Quantum-to-Classical Randomness Extractors

Kyle Marie Astroth [*] **Mohammad Aamir Sohail** [*] **Neha Rama Kumar** [*] **Samin Riasat** [*]

Wenfan Jiang [*]

Abstract

Randomness is an essential resource for information theory, cryptography, and computation. The goal of randomness extraction is to distill (almost) perfect randomness from a weak source of randomness. In this report, we first define classical randomness extractors, or when the source of randomness yields a classical string X. When considering a physical randomness source, X is itself ultimately the result of a measurement on an underlying quantum system, and the question arises of how much classical randomness can we extract from a quantum system. To understand and analyze this question, we will first provide the relevant quantum preliminary background, and then define quantum-to-classical (QC) and quantum-to-quantum (QQ) randomness extractors. Finally, we will explore cryptographic applications of QC randomness extractors, such as security in the noisy-storage model, and discuss possible future applications, such as privacy amplification.

Contents

[*] {kastroth,mdaamir,nehark,sriasat,jiangwf}@umich.edu

1 Introduction

Randomized algorithms are algorithms that use a degree of randomness as part of their logic. Randomized algorithms frequently outperform and simplify the best-known deterministic algorithms, and sources of randomness are a powerful but evasive resource. Further, access to randomness is an essential tool for cryptography. Randomized algorithms are designed and studied under the assumption that computers have access to true randomness in the form of a sequence of truly random bits. However, this randomness is taken from sources that only appear to have randomness, otherwise known as entropy. Entropy is a term borrowed from physics that refers to the amount of "disorder" in a system and is the measure of the uncertainty associated with a random variable. Some examples of these sources of randomness are generating and measuring electromagnetic or radioactive noise, measuring the timing of past events, or measuring user-dependent behavior [1]. The goal of randomness extraction is to convert these weak sources of randomness into uniformly random bits, which are measured in terms of the min-entropy. A visual representation of this process can be seen in Figure 1. This has led to the research and development of Classical Randomness Extractors (CC-Extractors). In Section 2, we give a thorough introduce the two main concepts of Classical Randomness Extractors, deterministic and seeded extractors.

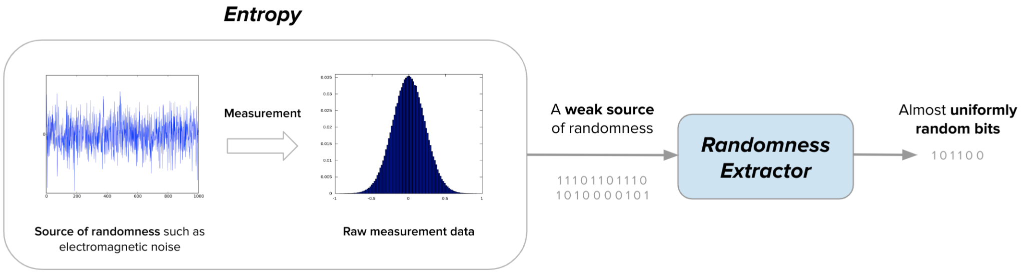
Entropy
Measurement
Source of randomness such as electromagnetic noise
Raw measurement data
A weak source of randomness
11101101110
1010000101
Randomness Extractor
Almost uniformly random bits
101100

Figure 1: High-level diagram of a randomness extractor

We now know, however, that the underlying world is not classical but rather quantum, resulting in the development of quantum mechanics. Subsequently, a randomness extractor may hold quantum side information about its (almost) uniformly random output sequence, X. This realization lends to several questions: where do X come from? How can we hope to harness even weak sources to obtain a surplus of classical randomness? How much randomness can we obtain from a quantum source rather than a classical string? [2] Questions such as these have culminated in the study of Quantum-to-Classical Randomness Extractors (QC-Extractors) with the goal of determining how we can extract classical randomness from a physical source by performing measurements on the quantum state of said source. In contrast to the classical world, quantum mechanics allow for the creation of true randomness given the correct circumstances. It is also important to note that in a quantum setting, there also exist Quantum-to-Quantum Randomness Extractors (QQ-Extractors) that we do not measure but determine if the resulting state is quantumly fully random (maximally mixed) and uncorrelated from the extractor. In Section 3, we introduce the necessary background quantum preliminaries, and in Section 4, we discuss the construction and evaluation of QC and QQ Randomness Extractors.

Finally, we will conclude our report in Section 5 by examining the applications of QC-Extractors to entropic uncertainty relations and cryptographic problems such as noisy storage models, and Section 6 where we explore future directions of this work. Entropic uncertainty relations are fundamental to quantum mechanics and crucial tools for quantum cryptography. We will provide and discuss the proof from [2] that any set of measurements forming a QC-extractor yields an entropic uncertainty relation with respect to quantum side information and thereby obtain relations both for the Shannon and the min-entropy. The second application we will discuss is proving security in the noisy-storage model. The noisy-storage model is a quantum cryptographic model that assumes an adversary is imperfect or noisy. The study of QC extractors can further be extended to other cryptographic problems, for example, privacy amplification. We refer the curious reader to the following articles, lecture notes, and textbooks [2, 3, 4, 5, 6, 7, 8, 9, 10] for further reading on quantum cryptography.

2 Classical Randomness Extractors

As discussed in § 1, randomness extraction is an efficient procedure for taking a sample from an imperfect random source, X with distribution p_X, and "extracting" the *pure*-randomness, i.e. being closer to uniformly distributed. A randomness extractor is a function that is applied to the output of a weakly random entropy source along with a short, uniformly random seed as input, and generates a highly random output that appears close to uniformly distributed and independent from the source [11]. Before formally defining a randomness extractor, we will define entropy, or how we measure the amount of randomness contained in a weak random source, as well as the statistical distance, or how we measure the closeness of the output distribution to the uniform distribution.

Definition 2.1. (Entropy) The Shannon Entropy of a discrete random variable X is defined as

$$H(X) = \mathbb{E}\left[\log \frac{1}{p_i}\right] = \sum_{i \in X} p_i \log \frac{1}{p_i},$$

where $p_i = \Pr[X = i]$.

Definition 2.2. (Min- Entropy) The min-entropy of a discrete random variable X is

$$H_{\min}(X) = \min_i \log \frac{1}{p_i},$$

or $H_{\min}(X)$ is the largest value of k such that all outcomes have the probability of at most 2^{-k}.

In general, we like to guess the most likely outcome, and the probability that we are correct is $P_{\text{guess}}(X) = \max_x p_X(x)$. This results in an operational interpretation of the min-entropy as

$$H_{\min}(X) = -\log P_{\text{guess}}(X).$$

When considering the above definitions, the question arises of why we use the min-entropy as the measure of uncertainty in cryptography as opposed to the Shannon entropy, which is used in information theory. Following Shannon's approach, $i(x) = -\log p_X(x)$ is the information gained when we observe X. Thus the Shannon entropy measured the average information gained, i.e., $H(X) = \sum_x p_X(x) i(x)$. However, when studying cryptography, we are interested in the worst case, not the average case, and the min-entropy $H_{\min}(X) = \min_x i(x)$ is precisely the smallest information gained. Figure 2 shows the difference between these quantities for a binary random variable. In general, $0 \leq H_{\min}(X) \leq H(X)$.

Definition 2.3. (Conditional Min-Entropy) Consider two dependent random variables X and E. The conditional min-entropy $H_{\min}(X|E)$ can be written as

$$H_{\min}(X|E) = -\log P_{\text{guess}}(X|E),$$

where $P_{\text{guess}}(X|E) = \max_x p_{X|E}(x|E)$.

Definition 2.4. (Statistical Distance) Let X and Y be two random variables with range $\mathcal{I}$. Then the statistical distance between X and Y is defined as

$$\Delta(X, Y) \equiv \frac{1}{2} \sum_{i \in \mathcal{I}} \left| \Pr[X = i] - \Pr[Y = i] \right|.$$

For $\varepsilon \geq 0$, we define the notion of two distributions being ε-close as

$$X \approx_\varepsilon Y \iff \Delta(X, Y) \leq \varepsilon.$$

We now formally illustrate the process of randomness extraction. Consider a single party, Alice, who has access to an n-bit string, x^n, obtained from a source X with distribution p_X. Perhaps, source X is correlated to an additional system or environment E. For example, E could contain information

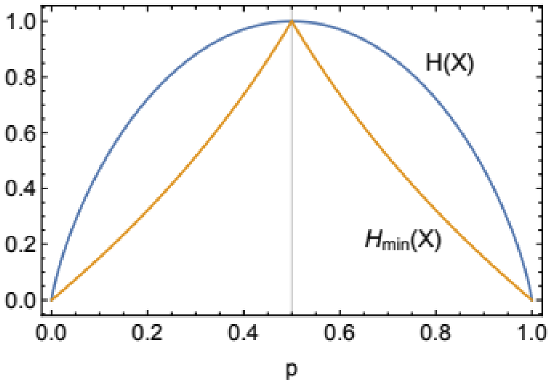

Figure 2: The comparison between Shannon entropy $H(X)$ and min-entropy $H_{\min}(X)$ for a binary random variable $X = \{0, 1\}$.

about the generation of the source X or an adversary who has gathered some prior information from protocols that include X. Alice has no access to system E except the lower bound on the min-entropy of the source X given environment E, i.e., $H_{\min}(X|E) \geq k$. In the task of randomness extraction, Alice's goal is to construct *randomness extractor*, denoted as Ext, that produces a m-bit string z^m, which is close to the uniform distribution in the statistical distance and uncorrelated with environment E.

Before formally discussing the construction of a randomness extractor, consider an example that shows how to extract uniform bits from an i.i.d. (*independent and identically distributed*) source.

Example 2.5. Consider an i.i.d. binary source X such that $X_i = 0$ w.p $p_0 = 1/4$ and $X_i = 1$ w.p $p_0 = 3/4$. Define the output Z of the randomness extractor $Z = \mathsf{Ext}(X) := X_1 \oplus X_2 \oplus \cdots \oplus X_n \in \{0, 1\}$, i.e., the parity of all n-bits sequence of X. To find if we can extract uniformly random bits from an i.i.d. source, we need to show that $\Pr(Z = 0) \approx 1/2 \pm \varepsilon$ for sufficiently small $\varepsilon > 0$, i.e., $Z \approx_\varepsilon$ uniform$(\{0, 1\})$.

Let's first examine how efficiently our strategy works for $n = 2$. We need to compute $\Pr(Z = 0) = \Pr(X_1 = 0, X_2 = 0) + \Pr(X_1 = 1, X_2 = 1) = p_0^2 + p_1^2 = 0.625$. Similarly, we can compute $\Pr(Z = 1) = 0.375$. Also, observe that $\Delta(X, U_2) = 0.25$ and $\Delta(Z, U_2) = 0.125$, where $U_2 \sim$ uniform$(\{0, 1\})$. In other words, the output distribution is not quite uniform, however, Z is more closer to uniform distribution than X. Hence, following the above analysis for sufficiently large n, we observe that $Z \approx_\varepsilon U_2$.

In the above example, we considered a function that takes only the source X as input. We call such functions deterministic or seedless extractors. Ideally, we wish to construct a deterministic extractor that, given a source of randomness with high min-entropy, outputs a distribution that is statistically close to random and near-perfect randomness without requiring an additional source of randomness. However, in reality, there does not exist a fixed deterministic procedure that can be used to extract even a single bit of randomness from a source with $H_{\min}(X) \geq k$, even when $k = n - 1$. The following proposition provides the proof that it is not possible to construct a deterministic extractor.

Proposition 2.6. *Let* $\mathsf{Ext} : \{0, 1\}^n \to \{0, 1\}^m$ *be a function taking input from a source. There exists a weak random source* X *with* $H_{\min} = n - 1$ *such that for* $m = 1$, $\mathsf{Ext}(X)$ *is a constant function.*

Proof. As defined above, Ext outputs a single bit and must output either 0 or 1 with probability $\geq \frac{1}{2}$. Suppose Ext outputs 0, and define X to be the flat distribution on $S = \{x : \mathsf{Ext}(x) = 0\}$. Then X has min-entropy of at least $n - 1$, but $\Pr[\mathsf{Ext}(X) = 0] = 1$, meaning the output distribution of Ext must be a constant. □

Therefore, in order to construct a randomness extractor, we must also provide additional input, a seed, that is uniformly random. As seen in Figure 3, every seeded extractor has five different parameters: the length of the source n, the output length m, the length of the seed d, the min-entropy threshold k, and the statistical error of the extractor ε.

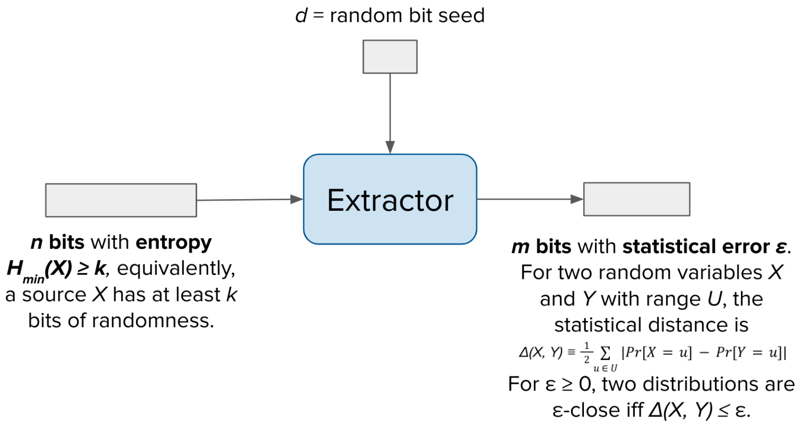
d = random bit seed
Extractor
***n* bits** with **entropy $H_{min}(X) \geq k$**, equivalently, a source *X* has at least *k* bits of randomness.
m* bits** with **statistical error *ε.
For two random variables *X* and *Y* with range *U*, the statistical distance is
$\Delta(X, Y) \equiv \frac{1}{2} \sum_{u \in U} |Pr[X = u] - Pr[Y = u]|$
For ε ≥ 0, two distributions are ε-close iff *Δ(X, Y)* ≤ ε.

Figure 3: Classical-to-classical (seeded) randomness extractor

Definition 2.7. (Seeded Extractor) The function $\mathsf{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is a (k, ε) extractor if for all X on $\{0,1\}^n$ with $H_{\min}(X) \geq k$,

$$\|E(X, U_d) - U_m\|_1 < 2\varepsilon,$$

where U_d is a uniform variable on d bits and U_m is uniform on m bits.

Recall that our motivation for extractors was to simulate randomization given only a weak random source, or without a seed. If the seed is of logarithmic length, i.e. $d = O(\log n)$, then instead of selecting it randomly we can enumerate all possibilities for the seed and take a majority vote. In summary, the randomness used for seeds can be eliminated by running all the possible seeds and taking the majority value. This is formally defined by the following lemma.

Lemma 2.8. *Let $A(w, r)$ be a randomized algorithm such that $A(w, U_m)$ has error probability at most γ, and let* $\mathsf{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *be a (k, ε) extractor. Define* $A' = \text{majority}_{y \in \{0,1\}^d}\{A(w, \mathsf{Ext}(x, y))\}$*. Then for every k-source*[2] *X on $\{0,1\}^n$, $A'(x, X)$ has error probability of at most* $2(\gamma + \varepsilon)$.

As stated above, we wish to extract randomness from weak random source X without any additional uniform randomness. Therefore it follows that we want to keep Y as small as possible, even though X, and k, could be very large. In other words, we would like a long output (i.e. large m) using a short seed (i.e. small d). This motivates the following definition of strong extractors.

Definition 2.9. (Strong Extractor) Extractor $\mathsf{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is a strong (k, ε)-extractor if for every k-source X on $\{0,1\}^n$, $(U_d, \mathsf{Ext}(X, U_d))$ is ε-close to (U_d, U_m). Equivalently, $\mathsf{Ext}'(x, y) = (y, \mathsf{Ext}(x, y))$ is a standard (k, ε)-extractor.

Before we discuss the explicit construction of a strong extractor, we revisit the question of why the min-entropy is a correct measure to quantify the amount of randomness that can be extracted from a given source? Informally, we can argue that the min-entropy is an upper bound on the amount of randomness that can be extracted: there does not exist any strong extractor that has an output length more than $H_{\min}(X)$. To understand this, first recall that $H_{\min}(X) = -\log P_{\text{guess}}(X)$. Suppose that we now apply some function f to source X, then how difficult is it to guess $f(X)$, i.e., what is $P_{\text{guess}}(f(X))$?. Clearly, we can guess $f(X)$ by first guessing X and then applying f to our guess. Thus, we get $P_{\text{guess}}(f(X)) \geq P_{\text{guess}}(X)$. However, this is equivalent to

$$H_{\min}(f(X)) \leq H_{\min}(X).$$

In other words, this also means that the output of the extractor Ext is obtained as a function $f(X) = \mathsf{Ext}(X, y)$, for a fixed seed y, must have min-entropy at most $H_{\min}(X)$. Thus, the output $\mathsf{Ext}(X, y)$ can be uniform on at most $H_{\min}(X)$ bits. How about a converse: does there exist a strong extractor

[2] A random variable X is k-source if $H_{\min}(X) \geq k$.

that can extract approximately $H_{\min}(X)$ bits from any k-source X? The answer to this question is yes.

We now explore a construction of randomness extractors that achieves well-performing parameters for this application, the 2-universal extractor. Our goal for our parameters is large m, or extracting as much randomness as possible, using the smallest possible seed and error, or small d and ε. First, we must define a 2-universal family.

Definition 2.10. (2-universal family) A family of hash functions $\mathcal{F} = \{f : \{0,1\}^n \to \{0,1\}^m\}$ is called *2-universal* if for every two strings $x, x' \in \{0,1\}^n$ with $x \neq x'$, and any two $z, z' \in \{0,1\}^m$, we have

$$\Pr_{f \in \mathcal{F}}[f(x) = z \oplus f(x') = z'] = \frac{1}{2^{2m}}.$$

Using 2-universal families, we are able to define 2-universal extractors as follows.

Definition 2.11. (2-universal extractor) Let $\mathcal{F} = \{f_y : \{0,1\}^n \to \{0,1\}^m, y \in \{0,1\}^d\}$ be a 2-universal family of hash functions such that $|\mathcal{F}| = 2^d$. The associated 2-universal extractor is

$$\mathsf{Ext}_{\mathcal{F}} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m, \mathsf{Ext}_{\mathcal{F}}(x,y) = f_y(x).$$

Conceptually, consider $\mathsf{Ext}_{\mathcal{F}}$ as using a seed y to select a function from the family $\mathcal{F}$ uniformly at random and returning the output of the function when evaluated on the source X. To evaluate how good this extractor is, we use the leftover hash lemma (insert reference), which is defined as follows.

Definition 2.12. (Leftover hash lemma) Let n and $k \leq n$ be arbitrary integers, $\varepsilon > 0$, $m = k - 2\log(\frac{1}{\varepsilon})$, and $\mathcal{F} = \{f : \{0,1\}^n \to \{0,1\}^m\}$ a 2-universal family of hash functions. Then the 2-universal extractor $\mathsf{Ext}_{\mathcal{F}}$ is a (k, ε)-strong seeded randomness extractor.

Due to page limit restrictions, for the leftover hash lemma proof, we refer the reader to [3].

3 Preliminaries

In this section, we recall the basic *Dirac* notation of quantum information science which we will use throughout this article. We refer the reader to [9, 10] for additional reading in quantum computation and quantum information. The Dirac notation represents a vector using the left vertical bar and the right angle bracket, known as *ket* vector. Thus it can be understand by the following map: $x \to |x\rangle$ for any index x. The conjugate transpose of the ket vector $|x\rangle$ is known as *bra* vector and denoted as $\langle x| = |x\rangle^\dagger$. In other words, the $|x\rangle$ in Dirac notation represents the column vector, whereas $\langle x|$ represents the row vector (conjugate transpose of the column vector $|x\rangle$).

3.1 Mathematical Background

In this subsection, we go through some of the mathematical tools that will be required to understand the QC and QQ randomness extractor. We restrict ourselves to definitions and a few important properties; for detailed understanding, we refer the reader to cite wilde2013quantum, nielsen2002quantum.

Definition 3.1. (Conjugate Transpose) The *conjugate transpose* or *Hermitian transpose* of a $m \times n$ complex matrix A is a $n \times m$ matrix $A^\dagger$ obtained by transposing A followed by applying complex conjugate on each entry or vice versa, i.e., $A^\dagger = (\bar{A^{\mathrm{T}}}) = (\bar{A})^{\mathrm{T}}$.

For real matrices, the conjugate transpose is just the transpose, $A^\dagger = A^{\mathrm{T}}$.

Definition 3.2. (Hilbert Space) A Hilbert space is a complex vector space $\mathcal{H}$ with an inner product $\langle x||y\rangle \equiv \langle x|y\rangle$, where $x, y \in \mathcal{H}$, such that the norm defined as $\|x\| = \sqrt{\langle x|x\rangle}$ make $\mathcal{H}$ a complete metric space. It allows generalizing the methods of linear algebra and calculus from (finite-dimensional) Euclidean vector spaces to spaces that may be infinite-dimensional.

Definition 3.3. (Linear Operator) A *linear operator* A on a Hilbert space $\mathcal{H}$ is a mapping $A : \mathcal{H} \to \mathcal{H}$ such that

$$A\left(\sum_i \alpha_i |x_i\rangle\right) = \sum_i \alpha_i A|x_i\rangle.$$

The set of linear operators is denoted as $\mathcal{L}(\mathcal{H}, \mathcal{H})$.

Definition 3.4. (Trace of Linear Operator) The trace of an operator $A \in \mathcal{L}(\mathcal{H}, \mathcal{H})$ is defined as

$$\mathrm{Tr}(A) = \sum_i \langle i|A|i\rangle,$$

where $\{|i\rangle\}$ is any orthonormal basis of $\mathcal{H}$.

Definition 3.5. (Hermitian Operator) A *linear operator* $A \in \mathcal{L}(\mathcal{H}, \mathcal{H})$ is *hermitian* if $A^\dagger = A$.

Definition 3.6. (Positive Semi-Definite Operator) A hermitian operator A is positive semi-definite if all its eigenvalues are non-negative.

Definition 3.7. (Adjoint) The *adjoint* or *Hermitian conjugate* of the operator $A \in \mathcal{L}(\mathcal{H}, \mathcal{H})$ is a *unique* linear operator $A^\dagger \in \mathcal{L}(\mathcal{H}, \mathcal{H})$ such that for all $|x\rangle, |y\rangle \in \mathcal{H}$,

$$\langle x| \left(A|y\rangle\right) = \left(A^\dagger|x\rangle\right)^\dagger |y\rangle.$$

In the following subsections, we go through the mathematical framework of quantum mechanics, namely, formalism of quantum states and time-evolution of quantum states. We refer the reader to [12, 13, 14] for additional understanding of concepts in quantum mechanics.

3.2 Quantum States

Definition 3.8. (Quantum System) A Quantum System is a complex vector space with an inner product, i.e., a Hibert space $\mathcal{H}$. By following the convention in quantum cryptography, we assume all Hilbert Space is finite-dimensional.

Example 3.9. The simplest quantum system is a *qubit* or *quantum bits*, which is a two-dimensional quantum system.

Definition 3.10. (Quantum States) Let $|A|$ be the dimension of a quantum system A acting on Hilbert space $\mathcal{H}_A$, and $\mathcal{L}(A)$ denote the set of linear operators on system A. We define a *quantum state* on system A as $\rho_A \in \mathcal{S}(A)$ where $\mathcal{S}(A) = \{\sigma_A \in \mathcal{L}(A) | \sigma_A \geq 0, \mathrm{Tr}(\sigma_A) = 1\}$, i.e., a quantum state is a unit-trace and positive semi-definite linear operator on $\mathcal{H}_A$.

Example 3.11. Let $|0\rangle$ and $|1\rangle$ form an orthonormal basis for a qubit system $\mathcal{H}_2$. Then any arbitrary qubit state ρ_2 can be written as $|\psi\rangle\langle\psi|$ where $|\psi\rangle \in \mathcal{H}_2$ is an arbitrary *superposition* of the basis state, i.e., $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ such that α and β are complex numbers and $|\alpha|^2 + |\beta|^2 = 1$. After simplifying, $\rho_2 = |\alpha|^2|0\rangle\langle 0| + \alpha\bar{\beta}|0\rangle\langle 1| + \beta\bar{\alpha}|1\rangle\langle 0| + |\beta|^2|1\rangle\langle 1|$. We can also write ρ_2 in matrix form w.r.t basis $\{|0\rangle, |1\rangle\}$ as

$$\rho_2 = \begin{pmatrix} |\alpha|^2 & \alpha\bar{\beta} \\ \beta\bar{\alpha} & |\beta|^2 \end{pmatrix}.$$

We call ρ_A a *pure state*, if it has rank 1. If $\mathrm{Tr}(\rho_A) \leq 1$, we call ρ_A a sub-normalized state. We use the notation $\mathcal{S}_{\leq}(A)$ to represent a collection of sub-normalized states of the system A. For the rest of the paper, the term *state* is referred to sub-normalized state unless otherwise specified.

Definition 3.12. (Multipartite Quantum States) We define a (separable) multipartite system[3] $A_1A_2 \cdots A_n$ by the *tensor product* of individual quantum systems $A_1, A_2, \cdots, A_n$ acting on the Hilbert space $\mathcal{H}_{A_1A_2\ldots A_n}$, where

$$\mathcal{H}_{A_1A_2\ldots A_n} = \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}, ..., \otimes\mathcal{H}_{A_n}.$$

Then, a *multipartite* quantum state $\rho_{A_1A_2\cdots A_n} \in \mathcal{S}_{\leq}(A_1A_2\cdots A_n)$.

If $n = 2$, the quantum state $\rho_{A_1A_2}$ is known as *bipartite* quantum state. The quantum state of the subsystem A_1 is defined as $\rho_{A_1} = \mathrm{Tr}_{A_2}[\rho_{A_1A_2}]$, where Tr_{A_2} is the partial trace[4] on system A_2. In other words, the quantum state of the subsystem A_1 is the restriction of $\rho_{A_1A_2}$ onto $\mathcal{H}_{A_1}$. Similarly, the quantum state of the subsystem A_2 can be obtained by partial tracing the system A_2.

[3] A multipartite system $A_1A_2\cdots A_n$ is called a *separable* system if it can be written as tensor product of individual systems, i.e., $A_1A_2\cdots A_n = A_1 \otimes A_2 \otimes \cdots \otimes A_n$, otherwise the multipartite system is called *entangled* system. We will mainly consider the bipartite state, where two systems A_1 and A_2 are combined using the tensor product and written as $A_1A_2 = A_1 \otimes A_2$

[4] For brief understanding partial trace information please see: Partial Trace (wikipedia)

Definition 3.13. (Purification) *Purification* is the completion of a quantum system by adding a purifying or reference system R. Let $\rho_A \in \mathcal{S}_{\leq}(A)$ be a sub-normalized state. A *purification* of ρ_A is a pure bipartite state $|\rho\rangle_{AR}$ on the purifying system R and the original system A such that

$$\rho_A = \mathrm{Tr}_R(|\rho\rangle\langle\rho|_{AR}).$$

Purification is not unique. However, all possible purifications of a quantum state ρ_A are related by an isometry [5] acting on the reference system R [9, Theorem 5.1.1].

Definition 3.14. (Classical States) For some set $\mathcal{X}$, let $\{|x\rangle\}_{x\in\mathcal{A}}$ be the orthogonal basis of a Hilbert space $\mathcal{H}_X$, where each basis basis vector $|x\rangle$ corresponds to a particular element $x \in \mathcal{X}$. A *classical state*, or a c-state, ρ_X defined using the distribution P_X over $\mathcal{X}$ as follows:

$$\rho_X = \sum_{x\in\mathcal{X}} P_X(x)|x\rangle\langle x|.$$

(Classical-Quantum States) The joint system of a classical system X and a quantum system A is defined as

$$\rho_{XA} = \sum_{x\in\mathcal{X}} P_X(x)\underbrace{|x\rangle\langle x|_X}_{\text{classical}} \otimes \underbrace{\rho_A^x}_{\text{quantum}},$$

and such states are called *classical-quantum* states, or cq-states. In general, when a multipartite state is partly classical and partly quantum, we use c and q to label the classical and quantum systems, respectively.

Example 3.15. In quantum cryptography, we often encounter cq-states. Suppose Alice tosses a fair coin, and if the head appears, she prepares a $|0\rangle$ state and $|1\rangle$ otherwise. Alice then transmits her state to Bob. Thus, if Alice state is $|0\rangle$ or $|1\rangle$, then Bob will receive ρ_0^B or ρ_1^B, respectively. The joint state of Alice and Bob can be written as a cq-state of the form:

$$\rho_{AB} = \frac{1}{2}\sum_{x\in\{0,1\}} |0\rangle\langle 0|_A \otimes \rho_x^B.$$

3.3 Quantum Operations

Definition 3.16. (Quantum Measurement) Consider a set of positive semi-definite operators $\{M_x^{A_2}\}_{x\in\mathcal{X}}$ acting on system A_2 such that $\sum_x M_x^{A_2} = \mathbb{I}_{A_2}$. For a bipartite system A_1A_2, a *measurement map* on the system A_2 is defined as $\mathcal{T}_{A_1A_2\to A_1} : \mathcal{L}(A_1A_2) \to \mathcal{L}(A_1)$,

$$\mathcal{T}(\mathbb{I}_{A_1}\otimes M_x^{A_2})_{A_1A_2\to A_1} = \sum_{a_1a_2}\langle a_1a_2|(\mathbb{I}_{A_1}\otimes M_x^{A_2})|a_1a_2\rangle|a_1\rangle\langle a_1|$$

where $\{|a_1\rangle\}, \{|a_2\rangle\}$ are standard orthogonal bases of A_1, A_2 respectively. The subscript x is used as a label for measurement outcomes. Figure 4 provides the schematic of a quantum measurement. The probability of observing x on system A_2 is given as $p_x^{A_2} = \langle a_1a_2|(\mathbb{I}_{A_1}\otimes M_x^{A_2})|a_1a_2\rangle = \langle a_2|M_x^{A_2}|a_2\rangle = \mathrm{Tr}(M_x^{A_2}|a_2\rangle\langle a_2|)$[6].

The set of positive semi-definite operators $\{M_x^{A_2}\}_{x\in\mathcal{X}}$ referred as positive valued measurements (POVMs). In quantum information theory and cryptography, we are mostly interested in the probabilities of measurement outcomes but not the output state after measurement. Thus, POVMs provide simpler expressions for finding probabilities of outcomes.

Example 3.17. Consider a distribution p_X and the classical state $\rho_X = \sum_x p_X(x)|x\rangle\langle x|$. If we measure ρ_X in the standard basis, i.e. $\{|x\rangle\}$, with associated POVM $M_x = |x\rangle\langle x|$, we obtain outcome x with probability $\mathrm{Tr}(M_x\rho_X) = \mathrm{Tr}(|x\rangle\langle x|\rho_x) = \langle x|M_x|x\rangle p_X(x) = p_X(x)$. Thus, we observe that ρ_X indeed captures the classical distribution given by the probabilities p_x.

[5] Given two Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ with dim($\mathcal{H}_1$) $\leq$ dim($\mathcal{H}_2$), an isometry V is a linear map from $\mathcal{H}_1$ to $\mathcal{H}_2$ such that $V^\dagger V = \mathbb{I}_{\mathcal{H}_1}$ [9, 10].

[6] The interpretation of inner product as probability follows from *Born rule*

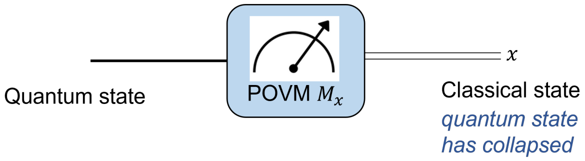

Figure 4: Quantum measurement

Definition 3.18. (Unitary Evolution) The evolution of a quantum state is described by a *unitary* transformation. Suppose a *unitary operator*[7] U is applied to system A_1 of $\rho_{A_1A_2}$. Then the evolved quantum state can be written as

$$\rho'_{A_1A_2} = U_{A_1}\rho_{A_1A_2}U^\dagger_{A_1} = (U \otimes \mathbb{I}_{A_2})\rho_{A_1A_2}(U \otimes \mathbb{I}_{A_2})^\dagger,$$

where $\mathbb{I}_{A_2}$ denotes the identity in $\mathcal{L}(A_2)$.

Definition 3.19. (Identity Channel) For quantum systems A_1, A_2 with orthogonal bases $\{|i\rangle_{A_1}\}_{i=1}^d, \{|i\rangle_{A_2}\}_{i=1}^d$, the *identity channel* $\mathbb{I}$, from $\mathcal{L}(A_1)$ to $\mathcal{L}(A_2)$ with respect to these bases is denoted by $\mathbb{I}_{A_1\to A_2}$, where $\mathbb{I}_{A_1\to A_2}(|i\rangle\langle j|_{A_1}) = |i\rangle\langle j|_{A_2}$.

Definition 3.20. (Quantum Channel) A linear map $\mathcal{E}_{A_1\to A_2} : \mathcal{L}(A_1) \to \mathcal{L}(A_2)$ is a quantum channel if it satisfies the following conditions:

- $\mathrm{Tr}(\mathcal{E}_{A_1\to A_2})(\rho_{A_1}) = \mathrm{Tr}(\rho_{A_1})$, i.e., trace-preserving and
- $(\mathbb{I}_A \otimes \mathcal{E}_{A_1\to A_2})(\mathbb{I}_A \otimes \rho_{A_1}) \geq 0$ for all $\rho_{A_1} \geq 0$, i.e., completely positive.

In other words, a *quantum channel* is a linear, completely positive and trace-preserving map.

We conclude the brief discussion about the mathematical framework of quantum mechanics. Figure 5 summarizes a quantum information processing task, which includes (i) the preparation of quantum states, i.e., encoding, (ii) performing some quantum operation, for example, passing the input quantum state through a quantum channel, and (iii) decoding the classical outcome by performing a quantum measurement.

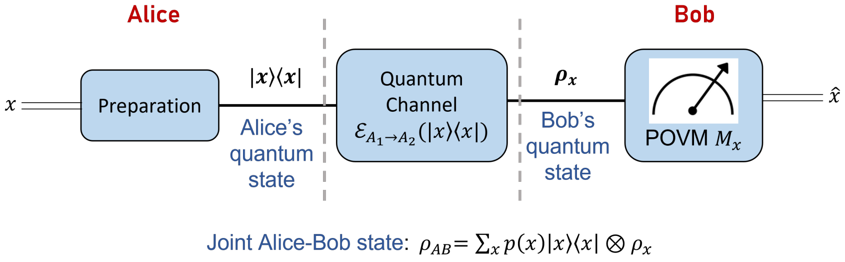
Alice
Bob
x
Preparation
$|x\rangle\langle x|$
Alice's quantum state
Quantum Channel
$\mathcal{E}_{A_1\to A_2}(|x\rangle\langle x|)$
ρ_x
Bob's quantum state
POVM M_x
$\hat{x}$
Joint Alice-Bob state: $\rho_{AB} = \sum_x p(x)|x\rangle\langle x| \otimes \rho_x$

Figure 5: Schematic of a quantum information processing task.

In the following subsections, we discuss the statistical distance between two quantum states, i.e., how to measure the closeness of two quantum states and quantum information quantities. We refer the reader to [9, 10] for additional understanding of distance and information measures.

3.4 Distance Measures

Distance measure quantifies the closeness of quantum states. In this subsection, we discuss two well-studied distance measures for sub-normalized quantum states, namely, (i) *trace distance* and (ii) *purified distance*. We begin by defining the trace distance followed by the purified distance. We further provide brief intuition about these distance measures. However, for detailed discussion, we refer to [8].

[7] Given two Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ with $\dim(\mathcal{H}_1) = \dim(\mathcal{H}_2)$, an unitary U is a linear map from $\mathcal{H}_1$ to $\mathcal{H}_2$ such that $V^\dagger V = VV^\dagger = \mathbb{I}_{\mathcal{H}_1}$ [9, 10].

Definition 3.21. **(Trace Norm)** The trace norm or Schatten 1-norm $\|\rho\|_1$ of a quantum state ρ is defined as

$$\|\rho\|_1 = \operatorname{Tr}\{\sqrt{\rho^\dagger \rho}\}.$$

The trace norm induces a distance measure between quantum states called *trace distance*.

Definition 3.22. **(Trace Distance)** Given any two quantum states ρ and σ, the trace distance between them is as follows:

$$\|\rho - \sigma\|_1.$$

For any two quantum states ρ and σ, the following bounds hold for the trace distance:

$$0 \leq \|\rho - \sigma\|_1 \leq 2.$$

The trace distance attains a lower bound when two quantum states are equivalent, i.e., there exists no measurement that can distinguish ρ and σ. The trace distance attains the upper bound when ρ and σ have support on orthogonal subspaces, i.e., there exists a measurement that can distinguish ρ and σ.

Definition 3.23. **(Generalized Fidelity)** The generalized fidelity between two quantum states ρ and σ is defined as

$$\bar{F}(\rho, \sigma) = F(\rho, \sigma) + \sqrt{(1 - \operatorname{Tr}(\rho) \operatorname{Tr}(\sigma))},$$

where $F(\rho, \sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1$ is the notion of fidelity between normalized quantum states. Note that if either of the quantum states is normalized, then generalized fidelity is the same as the fidelity, i.e., $\bar{F}(\rho, \sigma) = F(\rho, \sigma)$.

Definition 3.24. **(Purified Distance)** The purified distance between two quantum states ρ and σ is defined as

$$P(\rho, \sigma) = \sqrt{1 - \bar{F}(\rho, \sigma)}.$$

The *purified distance* is a metric on the set of sub-normalized quantum states. The purified distance and trace distance are closely related as, for any two states ρ, σ, we have [15],

$$\frac{1}{2}\|\rho - \sigma\|_1 \leq P(\rho, \sigma) \leq \sqrt{2\|\rho - \sigma\|_1}.$$

Definition 3.25. **(ε-quantum ball)** Let $\mathcal{H}_A$ be a Hilbert space. The ε-quantum ball around a quantum state $\rho_A \in \mathcal{S}_{\leq}(A)$ of the system A is defined as the collection of quantum states $\{\sigma_A \in \mathcal{S}_{\leq}(A)\}$ such that the purified distance between ρ_A and σ_A is not more than ε, i.e.,

$$\mathcal{B}^{\varepsilon}(\rho_A) = \{\sigma_A \in \mathcal{S}_{\leq}(A) : P(\rho_A, \sigma_A) \leq \varepsilon\}.$$

We use the above definition to describe the notion of smooth conditional $\min$-entropy of a quantum system in the next section.

3.5 Information Quantities

The term "information" in the context of information theory is a measure of how much we can learn from the outcome of a random experiment. Information can be classical, quantum, or both depending on the physical source of information. For example, measuring the position of an electron carries *quantum information*, whereas flipping a coin carries *classical information*. The fundamental information measure in classical and quantum information theory is *entropy*. Entropy is the expected amount of information contained in an outcome of a random experiment [16]. In this section, we define the various entropy measures that are required to provide the information-theoretic operational interpretations of randomness extractors. We discuss some of their mathematical properties. However, we exclude the proofs; for further understanding, we refer to [9, Ch-10,11]. We start by defining quantum entropy, also known as *Von Neumann entropy* for general quantum systems. Furthermore, we define quantum (Von-Neumann) conditional entropies. We then discuss the condition min-entropy of a bipartite quantum system analogous to classical conditional min-entropies. Finally, we conclude the subsection with the definition of smooth conditional min-entropy, which is helpful in quantum cryptography, especially in the context of entropic uncertainty, noisy storage model, and privacy amplification [17].

Definition 3.26. (Von Neumann Entropy) The entropy of a quantum state $\rho_A \in \mathcal{S}_{\leq}(A)$ is defined as

$$H(A)_\rho = -\operatorname{Tr}(\rho_A \log \rho_A)^8.$$

Definition 3.27. (Conditional Von Neumann Entropy) The conditional entropy of quantum system A given B for bipartite quantum state $\rho_{AB} \in \mathcal{S}_{\leq}(AB)$ is defined as

$$H(A|B)_\rho = H(AB)_\rho - H(B)_\rho,$$

where $H(AB)_\rho = -\operatorname{Tr}(\rho_{AB} \log \rho_{AB})$ is the Von Neumann entropy of the bipartite state ρ_{AB}.

We provide the definitions of the min- and max-based information measures analogous to Def. 2.2.

Definition 3.28. (Min-Conditional Entropy) The min-conditional entropy of a bipartite quantum state ρ_{AB} with respect to a quantum state σ_B is defined as

$$H_{\min}(A|B)_{\rho|\sigma} = \max\{\lambda \in \mathbb{R} : 2^{-\lambda} \cdot \mathbb{I} \otimes \sigma_B \geq \rho_{AB}\}$$

Definition 3.29. (Conditional Min-Entropy) The conditional min-entropy of a bipartite quantum state ρ_{AB} is defined as

$$H_{\min}(A|B)_\rho = \max_{\sigma_B \in \mathcal{S}(B)} H_{\min}(A|B)_{\rho|\sigma}$$

To interpret a conditional information measure, suppose Alice and Bob want to share a bipartite quantum state ρ_{AB}. Alice and Bob have access to systems A and B, respectively. The conditional entropy measures the average uncertainty Bob has about Alice's state upon sampling from his own system.

The above-mentioned entropies have operational interpretation only in an independent and identically (IID) distributed asymptotic setting. Therefore, for an operational characterization of a generalized quantum system, we need a notion of *smooth entopies* [15].

Definition 3.30. (Smooth Conditional Min-Entropy) Let $\rho_{AB} \in \mathcal{S}_{\leq}(AB)$ be a quantum state and $\varepsilon \geq 0$. The ε-smooth conditional min-entropy of A given B is defined as

$$H^{\varepsilon}_{\min}(A|B)_\rho = \sup_{\sigma_{AB} \in \mathcal{B}^{\varepsilon}(\rho_{AB})} H_{\min}(A|B)_\sigma.$$

4 Quantum-to-Classical Randomness Extractors

In this section, we study quantum-to-classical randomness extractors (QC-extractors). The main objective of this section is to answer the following question: how can we extract classical randomness from a physical (quantum) source ρ_{AE} by performing measurements on the quantum state ρ_A? Here, A is the accessible quantum source, and E is the environment or eavesdropper correlated with A. Similar to the study of classical extractors in § 2, we want to extract randomness from a quantum source given min-entropy $H_{\min}(A|E)_\rho \geq k$. It is worth noting that, unlike the classical world, quantum mechanics does allow for the generation of true randomness in case we can prepare the desired quantum source. For example, if we could prepare the state $|+\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$ or $|-\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)$ and measure it in the computational basis[9], i.e., $M_0 = |0\rangle\langle 0|$ and $M_1 = |1\rangle\langle 1|$. Then, we get a *true* random coin. However, this would require preparing the exact source of this form. In general, we want to construct a QC extractor that works for any unknown quantum source as long as it has a sufficiently high min-entropy.

To understand the definition of quantum extractors, consider a classical extractor as a family of permutations acting on the possible values of the source such that it applies a typical permutation from the family to the input for any probability distribution on input bits strings with high min-entropy, which induces an almost uniform probability distribution on a prefix of the output. We define a QQ-extractor similarly in the way that lets the operations be general unitary transformations and the input of the extractor be quantum.

[8] All logarithms are base 2 unless specified.

[9] $\{|0\rangle, |1\rangle\}$ is known as the computational basis of a qubit system, whereas $\{|+\rangle, |-\rangle\}$ is known as Hadamard basis of a qubit system

Definition 4.1. (QQ-extractor [2]) Let $A = A_1A_2$ (entangled system) with $n = \log|A|$, define the trace-out map $\mathrm{Tr}_{A_2} : \mathcal{L}(A) \to \mathcal{L}(A_1)$ by $\mathrm{Tr}_{A_2}(\cdot) = \sum_{a_2} \langle a_2|(\cdot)|a_2\rangle$, where $\{|a_2\rangle\}$ is an orthonormal basis of A_2. For $k \in [-n, n]$ and $\epsilon \in [0, 1]$, a (k, ϵ)-QQ-extractor is a set $\{U_1, \ldots, U_L\}$ of unitary transformations on A such that for all states $\rho_{AE} \in \mathcal{S}(AE)$ satisfying $H_{min}(A|E)_\rho \geq k$, we have

$$\frac{1}{L}\sum_{i=1}^{L}\left\|\mathrm{Tr}_{A_2}(U_i\rho_{AE}U_i^\dagger) - \frac{\mathbb{I}_{A_1}}{|A_1|} \otimes \rho_E\right\|_1 \leq \epsilon.$$

where $\log L$ is called the seed size of the QQ-extractor.

More often than not, we only need a quantum extractor as it is usually sufficient to extract random classical bits. Doing so is much easier than obtaining random qubits. This motivates our need for quantum-classical extractors, where the output system M is measured in the computational basis. Generally, our QC-extractor can be represented as given in Figure 6. We take a quantum input system with our seed and mix it. Mixing is done with the unitary operation, where we take one basis of the Hilbert space of the quantum system and rotate it into another Hilbert space. After mixing, we use the process of measuring and discarding to generate our classical output system. For that, first, we define the measurement map for $\mathcal{H}_M \subseteq \mathcal{H}_N$ as $\mathcal{T}_{N\to M} : \mathcal{H}_N \to \mathcal{H}_M$,

$$\mathcal{T}_{N\to M}(\cdot) = \sum_{m,m'} \langle mm'|(\cdot)|mm'\rangle|m\rangle\langle m|_M$$

where $\{|mm'\rangle\}, \{|m\rangle\}$ are orthonormal bases of $\mathcal{H}_N, \mathcal{H}_M$, respectively. We can also observe this map as tracing out N/M, and measuring the remaining system M in the basis $\{|m\rangle\}$. Using the above map, we will define quantum-classical min-entropy extractors against quantum side information.

Definition 4.2. (QC-extractor [2]) Let $A = A_1 \otimes A_2$ (separable system) with $n = \log|A|$. Define the *measurement map* $\mathcal{T}_{A\to A_1} : \mathcal{L}(A) \to \mathcal{L}(A_2)$ by

$$\mathcal{T}_{A\to A_1}(\cdot) = \sum_{a_1a_2} \langle a_1a_2|(\cdot)|a_1a_2\rangle|a_1\rangle\langle a_1|, \tag{4.1}$$

where $\{|a_1\rangle\}, \{|a_2\rangle\}$ are standard orthonormal bases for A_1, A_2 respectively.

For $k \in [-n, n]$ and $\varepsilon \in [0, 1]$, a (k, ε)-*QC-extractor* is a set $\{U_1, \ldots, U_L\}$ of unitary transformations on A such that for all states $\rho_{AE} \in \mathcal{S}(AE)$ satisfying $H_{\min}(A|E)_\rho \geq k$, we have

$$\frac{1}{L}\sum_{i=1}^{L}\left\|\mathcal{T}_{A\to A_1}(U_i\rho_{AE}U_i^\dagger) - \frac{\mathbb{I}_{A_1}}{|A_1|} \otimes \rho_E\right\|_1 \leq \varepsilon.$$

$\log L$ is called the *seed size* of the QC-extractor.

The reason we use this definition is that we want the output of the extractor to be determined by the source and the choice of the seed. In the quantum setting, a natural way of translating this requirement is by imposing that an adversary holding a system that is maximally entangled with the source can perfectly predict the output.

4.1 Examples of QC-extractors

Two-independent hashing, also known as universal hashing, is one of the most important extractor constructions. We discussed this briefly in § 2. Basically, it includes selecting two hash functions from a family of hash functions such that it guarantees that the hash codes of both the designated keys are independent random variables [18]. In this article, we focus on the theory of unitary 2-design, which can be seen as the quantum generalization of two-independent hash functions.

There are many known efficient constructors of unitary 2-designs [[19], [20]], and in an n-qubit space, such unitaries can be computed with circuits of size $O(n^2)$. The following is immediate using a general decoupling result from [21, 22].

Corollary 4.3. *Let $A = A_1 \otimes A_2$ with $n = \log|A|$. For all $k \in [-n, n]$ and all $\varepsilon > 0$, a unitary 2-design $\{U_1, ..., U_L\}$ on A is a (k, ε)-QC-extractor with output size*

$$\log|A_1| = \min(n, n + k - 2\log(1/\varepsilon)).$$

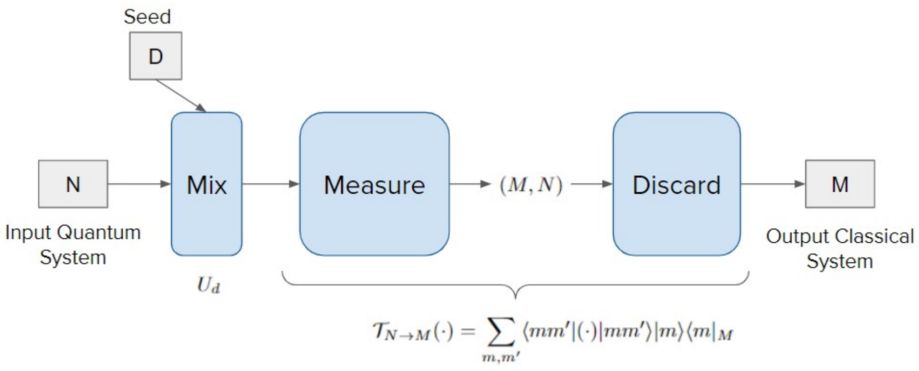
Seed
D
N
Mix
Measure
(M, N)
Discard
M
Input Quantum System
Output Classical System
U_d
$\mathcal{T}_{N\to M}(\cdot) = \sum_{m,m'} \langle mm'|(\cdot)|mm'\rangle|m\rangle\langle m|_M$

Figure 6: Quantum-to-Classical Extractor

Similar results as above also hold true for "almost" 2-design unitaries [[23], [24]]. Now, by choosing a reasonably small L, making a set of random unitaries, with the seed size of the same order as the output size of the extractor, defines a QC-extractor with high probability.

Theorem 4.4. *Let $A = A_1 \otimes A_2$ with $n = \log|A|$ and let $\mathcal{T}_{A\to A_1} : \mathcal{L}(A) \to \mathcal{L}(A_2)$ the measurement map defined in* (4.1). *Let $\varepsilon > 0$ and c be a sufficiently large constant, and suppose that*

$$\log|A_1| \leq n + k - 4\log(1/\varepsilon) - c \quad \textit{and} \quad \log L \geq \log|A_1| + \log n + 4\log(1/\varepsilon) + c.$$

Then, choosing $\{U_1, \ldots, U_L\}$ independently according to the Haar measure [25] defines a (k, ε)-QC-extractor with high probability.

4.2 Bitwise QC-extractor

In this section, we discuss constructing simpler unitaries to define a QC-extractor. The construction is composed of unitaries V acting on single qubits followed by permutations P of the computational basis elements. Because the measurement $\mathcal{T}$ and the permutations P are commutative in nature, we first apply V, measure in the computational basis, and then finally apply the permutation to the classical outcome of the measurement. Unitaries acting on single qubits is frequently a desired attribute for the design of cryptographic protocols, in addition to computational efficiency.

We consider a value $d \geq 2$ as a prime power so that there exists a complete set of mutually unbiased bases in dimension d. This set of bases can be represented by a set of unitary transformations given as $\{V_0, V_1, ..., V_d\}$ which maps the mutually unbiased bases to some standard basis. The following example, we represent the unitary transformations when we take a full set of mutually unbiased bases in dimension 2:

$$V_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad V_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad V_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & -1 \end{pmatrix}$$

We now define the set $\mathcal{V}_{d,n}$ of unitary transformations on n qubits as follows:

$$\mathcal{V}_{d,n} := \{V = V_{u_1} \otimes ... \otimes V_{u_n} | u_i \in \{0, 1, ..., d\}\}$$

Theorem 4.5. *Let $A = A_1 \otimes A_2$ with $|A| = d^n$, $|A_1| = d^{\xi n}$, $|A_2| = d^{(1-\xi)n}$ and d a prime power. Then, for $\delta \geq 0$ and $\delta' > 0$,*

$$\frac{1}{|\mathcal{P}|}\frac{1}{(d+1)^n}\sum_{P\in\mathcal{P}}\sum_{V\in\mathcal{V}_{d,n}}\left\|\mathcal{T}_{A\to A_1}\left(PV\rho_{AE}(PV)^\dagger\right) - \frac{\mathbb{I}}{|A_1|}\otimes\rho_E\right\|_1$$
$$\leq \sqrt{2^{(1-\log(d+1)+\xi\log d)n}\left(1 + 2^{-H^\delta_{\min}(A|E)_\rho + z}\right)} + 2(\delta + \delta'),$$

where $\mathcal{V}_{d,n}$ is defined as above, $\mathcal{P}$ is a family of pair-wise independent permutation matrices, and

$$z = \log\left(\frac{2}{\delta'^2} + \frac{1}{1-\delta}\right).$$

In particular, the set $\{PV : P \in \mathcal{P}, V \in \mathcal{V}_{d,n}\}$ is a (k, ε)-QC-extractor provided

$$\log |A_1| \leq (\log(d + 1) - 1)n + \min\{0, k\} - 4 \log(1/\varepsilon) - 7$$

and the number of unitaries is $L = (d + 1)^n d^n (d^n - 1)$.

4.3 Full set of mutually unbiased bases (MUB)

We saw that QC-extractors are defined by unitary 2-designs. It is reasonable to anticipate that we can create smaller and simpler sets of unitaries if we are simply interested in extracting random classical bits because unitary 2-designs also define QQ-extractors. Here, we build more basic sets of unitaries that define a QC-extractor, using a family of pair-wise independent permutations and a complete set of mutually unbiased bases.

Definition 4.6. (MUB) A *mutually unbiased basis* is defined as the set of unitaries $\{U_1, \ldots, U_L\}$ acting on A such that a state described by a vector $U_i^\dagger |a\rangle$ of the basis i gives a uniformly distributed outcome when measured in basis j for $i \neq j$. There can be at most $|A| + 1$ mutually unbiased bases for A.

Definition 4.7. A family $\mathcal{P}$ of of permutations of a set X is called *pair-wise independent* if for all $x_1 \neq x_2$ and $y_1 \neq y_2$, we have

$$\Pr[\pi(x_1) = y_1 \text{ and } \pi(x_2) = y_2] = \frac{1}{|X|(|X| - 1)},$$

for any π uniformly distributed over $\mathcal{P}$.

Observe that if X is a field (so that $|X|$ is a prime power), the family

$$\mathcal{P} = \{x \mapsto ax + b : x \in X^*, b \in X\}$$

is pair-wise independent. Observing permutations of the basis elements of a Hilbert space A as a unitary transformation on A, we have the following result.

Theorem 4.8. *Let $A = A_1 \otimes A_2$ with $n = \log |A|$, where $|A|$ is a prime power. If $\{U_1, \ldots, U_{|A|+1}\}$ defines a full set of mutually unbiased bases, then for $\delta \geq 0$ we have*

$$\frac{1}{|\mathcal{P}|} \frac{1}{|A| + 1} \sum_{P \in \mathcal{P}} \sum_{i=1}^{|A|+1} \left\| \mathcal{T}_{A \to A_1} \left(PU_i \rho_{AE} (PU_i)^\dagger \right) - \frac{\mathbb{I}_{A_1}}{|A_1|} \otimes \rho_E \right\|_1 \leq \sqrt{\frac{|A_1| 2^{-H_{\min}(A|E)_\rho}}{|A_1| + 1}} + 2\delta,$$

where $\mathcal{P}$ is a set of pair-wise independent permutation matrices. In particular, the set $\{PU_i : P \in \mathcal{P}, i \in [|A| + 1]\}$ defines a (k, ε)-QC-extractor provided

$$\log |A_1| \leq n + k - 2 \log(1/\varepsilon),$$

and the number of unitaries is

$$L = (|A| + 1)\mathcal{P} = (|A| + 1)|A|(|A| - 1).$$

The proofs of the above theorems require an understanding of concepts such as one-shot decoupling, permutation extractors, and advanced mathematical tools from linear algebra. Thus, due to page limit restrictions, for proof of the above theorems related to the construction of QC-extractors, we refer the reader to [2, 8].

We summarize all the results about QC-extractors in Table 2 in the discussion section, i.e., § 6.

5 Applications

In this section, we discuss the application of QC-extraction to achieve the performance of cryptographic models such as noisy storage models. We will mainly focus on two applications of QC-extractors. First, QC-extractor gives rise to entropic uncertainty relations with quantum side information, and second noisy storage model; in other words, any two-party cryptographic protocol can be implemented securely as long as the adversary's storage device has sufficiently low quantum capacity.

5.1 Entropic uncertainty relations with quantum side information

The uncertainty principle is one of the fundamental theories of quantum mechanics. Uncertainty relations, originally proposed by Heisenberg $\Delta x \Delta p \geq \frac{h}{4\pi}$, is one of the most prominent examples that show how quantum mechanics differs from the classical world. Perhaps, the best known in the form given by Robertson [26], who extended Heisenberg's result to two arbitrary observables [10] A and B. Uncertainty relation states that if we prepare many copies of the state $|\psi\rangle$, and measure each copy individually using either observable A or B, we have

$$\Delta A \Delta B \geq \frac{1}{2}|\langle\psi|[A,B]|\psi\rangle|$$

where $\Delta X = \sqrt{\langle\psi|X^2|\psi\rangle - \langle\psi|X|\psi\rangle}$ for $X = A, B$ is the standard deviation resulting from measuring $|\psi\rangle$ with observable X. This means that there is no way to simultaneously specify definite values of non-commuting[11] observables with great precision.

Entropic uncertainty relations provide a contemporary way to express the notion of uncertainty in quantum mechanics. It has interesting applications in quantum cryptography, the entropic uncertainty relations allow to provide the security proof of cryptographic protocols. Briefly, it provides a subtle interplay between uncertainty and entanglement. We consider a bipartite guessing game, which consist of Alice and Eve, to understand the entropic uncertainty relations. Entropic uncertainty relation allows us if Eve can or cannot predict the outcomes of two non-commuting measurements performed on Alice's state.

Assume Eve only has classical memory, i.e., she might make measurements on the qubits during the transmission, but she cannot keep any entanglement with herself. This is equivalent to Eve preparing Alice's qubits herself. We now define the *guessing game* below:

Guessing Game:

1. **Eve:** Prepares a qubit ρ_A and sends it to Alice
2. **Alice:** Chooses a random bit $\Theta \in \{0, 1\}$
3. **Alice:** If $\Theta = 0$, then Alice measures ρ_A in the computational basis, i.e., $\{|0\rangle, |1\rangle\}$; otherwise, she measures ρ_A in the Hadamard basis, i.e., $\{|+\rangle, |-\rangle\}$
4. **Alice:** Records the measurement outcome $X \in \{0, 1\}$
5. **Alice:** Announces Θ
6. **Eve:** Wins if she correctly guesses X

Figure 7 summarizes the guessing game defined above. The objective is to make sure that Eve cannot fully predict Alice's measurement outcome. Consider the following example, where the joint state between Alice and Eve is

$$\rho_{AE} = |0\rangle\langle 0|_A \otimes \rho_E,$$

where Alice measures system A in either the computational or the Hadamard basis to obtain the secret key. To see why this captures the essence of the uncertainty principle, note that if the measurements are non-commuting, then there exists no state ρ_A that Eve can prepare, which would allow her to guess the outcome for both choices of measurements with certainty. Uncertainty can be understand as a bound on the average probability that Eve correctly guesses X:

$$\begin{aligned}\Pr[X \mid \Theta] &= \Pr[\Theta = 0] \cdot \Pr[X \mid \Theta = 0] + \Pr[\Theta = 1] \cdot \Pr[X \mid \Theta = 1] \\ &= \frac{1}{2}[\Pr[X \mid \Theta = 0] + \Pr[X \mid \Theta = 1] \leq \epsilon,\end{aligned}$$

where the second equality holds if Alice chooses her measurement basis Θ at random, i.e. with uniform probability $1/2$ for each option. In the case where Eve holds no additional information

[10] In quantum physics, an observable is a physical quantity that can be measured, for example, position and momentum.

[11] Two observables A and B are said to be commuting if $AB = BA$, thus, commutator $[A, B] = 0$, where $[A, B] = AB - BA$.

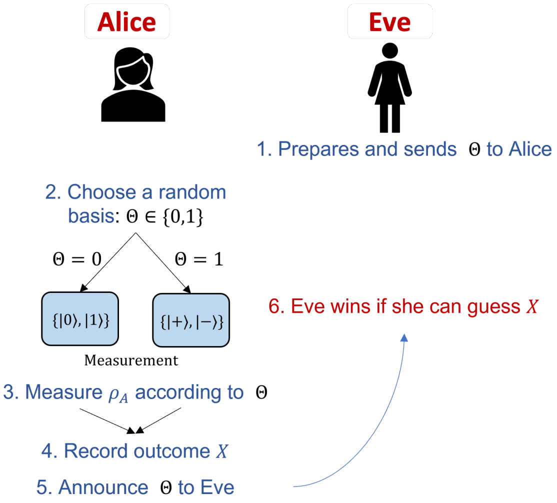
Alice
Eve
1. Prepares and sends Θ to Alice
2. Choose a random basis: Θ ∈ {0,1}
Θ = 0
Θ = 1
{|0⟩, |1⟩}
{|+⟩, |−⟩}
Measurement
6. Eve wins if she can guess X
3. Measure ρ_A according to Θ
4. Record outcome X
5. Announce Θ to Eve

Figure 7: The bipartite guessing game between Alice and Eve.

except for the basis where Alice has performed the measurement, it can be shown that $\epsilon < 1$. To understand this, suppose Eve always aims to correctly guess X regardless of whether $\Theta = 0$ or $\Theta = 1$. Then she requires $\Pr[X \mid \Theta = 0] = 1$, i.e. she should prepare a state that will always produce a deterministic outcome when Alice measures in the computational basis. In order for this to happen, Eve can send the state $|0\rangle\langle 0|_A$, where Alice, upon measuring in the computational basis, will always produce $X = 0$. However, if Eve has used the strategy of preparing $|0\rangle\langle 0|_A$ and Alice measures in the Hadamard basis, then

$$\begin{aligned}\Pr[X \mid \Theta = 1] &= \max\{\Pr[X = 0 \mid \Theta = 1], \Pr[X = 1 \mid \Theta = 1]\\ &= \max\{\mathrm{Tr}[|+\rangle\langle +||0\rangle\langle 0|], \mathrm{Tr}[|-\rangle\langle -||0\rangle\langle 0|]\} = \frac{1}{2}.\end{aligned}$$

Thus, if Eve uses this strategy of preparing $\rho_A = |0\rangle\langle 0|_A$ in order to guess Alice's outcome X, then whenever $\Theta = 1$, this corresponds only to a random guess. So, in this protocol, since Eve does not know beforehand what basis Alice will choose to measure in, she has to prepare a state that will maximize her guessing probability in both cases of Alice measuring in the standard basis, and also the Hadamard basis. The above example shows that this guessing probability can never be equal to 1.

Note that in order for Eve to maximize the guessing probability $\Pr[X \mid \Theta]$ over ρ_A, without loss of generality, we consider the outcome to be $X = 0$,

$$\Pr[X \mid \Theta] = \frac{1}{2}(\mathrm{Tr}[\rho_A|0\rangle\langle 0|] + \mathrm{Tr}[\rho_A|+\rangle\langle +|]) = \frac{1}{2}\mathrm{Tr}[\rho_A(|0\rangle\langle 0| + |+\rangle\langle +|)]$$

then she has to prepare ρ_A in the pure state corresponding to the eigenvector of $|0\rangle\langle 0| + |+\rangle\langle +|$ with the largest eigenvalue, which is $\lambda_{\max} = 1 + 1/\sqrt{2}$. Therefore,

$$\Pr[X|\Theta] = \frac{1}{2} + \frac{1}{2\sqrt{2}} < 1.$$

To calculate Eve's guessing probability, we write a quantum state in the following form [9, 10]:

$$\rho_A = \frac{1}{2}(\mathbb{I} + v_x X + v_y Y + v_z Z)$$

for a vector $v = (v_x, v_y, v_z)$. Then,

$$\mathrm{Tr}[\rho_A|0\rangle\langle 0|] = \frac{1}{2}(1 + v_z), \qquad \mathrm{Tr}[\rho_A|1\rangle\langle 1|] = \frac{1}{2}(1 - v_z),$$

$$\mathrm{Tr}[\rho_A|+\rangle\langle +|] = \frac{1}{2}(1 + v_x), \qquad \mathrm{Tr}[\rho_A|-\rangle\langle -|] = \frac{1}{2}(1 - v_x).$$

$$\text{Also, } \Pr[X \mid \Theta] = \frac{1}{2}\max\{\mathrm{Tr}[\rho_A|0\rangle\langle 0|], \mathrm{Tr}[\rho_A|1\rangle\langle 1|]\} + \frac{1}{2}\max\{\mathrm{Tr}[\rho_A|+\rangle\langle +|], \mathrm{Tr}[\rho_A|-\rangle\langle -|]\}$$

maximized over all possible states ρ_A. Since the maximizations of both expression are symmetric around $v_z = 0, v_x = 0$, respectively. Consider only the case where $v_z, v_x \geq 0$. Thus, we get,

$$\Pr[X \mid \Theta]_{\rho_A} = \frac{1}{2}\,\mathrm{Tr}[\rho_A(|0\rangle\langle 0| + |+\rangle\langle +|)] = \frac{1}{4}(2 + v_x + v_z), \qquad v_x^2 + v_z^2 \leq 1.$$

Note that the maximum occurs when $v_x^2 + v_z^2 = 1$. Therefore, by the change of variable as $v_x = \cos(t)$, $v_z = \sin(t)$, we get, the probability of Eve winning the game is

$$\Pr[X \mid \Theta]_{\rho_A} = \frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0.85.$$

In a more general scenario, Eve may even have classical information about ρ_A. Following the same steps as above, we can show that

$$\Pr[X|\Theta C]_{\rho_{AC}} = \frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0.85.$$

Thus, the min-entropy $H_{\min}(X \mid \Theta C) = -\log \Pr[X \mid \Theta C] \approx 0.22$.

If we always allow Eve maximum information about everything, she may prepare a larger state ρ_{AE}, i.e., Eve also holds the purification and send the ρ_A to Alice. Then one can show that if Eve can be entangled with Alice's qubit, then she can guess perfectly.

Finally, if we want to keep X secret from Eve, we need to use two aspects of quantum mechanics:

1. Uncertainty: If Eve has no (or little) entanglement with Alice, then she cannot certainly predict the outcomes of two non-commuting measurements. So it is difficult to guess Alice's measurement outcomes, i.e., $\Pr[X|E\Theta] < 1$, or equivalently, $H_{\min}(X|E\Theta) > 0$.
2. Entanglement: We need to ensure there exists some entanglement between Alice and Eve. For this, we can use the fact that entanglement is *monogamous* [12], that is if we find a large amount of entanglement between Alice and Bob, then we know that Eve has very little entanglement with either Alice or Bob, and therefore the min-entropy should be large. Hence, Eve cannot guess the outcome of Alice, and entropic uncertainty ensures security!

Below, in Table 1, we summarize the various methods used for constructing QC-extractions to achieve the uncertainty relations for the min-entropy [8, 2]:

	Lower bounds for smooth conditional min-entropy $H_{\min}$
Unitary 2-design	$\log\|A\| + H^{\delta}_{\min}(A\|E)_\rho - \log\left(\frac{1}{(\varepsilon^2/2-2\delta)^2}\right)$
Almost unitary 2-design	$\log\|A\| + H^{\delta}_{\min}(A\|E)_\rho - \log\left(\frac{1}{(\varepsilon^2/2-2\delta)^2}\right) - \log(1+\zeta)$
All $\|A\|+1$ MUBs	$\log(\|A\|+1) + H^{\delta}_{\min}(A\|E)_\rho - \log\left(\frac{1}{(\varepsilon^2/2-2\delta)^2}\right)$
Single qudit MUBs	$n(\log(d+1)-1) + \min\left\{0, H^{\delta}_{\min}(A\|E)_\rho - \log\left(\frac{2}{\delta'^2} + \frac{1}{1-2\delta}\right)\right\}$ $- \log\left(\frac{1}{(\varepsilon^2/2-2\delta-\delta')^2}\right) - 1$

Table 1: Entropic uncertainty relations with quantum side information for the smooth conditional min-entropy for approximation parameters $\varepsilon > 0$, $\zeta \geq 0$, $\delta \geq 0$, and $\delta' > 0$.

5.2 Noisy-Storage Model

Quantum computer benefits computing resources for those algorithms with computational assumptions, but a drawback is that the security can be broken retroactively. Most two-party protocols that have been executed to date will lose their security because the adversary can use the quantum computer to break the protocol. One way to solve this problem is to consider physical assumptions rather than computational assumptions. The most straightforward one is storage.

[12] Please see the page on Wikipedia Monogamy of entanglement

In classical cryptography, physical assumptions are usually made as the *bounded-storage model*, which assumes that the adversary can only store a certain number of classical bits. After introducing quantum communication, one now assumes that the adversary's quantum storage is limited to a certain number of qubits but no restriction on the classical bits. This is known as *bounded-quantum-storage model*. More generally, one can also invoke the noisy storage model, where the quantum storage is not only bounded but also noisy in general [3], to incorporate both the amount of storage and noise. [27] introduced the concept of a *noisy-storage model*.

Definition 5.1. (Noisy Quantum Memory) Given a device whose input states are in some Hilbert space $\mathcal{H}_{in}$, a *noisy quantum memory* is a state ρ stored in the device decoheres over time. That is, the content of the memory after some time t is a state $\mathcal{F}_t(\rho)$, where $\mathcal{F}_t : \mathcal{H}_{in} \rightarrow \mathcal{H}_{out}$ is a completely positive trace-preserving map corresponding to the noise in the memory.

Considering the security, the intuition is that security is possible as long as the amount of information that the adversary can store in his memory device is limited. Therefore, the central assumption of the model is that during waiting times δt introduced into the protocol, the adversary can only store quantum information using a limited and unreliable quantum memory device. In particular, the adversary can store an unlimited amount of classical information while also doing any operation at the moment. That means he is able to use any encoding and decoding operations before and after using his memory device. Notice that the input spaces can be in the form of $\mathcal{H}_{in} = (\mathbb{C}^d)^{\otimes N}$ and channels $\mathcal{F} = \mathcal{N}^{\otimes N}$ with $\mathcal{N} : \mathcal{H}_{in} \rightarrow \mathcal{H}_{out}$.

To analyze the security of a noisy-storage model, we first introduce a technique called *weak string ensure*.

Definition 5.2. (Weak String Erasure) In a two-party secure computation, *weak string erasure* is a primitive that provides Alice with a random bit string $X^n \in \{0,1\}^n$ and Bob with a randomly chosen substring $X_{\mathcal{I}=(X_{i_1},X_{i_2},\ldots,X_{i_r})}$ together with index set $\mathcal{I} = \{i_1, i_2, \ldots, i_r\}$ specifying the location of these bits [27].

The motivation behind the primitive weak string erasure was to create a basic quantum protocol that builds up classical correlations between Alice and Bob which are later used to implement more interesting cryptographic primitives. We can construct a very simple protocol for weak string erasure and prove its security using a bitwise QC-randomness extractor.

The protocol is basically the same as the one provided in [27], but in our case, instead of using only 2 MUBs per qubit, there will be 3. The procedure is as follows:

Protocol Weak String Erasure (WSE):
Output: $x^n \in \{0,1\}^n$ **to Alice,** $(\mathcal{I}, |\ddagger|^{\mathcal{I}}) \in 2^{[n]} \times \{0,1\}^{\mathcal{I}}$ **to Bob.**

1. **Alice:** Creates n EPR-pairs Φ, and sends half of each pair to Bob.
2. **Alice:** Chooses a bases-specifying string $\theta^n \in_R \{0,1,2\}^n$ uniformly at random. For all i, she measures the i-th qubit in the basis θ_i to obtain outcome x_i.
3. **Bob:** Chooses a basis string $\tilde{\theta}_i \in_R \{0,1,2\}^n$ uniformly at random. When receiving the i-th qubit, Bob measures it in the basis of $\tilde{\theta}^n$ to obtain outcome $\tilde{x}_i$.

Both parties wait time Δt.

4. **Alice:** Sends the basis information θ^n to Bob and outputs x^n.
5. **Bob:** Computes $\mathcal{I} = \{i \in [n] | \theta_i = \tilde{\theta}_i\}$, and outputs $(\mathcal{I}, |\ddagger|^{\mathcal{I}}) := (\mathcal{I}, \tilde{x}_{\mathcal{I}})$.

The proof of the correctness of the protocol and in regards to a dishonest Alice can be found in [27]. To prove the security against a dishonest Bob, we first consider the general form that any attack on Bob takes in the Figure 8.

Note that the noisy-storage model only assumes that Bob has to use his storage device during waiting times δt, which means when attacking the protocol above, he can store the incoming qubits perfectly until n qubits arrive. Let $\mathcal{Q}$ denote Bob's quantum register containing all n qubits. Since there is no communication between Alice and Bob during the transmission of these n qubits, we can assume that Bob first waits for all n qubits to arrive before mounting any form of attack. Besides, as any operation in quantum theory is a quantum channel, Bob's attack can be described by a quantum

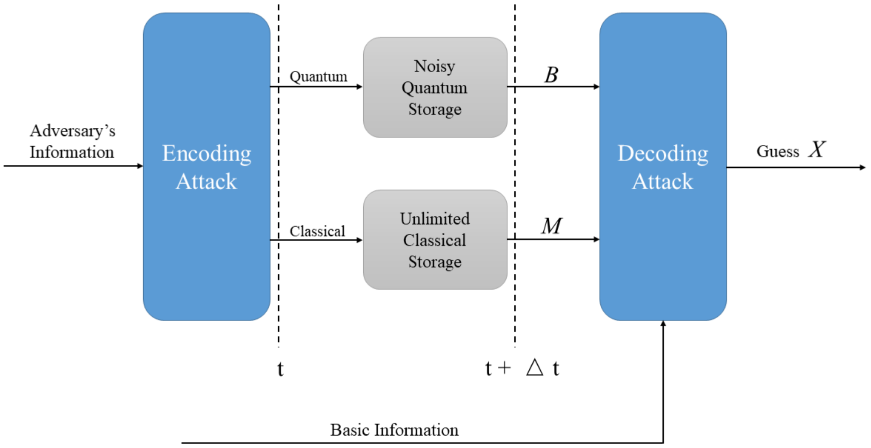

Figure 8: Any attack of dishonest Bob is described by an encoding attack E and a 'guessing' attack.

channel $\mathcal{E} : \mathcal{S}_{\leq}(\mathcal{Q}) \to \mathcal{S}_{\leq}(\mathcal{H}_{in} \otimes M)$, where this map takes $\mathcal{Q}$ to some quantum state on the input of Bob's storage device, $\mathcal{H}_{in}$, and M, some arbitrarily large amount of classical information. For example, $\mathcal{E}$ could be an encoding into an error-correcting code.

Then, by the assumption of the noisy-storage model, Bob's quantum memory is then affected by noise $\mathcal{F} : \mathcal{S}_{\leq}(\mathcal{H}_{in}) \to \mathcal{S}_{\leq}(\mathcal{H}_{out})$. After the waiting time, the joint state held by Alice and Bob in the purified version of the protocol (i.e., before Alice measures) is thus of the form

$$\rho_{ABM} = \mathcal{I}_A \otimes [(\mathcal{F} \otimes \mathcal{I}_M) \circ \mathcal{E}](\Phi^{\otimes n})$$

where Φ is an EPR-pair. And after the waiting time, Bob can perform any form of quantum operation to try and recover information from the storage device. Note that, in principle, Bob's goal is to recover X alone, for which he could potentially use his basis information Θ. In fact, we can ignore the basis information in the analysis. That is, we only need to analyze decoding maps $\mathcal{D} : \mathcal{S}_{\leq}(\mathcal{H}_{in} \otimes M) \to \mathcal{S}_{\leq}(\mathcal{Q})$ trying to recover the initial entanglement between Alice and Bob.

After implementing the task of 'Weak String Erasure' as above, we consider the usage of bitwise QC-extrators as linking security to the entanglement fidelity (quantum capacity) of the noisy quantum storage. Earlier, we came across the fact that one of the desirable properties of a bitwise QC-extrator is that, in addition to its computational efficiency, we observe that the unitaries act on single qubits. So, by changing the encoding from a qubit scheme to a qubit six-state scheme, we use the bitwise QC-extrator, defined in Theorem 4.5. This gives us a strong converse classical capacity replaced by the strong converse quantum capacity. This then extends the parameter regime where the security of all existing protocols can be proven. Even though there is in general, no closed expression for the strong converse quantum capacity, we can calculate security rates by means of the entanglement cost of quantum channels, which is an upper bound on the strong converse quantum capacity. As a brief overview, the entanglement cost of a quantum channel is the minimal rate at which entanglement (between sender and receiver) is needed in order to simulate many copies of a quantum channel in the presence of free classical communication.

6 Discussion

In this report, we introduced the concept of a randomness extractor. We discussed classical randomness extractors and provided examples and applications, namely, 2-universal extractors. We further discussed the concept of quantum-to-classical randomness extractors. We showed that for a QC-extractor to distill randomness from a quantum state ρ_{AE}, the relevant quantity to bound is the conditional min-entropy $H_{\min}(A|E)_\rho$. This is in formal analogy with classical-to-classical extractors, in which case the relevant quantity is $H_{\min}(X|E)_\rho$.

We showed various properties of QC-extractors and gave several examples for QC-extractors. We compare our results about QC-extractors with CC-extractors in Table 2.

		CC-extractors	QC-extractors
Seed	Lower bound	$\log(n-k)+2\log(1/\varepsilon)$	$\log(1/\varepsilon)$
	Upper bounds	$\log(n-k)+2\log(1/\varepsilon)$ (NE)	$m+\log n+4\log(1/\varepsilon)$
		$c\log(n/\varepsilon)$	$3n$
Output	Upper bound	$k-2\log(1/\varepsilon)$	$n+H_{\min}^{\sqrt{\varepsilon}}(A|E)$
	Lower bound	$k-2\log(1/\varepsilon)$	$n+k-2\log(1/\varepsilon)$

Table 2: Bounds on the seed size and output size in terms of (qu)bits for different kinds of (k, ε)-randomness extractors. Here, n refers to the number of input (qu)bits, m the number of output (qu)bits, and k the min-entropy of the input $H_{\min}(A|E)$.

There is an extensive difference between the upper and lower bounds for the seed size of QC-extractors. We were only able to show the existence of QC-extractors with seed length roughly the output size m, but we believe that it should be possible to find QC-extractors with much smaller seeds, say $O(\text{polylog}(n))$ bits long, where n is the input size. However, entirely different techniques might be needed to address this question.

We showed that every QC-extractor gives rise to entropic uncertainty relations with quantum side information for the Von Neumann (Shannon) entropy and the min-entropy. Here the seed size translates into the number of measurements in the uncertainty relation. Since it is, in general difficult to obtain uncertainty relations for a small set of measurements (except for the special case of two), finding QC-extractors with a small seed size is also worth pursuing from the point of view of uncertainty relations.

We used the bitwise QC-extractor from § 4 to show that the security in the noisy storage model can be related to the strong converse rate of the quantum storage, a problem that attracted quite some attention over the last few years. Here one can also see the usefulness of bitwise QC-extractors for quantum cryptography. Indeed, any bitwise QC-extractor would yield a protocol for weak string erasure. Bitwise measurements have a very simple structure and hence are implementable with current technology. In that respect, it would be interesting to see if a similar QC-extractor can also be proven for only two (complementary) measurements per qubit. This would give a protocol for weak string erasure. It is expected that QC-extractors will have many more applications in quantum cryptography, e.g., quantum key distribution and privacy amplification.

We encourage the reader to go through the following video, which provides a brief overview of the topic: Quantum-to-Classical Randomness Extractor[13].

References

[1] R. Shaltiel, "An introduction to randomness extractors," Berlin, Heidelberg, pp. 21–41, 2011.

[2] M. Berta, O. Fawzi, and S. Wehner, "Quantum to classical randomness extractors," *IEEE Transactions on Information Theory*, vol. 60, no. 2, pp. 1168–1192, feb 2014. [Online]. Available: https://doi.org/10.1109%2Ftit.2013.2291780

[3] S. Wehner and T. Vidick, "Quantum cryptography." [Online]. Available: https://ocw.tudelft.nl/courses/quantum-cryptography/

[4] H.-K. Lo and N. Lütkenhaus, "Quantum cryptography: from theory to practice," *arXiv preprint quant-ph/0702202*, 2007.

[5] D. Bruss, G. Erdélyi, T. Meyer, T. Riege, and J. Rothe, "Quantum cryptography: A survey," *ACM Computing Surveys (CSUR)*, vol. 39, no. 2, pp. 6–es, 2007.

[6] D. J. Bernstein, "Introduction to post-quantum cryptography," in *Post-quantum cryptography*. Springer, 2009, pp. 1–14.

[13] https://tinyurl.com/eecs572projectvideo

[7] C. H. Bennett, G. Brassard, and A. K. Ekert, “Quantum cryptography,” *Scientific American*, vol. 267, no. 4, pp. 50–57, 1992.

[8] M. Berta, “Quantum side information: Uncertainty relations, extractors, channel simulations,” *arXiv preprint arXiv:1310.4581*, 2013.

[9] M. M. Wilde, *Quantum information theory*. Cambridge University Press, 2013.

[10] M. A. Nielsen and I. Chuang, “Quantum computation and quantum information,” 2002.

[11] S. P. Vadhan, “Pseudorandomness,” *Foundations and Trends® in Theoretical Computer Science*, vol. 7, no. 1-3, pp. 1–336, 2012.

[12] J. J. Sakurai and E. D. Commins, “Modern quantum mechanics, revised edition,” 1995.

[13] N. Zettili, “Quantum mechanics: concepts and applications,” 2003.

[14] D. J. Griffiths and D. F. Schroeter, *Introduction to quantum mechanics*. Cambridge university press, 2018.

[15] M. Tomamichel, “A framework for non-asymptotic quantum information theory,” *arXiv preprint arXiv:1203.2142*, 2012.

[16] C. E. Shannon, “A mathematical theory of communication,” *The Bell system technical journal*, vol. 27, no. 3, pp. 379–423, 1948.

[17] U. V. Vazirani and T. Vidick, “Fully device-independent quantum key distribution.” *Physical Review Letters*, vol. 113, p. 140501, 2014.

[18] R. Impagliazzo, L. A. Levin, and M. Luby, “Pseudo-random generation from one-way functions,” in *Proceedings of the twenty-first annual ACM symposium on Theory of computing*, 1989, pp. 12–24.

[19] D. Gross, K. Audenaert, and J. Eisert, “Evenly distributed unitaries: On the structure of unitary designs,” *Journal of Mathematical Physics*, vol. 48, no. 5, p. 052104, may 2007.

[20] C. Dankert, R. Cleve, J. Emerson, and E. Livine, “Exact and approximate unitary 2-designs and their application to fidelity estimation,” *Physical Review A*, vol. 80, no. 1, jul 2009.

[21] F. Dupuis, O. Szehr, and M. Tomamichel, “A decoupling approach to classical data transmission over quantum channels,” *IEEE Transactions on Information Theory*, vol. 60, no. 3, pp. 1562–1572, mar 2014.

[22] F. Dupuis, M. Berta, J. Wullschleger, and R. Renner, “One-shot decoupling,” *Communications in Mathematical Physics*, vol. 328, no. 1, pp. 251–284, mar 2014.

[23] O. Szehr, F. Dupuis, M. Tomamichel, and R. Renner, “Decoupling with unitary approximate two-designs,” *New Journal of Physics*, vol. 15, no. 5, p. 053022, may 2013.

[24] O. Szehr, “Decoupling theorems,” 2012.

[25] H. F. Davis, “A note on haar measure,” *Proceedings of the American Mathematical Society*, vol. 6, no. 2, pp. 318–321, 1955.

[26] H. P. Robertson, “The uncertainty principle,” *Physical Review*, vol. 34, no. 1, p. 163, 1929.

[27] R. Konig, S. Wehner, and J. Wullschleger, “Unconditional security from noisy quantum storage,” *IEEE Transactions on Information Theory*, vol. 58, no. 3, pp. 1962–1984, mar 2012. [Online]. Available: https://doi.org/10.1109%2Ftit.2011.2177772