure their states in b-basis which results in,

$$\mathcal{M}(\mathbb{E}_b \left|b\right\rangle\!\left\langle b\right| \otimes \sigma^{\otimes n}) = \mathbb{E}_{bxy} \left|bxy\right\rangle\!\left\langle bxy\right| \otimes \rho^{E}_{bxy} \quad (3.46)$$

where $x, y \in \{0,1\}^n$

$$\rho^{E}_{bxy} := \bigotimes_{i=1}^{n} \sigma^{b_i}_{x_i y_i} \quad (3.47)$$

and,

$$\sigma^{b_i}_{x_i y_i} := \left|E^{b_i}_{x_i y_i}\right\rangle\!\left\langle E^{b_i}_{x_i y_i}\right| . \quad (3.48)$$

Since $\left|E^{b_i}_{x_i y_i}\right\rangle\!\left\langle E^{b_i}_{x_i y_i}\right|$'s are in tensor product, without loss of generality one can define it for the arbitrary $x, y \in \{0,1\}$ and $b \in \mathcal{B}$ where $\mathcal{B}$ only encodes one bit. Then the $\left|E^{b}_{xy}\right\rangle\!\left\langle E^{b}_{xy}\right|$ are defined with a vector v and the vector is defined according to the elements in basis set $\mathcal{B}$. Let unit vector $v := (v_1, v_2, v_3)$, $v_1, v_2, v_3 \in \mathbb{R}$ and $|\boldsymbol{v} \cdot \boldsymbol{m}\rangle$ denotes $v_1 |m_1\rangle + v_2 |m_2\rangle + v_3 |m_3\rangle$, then

$$\sigma^{v}_{xy} := \left|E^{v}_{xy}\right\rangle\!\left\langle E^{v}_{xy}\right| . \quad (3.49)$$

$$|E_{01}^{\boldsymbol{v}}\rangle = \frac{1}{\sqrt{1-\gamma}}\left[\sqrt{1-\frac{3}{2}\gamma}\,|m_0\rangle + \sqrt{\frac{\gamma}{2}}|\boldsymbol{v}\cdot\boldsymbol{m}\rangle\right] \tag{3.50}$$

$$|E_{10}^{\boldsymbol{v}}\rangle = \frac{1}{\sqrt{1-\gamma}}\left[\sqrt{1-\frac{3}{2}\gamma}\,|m_0\rangle - \sqrt{\frac{\gamma}{2}}|\boldsymbol{v}\cdot\boldsymbol{m}\rangle\right] \tag{3.51}$$

$$|E_{00}^{\boldsymbol{v}}\rangle = \frac{1}{\sqrt{2\left(1-v_3^2\right)}}\left[\left(-v_1v_3 - iv_2\right)|m_1\rangle + \left(-v_2v_3 + iv_1\right)|m_2\rangle + \left(1-v_3^2\right)|m_3\rangle\right] \tag{3.52}$$

$$|E_{11}^{\boldsymbol{v}}\rangle = \frac{1}{\sqrt{2\left(1-v_3^2\right)}}\left[\left(-v_1v_3 + iv_2\right)|m_1\rangle + \left(-v_2v_3 - iv_1\right)|m_2\rangle + \left(1-v_3^2\right)|m_3\rangle\right]. \tag{3.53}$$

To exemplify, in 8-state encoding v is defined as[13],

$$v = \frac{-1}{\sqrt{3}}\begin{pmatrix} (-1)^u \\ (-1)^{u+w} \\ (-1)^w \end{pmatrix} \tag{3.54}$$

where $(u,w) \in \{0,1\} \times \{0,1\}$ and $b \in \{(00),(01),(10),(11)\}$. An important property regarding σ_{xy}^b is[5],

$$\mathbb{E}_{xy}\sigma_{xy}^b = \left(1-\frac{3}{2}\gamma\right)|m_0\rangle\langle m_0| + \frac{\gamma}{2}\sum_{i=1}^{3}|m_i\rangle\langle m_i|. \tag{3.55}$$

The measurement is followed by the post-processing operator $\mathcal{P}$. The output state of $\mathcal{P}$ is written with assuming the authentications don't give false positive results. The probability of fail of the MAC functions with key length $\log|k_{MAC}| = \lambda$ is $P(\Gamma(k_{MAC},m') = \Gamma(k_{MAC},m)|m' \neq m) = 2^{-\lambda}$. Assuming this does not occur will add $2^{-\lambda}$ to the trace distance. Therefore, considering Γ is used two times, with separate keys k_{MAC}^1 and k_{MAC}^2 one can assume that authentications are successful by adding $2\cdot 2^{-\lambda}$ to the trace distance.

$$\|\mathcal{E}-\mathcal{F}\|_\diamond = \|\mathcal{E}-\mathcal{E}_{Auth}+\mathcal{E}_{Auth}-\mathcal{F}\|_\diamond \tag{3.56}$$

$$\leq \|\mathcal{E}_{Auth}-\mathcal{E}\|_\diamond + \|\mathcal{E}_{Auth}-\mathcal{F}\|_\diamond \tag{3.57}$$

$$\leq 2\cdot 2^{-\lambda} + \|\mathcal{E}_{Auth}-\mathcal{F}\|_\diamond \tag{3.58}$$

Hence upper bound of the authenticated protocol implies the upper bound of the actual protocol. Note that, authenticated protocol does not involve two MAC keys and

sets $s' = s, c' = c, \omega' = \omega$.

$$\begin{aligned}\mathcal{P}(\rho^{ABE}) = \mathbb{E}_{xyubk_{\text{syn}}} \sum_{zb's} |xyubzb'k_{\text{syn}}\rangle\langle xyubzb'k_{\text{syn}}| \\ \otimes \mathbb{E}_m \sum_{\tilde{b}\tilde{u}c\omega} |\tilde{b}\tilde{u}msc\omega\rangle\langle\tilde{b}\tilde{u}msc\omega| \otimes \rho^E_{bxy} \\ \cdot \delta_{s,k_{\text{syn}}\oplus\text{Syn}\,x}\delta_{z||b',\text{Ext}(u,x||b)}\delta_{c,m\oplus z}\left\{\omega\theta_{xy}\delta_{\tilde{u}u}\delta_{\tilde{b}b'} + \bar{\omega}\overline{\theta_{xy}}\frac{1}{|\mathcal{B}||\mathcal{U}|}\right\}\end{aligned} \tag{3.59}$$

where the success/fail of error correction is denoted by

$$\theta_{xy} := \begin{cases} 1 & \text{if Hamm}(x \oplus \bar{y}) \leq t \\ 0 & \text{otherwise} \end{cases} \tag{3.60}$$

$\text{Hamm}(.)$ denotes the Hamming weight (i.e. the number of non-zero symbols in its input). Hence, if the bit error is less than t, the error correction succeeds ($\theta_{xy} = 1$) and fails otherwise ($\theta_{xy} = 0$). Note that, for error parameter γ and tolerated error t [5],

$$P_{\text{corr}}(t,\gamma) = \mathbb{E}_{xy}\theta_{xy} = \sum_{k=0}^{t} \begin{pmatrix} n \\ k \end{pmatrix} \gamma^k(1-\gamma)^{n-k} \tag{3.61}$$

Some takeaways regarding (3.59),

- If Bob accepts ($w = 1$) the next round keys are $\tilde{b} = b', \tilde{u} = u$, if he rejects ($w = 0$), $\tilde{b}$ and $\tilde{u}$ is chosen uniformly at random from $\mathcal{B}$ and $\mathcal{U}$ respectively.
- k_{syn}, u, b have uniform distributions. This cannot be said for M contains m_{bare}, $m = m_{bare}||k$.

Finally, in accordance with the assumption that Alice's and Bob's devices are only accessible by Alice and Bob, the parts that are residing in their devices, i.e., $XYUBZB'K_{syn}$ will be traced out. The remaining parts are the outputs of the protocol; Eve's subsystem, the public messages and the next round keys, $E\Omega CSM\tilde{B}\tilde{U}$. Hence,

$$\mathcal{E}^{Auth}_{QKR}(\rho^{ABE}) = \text{tr}_{XYUBZB'K_{syn}}\,\mathcal{P}\circ\mathcal{M}(\rho^{ABE}) = \rho^{\tilde{B}\tilde{U}MSC\Omega E} \tag{3.62}$$

$$\begin{aligned}\rho^{\tilde{B}\tilde{U}MSC\Omega E} = \mathbb{E}_{\tilde{b}\tilde{u}ms} \sum_{c\omega} 2^{-\ell} |\tilde{b}\tilde{u}msc\omega\rangle\langle\tilde{b}\tilde{u}msc\omega| \\ \otimes \left[\omega\rho^E_{\tilde{b}\tilde{u}mc,[\omega=1]} + \bar{\omega}\rho^E_{\tilde{b}\tilde{u}mc,[\omega=0]}\right]\end{aligned} \tag{3.63}$$

where,

$$\rho^E_{\tilde{b}\tilde{u}mc,[\omega=1]} := \mathbb{E}_{xy}\theta_{xy}2^\ell \sum_b \delta_{(m\oplus c)\|\tilde{b},\mathrm{Ext}(\tilde{u},x\|b)}\rho^E_{bxy} \tag{3.64}$$

$$\rho^E_{\tilde{b}\tilde{u}mc,[\omega=0]} := \mathbb{E}_{xy}\overline{\theta_{xy}}\mathbb{E}_b\rho^E_{bxy} \tag{3.65}$$

Note that, S is decoupled and uniformly distributed in both $w = 0$ and $w = 1$ because S is one-time padded with k_{syn}.

3.9.1 Ideal protocol

The ideal protocol should decouple next round keys, from Eve's state and public states. Hence it can be defined as replacing $\tilde{B}\tilde{U}K$-state of $\rho^{\tilde{B}\tilde{U}MSC\Omega E}$ with a maximally mixed state. Moreover, if Eve does not know the plaintext m_{bare}, it should also decouple its state from the rest. Let $\mathcal{F}'$ represent the map induced by the ideal protocol when Eve does not know the plaintext and $\mathcal{F}$ when she does. Hence,

$$\mathcal{F}'\left(\sigma^{\otimes n}\right) = \mathcal{R}'\left(\rho^{\tilde{B}\tilde{U}MSC\Omega E}\right) = \mathbb{E}_{\tilde{b}\tilde{u}m}|\tilde{b}\tilde{u}m\rangle\langle\tilde{b}\tilde{u}m| \otimes \rho^{SC\Omega E} \tag{3.66}$$

$$\mathcal{F}\left(\sigma^{\otimes n}\right) = \mathcal{R}\left(\rho^{\tilde{B}\tilde{U}MSC\Omega E}\right) = \mathbb{E}_{\tilde{b}\tilde{u}k}|\tilde{b}\tilde{u}k\rangle\langle\tilde{b}\tilde{u}k| \otimes \rho^{M_{\text{bare}}\,SC\Omega E}. \tag{3.67}$$

Although there seems to be two different ideal maps, because of the 2-universal property of the extractor function (i.e. $\mathbb{E}_{\tilde{u}}\delta_{(m\oplus c)\|\tilde{b},\mathrm{Ext}(\tilde{u},x\|b)} = \frac{1}{2^l|\mathcal{B}|}$), m_{bare} is decoupled from the rest in both ideal states. Hence, $\mathcal{F}\left(\sigma^{\otimes n}\right) = \mathcal{F}'\left(\sigma^{\otimes n}\right)$ [5].

$$\begin{aligned}\rho^{M_{\text{bare}}\,SC\Omega E} = \mathbb{E}_{m_{\text{bare}}}\, |m_{\text{bare}}\rangle\langle m_{\text{bare}}| \otimes \tau^{SC} \\ \otimes \sum_\omega |\omega\rangle\langle\omega| \otimes \left[\omega\rho^E_{[\omega=1]} + \bar{\omega}\rho^E_{[\omega=0]}\right]\end{aligned} \tag{3.68}$$

$$\rho^E_{[\omega=1]} = \mathbb{E}_{xy}\theta_{xy}\mathbb{E}_b\rho^E_{bxy} \tag{3.69}$$

$$\rho^E_{[\omega=0]} = \mathbb{E}_{xy}\bar{\theta}_{xy}\mathbb{E}_b\rho^E_{bxy} \tag{3.70}$$

where τ^{SC} is the maximally mixed state in $\mathcal{S}(\mathcal{H}^{SC})$ space. The trace distance between the actual state and ideal state in the non-asymptotic case i.e. finite n, is as following[5]. Let

$$f(\gamma) := \sqrt{\left(1 - \frac{3}{2}\gamma\right)(1-\gamma)} + \sqrt{\frac{3}{2}\gamma(1+\gamma)} \tag{3.71}$$

then the trace distance between actual state and the ideal state can be upper bounded as,

$$\left\| \left(\mathcal{E}_{\mathrm{QKR}}^{Auth} - \mathcal{F} \right) \left(\sigma^{\otimes n} \right) \right\|_1 = \left\| \rho^{\tilde{B}\tilde{U}KM_{\text{bare}}\,C\Omega E} - \mu^{\tilde{B}\tilde{U}K} \otimes \rho^{M_{\text{bare}}\,C\Omega E} \right\|_1 \tag{3.72}$$

$$\leq \min \left\{ P_{\text{corr}}\left(t, \gamma\right), \frac{1}{2}\sqrt{2^{\ell - n + 2n \log f(\gamma)}} \right\} \tag{3.73}$$

The proof can be found in [5].

CHAPTER 4

NON-ASYMPTOTIC BOUND WITH SMOOTHING

4.1 Smoothing the state

We introduce smoothing on the state after measurement. The state after the measurement is defined as,

$$\rho := \mathcal{M}(\mathbb{E}_b \left|b\right\rangle\!\left\langle b\right| \sigma^{\otimes n}) = \mathbb{E}_{bxy} \left|bxy\right\rangle\!\left\langle bxy\right| \otimes \rho_{bxy}^E \tag{4.1}$$

Let $\mathcal{G} := \{0,1,2,3\}^n$, $g \in \mathcal{G}$, $|m_g\rangle\langle m_g| := \bigotimes_{i=1}^n |m_{g_i}\rangle\langle m_{g_i}|$, $\mathcal{S} \subseteq \mathcal{G}$, $P_{\mathcal{S}} := \sum_{g\in\mathcal{S}} |m_g\rangle\langle m_g|$. We introduce smoothing on ρ by projecting Eve's reduced state onto the eigenspace of $P_{\mathcal{S}}$,

$$\bar{\rho} := \mathbb{E}_{bxy} \left|bxy\right\rangle\!\left\langle bxy\right| \otimes P_{\mathcal{S}} \rho_{bxy}^E P_{\mathcal{S}} \tag{4.2}$$

The trace of $\bar{\rho}$ is as follows,

$$\begin{aligned} \mathrm{tr}(\bar{\rho}) &= \mathrm{tr}\left(\mathbb{E}_{bxy} P_{\mathcal{S}} \rho_{bxy}^E P_{\mathcal{S}}\right) && (4.3)\\ &= \mathrm{tr}\left(P_{\mathcal{S}} \left\{ \left(1 - \frac{3}{2}\gamma\right) |m_0\rangle\langle m_0| + \frac{\gamma}{2} \sum_{i=1}^{3} |m_i\rangle\langle m_i| \right\}^{\otimes n} P_{\mathcal{S}} \right) && (4.4) \end{aligned}$$

Let the set of probabilities $\{p_g\}_{g\in\mathcal{G}}$ be defined as,

$$p_g := \left(1 - \frac{3}{2}\gamma\right)^{n-\mathrm{Hamm}(g)} \left(\frac{\gamma}{2}\right)^{\mathrm{Hamm}(g)} \tag{4.5}$$

where $\mathrm{Hamm}(.)$ the is Hamming weight (i.e. number of non-zero symbols). Then (4.4) becomes

$$\mathrm{tr}\left(P_{\mathcal{S}} \sum_{g\in\mathcal{G}} p_g \left|m_g\right\rangle\!\left\langle m_g\right| P_{\mathcal{S}}\right) \tag{4.6}$$

$$= \mathrm{tr}\left(\sum_{g\in\mathcal{S}} p_g \left|m_g\right\rangle\!\left\langle m_g\right|\right) \tag{4.7}$$

$$= \sum_{g\in\mathcal{S}} p_g \tag{4.8}$$

The following lemma will be used to bound the ℓ_1 distance between ρ and $\bar{\rho}$.

Lemma [3]: *Let $\mathcal{P}(\mathcal{H})$ be the set of non-negative operators on Hilbert space $\mathcal{H}$, $\sigma, \bar{\sigma} \in \mathcal{P}(\mathcal{H})$ such that $\bar{\sigma} = P\sigma P$ for some projector P on $\mathcal{H}$. Then,*

$$\|\sigma - \bar{\sigma}\|_1 \leq 2\sqrt{\mathrm{tr}(\sigma)(\mathrm{tr}(\sigma) - \mathrm{tr}(\bar{\sigma}))} \tag{4.9}$$

Using (4.9), $\mathrm{tr}(\rho) = 1$ and $\mathrm{tr}(\bar{\rho}) = \sum_{g\in\mathcal{S}} p_g$,

$$\|\rho - \bar{\rho}\|_1 < 2\sqrt{1 - \sum_{g\in\mathcal{S}} p_g} \tag{4.10}$$

$$= 2\sqrt{\sum_{g\in\mathcal{G}\setminus\mathcal{S}} p_g} \tag{4.11}$$

4.2 Bounding the security with smoothing

The ℓ_1 distance between the actual state and the ideal state is defined in [5] as,

$$\left\| \left(\mathcal{E}_{\mathrm{QKR}}^{Auth} - \mathcal{F}\right)\left(\sigma^{\otimes n}\right)\right\|_1 = \left\|\left(\mathcal{P} - \mathcal{R}\circ\mathcal{P}\right)\left(\mathbb{E}_{bxy}\left|bxy\right\rangle\!\left\langle bxy\right| \otimes \rho_{bxy}^{E}\right)\right\|_1 \tag{4.12}$$

This can be upper bounded by the ℓ_1 distance on the smooth state,

$$\|\left(\mathcal{P} - \mathcal{R}\circ\mathcal{P}\right)(\rho)\|_1 \tag{4.13}$$

$$= \|\mathcal{P}(\rho - \bar{\rho} + \bar{\rho}) - \mathcal{R}\circ\mathcal{P}(\rho - \bar{\rho} + \bar{\rho})\|_1 \tag{4.14}$$

$$\leq \|\mathcal{P}(\bar{\rho}) - \mathcal{R}\circ\mathcal{P}(\bar{\rho})\|_1 + \|\mathcal{P}(\rho - \bar{\rho}) - \mathcal{R}\circ\mathcal{P}(\rho - \bar{\rho})\|_1 \tag{4.15}$$

$$\leq \|\mathcal{P}(\bar{\rho}) - \mathcal{R}\circ\mathcal{P}(\bar{\rho})\|_1 + \|\mathcal{P}(\rho - \bar{\rho})\|_1 + \|\mathcal{R}\circ\mathcal{P}(\rho - \bar{\rho})\|_1 \tag{4.16}$$

$$\leq \|\mathcal{P}(\bar{\rho}) - \mathcal{R}\circ\mathcal{P}(\bar{\rho})\|_1 + \|\rho - \bar{\rho}\|_1 + \|\rho - \bar{\rho}\|_1 \tag{4.17}$$

$$= \|\mathcal{P}(\bar{\rho}) - \mathcal{R}\circ\mathcal{P}(\bar{\rho})\|_1 + 2\|\rho - \bar{\rho}\|_1 \tag{4.18}$$

The inequality between (4.16) and (4.17) follows from the fact that CPTP maps do not increase ℓ_1 distance [3].

4.3 Post-processing on the smooth state

$$\begin{aligned}\mathcal{P}(\bar{\rho}) = \mathbb{E}_{xyubk_{\text{syn}}} \sum_{zb's} |xyubzb'k_{\text{syn}}\rangle\langle xyubzb'k_{\text{syn}}| \\ \otimes \mathbb{E}_m \sum_{\tilde{b}\tilde{u}c\omega} |\tilde{b}\tilde{u}msc\omega\rangle\langle\tilde{b}\tilde{u}msc\omega| \otimes P_{\mathcal{S}}\rho^E_{bxy}P_{\mathcal{S}} \\ \cdot \delta_{s,k_{\text{syn}}\oplus \text{Syn}\, x}\delta_{z||b',\text{Ext}(u,x||b)}\delta_{c,m\oplus z}\left\{\omega\theta_{xy}\delta_{\tilde{u}u}\delta_{\tilde{b}b'} + \bar{\omega}\overline{\theta_{xy}}\frac{1}{|\mathcal{B}||\mathcal{U}|}\right\}\end{aligned} \tag{4.19}$$

and taking the partial trace,

$$\begin{aligned}\bar{\rho}^{\tilde{B}\tilde{U}MSC\Omega E} = \text{tr}_{XYUBZB'K_{syn}}\, \mathcal{P}(\bar{\rho}) = \mathbb{E}_{\tilde{b}\tilde{u}ms} \sum_{c\omega} 2^{-\ell} |\tilde{b}\tilde{u}msc\omega\rangle\langle\tilde{b}\tilde{u}msc\omega| \\ \otimes \left[\omega\bar{\rho}^E_{\tilde{b}\tilde{u}mc,[\omega=1]} + \bar{\omega}\bar{\rho}^E_{\tilde{b}\tilde{u}mc,[\omega=0]}\right]\end{aligned} \tag{4.20}$$

where,

$$\bar{\rho}^E_{\tilde{b}\tilde{u}mc,[\omega=1]} := \mathbb{E}_{xy}\theta_{xy}2^{\ell}\sum_b \delta_{(m\oplus c)||\tilde{b},\text{Ext}(\tilde{u},x||b)}P_{\mathcal{S}}\rho^E_{bxy}P_{\mathcal{S}} \tag{4.21}$$

$$\bar{\rho}^E_{\tilde{b}\tilde{u}mc,[\omega=0]} := \mathbb{E}_{xy}\overline{\theta_{xy}}\mathbb{E}_b P_{\mathcal{S}}\rho^E_{bxy}P_{\mathcal{S}} \tag{4.22}$$

4.4 "Ideal" post-processing on the smooth state

The ideal map is defined by tracing out $\tilde{B}\tilde{U}K$ and adding a maximally mixed state in $\tilde{B}\tilde{U}K$ after post-processing,

$$\mathcal{R}\circ\mathcal{P}(\bar{\rho}) = \mathcal{R}(\bar{\rho}^{\tilde{B}\tilde{U}MSC\Omega E}) \tag{4.23}$$

$$= \mathbb{E}_{m_{\text{bare}}}\, |m_{\text{bare}}\rangle\langle m_{\text{bare}}| \otimes \tau^{SC} \otimes \sum_{\omega} |\omega\rangle\langle\omega| \otimes \left[\omega\bar{\rho}^E_{[\omega=1]} + \bar{\omega}\bar{\rho}^E_{[\omega=0]}\right] \tag{4.24}$$

where, $\bar{\rho}^E_{[\omega=1]} := \mathbb{E}_{xy}\theta_{xy}\mathbb{E}_b P_{\mathcal{S}}\rho^E_{bxy}P_{\mathcal{S}}$ and $\bar{\rho}^E_{[\omega=0]} := \mathbb{E}_{xy}\bar{\theta}_{xy}\mathbb{E}_b P_{\mathcal{S}}\rho^E_{bxy}P_{\mathcal{S}}$.

4.5 Security of the smooth state

The security of the smooth state is defined by the trace distance between $\mathcal{P}(\bar{\rho})$ and $\mathcal{R} \circ \mathcal{P}(\bar{\rho})$. Let this be denoted by $\bar{D}$,

$$\bar{D} := \frac{1}{2}\|\mathcal{P}(\bar{\rho}) - \mathcal{R} \circ \mathcal{P}(\bar{\rho})\|_1 \tag{4.25}$$

$$= \frac{1}{2}\|\bar{\rho}^{\tilde{B}\tilde{U}MSC\Omega E} - \mathcal{R}(\bar{\rho}^{\tilde{B}\tilde{U}MSC\Omega E})\| \tag{4.26}$$

Then applying $P_{\mathcal{S}}$ on the Eve's subspace on the derivations for bounding the trace distance in [5] we get,

$$2\bar{D} = \|\bar{\rho}^{\tilde{B}\tilde{U}MSC\Omega E} - \mathcal{R}(\bar{\rho}^{\tilde{B}\tilde{U}MSC\Omega E})\|_1 \tag{4.27}$$

$$\begin{aligned} &= \|\mathbb{E}_{\tilde{b}\tilde{u}mc}|\tilde{b}\tilde{u}mc\omega\rangle\langle\tilde{b}\tilde{u}msc\omega| \\ &\quad \otimes (\bar{\rho}^E_{\tilde{b}\tilde{u}mc,[\omega=1]} + \bar{\rho}^E_{\tilde{b}\tilde{u}mc,[\omega=0]} - \bar{\rho}^E_{[\omega=1]} - \bar{\rho}^E_{[\omega=0]})\|_1 \end{aligned} \tag{4.28}$$

$$= \|\mathbb{E}_{\tilde{b}\tilde{u}mc}|\tilde{b}\tilde{u}mc\omega\rangle\langle\tilde{b}\tilde{u}msc\omega| \otimes \left(\bar{\rho}^E_{\tilde{b}\tilde{u}mc,[\omega=1]} - \bar{\rho}^E_{[\omega=1]}\right)\|_1 \tag{4.29}$$

$$= \mathbb{E}_{\tilde{b}\tilde{u}mc}\|\bar{\rho}^E_{\tilde{b}\tilde{u}mc,[\omega=1]} - \bar{\rho}^E_{[\omega=1]}\|_1 \tag{4.30}$$

$$= \mathbb{E}_{\tilde{b}\tilde{u}mc}\,\mathrm{tr}\sqrt{(\bar{\rho}^E_{\tilde{b}\tilde{u}mc,[\omega=1]} - \bar{\rho}^E_{[\omega=1]})^2} \tag{4.31}$$

$$\leq \mathbb{E}_{\tilde{b}mc}\,\mathrm{tr}\sqrt{\mathbb{E}_{\tilde{u}}(\bar{\rho}^E_{\tilde{b}\tilde{u}mc,[\omega=1]} - \bar{\rho}^E_{[\omega=1]})^2} \tag{4.32}$$

By expanding the term inside the square root and using $P_{\mathcal{S}}^2 = P_{\mathcal{S}}$,

$$\mathbb{E}_{\tilde{u}}(P_{\mathcal{S}}\rho^E_{\tilde{b}\tilde{u}mc,[\omega=1]}P_{\mathcal{S}} - P_{\mathcal{S}}\rho^E_{[\omega=1]}P_{\mathcal{S}})^2 \tag{4.33}$$

$$\begin{aligned} &= \mathbb{E}_{\tilde{u}}(P_{\mathcal{S}}\rho^E_{\tilde{b}\tilde{u}mc,[\omega=1]}P_{\mathcal{S}}\rho^E_{\tilde{b}\tilde{u}mc,[\omega=1]}P_{\mathcal{S}} - P_{\mathcal{S}}\rho^E_{[\omega=1]}P_{\mathcal{S}}\rho_{\tilde{b}\tilde{u}mc,[\omega=1]}P_{\mathcal{S}} \\ &\qquad - P_{\mathcal{S}}\rho_{\tilde{b}\tilde{u}mc,[\omega=1]}P_{\mathcal{S}}\rho^E_{[\omega=1]}P_{\mathcal{S}} + P_{\mathcal{S}}\rho^E_{[\omega=1]}P_{\mathcal{S}}\rho^E_{[\omega=1]}P_{\mathcal{S}}) \end{aligned} \tag{4.34}$$

$$= \mathbb{E}_{\tilde{u}}(P_{\mathcal{S}}\rho^E_{\tilde{b}\tilde{u}mc,[\omega=1]}P_{\mathcal{S}}\rho^E_{\tilde{b}\tilde{u}mc,[\omega=1]}P_{\mathcal{S}} - P_{\mathcal{S}}\rho^E_{[\omega=1]}P_{\mathcal{S}}\rho_{\tilde{b}\tilde{u}mc,[\omega=1]}P_{\mathcal{S}}) \tag{4.35}$$

$$= \mathbb{E}_{\tilde{u}}(P_{\mathcal{S}}\rho^E_{\tilde{b}\tilde{u}mc,[\omega=1]}P_{\mathcal{S}}\rho^E_{\tilde{b}\tilde{u}mc,[\omega=1]}P_{\mathcal{S}} - P_{\mathcal{S}}\rho^E_{[\omega=1]}P_{\mathcal{S}}\rho^E_{[\omega=1]}P_{\mathcal{S}}) \tag{4.36}$$

By putting (4.23) into (4.36) with $\rho^E_{bx,[\omega=1]} := \sum_y p_{x|y}\theta_{xy}\rho^E_{bxy}$

$$\begin{aligned} &= \mathbb{E}_{xx'}\sum_{bb'}\left[2^{2\ell}\mathbb{E}_{\tilde{u}}\delta_{m\oplus c||\tilde{b},\mathrm{Ext}(\tilde{u},x\|b)}\delta_{m\oplus c||\tilde{b},\mathrm{Ext}(\tilde{u},x'||b')}\right] \\ &\qquad P_{\mathcal{S}}\rho^E_{bx,[\omega=1]}P_{\mathcal{S}}\rho^E_{b'x',[\omega=1]}P_{\mathcal{S}} - \left(P_{\mathcal{S}}\rho^E_{[\omega=1]}P_{\mathcal{S}}\right)^2 \end{aligned} \tag{4.37}$$

By using the 2-universal property of extractor, i.e. $\mathbb{E}_u \delta_{\mathrm{Ext}(u,x),z}\delta_{\mathrm{Ext}(x'),z'} = \delta_{x,x'}|Z|^{-1} + (1-\delta_{x,x'})|Z|^{-2}$,

$$= \mathbb{E}_{xx'} \sum_{bb'} \left[|\mathcal{B}|^{-2n} + \delta_{bb'}\delta_{xx'} \left(2^{\ell}|\mathcal{B}|^{-n} - |\mathcal{B}|^{-2n} \right) \right] P_{\mathcal{S}} \rho^E_{bx,[\omega=1]} P_{\mathcal{S}} \rho^E_{b'x',[\omega=1]} P_{\mathcal{S}} - \left(P_{\mathcal{S}} \rho^E_{[\omega=1]} P_{\mathcal{S}} \right)^2 \tag{4.38}$$

$$= \mathbb{E}_{xx'} \sum_{bb'} \delta_{bb'}\delta_{xx'} \left(2^{\ell}|\mathcal{B}|^{-n} - |\mathcal{B}|^{-2n} \right) P_{\mathcal{S}} \rho^E_{bx,[\omega=1]} P_{\mathcal{S}} \rho^E_{b'x',[\omega=1]} P_{\mathcal{S}} + \mathbb{E}_{xx'} \sum_{bb'} |\mathcal{B}|^{-2n} P_{\mathcal{S}} \rho^E_{bx,[\omega=1]} P_{\mathcal{S}} \rho^E_{b'x',[\omega=1]} P_{\mathcal{S}} - \left(P_{\mathcal{S}} \rho^E_{[\omega=1]} P_{\mathcal{S}} \right)^2 \tag{4.39}$$

$$= \mathbb{E}_{xx'} \sum_{bb'} \delta_{bb'}\delta_{xx'} \left(2^{\ell}|\mathcal{B}|^{-n} - |\mathcal{B}|^{-2n} \right) P_{\mathcal{S}} \rho^E_{bx,[\omega=1]} P_{\mathcal{S}} \rho^E_{b'x',[\omega=1]} P_{\mathcal{S}} + \left(P_{\mathcal{S}} \rho^E_{[\omega=1]} P_{\mathcal{S}} \right)^2 - \left(P_{\mathcal{S}} \rho^E_{[\omega=1]} P_{\mathcal{S}} \right)^2 \tag{4.40}$$

$$= \left(2^{\ell}|\mathcal{B}|^{n} - 1 \right) \mathbb{E}_{xx'} \mathbb{E}_{bb'} \delta_{bb'}\delta_{xx'} P_{\mathcal{S}} \rho^E_{bx,[\omega=1]} P_{\mathcal{S}} \rho^E_{b'x',[\omega=1]} P_{\mathcal{S}} \tag{4.41}$$

Inside $\rho^E_{bx,[\omega=1]}$ there is $\theta_{xy} \leq 1$ and a sum over non-negative operators ρ^E_{bxy} [5]. Hence, taking $\theta_{xy} = 1$ upper bounds (4.41)

$$\leq \left(2^{\ell}|\mathcal{B}|^{n} - 1 \right) \mathbb{E}_{xx'} \mathbb{E}_{bb'} \delta_{bb'}\delta_{xx'} P_{\mathcal{S}} \rho^E_{bx} P_{\mathcal{S}} \rho^E_{b'x'} P_{\mathcal{S}} \tag{4.42}$$

$$< \left(2^{\ell}|\mathcal{B}|^{n} \right) \mathbb{E}_{xx'} \mathbb{E}_{bb'} \delta_{bb'}\delta_{xx'} P_{\mathcal{S}} \rho^E_{bx} P_{\mathcal{S}} \rho^E_{b'x'} P_{\mathcal{S}} \tag{4.43}$$

$$= (2^{\ell-n}) \mathbb{E}_{bx} P_{\mathcal{S}} \rho^E_{bx} P_{\mathcal{S}} \rho^E_{bx} P_{\mathcal{S}} \tag{4.44}$$

By putting (4.44) into (4.32),

$$\bar{D} < \frac{1}{2}\sqrt{2^{\ell-n}}\, \mathrm{tr} \sqrt{\mathbb{E}_{bx} P_{\mathcal{S}} \rho^E_{bx} P_{\mathcal{S}} \rho^E_{bx} P_{\mathcal{S}}} \tag{4.45}$$

ρ^E_{bx} are non-negative operators so $\mathbb{E}_{bx}\rho^E_{bx} P_{\mathcal{S}} \rho^E_{bx} \leq \mathbb{E}_{bx}\rho_{bx} I \rho_{bx}$ and the square root is operator-monotone. Hence,

$$\leq \frac{1}{2}\sqrt{2^{\ell-n}}\, \mathrm{tr} \sqrt{P_{\mathcal{S}} \mathbb{E}_{bx} \rho^E_{bx} I \rho^E_{bx} P_{\mathcal{S}}} \tag{4.46}$$

$$= \frac{1}{2}\sqrt{2^{\ell-n}}\, \mathrm{tr} \sqrt{P_{\mathcal{S}} \mathbb{E}_{bx} (\rho_{bx})^2 P_{\mathcal{S}}} \tag{4.47}$$

The terms $\mathbb{E}_{bx}(\rho_{bx})^2$(4.49) and $P_{\mathcal{S}} := \sum_{g\in S} |m_g\rangle\langle m_g|$ commute. Hence,

$$= \frac{1}{2}\sqrt{2^{\ell-n}}\, \mathrm{tr}\, P_{\mathcal{S}} \sqrt{\mathbb{E}_{bx} (\rho_{bx})^2} P_{\mathcal{S}} \tag{4.48}$$

where [5],

$$\mathbb{E}_{bx}(\rho_{bx})^2 = \left\{ (1-\gamma) \left(1 - \frac{3}{2}\gamma \right) |m_0\rangle\langle m_0| + \frac{\gamma(1+\gamma)}{6} \sum_{i=1}^{3} |m_i\rangle\langle m_i| \right\}^{\otimes n} \tag{4.49}$$

Let a function $f(\gamma)$ be defined as[5],

$$f(\gamma) := \left\{ \sqrt{(1-\gamma)\left(1-\frac{3}{2}\gamma\right)} + \sqrt{\frac{3}{2}\gamma(1+\gamma)} \right\} \tag{4.50}$$

then, $f(\gamma)^n = \operatorname{tr} \sqrt{\mathbb{E}_{bx}(\rho_{bx})^2}$. Let the set of probabilities $\{q_g\}_{g\in\mathcal{G}}$ be defined as,

$$q_g := \frac{1}{f(\gamma)^n} \left((1-\gamma)\left(1-\frac{3}{2}\gamma\right)\right)^{\frac{1}{2}(n-\mathrm{Hamm}(g))} \left(\frac{\gamma(1+\gamma)}{6}\right)^{\frac{1}{2}\mathrm{Hamm}(g)} \tag{4.51}$$

then the term $\sqrt{\mathbb{E}_{bx}(\rho_{bx})^2}$ in (4.48) can be written as $\sqrt{\mathbb{E}_{bx}(\rho_{bx})^2} = f(\gamma)^n \sum_{g\in\mathcal{G}} q_g \left|m_g\right\rangle\!\left\langle m_g\right|$. Putting this into (4.48),

$$P_{\mathcal{S}} \sqrt{\mathbb{E}_{bx}(\rho_{bx})^2} P_{\mathcal{S}} = f(\gamma)^n \sum_{g\in\mathcal{S}} q_g \left|m_g\right\rangle\!\left\langle m_g\right| \tag{4.52}$$

Finally, putting (4.52) into (4.48) we can write $\bar{D}$ as

$$\bar{D} < \frac{1}{2} \sqrt{2^{\ell-n} f(\gamma)^{2n} (\operatorname{tr} \sum_{g\in\mathcal{S}} q_g \left|m_g\right\rangle\!\left\langle m_g\right|)^2} \tag{4.53}$$

$$= \frac{1}{2} \sqrt{2^{\ell-n+2n\log f(\gamma)+2\log\sum_{g\in\mathcal{S}} q_g}} \tag{4.54}$$

4.6 Security of the actual state

Putting (4.8) and (4.54) into (4.18) we have,

$$D < \frac{1}{2} \left(2^{\ell-n+2n\log f(\gamma)+2\log\left(\sum_{g\in\mathcal{S}} q_g\right)} \right)^{1/2} + \left(\sum_{g\in\mathcal{G}\setminus\mathcal{S}} p_g \right)^{1/2} \tag{4.55}$$

4.7 The asymptotic rate

In the inequality (4.55), the smoothing terms were induced by $\sum_{g\in\mathcal{G}\setminus\mathcal{S}} p_g \left|m_g\right\rangle\!\left\langle m_g\right|$ and $\sum_{g\in\mathcal{S}} q_g \left|m_g\right\rangle\!\left\langle m_g\right|$. Let $P_0 := \left|m_0\right\rangle\!\left\langle m_0\right|$ and $P_1 := \left|m_1\right\rangle\!\left\langle m_1\right| + \left|m_2\right\rangle\!\left\langle m_2\right| + \left|m_3\right\rangle\!\left\langle m_3\right|$ then,

$$\sum_{g\in\mathcal{G}} p_g \left|m_g\right\rangle\!\left\langle m_g\right| = \left(\left(1-\frac{3\gamma}{2}\right) P_0 + \frac{\gamma}{2} P_1 \right)^{\otimes n} \tag{4.56}$$

$$\sum_{g\in\mathcal{G}} q_g \left|m_g\right\rangle\!\left\langle m_g\right| = \frac{1}{f(\gamma)^n} \left(\sqrt{(1-\gamma)\left(1-\frac{3}{2}\gamma\right)} P_0 + \sqrt{\frac{3}{2}\gamma(1+\gamma)} P_1 \right)^{\otimes n} \tag{4.57}$$

Operators (4.56) and (4.57) can be seen as representations of a sequence of n i.i.d. Bernoulli random variables, $G := G_1, G_2, ..., G_n$ with probability mass functions P and Q that are defined on the same probability space $\mathcal{G} = \{0,1\}^n$. Then for any G_i in the random variable sequence G,

$$\mathrm{P}(G_i = 0) = \left(1 - \frac{3\gamma}{2}\right) \mathrm{tr}(P_0) = 1 - \frac{3\gamma}{2} \tag{4.58}$$

$$\mathrm{P}(G_i = 1) = \frac{\gamma}{2} \mathrm{tr}(P_1) = \frac{3\gamma}{2} \tag{4.59}$$

$$\mathrm{Q}(G_i = 0) = \frac{1}{f(\gamma)} \sqrt{(1-\gamma)\left(1 - \frac{3}{2}\gamma\right)} \tag{4.60}$$

$$\mathrm{Q}(G_i = 1) = \frac{1}{f(\gamma)} \sqrt{\frac{3}{2}\gamma(1+\gamma)} \tag{4.61}$$

Let, $p := \mathrm{P}(G_i = 1)$ and $q := \mathrm{Q}(G_i = 1)$ ($p \leq q$ for $0 \leq \gamma \leq 0.5$), $S_n := \sum_{i=1}^{n} G_i$. Then, $Q(S_n)$ and $P(S_n)$ describe two binomial distributions over the same random variable S_n. Let, the set $\mathcal{S}$ be $\{g : \sum_i g_i \leq n\alpha\}$ such that $p < \alpha < q$. Then, by using the Chernoff bound on the term $\sum_{g \in \mathcal{S}} q_g$ in (4.55) we get

$$D \leq \frac{1}{2}\left(2^{\ell - n + 2n \log f(\gamma) + 2 \log e^{\frac{-n(q-\alpha)^2}{2q}}}\right)^{1/2} + \left(\sum_{g \in \mathcal{G} \setminus \mathcal{S}} p_g\right)^{1/2} \tag{4.62}$$

Due to the weak law of large numbers the term $\sum_{g \in \mathcal{G} \setminus \mathcal{S}} p_g$ in (4.62) asymptotically goes to zero for $p < \alpha$. Also, when α is infinitesimally close to p, the term $2 \log e^{\frac{-n(q-\alpha)^2}{2q}}$ takes its minimum value. Selecting α as p in (4.62), defining β as the error correction rate t/n (3.61) [5] and setting γ in the definitions of p and q to β, we can compare the asymptotic rates implied by the distance "without smoothing" (3.72), and "with smoothing" (4.62). The distances (3.72) and (4.62) can be made exponentially small for $l/n < 1 - 2\log f(\beta)$ and $l/n < 1 - 2\log f(\beta) + \frac{(q-p)^2}{q} \log e$ respectively. The terms that are induced by the post-processing, $\mathrm{O}(log(n)/n)$, and the authentication, $2\lambda/n$, asymptotically go to zero. The syndrome length asymptotically goes to $a/n = h(\beta)$. The length of m_{bare} is specified as $\ell' := \ell - 2\lambda - a$ (3.8.3). Hence the asymptotic rates ℓ'/n are; $1 - 2\log f(\beta) - h(\beta)$ without smoothing, and $1 - 2\log f(\beta) + \frac{n(q-p)^2}{q} \log e - h(\beta)$ with smoothing.

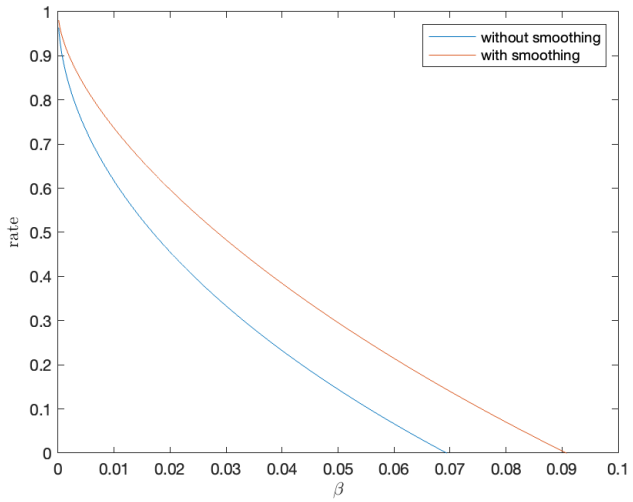

Figure 4.1: Asymptotic rates l'/n: "*with smoothing*", $1-2\log f(\beta)+\frac{n(q-p)^2}{q}\log e-h(\beta)$, and, "*without smoothing*" $1-2\log f(\beta)-h(\beta)$. (3.72), (4.62).

4.8 The non-asymptotic rate

The trace distance between the actual state and the ideal state is given by the minimum of two terms [5],

$$d(\tilde{B}\tilde{U}K \mid M_{\text{bare}}\, C\Omega E) \leq \min\left\{P_{\text{corr}}\,(t,\gamma), \frac{1}{2}\sqrt{2^{\ell-n+2n\log f(\gamma)}}\right\}. \tag{4.63}$$

In [5], an upper bound to d is selected as $d \leq 2^{-\nu}$ where ν is the security parameter. The maximum γ that makes $P_{\text{corr}}\,(t,\gamma) \leq 2^{-\nu}$ is denoted as γ_{max}. Note that, $P_{\text{corr}}\,(t,\gamma)$ is a decreasing function of γ, so when $\gamma \geq \gamma_{max}$ it is apparent that $d \leq 2^{-\nu}$. When $\gamma \leq \gamma_{max}$, observe that, $P_{\text{corr}}\,(t,\gamma) \geq 2^{-\nu}$. Hence, the second term should be upper bounded with $2^{-\nu}$ when $\gamma \leq \gamma_{max}$. The upper bound for γ_{max} is given in [5] by solving the Chernoff bound for γ as

$$\gamma_{\max}(t,\nu) \leq \gamma_0(t,\nu) := \frac{t}{n} + \frac{\nu\ln 2}{n} + \sqrt{2\frac{t}{n}\frac{\nu\ln 2}{n} + \left(\frac{\nu\ln 2}{n}\right)^2}. \tag{4.64}$$

The term $\log f(\gamma_0)$ in (4.63) is an increasing function of γ. Hence for $\gamma \leq \gamma_{max}$, ℓ can be upper bounded as

$$\ell \leq n - 2n\log f(\gamma_0) - 2\nu - 1. \tag{4.65}$$

This gives the non-asymptotic rate for ℓ without smoothing.

For finding the non-asymptotic rate with smoothing, we selecting $\mathcal{S}$ as $\{g : \sum_i g_i \leq n\alpha\}$ and use the upper and lower tail Chernoff bounds on (4.62),

$$D \leq \frac{1}{2}\left(2^{\ell - n + 2n\log f(\gamma) - \frac{n(q-\alpha)^2}{q}\log e}\right)^{1/2} + 2e^{\frac{-n(\alpha-p)^2}{2(p+\alpha)}}. \tag{4.66}$$

We select α that satisfies $e^{\frac{-n(\alpha-p)^2}{2(p+\alpha)}} \leq 2^{\nu'}$ for some $\nu' \in \mathbb{Z}^+$ as

$$\alpha = \frac{n\,p + \ln 2\,\nu' + \sqrt{\ln 2\,\nu'\,(4\,n\,p + \ln 2\,\nu')}}{n}, \tag{4.67}$$

and we select ℓ as,

$$\ell \leq n - 2n\log f(\gamma_0) + \frac{n(q-\alpha)^2}{q}\log e - 2\nu' + 4. \tag{4.68}$$

Putting (4.67) in (4.66) and defining $\nu' := \nu + 2$ we get

$$D \leq 2^{-\nu} \tag{4.69}$$

and using (3.58),

$$\left\|(\mathcal{E}_{\mathrm{QKR}} - \mathcal{F})\left(\sigma^{\otimes n}\right)\right\|_1 \leq 2^{1-\nu} + 2^{1-\lambda}. \tag{4.70}$$

Finally, the non-asymptotic bound on the rate of m_{bare} will be deduced as shown in [5]. Suppose Alice and Bob are willing to tolerate a maximum distance of θ. Each round adds $\eta := 2^{1-\nu} + 2^{1-\lambda}$ to the distance (4.70). Hence, after $N = \lfloor \theta/\eta \rfloor$ rounds of accept they will refresh the extractor and the basis keys, u and b. The amount of bits required are specified as [5] $\log|\mathcal{U}| = \log|\{0,1\}^n \times \mathcal{B}^n|$ and $\log|\mathcal{B}^n|$ will be sent as a part of m_{bare} in each round. The rate of useful classical payload after subtracting all the expenditure can be written as

$$A = 1 - \frac{a}{n} - 2\log f(\gamma_0) + \frac{(q-\alpha)^2}{q}\log e - \frac{30\log(n+1)}{n} - \frac{2\lambda + 2\nu}{n} - \frac{1 + 2\log|\mathcal{B}|}{N}. \tag{4.71}$$

$|\mathcal{B}|$ is chosen as $|\mathcal{B}| = 4$ (8-state encoding), and error correction length a is[18]

$$a = nh(\beta) + \sqrt{n}\Phi^{\mathrm{inv}}\left(10^{-6}\right)\sqrt{\beta(1-\beta)}\log\frac{1-\beta}{\beta}, \tag{4.72}$$

where $h(.)$ denotes the binary entropy function and $\Phi(z) := \int_z^\infty (2\pi)^{-1/2}\exp\left[-x^2/2\right]\mathrm{d}x$. Also note that, $\frac{30\log(n+1)}{n}$ term comes from the post-selection (3.5)

$$\|\mathcal{E}_{\mathrm{QKR}} - \mathcal{F}\|_\diamond \leq (n+1)^{15}\left\|(\mathcal{E}_{\mathrm{QKR}} - \mathcal{F})\left(\sigma^{\otimes n}\right)\right\|_1, \tag{4.73}$$

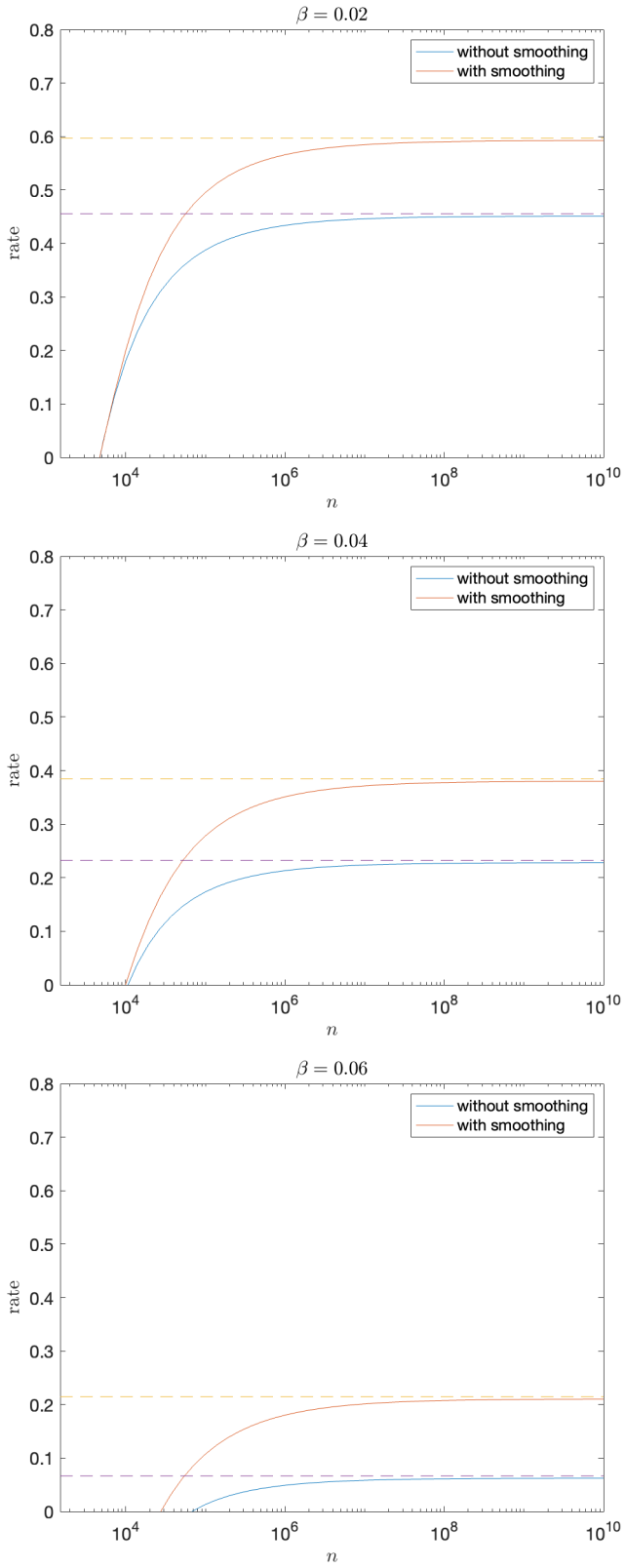

Figure 4.2: Non-asymptotic rates A: (4.71) and "*without smoothing*". Parameters are selected according to [5]: $N = 1000$, $\theta = 2^{-128}$, $\nu = \lambda$ and $\beta = 0.02, 0.04, 0.06$. The dashed lines are the asymptotic rates that are given in (4.7).

CHAPTER 5

CONCLUSION AND DISCUSSIONS

The properties of quantum mechanics, most notably, the no-cloning theorem and the destructive measurement, extended our capabilities of securing our information and let us develop classically impossible schemes like quantum key distribution and quantum key recycling.

This thesis introduces the main concepts and common techniques in quantum mechanics, information theory, and cryptography. Then, it gives a review of quantum key distribution, and quantum key recycling. Since the noise-tolerant quantum key recycling protocol was published in 2019, the protocol has lacked the use of smoothing method on the non-asymptotic security analysis, and this was left as an open question in the paper [5]. It was also argued by the authors that using smoothing can lead to better results on the rate of the protocol. In this thesis, smoothing is done in a particular way that would increase the rate. Finally, it is demonstrated that under the same security conditions, the rate with smoothing is higher than the rate in [5] in the non-asymptotic case.

As a final note, one may consider other ways of doing smoothing, and different concentration bounds in the security proof. One may also demonstrate that the non-asymptotic rate of the protocol converges to the asymptotic rate, which is equal to the rate of quantum key distribution with one-way post-processing [5].

REFERENCES

[1] Davies, D. (1997). A brief history of cryptography. Information Security Technical Report, 2(2), 14-17.

[2] Bennett, C. H., & Brassard, G. (2020). Quantum cryptography: Public key distribution and coin tossing. arXiv preprint arXiv:2003.06557.

[3] Renner, R. (2008). Security of quantum key distribution. International Journal of Quantum Information, 6(01), 1-127.

[4] Bennett, C. H., Brassard, G., & Breidbart, S. (2014). Quantum cryptography II: How to re-use a one-time pad safely even if P= NP. Natural computing, 13(4), 453-458.

[5] Leermakers, D., & Škorić, B. (2019). Security proof for quantum key recycling with noise. Quantum Information and Computation, 19(11-12), 913-934.

[6] Nielsen, M. A., & Chuang, I. (2002). Quantum computation and quantum information.

[7] Leermakers, D. (2021). Quantum key recycling and unclonable encryption. [Phd Thesis 1 (Research TU/e / Graduation TU/e), Mathematics and Computer Science]. Technische Universiteit Eindhoven.

[8] Tomamichel, M., Lim, C. C. W., Gisin, N., & Renner, R. (2012). Tight finite-key analysis for quantum cryptography. Nature communications, 3(1), 1-6.

[9] Ekert, A. K. (1992). Quantum Cryptography and Bell's Theorem. In Quantum Measurements in Optics (pp. 413-418). Springer, Boston, MA.

[10] Damgård, I., Pedersen, T. B., & Salvail, L. (2005, August). A quantum cipher with near optimal key-recycling. In Annual International Cryptology Conference (pp. 494-510). Springer, Berlin, Heidelberg.

[11] Fehr, S., & Salvail, L. (2017, April). Quantum authentication and encryption with key recycling. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 311-338). Springer, Cham.

[12] Portmann, C., & Renner, R. (2022). Security in quantum cryptography. Reviews of Modern Physics, 94(2), 025008.

[13] Skoric, B., & de Vries, M. (2017). Quantum Key Recycling with 8-state encoding (The Quantum One-Time Pad is more interesting than we thought). International Journal of Quantum Information, 15(3), [1750016]. https://doi.org/10.1142/S0219749917500162

[14] Pironio, S., Acín, A., Brunner, N., Gisin, N., Massar, S., & Scarani, V. (2009). Device-independent quantum key distribution secure against collective attacks. New Journal of Physics, 11(4), 045021.

[15] Renner, R., Gisin, N., & Kraus, B. (2005). Information-theoretic security proof for quantum-key-distribution protocols. Physical Review A, 72(1), 012332.

[16] Leermakers, D., & Škorić, B. (2018). Optimal attacks on qubit-based Quantum Key Recycling. Quantum Information Processing, 17(3), 1-31.

[17] Christandl, M., König, R., & Renner, R. (2009). Postselection technique for quantum channels with applications to quantum cryptography. Physical review letters, 102(2), 020504.

[18] Baron, D., Khojastepour, M. A., & Baraniuk, R. G. (2004, November). How quickly can we approach channel capacity?. In Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers, 2004. (Vol. 1, pp. 1096-1100). IEEE.