Practical and Non-Interactive Oblivious Transfer in the Bounded Quantum Storage Model

Final Thesis submitted to the
Indian Statistical Institute, Kolkata
For award of the degree
of

Masters of Technology in Cryptology and Security
by

Sudipa Mandal
CrS2220

under the guidance of

Primary supervisor(s):
Asso. Prof. Frédéric Dupuis
Département d'informatique et de recherche opérationnelle (Diro)
Université de Montréal , Canada
Prof. Louis Salvail
Département d'informatique et de recherche opérationnelle (Diro)
Université de Montréal , Canada

Institute Supervisor:
Asso. Prof. Goutam Paul
Cryptology & Security Research Unit (CSRU)
Indian Statistical Institute, Kolkata

INDIAN STATISTICAL INSTITUTE, KOLKATA
R. C. BOSE CENTRE FOR CRYPTOLOGY AND SECURITY

Université de Montréal, Quebec, Canada
Département d'informatique et de recherche opérationnelle (Diro)

Université de Montréal

Certificate

This is to certify that the thesis entitled "**Practical and Non-Interactive Oblivious Transfer in the Bounded Quantum Storage Model**" submitted by **Sudipa Mandal (CrS2220)** to the Indian Statistical Institute, Kolkata is a record of bonafide research work carried under our supervision and is worthy of consideration for the degree of Master of Cryptology and Security of the Institute.

Asso. Prof. Frédéric Dupuis , Prof. Louis Salvail

Date: 02.07.2024
Place : Université de Montréal
Quebec, Canada

Goutam Paul

Date: 02.07.2024
Cryptology & Security Research Unit (CSRU)
Indian Statistical Institute, Kolkata

Acknowledgements

Primarily, I would like to express my deepest gratitude to my supervisors, Assistant Professor Frederic Dupuis and Professor Luis Salvail. Their insightful feedback, invaluable guidance and support have been crutial in the completion of this thesis. Their profound expertise in quantum cryptography has provided me a strong base and greatly improved my research.

I also want to thank my family for their endless love and support. Their faith in me has been a constant source of motivation and strength.

Lastly, I am grateful to all those who have contributed, directly or indirectly, to this thesis. Your support and contributions have been immensely valuable, and I am sincerely thankful for your assistance.

Thank you all.

Sudipa Mandal

Indian Statistical Institute
Kolkata - 700108 , India.

Abstract

In the bounded quantum storage model (BQSM), it is possible to realize oblivious transfer (OT) non-interactively. However, existing schemes are non-interactive only when the erasure rate is low. Quantum communication, even over short distances, is subject to relatively high erasure rates. The standard approach to handle erasures is to retain only the successfully received pulses and then implement OT, which needs an additional message from the receiver to the sender. Consequently, the OT scheme becomes interactive.

Our research aims to investigate the possibility of achieving non-interactive OT in the BQSM, even under conditions of high erasure rates. To this end, we propose exploring the use of coding techniques, such as fountain codes, with a particular focus on Raptor codes. These codes have the potential to mitigate the need for an additional message from the receiver to the sender, thereby maintaining non-interactivity in the presence of high loss rates.

Contents

1 Introduction

Oblivious Transfer (OT) is a key element in many cryptographic protocols, playing a crucial role for secure multi-party computation and private information retrieval. OT lets a sender transfer one of many possible pieces of information to a receiver so that the sender doesn't know which piece was transferred, and the receiver gets only the desired piece without learning about the others. This special feature makes OT essential for ensuring security and privacy in complex cryptographic tasks.

The study of oblivious transfer (OT) has been very active since its first proposal in 1981 by Rabin [1] in the classical setting. Intriguingly enough, a similar concept(conjugate coding) was proposed by Wiesner using Quantum communication [40] but rejected for publication due to the lack of acceptance in the research community. This technique is the main building block of many important quantum cryptographic protocols. In quantum conjugate coding we encode classical information in two conjugate (non-orthogonal) bases. This allows us to have the distinctive property that measuring on one basis destroys the encoded information on the corresponding conjugate basis.

The first proposal of a quantum oblivious transfer protocol was by Bennett–Brassard–Crépeau–Skubiszewska, known as BBCS Protocol. The importance of OT comes from its wide number of applications.
In the paper [15], Damgaard et al. showed for the first time what happens if we consider protocols where quantum communication is used and we place a bound on the adversary's quantum memory size.
The quantum bounded storage model (QBSM) provides a framework where the adversary's quantum memory is limited, thus offering a different set of security guarantees compared to classical models.
The non-interacive QOT implies One time Program, which is impossible in Quantum model as well as in classical model [18]. But in Bounded Quantum storage model it is possible to implement.

1.1 Motivation

Designing efficient and robust QOT protocols in the QBSM presents significant challenges, particularly in the presence of high erasure rates.
In practical, it is "**almost impossible**" to send qubits without bit loss. When we send data through satellite, most of the data are lost and the receiver gets only a fraction of data.
The standard way we can deal with is the receiver will interact with sender

by sending feedback of the positions of the qubits that he recieved. But as a result, this OT becomes "interactive".
Is it possible to achieve a non-interactive OT when bit loss is high?
The answer is : **Yes**

1.2 Our Contribution

In this thesis, we explore the application of raptor codes to develop a non-interactive QOT protocol that can effectively handle high bit loss. Raptor codes, known for their robust error correction capabilities and low encoding/decoding complexity. By integrating raptor codes into our QOT scheme, we aim to achieve a protocol that can handle high amount of data loss and make the protocol non-interactive.
In the protocol we have assumed that the receiver gets atmost $4k$ qubits out of n qubits and can recover only one message.

During the short period of four months our contributions include:

- **Design and Analysis :** We present the design of a novel QOT protocol using raptor codes, specifically designed to handle high erasure rates in quantum communication systems.
- **Theoretical Proofs :** We provide rigorous theoretical proof of the security and efficiency of our protocol, demonstrating its robustness against adversarial attacks and its ability to maintain security under some condition.

Through this work, we aim to improve quantum cryptography, leading to more secure and reliable quantum communication systems. Our contributions make QOT protocols more resilient and efficient, and they also create new opportunities for future research in quantum cryptography.

1.3 Thesis Outline

In this work we have particularly used [12] [14] [15]. The detailed thesis outline is given below :

- Chapter 2: This chapter introduces fundamental concepts and terminology essential for understanding the thesis. It covers the basics of quantum information, including qubits and superposition, the operations that can be performed on qubits through quantum gates, and the mathematical representation of quantum states via density operators

and the concept of privacy amplification to enhance the security of quantum protocols. Lastly, We introduce the Min-Entropy-Splitting Lemma and discuss techniques for entanglement sampling.

- Chapter 3: This chapter details the concept of Oblivious Transfer (OT), a fundamental primitive in cryptography. It outlines quantum protocols for random 1-2 OT, providing two different approaches for implementing this protocol.
  An overview of Raptor codes, a class of error-correcting codes known for their efficiency and robustness.

- Chapter 4: The core contribution of the thesis is presented here. We introduce a new non-interactive Quantum Oblivious Transfer protocol designed for the Bounded Quantum Storage Model (BQSM), specifically optimized for environments with high erasure rates. The proposed protocol's design and security proof are discussed, highlighting its advantages and potential applications in secure quantum communication.

2 Preliminaries

2.1 Notation and terminology

2.1.1 Quantum Bit

In classical computing, the basic unit of information is called a "bit". In quantum computing, the analogous unit is a "quantum bit", or "qubit". A qubit, upon measurement, collapses to a definite state of a basis. Two bases commonly used are the Z-basis and the X-basis.

The Z-basis is defined as:

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

The X-basis is defined as:

$$|+\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle \right), \quad |-\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle - |1\rangle \right)$$

A basis is an orthonormal set of vectors.

2.1.2 Superposition

Superposition is a fundamental phenomenon in quantum mechanics where a qubit can exist simultaneously in both $|0\rangle$ and $|1\rangle$ states. A qubit in superposition is described by:

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$$

where α and β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$. Upon measurement, $|\phi\rangle$ collapses to $|0\rangle$ with probability $|\alpha|^2$ and to $|1\rangle$ with probability $|\beta|^2$. The state $|-\rangle$ is also a superposition in the Z-basis, with equal probabilities of collapsing to $|0\rangle$ and $|1\rangle$.

2.1.3 Entanglement

Entanglement is a key property of quantum systems where qubits cannot be described independently of each other. The most well-known entangled states are the Bell states:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Measurement of one qubit in an entangled pair instantaneously determines the state of the other, a phenomenon Einstein referred to as "spooky action at a distance".

2.1.4 Quantum Gates and Operations

Quantum gates are unitary transformations that act on qubits. The four fundamental single-qubit gates, known as Pauli matrices, are:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

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

The Hadamard gate (H) is another crucial gate that transforms a qubit between the Z-basis and the X-basis:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Applying the H gate to $|0\rangle$ results in $|+\rangle$, and applying it to $|+\rangle$ results in $|0\rangle$.

Initial State	**I**	**X**	**Y**	**Z**	**H**
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$-\|1\rangle$	$\|+\rangle$
$\|1\rangle$	$\|1\rangle$	$-\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|-\rangle$
$\|+\rangle$	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$
$\|-\rangle$	$\|-\rangle$	$\|+\rangle$	$-\|-\rangle$	$-\|+\rangle$	$\|1\rangle$

Table 1: Examples of five common quantum gates

2.1.5 Density operators

The behavior of a mixed quantum state in a register E is fully described by its density matrix ρ_E. If a quantum state depends on a classical random variable X, it is described by the density matrix ρ_E^x when $X = x$. For an observer without access to X, the behavior is described by:

$$\rho_E = \sum_x P_X(x)\rho_E^x \tag{1}$$

The joint state of the classical X and the quantum register E is described by:

$$\rho_{XE} = \sum_x P_X(x) \left|x\right\rangle \left\langle x\right| \otimes \rho_E^x \tag{2}$$

where $\{|x\rangle\}_{x\in X}$ is the standard (orthonormal) basis of H_X. These joint states, combining classical and quantum parts, are called cq-states. This notation extends to states depending on multiple classical random variables, resulting in ccq-states, cccq-states, etc. For a cq-state ρ_{XE}, if there exists a random variable Y such that ρ_{XYE} satisfies a certain condition, we mean that:

$$\rho_{XE} = \mathrm{tr}_Y(\rho_{XYE}) \tag{3}$$

for some ccq-state ρ_{XYE} satisfying the required condition. The quantum part is independent of X if and only if:

$$\rho_{XE} = \rho_X \otimes \rho_E \tag{4}$$

where $\rho_E^x = \rho_E$ for all x, implying no information about X can be learned by observing only ρ_E.

2.1.6 Classical and Quantum Entropy

We consider the notion of the classical Rényi entropy $H_\alpha(X)$ of order α of a random variable X, as well as its generalization to the Rényi entropy $H_\alpha(\rho)$ of a quantum state ρ. It holds that $H_\alpha(\rho_X) = H_\alpha(X)$ and $H_\alpha(\rho_X) \leq H_\beta(\rho_X)$ if $\alpha \geq \beta$.

The cases that are relevant for us are the classical min-entropy

$$H_\infty(X) = -\log\Big(\max_x P_X(x)\Big)$$

as well as the quantum versions of the max- and collision-entropy

$$H_0(\rho) = \log(\mathrm{rank}(\rho))$$

and

$$H_2(\rho) = -\log\left(\sum_i \lambda_i^2\right),$$

where $\{\lambda_i\}_i$ are the eigenvalues of ρ.

2.1.7 Smooth Rényi Entropy

We briefly recall the notion of (conditional) smooth min-entropy. For more details. Let X be a random variable over the alphabet $\mathcal{X}$ with distribution P_X. The standard notion of min-entropy is given by

$$H_\infty(X) = -\log\left(\max_x P_X(x)\right)$$

and that of max-entropy by

$$H_0(X) = \log\left(|\{x \in \mathcal{X} : P_X(x) > 0\}|\right).$$

More generally, for any event E (defined by $\rho_{E|X}(x)$ for all $x \in \mathcal{X}$), $H_\infty(XE)$ may be defined similarly by simply replacing ρ_X with ρ_{XE}. Note that the "distribution" ρ_{XE} is not normalized; however, $H_\infty(XE)$ is still well-defined.

For an arbitrary $\epsilon \geq 0$, the smooth version $H_\infty^\epsilon(X)$ is defined as follows. $H_\infty^\epsilon(X)$ is the maximum of the standard min-entropy $H_\infty(XE)$, where the maximum is taken over all events E with $\Pr(E) \geq 1-\epsilon$. Informally, this can be understood to mean that if $H_\infty^\epsilon(X) = r$, then the standard min-entropy of X equals r as well, except with probability ϵ. As ϵ can be interpreted as an error probability, we typically require ϵ to be negligible in the security parameter n.

For random variables X and Y, the conditional smooth min-entropy $H_\infty^\epsilon(X|Y)$ is defined as

$$H_\infty^\epsilon(X|Y) = \max_E \min_y H_\infty(XE|Y = y),$$

where the quantification over E is over all events E (defined by $P_{E|XY}$) with $\Pr(E) \geq 1 - \epsilon$.

We will make use of the following **chain rule** for smooth min-entropy:

Lemma 1. *For all $\epsilon, \epsilon' > 0$,*

$$H_\infty^{\epsilon+\epsilon'}(X|Y) \geq H_\infty^\epsilon(XY) - H_0(Y) - \log\left(\frac{1}{\epsilon'}\right).$$

This lemma provides a useful tool for analyzing the relationships between different entropy measures in the presence of conditioning and smoothing parameters.

2.1.8 Bounded Quantum storage

An adversarial player's state may consist of an arbitrary number of qubits, and they may perform arbitrary quantum computations. However, at a certain point in time, we impose a memory bound and his quantum memory is reduced to a certain size. This means that a measurement is applied to the system with the restriction that the resulting quantum state can be stored in at most q qubits. The classical outcome of the measurement can be of arbitrary size and may be classically stored for later use. After this point, the player is again unbounded in terms of quantum memory.

2.1.9 Privacy amplification

An important tool we use is universal hashing. A class $\mathcal{F}_n$ of hashing functions from $\{0,1\}^n$ to $\{0,1\}^l$ is called two-universal if for any pair $x, y \in \{0,1\}^n$ with $x \neq y$, and F uniformly chosen from $\mathcal{F}_n$,

$$\Pr[F(x) = F(y)] \leq \frac{1}{2^l}.$$

Several two-universal classes of hashing functions are such that evaluating and picking a function uniformly and at random in $\mathcal{F}_n$ can be done efficiently.

Theorem 1. *Let $\epsilon \geq 0$. Let ρ_{XUE} be a cq-state, where X is distributed over $\{0,1\}^n$, U is the uniform finite domain $\mathcal{U}$ and register E contains q qubits. Let F be the random variable corresponding to the random choice (with uniform distribution and independent from X) of a member of a two-universal class of hashing functions $\mathcal{F}_n$ form $\{0,1\}^n$ to $\{0,1\}^l$. Then*

$$\delta(\rho_{F(X)FUE}, \frac{1}{2^l} 1 \otimes \rho_{FUE}) \leq \frac{1}{2} \cdot 2^{-\frac{1}{2}(H_\infty^\epsilon(X|U)-q-1)} + 2\epsilon \tag{5}$$

2.2 Uncertainty Relations

Uncertainty relations play a fundamental role in quantum information and in particular in quantum cryptography. Many of the modern security proofs for quantum key distribution and quantum oblivious transfer are based on an uncertainty relation.

They are also at the heart of security proofs in the bounded quantum storage model. An uncertainty relation is a statement about a guaranteed uncertainty in the outcome of a measurement in a randomly chosen basis.

We now state and prove the new entropic uncertainty relation in its most general form. A special case will then be introduced (Corollary 1) and used in the security analysis of all protocols we consider in the following.

Definition 1. *Let $\mathcal{B}$ be a finite set of orthonormal bases in the d-dimensional Hilbert space $\mathcal{H}_d$. We call $h \geq 0$ an average entropic uncertainty bound for $\mathcal{B}$ if every state in $\mathcal{H}_d$ satisfies*

$$\frac{1}{|\mathcal{B}|} \sum_{\vartheta \in \mathcal{B}} H(P_\vartheta) \geq h,$$

where P_ϑ is the distribution obtained by measuring the state in basis ϑ.

Note that by the convexity of the Shannon entropy H, a lower bound for all pure states in $\mathcal{H}_d$ suffices to imply the bound for all (possibly mixed) states.

Theorem 2. *Let $\mathcal{B}$ be a set of orthonormal bases in $\mathcal{H}_d$ with an average entropic uncertainty bound h, and let $\rho \in \mathcal{P}(\mathcal{H}_d^{\otimes n})$ be an arbitrary quantum state. Let $\Theta = (\Theta_1, \ldots, \Theta_n)$ be uniformly distributed over $\mathcal{B}^n$ and let $X = (X_1, \ldots, X_n)$ be the outcome when measuring ρ in basis Θ, distributed over $\{0, \ldots, d-1\}^n$. Then for any $0 < \lambda < \frac{1}{2}$,*

$$H_\infty^\epsilon(X|\Theta) \geq (h - 2\lambda)n$$

with $\epsilon = \exp\left(-\frac{\lambda^2 n}{32(\log(|\mathcal{B}| \cdot d/\lambda))^2}\right)$.

For special case $\mathcal{B} = \{+, \times\}$ is the set of **BB84** bases, $\mathcal{B}$ has entropic uncertainty bound $h = \frac{1}{2}$. Then the theorem 2 gives the following corollary.

Corollary 1. *Let $\rho \in \mathcal{P}(\mathcal{H}_2^{\otimes n})$ be an arbitrary quantum state. Let $\Theta = (\Theta_1, \ldots, \Theta_n)$ be uniformly distributed over $\mathcal{B}^n$ and let $X = (X_1, \ldots, X_n)$ be the outcome when measuring ρ in basis Θ. Then for any $0 < \lambda < \frac{1}{2}$,*

$$H_\infty^\epsilon(X|\Theta) \geq (\frac{1}{2} - 2\lambda)n$$

with $\epsilon = \exp\left(-\frac{\lambda^2 n}{32(\log(|\mathcal{B}|\cdot d/\lambda))^2}\right)$

2.2.1 Min-Entropy-splitting Lemma

Lemma 2. *Let $\epsilon \geq 0$, and let X_0, X_1 be random variables (over possibly different alphabets) with $H_\infty^\epsilon(X_0X_1) \geq \alpha$. Then, there exists a binary random variable C over $\{0,1\}$ such that $H_\infty^\epsilon(X_{1-C}C) \geq \alpha/2$.*

The corollary below follows rather straightforwardly by noting that (for normalized as well as non-normalized distributions) $H_\infty(X_0X_1 \mid Z) \geq \alpha$ holds if $H_\infty(X_0X_1 \mid Z = z) \geq \alpha$ for all z, applying the Min-Entropy-Splitting Lemma, and then using the Chain Rule, Lemma 1.

Corollary 2. *Let $\epsilon \geq 0$, and let X_0, X_1 and Z be random variables such that $H_\infty^\epsilon(X_0X_1 \mid Z) \geq \alpha$. Then, there exists a binary random variable C over $\{0,1\}$ such that*

$$H_\infty^{\epsilon+\epsilon'}(X_{1-C} \mid ZC) \geq \alpha/2 - 1 - \log\bigl(1/\epsilon'\bigr)$$

for any $\epsilon' > 0$.

2.2.2 Entanglement Sampling

Here we consider a system A^n of n qubits. Then we measure each one of these qubits in either the standard basis (labeled 0 with vector $|0\rangle, |1\rangle$) or the Hadamard basis (labeled 1 with vectors $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$). More precisely, choose a random vector $\Theta^n \in \{0,1\}^n$ and measure qubit i in the basis specified by the i-th component of $\Theta^n = \Theta_1, \ldots, \Theta_n$. Call the outcome X_i. An uncertainty relation is a statement about the amount of uncertainty in the random variable $X^n = X_1, \ldots, X_n$ given the knowledge of the basis choice Θ^n. The uncertainty is often measured in terms of the Shannon entropy. However, for the applications we consider here, the measure of uncertainty needs to be stronger, i.e., we should use a higher order entropy like $H_{\min}$ or H_2. Such an uncertainty relation has been established in [14]:

$$H_{\min}^\epsilon(X^n|\Theta^n) \approx \frac{n}{2}. \tag{6}$$

The way this uncertainty relation was used in the context of the bounded storage model was to apply a chain rule to (6) to obtain $H_{\min}^\epsilon(X^n|E\Theta^n) \approx \frac{n}{2} - \log|E|$. There are two reasons for this inequality to be unsatisfactory: it depends on the dimension of E rather than on the correlations between

A^n and E, and it becomes trivial when $H_2(A^n|E) < -\frac{n}{2}$ as this implies $\log|E| > \frac{n}{2}$.

It is simple to see that if the system A^n is maximally entangled with some system E, then the outcome X^n of this measurement can be perfectly predicted by having access to E. In other words, if the conditional entropy $H_2(A^n|E) = -n$, then X^n can be correctly guessed with probability 1. The following theorem provides a converse: if $H_2(A^n|E) > -(1-\epsilon)n$ for $\epsilon > 0$, then X^n cannot be guessed with probability better than $2^{-n\delta(\epsilon)}$ with $\delta(\epsilon) > 0$ whenever $\epsilon > 0$.

Theorem 3. *Let $\rho_{A^nE} \in S(A^nE)$ where A^n is an n-qubit space and define $h_2 = \frac{H_2(A^n|E)_\rho}{n}$. Then we have*

$$H_2(X^n|E\Theta^n)_\rho > n\sigma(h_2) - 1$$

where $\rho_{X^nE\Theta^n} = \frac{1}{2^n}\sum_{x^n\in\{0,1\}^n,\theta^n\in\{0,1\}^n} |x^n\rangle\langle x^n|\langle x^n|H_{\theta^n}\rho_{A^nE}H_{\theta^n}|x^n\rangle|\theta^n\rangle\langle\theta^n|$ is the state obtained when system A^n is measured in the basis defined in the register Θ^n and the function σ is defined by

$$\sigma(h_2) = \begin{cases} h_2 & \text{if } h_2 > \frac{1}{2} \\ g^{-1}(h_2) & \text{if } h_2 < \frac{1}{2} \end{cases}$$

with $g(\alpha) = h(\alpha) + \alpha - 1$.

The following corollary expresses the uncertainty relation described in Theorem 3 in terms of min-entropies, which will be more convenient for cryptographic applications.

Corollary 3. *Using the same notation as in Theorem 3, we have*

$$H_{\min}(X^n|E\Theta^n)_\rho > \frac{1}{2}(n\sigma(h_2) - 1) \tag{7}$$

$$> \frac{1}{2}(n\sigma(h_{\min}) - 1)$$

where $h_{\min} = \frac{H_{\min}(A^n|E)_\rho}{n}$.
Moreover, for any $\epsilon \in (0,1]$, we have

$$H^\epsilon_{\min}(X^n|E\Theta^n)_\rho > n\sigma(h_2) - 1 - \log\frac{2}{\epsilon^2}. \tag{8}$$

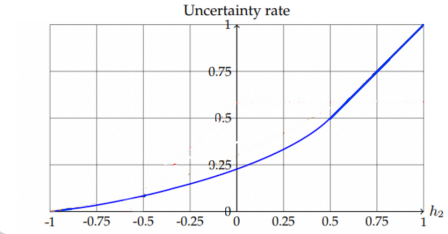

Figure 1: Plot of the function $\sigma(h_2)$ from Theorem 3 giving a lower bound on the uncertainty of the outcome of BB84 measurement as a function of the entropy rate h_2 of the state being measured.

.

3 Oblivious transfer and Raptor codes

3.1 Oblivious transfer

In 1-2 Oblivious Transfer (OT), the sender Alice sends two ℓ-bit strings S_0 and S_1 to the receiver Bob in such a way that Bob can choose which string to receive, but does not learn anything about the other. On the other hand, Alice does not get to know which string Bob has chosen. The common way to build 1-2 OT is by constructing a protocol for (Sender-)Randomized 1-2 OT, which then can easily be converted into an ordinary 1-2 OT. Randomized 1-2 OT essentially coincides with ordinary 1-2 OT, except that the two strings S_0 and S_1 are not input by the sender but generated uniformly at random during the protocol and output to the sender.

For the formal definition of the security requirements of a quantum protocol for Randomized 1-2 OT, let us fix the following notation: Let C denote the binary random variable describing receiver R's choice bit, let S_0, S_1 denote the ℓ-bit long random variables describing sender S's output strings, and let Y denote the ℓ-bit long random variable describing R's output string (supposed to be S_C). Furthermore, for a fixed candidate protocol for Randomized 1-2 OT, and for a fixed input distribution for C, the overall quantum state in the case of a dishonest sender $\tilde{S}$ is given by the ccq-state $\rho_{CYS\tilde{S}}$. Analogously, in the case of a dishonest receiver $\tilde{R}$, we have the ccq-state $\rho_{S_0S_1\tilde{R}}$.

Definition 2. *(Rand 1-2 OT). An ε-secure Rand 1-2 OT is a quantum protocol between S and R, with R having input $C \in \{0,1\}$ while S has no input, such that for any distribution of C, if S and R follow the protocol, then S gets output $S_0, S_1 \in \{0,1\}^\ell$ and R gets $Y = S_C$ except with probability ε, and the following two properties hold:*

- **ε-Receiver-security**: If R is honest, then for any $\tilde{S}$, there exist random variables S'_0, S'_1 such that $\Pr(Y = S'_C) \geq 1-\varepsilon$ and $\delta(\rho_{CS'_0S'_1\tilde{S}}, \rho_C \otimes \rho_{S'_0S'_1\tilde{S}}) \leq \varepsilon$.
- **ε-Sender-security**: If S is honest, then for any $\tilde{R}$, there exists a binary random variable C' such that $\delta(\rho_{S_{1-C'}S_{C'}C'\tilde{R}}, \frac{1}{|2^l|}\mathbf{1} \otimes \rho_{S_{C'}C'\tilde{R}}) \leq \varepsilon$.

If any of the above holds for $\varepsilon = 0$, then the corresponding property is said to hold perfectly. If one of the properties only holds with respect to a restricted class $\mathcal{S}$ of $\tilde{S}$'s respectively $\mathcal{R}$ of $\tilde{R}$'s, then this property is said to hold and the protocol is said to be secure against $\mathcal{S}$ respectively $\mathcal{R}$.

3.1.1 Quantum Protocol for Rand 1-2 OT$^\ell$

Rand 1-2 QOT$^\ell$:

1. Let c be R's choice bit.
2. S picks $x \in_R \{0,1\}^n$ and $\theta \in_R \{+,\times\}^n$, and sends $|x_1\rangle_{\theta_1}, ..., |x_n\rangle_{\theta_n}$ to R.
3. R measures all qubits in basis $[+,\times]^c$. Let $x' \in \{0,1\}^n$ be the result.
4. S picks two hash functions $f_0, f_1 \in_R \mathcal{F}$, announces θ and f_0, f_1 to R, and outputs $s_0 := f_0(x|_{I_0})$ and $s_1 := f_1(x|_{I_1})$ where $I_b := \{i : \theta_i = [+,\times]^b\}$.
5. R outputs $s_c = f_c(x'|_{I_c})$.

In this model dishonest receivers in Rand 1-2 QOT$^\ell$ under the assumption that the maximum size of their quantum storage is bounded. Such adversaries are only required to have bounded quantum storage when Step 3 in Rand 1-2 QOT$^\ell$ is reached; before and after that, the adversary can store and carry out arbitrary quantum computations involving any number of qubits. Let $\mathcal{R}_q$ denote the set of all possible quantum dishonest receivers $\tilde{R}$ in Rand 1-2 QOT$^\ell$ which have quantum memory of size at most q when Step 3 is reached. We stress once more that apart from the restriction on the size of the quantum memory avail able to the adversary, no other assumption is made. In particular, the adversary is not assumed to be computationally bounded and the size of his classical memory is not restricted.

3.1.2 Receiver Security

It is clear by the non-interactivity of Rand 1-2 QOT$^\ell$ that a dishonest sender cannot learn anything about the receiver's choice bit.

proposition 1. *Rand 1-2 QOT $^\ell$ is perfectly receiver-secure.*

This proposition is proven in [14]

3.1.3 Quantum protocol for Rand 1-2 OT$^\ell$

EPR Rand 1-2 QOT $^\ell$:

1. S prepares n EPR pairs each in state $|\Omega\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, and sends one half of each pair to R and keeps the other halves.
2. R measures all qubits in basis $[+, \times]^c$. Let $x' \in \{0,1\}^n$ be the result.
3. S picks random $\theta \in_R \{+, \times\}^n$, and she measures the i-th qubit in basis θ_i. Let $x \in \{0,1\}^n$ be the outcome. S picks two hash functions $f_0, f_1 \in_R \mathcal{F}$, announces θ and f_0, f_1 to R, and outputs $s_0 := f_0(x|_{I_0})$ and $s_1 := f_1(x|_{I_1})$ where $I_b := \{i : \theta_i = [+, \times]^b\}$.
4. R outputs $s_c = f_c(x'|_{I_c})$.

First, we consider a purified version of Rand 1-2 QOT$^\ell$, EPR Rand 1-2 QOT$^\ell$, where for each qubit $|\xi\rangle_{\theta_i}$ the sender S is instructed to send to the receiver, S instead prepares an EPR pair $|\Phi\rangle = \sqrt{\frac{1}{2}}(|00\rangle + |11\rangle)$, and sends one part to the receiver while keeping the other. Only when Step 3 is reached and $\tilde{R}$'s quantum memory is bound to γn qubits, S measures her qubits in basis $\theta \in_R \{+, \times\}^n$. It is easy to see that for any $\tilde{R}$, EPR Rand 1-2 QOT$^\ell$ is equivalent to the original Rand 1-2 QOT$^\ell$, and it suffices to prove sender-security for the former. Indeed, S's choices of θ and f_0, f_1, together with the measurements all commute with R's actions. Therefore, they can be performed right after Step 1 with no change for R's view. Modifying EPR Rand 1-2 QOT$^\ell$ that way results in Rand 1-2 QOT$^\ell$.

3.2 Modeling Dishonest Receivers

In our protocol, we consider dishonest receivers within the context of QOT and EPR-QOT, assuming their quantum storage capacity is limited. These adversaries must have bounded quantum storage only upon reaching step 4 of the (EPR-)QOT protocol. Prior to this, the adversary can store and execute quantum computations with any number of qubits. Besides the restriction on the quantum memory size, we make no other assumptions about the adversary. Specifically, the adversary is not assumed to be computationally bounded, nor is there any limitation on its classical memory capacity.

Definition 3. *We denote by R_γ the set of all possible dishonest quantum receivers $\{\tilde{R}_n\}_{n>0}$ in QOT or EPR-QOT, where each $\tilde{R}_n$ has a quantum memory of size at most γn when step 4 is reached.*

Generally, the adversary $\tilde{R}$ is permitted to perform any quantum computation that compresses the n qubits received from S into a quantum register M of size at most γn upon reaching step 4. More precisely, this compression is carried out by a unitary transformation C acting on the received quantum state and an ancillary system of arbitrary size. The compression involves a measurement, assumed to be in the computational basis without loss of generality. Before initiating step 4, the adversary applies the unitary transformation C as follows:

$$2^{-n/2} \sum_{x\in\{0,1\}^n} |x\rangle \otimes C|x\rangle|0\rangle \to 2^{-n/2} \sum_{x\in\{0,1\}^n} |x\rangle \otimes \sum_y \alpha_{x,y}|\phi_{x,y}\rangle_M |y\rangle_Y,$$

where for each x,

$$\sum_y |\alpha_{x,y}|^2 = 1.$$

A measurement in the computational basis is then applied to register Y, yielding the classical outcome y. The result is a quantum state in register M of size γn qubits. For simplicity, we ignore the value of y in the notation. Thus, the normalized state of the system, in its most general form when step 4 of EPR-QOT is reached, is:

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle \otimes |\phi_x\rangle_M,$$

where

$$\sum_x |\alpha_x|^2 = 1.$$

We will prove security for any such state $|\psi\rangle$, hence it is safe to omit the dependency on y in our notation.

Theorem 4. *Rand 1-2 QOT$^\ell$ is ϵ-sender-secure against R_q for a negligible (in n) ϵ if $n/4 - 2\ell - q \in \Omega(n)$.*

3.3 Raptor codes

An algorithm is given for constructing from a given Raptor Code of parameters $(k, C, \Omega(x))$ a systematic version of the code. First, a set of k positions is computed, which will be the positions of the systematic output symbols. This is done by considering the generator matrix G of the pre-code and the generator matrix S of the first $k(1+\epsilon)$ symbols of the LT code. Using Gaussian elimination, k rows of SG which form a full rank square submatrix R are identified. These rows correspond to the positions of the systematic output symbols.

Encoding of the first $k(1+\epsilon)$ symbols is done by first left-multiplying the vector of input symbols with GR^{-1} to obtain the vector u, and then left-multiplying the result with S. Subsequent output symbols are obtained by application of the LT code to the vector u.

Decoding is done by applying the decoding algorithm of the original Raptor Code to obtain a vector of symbols y. The original input symbols are then given by Ry.

4 Non interactive QOT in BQSM with high erasure rate

In recent advancements of Quantum Oblivious Transfer (QOT) protocols, mostly the focus has been on scenarios with low erasure rates, typically addressing bit loss at a manageable level. However, real-world quantum communication systems often face high erasure rates, leading to substantial bit loss that can severely impact the reliability and security of QOT protocols. Our work aims to address this gap by developing a robust QOT protocol that remains secure and efficient even under high erasure conditions.

Assumption : We specifically target a scenario where the receiver, R, obtains at least $2(1+\delta)k$ bits but not more than $4k$ bits. This constraint is crucial; if R were to receive more than $4k$ bits, R could potentially recover both messages, undermining the security of the protocol.

In our Protocol the formal definition is same as before, i.e., **Definition 2**.

4.1 Our Proposed Protocol

4.1.1 Quantum protocol for random 1-out-of-2 OT^ℓ

Rand 1-2 QOT^ℓ:

1. Let c be R's choice bit.
2. S picks $x \in_R \{0,1\}^n$ and $\theta \in_R \{+,\times\}^n$, and sends $|x_1\rangle_{\theta_1}, ..., |x_n\rangle_{\theta_n}$ to R.
3. Due to high erasure rate let R gets m qubits, where $2(1+\delta)k \leq m < 4k$. R measures all qubits in basis $[+,\times]^c$. Let $x' \in \{0,1\}^m$ be the result.
4. Let S picks $z_0, z_1 \in_R \{0,1\}^k$. S computes $w_0 = rapt(z_0) \oplus x_0$ and $w_1 = rapt(z_1) \oplus x_1$ where for $rapt(z_C)$ S takes first n bits for $c \in \{0,1\}$. S picks two hash functions $f_0, f_1 \in_R \mathcal{F}$, announces $\theta, f_0, f_1, w_0, w_1$ to R, and outputs $s_0 := f_0(x_0)$ and $s_1 := f_1(x_1)$ where x_0 ans x_1 are the sequence of bits encoded by $+$ and $\times$
5. R recovers z_c from w_c. Then computes $x_c = rapt(z_c) \oplus w_c$ and outputs $s_c = f_c(x_c)$.

In the simple protocol for random 1-2 QOT$^\ell$, at first receiver R chooses a bit c from 0 or 1. The sender S first randomly chooses a n bit string x from $\{0,1\}^n$ and encodes this string with randomly chosen basis sequence from $\theta \in_R \{+,\times\}^n$. Let x_0 and x_1 be sequence of bits encoded by $+$ and $\times$ respectively. The sender S sends random BB84 states to the receiver R, who gets a fraction of n bits due to high erasure rate and measures all received qubits according to his choice bit c (for $c = 0$ he chooses $+$ and for $c = 1$ he chooses $\times$). S then picks randomly two k bit strings z_0, z_1 from $\{0,1\}^k$ and applies raptor code on z_0 and z_1. Then takes first n bits of $rapt(z_0)$ and first n bits of $rapt(z_1)$. Then computes $w_0 = rapt(z_0) \oplus x_0$ and $w_1 = rapt(z_1) \oplus x_1$. S then picks two functions f_0, f_1 randomly from a fixed two-universal class of hash functions $\mathcal{F}$ from $\{0,1\}^n$ to $\{0,1\}^\ell$, where ℓ is to be determined later, and applies them to the bits encoded in the $+$ respectively the bits encoded in the $\times$-basis to obtain the output strings s_0 and s_1. Note that we may apply a function $f \in \mathcal{F}$ to a $n'-$bit string with $n' < n$ by padding it with zeros (which does not decrease its entropy). S announces the encoding bases, w_0, w_1 and the hash functions to the receiver who then can compute s_c. Intuitively, a dishonest receiver who cannot store all the qubits until the right bases are announced, will measure some qubits in the wrong basis and thus cannot learn both strings simultaneously.

4.1.2 Proof scetch for Rand 1-2 QOT$^\ell$

Theorem 5. *Rand 1-2 QOT$^\ell$ is ϵ-secure against R_q for a negligible (in n) ϵ if*

$$\frac{n\sigma(h_2)}{2} - 2l - q \in \Omega(n)$$

Proof. For better clarity, we present a brief overview of the proof here, with the detailed proof, addressing all the ϵ terms, provided in the following section.

Proof (Overview): Let X represent the random variable for the sender's choice of x, with the distribution of X conditioned on the classical information $\tilde{R}$ obtained by measuring all but γm qubits. Using a standard purification argument, as in the previous chapter, we show that X can be obtained by measuring a quantum state in a randomly chosen basis $\theta \in_R \{+,\times\}^n$, represented by the random variable Θ: for each qubit $|x_i\rangle_{\theta_i}$ that the sender S needs to send to R, S prepares an EPR pair $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, sends one part to R while keeping the other, and measures her qubits in Step 3.

The uncertainty relation, as stated in Corollary 3, indicates that the smooth min-entropy of X given $W_0W_1\Theta$ is approximately $n\sigma(h_2) - 1$. Let

X_0 and X_1 be the substrings of X composed of the bits encoded in the $+$ or $\times$ basis, respectively. The Min-Entropy-Splitting Lemma, specifically Corollary 2, implies the existence of a binary variable C' such that $X_{1-C'}$ has approximately $\frac{n\sigma(h_2)-1}{2}$ bits of smooth min-entropy given $\Theta W_0 W_1$ and C'.

Given the random and independent selection of hash functions F_0, F_1 and applying the Chain Rule, Lemma 1, $X_{1-C'}$ retains about $\frac{n\sigma(h_2)-1}{2} - 1 - \ell$ bits of smooth min-entropy when conditioned on Θ, C', W_0, W_1 $F_{C'}$, $F_{C'}(X_{C'})$,. The Privacy Amplification Theorem 1 then ensures that $S_{1-C'} = F_{1-C'}(X_{1-C'})$ is nearly random, given Θ, C', $F_{C'}$, W_0, W_1, $S_{C'}$, $F_{1-C'}$, and $\tilde{R}$'s quantum state of size q, provided $\frac{n\sigma(h_2)-1}{2} - 1 - 2\ell - q$ is positive and scales linearly with n. □

4.1.3 Protocol for EPR-based Rand 1-2 QOT$^\ell$

EPR Rand 1-2 QOT$^\ell$:

1. S prepares n EPR pairs each in state $|\Omega\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, and sends one half of each pair to R and keeps the other halves.

2. Due to high erasure rate let R gets m qubits, where $2(1+\delta)k \leq m < 4k$. R measures all qubits in basis $[+, \times]^c$. Let $x' \in \{0,1\}^m$ be the result.

3. S picks random $\theta \in_R \{+, \times\}^n$, and she measures the i-th qubit in basis θ_i. Let $x \in \{0,1\}^n$ be the outcome. Let x_0 be the result for $+$ and x_1 be the result for $\times$.
   Let S picks $z_0, z_1 \in_R \{0,1\}^k$. S computes $w_0 = rapt(z_0) \oplus x_0$ and $w_1 = rapt(z_1) \oplus x_1$ where for $rapt(z_C)$ S takes first n bits for $C \in \{0,1\}$. S picks two hash functions $f_0, f_1 \in_R \mathcal{F}$, announces $\theta, f_0, f_1, w_0, w_1$ to R, and outputs $s_0 := f_0(x_0)$ and $s_1 := f_1(x_1)$

4. R recovers z_c from w_c. Then computes $x_c = rapt(z_c) \oplus w_c$ and outputs $s_c = f_c(x_c)$.

Consider the common quantum state in EPR Rand 1-2 QOT l after $\tilde{R}$ has measured all but γm of his qubits. Let X be the random variable that describes the outcome of the sender measuring her part of the state in random basis Θ, and let E be the random state that describes $\tilde{R}$'s part of the state. Also, let F_0 and F_1 be the random variables that describe the random and

independent choices of $f_0, f_1 \in F$. Let X_b be $X_b = X|_{\{i:\Theta_i=[+,\times]_b\}}$ (padded with zeros so it makes sense to apply F_b).Finally Let S picks $z_0, z_1 \in_R \{0,1\}^k$. S computes $w_0 = rapt(z_0) \oplus x_0$ and $w_1 = rapt(z_1) \oplus x_1$ where for $rapt(z_c)$ S takes first n bits for $C \in \{0,1\}$. Let Z_0, Z_1 be random variables for z_0, z_1 respectively. So W_0, W_1 are random variables for w_0, w_1 respectively.

4.2 Security proof

Choose ϵ, ϵ', and κ all positive, but small enough such that

$$\gamma m \leq \frac{1}{2}(n\sigma(h_{\min}) - log\frac{2}{\epsilon^2} + 4\log\epsilon') - \kappa n - 2\ell - 1. \tag{9}$$

Step 1 : From the uncertainty relation (Corollary 3) $[H^{\epsilon}_{\min}(X^n|E\Theta^n)_\rho > n\sigma(h_2) - 1 - \log\frac{2}{\epsilon^2}]$, we know that

$$H^{\epsilon}_{\infty}(X_0X_1|\Theta W_0W_1) \geq (n\sigma(h_{\min}) - 1) - \log\frac{2}{\epsilon^2} \tag{10}$$

for ϵ exponentially small in n. Here system E is acting as information W_0, W_1.

Step 2 : Therefore, by Corollary 2 (Min-entropy Splitting Lemma) $[H^{\epsilon+\epsilon'}_{\infty}(X_{1-C} \mid ZC) \geq \alpha/2 - 1 - \log(1/\epsilon')$ for any $\epsilon' > 0]$ applying on equation (10), there exists a binary random variable C' such that for $\epsilon' = 2^{-\lambda' n}$, it holds that

$$H^{\epsilon+\epsilon'}_{\infty}(X_{1-C'}|\Theta W_0W_1C') \geq \frac{(n\sigma(h_{\min}) - 1) - \log\frac{2}{\epsilon^2}}{2} - 1 - \log\frac{1}{\epsilon'}. \tag{11}$$

Step 3 : We denote by the random variables F_0, F_1 the sender's choices of hash functions. It is clear that we can condition on the independent $F_{C'}$ and using equation (11) we can write

$$H^{\epsilon+2\epsilon'}_{\infty}(X_{1-C'}F_{C'}(X_{C'})|\Theta F_{C'}W_0W_1C') \geq \frac{(n\sigma(h_{\min}) - 1) - \log\frac{2}{\epsilon^2}}{2} - 1 - \log\frac{1}{\epsilon'}$$

and use the chain rule (Lemma 1)$[H^{\epsilon+\epsilon'}_{\infty}(X|Y) \geq H^{\epsilon}_{\infty}(XY) - H_0(Y) - \log\left(\frac{1}{\epsilon'}\right).]$ to obtain

$$\begin{aligned} H^{\epsilon+2\epsilon'}_{\infty}(X_{1-C'}|\Theta F_{C'}(X_{C'})F_{C'}W_0W_1C') &\geq H^{\epsilon+2\epsilon'}_{\infty}(X_{1-C'}F_{C'}(X_{C'})|\Theta F_{C'}W_0W_1C') \\ &\quad - H_0(F_{C'}(X_{C'})|F_{C'}W_0W_1C') - \log\frac{1}{\epsilon'} \\ &\geq \frac{(n\sigma(h_{\min}) - 1) - \log\frac{2}{\epsilon^2}}{2} - 1 - \log\frac{1}{\epsilon'} - \ell - \log\frac{1}{\epsilon'} \\ &= \frac{(n\sigma(h_{\min}) - 1) - \log\frac{2}{\epsilon^2}}{2} - 1 - \ell - 2\log\frac{1}{\epsilon'} \end{aligned}$$

$$= \frac{(n\sigma(h_{\min}) - 1) - \log \frac{2}{\epsilon^2}}{2} - 1 - \ell + 2\log \epsilon'$$
$$= \frac{(n\sigma(h_{\min}) - 1) - \log \frac{2}{\epsilon^2} + 4\log \epsilon'}{2} - 1 - \ell$$
$$= \frac{(n\sigma(h_{\min}) - 1) - \log \frac{2}{\epsilon^2} + 4\log \epsilon'}{2} - 1 - 2\ell + \ell$$

So, we get

$$H_\infty^{\epsilon+2\epsilon'}(X_{1-C'}|\Theta F_{C'}(X_{C'})F_{C'}W_0W_1C') \geq \frac{(n\sigma(h_{\min}) - 1) - \log \frac{2}{\epsilon^2} + 4\log \epsilon'}{2} - 1 - 2\ell + \ell \quad (12)$$

Now, using the equation (9) in the above inequality we get,

$$H_\infty^{\epsilon+2\epsilon'}(X_{1-C'}|\Theta F_{C'}(X_{C'})F_{C'}W_0W_1C') \geq \gamma m + \ell + \kappa n$$

by the choice of ϵ, ϵ', and κ.

Step 4 : We can now apply privacy amplification in form of Theorem 3 $[\delta(\rho_{F(X)FUE}, \frac{1}{2^l}1 \otimes \rho_{FUE}) \leq \frac{1}{2} \cdot 2^{-\frac{1}{2}(H_\infty^\epsilon(X|U)-q-1)} + 2\epsilon]$ to obtain

$$\delta(\rho_{F_{C'}(X_{C'})F_{1-C'}(X_{1-C'})F_{C'}F_{1-C'}\theta W_0W_1}, 1 \otimes \rho_{F_{C'}(X_{C'})F_{C'}F_{1-C'}\Theta C'W_0W_1})$$
$$\leq \frac{1}{2}2^{-\frac{1}{2}\left(H_\infty^{\epsilon+2\epsilon'}(X_{1-C'}|\Theta F_{C'}(X_{C'})F_{C'}W_0W_1C') - \gamma m - l\right)} + 2(\epsilon + 2\epsilon')$$
$$\leq \frac{1}{2}2^{-\frac{1}{2}(\gamma m + \ell + \kappa n - \gamma m - l)} + 2(\epsilon + 2\epsilon') \qquad [using (12)]$$

So, we obtain,

$$\delta(\rho_{F_{C'}(X_{C'})F_{1-C'}(X_{1-C'})F_{C'}F_{1-C'}\theta W_0W_1}, 1 \otimes \rho_{F_{C'}(X_{C'})F_{C'}F_{1-C'}\Theta C'W_0W_1}) \leq \frac{1}{2}2^{-\frac{1}{2}\kappa n} + 2\epsilon + 4\epsilon',$$

which is negligible.

5 Conclusion

In this thesis, we have analyzed a non-interactive quantum oblivious transfer (QOT) protocol that effectively handles high bit loss when sending bits through satellites by leveraging the robust error correction capabilities of raptor codes and using min-entropy sampling properly.

Finally, we have achieved a non-interactive QOT protocol when the receiver gets only a fraction (assuming atmost $4k$ bits out of n bits) of qubits, does not send any feedback to the sender and keeping the whole process non-interactive. So our protocol addresses the critical challenges posed by data loss in quantum communication systems through satellite, providing a secure and non-interactive solution within the bounded quantum storage model (BQSM).

6 Future Work

In this thesis, we assumed that if the receiver gets not more than $4k$ bits, then the proposed protocol for 1-2 QOT^{ℓ} will hold properly. This assumption has served as a foundational aspect of our protocol. However, an interesting direction for future research is to explore the scenario where the adversary obtains more than $4k$ bits.

One next possible approach to address this challenge is to develop a new protocol using an extra basis i.e., circular basis so that this protocol remains secure and non-interactive even when the adversary has access to more than $4k$ bits.

References

[1] Rabin M.O. *How to Exchange Secrets with Oblivious Transfer.* Aiken Computation Laboratory, Harvard University; Cambridge, MA, USA: 1981. Technical Report TR-81.

[2] N. Alon and J. Spencer. *The Probabilistic Method*. Series in Discrete Mathematics and Optimization. Wiley-Interscience, 2nd edition, 2000.

[3] K. Azuma. Weighted sums of certain dependent random variables. *Tohoku Mathematical Journal*, 19:357–367, 1967.

[4] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179, 1984.

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

[6] C. H. Bennett, G. Brassard, and J.-M. Robert. Privacy amplification by public discussion. *SIAM J. Comput.*, 17(2):210–229, 1988.

[7] I. Bialynicki-Birula. Formulation of the uncertainty relations in terms of the Renyi entropies. *Physical Review A*, 74:052101, 2006.

[8] I. Bialynicki-Birula and J. Mycielski. Uncertainty relations for information entropy. *Communications in Mathematical Physics*, 129(44), 1975.

[9] C. Cachin. Smooth entropy and Renyi entropy. In *Advances in Cryptology—EUROCRYPT '97*, volume 1233 of *Lecture Notes in Computer Science*, pages 193–208. Springer, 1997.

[10] J. L. Carter and M. N. Wegman. Universal classes of hash functions. In *9th Annual ACM Symposium on Theory of Computing (STOC)*, pages 106–112, 1977.

[11] C. Crepeau, G. Savvides, C. Schaffner, and J. Wullschleger. Information-theoretic conditions for two-party secure function evaluation. In *Advances in Cryptology—EUROCRYPT '06*, volume 4004 of *Lecture Notes in Computer Science*, pages 538–554. Springer, 2006.

[12] Frédéric Dupuis, Omar Fawzi, and Stephanie Wehner, *Entanglement Sampling and Applications*, IEEE transactions on information theory, VOL. 61, NO. 2, February 2015

[13] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 24(3):339–348, May 1978.

[14] I. B. Damgaard, S. Fehr, R. Renner, L. Salvail, and C. Schaffner. A tight high-order entropic quantum uncertainty relation with applications. In *Advances in Cryptology—CRYPTO '07*, volume 4622 of *Lecture Notes in Computer Science*, pages 360–378. Springer, 2007.

[15] I. B. Damgaard, S. Fehr, L. Salvail, and C. Schaffner. Cryptography in the bounded quantum-storage model. In *46th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 449–458, 2005.

[16] I. B. Damgaard, S. Fehr, L. Salvail, and C. Schaffner. Oblivious transfer and linear functions. In *Advances in Cryptology—CRYPTO '06*, volume 4117 of *Lecture Notes in Computer Science*, pages 427–444. Springer, 2006.

[17] I. B. Damgaard, T. B. Pedersen, and L. Salvail. On the key-uncertainty of quantum ciphers and the computational security of one-way quantum transmission. In *Advances in Cryptology—EUROCRYPT '04*, volume 3027 of *Lecture Notes in Computer Science*, pages 91–108. Springer, 2004.

[18] Mohammed Barhoush, Louis Salvail. *Composable Security in the Bounded-Quantum-Storage Model*, arXiv:2302.05724.

[19] D. Deutsch. Uncertainty in quantum measurements. *Physical Review Letters*, 50(9):631–633, February 1983.

[20] P. Dumais, D. Mayers, and L. Salvail. Perfectly concealing quantum bit commitment from any quantum one-way permutation. In *Advances in Cryptology—EUROCRYPT '00*, volume 1807 of *Lecture Notes in Computer Science*, pages 300–315. Springer, 2000.

[21] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres. Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy. *Physical Review A*, 56:1163–1172, 1997.

[22] O. Goldreich and S. Vadhan. Comparing entropies in statistical zero knowledge with applications to the structure of SZK. In *14th Annual IEEE Conference on Computational Complexity (CCC 99)*, pages 54–75. IEEE Computer Society, 1999.

[23] J. Hilgevood and J. Uffink. The mathematical expression of the uncertainty principle. In *Microphysical Reality and Quantum Description*. Kluwer Academic, 1988.

[24] R. Impagliazzo, L. A. Levin, and M. Luby. Pseudo-random generation from one-way functions. In *21st Annual ACM Symposium on Theory of Computing (STOC)*, pages 12–24, 1989.

[25] K. Jones. Riemann-Liouville fractional integration and reduced distributions on hyperspheres. *Journal of Physics A: Mathematical and General*, 24:1237–1244, 1991.

[26] R. Jozsa, D. Robb, and W. K. Wootters. Lower bound for accessible information in quantum mechanics. *Physical Review A*, 49(2):668–677, 1994.

[27] K. Kraus. Complementary observables and uncertainty relations. *Physical Review D*, 35(10):3070–3075, May 1987.

[28] U. Larsen. Superspace geometry: the exact uncertainty relationship between complementary aspects. *Journal of Physics A: Mathematical and General*, 23(7):1041–1061, April 1990.

[29] N. Lutkenhaus. Security against individual attacks for realistic quantum key distribution. *Physical Review A*, 61:052304, 2000.

[30] H. Maassen and J. B. M. Uffink. Generalized entropic uncertainty relations. *Physical Review Letters*, 60(12):1103–1106, March 1988.

[31] R. Renner. Security of Quantum Key Distribution. PhD thesis, ETH Zurich (Switzerland), September 2005. http://arxiv.org/abs/quant-ph/0512258

[32] R. Renner, N. Gisin, and B. Kraus. An information-theoretic security proof for QKD protocols. *Physical Review A*, 72(012332), July 2005.

[33] R. Renner and R. König. Universally composable privacy amplification against quantum adversaries. In *Theory of Cryptography Conference (TCC)*, volume 3378 of *Lecture Notes in Computer Science*, pages 407–425. Springer, 2005.

[34] R. Renner and S. Wolf. Simple and tight bounds for information reconciliation and privacy amplification. In *Advances in Cryptology—ASIACRYPT 2005*, Lecture Notes in Computer Science, pages 199–216. Springer, 2005.

[35] J. Sanchez-Ruiz. Entropic uncertainty and certainty relations for complementary observables. *Physics Letters A*, 173(3):233–239, February 1993.

[36] J. Sanchez-Ruiz. Improved bounds in the entropic uncertainty and certainty relations for complementary observables. *Physics Letters A*, 201(2–3):125–131, May 1995.

[37] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 85(2):441–444, July 2000.

[38] S. Sykora. Quantum theory and the Bayesian inference problems. *Journal of Statistical Physics*, 11(1):17–27, 1974.

[39] M. N. Wegman and J. L. Carter. New classes and applications of hash functions. In *20th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 175–182, 1979.

[40] S. Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983. Original manuscript written circa 1970.

[41] J. Wullschleger. Oblivious-Transfer amplification. In *Advances in Cryptology—EUROCRYPT '07*, Lecture Notes in Computer Science. Springer, 2007.

[42] M. A. Ballester, S. Wehner, and A. Winter, *State Discrimination with Post-Measurement Information*, arXiv:quant-ph/0608014, 2006.

[43] R. Bhatia, *Matrix Analysis*, Grad. Texts in Math. 169, Springer, Berlin, 1997.

[44] G. Brassard, N. Lutkenhaus, T. Mor, and B. C. Sanders, *Limitations on practical quantum cryptography*, Phys. Rev. Lett., 85 (2000), pp. 1330–1333.

[45] G. Brassard, N. Lutkenhaus, T. Mor, and B. C. Sanders, *Security aspects of practical quantum cryptography*, in Advances in Cryptology—EUROCRYPT '00, Lecture Notes in Comput. Sci. 1807, Springer, Berlin, 2000, pp. 289–299.

[46] G. Brassard and L. Salvail, *Secret-key reconciliation by public discussion*, in Advances in Cryptology—EUROCRYPT '93, Lecture Notes in Comput. Sci. 765, Springer, Berlin, 1993, pp. 410–423.

[47] C. Cachin, C. Crepeau, and J. Marcil, *Oblivious transfer with a memory-bounded receiver*, in Proceedings of the 39th Annual IEEE Symposium on Foundations of Computer Science (FOCS), 1998, pp. 493–502.

[48] C. Crepeau, *Efficient cryptographic protocols based on noisy channels*, in Advances in Cryptology—EUROCRYPT '97, Lecture Notes in Comput. Sci. 1233, Springer, Berlin, 1997, pp. 306–317.

[49] C. Crepeau and J. Kilian, *Achieving oblivious transfer using weakened security assumptions*, in Proceedings of the 29th Annual IEEE Symposium on Foundations of Computer Science (FOCS), 1988, pp. 42–53.

[50] I. Damgård, J. Kilian, and L. Salvail, *On the (im)possibility of basing oblivious transfer and bit commitment on weakened security assumptions*, in Advances in Cryptology—EUROCRYPT '99, Lecture Notes in Comput. Sci. 1592, Springer, Berlin, 1999, pp. 56–73.

[51] I. B. Damgård, S. Fehr, K. Morozov, and L. Salvail, *Unfair noisy channels and oblivious transfer*, in Theory of Cryptography Conference (TCC), Lecture Notes in Comput. Sci. 2951, Springer, Berlin, 2004, pp. 355–373.

[52] Y. Z. Ding, D. Harnik, A. Rosen, and R. Shaltiel, *Constant-round oblivious transfer in the bounded storage model*, in Theory of Cryptography Conference (TCC), Lecture Notes in Comput. Sci. 2951, Springer, Berlin, 2004, pp. 446–472.

[53] Y. Dodis, L. Reyzin, and A. Smith, *Fuzzy extractors: How to generate strong keys from biometrics and other noisy data*, in Advances in Cryptology—EUROCRYPT '04, Lecture Notes in Comput. Sci. 3027, Springer, Berlin, 2004, pp. 523–540.

[54] S. Dziembowski and U. M. Maurer, *On generating the initial key in the bounded-storage model*, in Advances in Cryptology—EUROCRYPT '04, Lecture Notes in Comput. Sci. 3027, Springer, Berlin, 2004, pp. 126–137.

[55] A. K. Ekert, *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett., 67 (1991), pp. 661–663.

[56] C. A. Fuchs and J. van de Graaf, *Cryptographic distinguishability measures for quantum-mechanical states*, IEEE Trans. Inform. Theory, 45 (1999), pp. 1216–1227.

[57] B. Huttner, N. Imoto, N. Gisin, and T. Mor, *Quantum cryptography with coherent states*, Phys. Rev. A, 51 (1995), pp. 1863–1869.

[58] F. Kittaneh, *Norm inequalities for certain operator sums*, J. Funct. Anal., 143 (1997), pp. 337–348.

[59] H.-K. Lo and H. F. Chau, *Is quantum bit commitment really possible?*, Phys. Rev. Lett., 78 (1997), pp. 3410–3413.

[60] U. M. Maurer, *Perfect cryptographic security from partially independent channels*, in Proceedings of the 23rd Annual ACM Symposium on Theory of Computing (STOC), 1991, pp. 561–572.

[61] D. Mayers, *Unconditionally secure quantum bit commitment is impossible*, Phys. Rev. Lett., 78 (1997), pp. 3414–3417.

[62] T. Moran, R. Shaltiel, and A. Ta-Shma, *Non-interactive timestamping in the bounded storage model*, in Advances in Cryptology—CRYPTO '04, Lecture Notes in Comput. Sci. 3152, Springer, Berlin, 2004, pp. 460–476.

[63] A. Rényi, *On measures of entropy and information*, in Proceedings of the 4th Berkeley Symposium on Mathematical Statistics and Probability, Vol. 1, University of California Press, Berkeley, CA, 1961, pp. 547–561.

[64] L. Salvail, *Quantum bit commitment from a physical assumption*, in Advances in Cryptology—CRYPTO '98, Lecture Notes in Comput. Sci. 1462, Springer, Berlin, 1998, pp. 338–353.

[65] S. Wehner and J. Wullschleger, *Composable Security in the Bounded-Quantum-Storage Model*, arXiv:0709.0492, 2007.