# Quantum ramp secret sharing from Haar scrambling

Kiran Adhikari

Emmy Noether Group for Theoretical Quantum Systems Design, Technical University of Munich, Germany

Quantum information scrambling has emerged as a powerful tool for studying the dynamics of chaotic quantum many-body systems, assessing benchmarking protocols, and even investigating exotic black hole models [1, 2]. During quantum information scrambling, localized quantum information disperses across the entire system, hiding from the observers who can only access part of it. On the other side, we have a fundamental cryptographic primitive called secret-sharing schemes, where a dealer shares a quantum secret with a group of parties, such that any subset of parties above a specific threshold size can reconstruct it. In this paper, we demonstrate that two protocols, Haar scrambling, which serves as a baseline for other scrambling techniques, and quantum secret sharing, are indeed equivalent. The scheme one gets out of this is of a ramp secret-sharing nature rather than a threshold scheme. We expect this because of the inherent randomness present in Haar unitaries. Moreover, by varying the purity of the initial states, we demonstrate that it is possible to obtain all possible types of ramp secret-sharing schemes. Furthermore, utilizing complexity theoretic arguments, we argue that the protocol can be implemented efficiently, i.e., in polynomial time. Finally, we explore potential applications, ranging from security implications for distributed quantum networks to cryptography in the Noisy Intermediate-Scale Quantum (NISQ) era, and draw insights for fundamental physics, such as many-body physics and quantum black holes.

## 1 Introduction

Quantum information scrambling has emerged as a crucial tool for studying complicated quantum systems [3, 4, 2] ranging from chaotic many-body quantum systems to exotic quantum black hole physics [5, 6] and facilitating various randomization and benchmarking protocols [7, 8]. The process of quantum scrambling leads to the generation of global entanglement, causing initially localized quantum information to disperse throughout the system, thereby concealing it from observers who can only access part of it. Therefore, this phenomenon can also be seen as a form of "thermalization of the quantum information" and is crucial in understanding information spreading in quantum systems.

The literature on quantum information scrambling encompasses diverse forms and definitions, which can broadly be classified into three types. The first family emphasizes Hamiltonians exhibiting quantum chaotic features with out-of-time ordered correlators (OTOCs) being a popular diagnostic tool [9, 10, 11]. In this context, the decay of OTOCs serves as a signature of quantum information scrambling. The second family focuses on information-theoretic tools, such as mutual information and tri-partite information, to track the spread of information and, therefore, to define quantum information scrambling [2]. However, obtaining exact analytical results for these information theoretic quantities is challenging. The third family of models, where exact analytical results can be obtained, involves random unitaries drawn from the Haar measure, which is called Haar scrambling [5]. Haar scrambling serves as a baseline for scrambling, as we expect the late-time values of entropy and mutual information for any scrambling unitary to match those of Haar scrambling. Furthermore, Haar scrambling falls under the category of chaotic scrambling, as the out-of-time ordered correlators (OTOCs) for Haar random unitaries exhibit characteristic decay behavior.

Kiran Adhikari: kiran.adhikari@tum.de

From the realm of many-body quantum systems, let us now traverse into the fascinating land of cryptography. Secret-sharing schemes serve as a fundamental primitive for various cryptographic protocols. In a threshold quantum secret sharing protocol [12], a dealer shares a quantum secret with a group of parties such that any subset of parties above a specific threshold size can reconstruct it. In contrast, parties below the threshold size are not allowed to. Shamir [13] and Blakley [14] proposed the first classical secret sharing schemes, while various quantum secret sharing schemes were proposed in [15, 16, 17, 12]. In the literature, various types of secret sharing schemes can be found. In a quantum threshold scheme $((k, n))$, an arbitrary quantum secret is divided into $n$ parties such that any set of parties larger than $k$ can perfectly reconstruct it while parties of size less than $k$ have no information about it [15]. Unlike in threshold secret sharing schemes, there also exists a ramp secret sharing protocol, where partial information about the secret is allowed to leak to a set of participants that cannot fully reconstruct the secret. In particular, there are parameters $1 \leq b < g \leq n$ such that the set of parties of size at least $g$ should be able to reconstruct the secret, while sets of parties of size at most $b$ cannot learn anything about the secret. Furthermore, we make no requirement on the parties of size $g - b$. Blakley [14] and Meadows [18] first introduced the classical ramp secret sharing scheme, which they later used to construct efficient and secure multiparty computation protocols [19]. Compared to quantum threshold secret sharing, quantum ramp secret sharing has not been extensively explored [20, 21].

Intuitively, classical cryptography can be viewed as the scrambling and descrambling (encryption and decryption) of messages between two parties. Our goal in this paper is to have a quantum version of it. We primarily focus on Haar scrambling for two reasons. Firstly, it allows us to derive analytical results. Secondly, Haar scrambling serves as a baseline for other scrambling unitaries, enabling the extension of results obtained for Haar scrambling to other scenarios as well. A Haar scrambling unitary has the capacity to generate global entanglement, which implies that they can be a good encoder for quantum error correction codes, as implied by the decoupling theorem [22]. Given that all quantum secret sharing schemes are variants of quantum error correcting codes [15, 17, 23], it is natural to anticipate a connection between scrambling and secret sharing. In particular, bounds from standard as well as entanglement-assisted quantum error-correcting codes [24, 25] can be used to create various kinds of secret-sharing schemes.

In this paper, we show that two protocols, Haar scrambling, and quantum secret sharing, are indeed equivalent. The scheme one gets out of this is of a ramp secret-sharing nature rather than a threshold scheme. The ramp nature is expected because of the inherent randomness in Haar scrambling. By changing the purity of the initial states, we show that it is possible to obtain all possible ramp secret-sharing schemes. Furthermore, the protocol can be efficiently implemented in polynomial time by approximating the scrambling unitary using $t$-design circuits. We also discuss some potential applications of our work, such as security applications in a distributed quantum network, cryptography in the Noisy Intermediate-Scale Quantum (NISQ) era [26], and drawing insights for fundamental physics domains, including many-body physics and quantum black holes. The structure of the paper is as follows. In Section 2, we review concepts from quantum information theory relevant to the paper. In section 4, we review various notions of quantum information scrambling introduced in the literature. We also propose a novel definition of information scrambling based on quantum information theoretic quantities. In section 5, we formalize the notion of ramp secret sharing and show that it is equivalent to Haar scrambling.

## 2 Preliminaries

In this section, we provide a brief review of the concepts from quantum information theory relevant to this paper. For a more comprehensive introduction to these concepts, interested readers can refer to the literature [27, 28]. Let us consider a quantum system $X$ consisting of $m$ degrees of freedom modeled by the algebra of $m \times m$ matrices over the complex numbers, denoted by $\mathcal{M}_m$. The state of $X$ is described by its density matrix $\rho_X \in \mathcal{M}_m$. In classical information theory, Shannon entropy provides a measure of uncertainty of a random variable, whereas von Neumann entropy generalizes it to the quantum case. The von Neumann entropy of $X$ with density matrix

$\rho_X$ is given by:

$$S(X) = -\operatorname{Tr}(\rho_X \log \rho_X) = -\sum_{j=1}^{m} \lambda_j \log \lambda_j, \tag{1}$$

where $\lambda_1, \ldots, \lambda_m$ are the eigenvalues of $\rho_X$. Using quantum entropy, one can introduce a quantum generalization of classical mutual information, called quantum mutual information, which gives a measure of the correlation between different quantum systems. Let us consider two quantum systems, $X$ and $Y$, with density matrices $\rho_X$ and $\rho_Y$, respectively. The quantum mutual information between $X$ and $Y$ is defined as:

$$I(X:Y) = S(X) + S(Y) - S(XY), \tag{2}$$

where $S(X)$, $S(Y)$, and $S(XY)$ are the von Neumann entropies of $X$, $Y$, and the joint system $XY$, respectively. In addition to the von Neumann entropy, there exists a quantum version of the classical Rényi entropy, called the quantum Rényi entropy. For a given quantum system $X$ with density matrix $\rho_X$, the Rényi entropy of order $\alpha$ is defined as:

$$S^{\alpha}(X) = \frac{1}{1-\alpha} \log \operatorname{Tr}[\rho_X^{\alpha}], \tag{3}$$

where $\alpha \geq 0$ and $\alpha \neq 1$. For integer values of $\alpha$, the Rényi entropy only involves integer powers and traces of the density matrices, making it easier to compute for physically relevant situations. Moreover, in the limit $\alpha \to 1$, the Rényi entropy reduces to the von Neumann entropy:

$$\lim_{\alpha \to 1} S^{\alpha}(X) = S(X). \tag{4}$$

The Rényi entropy is upper bounded by $\log d$, where $d$ is the dimension of the Hilbert space of the system, and this upper bound is achieved if and only if $\rho_X$ is a maximally mixed state, i.e., $\rho_X = \frac{\mathbf{1}}{d}$. We can also define the Rényi version of mutual information between two quantum systems $X$ and $Y$ as:

$$I^{\alpha}(X:Y) = S^{\alpha}(X) + S^{\alpha}(Y) - S^{\alpha}(XY). \tag{5}$$

Frequently, there is a need to compare two different quantum states. Such a comparison can aid in, for instance, evaluating the output of an ideal quantum protocol against a noisy one. One possible method is to employ the operator trace norm, also referred to as the $L_1$ norm. The $L_1$ norm for any operator $M$ is defined as follows:

$$||M||_1 = \operatorname{Tr}\sqrt{M^{\dagger}M}. \tag{6}$$

This norm can be used to calculate the distance between two density matrices $\rho$ and $\sigma$, which is represented by $||\rho - \sigma||_1$. The trace norm distance is motivated physically because for $||\rho - \sigma||_1 < \epsilon$, $\operatorname{Tr}(\Pi(\rho - \sigma)) < \epsilon$ for any projection operator $\Pi$. This implies that the probability outcome of any experiment between two density matrices $\rho$ and $\sigma$ differs by at most $\epsilon$. Once the distance between two density matrices is established, the quantum mutual information can be employed to place an upper bound on the correlation between two distinct quantum systems. This bound is also referred to as quantum Pinsker's inequality [28]. The normalized trace distance between $\rho(XY)$ and $\rho(X) \otimes \rho(Y)$ can be defined as $\Delta = \frac{1}{2}||\rho(XY) - \rho(X) \otimes \rho(Y)||_1$. Then quantum Pinsker's inequality implies [28]:

$$\frac{2}{\ln 2}\Delta^2 \leq I(X:Y) \tag{7}$$

When the mutual information $I(X:Y)$ is small, it indicates little correlation between the two quantum systems $X$ and $Y$. Thus the joint state $\rho(XY)$ can be approximated by the tensor product of the marginal states $\rho(X)$ and $\rho(Y)$. Another measure of distance between two quantum states is the fidelity, which is defined as $F(\rho(X), \rho(Y)) = (\operatorname{Tr}\sqrt{\rho(X)\rho(Y)})^2$, where $\sqrt{M}$ denotes the unique positive square root of a positive semidefinite matrix $M$. The trace distance can be used to provide upper and lower bounds on the fidelity through the Fuchs-van de Graaf inequalities [28], which are given by

$$1 - \sqrt{F(\rho(X), \rho(Y))} \leq \Delta \leq \sqrt{1 - F(\rho(X), \rho(Y))} \tag{8}$$

where $\Delta$ is the normalized trace distance. The fidelity is bounded below by 0 and above by 1. Two density matrices $\rho(X)$ and $\rho(Y)$ are said to be $\mu$-distinguishable if $F(\rho(X), \rho(Y)) \leq 1 - \mu$, and $\nu$-indistinguishable if $F(\rho(X), \rho(Y)) \geq 1 - \nu$.

Another extremely important concept in quantum information theory is the decoupling inequality, which has wide-ranging applications such as quantum error correction, transmission of quantum information, protocols such as state merging, coherent state merging, thermodynamics, many-body physics, and even black hole information theory [6, 22, 24, 5]. Suppose a composite system $XY$ is in a joint state $\rho(XY)$. The subsystem $X$ is decoupled from $Y$ if: $\rho(XY) = \rho(X) \otimes \rho(Y)$. This means that the system $X$ is uncorrelated with $Y$ and is therefore statistically independent of any measurement on $Y$. One common way to analyze this setup is to start with the pure state system $RA$, Alice's message $A$ purified with reference $R$. After this, we encode Alice's message $A$ using a unitary encoding and allow it to interact with the environment, which yields the final output $BE$. $B$ here can represent Bob's received message. If the encoding is done such that $R$ and $E$ decouple, then this implies that there exists a decoding protocol, allowing Bob to recover Alice's message $A$ just by having system $B$. This works even for the case when $R$ and $E$ are approximately decoupled, $\rho(RE) \overset{\epsilon}{\approx} \rho(R) \otimes \rho(E)$, that is,

$$F(\rho(RE), \rho(R) \otimes \rho(E)) \geq 1 - \epsilon \text{ for some } \epsilon \geq 0 \tag{9}$$

Uhlmann's theorem [28] guarantees that there exists a decoder such that having system $B$, one can approximately reconstruct Alice's message $\rho(A') \overset{\epsilon}{\approx} \rho(A)$, that is:

$$F(\rho(A'), \rho(A)) \geq 1 - \epsilon \text{ for some } \epsilon \geq 0 \tag{10}$$

We will later utilize the decoupling theorem to define the concept of quantum information scrambling.

## 2.1 Secret sharing schemes

Secret-sharing schemes serve as cryptographic primitives and are commonly employed in the construction of various cryptographic protocols. Classical secret sharing schemes were proposed by Shamir [13] and Blakley [14], while various quantum secret sharing schemes were proposed in [15, 16, 17, 12]. In a secret sharing scheme protocol, a dealer $\mathcal{D}$ distributes a secret $S$ among a set of players $\mathcal{P}$ such that only a certain sufficiently large group can reconstruct it [12]. Let $\mathcal{P} = \{P_1....P_m\}$ be a set of players. A collection $\Gamma \subseteq 2^{\{P_1....P_m\}}$ is monotone if $B \in \Gamma$ and $B \subseteq C$ imply that $C \in \Gamma$. An access structure $\Gamma = (\Gamma_{\text{YES}}, \Gamma_{\text{NO}})$ is a pair of collections of sets such that $\Gamma_{\text{YES}}, \Gamma_{\text{NO}} \subseteq 2^{\{P_1....P_m\}}$, the collections $\Gamma_{\text{YES}}$ and $2^{\{P_1....P_m\}} \setminus \Gamma_{\text{NO}}$ are monotone and $\Gamma_{\text{YES}} \cap \Gamma_{\text{NO}} = \emptyset$. Sets in $\Gamma_{\text{YES}}$ are called authorized sets, and the sets in $\Gamma_{\text{NO}}$ are called unauthorized sets. The access structure is called an incomplete access structure if there is at least one subset of parties $A \subseteq P$ such that $A \notin \Gamma_{\text{YES}} \cup \Gamma_{\text{NO}}$. Otherwise, it is referred to as a complete access structure.

In a quantum secret sharing scheme, a dealer $D$ wants to share a quantum state $|X\rangle$ with a set of players $\mathcal{P}$ with access structure $\Gamma \in 2^{\mathcal{P}}$. The quantum secret $|X\rangle$ is choosen from set of possible quantum set $\mathcal{X} = \{|X_1\rangle, |X_2\rangle, ...., |X_n\rangle\}$, where $|X_i\rangle$ is chosen with probability $p_i$. Then, the state of the quantum secret can be represented by the density matrix $\rho_S$ as:

$$\rho_S = p_1 |X_1\rangle \langle X_1| + p_2 |X_2\rangle \langle X_2| + ..... + p_n |X_n\rangle \langle X_n| \tag{11}$$

Let us introduce a reference system $R$ with Hilbert space $\mathcal{H}_R$, and a purification denoted by $|SR\rangle \in \mathcal{H}_S \otimes \mathcal{H}_R$. Let us denote by $A$ a subset of players described by a set $A = \{P_1, ..., P_j\} \subseteq \mathcal{P}$. Distribution of shares is given by a completely positive isometric map,

$$\Lambda_D : S(\mathcal{H}_S) \to S(\mathcal{H}_1 \otimes ..... \otimes \mathcal{H}_m) \tag{12}$$

where $S(\mathcal{H}_A)$ represents the state space of the system $A$. We denote by $|RP_1....P_m\rangle$ the state of quantum system $RP_1....P_m$ after applying $\Lambda_D$ to S, and identity to $R$. Now, we provide the information-theoretic definition of a quantum secret sharing scheme based on [12].

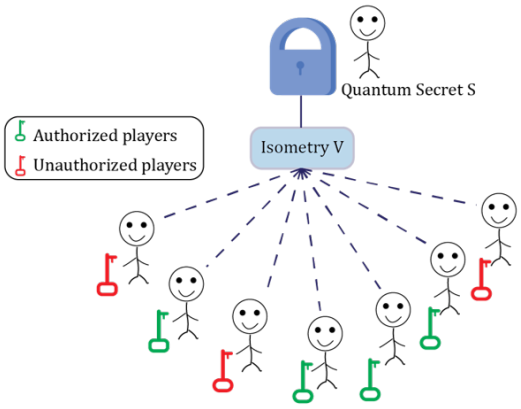



Figure 1: $((k,n))$ Quantum Secret Sharing(QSS) threshold schemes; $k$ players out of $n$ players have to come together to reconstruct the original secret. Any arbitrary collection of players larger than size $k$ is called authorized players, while one with fewer than $k$ is called unauthorized players.

**Definition 1** ([12]). *Let $R$ be a reference system such that $SR$ is in a pure state. A quantum secret sharing scheme is a completely positive map which distributes a quantum secret $S$ among a set of players $\mathcal{P} = \{P_1....P_m\}$ such that it realizes an access structure $\Gamma = (\Gamma_{YES}, \Gamma_{NO})$ with the following two requirements:*

- *recoverability requirement: For all $A \in \Gamma_{YES}$, we have that $I(R:A) = I(R:S)$.*
- *secrecy requirement: For all $A \in \Gamma_{NO}$, we have $I(R:A) = 0$*

Such a scheme is also called a threshold or "all or nothing" scheme because every set of players in $\Gamma_{\text{YES}}$ can reconstruct the secret perfectly, while a set in $A \in \Gamma_{\text{NO}}$ has no information about it. Furthermore, it is known that these conditions are necessary and sufficient for quantum error correction [29]. A quantum threshold scheme is also denoted by $((k,n))$ where an arbitrary quantum secret is divided into $n$ parties such that any $k$ or more parties can perfectly reconstruct the secret while any $k-1$ or fewer parties have no information at all about the secret. This also means that the reduced density matrix of these $k-1$ parties is independent of the secret.

**Definition 2** ([17]). *Let $1 \leq k \leq n$. A $k$ out of $n$, $((k,n))$, quantum threshold access structure $\Gamma$ over a set of players $\mathcal{P} = \{P_1....P_n\}$ is the complete access structure accepting all subsets of size at least $k$, that is $\Gamma_{YES} = \{A \subseteq \mathcal{P} : |A| \geq k\}$ and $\Gamma_{NO} = \{A \subseteq \mathcal{P} : |A| \leq k-1\}$*

An example of a $((2,3))$ quantum threshold scheme is given in Appendix D. In quantum secret sharing schemes, it is possible to encode the quantum secret into the players, which can be in a pure or mixed state. A pure state quantum secret sharing is a scheme to encode quantum secrets as a pure state, while a mixed state quantum secret sharing is a scheme to encode the quantum secret as mixed states [15, 17]. Furthermore, the scheme itself can be perfect or approximate.

**Definition 3.** *Let $R$ be a reference system such that $SR$ is in a pure state. A approximate quantum secret sharing is a scheme where a quantum secret $S$ among a set of players $\mathcal{P} = \{P_1....P_m\}$ such that it realizes an access structure $\Gamma = (\Gamma_{YES}, \Gamma_{NO})$ with relaxed conditions:*

- *Relaxed recoverability requirement: For all $A \in \Gamma_{YES}$, we have $I(R:A) \geq I(R:S) - \delta$ for some small $\delta$.*
- *Relaxed secrecy requirement: for all $A \in \Gamma_{NO}$, we have $I(R:A) \leq \gamma$ for some small $\gamma$.*

A relaxed recoverability requirement guarantees that the authorized parties can reconstruct the secret with high fidelity. The relaxed secrecy requirement ensures that the correlation between the quantum secret $S$ and unauthorized parties $B$ is small, preventing unauthorized parties from having much information about the secret.

Unlike in threshold secret sharing schemes, a ramp secret sharing protocol exists where partial information about the secret is allowed to leak to a set of participants that cannot fully reconstruct the secret. In particular, there are parameters $1 \leq b < g \leq n$ such that the set of parties of size at least $g$ should be able to reconstruct the secret, while sets of parties of size at most $b$ cannot learn anything about the secret. Furthermore, we make no requirement on the parties of size $g - b$. $g$ and $b$ stand for good and bad, respectively. Such a scheme is denoted by $(b, g)$ ramp secret sharing scheme. A quantum version would be denoted by $((b, g))$. The classical ramp secret sharing scheme was first introduced by Blakley and Meadows [18], and later used to construct the efficient secure multiparty computation protocols [19]. Compared to quantum threshold secret sharing, quantum ramp secret sharing has not been extensively explored [20, 21].

## 3 Our contributions

In this section, we provide an overview of our main contributions, outlined as follows

- In the literature, one can find various notions of quantum information scrambling. We have provided a novel information-theoretic definition of scrambling that encompasses these other notions. This information-theoretic definition, which we refer to as $l$ scrambling, goes as follows. Suppose $RA$ is in a pure state. A unitary operator $U_{AB} : A \otimes B \to C \otimes D$ is called $l$-scrambling if any arbitrary subsystem $C$ of size less than $l$ approximately decouples from $R$.
- Information theoretic definition of scrambling allows us to show that Haar scrambling, a random unitary chosen from Haar measure, is equivalent to $\left(\left(\frac{N+s(\mathcal{P})}{2} - \epsilon, \frac{N+s(\mathcal{P})}{2} + \epsilon\right)\right)$ quantum ramp secret sharing scheme. Here $N$ is the total size of players $\mathcal{P}$, $s(\mathcal{P})$ is the Von Neumann entropy of the players, and $\epsilon$ is a measure of accuracy.
- The simple counting argument shows that it requires an exponential number of gates, $\mathcal{O}(4^n)$, to implement the $n$ qubit Haar unitary. This would make this protocol exponentially hard to implement. However, using $t$ design arguments, we show that the protocol, both encoding and decoding, can be implemented efficiently, i.e., using only a polynomial number, $\mathcal{O}(n^2)$, of one and two-qubit gates.

## 4 Quantum Information Scrambling

The phenomenon of "scrambling" of quantum information is a fundamental concept closely related to many-body physics, quantum chaos, complexity theory, and black holes [1, 2]. This phenomenon can be viewed as a form of "thermalization of the quantum information" and is crucial for understanding the spread of information in quantum systems. As illustrated in Figure 2, at time $t = 0$, the reference $R$ is only entangled with the Alice qubit $q_A$, such that $S(R) = S(q_A) = 1$, $S(Rq_A) = 0$, and $I(R : q_A) = 2$. As time progresses, the quantum information from Alice's qubit becomes increasingly scrambled, depending on the system's dynamics. This is because the initially localized entanglement of Alice's qubit with the reference $R$ begins to expand across the system. In one scenario, the dynamics can be such that the information is carried coherently, for example, through a circuit using only SWAP gates. The information is highly localized in this case, and the unitary cannot be considered scrambling. Conversely, in strongly interacting systems, the entanglement spreads in a complex fashion such that the reference $R$ becomes entangled with a large collection of qubits. In this case, the information is considered to be scrambled. Because quantum mechanics is unitary, information cannot be lost globally. Therefore, to define information scrambling, we must focus on subsystems.

To study the spreading of information in quantum dynamics, we consider the following simple model where we have a Hilbert space of $n = |A| + |B| = |C| + |D|$ qudits partitioned as:

$$\mathcal{H} = A \otimes B = C \otimes D \tag{13}$$

and a unitary map

$$U_{AB} : A \otimes B \to C \otimes D \tag{14}$$

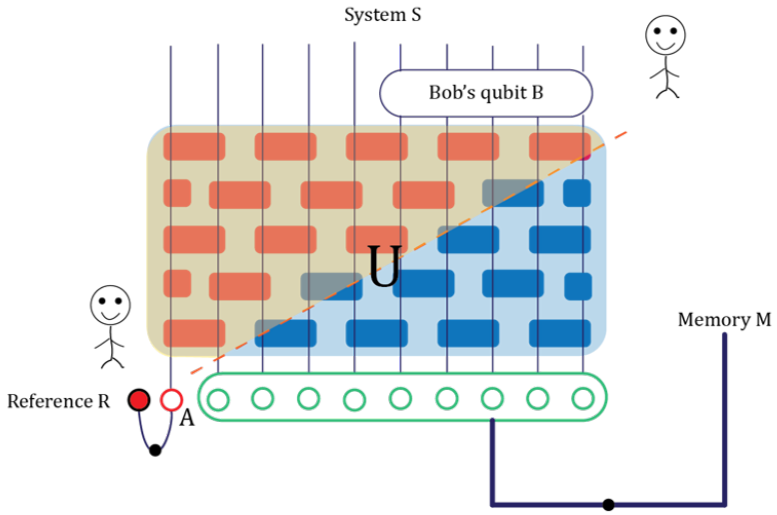



Figure 2: Alice and Bob try to communicate via a scrambling unitary $U$ acting on N qubits. Alice has full control of the first qubit $A$, which is entangled with the reference system $R$. The rest of the qubits, marked green, can be in a mixed state $\rho$ purified by an external system called Memory. This pure state is denoted by $\left|\sqrt{\rho}\right\rangle$. The scrambling unitary acts only on Alice's qubit and the system's qubit, which is marked green. After the unitary evolution, Bob then has access to the system's set of qubits. If the scrambling unitary has a local structure, it is also possible to have an information light cone indicated by a yellow cone. The initial state of the system, including the reference, the system, and the memory, is: $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_R |0\rangle_{q_A} + |1\rangle_R |1\rangle_{q_A}) \left|\sqrt{\rho}\right\rangle$ Since the time evolution unitary doesn't act on reference and memory, the total dynamics is then given by: $|\psi(t)\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle_R U_S \otimes I_{\text{MEM}} \left|0, \sqrt{\rho}\right\rangle + |1\rangle_R U_S \otimes I_{\text{MEM}} \left|1, \sqrt{\rho}\right\rangle\right)$. More detail about this figure is in Appendix A.

Suppose Alice chooses to encode her quantum information in system $A$. Additionally, we introduce an external reference system $R$, which is perfectly entangled with $A$. The Alice system then interacts with another system $B$, which is purified by the external system $B'$. Thus, the total initial state is $|RA\rangle |BB'\rangle$, and the final state is:

$$|\psi\rangle_{RB'CD} = U_{AB} \otimes I_{RB'} |RA\rangle |BB'\rangle \tag{15}$$

The overall setup is depicted in Figure 3. In the literature, various notions of quantum information scrambling are presented, which we have classified into three levels of hierarchy. The first level is Haar scrambling, where the unitary $U$ is a random quantum circuit selected from the Haar measure. The objective is to determine whether a part of the system is maximally mixed and, if not, how close it is to being in a maximally mixed state. A maximally mixed state represents a state in which information is thermalized. At the second level, we encounter chaotic scrambling, where the Hamiltonian governing the quantum dynamics exhibits quantum chaotic behavior. Chaotic scrambling includes Haar scrambling, as proven in [30], but can also involve other families of unitaries. At the third level, we provide an information-theoretic definition of scrambling, encompassing both Haar and chaotic scrambling.

## 4.1 Haar scrambling

In Haar scrambling, we have a unitary $U$ that is chosen at random from the Haar measure. This serves as a baseline for scrambling, as we expect the late-time values of entropy and mutual information for any scrambling unitary $U(t)$ to match those of Haar random unitaries. However, a pure random unitary circuit of size $2^n \times 2^n$ does not have any inherent local structure. To account for locality, one can restrict the situation to be local in one or two-qubit gates.

**Definition 4** ([2]). *A Haar scrambled quantum state is the state obtained by applying a random unitary $U$ chosen from group-invariant Haar measure, $|\psi(U)\rangle = U |\psi_0\rangle$.*

The Haar measure possesses several interesting mathematical properties, enabling the derivation of analytical results for various information-theoretic quantities [31]. We briefly review some of these properties in Appendix B. One important physical characteristic of Haar scrambling is that a randomly chosen pure state in $\mathcal{H}_{AB}$ is likely close to a maximally entangled state if $\frac{|A|}{|B|} << 1$. This property is known as Page scrambling, named after Page, who first introduced it to explain black hole physics [32]. Mathematically, for any bipartite Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, we have:

$$\int dU ||\rho_A(U) - \frac{I_A}{|A|}||_1 \leq \sqrt{\frac{|A|^2 - 1}{|A||B| + 1}} < \frac{\rho + 2}{1} \tag{16}$$

and when $|B|$ is significantly larger than $|A|$, the typical deviation of $\rho_A$ from maximally mixed state is extremely small. For example, if $B$ has 10 more qubits than $A$, then the typical deviation from maximal entanglement is bounded by $2^{-5}$. Using the analytical results from Appendix B, it is possible to analytically compute the Rényi entropy between the reference $R$ and the subsystem $C$ using Eq. 48. Unfortunately, the quantity $I_2(X : Y) = S_2(X) + S_2(Y) - S_2(XY)$ is not a good candidate for mutual information as it violates the data processing inequality [33]. Moreover, it is generally not even possible to use this quantity to obtain bounds for the quantum mutual information, which is the actual quantity of interest. However, for the Haar scrambling case, $R$ is in a maximally mixed state, and $C$ is expected to be close to a maximally mixed state [34]. In this case, we can use Rényi entropy to upper-bound the mutual information as follows:

$$I(R : C) \leq \log |R| + \log |C| - S_2(RC), \tag{17}$$

where $S_2$ denotes the second Rényi entropy. For example, let us consider a case where $A$ is a single qubit. Let $p$ be the size of region $C_p$. The Rényi entropy of $C_p$ and $RC_p$ can be analytically computed using Eq. 48 and can be found in [35, 1, 36]. Then, using Eq. 17, we can upper-bound the quantum mutual information between $R$ and $C_p$ as

$$I(R : C_p) \leq 1 + \log_2 \left(2 - \frac{3(1 - 2^{2p-2N})}{2 + (2^{-s} - 2^{-N+1})4^{p-N/2}}\right), \tag{18}$$

where $s$ is the second Rényi entropy of system $B$.

## 4.2 Chaotic Scrambling (OTOC measure)

In this section, we review the concept of chaotic scrambling, which involves a Hamiltonian exhibiting quantum chaotic features. Quantum chaotic Hamiltonians are typically strongly interacting systems that spread quantum information throughout the whole system. The measurement of Out-of-Time-Ordered Correlators (OTOCs) [9, 10, 11] is often employed to gauge quantum chaos. For a brief overview of OTOCs, refer to Appendix C. To formulate the chaotic scrambling in the language of quantum channels, we consider a Hilbert space of $n = |A|+|B| = |C|+|D|$ qubits that are partitioned as: $\mathcal{H} = A \otimes B = C \otimes D$, and a unitary map $U_{AB} : A \otimes B \to C \otimes D$. Let the dimension for the system be denoted by $d$. Suppose $a$, $b$, $c$, and $d$ corresponds to the size of $A$, $B$, $C$ and $D$ respectively and the corresponding dimensions be denoted by $d_A$, $d_B$, $d_C$ and $d_D$ respectively. For systems consisting of qubits only, it would be $d = d_A d_B = 2^a 2^b = d_C d_D = 2^c 2^d = 2^{a+b} = 2^{c+d} = 2^n$. Let $O_i$ be hermitian operators supported on region $i$, where $i \in A, B, C, D$ and define $O_i(t) = U^\dagger O(0) U$. With this setup, we refer to the chaotic scrambling as unitary exhibiting chaotic features given by the OTOCs measure [30].

**Definition 5** ([30]). *A unitary operator $U_{AB}$ is called chaotic scrambling iff it satisfies:*

$$\langle O_A(0) O_B(t) O_C(0) O_D(t) \rangle \simeq \langle O_A O_C \rangle \langle O_B \rangle \langle O_D \rangle + \langle O_B O_D \rangle \langle O_A \rangle \langle O_C \rangle - \langle O_A \rangle \langle O_B \rangle \langle O_C \rangle \langle O_D \rangle \tag{19}$$

*where $\simeq$ means up to an order $d^{-2}$.*

In terms of the size of subsystems, this definition implies that a unitary $U_{AB}$ is chaotic scrambling if it satisfies:

$$\langle O_A(0) O_B(t) O_C(0) O_D(t) \rangle \simeq \frac{1}{d_A^2} + \frac{1}{d_D^2} - \frac{1}{d_A^2 d_D^2} \tag{20}$$

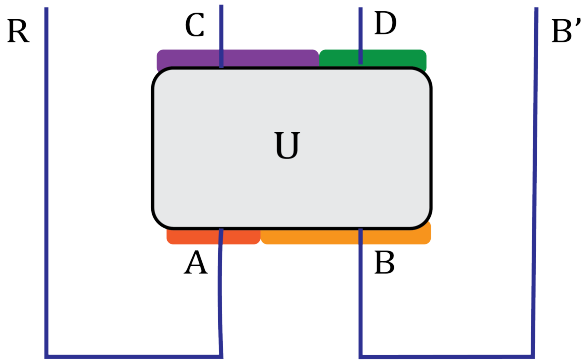



Figure 3: Suppose Alice decides to encode her quantum information in $A$, which is perfectly entangled with external reference state $R$. Alice's qubit then interacts with system $B$, which is also purified with external system $B'$. Thus the total initial state is $|RA\rangle |BB'\rangle$ while final state after scrambling unitary $U_{AB}$ is $|\psi\rangle_{RB'CD} = U_{AB} \otimes I_{RB'} |RA\rangle |BB'\rangle$.

However, it's important to note that defining quantum chaos via OTOCs doesn't always correspond to true quantum chaos [37]. When averaging $\langle O_A(0)O_B(t)O_C(0)O_D(t)\rangle$ over Haar random unitary $U$, it also satisfies the condition for chaotic scrambling. Thus, Haar scrambling belongs to the family of chaotic scrambling.

### 4.3 $l$ scrambling

During scrambling, a generation of global entanglement causes the initially localized quantum information to spread across the system, thereby hiding it from the observer, who can only access a portion of it. Consequently, information-theoretic measures like entanglement entropy and mutual information emerge as natural and powerful tools for formally defining quantum information scrambling. To give an information theoretic setting, we will again consider the Hilbert space of $n = |A| + |B| = |C| + |D|$ qubits partitioned as:

$$\mathcal{H} = A \otimes B = C \otimes D \tag{21}$$

and a unitary map

$$U_{AB} : A \otimes B \to C \otimes D \tag{22}$$

Suppose Alice chooses to encode her quantum information in system $A$. Additionally, we introduce an external reference system $R$, which is perfectly entangled with $A$. The Alice system then interacts with another system $B$, which is purified by the external system $B'$. Thus, the total initial state is $|RA\rangle |BB'\rangle$, and the final state is:

$$|\psi\rangle_{RB'CD} = U_{AB} \otimes I_{RB'} |RA\rangle |BB'\rangle \tag{23}$$

The overall setup is depicted in Figure 3.

Thus, it becomes evident that a definition of scrambling must entail that accessing a small part of the subsystem $C$ should not grant one the ability to obtain much information about system $A$. In the literature, it is frequently assumed that the state $BB'$ is maximally entangled [2]. In such a scenario, system $C$ becomes decoupled from $R$ provided that the size $D$ is larger than that of $A$. However, it becomes more complicated when $BB'$ does not form a maximally entangled state. To address this issue, we propose a new definition of scrambling unitary where $R$ and $C$ are nearly

independent for most $C$ with a size smaller than some parameter $l$, which interestingly depends upon the purity of $B$.

**Definition 6** ($l$- scrambling)**.** *Suppose $RA$ is in a pure state. A unitary operator $U_{AB} : A \otimes B \to C \otimes D$ is called $l$-scrambling if any arbitrary subsystem $C$ of size less than $l$ approximately decouples from $R$: $\rho_{RC} \overset{\epsilon}{\approx} \rho_R \otimes \rho_C$ that is,*

$$F(\rho_{RC}, \rho_R \otimes \rho_C) \geq 1 - \epsilon \text{ for some } \epsilon \geq 0 \text{ for any } C \text{ with } |C| < l \tag{24}$$

Hence, the outcome of any measurement on $C$ is statistically independent of any measurement on $R$. Moreover, the decoupling theorem [22, 34] implies that having access to the system $DB'$ allows for the existence of a decoder that can reconstruct a state $\rho_A$ with high fidelity. Thus, $l$-scrambling is related to both information hiding and retrieval.

The parameter $l$ depends on the purity of the state $B$ but is independent of how information was scrambled, i.e., on the structure of the scrambling unitary $U_{AB}$. However, there are other quantities, such as scrambling time (the time taken to scramble quantum information) and the complexity of the scrambling unitary, which depends on the structure of the unitary $U_{AB}$. These quantities are crucial while studying the dynamics of physical systems and quantum circuits. It is worth noting that this definition of $l$-scrambling doesn't allow us to make a statement for system $C$ with sizes greater than $l$. For example, subsystem $D$ could have partial or no correlation with $R$.

Another measure of information scrambling often considered in the literature is the tripartite information [2, 38], denoted as $I_3(R : C : D) = I(R : C) + I(R : D) - I(R : CD)$. This quantifies the information about system $A$ that is non-locally hidden over arbitrary subsets $C$ and $D$. It is commonly asserted that a quantum system that scrambles information must have a non-positive tripartite information $I_3(A : C : D)$, and that the maximal negativity of $I_3(R : C : D)$ is indicative of the circuit that scrambles information most effectively. However, this notion only applies when $B$ is maximally mixed. In fact, for any unitary $U_{AB} : A \otimes B \to C \otimes D$, we have $I(R : C) + I(R : D) \leq I(R : CD)$ and $I_3(R : C : D)$ is always non-positive. Hence, it cannot serve as a reliable indicator of scrambling. To overcome this issue, we propose a new variant of tripartite information based on the definition of $l$-scrambling, $l$-tripartite information, denoted by $I_3(R : C_l : D_l)$. Here, $C_l$ and $D_l$, which may or may not overlap, have sizes less than $l$, but $C_lD_l$ together have a size greater than or equal to $l$.

**Definition 7** ($l$- tripartite information)**.** *Suppose we have a quantum state $RCD$ which can be pure or mixed. We define $l$-tri partite information, $I_3(R : C_l : D_l)$ as:*

$$I_3(R : C_l : D_l) = I(R : C_l) + I(R : D_l) - I(R : C_lD_l) \tag{25}$$

*where $C_l$ and $D_l$ are subsystems of $CD$ with $|C_l| < l$, $|D_l| < l$ and $|C_lD_l| \geq l$.*

**Remark 1.** *Suppose $RA$ is in a pure state. A unitary operator $U_{AB} : A \otimes B \to C \otimes D$ is $l$-scrambling iff $I_3(R : C_l : D_l)$ is maximally negative i.e. $I_3(R : C_l : D_l) = -I(R : C_lD_l) + \mathcal{O}(\epsilon)$ for some $\epsilon \geq 0$.*

*Proof.* If $U_{AB}$ is $l$- scrambling, then system $C_l$ and $D_l$ decouples from $R$, thus $I(R : C_l) = I(R : D_l) = \mathcal{O}(\epsilon)$. This implies $I_3(R : C_l : D_l) = -I(R : C_lD_l) + \mathcal{O}(\epsilon)$. Furthermore, if $I_3(R : C_l : D_l) = -I(R : C_lD_l) + \mathcal{O}(\epsilon)$, then $I(R : C_l)$ and $I(R : D_l)$ are of order $\mathcal{O}(\epsilon)$. Thus, $C_l$ and $D_l$ decouples from $R$ which implies that $U_{AB}$ is $l$- scrambling. □

Although there are three distinct notions of quantum information scrambling, a hierarchy exists in that $l$-scrambling encompasses both chaotic and Haar scrambling. Chaotic scrambling includes Haar scrambling unitaries [2, 30, 39, 34]. However, the reverse is not always true. $l$-scrambling can be constructed using only Clifford gates, which lack quantum chaotic features [40, 41]. And chaotic unitaries may include other dynamics, such as the mixed-field Ising model, which are not Haar unitary. Since calculating OTOCs typically involves averaging over maximally mixed states, $l$-scrambling offers a more nuanced understanding of information scrambling by considering purity. We plan to establish a more detailed relationship between $l$-scrambling and OTOCs in the future.

## 5 Ramp secret sharing from Haar scrambling

In the definition of $l$-scrambling, we saw that the subsystem with a size less than $l$ has little correlation with the reference system. In secret sharing terminology, this subsystem would be referred to as the unauthorized set. In this section, we will formally show that Haar scrambling exhibits characteristics of ramp secret sharing. This scheme, rather than a threshold one, is expected, as the threshold scheme is hard to obtain from a randomly selected unitary operation. To do the proper analysis, we will first provide an information-theoretic definition of the quantum ramp secret sharing scheme.

**Definition 8.** *Let $1 \leq b < g \leq n$, and $R$ be a reference system such that $SR$ is in a pure state. The $((b, g))$ quantum ramp secret sharing is a a completely positive map which distributes a quantum secret $S$ among a set of players $\mathcal{P} = \{P_1....P_m\}$ such that it realizes an incomplete access structure $\Gamma_{b,g} = (\Gamma_{YES}, \Gamma_{NO})$ with conditions:*

- *Recoverability requirement: If $I(R : A) = I(R : S)$ for all $|A| \geq g$ then $A \in \Gamma_{YES}$. This implies that $A$ can reconstruct the secret.*
- *Secrecy requirement: If $I(R : A) = 0$ for all $|A| \leq b$, then $A \in \Gamma_{NO}$. This implies that $A$ cannot learn anything about secret $S$.*
- *No requirements on sets $A$ where $b < |A| < g$ which we refer as grey area.*

The scheme is then referred to as the $((b, g))$ ramp scheme and can be made approximate with relaxed recoverability and relaxed secrecy requirements as follows.

**Definition 9.** *Let $1 \leq b < g \leq n$, and $R$ be a reference system such that $SR$ is in a pure state. The $((b, g))$ approximate quantum ramp secret sharing is a a completely positive map which distributes a quantum secret $S$ among a set of players $\mathcal{P} = \{P_1....P_m\}$ such that it realizes an incomplete access structure $\Gamma_{b,g} = (\Gamma_{YES}, \Gamma_{NO})$ with conditions:*

- *Relaxed recoverability requirement: If $I(R : A) \geq I(R : S) - \delta$ for all $|A| \geq g$ then $A \in \Gamma_{YES}$.*
- *Relaxed secrecy requirement: If $I(R : A) \leq \gamma$ for all $|A| \leq b$, then $A \in \Gamma_{NO}$.*
- *No requirements on sets $A$ where $b < |A| < g$*

The relaxing parameters $\delta$ and $\gamma$ give a measure of how well authorized parties can reconstruct the secret while unauthorized parties are prevented from recovering it. It the the scheme of this nature that Haar scrambling shows rather than a perfect one. Figure 4 shows the relation between mutual information and the size of parties for perfect and approximate threshold and ramp schemes when a single qubit secret is shared among $N$ parties.

To analyze the quantum ramp schemes $((g, b))$, we introduce two metrics: the gap $G$ and the Rampiness $R$. The gap is defined as the difference between $g$ and $b$, expressed as $G = g - b$. The Rampiness, denoted by $R$, is the ratio of the gap to the total number of players, represented as $R = \frac{G}{N}$. The Rampiness value ranges from zero to one, where $R = 0$ corresponds to the threshold scheme with a gap $G = 0$, and $R = 1$ signifies the absence of any secret sharing scheme with a gap $G = N$. A lower value of $R$ suggests a superior scheme since it indicates a smaller grey region. Naturally, we can extend this definition of rampiness and gap to the approximate scenario by selecting $g$ and $b$ based on relaxed parameters $\delta$ and $\epsilon$.

**Remark 2.** *The lower bound on the size of gap, $G = g - b$ is equal to the size of the quantum secret.*

*Proof.* We call $S$ an important share if there is an unauthorized set T such that $S \cup T$ becomes authorized. The dimension of each important share of a quantum secret sharing scheme must be at least as large as the dimension of the secret [17]. $G$ is an important share, as adding size $G$ parties to the size $b$ parties gives us an authorized set. Thus, $G$ must at least have the size of a quantum secret. □

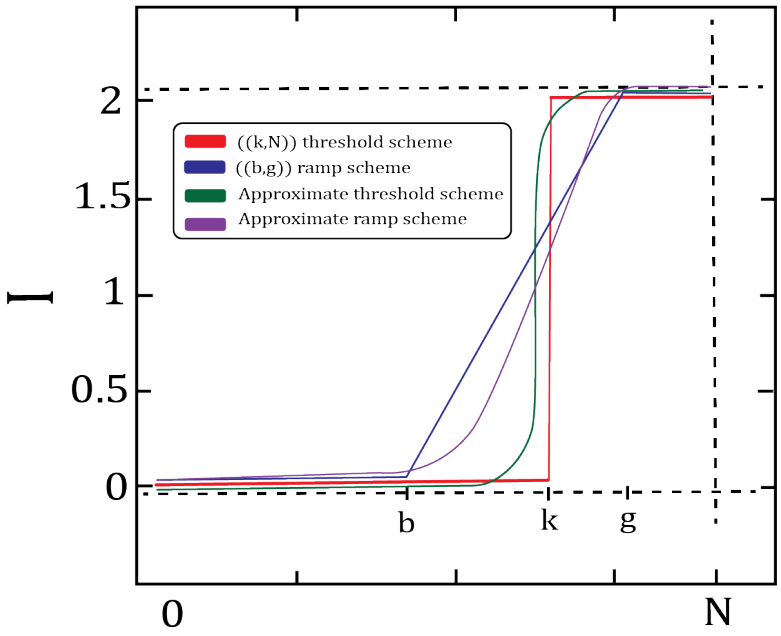



Figure 4: A qubit secret shared among $N$ parties in different scenarios. For the $((k, N))$ scheme, the mutual information between the reference $R$ and the parties goes through a sharp step function-like transition from 0 to 2 as the number of parties crosses the threshold $k$. In $((b, g))$ ramp scheme, the mutual information is zero for parties less than the size $b$ and two when it is greater than $g$ while some mutual information in the grey area i.e. when the player's size is greater than $b$ but less than $g$. Fig b: Includes also approximate $((k, N))$ scheme as for all $|A| \geq k$, $I(R : A) \geq 2 - \delta$ for some small $\delta$ and for all $|A| \geq k$, $I(R : A) \leq \epsilon$ for some small $\epsilon$ and the approximate $((b, g))$ scheme as $I(R : A) \geq 2 - \delta$ for all $|A| \geq g$ and $I(R : A) \leq \epsilon$ for all $|A| \leq b$.

Having established the formal definition of quantum ramp secret sharing, let us delve into the relationship between secret sharing and Haar scrambling. The parameter $l$ of $l$-scrambling has to be less than or equal to the parameter $b$ of the quantum ramp secret sharing scheme: $l \leq b$. We discussed before that the parameter $l$ of $l$-scrambling depends upon the purity of the initial state. Therefore, we will see that, by changing the purity of players, all possible approximate quantum ramp secret-sharing schemes can be obtained. First, we consider the scenario of a pure state and subsequently demonstrate how one can get the mixed state case by discarding players from the pure state case.

For this, let us denote the total system size, i.e., number of players $\mathcal{P} = \{P_1....P_m\}$ by $N$ and the entropy of the $\mathcal{P}$ before the quantum secret is encoded by $s(\mathcal{P})$. Let $1 \leq b < g \leq n$, $S$ be the quantum secret, and $R$ be a reference system such that $SR$ is in a pure state, $((b, g))$ be a quantum ramp schem,e and $P(x)$ be the arbitrary set of players with size $x$.

## 5.1 Ramp secret sharing from Haar scrambling: Pure state case

A pure-state quantum secret sharing scheme encodes quantum secrets into pure states of the players. For a pure initial state of the players, the entropy satisfies $s(\mathcal{P}) = 0$, and for any two disjoint subsets $P(b)$ and $P(N - b)$ we have

$$I(R : P(b)) + I(R : P(N - b)) = I(R : S), \tag{26}$$

since the global state on $RP(N)$ is pure. If $I(R : P(b)) = 0$, then $P(b)$ is an unauthorized set. Because the complementary region $P(N - b)$ cannot both be unauthorized (by the above identity) and cannot overlap with another authorized region (by the no-cloning theorem), one obtains the

constraints

$$\frac{N+1}{2}+1 \;\le\; g \;\le\; N-b, \tag{27}$$

$$N-g \;\le\; b \;\le\; \frac{N-1}{2}. \tag{28}$$

We now analyze the case where the scrambling unitary $U$ is drawn from the Haar measure. Let $P(\ell)$ be any subsystem of size $\ell$ after scrambling, and let $I(P(\ell))$ denote the mutual information between the reference $R$ (one qubit) and this region. Using the average second Rényi entropy of Haar-random states (Appendix B) together with the bound

$$I(R:C) \le \log|R| + \log|C| - S_2(RC), \tag{29}$$

we obtain the general inequality

$$I(P(\ell)) \;\le\; 2\ell - N + \log_2\!\left(1+2^{\,N-2\ell}\right). \tag{30}$$

This expression shows that Haar scrambling cannot realize a threshold secret-sharing scheme: for $\ell = N/2$, one finds $I(P(\ell)) \le 1$, strictly below the value 2 required for perfect recovery of a qubit secret. Thus $\ell = N/2$ lies inside the "grey region" of a ramp scheme. We now show that Haar scrambling realizes an approximate ramp secret-sharing scheme.

**Theorem 1.** *A unitary $U$ drawn from the Haar measure implements an approximate $\left(\left(\frac{N}{2}-\epsilon,\ \frac{N}{2}+\epsilon\right)\right)$ quantum ramp secret sharing scheme when the quantum secret is encoded into pure-state players.*

*Proof.* Set $\ell = \frac{N}{2} - \epsilon$ in Eq. (30). The linear term becomes

$$2\ell - N = -2\epsilon,$$

and the exponent in the logarithmic term becomes

$$N - 2\ell = 2\epsilon.$$

Thus,

$$I(P(\ell)) \;\le\; -2\epsilon \;+\; \log_2\!\left(1+2^{\,2\epsilon}\right). \tag{31}$$

Using $\log_2(1+x) \le x/\ln 2$,

$$I(P(\ell)) \;\le\; -2\epsilon \;+\; \frac{2^{2\epsilon}}{\ln 2}. \tag{32}$$

For any target accuracy $\gamma > 0$, choose $\epsilon = O(\gamma)$ so that RHS (32) is at most $\gamma$. Therefore,

$$I(R:P(b)) \;=\; I\!\left(P\!\left(\tfrac{N}{2}-\epsilon\right)\right) \;\le\; \gamma,$$

establishing the relaxed secrecy condition.

Since the global state on $RP(N)$ is pure, for all $\ell$ we have the identity

$$I(P(\ell)) + I(R:P(N-\ell)) = I(R:S) = 2. \tag{33}$$

Hence,

$$I(R:P(N-\ell)) \;\ge\; 2-\gamma,$$

which is the relaxed recoverability requirement for authorized sets. Thus the authorized and unauthorized regions are characterized by

$$b = \frac{N}{2} - \epsilon, \qquad g = \frac{N}{2} + \epsilon, \tag{34}$$

completing the proof. □

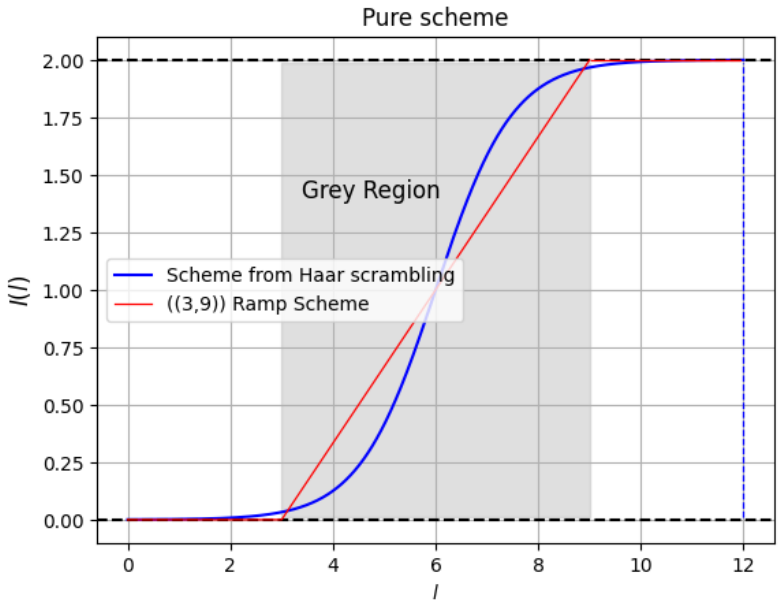



Figure 5: Mutual information between quantum secret and subsystem/parties of size $l$ for Haar scrambling and what we expect from the ramp scheme when the parties are in a pure state. Haar scrambling approximately behaves like a quantum ramp secret sharing scheme. In figure 5, we have plotted the mutual information between the reference qubit $R$ and $l$ arbitrary qubits in the system of size 12 after applying Haar scrambling. The curve for Haar scrambling approximates the $((3, 9))$ ramp scheme with a grey area when $l$ is between 3 and 9, which gives the gap $G = 6$ and rampiness $R = 0.5$.

The relaxed secrecy condition guarantees that any region $P(b)$ of size at most $b$ is nearly uncorrelated with the reference system. Using quantum Pinsker's inequality,

$$\frac{1}{2\ln 2}\big(\Delta(\rho_{RP(b)}, \rho_R \otimes \rho_{P(b)})\big)^2 \;\leq\; I(R:P(b)) \;\leq\; \gamma, \tag{35}$$

we obtain

$$\Delta(\rho_{RP(b)}, \rho_R \otimes \rho_{P(b)}) \;\leq\; O(\sqrt{\gamma}), \tag{36}$$

showing that unauthorized parties learn essentially nothing about the secret.

Finally, for the pure Haar-scrambled case, the scheme gap is

$$G = g - b = 2\epsilon,$$

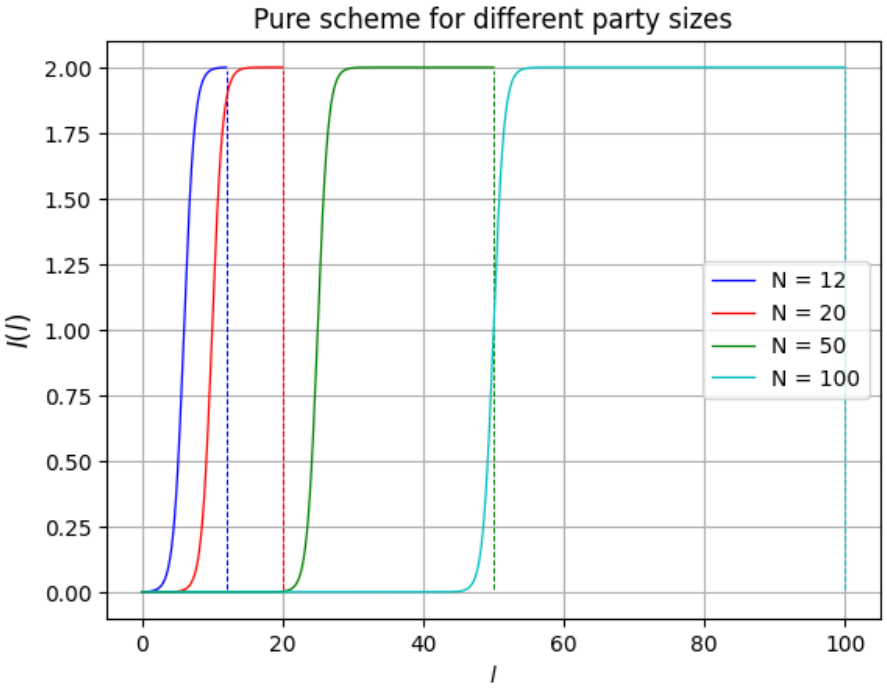
which is independent of $N$, and the rampiness is

$$R = \frac{G}{N} = \frac{2\epsilon}{N}.$$

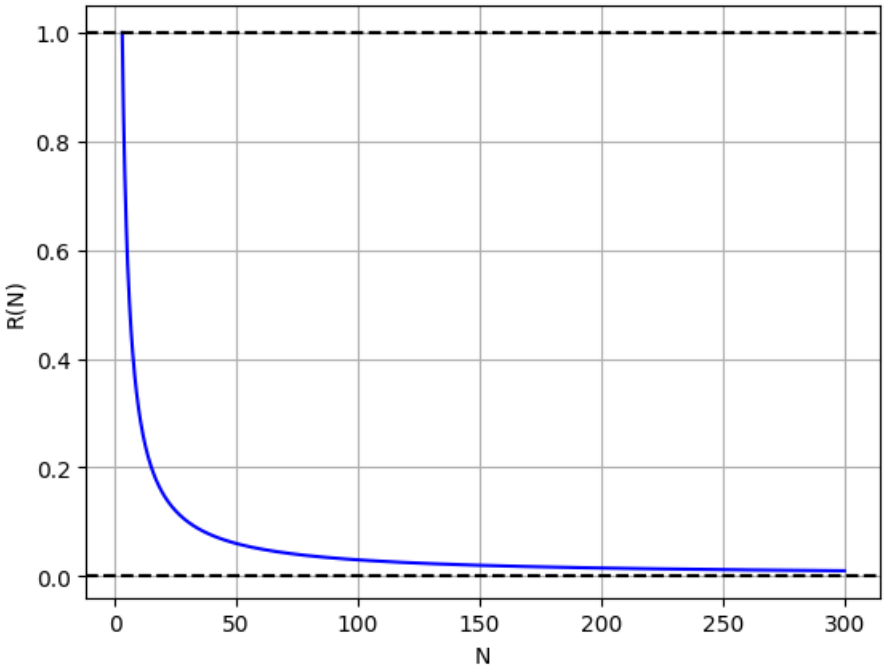
Thus the rampiness decays polynomially in $N$, and the scheme becomes increasingly sharp as the system size grows. In Figure 5, we have plotted the scheme when Haar scrambling a single qubit into a system of size 12, and in Figure 6a, into a system of other different sizes. One interesting observation is that while we increase the system size, the gap remains constant and is independent of the system size. This implies that the rampiness drops polynomially, as shown in figure 6b. Thus, the secret sharing protocol improves as the system size increases.

## 5.2 Ramp secret sharing from Haar scrambling: Mixed state case

We now generalize the pure-state analysis to the case where the players $\mathcal{P} = \{P_1, \ldots, P_m\}$ begin in a mixed state with nonzero entropy $s(\mathcal{P})$. Let $N = |\mathcal{P}|$ denote the number of players, and let $s(\mathcal{P})$ denote the von Neumann entropy of their joint state before scrambling. For pure states ($s(\mathcal{P}) = 0$),




(a) Pure schemes with different party sizes




(b) Rampiness with increasing party size $N$

Figure 6: a: Quantum ramp secret sharing schemes from Haar scrambling for different party sizes for the pure case. As the party sizes increase, the gap becomes small compared to the total size. b: Rampiness drops down as the system/players' size increases. This implies that secret sharing schemes become more effective for larger systems.

Theorem 1 shows that Haar scrambling implements an approximate ramp secret-sharing scheme with parameters

$$b_{\text{pure}} = \frac{N}{2} - \epsilon, \qquad g_{\text{pure}} = \frac{N}{2} + \epsilon.$$

In the mixed case, we will see that the ramp parameters are shifted by the initial entropy $s(\mathcal{P})$, yielding the more general expressions

$$\begin{aligned} g &= \frac{N + s(\mathcal{P})}{2} + \epsilon, \\ b &= \frac{N + s(\mathcal{P})}{2} - \epsilon, \end{aligned} \tag{37}$$

which reduce to the pure-state values when $s(\mathcal{P}) = 0$.

The central difficulty in the mixed-state setting is that the key identity used in the pure case,

$$I(P(\ell)) + I(R : P(N - \ell)) = I(R : S), \tag{38}$$

no longer holds. For mixed initial states, the corresponding relation becomes

$$I(R : P(\ell)) + I(R : P(N - \ell)) \;\leq\; I(R : S), \tag{39}$$

which is insufficient for guaranteeing the recoverability condition: even if $I(R : P(\ell))$ is made small, Eq. (39) does not imply that $I(R : P(N - \ell))$ is large. Thus, a direct analogue of the pure-state proof fails for mixed states, and we cannot establish recoverability using mutual-information bounds alone.[1]

Nevertheless, a complete characterization of mixed-state ramp schemes can be obtained using a structural fact:any mixed-state encoding can be realized as a pure-state encoding followed by discarding a subset of shares [15, 17]. Equivalently, any mixed state on $N$ players with entropy $s(\mathcal{P})$ can be purified by introducing $s(\mathcal{P})$ additional qubits that were subsequently traced out. This observation allows us to lift the pure-state theorem to the mixed setting.

**Theorem 2.** *A Haar-random scrambling unitary $U$ implements an approximate quantum ramp secret sharing scheme with parameters*

$$\left(b = \frac{N + s(\mathcal{P})}{2} - \epsilon, \quad g = \frac{N + s(\mathcal{P})}{2} + \epsilon\right),$$

*where $s(\mathcal{P})$ is the von Neumann entropy of the players' initial state.*

*Proof.* Consider a purification of the mixed initial state of the players $\mathcal{P}$. Let $N'$ denote the number of qubits in the purified system before any discarding occurs. Tracing out $s = s(\mathcal{P})$ qubits yields the mixed state on $N = N' - s$ players.

Applying Theorem 1 to the purified system: it yields a pure approximate ramp scheme with parameters

$$b_{\text{pure}} = \frac{N'}{2} - \epsilon, \qquad g_{\text{pure}} = \frac{N'}{2} + \epsilon.$$

Now discard $s$ of the $N'$ output shares. Discarding cannot increase the amount of information available to an unauthorized set, nor can it improve recoverability for an authorized set. Thus the ramp parameters $(b_{\text{pure}}, g_{\text{pure}})$ remain valid as long as $g_{\text{pure}} \leq N$, i.e. as long as every authorized set remains contained in the retained system.

Since $N' = N + s(\mathcal{P})$, we obtain

$$b = \frac{N + s(\mathcal{P})}{2} - \epsilon, \qquad g = \frac{N + s(\mathcal{P})}{2} + \epsilon,$$

establishing the claimed mixed-state parameters. □

As consistency checks:

[1] A detailed examination of the mixed-state Rényi mutual information appears in Appendix E.

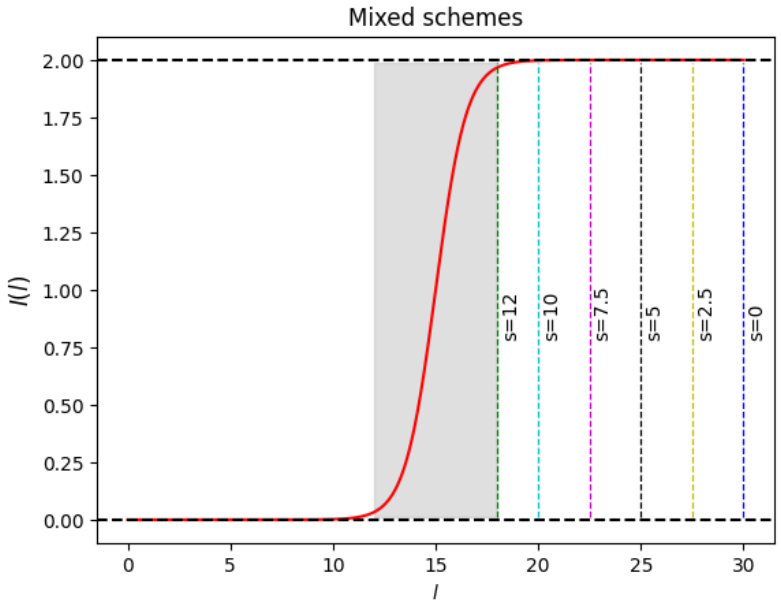



Figure 7: Mixed scheme can be thought of as a pure scheme with some players/systems discarded. $S = 0$ corresponds to the pure case where no players are discarded, while $s = 12$ corresponds to twelve players discarded. While the ramp parameters are the same, the total system size changes as the players are discarded. This formalism can also be thought of as a scheme where players have different entropies. By changing the entropy, one can then obtain all possible ramp schemes.

- If $s(\mathcal{P}) = 0$ (pure players), we recover the scheme of Theorem 1.
- If $s(\mathcal{P}) = N$ (maximally mixed players), then $g = b = N$, yielding a trivial scheme $((N, N))$ in which all $N$ players are required to reconstruct the secret.

The maximally mixed case can also be seen directly from the Rényi mutual information. Substituting $s(\mathcal{P}) = N$ into Eq. (18) gives

$$I^{(2)}(\ell) = \log_2\big(1 + 3 \cdot 4^{\,\ell - N}\big). \tag{40}$$

At $\ell = N$, we obtain $I^{(2)} = 2$, the maximum possible for a single-qubit secret, while for $\ell < N$ the mutual information decays exponentially in $N - \ell$. Thus only the full set of $N$ players can recover the secret.

Figure 7 illustrates how discarding different numbers of players (equivalently: increasing $s(\mathcal{P})$) transforms the pure scheme into different mixed-state ramp schemes. By varying $s(\mathcal{P})$ and the approximation parameter $\epsilon$, one can realize all possible ramp secret-sharing parameters.

## 5.3 Complexity Analysis

In this section, we will perform the complexity analysis of our protocol. So far, we have assumed the Haar random unitaries for implementing the information scrambling circuit. Unfortunately, a simple counting argument shows that it requires an exponential number of gates, $\mathcal{O}(4^n)$, to implement the $n$ qubit Haar unitary [42]. Furthermore, if we want to implement it with local 1 and 2 qubit gates, then it would take $\mathcal{O}(n^2 2^{2n})$ gates [43]. This gives the impression that implementing this protocol efficiently is almost impossible. Fortunately, this is not true. For a unitary to be scrambling, it doesn't have to be a perfect Haar unitary. In fact, very simple operators can actually be pretty good scramblers. Both Haar-random and unitary design states, for $t \geq 2$, exhibit near-maximal entanglement. This implies that the state one obtains from t-design circuits [44] is information theoretically indistinguishable from a Haar scrambling circuit up to t moments [45]. Since we used an information-theoretic argument to obtain ramp secret sharing schemes from Haar scrambling, for our purpose, t-design circuits are already enough. An example of a perfect

2-design circuit is provided by the ensemble of operators that form the Clifford group [46]. This is a particularly useful result for us because Clifford circuits can be obtained by using only $\mathcal{O}(n^2)$ one and two-qubit gates, which means our proposed protocol can be performed efficiently, i.e., with a polynomial number of gates.

There are several comments now in order. Gottesmann Knill's theorem [47] implies that to get any quantum advantage, one needs to use gates outside of the Clifford group, as a circuit involving only Clifford gates can be efficiently simulated by a classical computer. However, this is true only for computational tasks, and in several areas, such as quantum communication and quantum cryptography, protocols involving only Clifford group gates are very prominent. For example, quantum teleportation and superdense coding use only Clifford gates. For the NISQ Era, when errors are particularly prone, quantum cryptography protocols like the one we propose may be a promising quantum application, as Clifford gates are easier to correct errors compared to non-Clifford ones. The second comment is that while unitary design circuits are enough for our purpose, pseudorandom quantum states, on the other hand, are not. Quantum pseudorandom states are efficiently constructible states that nevertheless masquerade as Haar-random states to polynomial-time observers. Therefore, pseudorandom quantum states are not information-theoretically equivalent to Haar-random unitaries and are only equivalent from the perspective of observers with polynomial time complexity. In fact, it is possible to construct pseudoranodm states with only polylogarithmic entanglement entropy across an equipartition of the qubits [48]. Therefore, these pseudorandom unitaries lack sufficient scrambling features to implement the secret sharing protocol.

Now that we have discussed the complexity of information scrambling, let us discuss the complexity of the descrambling. Cryptography involves both encoding and decoding secrets, which in our framework refers to scrambling and descrambling quantum information. Fortunately, quantum mechanics is unitary, and if we have the knowledge about how the information was scrambled, in principle, we should be able to descramble it. It was shown that if $C$ is the complexity of the scrambling circuit, then one can construct the descrambling/decoding circuit of the complexity order $d_S C$, where $d_S$ is the Hilbert space dimension of the quantum secret [30]. For our protocol, where scrambling is implemented using only a polynomial number of Clifford gates, efficient descrambling is also possible, that is, using only a polynomial number of gates. While it is true that one needs to be provided with the encoding unitary to perform the decoding, one can sometimes do better. For example, one can perform the tomography to learn enough about the circuit and decode it. This is particularly true for the Clifford circuit, for which even without a scrambling unitary, we can perform tomography and learn enough to perform the decoding operation. In [41, 40], it was shown that this is possible even for certain families of non-Clifford circuits which are quasi-chaotic in nature. In particular, they showed that if the scrambling unitary $U_t$ is a $t$-doped Clifford circuit, it is possible to learn the scrambling circuit using only $\mathcal{O}(\text{poly}(n)\exp(t))$ queries. Interestingly, the decoder can still be a family of Clifford gates only. This fails if the scrambling circuit is fully chaotic, and then it is not possible to learn the circuit efficiently. Being able to perform the full tomography doesn't affect our protocol, as in quantum secret sharing schemes, it is possible to allow the parties to have full knowledge of how encoding as well as decoding is performed.

**Theorem 3.** *The protocol, both encoding and decoding, can be implemented efficiently, i.e., using only polynomial number, $\mathcal{O}(n^2)$, one and two qubit gates.*

# 6 Applications

In this section, we will briefly discuss potential applications of our work, spanning from establishing secure quantum networks to evaluating cryptographic tasks in the NISQ Era.

## 6.1 Information Scrambling protocol in Quantum Network and Security Implications

Classical communication networks serve as the foundation of our modern society. Alongside classical data, it is also possible to exchange quantum data over a long distance. These large-scale quantum networks [27, 49, 50, 51] offer novel capabilities, such as key distribution, clock synchronization, and increasing the baseline of telescopes, among others. One crucial question in the field of quantum networks is to find killer applications to justify actually building it. In this context,

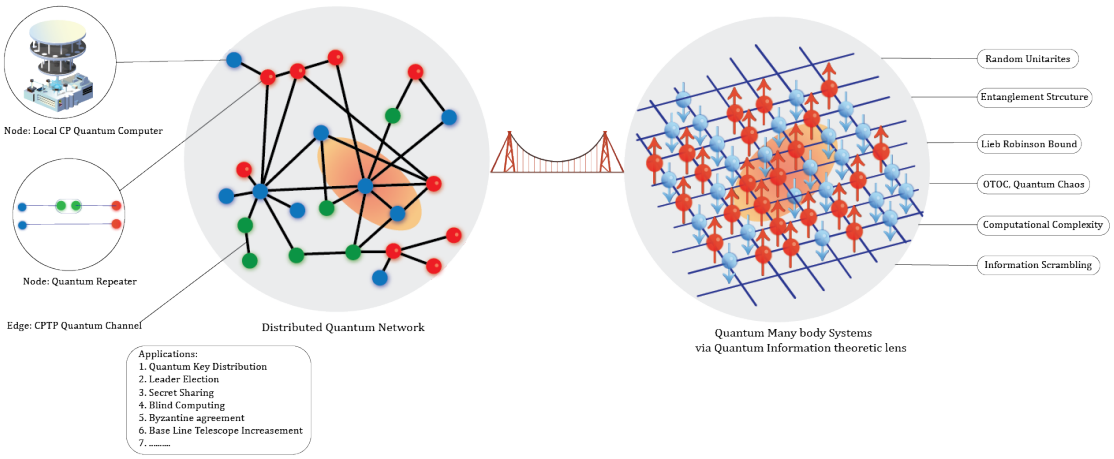



Figure 8: A bridge between distributed quantum networks and quantum many-body systems using the language of quantum information theory. There are several interesting results obtained in the field of quantum many-body systems using quantum information theory, such as Random unitaries, entanglement structure, quantum chaos, information scrambling, and phase transitions and so on. Thinking of quantum networks as a many-body system, similar techniques can be implemented to design new protocols. For example, Quantum chaos could be used to model hacking of the quantum network, phase transitions in entanglement structure can be used to study maximally entangled network clusters,

the utilization of information scrambling protocols opens up exciting possibilities for exploring the unique features of quantum networks, leading to novel security implications. We observed that by varying the purity of parties, one can construct all possible types of secret sharing schemes. Therefore, it is possible to construct a scrambling protocol such that the malicious party would need to get access to a significant fraction of the network to get any information out of the network. This theme can be further extended to establish a connection between two distinct fields: distributed quantum networks and quantum many-body systems, as depicted in Figure 8.

## 6.2 Benchmarking and cryptography protocols in NISQ Computers

In the NISQ Era [26], focus is often given to optimization and simulation problems, which, unfortunately, require many qubits. In contrast, cryptographic protocols require much fewer qubits, such as quantum key distribution, quantum teleportation, quantum money, and superdense coding. One can implement our protocol in the NISQ Era with low-depth circuits, which can be used for benchmarking and finding novel quantum cryptography applications.

## 6.3 Fundamental physics perspective

Quantum information scrambling is emerging as an essential tool in exploring quantum many-body dynamics, randomization and benchmarking, quantum computing protocols, the onset of quantum chaos, and even in black-hole physics [52, 53, 54, 55]. By establishing a connection between information scrambling and secret sharing, applying quantum secret-sharing tools can offer fresh insights into these areas. For example, employing the concept of dividing the quantum system into authorized and unauthorized parties allows us to tell exactly where the quantum information is located. When modeling an old black hole as a scrambling unitary [32, 6], one can deduce that after emitting $d$ Hawking radiation, where $d$ represents the size of the diary fallen into the black hole, the black hole essentially becomes an unauthorized set and can no longer retain any information

about the diary. All the information about the diary should be in Hawking radiation, as it is an authorized set.

## 7 Conclusion

We have demonstrated that Haar scrambling features possess quantum secret sharing properties. Rather than having the perfect threshold scheme, the secret sharing feature of Haar scrambling is closer to that of approximate ramp secret sharing schemes. By changing the purity of the initial state, one can then achieve all possible schemes. Furthermore, using complexity theoretic arguments, we have shown that the protocol can be implemented efficiently just by using a polynomial circuit. Besides this, our work has several potential applications, such as building secure quantum internet protocols, benchmarking and cryptography tasks, and lessons for fundamental physics. There are several interesting open questions one could explore. One could work out the applications in full detail and find other applications too. One could also extend this work to the noisy cases. While our model has inherent error correcting features, as one could still reconstruct the secret while losing qubits, provided they are authorized, it would be very hard to decode the secret out if we don't know the scrambling unitary, which would be the case for the noisy regime. Therefore, analyzing this model in the presence of noise is important. Another important question is of a more theoretical nature such as finding the relation between $l$- scrambling and OTOCs, building up theory of quantum ramp secret sharing, and exploring secret sharing features of other quantum systems

## 8 Acknowledgements

The research is part of the Munich Quantum Valley, which is supported by the Bavarian state government with funds from the Hightech Agenda Bayern Plus.

## A Toy model of Figure 2

In Figure 2, we start with a system of $N$ qubits that has a total Hilbert space of $2^N$. The time evolution of an initial state $|\psi\rangle$ can be described by a unitary operator $U(t)$ as follows:

$$|\psi(t)\rangle = U(t)\,|\psi\rangle \tag{41}$$

In order to have an information theoretic setting, we assume that Alice and Bob aim to communicate via the scrambling unitary $U$. Additionally, Alice controls the first qubit $q_A$, while Bob has access to a set of qubits $B$ (see Fig. 2). To describe a general scenario, we consider the initial state to be mixed:

$$\begin{aligned} \rho_0 &= |0\rangle\langle 0| \otimes \rho \\ \rho_1 &= |1\rangle\langle 1| \otimes \rho \end{aligned} \tag{42}$$

Here, $|0\rangle$ and $|1\rangle$ denote two possible orthogonal states of Alice's qubit $q_A$, and $\rho$ is the density matrix of the system excluding Alice's qubit. Alice's qubit is entangled with an external reference system $R$, and an external system called "Memory" purifies the density matrix $\rho$ (as depicted in Fig. 2). We represent this purified state as $\left|\sqrt{\rho}\right\rangle$, and by tracing out the memory system, we can retrieve the density matrix $\rho$:

$$\rho = \mathrm{Tr}_{\mathrm{MEM}}\,|\sqrt{\rho}\rangle\langle\sqrt{\rho}| \tag{43}$$

The initial state of the system, including the reference, system and the memory is:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_R\,|0\rangle_{q_A} + |1\rangle_R\,|1\rangle_{q_A})\,|\sqrt{\rho}\rangle \tag{44}$$

Since the time evolution unitary doesn't act on reference and memory, the time evolved state is given by:

$$|\psi(t)\rangle = \frac{1}{\sqrt{2}}(|0\rangle_R\,U_S \otimes I_{\mathrm{MEM}}\,|0,\sqrt{\rho}\rangle + |1\rangle_R\,U_S \otimes I_{\mathrm{MEM}}\,|1,\sqrt{\rho}\rangle) \tag{45}$$

## B Haar Integrals

An integral over the unitary group $U$ ($2^n \times 2^n$) of the matrix function $f(U)$ with respect to the Haar measure can be represented as:

$$I = \int dU f(U) \tag{46}$$

The defining property of the Haar measure is left- (respectively, right-) invariance with respect to shifts via multiplication. If $V$ is a fixed unitary, then:

$$\int dU f(UV) = \int d(U'V^\dagger) f(U') = \int dU' f(U') \tag{47}$$

In order to properly analyze the setting, we divide the input state as $AB$ and output state $CD$. Furthermore, the unitary $U$ is taken to be random $2^n \times 2^n$ matrix taken from Haar ensemble. The Haar average lets us consider expectations over a number of unitary matrices and is non-zero only when the number of $U$ equals the number of $U^\dagger$. For example with the case of two $U$s and two $U^\dagger$s, we get:

$$\begin{aligned} \int dU U_{i_1 j_1} U_{i_2 j_2} U^*_{i'_1 j'_1} U^*_{i'_2 j'_2} = \frac{1}{2^{2n}-1}(\delta_{i_1 i'_1}\delta_{i_2 i'_2}\delta_{j_1 j'_1}\delta_{j_2 j'_2} + \delta_{i_1 i'_2}\delta_{i_2 i'_1}\delta_{j_1 j'_2}\delta_{j_2 j'_1}) \\ - \frac{1}{2^n(2^{2n}-1)}(\delta_{i_1 i'_1}\delta_{i_2 i'_2}\delta_{j_1 j'_2}\delta_{j_2 j'_1} + \delta_{i_1 i'_2}\delta_{i_2 i'_1}\delta_{j_1 j'_1}\delta_{j_2 j'_2}) \end{aligned} \tag{48}$$

Let $d = d_A d_B = 2^a 2^b = d_C d_D = 2^c 2^d = 2^{a+b} = 2^{c+d} = 2^n$, then $d = 2^n$.

This formula will let us compute the average over the trace of the square of the density matrix $\rho_{AC}$:

$$\int dU \mathrm{Tr}(\rho^2_{AC}) = \frac{1}{2^{2n}} \int dU U_{klmo} U^*_{k'lm'o} U_{k'l'm'o'} U^*_{kl'mo'} \tag{49}$$

where, $k = 1, ..., 2^a$ are $A$ indices, $l = 1, ....., 2^b$ are $B$ indices, $m = 1, ....., 2^c$ are $C$ indices, and $o = 1, ....., 2^d$ are $D$ indices. Now, using equation 48,

$$\int dU \mathrm{Tr}(\rho_{AC}^2) = \frac{1}{d^2}\left(\frac{1}{d^2-1}(d_A d_B^2 d_C d_D^2 + d_A^2 d_B d_C^2 d_D) - \frac{1}{d(d^2-1)}(d_A d_B^2 d_C^2 d_D + d_A^2 d_B d_C d_D^2)\right) \tag{50}$$

We can approximate above equation as:

$$\int dU \mathrm{Tr}(\rho_{AC}^2) = d_A^{-1} d_C^{-1} + d_B^{-1} d_D^{-1} - d^{-1} d_A^{-1} d_D^{-1} - d^{-1} d_B^{-1} d_C^{-1} \tag{51}$$

From these quantities, it is possible to obtain the expression for Rényi enropies, which allow us to obtain bound for other information theoretic quantities.

# C Out of time ordered correlators (OTOCs)

To illustrate how correlators can be used to study information spreading, we consider a toy model of Alice and Bob communicating via a system of $N$ qubits. Alice controls the first qubit $q_A$, and Bob has access to a set of qubits $B$. Alice wants to send a bit $a \in 0, 1$ to Bob, which she does by flipping her qubit with the $\sigma_{q_A}^x$ operator depending on $a$. Bob then measures his qubits using $O_B$ after the system evolves for some time $t$.

Alice's qubit flip affects Bob's expectation value, with $\langle O_B \rangle_0$ and $\langle O_B \rangle_1$ denoting the respective values. By assuming that Alice and Bob repeat the measurements many times, the difference in expectation values can be bounded using the Cauchy-Schwarz inequality. This difference is bounded by the operator norm of the commutator $[\sigma_{q_A}^x(-t), O_B]$, where $\sigma^x(-t) = U\sigma^x U^\dagger$ is a Heisenberg operator. A simple and intuitive way to understand this phenomenon is as follows: at $t = 0$, the operator $\sigma^x$ only acts on Alice's qubit and has no overlap with Bob's qubit. Therefore, the commutator between $\sigma^x(-t)$ and Bob's observable $O_B$ is initially zero. As time progresses, the support of $\sigma^x(-t)$ grows as a Heisenberg operator, and the overlap with $O_B$ increases. This results in a non-zero commutator, indicating that Bob can now gain information about Alice's qubit. This spreading of information can be bounded rigorously using the Lieb-Robinson bound, which provides an upper bound on the rate at which information can travel through a quantum system.

Now we will define quantum chaos using out-of-time order correlators (OTOCs) [9, 10, 5], following the previous discussion of a toy model. OTOCs can be seen as the quantum version of the classical observation that the sensitivity to initial conditions can be quantified by a Poisson bracket: $q(t), p = \partial q(t)/\partial q(0)$, where $q$ and $p$ are a conjugate pair. In a classically chaotic system, this quantity would be proportional to $e^{\lambda t}$, where $\lambda$ is the Lyapunov exponent. The exponential growth of OTOCs is then defined as the thermal average of the square of the commutator $[\hat{q}(t), \hat{p}]$, obtained by quantizing $q(t), p$.

Generally, we consider a function involving the commutation of arbitrary operators (out-of-time ordered commutator) $C(t)$ given by:

$$\begin{aligned} C(t) &= \langle [V(0), W(t)]^\dagger [V(0), W(t)] \rangle \\ &= 2\mathrm{Re}\langle W^\dagger(t) W(t) V(0) V^\dagger(0) \rangle - 2\mathrm{Re}\langle W^\dagger(t) V^\dagger(0) W(t) V(0) \rangle \end{aligned} \tag{52}$$

Here, $O(0) = O$, $O(t) = U^\dagger O U$, and $\langle O \rangle = \mathrm{Tr} O\rho$ denotes an average of an operator $O$ over some set of states. Usually, the average is taken over a thermal state, $\rho \propto d^{-1} I$, where $d$ is the Hilbert space dimension. The first term in Eq. 52 is the time-ordered correlator and equilibrates at the thermalization time, while the second term is the out-of-time ordered correlator (OTOCs), which we refer to as $F(t)$, and characterizes the quantum chaotic effect:

$$F(t) = \langle W^\dagger(t) V^\dagger(0) W(t) V(0) \rangle. \tag{53}$$

OTOCs measure the overlap between two states, $F(t) = \langle \psi_B | \psi_A \rangle$, where the states are given by:

$$\begin{aligned} |\psi_A\rangle &= U^\dagger W U V |\psi\rangle = W(t) V |\psi\rangle , \\ |\psi_B\rangle &= V U^\dagger W U |\psi\rangle = V W(t) |\psi\rangle . \end{aligned} \tag{54}$$

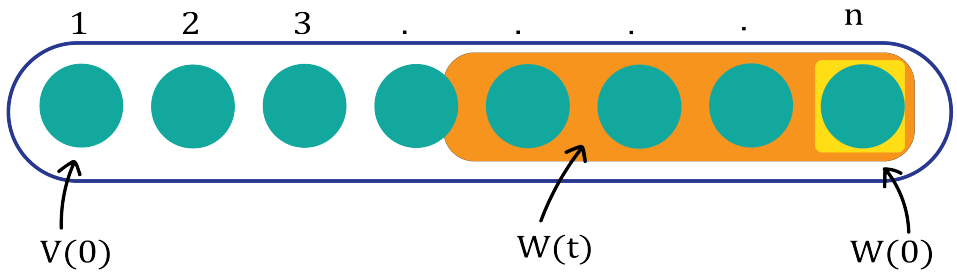



Figure 9: Evolution of local operator $W(0)$ under local Hamiltonian given by $W(t)$. As time increases, $W(t)$ is supported on larger region of the system. Commutation between $V(0)$ and $W(t)$ is non-zero only when region supported by $W(t)$ and $V(0)$ overlaps.

One can think of $F(t)$ as a four-point correlation function that probes the way in which (local) perturbations inhibit the cancellation between forward and backward evolution, and it diagnoses the spread of quantum information by measuring how quickly two commuting operators fail to commute. Since $W(0)$ and $V(0)$ are supported on non-overlapping subsystems, we have $[W(0), V(0)] = 0$ thus

$$F(t) = \langle W^\dagger(t)V^\dagger(0)W(t)V(0)\rangle = \langle W^\dagger(t)W(t)V^\dagger V(0)\rangle = 1. \tag{55}$$

Under a chaotic time evolution with Hamiltonian $H$, a local operator $W(0)$ will evolve into a complicated operator with an expansion as a sum of products of many local operators:

$$W(t) = e^{iHt}We^{-iHt} = W + it[H, W] - \frac{t^2}{2!}[H, [H, W]] - \frac{it^3}{3!}[H, [H, [H, W]]] + \ldots, \tag{56}$$

where the ellipsis denotes higher-order terms. Assuming a generic Hamiltonian $H$, the time-evolved operator $W(t)$, starting from a local operator $W(0)$, is supported on a larger region and hence does not commute with the initially non-overlapping operator $V(0)$, i.e., $[W(t), V(0)] \neq 0$. Consequently, the four-point correlation function $F(t)$, which measures the spread of quantum information, starts to decay and eventually goes to zero. This decay behavior is depicted in the cartoon representation shown in Figure 9. If this decay behavior occurs, we refer to the unitary as chaotic scrambling. Intuitively, this implies that over time, a chaotic scrambling unitary requires access to a larger region to access the initially localized information.

## D $((2, 3))$ quantum threshold scheme

Here a dealer share an arbitrary qutrit among three parties $V_{2,3} : \mathcal{C}^3 \to \mathcal{C}^3 \otimes \mathcal{C}^3 \otimes \mathcal{C}^3$ defined as:

$$\begin{aligned} V_{2,3}(\alpha\,|0\rangle + \beta\,|1\rangle + \gamma\,|2\rangle) = \frac{1}{\sqrt{3}}(&\alpha(|000\rangle + |111\rangle + |222\rangle) + \\ &\beta(|012\rangle + |120\rangle + |201\rangle) + \\ &\gamma(|021\rangle + |102\rangle + |210\rangle)) \end{aligned} \tag{57}$$

Indeed, $V_{2,3}$ is an isometry. Each resulting qutrit is taken as a share. From a single share, no information can be obtained about the secret as it is totally mixed and therefore it is independent about the secret.

$$\rho_1 = \frac{1}{3}(|0\rangle\langle 0| + |1\rangle\langle 1| + |2\rangle\langle 2|) \tag{58}$$

However, the secret can be perfectly reconstructed from any two of the three shares. For example, if we have two first shares, then the secret can be reconstucted as:

$$(\alpha\,|0\rangle + \beta\,|1\rangle + \gamma\,|2\rangle)(|00\rangle + |12\rangle + |21\rangle) \tag{59}$$

So, the first qutrit now contains the secret. Here, the reconstruction procedure can be done by adding the value of the first share to the second (modulo three), and then adding the value of the second share to the first. For the other cases, we can follow the similar procedure because of it's symmetric nature.

# E Information theoretic analysis for the mixed states

Let $P(\ell)$ be an arbitrary region of size $\ell$ in the system after the Haar scrambling unitary is applied, and let $I(P(\ell))$ denote the mutual information between the original secret (one qubit) and this region. Using the Rényi-based upper bound on the quantum mutual information derived in Eq. (18), we obtain an inequality of the form

$$I(P(\ell)) \;\le\; F\big(N, s(\mathcal{P}), \ell\big), \tag{60}$$

where $F$ is an explicit function depending on the total number of players $N$, the initial entropy $s(\mathcal{P})$ of the players, and the subsystem size $\ell$. Concretely, Eq. (18) yields

$$I(P(\ell)) \;\le\; 1 + \log_2\left(2 - \frac{3\big(1 - 2^{2\ell-2N}\big)}{2 + \big(2^{-s(\mathcal{P})} - 2^{-N}\big)\,4^{\ell-N/2}}\right), \tag{61}$$

which reduces to the pure-state expression when $s(\mathcal{P}) = 0$.

To connect this to ramp secret sharing, it is natural to consider the values of $\ell$ near the "transition" scale

$$\ell_\star = \frac{N + s(\mathcal{P})}{2},$$

as the center of the ramp region for mixed-state schemes. In particular, for

$$\ell = \frac{N + s(\mathcal{P})}{2} - \epsilon, \tag{62}$$

and fixed $N$ and $s(\mathcal{P})$, the function $F\big(N, s(\mathcal{P}), \ell\big)$ can be made arbitrarily small by choosing $\epsilon$ appropriately. That is, for any target accuracy $\gamma > 0$, there exists $\epsilon = \epsilon(\gamma)$ such that

$$I\Big(P\Big(\tfrac{N+s(\mathcal{P})}{2} - \epsilon\Big)\Big) \;\le\; \gamma. \tag{63}$$

This establishes a relaxed secrecy condition for subsets of size $\ell = \frac{N+s(\mathcal{P})}{2} - \epsilon$: they have vanishingly small correlation with the reference as $\gamma \to 0$.

However, in the mixed-state scenario, the complementary mutual information no longer satisfies the pure-state equality (38). Instead, one has only the inequality

$$I(R : P(\ell)) + I\big(R : P(N - \ell)\big) \;\le\; I(R : S), \tag{64}$$

which follows from strong subadditivity and the fact that the global state is no longer pure on $RP(N)$ alone. For

$$\ell = \frac{N + s(\mathcal{P})}{2} - \epsilon,$$

the relaxed secrecy bound (63) gives

$$I\big(R : P(\ell)\big) \le \gamma, \tag{65}$$

and the inequality (64) then implies only

$$I\big(R : P(N - \ell)\big) \;\le\; I(R : S) - I(R : P(\ell)) \;\le\; I(R : S), \tag{66}$$

which is a trivial upper bound and provides no nontrivial lower bound on $I\big(R : P(N-\ell)\big)$. In other words, from the direct Rényi-based analysis we obtain

$$I\big(R : \text{unauthorized region}\big) \approx 0, \tag{67}$$

but we cannot conclude that

$$I\big(R : \text{complementary region}\big) \approx 2 \tag{68}$$

purely from Eq. (64).

Thus, this information-theoretic approach suffices to verify a secrecy condition for the mixed-state case, namely, that suitably small subsets have negligible mutual information with the secret, but it fails to establish the recoverability condition: we cannot show that large subsets necessarily contain almost all the information about the secret. Consequently, the direct analysis based solely on Eq. (60) and the inequality (64) does not yield a complete mixed-state quantum ramp secret-sharing scheme.

This motivates the more structural approach adopted in Section 2, where mixed-state schemes are obtained from pure ones via purification and discarding of shares. That approach provides both secrecy and recoverability and leads to the ramp parameters

$$b = \frac{N + s(\mathcal{P})}{2} - \epsilon, \qquad g = \frac{N + s(\mathcal{P})}{2} + \epsilon.$$

## References


[1] Shenglong Xu and Brian Swingle. "Scrambling Dynamics and Out-of-Time Ordered Correlators in Quantum Many-Body Systems: a Tutorial" (2022). arXiv:2202.07060.

[2] Pavan Hosur, Xiao-Liang Qi, Daniel A. Roberts, and Beni Yoshida. "Chaos in quantum channels". Journal of High Energy Physics**2016** (2016).

[3] K. A. Landsman, C. Figgatt, T. Schuster, N. M. Linke, B. Yoshida, N. Y. Yao, and C. Monroe. "Verified Quantum Information Scrambling". Nature **567**, 61–65 (2019). arXiv:1806.02807.

[4] Thomas Schuster, Bryce Kobrin, Ping Gao, Iris Cong, Emil T. Khabiboulline, Norbert M. Linke, Mikhail D. Lukin, Christopher Monroe, Beni Yoshida, and Norman Y. Yao. "Many-Body Quantum Teleportation via Operator Spreading in the Traversable Wormhole Protocol". Phys. Rev. X **12**, 031013 (2022). arXiv:2102.00010.

[5] Yasuhiro Sekino and L Susskind. "Fast scramblers". Journal of High Energy Physics **2008**, 065–065 (2008).

[6] Patrick Hayden and John Preskill. "Black holes as mirrors: quantum information in random subsystems". Journal of High Energy Physics **2007**, 120–120 (2007).

[7] Xiao Mi, Pedram Roushan, Chris Quintana, Salvatore Mandrà, Jeffrey Marshall, Charles Neill, Frank Arute, Kunal Arya, Juan Atalaya, Ryan Babbush, Joseph C. Bardin, Rami Barends, Joao Basso, Andreas Bengtsson, Sergio Boixo, Alexandre Bourassa, Michael Broughton, Bob B. Buckley, David A. Buell, Brian Burkett, Nicholas Bushnell, Zijun Chen, Benjamin Chiaro, Roberto Collins, William Courtney, Sean Demura, Alan R. Derk, Andrew Dunsworth, Daniel Eppens, Catherine Erickson, Edward Farhi, Austin G. Fowler, Brooks Foxen, Craig Gidney, Marissa Giustina, Jonathan A. Gross, Matthew P. Harrigan, Sean D. Harrington, Jeremy Hilton, Alan Ho, Sabrina Hong, Trent Huang, William J. Huggins, L. B. Ioffe, Sergei V. Isakov, Evan Jeffrey, Zhang Jiang, Cody Jones, Dvir Kafri, Julian Kelly, Seon Kim, Alexei Kitaev, Paul V. Klimov, Alexander N. Korotkov, Fedor Kostritsa, David Landhuis, Pavel Laptev, Erik Lucero, Orion Martin, Jarrod R. McClean, Trevor McCourt, Matt McEwen, Anthony Megrant, Kevin C. Miao, Masoud Mohseni, Shirin Montazeri, Wojciech Mruczkiewicz, Josh Mutus, Ofer Naaman, Matthew Neeley, Michael Newman, Murphy Yuezhen Niu, Thomas E. O'Brien, Alex Opremcak, Eric Ostby, Balint Pato, Andre Petukhov, Nicholas Redd, Nicholas C. Rubin, Daniel Sank, Kevin J. Satzinger, Vladimir Shvarts, Doug Strain, Marco Szalay, Matthew D. Trevithick, Benjamin Villalonga, Theodore White, Z. Jamie Yao, Ping Yeh, Adam Zalcman, Hartmut Neven, Igor Aleiner, Kostyantyn Kechedzhi, Vadim Smelyanskiy, and Yu Chen. "Information scrambling in quantum circuits". Science **374**, 1479–1483 (2021).

[8] M. S. Blok, V. V. Ramasesh, T. Schuster, K. O'Brien, J. M. Kreikebaum, D. Dahlen, A. Morvan, B. Yoshida, N. Y. Yao, and I. Siddiqi. "Quantum information scrambling on a superconducting qutrit processor". Physical Review X**11** (2021).
[9] A. I. Larkin and Yu. N. Ovchinnikov. "Quasiclassical Method in the Theory of Superconductivity". Soviet Journal of Experimental and Theoretical Physics **28**, 1200 (1969).
[10] Juan Maldacena, Stephen H. Shenker, and Douglas Stanford. "A bound on chaos". Journal of High Energy Physics**2016** (2016).
[11] Koji Hashimoto, Keiju Murata, and Ryosuke Yoshii. "Out-of-time-order correlators in quantum mechanics". Journal of High Energy Physics**2017** (2017).
[12] Hideki Imai, Jörn Müller-Quade, Anderson C. A. Nascimento, Pim Tuyls, and Andreas Winter. "An information theoretical model for quantum secret sharing". Quantum Info. Comput. **5**, 69–80 (2005).
[13] Adi Shamir. "How to share a secret". Commun. ACM **22**, 612–613 (1979).
[14] G. R. Blakley. "Safeguarding cryptographic keys". In 1979 International Workshop on Managing Requirements Knowledge (MARK). Pages 313–318. (1979).
[15] Richard Cleve, Daniel Gottesman, and Hoi-Kwong Lo. "How to share a quantum secret". Physical Review Letters **83**, 648–651 (1999).
[16] Mark Hillery, Vladimí r Bužek, and André Berthiaume. "Quantum secret sharing". Physical Review A **59**, 1829–1834 (1999).
[17] Daniel Gottesman. "Theory of quantum secret sharing". Physical Review A**61** (2000).
[18] G R Blakley and Catherine Meadows. "Security of ramp schemes". In Proceedings of CRYPTO 84 on Advances in Cryptology. Page 242–268. Berlin, Heidelberg (1985). Springer-Verlag.
[19] Matthew Franklin and Moti Yung. "Communication complexity of secure computation (extended abstract)". In Association for Computing Machinery. Page 699–710. STOC '92New York, NY, USA (1992).
[20] Paul Zhang and Ryutaroh Matsumoto. "Quantum strongly secure ramp secret sharing". Quantum Information Processing **14**, 715–729 (2014).
[21] Ryutaroh Matsumoto. "Coding theoretic construction of quantum ramp secret sharing". IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences **E101.A**, 1215–1222 (2018).
[22] Winton Brown and Omar Fawzi. "Decoupling with random quantum circuits". Communications in Mathematical Physics **340**, 867–900 (2015).
[23] Anne Marin and Damian Markham. "Equivalence between sharing quantum and classical secrets and error correction". Physical Review A**88** (2013).
[24] Markus Grassl, Felix Huber, and Andreas Winter. "Entropic proofs of singleton bounds for quantum error-correcting codes". IEEE Transactions on Information Theory **68**, 3942–3950 (2022).
[25] Min-Hsiu Hsieh, Igor Devetak, and Todd Brun. "General entanglement-assisted quantum error-correcting codes". Phys. Rev. A **76**, 062313 (2007).
[26] John Preskill. "Quantum computing in the NISQ era and beyond". Quantum **2**, 79 (2018).
[27] Riccardo Bassoli, Holger Boche, Christian Deppe, Roberto Ferrara, Frank H. P. Fitzek, Gisbert Janssen, and Sajad Saeedinaeeni. "Quantum communication networks". Springer Cham. (2021).
[28] Mark M. Wilde. "Quantum information theory". Cambridge University Press. (2013).
[29] Benjamin Schumacher and M. A. Nielsen. "Quantum data processing and error correction". Phys. Rev. A **54**, 2629–2635 (1996).
[30] Beni Yoshida and Alexei Kitaev. "Efficient decoding for the hayden-preskill protocol" (2017). arXiv:1710.03363.
[31] Antonio Anna Mele. "Introduction to haar measure tools in quantum information: A beginner's tutorial" (2023). arXiv:2307.08956.
[32] Don N. Page. "Information in black hole radiation". Physical Review Letters **71**, 3743–3746 (1993).
[33] Noah Linden, Milá n Mosonyi, and Andreas Winter. "The structure of rényi entropic inequalities". Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences **469**, 20120737 (2013).

[34] Patrick Hayden, Debbie W. Leung, and Andreas Winter. "Aspects of generic entanglement". Communications in Mathematical Physics **265**, 95–117 (2006).
[35] Daniel A. Roberts and Beni Yoshida. "Chaos and complexity by design". JHEP **04**, 121 (2017). arXiv:1610.04903.
[36] J. Ignacio Cirac, David Pé rez-García, Norbert Schuch, and Frank Verstraete. "Matrix product states and projected entangled pair states: Concepts, symmetries, theorems". Reviews of Modern Physics**93** (2021).
[37] Tianrui Xu, Thomas Scaffidi, and Xiangyu Cao. "Does scrambling equal chaos?". Physical Review Letters**124** (2020).
[38] Alexei Kitaev and John Preskill. "Topological entanglement entropy". Physical Review Letters**96** (2006).
[39] Aram W. Harrow, Linghang Kong, Zi-Wen Liu, Saeed Mehraban, and Peter W. Shor. "Separation of out-of-time-ordered correlation and entanglement". PRX Quantum**2** (2021).
[40] Lorenzo Leone, Salvatore F. E. Oliviero, Seth Lloyd, and Alioscia Hamma. "Learning efficient decoders for quasi-chaotic quantum scramblers" (2023). arXiv:2212.11338.
[41] Salvatore F. E. Oliviero, Lorenzo Leone, Seth Lloyd, and Alioscia Hamma. "Black hole complexity, unscrambling, and stabilizer thermal machines" (2022). arXiv:2212.11337.
[42] E. Knill. "Approximation by quantum circuits" (1995). arXiv:quant-ph/9508006.
[43] Joseph Emerson, Yaakov S. Weinstein, Marcos Saraceno, Seth Lloyd, and David G. Cory. "Pseudo-random unitary operators for quantum information processing". Science **302**, 2098–2100 (2003).
[44] D. Gross, K. Audenaert, and J. Eisert. "Evenly distributed unitaries: On the structure of unitary designs". Journal of Mathematical Physics**48** (2007).
[45] Andris Ambainis and Joseph Emerson. "Quantum t-designs: t-wise independence in the quantum world" (2007). arXiv:quant-ph/0701126.
[46] Christoph Dankert, Richard Cleve, Joseph Emerson, and Etera Livine. "Exact and approximate unitary 2-designs and their application to fidelity estimation". Physical Review A**80** (2009).
[47] Daniel Gottesman. "The heisenberg representation of quantum computers" (1998). arXiv:quant-ph/9807006.
[48] Scott Aaronson, Adam Bouland, Bill Fefferman, Soumik Ghosh, Umesh Vazirani, Chenyi Zhang, and Zixin Zhou. "Quantum pseudoentanglement" (2023). arXiv:2211.00747.
[49] Stephanie Wehner, David Elkouss, and Ronald Hanson. "Quantum internet: A vision for the road ahead". Science **362**, eaam9288 (2018).
[50] Amoldeep Singh, Kapal Dev, Harun Siljak, Hem Dutt Joshi, and Maurizio Magarini. "Quantum internet- applications, functionalities, enabling technologies, challenges, and research directions" (2021). arXiv:2101.04427.
[51] Kiran Adhikari and Christian Deppe. "Quantum information spreading and scrambling in a distributed quantum network: A hasse/lamport diagrammatic approach" (2023). arXiv:2309.10363.
[52] Kiran Adhikari and Sayantan Choudhury. "Cosmological krylov complexity". Fortschritte der Physik**70** (2022).
[53] Kiran Adhikari, Sayantan Choudhury, and Abhishek Roy. "Krylov complexity in quantum field theory". Nuclear Physics B **993**, 116263 (2023).
[54] Kiran Adhikari, Adwait Rijal, Ashok Kumar Aryal, Mausam Ghimire, Rajeev Singh, and Christian Deppe. "Krylov complexity of fermionic and bosonic gaussian states". Fortschritte der Physik**72** (2024).
[55] Kiran Adhikari Chhetriya. "Quantum State-Aware Query Complexity: Krylov Compression and Polynomial Query Duality" (2025). arXiv:2510.11786.