



Optimal Untelegraphable Encryption and Implications for Uncloneable Encryption

Anne Broadbent¹ , Eric Culf² and Denis Rochette¹

¹ University of Ottawa, Department of Mathematics and Statistics, Canada

² Institute for Quantum Computing and University of Waterloo, Canada

Abstract. We investigate the notion of untelegraphable encryption (UTE), a quantum encryption primitive that is a special case of uncloneable encryption (UE), where the adversary’s capabilities are restricted to producing purely classical information rather than arbitrary quantum states. We present an unconditionally secure construction of UTE that achieves untelegraphable-indistinguishability security, together with natural multi-ciphertext and bounded collusion-resistant extensions, without requiring any additional assumptions. We also extend this to the unbounded case, assuming pseudo-random unitaries, yielding everlasting security. Furthermore, we derive results on UE using approaches from UTE in the following ways: first, we provide new lower bounds on UTE, which give new lower bounds on UE; second, we prove an asymptotic equivalence between UTE and UE in the regime where the number of adversaries in UE grows. These results suggest that UTE may provide a new path toward achieving a central open problem in the area: indistinguishability security for UE in the plain model.

1 Introduction

Uncloneable encryption (UE), originally introduced by Broadbent and Lord [BL20], and named after the no-cloning principle [WZ82, Die82], is an encryption scheme that provides a level of security unachievable classically: no pirating adversary $\mathcal{A}$, receiving a ciphertext encoding a message m as a quantum state, can apply a quantum operation that produces a bipartite state over registers B and C such that two local receiving adversaries, $\mathcal{B}$ and $\mathcal{C}$, each accessing one of these registers, can both recover information about m , even when given the classical secret key. When m is sampled uniformly from the message space and both $\mathcal{B}$ and $\mathcal{C}$ are required to recover the entire message, this is referred to as *one-way*, or *search* security. A more robust notion, called *indistinguishability*, or *decision* security, allows $\mathcal{A}$ to fix two messages, receive an encryption of one of them at random, and then have $\mathcal{B}$ and $\mathcal{C}$ attempt to guess which one. Search security has been achieved in an information-theoretic sense in [BL20], but indistinguishability security remains an open problem. Existing positive results rely on additional assumptions such as oracles [BL20, AKL⁺22], relaxed definitions [KN23, AKY25, CG24c, BC26], or new conjectures [AB24, BBC⁺26].

Since its introduction, uncloneable encryption has become a fundamental building block of quantum cryptography, supporting applications such as secure software leasing [KNY21, BJL⁺21, ALP21], uncloneable zero-knowledge proofs [JK24], quantum copy-protection [AK21, ALL⁺21, CLLZ21, CMP24], private-key quantum money [BL20], uncloneable

E-mail: anne.broadbent@uottawa.ca (Anne Broadbent), eculf@uwaterloo.ca (Eric Culf), denis.inria@inria.fr (Denis Rochette)



decryption [GZ20, CLLZ21, SW22, KT25], quantum functional encryption [MM24]. It has moreover inspired the study of numerous other uncloneable cryptographic primitives¹.

Untelegraphable encryption (UTE), introduced in [CKNY26] (and also, independently in [CG24a] under the name unbounded leakage-resilience), is a natural relaxation of UE, inspired by the *no-telegraphing principle*, which asserts that, without pre-shared entanglement, quantum information cannot be transmitted through classical channel alone [Wer98]². The security guarantee for UTE is as follows: any telegraphing adversary $\mathcal{A}$ who receives a quantum ciphertext of a message cannot generate *classical* information that would enable another adversary, the receiver $\mathcal{B}$, to recover information about the message even when given the classical secret key. The notions of search and indistinguishability security in UTE are analogous to those defined for UE. We note that early work [BL20] has already established indistinguishable-UE in the oracle model for unentangled adversaries, thus implying indistinguishable-UTE in the oracle model. [CKNY26] improves this to an unconditional construction. They further introduce the notion of collusion-resistant UTE, in which security is preserved even when the adversary $\mathcal{A}$ adaptively selects multiple pairs of messages across successive rounds. Constructions of such schemes are obtained from pseudorandom functions, or from pseudorandom states when the number of rounds is bounded. Finally, they present an everlasting collusion-resistant UTE scheme in the quantum random oracle model.

A central reason for studying UTE lies in its conceptual connection to the two foundational no-go theorems already mentioned: the no-cloning theorem and the no-telegraphing theorem. These two no-go theorems are in fact informationally equivalent [NZ24]: to construct a copy using a telegrapher, one may simply copy the intermediate classical output produced by the telegrapher’s channel and subsequently apply the reconstruction procedure to each of these classical copies. Conversely, to achieve telegraphing from a cloner, if one can generate a sufficiently large number of copies to enable a full classical characterization of the quantum state (*e.g.*, via quantum state tomography), then this classical description can be transmitted through the telegrapher’s channel to reconstruct the original state. Naturally, this latter direction incurs a significantly higher computational cost. The computational separation between the no-cloning and no-telegraphing principles has been explored in detail in [NZ24]. The informational equivalence between the no-cloning and no-telegraphing theorems motivates our investigation of UE via UTE.

1.1 Results

Our work investigates the existence of a UTE scheme that achieves private-key untelegraphable-indistinguishability security unconditionally, as well as its implications for UE. In particular, we analyze different notions of *indistinguishability* security for *quantum encryption of classical messages* (QECM) schemes, *i.e.* protocols that encrypt classical messages using quantum ciphertexts and classical keys. These notions can be formalized through multiplayer games involving pirating and receiving parties; we say that a scheme achieves indistinguishable security if the *winning advantage* of the following security game is negligible in the security parameter:

1. The adversaries decide on the strategy and a pair of messages to distinguish (m_0, m_1) .
2. The referee samples a uniformly random bit b and sends the encryption of m_b to the pirate adversary $\mathcal{A}$.
3. $\mathcal{A}$ applies a quantum channel map to the ciphertext states, getting a state in the receiving adversaries’ registers. She sends these registers to the corresponding adversaries.

¹see, for instance: [CG24b, LLQZ22, PRV26]

²The no-telegraphing principle is also referred to as the no-classical-teleportation theorem.

4. The receiving adversaries are given the encryption key by the referee and attempt to guess the bit b , without communicating.
5. The adversaries win if all receivers are able to guess b correctly.

The difference between *uncloneable-indistinguishable* security (for UE) and *untelegraphable-indistinguishable* security (for UTE) lies in the nature of the quantum channel: in UE it may be arbitrary, while in UTE it must be quantum-to-classical (in which case the output can be freely copied). Also, for UTE, the security game is played with one receiver rather than two or more as for UE, but since classical information can be perfectly cloned, the optimal winning probability is the same for any number of receivers. When $\mathcal{A}$ receives t copies of the ciphertext, we obtain the notions of *t-copy uncloneable-indistinguishable* security and *t-copy untelegraphable-indistinguishable* security, respectively.

The relationship between our study of UTE and UE manifests in three complementary ways. First, we show that the scheme we analyze for UTE also satisfies a minimality property when evaluated under the UE framework. Second, by leveraging a lower bound established for UTE, we derive a new lower bound for UE. Finally, we establish a form of asymptotic equivalence between the two security regimes.

We prove that the Haar-measure scheme (Definition 1) (see [MST21]), satisfies several forms of untelegraphable security.

Definition 1 (Haar-measure encryption). For a $\log n$ -bit message $m \in [n]$ and a Haar-random unitary $U \in \mathcal{U}(d)$ as the key, encryption is given by

$$\text{Enc}(m, U) := U \left(\underbrace{|m\rangle\langle m|}_{n \times n \text{ matrix}} \otimes \underbrace{I_{d/n}}_{\text{identity}} \right) U^*,$$

and decryption is performed by first applying U^* to cancel the conjugation, and then measuring the first register.

Results 1 to 3 below are unconditional, information-theoretic statements about Haar-measure encryption, and thus do not rely on pseudorandom unitaries or any other computational assumptions (see the full Theorem statements for details). Note that we also study efficient versions of this encryption arising from unitary designs (see Remark 1). This yields efficient schemes which satisfy the security bounds of Results 1 to 3.

Result 1 (Theorem 1). *The Haar-measure encryption scheme for classical bits ($n = 2$ messages) achieves one-copy untelegraphable-indistinguishable security with winning probability upper bounded by*

$$\frac{1}{2} + \frac{1}{2\sqrt{d+1}}.$$

Result 2 (Theorem 2). *The Haar-measure encryption scheme for n messages achieves t -copy untelegraphable-indistinguishable security with winning probability upper bounded by*

$$\frac{1}{2} + \frac{7t\sqrt{n}}{\sqrt{d}}.$$

We also consider the notion of collusion-resistant security, introduced by [CKNY26], in which $\mathcal{A}$ may adaptively select multiple message pairs across Q successive rounds, and its everlasting variant where adversaries are computationally bounded.

Result 3 (Theorem 3). *The Haar-measure encryption scheme for n messages achieves Q -round collusion-resistant untelegraphable-indistinguishable security with winning probability upper bounded by*

$$\frac{1}{2} + \frac{7Q\sqrt{n}}{\sqrt{d}}.$$

Next, **Result 4** below contains two different security regimes. Its bounded-round construction is unconditional and is instantiated using unitary designs. Its unbounded-round construction provides everlasting security and is the only one of our main results that assumes the existence of pseudorandom unitaries.

Result 4 (Corollary 1). *The Haar-measure encryption scheme achieves unconditional collusion-resistant untelegraphable-indistinguishable security for a polynomially-bounded number of rounds; and everlasting security for an unbounded number of rounds, under the assumption of pseudorandom unitaries.*

This improves upon the result of [CKNY26], where collusion-resistant security relied on pseudorandom functions (an assumption stronger than pseudorandom unitaries), bounded-round security relied on pseudorandom states, and everlasting security relied on the QROM. Our plain-model achievability of everlasting security in the private key model contrasts with the result of [CKNY26] showing impossibility in the public-key model.

Then, in analogy with the informational equivalence of no-cloning and no-telegraphing principles in specific asymptotic regimes, we show that UTE can be expressed as a limit of UE as the number of receiving adversaries increases.

Result 5 (Theorem 4). *For any UE scheme, the winning probability of the uncloneability-indistinguishability game with s receiving adversaries converges to that of the untelegraphability-indistinguishability game at rate*

$$\mathcal{O}\left(\frac{1}{\sqrt[3]{s}}\right).$$

More precisely, for any fixed scheme, the additive gap between the optimal winning probabilities in the two games tends to zero as the number s of receiving adversaries tends to infinity.

Additionally we derive several lower bounds for the securities of the Haar-measure scheme. Since the winning probability for UE indistinguishability is always at least that for UTE, any lower bound for UTE also applies to UE (see Figure 1).

Result 6. [Corollary 2] *The Haar-measure encryption scheme for classical bits ($n = 2$ messages) achieves one-copy untelegraphable-indistinguishable security with winning probability lower bounded by*

$$\frac{1}{2} + \frac{1}{\sqrt{2\pi d}} + \mathcal{O}\left(\frac{1}{d^{3/2}}\right).$$

Result 7 (Corollary 4). *The Haar-measure encryption scheme for n messages achieves t -copy untelegraphable-indistinguishable security with winning probability lower bounded by*

$$\frac{1}{2} + \frac{\sqrt{tn}}{6\sqrt{\pi d}} + \mathcal{O}\left(\frac{\sqrt{t}\sqrt[3]{n}}{\sqrt[3]{d}}\right).$$

In particular our result on the one-copy untelegraphable-indistinguishable security for classical bits, of the Haar-measure scheme, is tight (to order).

Finally, we prove a minimality property of the Haar-measure scheme extending the result of [MST21].

Result 8 (Theorem 5). *For any UE or UTE scheme with n messages in dimension d , the winning probability of the uncloneability-indistinguishability game or the untelegraphability-indistinguishability game is lower-bounded by the corresponding winning probability of the n -message Haar-measure encryption scheme in dimension $(d - n + 1)n$.*

Result 9 (Corollary 5). *Writing w for the winning probability of the t -to- $(t + 1)$ copy uncloneability-indistinguishability game for the n -message Haar-measure scheme in dimension $(d - n + 1)n$, the winning probability of the t -to- $(t + 1)$ copy uncloneability-indistinguishability game for any n -message UE scheme in dimension d is lower-bounded by*

$$\frac{1}{2} + \Omega\left(\frac{w - \frac{1}{2}}{t^2}\right).$$

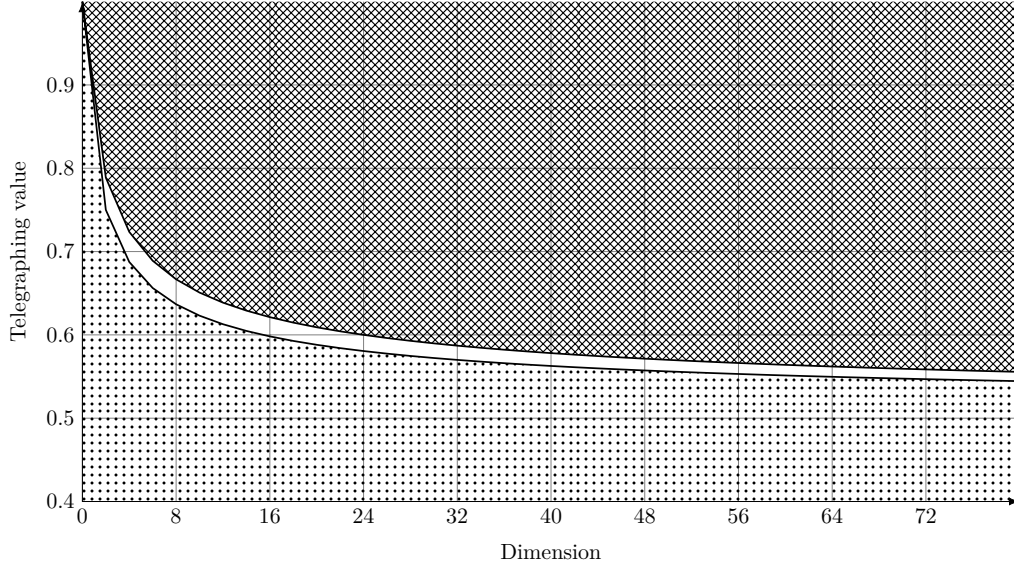


Figure 1: Bounds on the telegraphing value of the Haar-measure encryption of one bit, where the outlined white region is the range of possible values. The crosshatched XXXX region represents the upper bound of [Theorem 1](#) and the dotted XXXX region represents the general lower bound of [Proposition 1](#).

Table 1: Improvements on lower bounds for uncloneable encryption

Winning probability lower bound	[MST21]	Our work
2 messages, dimension d	$\frac{1}{2} + \Omega(\frac{1}{d})$	$\frac{1}{2} + \Omega(\frac{1}{\sqrt{d}})$
n messages, dimension d	$\frac{1}{2} + \Omega(\frac{n}{d})$	$\frac{1}{2} + \Omega(\sqrt{\frac{n}{d}})$
t -to- $(t+1)$ copies, n messages, dimension d	—	$\frac{1}{2} + \Omega(\sqrt{\frac{tn}{d}})$

The minimality of the Haar-measure scheme yields general lower bounds for UTE, and consequently for UE (see [Figure 2](#)).

Result 10 ([Corollary 6](#)). *For any UE scheme with ciphertext dimension d , the winning probability of the uncloneability-indistinguishability game is lower bounded by*

$$\frac{1}{2} + \Omega\left(\frac{1}{\sqrt{d}}\right).$$

This lower bound improves upon the previously best-known bound for UE, namely $\frac{1}{2} + \Omega(\frac{1}{d})$, established in [\[MST21\]](#). The improved lower bounds on attacks against UE in different models are summarised in [Table 1](#).

We further study a strengthened notion of UTE security where adversarial quantum channels are restricted only to entanglement-breaking channels, which strictly generalize quantum-to-classical maps. This yields novel generalised guarantees for both untelegraphable-indistinguishable and t -copy untelegraphable-indistinguishable security (see [Lemma 1](#)).

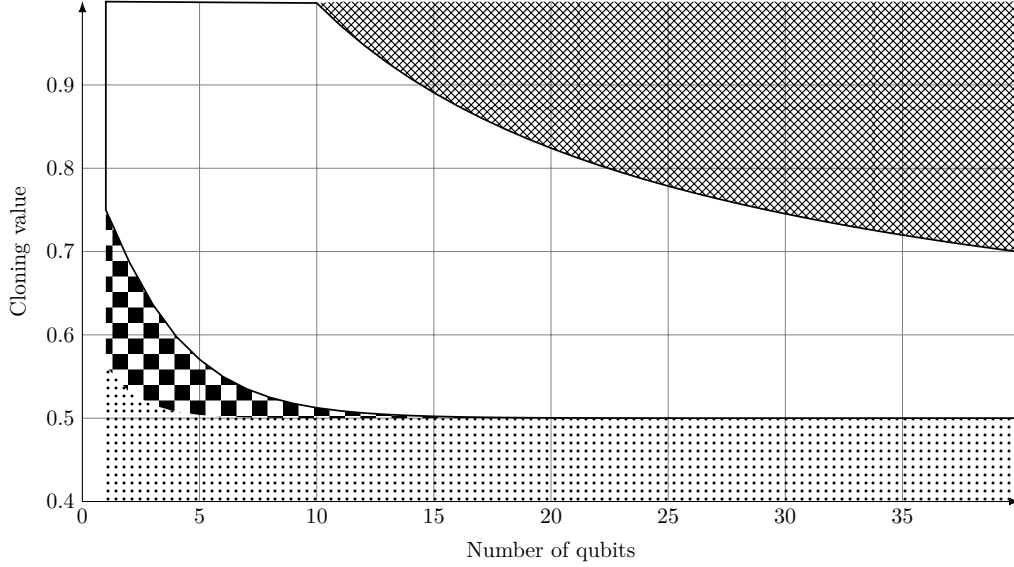


Figure 2: Bounds on the cloning value of the Haar-measure encryption of one bit, where the outlined white region is the range of possible values. The crosshatched $\boxtimes$ region represents the upper bound due to [BC26], the dotted $\cdots$ region represents the lower bound due to [MST21], and the checkered $\blacksquare$ region represents the improved lower bound of Proposition 1.

1.2 Technical overview

The proofs of our main results can be organised into four groups. We give here the common ideas behind each group, while deferring the operator calculations and the precise estimates to the corresponding sections.

Upper bounds from Haar moments. The upper bounds in Results 1 to 4 all rely on the fact that, before the key is revealed, a Haar-random conjugation makes the outcome of any fixed measurement nearly independent of the encrypted message. For the one-copy encryption of a bit, we express the success probability of a telegraphing attack in terms of the Choi operator ρ of its channel. Since a telegraphing channel is entanglement-breaking, the normalised Choi operator is separable; by convexity, it is therefore enough to consider pure product states. The receiver’s POVM then contributes only convex weights, and the adversary’s success probability is bounded by

$$\int \max_{b \in \{0,1\}} \text{Tr}[\tilde{\rho}_1 \bar{U} \Pi_{m_b} U^\top] dU,$$

where Π_{m_0} and Π_{m_1} are complementary rank- $d/2$ projections. Writing the maximum as the sum of its mean and half of the absolute difference, and applying Jensen’s inequality, reduces the problem to the second Haar moment of this difference. The second-moment twirl lies in the span of the identity and flip operators, and an explicit Weingarten calculation gives the bound in Theorem 1.

For t copies, an exact evaluation of the $2t^{\text{th}}$ Haar moment would be cumbersome. Instead, we compare the Haar moment operator with a simpler permutation operator, following [SHH25]. If σ has operator norm at most $1/r$, this comparison shows that, for

every effect $0 \leq P \leq I$ and every relevant k ,

$$\left| \int \text{Tr}[P(U\sigma U^*)^{\otimes k}] dU - \frac{\text{Tr}[P]}{d^k} \right| \leq \frac{7k^2}{r} \frac{\text{Tr}[P]}{d^k}.$$

Applying this estimate for $k = t$ and $k = 2t$ controls the variance of every POVM outcome around its maximally mixed value. Cauchy–Schwarz, followed by the identity $\sum_x \text{Tr}[P_x] = d^t$, converts this variance bound into an $O(t/\sqrt{r})$ distinguishing advantage, yielding [Theorem 2](#). The collusion-resistant proof follows the same scheme. The sequence of adaptive generalised measurements is first folded into a single POVM on all Q ciphertexts, indexed by the complete transcript. A multivariate version of the moment estimate applies to the resulting tensor product of orthogonal message states, and gives an $O(Q/\sqrt{r})$ advantage. Finally, only moments up to order $2Q$ are used, so sufficiently accurate unitary designs give bounded-round security. For everlasting security, the proof first removes the possibly unbounded post-key decision rule from the estimate; the remaining moment quantity is efficiently testable and can therefore be transferred from Haar-random unitaries to pseudorandom unitaries.

Untelegraphable encryption as a many-receiver limit. The proof of [Theorem 4](#) uses monogamy of entanglement rather than Haar integration. Starting from a 1-to- s cloning attack with channel Φ , we pass to its Choi state and symmetrise the s receiving registers, while retaining classical labels for their measurements. The resulting state has identical one-receiver marginals. Since the input register has dimension d , its entanglement of formation with all receivers is at most $\log d$. Yang’s monogamy inequality [[Yan06](#)] therefore implies that the convex-roof classical correlation between the input and one receiver is at most $\log(d)/s$.

We then choose a convex decomposition witnessing this bound. Components with classical correlation larger than a threshold ε have small total weight. On every remaining component, the receiver’s measurement creates a classical–quantum ensemble with Holevo information at most ε ; Pinsker’s inequality then shows that the corresponding conditional input states are close, on average, to their marginal state. Replacing every bipartite component by the product of its marginals produces the Choi state of an entanglement-breaking channel, and hence a telegraphing attack. The low-correlation components are controlled by Pinsker’s inequality, while the remaining components are controlled by their small total weight. The operator-norm bound on the ciphertexts converts the trace-distance approximation into a bound on the difference between the cloning and telegraphing values. Optimising over ε gives the convergence rate of order $s^{-1/3}$.

Explicit attacks and lower bounds. The lower bounds in [Corollaries 2](#) and [4](#) arise from a concrete telegraphing strategy. The telegrapher measures the ciphertext in the computational basis and sends the outcome. Once the key U is revealed, the receiver outputs the message whose encrypted subspace gives the larger diagonal probability at that outcome. By Haar invariance, the success probability is the expected maximum of the weights of two fixed rank- r blocks in a uniformly random pure state. Using the Gaussian representation of a Haar-random vector, these block weights form a normalised collection of Gamma random variables. In the binary case this gives the exact expression

$$\frac{1}{2} + \frac{1}{2^{2r+1}} \binom{2r}{r},$$

and Stirling’s approximation yields the claimed $\Theta(1/\sqrt{r})$ advantage. For n messages, a distinguishing attack fixes two message blocks of rank $r = d/n$; the remaining coordinates integrate out, so the same binary calculation applies. With t ciphertext copies, the attack is

run independently on each copy and the receiver takes a majority vote. Standard binomial estimates amplify a one-copy bias δ to order $\sqrt{t}\delta$, which gives the stated t -copy lower bound.

Minimality of Haar-measure encryption. The universal lower bounds follow from the minimality theorem [Theorem 5](#). Let $\mathbf{Q}$ be any correct QECM with $n = |M|$ messages. Perfect correctness implies that, for each key, the supports of the ciphertexts are mutually orthogonal. After an isometric embedding into $\mathbb{C}^{r^n}$, where $r = \dim H - n + 1$, each ciphertext can therefore be written as $U_k \delta_m^k U_k^*$, with δ_m^k supported in the m -th block of dimension r . We then pass through a sequence of increasingly symmetric hybrid schemes. First, the common basis is replaced by an independent Haar-random basis. Next, each message block is randomly permuted. Haar invariance and averaging show that neither transformation increases the optimal attack value: every attack against a hybrid induces an attack of at least the same value against the preceding scheme. Averaging within a block maps every δ_m^k to the maximally mixed state σ_m on that block. Hence, any attack against the rank- r Haar-measure scheme $\mathbf{Q}_{r,n}$ can be lifted to an attack against the final hybrid, with the same averaged value, by ignoring the additional block information contained in the key. Consequently,

$$\mathbf{c}_{1 \rightarrow s}^N(\mathbf{Q}_{r,n} | \mathcal{F}) \leq \mathbf{c}_{1 \rightarrow s}^N(\mathbf{Q} | \mathcal{F})$$

for all channel classes $\mathcal{F}$ considered here. Combining this comparison with the explicit Haar attack gives the general UTE lower bound; since cloning attacks include telegraphing attacks, the same bound applies to UE and yields [Corollary 6](#). For several ciphertext copies, the same symmetrisation is approximate rather than exact, and the higher-moment estimate above controls the resulting error.

1.3 Open questions

1. Untelegraphable encryption constitutes a restriction of uncloneable encryption in the sense that it imposes a strict classicality on the messages that the pirate can send to the receiving adversaries. There are also a variety of intermediate restrictions that can be imposed on the pirate channel, *e.g.*, bounded storage [[DFSS05](#)] or noisy communication [[WST08](#)]. These do not achieve the full generality of cloning attacks, but they do give rise to a much wider range of possible attacks than telegraphing. Is it possible to find similar upper bounds on the value to the ones we find in those models?
2. In this work, we use untelegraphable encryption to constrain the value of uncloneable encryption. Is it possible to use this line of reasoning to find stronger results? For example, could we show the existence of an uncloneable bit by reducing to an untelegraphable encryption protocol?

1.4 Organization

The remainder of this paper is organized as follows. [Section 2](#) introduces notation, background in quantum information theory, and formal definitions of the encryption schemes and security notions. [Section 3](#) defines the Haar-random scheme and proves untelegraphable-indistinguishability security. [Section 4](#) proves that the Haar-measure scheme is secure against telegraphing-distinguishing attacks with collusion. [Section 5](#) establishes the asymptotic equivalence of UTE and UE. [Section 6](#) derives lower bounds for Haar-measure security. [Section 7](#) proves a minimality property of the Haar-measure scheme and lower bounds for all UTE and UE schemes.

2 Preliminaries

We let $\mathbb{N}$ denote the set of natural numbers, and write $[n]$ for the set $\{0, \dots, n-1\}$. The logarithm with base b is denoted by $\log_b(\cdot)$, and in particular, we use $\log(\cdot)$ to denote the binary logarithm.

All Hilbert spaces considered in this work are assumed to be finite-dimensional. Given a finite set A , write $H_A = \mathbb{C}^A$ for the Hilbert space with canonical orthonormal basis $\{|a\rangle \mid a \in A\}$; in this case, A is called a register. For Hilbert spaces H and K , we denote by $\mathcal{B}(H, K)$ the space of bounded linear operators from H to K . In the special case $K = H$, we simply write $\mathcal{B}(H)$. The identity operator on $H \simeq \mathbb{C}^d$ is denoted by I_d , where the subscript is dropped if clear from context, and the trace over H is written as $\text{Tr}[\cdot]$. An operator $M \in \mathcal{B}(H)$ is positive semi-definite if and only if it is Hermitian (*i.e.*, $M^* = M$) with non-negative eigenvalues, in which case we write $M \succeq 0$. The Hilbert space norm is denoted by $\|\cdot\|$. The operator norm on $\mathcal{B}(H)$ is also denoted $\|\cdot\|$, and the trace norm is denoted $\|\cdot\|_{\text{Tr}} = \frac{1}{2}\|\cdot\|_1$.

A Hilbert space H will be regarded as a quantum system. A quantum state (or density operator) on H is a positive semi-definite operator $\rho \in \mathcal{B}(H)$ with unit trace. The set of all density operators is convex, with extreme points given by rank-one projectors $|\psi\rangle\langle\psi|$, where $|\psi\rangle \in H$ is a unit vector, referred to as a pure state. We shall use both vector and matrix notations for pure states interchangeably. We sometimes write $\rho_{A_1 \dots A_n}$ to mean $\rho \in \mathcal{B}(H_{A_1} \otimes \dots \otimes H_{A_n})$.

For a composite system $H \simeq H_{A_1} \otimes \dots \otimes H_{A_n}$ consisting of n subsystems, the partial trace over the i -th subsystem is denoted by $\text{Tr}_{A_i}[\cdot]$. We write partial traces of states $\rho_{A_1 \dots A_n}$ as $\rho_{A_1 \dots A_{i-1} A_{i+1} \dots A_n} = \text{Tr}_{A_i}(\rho)$. When subsystems have different dimensions, we also index the partial trace by the dimension being traced out. For instance, if $H \simeq \mathbb{C}^d \otimes \mathbb{C}^D$, the notation $\text{Tr}_D[\cdot]$ refers to the partial trace over the second tensor factor.

A linear map $\Phi : \mathcal{B}(H) \rightarrow \mathcal{B}(H)$ is said to be completely positive if, for every $k \in \mathbb{N}$, the extended map $\Phi \otimes \text{id}_k$ is positive (*i.e.*, it maps positive operators to positive operators), where id_k denotes the identity map on $\mathcal{B}(\mathbb{C}^k)$. The map Φ is trace preserving if $\text{Tr}[\Phi(\rho)] = \text{Tr}[\rho]$ for all $\rho \in \mathcal{B}(H)$. A quantum channel is a map that is both Completely Positive and Trace Preserving (CPTP).

A positive operator-valued measure (POVM) on H is a finite family of positive semi-definite operators $\{M_i\}$ satisfying $\sum_i M_i = I$. A projection-valued measure (PVM) is a special case of a POVM in which each M_i is an orthogonal projector. A generalised measurement on H is a finite family of linear maps $\{V_i : H \rightarrow K\}$ for some Hilbert space K such that $\sum_i V_i^* V_i = I$.

We denote by $\mathfrak{S}_n$ the symmetric group on n elements. A unitary representation of a finite group G is a group homomorphism $G \rightarrow \mathcal{U}(H)$. We make use of the representation $V_d : \mathfrak{S}_n \rightarrow \mathcal{U}((\mathbb{C}^d)^{\otimes n})$ defined via $V_d(\pi)(|\psi_1\rangle \otimes \dots \otimes |\psi_n\rangle) = |\psi_{\pi^{-1}(1)}\rangle \otimes \dots \otimes |\psi_{\pi^{-1}(n)}\rangle$. The group of $d \times d$ unitary matrices is written as $\mathcal{U}(d) = \mathcal{U}(\mathbb{C}^d)$, consisting of all matrices U such that $UU^* = U^*U = I_d$.

There is a unique translation-invariant probability measure on $\mathcal{U}(d)$ called the Haar measure. We denote this measure as μ_{Haar} , since d is usually clear from context. We denote integration with respect to the Haar measure by $\int \cdot dU = \int \cdot d\mu_{\text{Haar}}(U)$.

A family of functions $G_\lambda : K_\lambda \rightarrow \mathcal{U}(2^\lambda)$ is a pseudorandom unitary if there is a quantum polynomial-time (in λ) algorithm that implements $k \mapsto G_\lambda(k)$, and any quantum polynomial-time distinguisher can only distinguish Haar-random U from $G_\lambda(k)$ with uniformly random k with negligible advantage, given oracle and inverse oracle access to either.

2.1 Untelegraphable and uncloneable encryption

Untelegraphable encryption, introduced in [CKNY26], is a relaxation of *uncloneable encryption* [BL20]: a symmetric-key encryption scheme of classical messages in which ciphertexts are quantum states, designed to prevent unauthorized replication of information by adversaries.

Parameter conventions. Throughout the paper, $n = |M|$ denotes the total number of messages, $N = |M_0|$ the number of messages considered in a particular attack, r the rank of each ciphertext state in the Haar-measure scheme, and $d = rn$ the corresponding ciphertext dimension. We use t for the number of input ciphertext copies, s for the number of receiving adversaries, Q for the number of rounds in a collusion attack, and k for the order of a Haar moment or unitary design. For an arbitrary QECM with codespace H , we write $D = \dim H$ when it is necessary to distinguish its dimension from the dimension rn of the associated Haar-measure scheme.

Definition 2. A *quantum encryption of classical messages (QECM)* is a tuple $\mathbf{Q} = (M, K, \pi, H, \{\sigma_m^k\}_{k \in K, m \in M})$, where

- M is a finite set, called the set of *messages*;
- K is a measurable space, called the set of *keys*;
- π is a probability measure on K , called the *key distribution*;
- H is a finite-dimensional Hilbert space, called the *codespace*;
- σ_m^k are quantum states on H , called the *ciphertexts*.

The QECM $\mathbf{Q}$ is ε -correct if for each $k \in K$, there is a POVM $\{P_m^k\}_{m \in M}$ such that for any $m \in M$,

$$\int_K \text{Tr}(P_m^k \sigma_m^k) d\pi(k) \geq 1 - \varepsilon.$$

We say $\mathbf{Q}$ is *correct* if it is 0-correct.

An *efficient QECM* is a collection of QECMs $\{\mathbf{Q}_\lambda\}_{\lambda \in \mathbb{N}}$ such that there exists a negligible function η such that $\mathbf{Q}_\lambda$ is $\eta(\lambda)$ -correct and a triple of quantum algorithms:

- $\text{Gen} : \{1\}^* \rightarrow \bigcup_\lambda K_\lambda$ such that $\text{Gen}(1^\lambda)$ samples from π_λ , called the *key generation algorithm*;
- $\text{Enc} : \bigcup_\lambda \{1^\lambda\} \times M_\lambda \times K_\lambda \rightarrow \bigcup_\lambda D(H_\lambda)$ such that $\text{Enc}(1^\lambda, m, k) = \sigma_m^{\lambda, k}$, called the *encryption algorithm*;
- $\text{Dec} : \bigcup_\lambda \{1^\lambda\} \times D(H_\lambda) \times K_\lambda \rightarrow \bigcup_\lambda M_\lambda$ such that for all $m \in M_\lambda$,

$$\Pr \left[\text{Dec}(1^\lambda, \sigma_m^{\lambda, k}, k) = m \mid k \leftarrow \pi \right] \geq 1 - \eta(\lambda).$$

We can capture cloning and telegraphing attacks in tandem with the following general form of attack against a QECM. Unless otherwise specified, we assume that the adversaries are computationally unbounded.

Definition 3. Let $N, t, s \in \mathbb{N}$ and let $\mathcal{F}$ be a collection of quantum channels. A *t-to-s N-message cloning attack over $\mathcal{F}$* against a QECM $\mathbf{Q}$ is a tuple

$$\mathbf{A} = (M_0, \{B_i\}_{i \in [s]}, \{P_m^{i, k}\}_{i \in [s], k \in K, m \in M_0}, \Phi),$$

where

- $M_0 \subseteq M$ is a set of N messages;
- B_i is a finite-dimensional Hilbert space for each i ;
- For each $i \in [s]$ and $k \in K$, $\{P_m^{i,k}\}_{m \in M_0} \subseteq \mathcal{B}(B_i)$ is a POVM;
- $\Phi : \mathcal{B}(H^{\otimes t}) \rightarrow \mathcal{B}(B_0 \otimes \cdots \otimes B_{s-1})$ is a quantum channel such that $\Phi \in \mathcal{F}$.

The *cloning probability* of $\mathbf{A}$ against $\mathbf{Q}$ is

$$\mathbf{c}_{t \rightarrow s}^N(\mathbf{Q}|\mathbf{A}) = \int_K \frac{1}{N} \sum_{m \in M_0} \text{Tr}[(P_m^{1,k} \otimes \cdots \otimes P_m^{s,k}) \Phi((\sigma_m^k)^{\otimes t})] d\pi(k).$$

The *t-to-s N-message cloning value over $\mathcal{F}$* of $\mathbf{Q}$ is $\mathbf{c}_{t \rightarrow s}^N(\mathbf{Q}|\mathcal{F}) = \sup_{\mathbf{A}} \mathbf{c}_{t \rightarrow s}^N(\mathbf{Q}|\mathbf{A})$, where the supremum is over all *t-to-s N-message cloning attacks* from $\mathcal{F}$; N is omitted when $N = |M|$ and $\mathcal{F}$ is omitted when it is the set of all channels. If $N = |M|$, we omit M_0 in $\mathbf{A}$, and if $s = 1$, we omit i in B_i and $P_m^{i,k}$.

It is easy to see that if $\mathcal{F}$ is closed under pre- and post-composition with partial traces, then $\mathbf{c}_{t \rightarrow s}^N(\mathbf{Q}|\mathcal{F}) \leq \mathbf{c}_{t' \rightarrow s'}^N(\mathbf{Q}|\mathcal{F})$ for $t' \geq t$ and $s' \leq s$.

We recover the various values studied in the context of uncloneable and untelegraphable encryption as special cases of this definition.

Definition 4. Let $\mathbf{Q}$ be a QECM. Let $\mathcal{M}$ be the set of all measurement channels.

- A *cloning attack* against $\mathbf{Q}$ is a 1-to-2 $|M|$ -message cloning attack. The *cloning value* of $\mathbf{Q}$ is $\mathbf{c}_{1 \rightarrow 2}(\mathbf{Q})$. We say $\mathbf{Q}$ is ε -*uncloneable secure* if $\mathbf{c}_{1 \rightarrow 2}(\mathbf{Q}) \leq \frac{1}{|M|} + \varepsilon$. An efficient QECM $\{\mathbf{Q}_\lambda\}_\lambda$ is η -*uncloneable secure* if $\mathbf{Q}_\lambda$ is $\eta(\lambda)$ -uncloneable secure for each λ . We say $\{\mathbf{Q}_\lambda\}_\lambda$ is *weakly uncloneable secure* if $\lim_{\lambda \rightarrow \infty} \eta(\lambda) = 0$ and *strongly uncloneable secure* if η is a negligible function.
- A *cloning-distinguishing attack* against $\mathbf{Q}$ is a 1-to-2 2-message cloning attack. The *cloning-distinguishing value* of $\mathbf{Q}$ is $\mathbf{c}_{1 \rightarrow 2}^2(\mathbf{Q})$. We say $\mathbf{Q}$ is ε -*uncloneable-indistinguishable secure* if $\mathbf{c}_{1 \rightarrow 2}^2(\mathbf{Q}) \leq \frac{1}{2} + \varepsilon$. An efficient QECM $\{\mathbf{Q}_\lambda\}_\lambda$ is η -*uncloneable-indistinguishable secure* if $\mathbf{Q}_\lambda$ is $\eta(\lambda)$ -uncloneable-indistinguishable secure for each λ . We say $\{\mathbf{Q}_\lambda\}_\lambda$ is *weakly uncloneable-indistinguishable secure* if $\lim_{\lambda \rightarrow \infty} \eta(\lambda) = 0$ and *strongly uncloneable-indistinguishable secure* if η is a negligible function.
- A *telegraphing attack* is a 1-to-1 $|M|$ -message cloning attack over $\mathcal{M}$. The *telegraphing value* of $\mathbf{Q}$ is $\mathbf{c}_{1 \rightarrow 1}(\mathbf{Q}|\mathcal{M})$. We say $\mathbf{Q}$ is ε -*untelegraphable secure* if $\mathbf{c}_{1 \rightarrow 1}(\mathbf{Q}|\mathcal{M}) \leq \frac{1}{|M|} + \varepsilon$. An efficient QECM $\{\mathbf{Q}_\lambda\}_\lambda$ is η -*untelegraphable secure* if $\mathbf{Q}_\lambda$ is $\eta(\lambda)$ -untelegraphable secure for each λ . We say $\{\mathbf{Q}_\lambda\}_\lambda$ is *weakly untelegraphable secure* if $\lim_{\lambda \rightarrow \infty} \eta(\lambda) = 0$ and *strongly untelegraphable secure* if η is a negligible function.
- A *telegraphing-distinguishing attack* is a 1-to-1 2-message cloning attack over $\mathcal{M}$. The *telegraphing-distinguishing value* of $\mathbf{Q}$ is $\mathbf{c}_{1 \rightarrow 1}^2(\mathbf{Q}|\mathcal{M})$. We say $\mathbf{Q}$ is ε -*untelegraphable-indistinguishable secure* if $\mathbf{c}_{1 \rightarrow 1}^2(\mathbf{Q}|\mathcal{M}) \leq \frac{1}{2} + \varepsilon$. An efficient QECM $\{\mathbf{Q}_\lambda\}_\lambda$ is η -*untelegraphable-indistinguishable secure* if $\mathbf{Q}_\lambda$ is $\eta(\lambda)$ -untelegraphable-indistinguishable secure for each λ . We say $\{\mathbf{Q}_\lambda\}_\lambda$ is *weakly untelegraphable-indistinguishable secure* if $\lim_{\lambda \rightarrow \infty} \eta(\lambda) = 0$ and *strongly untelegraphable-indistinguishable secure* if η is a negligible function.

Observe that $\mathbf{c}_{t \rightarrow s}^2(\mathbf{Q}|\mathcal{M}) = \mathbf{c}_{t \rightarrow s'}^2(\mathbf{Q}|\mathcal{M})$ for any s and s' , since the outputs of measurement channels in $\mathcal{M}$ can be prepared into an arbitrary number of copies.

Definition 5. An *efficient attack* against an efficient QECM $\{Q_\lambda\}_\lambda$ is a collection of attacks $\{A_\lambda = (M_0^\lambda, \{B_i^\lambda\}, \{P_m^{\lambda,i,k}\}, \Phi^\lambda)\}_\lambda$ such that A_λ is an attack against Q_λ , and the attacks can be implemented in polynomial time in λ .

An efficient QECM $\{Q_\lambda\}_\lambda$ is *uncloneable-indistinguishable secure against efficient adversaries* if for every efficient attack $\{A_\lambda\}_\lambda$ against $\{Q_\lambda\}_\lambda$ where A_λ is a cloning-distinguishing attack, $c_{1 \rightarrow 2}^2(Q_\lambda|A_\lambda) = \frac{1}{2} + \text{negl}(\lambda)$. An efficient QECM $\{Q_\lambda\}_\lambda$ is *untelegraphable-indistinguishable secure against efficient adversaries* if for every efficient attack $\{A_\lambda\}_\lambda$ against $\{Q_\lambda\}$ where A_λ is a telegraphing-distinguishing attack, $c_{1 \rightarrow 1}^2(Q_\lambda|A_\lambda) = \frac{1}{2} + \text{negl}(\lambda)$.

An efficient QECM $\{Q_\lambda\}_\lambda$ is *everlasting uncloneable-indistinguishable secure against efficient adversaries* if for every collection of attacks $\{A_\lambda\}_\lambda$ where A_λ is a cloning-distinguishing attack against Q_λ and Φ^λ can be efficiently implemented (but not necessarily the measurements $P_m^{\lambda,i,k}$), $c_{1 \rightarrow 2}^2(Q_\lambda|A_\lambda) = \frac{1}{2} + \text{negl}(\lambda)$. An efficient QECM $\{Q_\lambda\}_\lambda$ is *everlasting untelegraphable-indistinguishable secure against efficient adversaries* if for every collection of attacks $\{A_\lambda\}_\lambda$ where A_λ is a telegraphing-distinguishing attack against Q_λ and Φ^λ can be efficiently implemented, $c_{1 \rightarrow 1}^2(Q_\lambda|A_\lambda) = \frac{1}{2} + \text{negl}(\lambda)$.

In [CKNY26], a further security notion was also considered, which is not captured by the above framework.

Definition 6. A *telegraphing-distinguishing attack with collusion* A against a QECM $Q = (M, K, \pi, H, \{\sigma_m^k\}_{k,m})$ consists of $Q \in \mathbb{N}$ rounds, a finite set X of telegraphing messages, a probability distribution $p(\cdot|x, k)$ on $\{0, 1\}$ for all $x \in X$ and $k \in K$, Hilbert spaces H_i for $i \in [Q+1]$ where $H_0 = \mathbb{C}$, generalised measurements $\{V_{m_0, m_1}^i : H_i \otimes H \rightarrow H_{i+1}\}_{(m_0, m_1) \in M^2, m_0 \neq m_1}$ for $i \in [Q]$, and a POVM $\{P_x\}_{x \in X} \subseteq \mathcal{B}(H_Q \otimes H)$. The *value* of A against Q is

$$t(Q|A) = \int_K \frac{1}{2} \sum_{\substack{b \in \{0,1\} \\ x \in X \\ m_0^{(1)}, m_1^{(1)}, \dots, \\ m_0^{(Q)}, m_1^{(Q)}}} p(b|x, k) \text{Tr} \left[P_x \cdot V_{m_0^{(Q)}, m_1^{(Q)}}^{Q-1} \cdots (V_{m_0^{(1)}, m_1^{(1)}}^0 (V_{m_0^{(1)}, m_1^{(1)}}^0)^\dagger \otimes \sigma_{m_b^{(1)}}^k) \cdots V_{m_0^{(Q)}, m_1^{(Q)}}^{Q-1} \otimes \sigma_{m_b^{(Q)}}^{(Q)} \right] d\pi(k)$$

An efficient QECM $\{Q_\lambda\}_\lambda$ is *collusion-resistant untelegraphable-indistinguishable secure* if for any efficient telegraphing-distinguishing attack with collusion $\{A_\lambda\}_\lambda$, $t(Q_\lambda|A_\lambda) \leq \frac{1}{2} + \text{negl}(\lambda)$.

An efficient QECM $\{Q_\lambda\}_\lambda$ is *everlasting collusion-resistant untelegraphable-indistinguishable secure* if for any collection of telegraphing-distinguishing attacks with collusion $\{A_\lambda\}_\lambda$ such that the $V_{m_0, m_1}^{\lambda,i}$ and P_x^λ are efficiently implemented, $t(Q_\lambda|A_\lambda) \leq \frac{1}{2} + \text{negl}(\lambda)$.

It follows directly from the above definitions that collusion-resistant untelegraphable-indistinguishable security is a stronger security notion than multi-copy untelegraphable-indistinguishable security, in the sense that $t(Q) \geq c_{Q \rightarrow 1}^N(Q|\mathcal{M})$.

Telegraphing attacks admit an alternate characterisation owing to the fact that the message the telegrapher sends is classical.

Lemma 1. Let $Q = (M, K, \pi, H, \{\sigma_m^k\})$ be a QECM. If $A = (M_0, B, \{P_m^k\}, \Phi)$ is a 1-to-1 N -message cloning attack where Φ is an entanglement-breaking channel, then there exists a set X , probability distributions $p(\cdot|x, k)$ over M_0 for all $x \in X$ and $k \in K$, and a POVM $\{P_x\}_{x \in X} \subseteq \mathcal{B}(H)$ such that

$$c_{1 \rightarrow 1}^N(Q|A) = \int_K \frac{1}{N} \sum_{m \in M_0} \sum_{x \in X} p(m|x, k) \text{Tr}[P_x \sigma_m^k] d\pi(k).$$

Conversely, for any set X , subset $M_0 \subseteq M$ of size N , probability distributions $p(\cdot|x, k)$ over M_0 for all $x \in X$ and $k \in K$, and POVM $\{P_x\}_{x \in X} \subseteq \mathcal{B}(H)$, there exists a 1-to-1 N -message cloning attack $A = (M_0, B, \{P_m^k\}, \Phi)$ such that Φ is a measurement channel and the same equality holds.

It follows that, if $\mathcal{E}$ is the set of entanglement-breaking channels, then $\mathfrak{c}_{1 \rightarrow 1}^N(\mathbb{Q}|\mathcal{E}) = \mathfrak{c}_{1 \rightarrow 1}^N(\mathbb{Q}|\mathcal{M})$.

Proof. Let $\mathbf{A} = (M_0, B, \{P_m^k\}, \Phi)$ be a 1-to-1 N -message cloning attack against $\mathbb{Q}$ where Φ is entanglement-breaking. Then, there exists a POVM $\{P_x\}_{x \in X}$ and states σ_x such that $\Phi(\rho) = \sum_{x \in X} \text{Tr}[P_x \rho] \sigma_x$. Let $p(m|x, k) = \text{Tr}[P_m^k \sigma_x]$. Therefore, we have that

$$\begin{aligned} \mathfrak{c}_{1 \rightarrow 1}^N(\mathbb{Q}|\mathbf{A}) &= \int_K \frac{1}{N} \sum_{m \in M_0} \text{Tr}[P_m^k \Phi(\sigma_m^k)] d\pi(k) \\ &= \int_K \frac{1}{N} \sum_{m \in M_0} \sum_{x \in X} \text{Tr}[P_m^k \sigma_x] \text{Tr}[P_x \sigma_m^k] d\pi(k) \\ &= \int_K \frac{1}{N} \sum_{m \in M_0} \sum_{x \in X} p(m|x, k) \text{Tr}[P_x \sigma_m^k] d\pi(k). \end{aligned}$$

For the converse, let $B = \mathbb{C}^X$, $P_m^k = \sum_{x \in X} p(m|x, k) |x\rangle\langle x|$, $\Phi(\rho) = \sum_{x \in X} \text{Tr}[P_x \rho] |x\rangle\langle x|$. By construction, this is a 1-to-1 N -message cloning attack over $\mathcal{M}$ against $\mathbb{Q}$, and by the same argument, the same equality holds. $\square$

Unccloneable-indistinguishable security provides a stronger guarantee for a QECM scheme than untelegraphable-indistinguishable security. In particular, if a QECM scheme achieves uncloneable-indistinguishable security, then the cloning probability $\mathfrak{c}_{1 \rightarrow 2}^2(\mathbb{Q})$ is negligible. Since $\mathfrak{c}_{1 \rightarrow 1}^2(\mathbb{Q}|\mathcal{M}) \leq \mathfrak{c}_{1 \rightarrow 2}^2(\mathbb{Q})$, then the scheme also satisfies untelegraphable-indistinguishable security.

However the two notions are not equivalent: there exist schemes that satisfy untelegraphable-indistinguishable security but not uncloneable-indistinguishable security. Consider a QECM scheme that is 2-copy untelegraphable-indistinguishable secure for a collection of ciphertexts $\{\rho\}$. Then, the modified 1-copy untelegraphable-indistinguishable secure scheme with ciphertexts of the form $\{\rho \otimes \rho\}$ fails to achieve uncloneable-indistinguishable security, as an attack can trivially apply the identity channel to win with certainty (see [CKNY26] for a separation between UTE and UE with unbounded polynomial number of adversaries, under the classical oracle model).

3 The security of Haar-measure encryption

The Haar-random QECM scheme was introduced by [MST21] as a potential candidate for achieving uncloneable-indistinguishable security without computational assumptions. While a proof of *strong* uncloneable-indistinguishable security for this scheme remains an open question—[BC26] established a *weaker* variant with inverse-logarithmic success probability—in this work, we demonstrate that this scheme satisfies both untelegraphable-indistinguishable security and t -copy untelegraphable-indistinguishable security.

Definition 7. Let $r, n \in \mathbb{N}$. The *rank- r Haar-measure encryption of n messages* is the QECM $\mathbb{Q}_{r,n} = ([n], \mathcal{U}(rn), \mu_{\text{Haar}}, \mathbb{C}^{rn}, \{U \sigma_i U^*\}_{U \in \mathcal{U}(rn), i \in [n]})$, where $\sigma_i = \frac{1}{r} \sum_{j=ri}^{r(i+1)-1} |j\rangle\langle j|$. We call the rank- r Haar-measure encryption of 2 messages the *rank- r Haar-measure encryption of a bit*

We can also express $\sigma_i = \frac{1}{r} |i\rangle\langle i| \otimes I_r$, following from the isomorphism $\mathbb{C}^{rn} \cong \mathbb{C}^n \otimes \mathbb{C}^r$.

Remark 1. The Haar-random QECM scheme can be made computationally efficient, for unitaries of dimension $2^{\#qubits}$, by replacing the Haar-random unitary with a unitary sampled from a t -design. As will become evident from the proof below, achieving t -copy telegraphing security requires the use of a unitary $2t$ -design. Such designs admit efficient implementations, as demonstrated in [MPSY24]. An explicit construction based on a unitary 2-design is presented in [BC26].

The telegraphing-distinguishing value of an attack $\mathbf{A} = (\{m_0, m_1\}, B, \{P_m^k\}_{k \in K, m \in M_0}, \Phi)$ against the Haar-random QECM scheme is given by [Definition 3](#) as

$$\mathfrak{c}_{1 \rightarrow 1}^2(\mathbf{Q}|\mathbf{A}) = \int_{\mathcal{U}(rn)} \frac{1}{2} \sum_{b=0}^1 \text{Tr}[P_{m_b}^U \cdot \Phi(U\sigma_{m_b}U^*)] dU.$$

where the integral is taken over normalized Haar measure of the unitary group. Let ρ denote the positive operator corresponding to the CPTP map Φ defined via the Choi–Jamiołkowski isomorphism as: $\rho := (\text{id} \otimes \Phi) \sum_{ij} |ii\rangle\langle jj|$. In terms of ρ , the telegraphing-distinguishing value can be rewritten as

$$\mathfrak{c}_{1 \rightarrow 1}^2(\mathbf{Q}|\mathbf{A}) = \int \frac{1}{2} \sum_{b=0}^1 \text{Tr}[\rho((U\sigma_{m_b}U^*)^\top \otimes P_{m_b}^U)] dU = \int \frac{1}{2} \sum_{b=0}^1 \text{Tr}[\rho((\bar{U}\sigma_{m_b}U^\top) \otimes P_{m_b}^U)] dU.$$

3.1 One copy untelegraphable-indistinguishable security

We first establish the case of 1-copy untelegraphable-indistinguishable security for Haar-measure encryption of a single classical bit, using unitaries of dimension $d = 2^{\#qubits}$. The full generalization to arbitrary message lengths and multiple-copy will be addressed subsequently.

Theorem 1. *The rank- $d/2$ Haar-measure encryption of classical bits (i.e. 2 messages) achieves strong untelegraphable-indistinguishable security, with telegraphing-distinguishing value upper bounded as*

$$\mathfrak{c}_{1 \rightarrow 1}^2(\mathbf{Q}|\mathcal{M}) \leq \frac{1}{2} + \frac{1}{2\sqrt{d+1}}.$$

Proof. Let Π_i be the projection $\Pi_i := |i\rangle\langle i| \otimes I_{d/2}$, such that the ciphertexts become $\sigma_i = \frac{2}{d} \cdot \Pi_i$. The telegraphing-distinguishing value is given by:

$$\begin{aligned} \mathfrak{c}_{1 \rightarrow 1}^2(\mathbf{Q}|\mathcal{M}) &= \sup_{\mathbf{A}} \int \frac{1}{2} \sum_{b=0}^1 \text{Tr}[\rho((\bar{U}\sigma_{m_b}U^\top) \otimes P_{m_b}^U)] dU \\ &= \sup_{\mathbf{A}} \int \sum_{b=0}^1 \text{Tr}[\frac{1}{d}\rho \cdot ((\bar{U}\Pi_{m_b}U^\top) \otimes P_{m_b}^U)] dU, \end{aligned}$$

where the supremum is taken over all telegraphing-distinguishing attacks. Since $\frac{1}{d}\rho$ is now a normalised density operator, the optimisation can be relaxed by substituting $\tilde{\rho} = \frac{1}{d}\rho$ and optimising over all quantum states:

$$\mathfrak{c}_{1 \rightarrow 1}^2(\mathbf{Q}|\mathcal{M}) \leq \sup_{\tilde{\mathbf{A}}} \int \sum_{b=0}^1 \text{Tr}[\tilde{\rho} \cdot ((\bar{U}\Pi_{m_b}U^\top) \otimes P_{m_b}^U)]$$

Since the CPTP map Φ corresponding to the telegraphing attack is entanglement-breaking, its Choi matrix ρ as well as the associated state $\tilde{\rho}$ are necessarily separable. As the optimization is over the convex set of separable states $\tilde{\rho}$, the supremum is attained at the extremal points of this set, namely the pure product states $\tilde{\rho} = \tilde{\rho}_1 \otimes \tilde{\rho}_2$. Consequently, we may write

$$\begin{aligned} \mathfrak{c}_{1 \rightarrow 1}^2(\mathbf{Q}|\mathcal{M}) &\leq \sup_{\tilde{\mathbf{A}}} \int \sum_{b=0}^1 \text{Tr}[\tilde{\rho}_1 \otimes \tilde{\rho}_2 \cdot ((\bar{U}\Pi_{m_b}U^\top) \otimes P_{m_b}^U)] \\ &= \sup_{\tilde{\mathbf{A}}} \int \sum_{b=0}^1 \underbrace{\text{Tr}[\tilde{\rho}_2 \cdot P_{m_b}^U]}_{:=q(U, m_b)} \text{Tr}[\tilde{\rho}_1 \cdot (\bar{U}\Pi_{m_b}U^\top)] dU, \end{aligned}$$

Since the $q(U, m_b)$ are non-negative reals and sum to 1 over b , then by convexity

$$\sum_{b=0}^1 q(U, m_b) \cdot \text{Tr}[\tilde{\rho}_1 \cdot (\bar{U} \Pi_{m_b} U^\top)] \leq \max_b \left\{ \underbrace{\text{Tr}[\tilde{\rho}_1 \cdot (\bar{U} \Pi_{m_b} U^\top)]}_{:= M_b} \right\}.$$

Applying the identity $\max\{a, b\} = \frac{a+b}{2} + \frac{|a-b|}{2}$ yields:

$$\mathfrak{c}_{1 \rightarrow 1}^2(\mathbb{Q}|\mathcal{M}) \leq \sup_{\bar{\mathbf{A}}} \frac{1}{2} \int M_0 + M_1 dU + \frac{1}{2} \int |M_0 - M_1| dU.$$

Now observe that $\Pi_0 + \Pi_1 = I_d$; thus we have

$$\int M_0 + M_1 dU = \int \text{Tr}[\tilde{\rho}_1 \cdot (\bar{U}(\Pi_0 + \Pi_1)U^\top)] dU = 1,$$

so that:

$$\mathfrak{c}_{1 \rightarrow 1}^2(\mathbb{Q}|\mathcal{M}) \leq \sup_{\bar{\mathbf{A}}} \frac{1}{2} + \frac{1}{2} \int |M_0 - M_1| dU \leq \frac{1}{2} + \frac{1}{2} \sqrt{\int (M_0 - M_1)^2 dU},$$

where the final inequality follows from Jensen's inequality. To evaluate the second moment, we write:

$$(M_0 - M_1)^2 = \text{Tr} \left[\left(\tilde{\rho}_1 \otimes \tilde{\rho}_1 \right) \cdot \left(\bar{U} \otimes \bar{U} \right) \left(\Pi_0 - \Pi_1 \right)^{\otimes 2} \left(U^\top \otimes U^\top \right) \right].$$

Applying the Weingarten calculus for the second moment (see e.g. [Mel24, Cor. 13]), we obtain:

$$\int \left(\left(\bar{U} \otimes \bar{U} \right) \left(\Pi_0 - \Pi_1 \right)^{\otimes 2} \left(U^\top \otimes U^\top \right) \right) dU = c_I \cdot \mathbf{I} + c_F \cdot \mathbf{F},$$

where $\mathbf{I}$ and $\mathbf{F}$ denote respectively the identity and flip (swap) operator on $\mathbb{C}^d \otimes \mathbb{C}^d$, defined by $\mathbf{I}(|a\rangle \otimes |b\rangle) = |a\rangle \otimes |b\rangle$ and $\mathbf{F}(|a\rangle \otimes |b\rangle) = |b\rangle \otimes |a\rangle$. The corresponding Weingarten coefficients c_I and c_F are given by:

$$\begin{aligned} c_I &= \frac{\text{Tr}[(\Pi_0 - \Pi_1)^{\otimes 2} \cdot \mathbf{I}] - \frac{1}{d} \text{Tr}[(\Pi_0 - \Pi_1)^{\otimes 2} \cdot \mathbf{F}]}{d^2 - 1} = \frac{-1}{d^2 - 1}, \\ c_F &= \frac{\text{Tr}[(\Pi_0 - \Pi_1)^{\otimes 2} \cdot \mathbf{F}] - \frac{1}{d} \text{Tr}[(\Pi_0 - \Pi_1)^{\otimes 2} \cdot \mathbf{I}]}{d^2 - 1} = \frac{d}{d^2 - 1}. \end{aligned}$$

The operator $\Pi_0 - \Pi_1$ is a traceless Hermitian unitary operator on $\mathbb{C}^d$. Using the swap trick $\text{Tr}[(A \otimes B) \cdot \mathbf{F}] = \text{Tr}[A \cdot B]$, we conclude:

$$\int (M_0 - M_1)^2 dU = \frac{-1}{d^2 - 1} \text{Tr}[\tilde{\rho}_1]^2 + \frac{d}{d^2 - 1} \text{Tr}[\tilde{\rho}_1^2] \leq \frac{1}{d+1},$$

where we have used the facts that $\text{Tr}[\tilde{\rho}_1]^2 = 1$ and $\text{Tr}[\tilde{\rho}_1^2] \leq 1$ for all quantum states $\tilde{\rho}_1$. Hence, we obtain the claimed upper bound: $\frac{1}{2} + \frac{1}{2\sqrt{d+1}}$. $\square$

3.2 Many copy untelegraphable-indistinguishable security

The above proof relies on the exact expression of the second unitary moment operator, derived via Weingarten calculus. In contrast, the proof of t -copy untelegraphable-indistinguishable security requires the analysis of higher-order moments. While exact evaluations are feasible for low-order moments, they become intractable as the order increases. To address this, we approximate the higher-order moments using the following lemma.

Lemma 2 ([SHH25, Lem. 1]). *Let Φ_k and Ψ_k be two hermitian-preserving maps from $\mathcal{B}(\mathbb{C}^{d^k})$ to $\mathcal{B}(\mathbb{C}^{d^k})$ defined by*

$$\Phi_k(X) := \int_{\mathcal{U}(d)} U^{\otimes k} X U^{*\otimes k} dU \stackrel{\text{weingarten calculus}}{=} \sum_{\pi, \sigma \in \mathfrak{S}_k} \text{Wg}(\pi^{-1}\sigma, d) \text{Tr} \left[V_d(\sigma)^{-1} X \right] \cdot V_d(\pi)$$

$$\Psi_k(X) := \frac{1}{d^k} \sum_{\pi \in \mathfrak{S}_k} \text{Tr} \left[V_d(\pi)^{-1} X \right] \cdot V_d(\pi),$$

where $\mathfrak{S}_k$ denotes the symmetric group on k elements, $\text{Wg}(\cdot, \cdot)$ the Weingarten function, and $V_d(\pi)$ is defined as the tensor permutation of $(\mathbb{C}^d)^{\otimes k}$ associated with $\pi \in \mathfrak{S}_k$. If $d > \sqrt{6}k^{7/4}$, then we have the inequalities

$$\left(1 - \frac{k^2}{d}\right) \Psi_k \preceq \Phi_k \preceq \left(1 + \frac{k^2}{d}\right) \Psi_k,$$

where $\preceq$ is the order on hermitian-preserving maps given by $\Phi \preceq \Psi$ if $(\text{id} \otimes \Phi)(P) \leq (\text{id} \otimes \Psi)(P)$ for all positive semidefinite P .

The value of a t -copy telegraphing-distinguishing attack against the Haar-random QECM scheme $\mathbf{A} = (\{m_0, m_1\}, X, \{P_x\}_{x \in X}, \{p(0|x, k), p(1|x, k)\}_{x \in X, k \in K})$ is given by Definition 3 and Lemma 1 as:

$$\mathfrak{c}_{t \rightarrow 1}^2(\mathbf{Q}|\mathbf{A}) = \int_{\mathcal{U}(rn)} \frac{1}{2} \sum_{b \in \{0,1\}} \sum_{x \in X} p(b|x, U) \text{Tr}[P_x \cdot (U \sigma_{m_b} U^*)^{\otimes t}] dU.$$

where the integral is taken over normalized Haar measure of the unitary group. We can now prove the t -copy untelegraphable-indistinguishable security for rank- r Haar-measure encryption of n messages, using unitaries of dimension $rn = 2^{\# \text{qubits}}$.

Theorem 2. *The rank- r Haar-measure encryption of n messages achieves strong untelegraphable-indistinguishable security, with t -copy telegraphing-distinguishing value upper bounded as*

$$\mathfrak{c}_{t \rightarrow 1}^2(\mathbf{Q}_{r,n}|\mathcal{M}) \leq \frac{1}{2} + \frac{7t}{\sqrt{r}}.$$

Lemma 3. *Let $P \in \mathcal{B}(\mathbb{C}^{d^k})$ such that $0 \leq P \leq I$, and let $\sigma \in \mathcal{B}(\mathbb{C}^d)$ be a state such that $\|\sigma\| \leq \varepsilon$. Suppose $k^2 \leq \frac{1}{\varepsilon}$, then*

$$\left| \int \text{Tr} \left[P \cdot (U \sigma U^*)^{\otimes k} \right] dU - \frac{\text{Tr}[P]}{d^k} \right| \leq \frac{\text{Tr}[P]}{d^k} 7k^2 \varepsilon.$$

It follows from the lemma that $\left\| \int_{\mathcal{U}(d)} (U \sigma U^*)^{\otimes k} dU - \frac{I}{d^k} \right\|_{\text{Tr}} \leq 7k^2 \varepsilon$, and that if $\sigma := \frac{1}{r} \Pi$ for $\Pi \in \mathcal{B}(\mathbb{C}^d)$ a rank r projector and $k^2 \leq r$, then

$$\left| \int \text{Tr} \left[P \cdot (U \sigma U^*)^{\otimes k} \right] dU - \frac{\text{Tr}[P]}{d^k} \right| \leq \frac{\text{Tr}[P]}{d^k} \frac{7k^2}{r}.$$

Proof. First, using Lemma 2, since $k^2 \leq \frac{1}{\varepsilon} \leq d$, we see that

$$\int \text{Tr} \left[P \cdot (U \sigma U^*)^{\otimes k} \right] dU \leq \left(1 + \frac{k^2}{d}\right) \frac{1}{d^k} \sum_{\pi \in \mathfrak{S}_k} \text{Tr} [P \cdot V_d(\pi)] \prod_{i=1}^{\# \pi} \text{Tr}(\sigma^{n_i(\pi)}),$$

where $\#\pi$ is the number of cycles in the cycle decomposition of π and $(n_1(\pi), \dots, n_{\#\pi}(\pi))$ is the cycle shape. We have that $\text{Tr}(\sigma^n) \leq \text{Tr}(\|\sigma\|^{n-1}\sigma) = \|\sigma\|^{n-1}$. Using this and the upper bound $\text{Re Tr}[P \cdot V_d(\pi)] \leq \text{Tr}[P]$,

$$\begin{aligned} \int \text{Tr} [P \cdot (U\sigma U^*)^{\otimes k}] dU &\leq \left(1 + \frac{k^2}{d}\right) \frac{\text{Tr}[P]}{d^k} \sum_{\pi \in \mathfrak{S}_k} \prod_{i=1}^{\#\pi} \text{Tr}(\sigma^{n_i(\pi)}) \\ &\leq \left(1 + \frac{k^2}{d}\right) \frac{\text{Tr}[P]}{d^k} \sum_{\pi \in \mathfrak{S}_k} \varepsilon^{\sum_{i=1}^{\#\pi} (n_i(\sigma)-1)} \\ &\leq \left(1 + \frac{k^2}{d}\right) \text{Tr}[P] \left(\frac{\varepsilon}{d}\right)^k \sum_{\pi \in \mathfrak{S}_k} \varepsilon^{-\#\pi}. \end{aligned}$$

Then we use that

$$\sum_{\pi \in \mathfrak{S}_k} x^{\#\pi} = \sum_{i=0}^k \begin{bmatrix} k \\ i \end{bmatrix} x^i = x^{\bar{k}},$$

where $\begin{bmatrix} k \\ i \end{bmatrix}$ denotes the unsigned Stirling numbers of the first kind, and $x^{\bar{k}}$ is the rising factorial

$$x^{\bar{k}} := x(x+1) \cdots (x+k-1).$$

Then

$$\begin{aligned} \int \text{Tr} [P \cdot (U\sigma U^*)^{\otimes k}] dU &\leq \left(1 + \frac{k^2}{d}\right) \text{Tr}[P] \left(\frac{\varepsilon}{d}\right)^k \varepsilon^{-1} (\varepsilon^{-1} + 1) \cdots (\varepsilon^{-1} + k - 1) \\ &\leq \left(1 + \frac{k^2}{d}\right) \frac{\text{Tr}[P]}{d^k} (1 + \varepsilon) \cdots (1 + (k-1)\varepsilon) \\ &\leq \left(1 + \frac{k^2}{d}\right) \frac{\text{Tr}[P]}{d^k} \prod_{i=0}^{k-1} (1 + i\varepsilon). \end{aligned}$$

Then using the assumption $k^2 \leq \varepsilon^{-1}$

$$\prod_{i=0}^{k-1} (1 + i\varepsilon) \leq (1 + k\varepsilon)^k \leq 1 + \left(1 + \frac{1}{k}\right)^k k^2 \varepsilon \leq 1 + ek^2 \varepsilon.$$

Thus we have the upper bound

$$\begin{aligned} \int \text{Tr} [P \cdot (U\sigma U^*)^{\otimes k}] dU &\leq \left(1 + \frac{k^2}{d}\right) \frac{\text{Tr}[P]}{d^k} (1 + ek^2 \varepsilon) \\ &\leq \frac{\text{Tr}[P]}{d^k} (1 + (2e+1)k^2 \varepsilon). \end{aligned}$$

On the other hand, using [Lemma 2](#), we can lower bound

$$\begin{aligned} \int \text{Tr} [P \cdot (U\sigma U^*)^{\otimes k}] dU &\geq \left(1 - \frac{k^2}{d}\right) \frac{1}{d^k} \sum_{\pi \in \mathfrak{S}_k} \text{Tr} [V_d(\pi)^{-1} \cdot \sigma^{\otimes k}] \text{Tr} [P \cdot V(\pi)] \\ &\geq \left(1 - \frac{k^2}{d}\right) \frac{\text{Tr}(P)}{d^k} \left(2 - \sum_{\pi \in S_k} \text{Tr} [V_d(\pi)^* \sigma^{\otimes k}]\right) \\ &\geq \left(1 - \frac{k^2}{d}\right) \frac{\text{Tr}(P)}{d^k} (2 - (1 + k\varepsilon)^k) \end{aligned}$$

$$\begin{aligned}
&\geq \frac{\text{Tr}(P)}{d^k} \left(1 - \frac{k^2}{d}\right) (1 - ek^2\varepsilon) \\
&\geq \frac{\text{Tr}(P)}{d^k} (1 - (e+1)k^2\varepsilon). \quad \square
\end{aligned}$$

Proof of Theorem 2. Let $\mathbf{A} = (\{m_0, m_1\}, B, \{P_m^k\}, \Phi)$ be a t -copy telegraphing attack against $\mathbf{Q}_{r,n}$. Using Lemma 1, there exists a finite set X , probability distributions $p(\cdot|x, U)$ on $[2]$ for all $x \in X$ and $U \in \mathcal{U}(rn)$, and a POVM $\{P_x\}_{x \in X}$ such that

$$\mathfrak{c}_{t \rightarrow 1}^2(\mathbf{Q}|\mathbf{A}) = \int \frac{1}{2r} \sum_{b \in \{0,1\}} \sum_{x \in X} p(b|x, U) \text{Tr}[P_x \cdot (U \Pi_{m_b} U^*)^{\otimes t}] dU,$$

where $\Pi_i := |i\rangle\langle i| \otimes I_r$. We want to upper-bound this value. To achieve this, it suffices to establish an upper bound on the following quantity:

$$\begin{aligned}
D := &\left| \frac{1}{r} \int \sum_x p(0|x, U) \cdot \text{Tr} \left[P_x \cdot (U \Pi_{m_0} U^*)^{\otimes t} \right] dU \right. \\
&\left. - \frac{1}{r} \int \sum_x p(1|x, U) \cdot \text{Tr} \left[P_x \cdot (U \Pi_{m_1} U^*)^{\otimes t} \right] dU \right|.
\end{aligned}$$

First using the triangle inequality,

$$\begin{aligned}
D &= \left| \frac{1}{r} \int \sum_x p(0|x, U) \cdot \left(\text{Tr} \left[P_x \cdot (U \Pi_{m_0} U^*)^{\otimes t} \right] - \frac{\text{Tr}[P_x]}{d^t} \right) dU \right. \\
&\quad \left. - \frac{1}{r} \int \sum_x p(1|x, U) \cdot \left(\text{Tr} \left[P_x \cdot (U \Pi_{m_1} U^*)^{\otimes t} \right] - \frac{\text{Tr}[P_x]}{d^t} \right) dU \right| \\
&\leq \left| \frac{1}{r} \int \sum_x p(0|x, U) \cdot \left(\text{Tr} \left[P_x \cdot (U \Pi_{m_0} U^*)^{\otimes t} \right] - \frac{\text{Tr}[P_x]}{d^t} \right) dU \right| \\
&\quad + \left| \frac{1}{r} \int \sum_x p(1|x, U) \cdot \left(\text{Tr} \left[P_x \cdot (U \Pi_{m_1} U^*)^{\otimes t} \right] - \frac{\text{Tr}[P_x]}{d^t} \right) dU \right|,
\end{aligned}$$

where we write $d := rn$. Therefore, for any m_b , we can bound by Cauchy-Schwarz as

$$\begin{aligned}
&\left| \frac{1}{r} \int \sum_x p(0|x, U) \cdot \left(\text{Tr} \left[P_x \cdot (U \Pi_{m_b} U^*)^{\otimes t} \right] - \frac{\text{Tr}[P_x]}{d^t} \right) dU \right| \\
&\leq \sum_x \left| \frac{1}{r} \int p(0|x, U) \cdot \left(\text{Tr} \left[P_x \cdot (U \Pi_{m_b} U^*)^{\otimes t} \right] - \frac{\text{Tr}[P_x]}{d^t} \right) dU \right| \\
&\leq \sum_x \sqrt{\int p(0|x, U)^2 dU \cdot \int \left(\text{Tr} \left[P_x \cdot \left(U \left(\frac{1}{r} \cdot \Pi_{m_b} \right) U^* \right)^{\otimes t} \right] - \frac{\text{Tr}[P_x]}{d^t} \right)^2 dU} \\
&\leq \sum_x \sqrt{\int \left(\text{Tr} \left[P_x \cdot \left(U \left(\frac{1}{r} \cdot \Pi_{m_b} \right) U^* \right)^{\otimes t} \right] - \frac{\text{Tr}[P_x]}{d^t} \right)^2 dU}.
\end{aligned}$$

The inner term expands to

$$\begin{aligned} & \left(\text{Tr} \left[P_x \cdot \left(U \left(\frac{1}{r} \cdot \Pi_{m_b} \right) U^* \right)^{\otimes t} \right] - \frac{\text{Tr}[P_x]}{d^t} \right)^2 \\ &= \text{Tr} \left[(P_x \otimes P_x) \cdot \left(U \left(\frac{1}{r} \cdot \Pi_{m_b} \right) U^* \right)^{\otimes 2t} \right] \\ &\quad - 2 \frac{\text{Tr}[P_x]}{d^t} \text{Tr} \left[P_x \cdot \left(U \left(\frac{1}{r} \cdot \Pi_{m_b} \right) U^* \right)^{\otimes t} \right] + \frac{\text{Tr}[P_x]^2}{d^{2t}}. \end{aligned}$$

Then, using [Lemma 3](#) for sufficiently large d ,

$$\begin{aligned} \int \text{Tr} \left[(P_x \otimes P_x) \cdot \left(U \left(\frac{1}{r} \cdot \Pi_{m_b} \right) U^* \right)^{\otimes 2t} \right] dU &\leq \frac{\text{Tr}[P_x \otimes P_x]}{d^{2t}} \left(1 + \frac{7(2t)^2}{r} \right) \\ &= \frac{\text{Tr}[P_x]^2}{d^{2t}} \left(1 + 28 \frac{t^2}{r} \right), \end{aligned}$$

and

$$\text{Tr} \left[P_x \cdot \left(U \left(\frac{1}{r} \cdot \Pi_{m_b} \right) U^* \right)^{\otimes t} \right] \geq \frac{\text{Tr}[P_x]}{d^t} \left(1 - 7 \frac{t^2}{r} \right).$$

Putting these together,

$$\begin{aligned} & \int \left(\text{Tr} \left[P_x \cdot \left(U \left(\frac{1}{r} \cdot \Pi_{m_b} \right) U^* \right)^{\otimes t} \right] - \frac{\text{Tr}[P_x]}{d^t} \right)^2 dU \\ &\leq \frac{\text{Tr}[P_x]^2}{d^{2t}} \left(1 + 28 \frac{t^2}{r} \right) - 2 \frac{\text{Tr}[P_x]^2}{d^{2t}} \left(1 - 7 \frac{t^2}{r} \right) + \frac{\text{Tr}[P_x]^2}{d^{2t}} \\ &\leq 42 \frac{t^2}{r} \frac{\text{Tr}[P_x]^2}{d^{2t}}, \end{aligned}$$

and get

$$\left| \frac{1}{r} \int \sum_x p(0|x, U) \cdot \left(\text{Tr} \left[P_x \cdot (U \Pi_{m_b} U^*)^{\otimes t} \right] - \frac{\text{Tr}[P_x]}{d^t} \right) dU \right| \leq \frac{7t}{\sqrt{r}}.$$

As this holds for both b , then $D \leq \frac{14t}{\sqrt{r}}$.

Now we can write the t -copy telegraphing-distinguishing value $\mathfrak{c}_{t \rightarrow 1}^2(\mathbf{Q}|\mathbf{A})$ as

$$\mathfrak{c}_{t \rightarrow 1}^2(\mathbf{Q}|\mathbf{A}) = \frac{1}{2} \Pr[b' = 0|b = 0] + \frac{1}{2} \Pr[b' = 1|b = 1],$$

where b' is the random variable corresponding to the adversary's guess of b . Then

$$\begin{aligned} \mathfrak{c}_{t \rightarrow 1}^2(\mathbf{Q}|\mathbf{A}) &\leq \frac{1}{2} \Pr[b' = 0|b = 1] + \frac{1}{2} \Pr[b' = 1|b = 1] + \frac{1}{2} D \\ &\leq \Pr \left[(b' = 0 \wedge b = 1) \vee (b' = 1 \wedge b = 1) \right] + \frac{1}{2} D \\ &\leq \frac{1}{2} + \frac{1}{2} D. \end{aligned}$$

□

4 Collusion-resistant security

In this section, we adapt the techniques of [Section 3](#) to the setting of collusion-resistant security. In doing so, we find that the same bounds hold on telegraphing-distinguishing attacks with collusion. We use this to strengthen some results of [\[CKNY26\]](#) by removing or weakening computational assumptions.

Lemma 4. *Let $P \in \mathcal{B}(\mathbb{C}^{d^k})$ such that $0 \leq P \leq I$, and let $\sigma_1, \dots, \sigma_n \in \mathcal{B}(\mathbb{C}^d)$ be orthogonal states such that $\|\sigma_i\| \leq \varepsilon$. Let $k = \sum_{i=1}^n k_i$ and suppose $k^2 \leq \frac{1}{\varepsilon}$. Then*

$$\left| \int \text{Tr} \left[P \cdot (U\sigma_1 U^*)^{\otimes k_1} \otimes \dots \otimes (U\sigma_n U^*)^{\otimes k_n} \right] dU - \frac{\text{Tr}[P]}{d^k} \right| \leq \frac{\text{Tr}[P]}{d^k} 7k^2 \varepsilon.$$

Proof. First, using [Lemma 2](#), since $k^2 \leq \frac{1}{\varepsilon} \leq d$, we see that

$$\begin{aligned} & \int \text{Tr} \left[P \cdot (U\sigma_1 U^*)^{\otimes k_1} \otimes \dots \otimes (U\sigma_n U^*)^{\otimes k_n} \right] dU \\ & \leq \left(1 + \frac{k^2}{d} \right) \frac{1}{d^k} \sum_{\pi \in \mathfrak{S}_k} \text{Tr} [P \cdot V_d(\pi)] \text{Tr} \left[V_d(\pi)^{-1} (\sigma_1^{\otimes k_1} \otimes \dots \otimes \sigma_n^{\otimes k_n}) \right]. \end{aligned}$$

Now, write the cycle decomposition of π as $\pi = (i_{1,1} \dots i_{1,n_1}) \dots (i_{\#\pi,1} \dots i_{\#\pi,n_{\#\pi}})$ and let $f : \{1, \dots, k\} \rightarrow \{1, \dots, n\}$ be the function such that $\sigma_1^{\otimes k_1} \otimes \dots \otimes \sigma_n^{\otimes k_n} = \sigma_{f(1)} \otimes \dots \otimes \sigma_{f(k)}$. Then,

$$\begin{aligned} \text{Tr} \left[V_d(\pi)^{-1} (\sigma_1^{\otimes k_1} \otimes \dots \otimes \sigma_n^{\otimes k_n}) \right] &= \prod_{j=1}^{\#\pi} \text{Tr} \left[\sigma_{f(i_{j,1})} \dots \sigma_{f(i_{j,n_j})} \right] \\ &= \begin{cases} 0 & \exists j, l, m. f(i_{j,l}) \neq f(i_{j,m}) \\ \prod_{j=1}^{\#\pi} \text{Tr} \left[\sigma_{f(i_{j,1})}^{n_j} \right] & \text{else} \end{cases} \\ &\leq \varepsilon^{k - \#\pi}. \end{aligned}$$

Note also that $\text{Tr} \left[V_d(\pi)^{-1} (\sigma_1^{\otimes k_1} \otimes \dots \otimes \sigma_n^{\otimes k_n}) \right] \geq 0$. Therefore, using the upper bound $\text{Re Tr}[P \cdot V_d(\pi)] \leq \text{Tr}[P]$, and hence

$$\begin{aligned} & \int \text{Tr} \left[P \cdot (U\sigma_1 U^*)^{\otimes k_1} \otimes \dots \otimes (U\sigma_n U^*)^{\otimes k_n} \right] dU \\ & \leq \left(1 + \frac{k^2}{d} \right) \frac{\text{Tr}[P]}{d^k} \sum_{\pi \in \mathfrak{S}_k} \text{Tr} \left[V_d(\pi)^{-1} (\sigma_1^{\otimes k_1} \otimes \dots \otimes \sigma_n^{\otimes k_n}) \right] \\ & \leq \left(1 + \frac{k^2}{d} \right) \text{Tr}[P] \left(\frac{\varepsilon}{d} \right)^k \sum_{\pi \in \mathfrak{S}_k} \varepsilon^{-\#\pi}. \end{aligned}$$

So, proceeding exactly as in [Lemma 3](#), we get the upper bound

$$\int \text{Tr} \left[P \cdot (U\sigma_1 U^*)^{\otimes k_1} \otimes \dots \otimes (U\sigma_n U^*)^{\otimes k_n} \right] dU \leq \frac{\text{Tr}[P]}{d^k} \left(1 + (2e + 1)k^2 \varepsilon \right).$$

For the lower bound, we proceed the same way, getting

$$\begin{aligned}
& \int \text{Tr} \left[P \cdot (U\sigma_1 U^*)^{\otimes k_1} \otimes \cdots \otimes (U\sigma_n U^*)^{\otimes k_n} \right] dU \\
& \geq \left(1 - \frac{k^2}{d} \right) \frac{1}{d^k} \sum_{\pi \in \mathfrak{S}_k} \text{Tr} \left[V_d(\pi)^{-1} \cdot (\sigma_1^{\otimes k_1} \otimes \cdots \otimes \sigma_n^{\otimes k_n}) \right] \text{Tr} [P \cdot V_d(\pi)] \\
& \geq \left(1 - \frac{k^2}{d} \right) \frac{\text{Tr}(P)}{d^k} \left(2 - \sum_{\pi \in S_k} \text{Tr} [V_d(\pi)^{-1} (\sigma_1^{\otimes k_1} \otimes \cdots \otimes \sigma_n^{\otimes k_n})] \right) \\
& \geq \frac{\text{Tr}(P)}{d^k} (1 - (e+1)k^2 \varepsilon). \quad \square
\end{aligned}$$

Theorem 3. *Let*

$$A = (Q, X, \{p(b|x, U)\}_{b \in \{0,1\}, k \in \mathcal{U}(rn), x \in X}, \{H_i\}_{i \in [Q+1]}, \{V_{m_0, m_1}^i\}_{i \in [Q]; m_0 \neq m_1 \in M}, \{P_x\}_{x \in X})$$

be a telegraphing-distinguishing attack with collusion against $\mathcal{Q}_{r,n}$. Then,

$$\mathfrak{t}(\mathcal{Q}_{r,n} | A) \leq \frac{1}{2} + 7 \frac{Q}{\sqrt{r}}.$$

Proof. Write $M^{(2)} = \{(m_0, m_1) \in M^2 \mid m_0 \neq m_1\}$ and let $P_{x, m^{(1)}, \dots, m^{(Q)}} = ((V_{m^{(1)}}^0)^\dagger \otimes I) \cdots ((V_{m^{(Q)}}^{Q-1})^\dagger \otimes I) P_x (V_{m^{(Q)}}^{Q-1} \otimes I) \cdots (V_{m^{(1)}}^0 \otimes I)$ for $x \in X$ and $m^{(1)}, \dots, m^{(Q)} \in M^{(2)}$. $\{P_{x, m^{(1)}, \dots, m^{(Q)}}\}_{x \in X; m^{(1)}, \dots, m^{(Q)} \in M^{(2)}}$ is a POVM on $(\mathbb{C}^{rn})^{\otimes Q}$, and the value of A against $\mathcal{Q}_{r,n}$ is

$$\mathfrak{t}(\mathcal{Q}_{r,n} | A) = \int_{\mathcal{U}(rn)} \frac{1}{2} \sum_{\substack{x \in X \\ b \in \{0,1\} \\ m^{(1)}, \dots, m^{(Q)} \in M^{(2)}}} p(b|x, U) \text{Tr}[P_{x, m^{(1)}, \dots, m^{(Q)}} (U\sigma_{m_b^{(1)}} U^* \otimes \cdots \otimes U\sigma_{m_b^{(Q)}} U^*)] dU.$$

Now, we bound the quantity

$$\begin{aligned}
D &:= \left| \int \sum_{\substack{x, \\ m^{(1)}, \dots, m^{(Q)}}} p(0|x, U) \text{Tr}[P_{x, m^{(1)}, \dots, m^{(Q)}} \right. \\
&\quad \times (U\sigma_{m_0^{(1)}} U^* \otimes \cdots \otimes U\sigma_{m_0^{(Q)}} U^* - U\sigma_{m_1^{(1)}} U^* \otimes \cdots \otimes U\sigma_{m_1^{(Q)}} U^*)] dU \Big|.
\end{aligned}$$

As in [Theorem 2](#), the value $\mathfrak{t}(\mathcal{Q}_{r,n} | A) \leq \frac{1}{2} + \frac{1}{2} D$. Then, using the triangle inequality, we can upper bound

$$\begin{aligned}
D &\leq \left| \int \sum_{\substack{x, \\ m^{(1)}, \dots, m^{(Q)}}} p(0|x, U) \left(\text{Tr} \left[P_{x, m^{(1)}, \dots} \left(\bigotimes_i U\sigma_{m_0^{(i)}} U^* \right) \right] - \frac{\text{Tr}[P_{x, m^{(1)}, \dots}]}{d^Q} \right) dU \right| \\
&\quad + \left| \int \sum_{\substack{x, \\ m^{(1)}, \dots, m^{(Q)}}} p(0|x, U) \left(\text{Tr} \left[P_{x, m^{(1)}, \dots} \left(\bigotimes_i U\sigma_{m_1^{(i)}} U^* \right) \right] - \frac{\text{Tr}[P_{x, m^{(1)}, \dots, m^{(Q)}}]}{d^Q} \right) dU \right|.
\end{aligned}$$

Applying Cauchy-Schwarz as in [Theorem 2](#),

$$\begin{aligned}
& \left| \int \sum_{\substack{x, \\ m^{(1)}, \dots, m^{(Q)}}} p(0|x, U) C_{U, x, m^{(1)}, \dots, m^{(Q)}} dU \right| \\
& \leq \sum_{\substack{x, \\ m^{(1)}, \dots, m^{(Q)}}} \left| \int p(0|x, U) C_{U, x, m^{(1)}, \dots, m^{(Q)}} dU \right| \\
& \leq \sum_{\substack{x, \\ m^{(1)}, \dots, m^{(Q)}}} \sqrt{\int p(0|x, U)^2 dU \cdot \int C_{U, x, m^{(1)}, \dots, m^{(Q)}}^2 dU} \\
& \leq \sum_{\substack{x, \\ m^{(1)}, \dots, m^{(Q)}}} \sqrt{\int C_{U, x, m^{(1)}, \dots, m^{(Q)}}^2 dU},
\end{aligned}$$

where

$$C_{U, x, m^{(1)}, \dots, m^{(Q)}} := \text{Tr}[P_{x, m^{(1)}, \dots, m^{(Q)}} (U \sigma_{m_b^{(1)}} U^* \otimes \dots \otimes U \sigma_{m_b^{(Q)}} U^*)] - \frac{\text{Tr}[P_{x, m^{(1)}, \dots, m^{(Q)}}]}{d^Q}.$$

Fix $x, m^{(1)}, \dots, m^{(Q)}$ and write $P = P_{x, m^{(1)}, \dots, m^{(Q)}}$ and $\sigma = \sigma_{m_b^{(1)}} \otimes \dots \otimes \sigma_{m_b^{(Q)}}$. Expanding,

$$\begin{aligned}
& \left(\text{Tr}[P U^{\otimes Q} \sigma (U^*)^{\otimes Q}] - \frac{\text{Tr}[P]}{d^Q} \right)^2 \\
& = \text{Tr}[(P \otimes P) U^{\otimes 2Q} (\sigma \otimes \sigma) (U^*)^{\otimes 2Q}] - 2 \frac{\text{Tr}[P]}{d^Q} \text{Tr}[P U^{\otimes Q} \sigma (U^*)^{\otimes Q}] + \frac{\text{Tr}[P]^2}{d^Q}.
\end{aligned}$$

Taking the integral and using [Lemma 4](#), we get

$$\begin{aligned}
& \int \left(\text{Tr}[P U^{\otimes Q} \sigma (U^*)^{\otimes Q}] - \frac{\text{Tr}[P]}{d^Q} \right)^2 dU \\
& \leq \frac{\text{Tr}[P \otimes P]}{d^{2Q}} \left(1 + \frac{7(2Q)^2}{r} \right) - 2 \frac{\text{Tr}[P]}{d^Q} \frac{\text{Tr}[P]}{d^Q} \left(1 - \frac{7Q^2}{r} \right) + \frac{\text{Tr}[P]^2}{d^Q} \quad (1) \\
& \leq \frac{\text{Tr}[P]^2}{d^{2Q}} 42 \frac{Q^2}{r}.
\end{aligned}$$

Using this,

$$\begin{aligned}
& \sum_{\substack{x, \\ m^{(1)}, \dots, m^{(Q)}}} \sqrt{\int C_{U, x, m^{(1)}, \dots, m^{(Q)}}^2 dU} \\
& \leq \sum_{\substack{x, \\ m^{(1)}, \dots, m^{(Q)}}} \frac{\text{Tr}[P_{x, m^{(1)}, \dots, m^{(Q)}}]}{d^Q} \sqrt{42} \frac{Q}{\sqrt{r}} \leq 7 \frac{Q}{\sqrt{r}}.
\end{aligned}$$

Hence, $D \leq 14 \frac{Q}{\sqrt{r}}$, giving the result. $\square$

Corollary 1. (i) For any polynomial p , there exists an efficient QECM that is collusion-resistant untelegraphable-indistinguishable secure against any attack $\{A_\lambda\}_\lambda$ with number of rounds bounded as $Q^\lambda \leq p(\lambda)$.

- (ii) If pseudorandom unitaries exist, there exists an efficient QECM that is everlasting collusion-resistant untelegraphable-indistinguishable secure.

This corollary strengthens some results of [CKNY26]. First, their construction of a collusion-resistant untelegraphable-indistinguishable secure relies on pseudorandom functions, which may be a stronger assumption than pseudorandom unitaries. Next, to construct the weaker notion of a QECM that is secure against attacks with the number of rounds bounded by a fixed polynomial, [CKNY26] require pseudorandom states whereas we do it unconditionally — nevertheless their construction has succinct keys, where we require polynomial-length keys. Finally, we are able to achieve everlasting security under standard computational assumptions, whereas [CKNY26] require a quantum random oracle model.

Proof. Note first that in Theorem 3, only Equation (1) depends on the measure being the Haar measure. As such, if we replace the question distribution with a different distribution on the unitaries that has the same (or similar) behaviour in (1), then we can get the same (or similar) upper bound on the value. We show the results for messages of a fixed bit length $\ell \in \mathbb{N}$, but they extend identically to messages of polynomially-varying length in λ .

- (i) Let $\mathbf{Q}_{q,\ell,d}$ be the QECM that is identical to $\mathbf{Q}_{2^q,2^\ell}$ except that the key distribution is the uniform distribution on unitaries corresponding to circuits of depth d on $n = \ell + q$ qubits. Due to [Haf22], random circuits in depth $f(n, t) = O(nt^{5+o(1)})$ are t -designs. Let $\mathbf{Q}_\lambda = \mathbf{Q}_{\lambda,\ell,f(\lambda+\ell,2p(\lambda))}$. Then, $\{\mathbf{Q}_\lambda\}_\lambda$ is an efficient QECM by construction. Since the distribution on keys is a $2p(\lambda)$ -design, Equation (1) holds as long as $Q^\lambda \leq p(\lambda)$ and hence for any collection of attacks $\{\mathbf{A}_\lambda\}_\lambda$ such that $Q^\lambda \leq p(\lambda)$, $t(\mathbf{Q}_\lambda|\mathbf{A}_\lambda) \leq \frac{1}{2} + 7\frac{Q^\lambda}{\sqrt{2}^\lambda} = \frac{1}{2} + \text{negl}(\lambda)$.
- (ii) Let G_λ be a pseudorandom unitary in dimension 2^λ . Let $\mathbf{Q}_\lambda$ be the same as $\mathbf{Q}_{2^\lambda,2^\ell}$ except that the key distribution is $G_\lambda(k)$ on uniform input. Then $\{\mathbf{Q}_\lambda\}_\lambda$ is an efficient QECM. Let $\{\mathbf{A}_\lambda\}_\lambda$ be a telegraphing-distinguishing attack with collusion against $\{\mathbf{Q}_\lambda\}_\lambda$ such that the measurements $V_{m_0,m_1}^{\lambda,i}$ and P_x^λ are implemented efficiently. In Theorem 3, everything before Equation (1) does not depend on the key distribution. In particular, we can still find an upper bound independent of $p(b|x, U)$ since the key distribution need not look Haar-random to the second-stage adversary. Hence sampling $p(b|x, U)$ need not be efficient, which step allows for everlasting security. Also, replacing the Haar measure with the pseudorandom unitary, the upper bound in (1) will increase at most negligibly because the integrand depends polynomially on the unitary. More precisely, in this context,

$$D := \left| \int_K \sum_{\substack{x, \\ m^{(1)}, \dots, m^{(Q)}}} p(0|x, G_\lambda(k)) \text{Tr}[P_{x,m^{(1)}, \dots, m^{(Q)}} \right. \\ \times (G_\lambda(k)\sigma_{m_0^{(1)}}G_\lambda(k)^* \otimes \dots \otimes G_\lambda(k)\sigma_{m_0^{(Q)}}G_\lambda(k)^* \\ \left. - G_\lambda(k)\sigma_{m_1^{(1)}}G_\lambda(k)^* \otimes \dots \otimes G_\lambda(k)\sigma_{m_1^{(Q)}}G_\lambda(k)^*)] dk \right|$$

quantifies the advantage of $\mathbf{A}_\lambda$. Using the bounds of Theorem 3, this is bounded as

$$D \leq 2 \sum_{\substack{x, \\ m^{(1)}, \dots, m^{(Q)}}} \sqrt{\int_K C_{G_\lambda(k), x, m^{(1)}, \dots, m^{(Q)}}^2 dk}.$$

However, this upper bound can be efficiently approximated by a quantum algorithm. As such, by pseudorandomness,

$$D \leq 2 \sum_{\substack{x, \\ m^{(1)}, \dots, m^{(Q)}}} \sqrt{\int C_{U, x, m^{(1)}, \dots, m^{(Q)}}^2 dU} + \text{negl}(\lambda).$$

Therefore, we get the upper bound $t(Q_\lambda | A_\lambda) \leq \frac{1}{2} + 7 \frac{Q^\lambda}{\sqrt{2^\lambda}} + \text{negl}(\lambda) = \frac{1}{2} + \text{negl}(\lambda)$

□

5 Untelegraphable encryption as a limit of uncloneable encryption

In this section, we show that the cloning value of a QECM tends to the telegraphing value as the number of adversaries increases. To do so, we use information theoretic tools from work of Brandão [Bra08], where they were used to study QMA(2) proof systems.

Definition 8. The *entanglement entropy* of a pure state $\psi_{AB} = |\psi\rangle\langle\psi|_{AB}$ is $E(\psi) = S(\psi_A) = S(\psi_B)$.

The *entanglement of formation* of a state ρ_{AB} is $E_F(\rho) = \min_{\{p_i, |\psi_i\rangle\}_i} \sum_i p_i E(\psi_i)$, where the minimisation is over ensembles of pure states such that $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$.

The *Henderson-Vedral measure* of a state ρ_{AB} is

$$C^\leftarrow(\rho) = \max_{\{p_i, \rho_i\}} S(\rho_A) - \sum_i p_i S(\rho_i),$$

where the maximisation is over ensembles such that there exists a POVM $\{P_i\}_i$ on register B such that $p_i = \text{Tr}(P_i \rho_B)$ and $\rho_i = \frac{1}{p_i} \text{Tr}_B((I \otimes P_i) \rho_{AB})$.

The *convex roof of the Henderson-Vedral measure* of a state ρ_{AB} is

$$G^\leftarrow(\rho) = \min_{\{p_i, \rho_i\}} \sum_i p_i C^\leftarrow(\rho_i),$$

where the minimisation is over ensembles of states such that $\rho = \sum_i p_i \rho_i$.

Lemma 5 (Yang's monogamy inequality [Yan06]). *Let $A, B_1, \dots, B_N$ be registers and let $\rho_{AB_1 \dots B_N}$ be a quantum state. Then,*

$$E_F(\rho_{A; B_1 \dots B_N}) \geq \sum_{i=1}^N G^\leftarrow(\rho_{AB_i}).$$

Theorem 4. *Let $Q = (M, K, \pi, H, \{\sigma_m^k\}_{k,m})$ be a QECM, and suppose $\eta \geq \int_K \|\sigma_m^k\| d\pi(k)$ for all $m \in M$. Then, writing $d = \dim H$*

$$\mathbf{c}_{1 \rightarrow s}^N(Q) \leq \mathbf{c}_{1 \rightarrow 1}^N(Q | \mathcal{M}) + 3\eta d \left(\frac{\log d}{N^2 s} \right)^{1/3}.$$

From here, it is direct to see that $\lim_{s \rightarrow \infty} \mathbf{c}_{1 \rightarrow s}^N(Q) = \mathbf{c}_{1 \rightarrow 1}^N(Q | \mathcal{M})$. As a corollary, we also find that if $\|\sigma_m^k\| \leq \eta$ for all k, m , then $\mathbf{c}_{t \rightarrow s}^N(Q) \leq \mathbf{c}_{t \rightarrow 1}^N(Q | \mathcal{M}) + 3(\eta d)^t \left(\frac{t \log d}{N^2 s} \right)^{1/3}$. For example, in the case of $Q = Q_{r,n}$ we can take $\eta = \frac{1}{r}$, so

$$\mathbf{c}_{t \rightarrow s}^N(Q_{r,n}) \leq \mathbf{c}_{t \rightarrow 1}^N(Q_{r,n} | \mathcal{M}) + 3n^t \left(\frac{t \log d}{N^2 s} \right)^{1/3} \leq \frac{1}{N} + \frac{14t}{N\sqrt{r}} + 3n^t \left(\frac{t \log d}{N^2 s} \right)^{1/3}.$$

Proof. Let $\mathbf{A} = (M_0, \{B_i\}_i, \{P_m^{i,k}\}_{i,k,m}, \Phi)$ be a 1-to- s N -message cloning attack against $\mathbf{Q}$. First, we can write the cloning probability in an entanglement-based picture:

$$\begin{aligned} \mathfrak{c}_{1 \rightarrow s}^N(\mathbf{Q}|\mathbf{A}) &= \int_K \frac{1}{N} \sum_{m \in M_0} \text{Tr}[(P_m^{1,k} \otimes \cdots \otimes P_m^{s,k})\Phi(\sigma_m^k)]d\pi(k) \\ &= \int_K \frac{1}{N} \sum_{m \in M_0} \sum_{i,j=1}^d \text{Tr}[(P_m^{1,k} \otimes \cdots \otimes P_m^{s,k})\Phi(|i\rangle\langle i| \sigma_m^k |j\rangle\langle j|)]d\pi(k) \\ &= \int_K \frac{1}{N} \sum_{m \in M_0} \sum_{i,j=1}^d \text{Tr}[(\bar{\sigma}_m^k \otimes P_m^{1,k} \otimes \cdots \otimes P_m^{s,k})(|i\rangle\langle j| \otimes \Phi(|i\rangle\langle j|))]d\pi(k) \\ &= \int_K \frac{1}{N} \sum_{m \in M_0} \text{Tr}[(d\bar{\sigma}_m^k \otimes P_m^{1,k} \otimes \cdots \otimes P_m^{s,k})J(\Phi)]d\pi(k), \end{aligned}$$

where $J(\Phi)$ is the Choi state of Φ . By embedding into larger Hilbert spaces, we can assume $B_i = B$ for all i . Let

$$\rho_{AB^s} = \frac{1}{s!} \sum_{\tau \in \mathfrak{S}_s} (I \otimes V_B(\tau))J(\Phi)(I \otimes V_B(\tau))^* \otimes |\tau(1) \cdots \tau(s)\rangle\langle \tau(1) \cdots \tau(s)|$$

and let $P_m^k = \sum_i P_m^{i,k} \otimes |i\rangle\langle i|$. This achieves a labelled symmetrisation of the adversaries' registers, so

$$\mathfrak{c}_{1 \rightarrow s}^N(\mathbf{Q}|\mathbf{A}) = \int_K \frac{1}{N} \sum_{m \in M_0} \text{Tr}[(d\bar{\sigma}_m^k \otimes (P_m^k)^{\otimes s})\rho_{AB^s}]d\pi(k).$$

Now, we know that $E_F(\rho_{A;B^s}) \leq \log d$, where $d = \dim H$ and ρ is symmetric under permutations of the B registers, so $\log d \geq sG^\leftarrow(\rho_{AB})$. Let $\{p_i, \rho_i\}_i$ be the optimising ensemble in the definition of the convex roof of the Henderson-Vedral measure, so $\sum_i p_i C^\leftarrow(\rho_i) \leq \frac{\log d}{s}$. Fix $\varepsilon > 0$ and let $I = \{i \mid C^\leftarrow(\rho_i) \geq \varepsilon\}$. Then,

$$\frac{\log d}{s} \geq \sum_{i \in I} p_i \varepsilon.$$

Else, if $i \notin I$, $C^\leftarrow(\rho_i) \leq \varepsilon$. Consider the ensemble $\{p_{ikm}, \rho_{ikm}\}_m$ induced by the measurement P_m^k . We must have $S(\rho_{i,A}) - \sum_m p_{ikm} S(\rho_{ikm}) \leq \varepsilon$. This is equal to the divergence $D(\sum_m p_{ikm} \rho_{ikm} \otimes |m\rangle\langle m| \parallel \rho_{i,A} \otimes \sum_m p_{ikm} |m\rangle\langle m|)$, so Pinsker's inequality implies $\sum_m p_{ikm} \|\rho_{i,A} - \rho_{ikm}\|_{\text{Tr}} \leq \sqrt{\frac{\varepsilon}{2}}$. Now, let $\tau_{AB} = \sum_i p_i \rho_{i,A} \otimes \rho_{i,B}$, which is a Choi state of some channel Ψ , and let $\mathbf{B} = (M_0, B, \{P_m^k\}_{k,m}, \Psi)$ be a 1-to-1 N -message cloning attack against $\mathbf{Q}$. Since Ψ is an entanglement-breaking channel, $\mathfrak{c}_{1 \rightarrow 1}^N(\mathbf{Q}|\mathbf{B}) \leq \mathfrak{c}_{1 \rightarrow 1}^N(\mathbf{Q}|\mathcal{M})$. On the other hand, let $\tilde{\mathbf{A}} = (M_0, B, \{P_m^k\}, \Phi)$ be a 1-to-1 N -message cloning attack against $\mathbf{Q}$. By construction $\mathfrak{c}_{1 \rightarrow s}^N(\mathbf{Q}|\mathbf{A}) \leq \mathfrak{c}_{1 \rightarrow 1}^N(\mathbf{Q}|\tilde{\mathbf{A}})$, and we also have

$$\begin{aligned} &\left| \mathfrak{c}_{1 \rightarrow 1}^N(\mathbf{Q}|\tilde{\mathbf{A}}) - \mathfrak{c}_{1 \rightarrow 1}^N(\mathbf{Q}|\mathbf{B}) \right| \\ &\leq \int_K \frac{1}{N} \sum_{m \in M_0} \left| \text{Tr}[(d\bar{\sigma}_m^k \otimes P_m^k)\rho_{AB}] - \text{Tr}[(d\bar{\sigma}_m^k \otimes P_m^k)\tau_{AB}] \right| d\pi(k) \\ &\leq \int_K \frac{1}{N} \sum_{m \in M_0} \sum_i p_i \left| \text{Tr}[(d\bar{\sigma}_m^k \otimes P_m^k)\rho_i] - \text{Tr}[(d\bar{\sigma}_m^k \otimes P_m^k)(\rho_{i,A} \otimes \rho_{i,B})] \right| d\pi(k) \\ &= \int_K \frac{1}{N} \sum_i p_i \sum_{m \in M_0} p_{ikm} \left| \text{Tr}[d\bar{\sigma}_m^k \rho_{ikm}] - \text{Tr}[d\bar{\sigma}_m^k \rho_{i,A}] \right| d\pi(k) \end{aligned}$$

$$\begin{aligned}
&= \sum_i p_i \int_K \frac{d}{N} \sum_{m \in M_0} p_{ikm} \|\sigma_m^k\| \|\rho_{ikm} - \rho_{i,A}\|_{\text{Tr}} d\pi(k) \\
&\leq \sum_{i \in I} p_i (2\eta d) + \sum_{i \notin I} p_i \frac{\eta d}{N} \sqrt{\frac{\varepsilon}{2}} \\
&\leq \frac{2\eta d \log d}{s\varepsilon} + \frac{\eta d}{N} \sqrt{\frac{\varepsilon}{2}}.
\end{aligned}$$

Taking $\varepsilon = \left(4\sqrt{2} \frac{N \log d}{s}\right)^{2/3}$ gives the upper bound $3\eta d \left(\frac{\log d}{N^2 s}\right)^{1/3}$. Hence, we get that

$$c_{1 \rightarrow 1}^N(\mathbf{Q}|\mathcal{M}) \geq c_{1 \rightarrow 1}^N(\mathbf{Q}|\mathbf{B}) \geq c_{1 \rightarrow 1}^N(\mathbf{Q}|\tilde{\mathbf{A}}) - 3\eta d \left(\frac{\log d}{N^2 s}\right)^{1/3} \geq c_{1 \rightarrow s}^N(\mathbf{Q}|\mathbf{A}) - 3\eta d \left(\frac{\log d}{N^2 s}\right)^{1/3}.$$

Taking the supremum over attacks $\mathbf{A}$ gives the wanted result. $\square$

6 Lower bounds

In this section, we study lower bounds on telegraphing attacks against the Haar measure encryption.

6.1 Encryption of a bit

Consider the following telegraphing attack for the rank- r Haar-measure encryption of a bit: $\mathbf{A} = (B, \{P_m^k\}, \Phi)$, where $B = H = \mathbb{C}^{[2r]}$, Φ is measurement in the computational basis $\Phi(\rho) = \sum_{i=0}^{2r-1} |i\rangle\langle i| \rho |i\rangle\langle i|$, and let $P_b^U = \sum_{i \in G_{b,U}} |i\rangle\langle i|$, where $G_{0,U} = \{i \in [2r] \mid \langle i|U\sigma_0 U^*|i\rangle \geq \langle i|U\sigma_1 U^*|i\rangle\}$ and $G_{1,U} = [2r] \setminus G_{0,U}$.

Proposition 1. *The winning probability of the attack $\mathbf{A}$ above is*

$$c_{1 \rightarrow 1}(\mathbf{Q}_{r,2}|\mathbf{A}) = \frac{1}{2} + \frac{1}{2^{2r+1}} \binom{d}{r}.$$

Lemma 6. *Let $f : S^{n-1} \rightarrow \mathbb{R}$ be a function. Then*

$$\begin{aligned}
\int_{\mathbb{R}^n} f\left(\frac{v}{\|v\|}\right) e^{-\|v\|^2} d^n v &= \frac{1}{2} \Gamma(n/2) \int_{S^{n-1}} f(\Omega) d^{n-1} \Omega \\
\int_{\mathbb{R}^n} f\left(\frac{v}{\|v\|}\right) e^{-\|v\|^2} \|v\|^2 d^n v &= \frac{n}{4} \Gamma(n/2) \int_{S^{n-1}} f(\Omega) d^{n-1} \Omega,
\end{aligned}$$

where the integrations are with respect to the unnormalised Lebesgue measures.

Proof. We can express the integrations in spherical coordinates, that is the change of variables $v = r\Omega$, where $r \geq 0$ and Ω is a unit vector to get $d^n v = r^{n-1} dr d^{n-1} \Omega$. As such, we get in the first case that

$$\int_{\mathbb{R}^n} f\left(\frac{v}{\|v\|}\right) e^{-\|v\|^2} d^n v = \int_{S^{n-1}} \int_0^\infty f(\Omega) e^{-r^2} r^{n-1} dr d^{n-1} \Omega.$$

With the change of variables $t = r^2$, $\int_0^\infty e^{-r^2} r^{n-1} dr = \frac{1}{2} \int_0^\infty t^{n/2-1} e^{-t} dt = \frac{\Gamma(n/2)}{2}$, as wanted. The other case is similar. There,

$$\int_{\mathbb{R}^n} f\left(\frac{v}{\|v\|}\right) e^{-\|v\|^2} \|v\|^2 d^n v = \int_{S^{n-1}} \int_0^\infty f(\Omega) e^{-r^2} r^{n+1} dr d^{n-1} \Omega,$$

and with the same change of variables $\int_0^\infty e^{-r^2} r^{n+1} dr = \frac{1}{2} \int_0^\infty t^{n/2} e^{-t} dt = \frac{\Gamma(n/2+1)}{2} = \frac{n}{4} \Gamma(n/2)$. $\square$

Proof of Proposition 1. The winning probability of the strategy is

$$\begin{aligned} \mathbf{c}_{1 \rightarrow 1}(\mathbf{Q}_{r,2}|\mathbf{A}) &= \int \frac{1}{2} \sum_b \text{Tr} \left[\Phi(U_r^\dagger \Pi_b U_r^*) P_{b|U} \right] dU \\ &= \frac{1}{d} \int \sum_b \sum_{x \in G_{b,U}} \langle x | U \Pi_b U^* | x \rangle dU \\ &= \frac{1}{d} \sum_x \int \max_b \langle x | U \Pi_b U^* | x \rangle dU \\ &= \int \max_b \langle 0 | U \Pi_b U^* | 0 \rangle dU, \end{aligned}$$

by Haar invariance, where $d = 2r$. Now, $U^*|0\rangle$ is just a uniformly random pure state, so this is just the normalised integral over the set of pure states $\mathbf{c}_{1 \rightarrow 1}(\mathbf{Q}_{r,2}|\mathbf{A}) = \int \max_b \langle \psi | \Pi_b | \psi \rangle d\psi = \int \max_b \sum_{i=br}^{(b+1)r-1} |\psi_i|^2 d\psi$. This is now equivalent to the integral over the real $2d-1$ -sphere $\mathbf{c}_{1 \rightarrow 1}(\mathbf{Q}_{r,2}|\mathbf{A}) = \frac{\Gamma(d)}{2\pi^d} \int_{S^{2d-1}} \max_b \sum_{i=bd}^{(b+1)d-1} \Omega_i^2 d^{2d-1} \Omega$, since $\frac{2\pi^d}{\Gamma(d)}$ is the volume of the $2d-1$ -sphere. Using the lemma,

$$\begin{aligned} \mathbf{c}_{1 \rightarrow 1}(\mathbf{Q}_{r,2}|\mathbf{A}) &= \frac{\Gamma(d)}{2\pi^d} \frac{2}{d\Gamma(d)} \int_{\mathbb{R}^{2d}} \max_b \sum_{i=bd}^{(b+1)d-1} \frac{v_i^2}{\|v\|^2} e^{-\|v\|^2} \|v\|^2 d^{2d} v \\ &= \frac{1}{\pi^d d} \int_{\mathbb{R}^{2d}} \max_b \sum_{i=bd}^{(b+1)d-1} v_i^2 e^{-\|v\|^2} d^{2d} v \end{aligned}$$

Now, let the vectors $v^0 = (v_0, \dots, v_{d-1})$ and $v^1 = (v_d, \dots, v_{2d-1})$. Then, using a change of variables to spherical coordinates

$$\begin{aligned} \mathbf{c}_{1 \rightarrow 1}(\mathbf{Q}_{r,2}|\mathbf{A}) &= \frac{1}{\pi^d d} \int_{\mathbb{R}^d} \int_{\mathbb{R}^d} \max_b \|v^b\|^2 e^{-\|v^0\|^2 - \|v^1\|^2} d^d v^0 d^d v^1 \\ &= \frac{1}{\pi^d d} \int_{S^{d-1}} \int_0^\infty \int_{S^{d-1}} \int_0^\infty \max_b (r^b)^2 e^{-(r^0)^2 - (r^1)^2} (r^0)^{d-1} dr^0 d^{d-1} \Omega^0 (r^1)^{d-1} dr^1 d^{d-1} \Omega^1 \\ &= \frac{1}{\pi^d d} \left(\frac{2\pi^{d/2}}{\Gamma(d/2)} \right)^2 \int_0^\infty \int_0^\infty \max_b (r^b)^2 e^{-(r^0)^2 - (r^1)^2} (r^0)^{d-1} dr^0 (r^1)^{d-1} dr^1 \\ &= \frac{4}{d(d/2-1)!^2} \int_0^\infty \int_0^\infty \max_b (r^b)^2 e^{-(r^0)^2 - (r^1)^2} (r^0)^{d-1} (r^1)^{d-1} dr^0 dr^1. \end{aligned}$$

Next, take the change of variables $s = (r^0)^2$ and $t = (r^1)^2$. We find that

$$\begin{aligned} \mathbf{c}_{1 \rightarrow 1}(\mathbf{Q}_{r,2}|\mathbf{A}) &= \frac{1}{d(d/2-1)!^2} \int_0^\infty \int_0^\infty \max\{s, t\} e^{-s-t} s^{d/2-1} t^{d/2-1} ds dt \\ &= \frac{2}{d(d/2-1)!^2} \int_0^\infty \int_0^t e^{-s-t} s^{d/2-1} t^{d/2} ds dt. \end{aligned}$$

Now, $\int_0^t s^{d/2-1} e^{-s} ds = \gamma(d/2, t) = (d/2-1)! - (d/2-1)! e^{-t} \sum_{q=0}^{d/2-1} \frac{t^q}{q!}$, the lower incomplete

gamma function. Therefore,

$$\begin{aligned}
c_{1 \rightarrow 1}(\mathbb{Q}_{r,2}|\mathbb{A}) &= \frac{2}{d(d/2-1)!} \int_0^\infty t^{d/2} e^{-t} (d/2-1)! \left(1 - e^{-t} \sum_{q=0}^{d/2-1} \frac{t^q}{q!} \right) dt \\
&= \frac{1}{(d/2)!} \int_0^\infty t^{d/2} e^{-t} - \sum_{q=0}^{d/2-1} \frac{1}{q!} t^{d/2+q} e^{-2t} dt \\
&= \frac{1}{(d/2)!} \left((d/2)! - \sum_{q=0}^{d/2-1} \frac{1}{q!} \frac{(d/2+q)!}{2^{d/2+q+1}} \right) \\
&= 1 - \sum_{q=0}^{d/2-1} \binom{d/2+q}{q} \frac{1}{2^{q+d/2+1}}.
\end{aligned}$$

To simplify this formula, the Beta function is $B(a, b) = \int_0^1 t^{a-1} (1-t)^{b-1} dt$ and the regularised incomplete Beta function is $I_p(a, b) = \frac{1}{B(a, b)} \int_0^p t^{a-1} (1-t)^{b-1} dt$. $I_p(a, b)$ satisfies the relations $I_p(a, b) = I_{1-p}(b, a)$, and for integers m, n , $I_p(m, n-m+1) = \sum_{j=m}^n \binom{n}{j} p^j (1-p)^{n-j}$ and $I_p(m, n) = \sum_{j=m}^\infty \binom{n+j-1}{j} p^j (1-p)^n$ [DLMF, (8.17)]. Also, $I_p(1, b) = 1 - (1-p)^b$, giving that

$$\begin{aligned}
\sum_{q=0}^{d/2-1} \binom{d/2+q}{q} \frac{1}{2^{q+d/2+1}} &= \frac{1}{2^{d/2+1}} + I_{1/2}(1, d/2+1) - I_{1/2}(d/2, d/2+1) \\
&= 1 - I_{1/2}(d/2, d/2+1).
\end{aligned}$$

Hence,

$$c_{1 \rightarrow 1}(\mathbb{Q}_{r,2}|\mathbb{A}) = I_{1/2}(d/2, d/2+1) = \sum_{j=d/2}^d \binom{d}{j} \frac{1}{2^d}.$$

We have that $\sum_{j=0}^d \binom{d}{j} = 2^d$ and $\sum_{j=d/2}^d \binom{d}{j} = \sum_{j=0}^{d/2} \binom{d}{j}$. Hence,

$$2^d = \sum_{j=d/2}^d \binom{d}{j} + \sum_{j=1}^{d/2-1} \binom{d}{j} = 2 \sum_{j=d/2}^d \binom{d}{j} - \binom{d}{d/2},$$

and hence

$$c_{1 \rightarrow 1}(\mathbb{Q}_{r,2}|\mathbb{A}) = I_{1/2}(d/2, d/2+1) = \frac{1}{2^d} \left(2^{d-1} + \frac{1}{2} \binom{d}{d/2} \right) = \frac{1}{2} + \frac{1}{2^{d+1}} \binom{d}{d/2}. \quad \square$$

Corollary 2. $c_{1 \rightarrow 1}(\mathbb{Q}_{r,2}|\mathbb{A}) = \frac{1}{2} + \frac{1}{\sqrt{2\pi d}} + O\left(\frac{1}{d^{3/2}}\right)$.

Proof. By Stirling's approximation $\sqrt{2\pi n} \left(\frac{n}{e}\right)^n e^{\frac{1}{12n+1}} \leq n! \leq \sqrt{2\pi n} \left(\frac{n}{e}\right)^n e^{\frac{1}{12n}}$ [Rob55], so

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2} \leq \frac{\sqrt{4\pi n} \left(\frac{2n}{e}\right)^{2n} e^{\frac{1}{24n}}}{2\pi n \left(\frac{n}{e}\right)^{2n} e^{\frac{2}{12n+1}}} = \frac{4^n}{\sqrt{\pi n}} e^{\frac{1}{24n} - \frac{2}{12n+1}} \leq \frac{4^n}{\sqrt{\pi n}},$$

and

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2} \geq \frac{\sqrt{4\pi n} \left(\frac{2n}{e}\right)^{2n} e^{\frac{1}{24n+1}}}{2\pi n \left(\frac{n}{e}\right)^{2n} e^{\frac{2}{12n}}} = \frac{4^n}{\sqrt{\pi n}} e^{\frac{1}{24n+1} - \frac{2}{12n}} \geq \frac{4^n}{\sqrt{\pi n}} \left(1 - \frac{1}{6n}\right).$$

Therefore, $\frac{1}{2} + \frac{1}{\sqrt{2\pi d}} \left(1 - \frac{1}{3d}\right) \leq \mathbf{c}_{1 \rightarrow 1}(\mathbf{Q}_{r,2}|\mathbf{A}) \leq \frac{1}{2} + \frac{1}{\sqrt{2\pi d}}$, giving the wanted asymptotic formula. $\square$

6.2 Extension to more copies

To extend to t copies, we can apply the same strategy $\mathbf{A}$ of the previous section independently t times by measuring in a uniformly random basis for each copy. Then, the player chooses their output by choosing the most common bit, guessing uniformly random if 0 and 1 are equally common. Formally, $\mathbf{A}^{(t)} = (B^{(t)}, \{P_m^{(t),U}\}, \Phi^{(t)})$, where $B^{(t)} = B^{\otimes t}$, $\Phi^{(t)} = \Phi^{\otimes t}$, and $P_m^{(t),U} = \sum_{\text{MAJ}(m_1, \dots, m_t) = m} P_{m_1}^U \otimes \dots \otimes P_{m_t}^U$. Then, if p is the winning probability of one round,

$$\mathbf{c}_{t \rightarrow 1}(\mathbf{Q}_{r,2}|\mathbf{A}^{(t)}) = \begin{cases} \sum_{\ell=\frac{t+1}{2}}^t \binom{t}{\ell} p^\ell (1-p)^{t-\ell} & t \text{ odd} \\ \sum_{\ell=\frac{t}{2}+1}^t \binom{t}{\ell} p^\ell (1-p)^{t-\ell} + \frac{1}{2} \binom{t}{t/2} (p(1-p))^{t/2} & t \text{ even} \end{cases}$$

Lemma 7. *Let $p = \frac{1}{2} + \delta$. Suppose that $t \geq 4$ and $\delta \leq \frac{1}{2\sqrt{t-1}}$. Then,*

$$\frac{1}{2} + \frac{1}{3}\sqrt{t}\delta \leq \mathbf{c}_{t \rightarrow 1}(\mathbf{Q}_{r,2}|\mathbf{A}^{(t)}) \leq \frac{1}{2} + \sqrt{t}\delta.$$

Proof. First, consider the case where t is odd. We will again use properties of the regularised incomplete beta function [DLMF, (8.17)]. First, $\mathbf{c}_{t \rightarrow 1}(\mathbf{Q}_{r,2}|\mathbf{A}^{(t)}) = I_p(\frac{t+1}{2}, \frac{t+1}{2})$. Using the property $I_x(a, a) = \frac{1}{2} I_{4x(1-x)}(a, 1/2)$ for $x \in [0, 1/2]$, we find that

$$\begin{aligned} \mathbf{c}_{t \rightarrow 1}(\mathbf{Q}_{r,2}|\mathbf{A}^{(t)}) &= 1 - I_{1-p}(\frac{t+1}{2}, \frac{t+1}{2}) \\ &= 1 - \frac{1}{2} I_{4p(1-p)}(\frac{t+1}{2}, \frac{1}{2}) \\ &= \frac{1}{2} + \frac{1}{2} I_{1-4p(1-p)}(\frac{1}{2}, \frac{t+1}{2}). \end{aligned}$$

Now, note that $1 - 4p(1-p) = 4\delta^2$, so

$$\begin{aligned} \mathbf{c}_{t \rightarrow 1}(\mathbf{Q}_{r,2}|\mathbf{A}^{(t)}) &= \frac{1}{2} + \frac{1}{2} \frac{\Gamma(\frac{t+1}{2} + \frac{1}{2})}{\Gamma(\frac{t+1}{2})\Gamma(\frac{1}{2})} \int_0^{4\delta^2} t^{-\frac{1}{2}} (1-t)^{\frac{t-1}{2}} dt \\ &\geq \frac{1}{2} + \frac{1}{2} \frac{\frac{(t+1)!}{2^{t+1}(\frac{t+1}{2})!} \sqrt{\pi}}{\left(\frac{t-1}{2}\right)! \sqrt{\pi}} \int_0^{4\delta^2} t^{-\frac{1}{2}} (1-4\delta^2)^{\frac{t-1}{2}} dt \\ &= \frac{1}{2} + \frac{1}{2^{t+2}} \frac{t+1}{2} \binom{t+1}{\frac{t+1}{2}} (1-4\delta^2)^{\frac{t-1}{2}} 2\sqrt{4\delta^2} \\ &\geq \frac{1}{2} + (1-4\delta^2)^{\frac{t-1}{2}} (t+1) \frac{1}{\sqrt{\pi^{\frac{t+1}{2}}}} \left(1 - \frac{1}{3(t+1)}\right) \delta \\ &\geq \frac{1}{2} + \frac{1}{2} \sqrt{\frac{2}{\pi}} \frac{14}{15} \sqrt{t+1} \delta \\ &\geq \frac{1}{2} + \frac{1}{3} \sqrt{t} \delta. \end{aligned}$$

In the same way we can upper bound

$$\begin{aligned}
c_{t \rightarrow 1}(\mathbf{Q}_{r,2}|\mathbf{A}^{(t)}) &\leq \frac{1}{2} + \frac{1}{2^{t+2}} \frac{t+1}{2} \left(\frac{t+1}{2} \right) \int_0^{4\delta^2} t^{-\frac{1}{2}} dt \\
&\leq \frac{1}{2} + \frac{1}{2} \frac{t+1}{2} \frac{1}{\sqrt{\pi \frac{t+1}{2}}} 2\sqrt{4\delta^2} \\
&= \frac{1}{2} + \sqrt{\frac{2}{\pi}} \sqrt{t+1} \delta \\
&\leq \frac{1}{2} + \sqrt{t} \delta
\end{aligned}$$

Now, in the case that t is even,

$$\begin{aligned}
c_{t \rightarrow 1}(\mathbf{Q}_{r,2}|\mathbf{A}^{(t)}) &= I_p\left(\frac{t}{2} + 1, \frac{t}{2}\right) + \frac{1}{2} \binom{t}{t/2} (p(1-p))^{t/2} \\
&= I_p\left(\frac{t}{2}, \frac{t}{2}\right) - \frac{(p(1-p))^{t/2} \Gamma(t)}{\frac{t}{2} \Gamma(t/2)^2} + \frac{1}{2} \binom{t}{t/2} (p(1-p))^{t/2} \\
&= I_p\left(\frac{t}{2}, \frac{t}{2}\right) \\
&\in \left[\frac{1}{2} + \frac{1}{3} \sqrt{t} \delta, \frac{1}{2} + \sqrt{t} \delta \right],
\end{aligned}$$

by the above calculation with $t+1$ replaced by t . $\square$

6.3 Extension to more messages

We can use essentially the same strategy for the Haar-random encryption of longer messages. Let $\mathbf{A} = (B, \{P_m^U\}, \Phi)$ be the telegraphing attack against $\mathbf{Q}_{r,n}$ where $B = H = \mathbb{C}^{rn}$, Φ is measurement in the computational basis, and $P_m^U = \sum_{i \in G_{m,U}} |i\rangle\langle i|$ where $G_{m,U}$ is the set

$$\left\{ i \mid \forall m' < m. \langle i|U\sigma_m U^*|i\rangle > \langle i|U\sigma_{m'} U^*|i\rangle \wedge \forall m' > m. \langle i|U\sigma_m U^*|i\rangle \geq \langle i|U\sigma_{m'} U^*|i\rangle \right\}.$$

Proposition 2. *The winning probability for the strategy $\mathbf{A}$ above is*

$$c_{1 \rightarrow 1}(\mathbf{Q}_{r,n}|\mathbf{A}) = \sum_{q_1, \dots, q_{n-1}=r}^{\infty} \binom{q_1 + \dots + q_{n-1} + r}{q_1, \dots, q_{n-1}, r} n^{-(q_1 + \dots + q_{n-1} + r + 1)}.$$

Proof. The winning probability can be simplified to

$$\begin{aligned}
c_{1 \rightarrow 1}(\mathbf{Q}_{r,n}|\mathbf{A}) &= \int \frac{1}{n} \sum_m \text{Tr} \left[\Phi(U_r^\dagger \Pi_m U^*) P_m^U \right] dU \\
&= \frac{1}{d} \int \sum_m \sum_{i \in G_{m,U}} \langle i|U \Pi_m U^*|i\rangle dU \\
&= \int \max_m \langle 0|U \Pi_m U^*|0\rangle dU,
\end{aligned}$$

where $d = rn$ and $\Pi_m = |m\rangle\langle m| \otimes I_r = r\sigma_m$. As in the one-bit case, $U^*|0\rangle$ is just a uniformly random pure state, so the winning probability can be expressed as an integral

over the real $2d - 1$ -sphere:

$$\begin{aligned} \mathbf{c}_{1 \rightarrow 1}(\mathbb{Q}_{r,n}|\mathbf{A}) &= \frac{\Gamma(d)}{2\pi^d} \int_{S^{2d-1}} \max_m \sum_{j=2rm}^{2r(m+1)-1} \Omega_j^2 d^{2d-1} \Omega \\ &= \frac{1}{\pi^d d} \int_{\mathbb{R}^{2d}} \max_m \sum_{j=2rm}^{2r(m+1)-1} |v_j|^2 e^{-\|v\|^2} d^{2d} v. \end{aligned}$$

We rewrite the integration as an integration over n vectors $v^m = (v_{2rm+1}, \dots, v_{2r(m+1)})$, and then change to spherical coordinates:

$$\begin{aligned} \mathbf{c}_{1 \rightarrow 1}(\mathbb{Q}_{r,n}|\mathbf{A}) &= \frac{1}{\pi^d d} \int_{\mathbb{R}^{2r}} \cdots \int_{\mathbb{R}^{2r}} \max_m \|v^m\|^2 e^{-\sum_m \|v^m\|^2} dv^1 \cdots dv^n \\ &= \frac{1}{\pi^d d} \left(\frac{2\pi^r}{\Gamma(r)} \right)^m \int_0^\infty \cdots \int_0^\infty \max_m (r^m)^2 e^{-\sum_{m'} (r^{m'})^2} (r^1)^{2r-1} dr^1 \cdots (r^n)^{2r-1} dr^n \\ &= \frac{1}{d(r-1)!^m} \int_0^\infty \cdots \int_0^\infty \max_m t_m e^{-\sum_{m'} t_{m'} t_1^{r-1} dt_1 \cdots t_n^{r-1} dt_n}, \end{aligned}$$

via the change of variables $t_m = (r^m)^2$. Now, we can split the integration over n subsets $D_m = \{(t_1, \dots, t_n) \mid t_m \geq t_{m'} \forall m'\}$. By symmetry, we have that

$$\begin{aligned} \mathbf{c}_{1 \rightarrow 1}(\mathbb{Q}_{r,n}|\mathbf{A}) &= \frac{m}{d(r-1)!^m} \int_0^\infty \int_0^{t_n} \cdots \int_0^{t_n} t_n e^{-\sum_m t_m t_1^{r-1} dt_1 \cdots t_m^{r-1} dt_m} \\ &= \frac{1}{r!(r-1)!^{m-1}} \int_0^\infty \left(\int_0^t s^{r-1} e^{-s} ds \right)^{n-1} t^r e^{-t} dt. \end{aligned}$$

Again, $\int_0^t s^{r-1} e^{-s} ds = \gamma(r, t) = (r-1)! e^{-t} \sum_{q=r}^\infty \frac{t^q}{q!}$, so

$$\begin{aligned} \mathbf{c}_{1 \rightarrow 1}(\mathbb{Q}_{r,n}|\mathbf{A}) &= \frac{1}{r!} \int_0^\infty \left(e^{-t} \sum_{q=r}^\infty \frac{t^q}{q!} \right)^{n-1} t^r e^{-t} dt \\ &= \frac{1}{r!} \sum_{q_1, \dots, q_{n-1}=r}^\infty \frac{1}{q_1! \cdots q_{n-1}!} \int_0^\infty t^{q_1 + \dots + q_{n-1} + r} e^{-nt} dt \\ &= \sum_{q_1, \dots, q_{n-1}=r}^\infty \frac{(q_1 + \dots + q_{n-1} + r)!}{q_1! \cdots q_{n-1}! r!} n^{-(q_1 + \dots + q_{n-1} + r + 1)}. \quad \square \end{aligned}$$

6.4 Untelegraphable-indistinguishable security

We can study a telegraphing-distinguishing attack similar to the telegraphing attack of the previous section, which allows us to find a more concrete lower bound on the Haar measure encryption, with a closed-form expression. Consider the telegraphing-distinguishing attack $\mathbf{A} = (\{m_0, m_1\}, B, \{P_b^U\}, \Phi)$ against the Haar-measure encryption of n messages, where m_0, m_1 are arbitrary distinct messages, $B = H = \mathbb{C}^{[rn]}$, Φ is measurement in the computational basis, and $P_b^U = \sum_{i \in G_{b,U}} |i\rangle\langle i|$, where $G_{0,U} = \{i \mid \langle i|U\sigma_{m_0}U^*|i\rangle \geq \langle i|U\sigma_{m_1}U^*|i\rangle\}$ and $G_{1,U} = [2r] \setminus G_{0,U}$.

Proposition 3. *The telegraphing-distinguishing probability of the attack $\mathbf{A}$ above is*

$$\mathbf{c}_{1 \rightarrow 1}^2(\mathbb{Q}_{r,n}|\mathbf{A}) = \frac{1}{2} + \frac{1}{2^{2r+1}} \binom{2r}{r} = \frac{1}{2} + \frac{1}{2\sqrt{\pi r}} + O\left(\frac{1}{r^{3/2}}\right).$$

Proof. The proof begins identically to the one-bit case, but with $d/2$ replaced with r . First,

$$\begin{aligned}
\mathfrak{c}_{1 \rightarrow 1}(\mathbf{Q}_{r,n}|\mathbf{A}) &= \int \frac{1}{2} \sum_b \text{Tr} \left[\Phi(U_r^{\frac{1}{r}} \Pi_{m_b} U^*) P_b^U \right] dU \\
&= \frac{1}{2r} \int \sum_b \sum_{i \in G_{b,U}} \langle i | U \Pi_{m_b} U^* | i \rangle dU \\
&= \frac{n}{2} \int \max_b \langle 0 | U \Pi_{m_b} U^* | 0 \rangle dU \\
&= \frac{n\Gamma(d)}{4\pi^d} \int_{S^{2d-1}} \max_b \sum_{i=2br}^{2(b+1)r-1} \Omega_i^2 d^{2d-1} \Omega \\
&= \frac{1}{2r\pi^d} \int_{\mathbb{R}^{2d}} \max_b \sum_{i=2br}^{2(b+1)r-1} v_i^2 e^{-\|v\|^2} d^{2d} v.
\end{aligned}$$

Now, we rewrite the integration as an integration over 3 vectors $v^0 = (v_0, \dots, v_{2r-1})$, $v^1 = (v_{2r}, \dots, v_{4r-1})$, $v^2 = (v_{4r}, \dots, v_{6r-1})$, and then integrate v^2 :

$$\begin{aligned}
w_{dist}(\Phi, P) &= \frac{1}{2r\pi^d} \int_{\mathbb{R}^{2d-4r}} \int_{\mathbb{R}^{2r}} \int_{\mathbb{R}^{2r}} \max_{b=0,1} \|v^b\|^2 e^{-\|v^0\|^2 - \|v^1\|^2 - \|v^2\|^2} d^{2r} v^0 d^{2r} v^1 d^{2d-4r} v^2 \\
&= \frac{1}{2r\pi^d} \pi^{d-2r} \int_{\mathbb{R}^{2r}} \int_{\mathbb{R}^{2r}} \max_{b=0,1} \|v^b\|^2 e^{-\|v^0\|^2 - \|v^1\|^2} d^{2r} v^0 d^{2r} v^1.
\end{aligned}$$

This is equal to the winning probability of the one-bit game with $d = 2r$, giving the result by [Proposition 1](#) and [Corollary 2](#). $\square$

Corollary 3. *The telegraphing value of the rank- r Haar-measure encryption of n messages is lower-bounded as*

$$\mathfrak{c}_{1 \rightarrow 1}(\mathbf{Q}_{r,n}|\mathcal{M}) \geq \frac{1}{n} + \frac{1}{n\sqrt{\pi r}} + O\left(\frac{1}{nr^{3/2}}\right)$$

This follows by applying the argument of [[BL20](#), Theorem 12]. Essentially, to adapt the attack to a telegraphing attack, it proceeds in the same way and on output b from the telegraphing-distinguishing attack, the adversary outputs m_b . Then, if the original message is not m_0 or m_1 , the attack always loses; but if the original message was m_0 or m_1 , then the attack succeeds with the same probability as the telegraphing-distinguishing attack. As such, the new attack wins with probability $\frac{2}{n}$ times the telegraphing-distinguishing probability.

To finish this section, note we can combine this theorem with the results of [Section 3](#) to get upper and lower bounds on the telegraphing-distinguishing value that are tight in the order of r .

Corollary 4. *The t -copy telegraphing-distinguishing value of the rank- r Haar-measure encryption of n messages is bounded as*

$$\frac{1}{2} + \frac{1}{6} \sqrt{\frac{t}{\pi r}} + O\left(\frac{t^{1/2}}{r^{3/2}}\right) \leq \mathfrak{c}_{t \rightarrow 1}(\mathbf{Q}_{r,n}|\mathcal{M}) \leq \frac{1}{2} + \frac{7t}{\sqrt{r}}.$$

This corollary follows by combining [Proposition 3](#), [Lemma 7](#), and [Theorem 2](#)

7 Minimality of the Haar measure game

7.1 One-copy minimality

In this section, we extend the minimality result of [MST21] to the context of general cloning attacks, which will allow us to get minimality for telegraphing attacks as well as cloning attacks to an arbitrary number of receivers.

Theorem 5. *Let $Q = (M, K, \pi, H, \{\sigma_m^k\}_{k,m})$ be a correct QECM and let $\mathcal{F}$ be a class of channels that is closed under $\Phi \mapsto \Phi(V \cdot V^*)$ for every isometry V . Then for $r = \dim H - |M| + 1$ and $n = |M|$, $\mathfrak{c}_{1 \rightarrow s}^N(Q_{r,n}|\mathcal{F}) \leq \mathfrak{c}_{1 \rightarrow s}^N(Q|\mathcal{F})$.*

For example, the classes of all channels, of measurement channels, and of entanglement-breaking channels satisfy the conditions of the theorem.

Proof. We can assume without loss of generality that $M = [n]$. We proceed via a sequence of hybrid QECMs $Q^{(i)}$. First, we enlarge the dimension of the ciphertext. Let $V : H \rightarrow \mathbb{C}^{rn}$ be an isometry and let $\tilde{\sigma}_m^k = V \sigma_m^k V^*$. Since $\mathcal{F}$ is closed under preconjugation by isometries, it is clear $\mathfrak{c}_{1 \rightarrow s}^N(Q^{(1)}|\mathcal{F}) \leq \mathfrak{c}_{1 \rightarrow s}^N(Q|\mathcal{F})$.

Next, note that as $Q^{(1)}$ is correct, $\sum_m \text{rk}(\tilde{\sigma}_m^k) = \sum_m \text{rk}(\sigma_m^k) \leq \dim H$, so since $\text{rk}(\tilde{\sigma}_m^k) \geq 1$,

$$\text{rk}(\tilde{\sigma}_m^k) \leq \dim H - \sum_{m' \neq m} \text{rk}(\tilde{\sigma}_{m'}^k) \leq \dim H - (n - 1) = r.$$

Knowing this, we can write $\tilde{\sigma}_m^k = U_k \delta_m^k U_k^*$, where U_k is unitary and δ_m^k is diagonal with support contained in $\text{span}\{|i + r(m - 1)\rangle \mid i \in [r]\}$. Then, π induces a distribution π' on $\mathcal{U}(rn) \times D_{rn}^n$, where $D_{rn} \subseteq \mathcal{D}(\mathbb{C}^{rn})$ is the set of diagonal density matrices, as

$$\int_{\mathcal{U}(rn) \times D_{rn}^n} f(U, \delta_1, \dots, \delta_n) d\pi'(U, \delta_1, \dots, \delta_n) = \int_k f(U_k, \delta_1^k, \dots, \delta_n^k) d\pi(k).$$

Let μ be the marginal of π' on D_{rn}^n , let $\pi'_{\delta_1, \dots, \delta_n}$ be the conditional distribution of π' on $\mathcal{U}(rn)$ given $\delta_1, \dots, \delta_n$, and define $\sigma_m^{U, \delta_1, \dots, \delta_n} = U \delta_m U^*$. Define the QECM $Q^{(2)} = ([n], \mathcal{U}(rn) \times D_{rn}^n, \mu_{\text{Haar}} \times \mu, \mathbb{C}^{rn}, \{\sigma_m^{U, \delta_1, \dots, \delta_n}\}_{(U, \delta_1, \dots, \delta_n), m})$. This is again a correct QECM. Let $A = (M_0, \{B_i\}_i, \{P_m^{i, U, \delta_1, \dots, \delta_n}\}_{i, U, \delta_1, \dots, \delta_n, m}, \Phi)$ be a 1-to- s N -message cloning attack over $\mathcal{F}$ against $Q^{(2)}$. For each $U \in \mathcal{U}(rn)$, define the 1-to- s N -message cloning attack over $\mathcal{F}$ against $Q^{(1)}$ as $A_U = (M_0, \{B_i\}_i, \{P_m^{i, U U_k, \delta_1^k, \dots, \delta_n^k}\}_{i, k, m}, \Phi_U)$, where $\Phi_U(\rho) = \Phi(U \rho U^*)$. Using Haar invariance, denoting

$$C_{U, m, \delta_1, \dots, \delta_n} = \text{Tr}[(P_m^{1, U, \delta_1, \dots, \delta_n} \otimes \dots \otimes P_m^{s, U, \delta_1, \dots, \delta_n}) \Phi(U \delta_m U^*)],$$

we find that,

$$\begin{aligned} \mathfrak{c}_{1 \rightarrow s}^N(Q^{(2)}|A) &= \int_{\mathcal{U}(rn)} \int_{D_{rn}^n} \frac{1}{N} \sum_{m \in M_0} C_{U, m, \delta_1, \dots, \delta_n} d\mu(\delta_1, \dots, \delta_n) dU \\ &= \int_{\mathcal{U}(rn)} \int_{D_{rn}^n} \int_{\mathcal{U}(rn)} \frac{1}{N} \sum_{m \in M_0} C_{U, m, \delta_1, \dots, \delta_n} d\pi'_{\delta_1, \dots, \delta_n}(V) d\mu(\delta_1, \dots, \delta_n) dU \\ &= \int_{\mathcal{U}(rn)} \int_{\mathcal{U}(rn) \times D_{rn}^n} \frac{1}{N} \sum_{m \in M_0} C_{UV, m, \delta_1, \dots, \delta_n} d\pi'(V, \delta_1, \dots, \delta_n) dU \\ &= \int_{\mathcal{U}(rn)} \int_K \frac{1}{N} \sum_{m \in M_0} C_{U U_k, m, \delta_1^k, \dots, \delta_n^k} d\pi(k) dU \\ &= \int_{\mathcal{U}(rn)} \mathfrak{c}_{1 \rightarrow s}^N(Q^{(1)}|A_U) dU \leq \mathfrak{c}_{1 \rightarrow s}^N(Q^{(1)}|\mathcal{F}), \end{aligned}$$

so $\mathbf{c}_{1 \rightarrow s}^N(\mathbf{Q}^{(2)}|\mathcal{F}) \leq \mathbf{c}_{1 \rightarrow s}^N(\mathbf{Q}^{(1)}|\mathcal{F})$.

Now, for any permutation τ of $[rn]$, write V_τ for the action on $\mathbb{C}^{rn}$ given by $V_\tau|i\rangle = |\tau(i)\rangle$. Let $S \subseteq \mathfrak{S}_{rn}$ be the set of permutations that preserves the intervals $[r(m-1)+1, \dots, rm]$ for each $m \in [n]$. We have that $S \cong \mathfrak{S}_r^n$. Let v be the uniform distribution S and define the correct QECM $\mathbf{Q}^{(3)} = ([n], \mathcal{U}(rn) \times D_{rn}^n \times S, \mu_{Haar} \times \mu \times v, \mathbb{C}^{rn}, \{\sigma_m^{UV_\tau, \delta_1, \dots, \delta_n}\}_{(U, \delta_1, \dots, \delta_n, \tau), m})$. Let $\mathbf{A} = (M_0, \{B_i\}_i, \{P_m^{i, U, \delta_1, \dots, \delta_n, \tau}\}_{i, U, \delta_1, \dots, \delta_n, \tau, m}, \Phi)$ be a 1-to- s N -message cloning attack over $\mathcal{F}$ against $\mathbf{Q}^{(3)}$. Then for each $\tau \in S$, $\mathbf{A}_\tau = (M_0, \{B_i\}_i, \{P_m^{i, UV_\tau^*, \delta_1, \dots, \delta_n, \tau}\}_{i, U, \delta_1, \dots, \delta_n, m}, \Phi)$ is a 1-to- s N -message cloning attack over $\mathcal{F}$ against $\mathbf{Q}^{(2)}$, so, denoting similarly to above

$$C_{U, m, \delta_1, \dots, \delta_n, \tau} = \text{Tr}[(P_m^{1, U, \delta_1, \dots, \delta_n, \tau} \otimes \dots \otimes P_m^{s, U, \delta_1, \dots, \delta_n, \tau}) \Phi(UV_\tau \delta_m V_\tau^* U^*)],$$

$$\begin{aligned} \mathbf{c}_{1 \rightarrow s}^N(\mathbf{Q}^{(3)}|\mathbf{A}) &= \int_{\mathcal{U}(rn)} \int_{D_{rn}^n} \int_S \frac{1}{N} \sum_{m \in M_0} C_{U, m, \delta_1, \dots, \delta_n, \tau} dv(\tau) d\mu(\delta_1, \dots, \delta_n) dU \\ &= \int_S \int_{\mathcal{U}(rn)} \int_{D_{rn}^n} \frac{1}{N} \sum_{m \in M_0} C_{UV_\tau^*, m, \delta_1, \dots, \delta_n, \tau} d\mu(\delta_1, \dots, \delta_n) dU dv(\tau) \\ &= \int_S \mathbf{c}_{1 \rightarrow s}^N(\mathbf{Q}^{(2)}|\mathbf{A}_\tau) dv(\tau) \leq \mathbf{c}_{1 \rightarrow s}^N(\mathbf{Q}^{(2)}|\mathcal{F}), \end{aligned}$$

and hence $\mathbf{c}_{1 \rightarrow s}^N(\mathbf{Q}^{(3)}|\mathcal{F}) \leq \mathbf{c}_{1 \rightarrow s}^N(\mathbf{Q}^{(2)}|\mathcal{F})$.

To finish, note that if δ_m is supported on $\text{span}\{|r(m-1)+1\rangle, \dots, |rm\rangle\}$,

$$\int_S \sigma_m^{UV_\tau, \delta_1, \dots, \delta_n} dv(\tau) = U \int V_\tau \delta_m V_\tau^* dv(\tau) U^* = U \sigma_m U^*.$$

Now, let $\mathbf{A} = (M_0, \{B_i\}_i, \{P_m^{i, U}\}_{i, U, m}, \Phi)$ be a 1-to- s N -message cloning attack over $\mathcal{F}$ against $\mathbf{Q}_{r, n}$. Define the 1-to- s N -message cloning attack over $\mathcal{F}$ against $\mathbf{Q}^{(3)}$ $\mathbf{A}' = (M_0, \{B_i\}_i, \{P_m^{i, U}\}_{i, U, \delta_1, \dots, \delta_n, \tau, m}, \Phi)$. Then,

$$\begin{aligned} \mathbf{c}_{1 \rightarrow s}^N(\mathbf{Q}_{r, n}|\mathbf{A}) &= \int_{\mathcal{U}(rn)} \frac{1}{N} \sum_{m \in M_0} \text{Tr}[(P_m^{1, U} \otimes \dots \otimes P_m^{s, U}) \Phi(U \sigma_m U^*)] dU \\ &= \int_S \int_{D_{rn}^n} \int_{\mathcal{U}(rn)} \frac{1}{N} \sum_{m \in M_0} \text{Tr}[(P_m^{1, U} \otimes \dots \otimes P_m^{s, U}) \Phi(\sigma_m^{UV_\tau, \delta_1, \dots, \delta_n, \tau})] dU d\pi(\delta_1, \dots, \delta_n) dv(\tau) \\ &= \mathbf{c}_{1 \rightarrow s}^N(\mathbf{Q}^{(3)}|\mathbf{A}'). \end{aligned}$$

Taking suprema, we get that

$$\mathbf{c}_{1 \rightarrow s}^N(\mathbf{Q}_{r, n}|\mathcal{F}) \leq \mathbf{c}_{1 \rightarrow s}^N(\mathbf{Q}^{(3)}|\mathcal{F}) \leq \mathbf{c}_{1 \rightarrow s}^N(\mathbf{Q}^{(2)}|\mathcal{F}) \leq \mathbf{c}_{1 \rightarrow s}^N(\mathbf{Q}^{(1)}|\mathcal{F}) \leq \mathbf{c}_{1 \rightarrow s}^N(\mathbf{Q}|\mathcal{F}).$$

□

7.2 t -copy approximate minimality

In this section, we show that an approximate form of the minimality of the Haar-measure encryption also holds for attacks using multiple copies of the encrypted state.

Theorem 6. *Let $\mathbf{Q} = (M, K, \pi, H, \{\sigma_m^k\}_{k, m})$ be a correct QECM, let $\varepsilon > 0$ such that $\int \|\sigma_m^k\| d\pi(k) \leq \varepsilon$ for each m , and let $\mathcal{F}$ be a class of channels that is closed under $\Phi \mapsto \Phi(V \cdot V^*)$ for every isometry V . Then for $r = \dim H - |M| + 1$ and $n = |M|$, $\mathbf{c}_{t \rightarrow s}^N(\mathbf{Q}_{r, n}|\mathcal{F}) \leq \mathbf{c}_{t \rightarrow s}^N(\mathbf{Q}|\mathcal{F}) + 7t^2\varepsilon$.*

Proof. The proof proceeds similarly to the proof of [Theorem 5](#). First, we enlarge the dimension via an isometry $V : H \rightarrow \mathbb{C}^{rn}$. Let $\mathbf{Q}^{(1)} = ([n], K, \pi, \mathbb{C}^{rn}, \{\tilde{\sigma}_m^k\}_{k,n})$, where $\tilde{\sigma}_m^k = V\sigma_m^k V^*$. It is clear that $\mathbf{c}_{t \rightarrow s}^N(\mathbf{Q}^{(1)}|\mathcal{F}) = \mathbf{c}_{t \rightarrow s}^N(\mathbf{Q}|\mathcal{F})$. Next, noting that $\text{rk } \tilde{\sigma}_m^k \leq r$, there exist unitaries U_k and diagonal density matrices δ_m^k supported on $\text{span}\{|r(m-1)+1\rangle, \dots, |rm\rangle\}$ such that $\tilde{\sigma}_m^k = U_k \delta_m^k U_k^*$.

Then, π induces a distribution π' on $\mathcal{U}(rn) \times D_{rn}^n$, where $D_{rn} \subseteq \mathcal{D}(\mathbb{C}^{rn})$ is the set of diagonal density matrices, as

$$\int_{\mathcal{U}(rn) \times D_{rn}^n} f(U, \delta_1, \dots, \delta_n) d\pi'(U, \delta_1, \dots, \delta_n) = \int_k f(U_k, \delta_1^k, \dots, \delta_n^k) d\pi(k).$$

Let μ be the marginal of π' on D_{rn}^n , let $\pi'_{\delta_1, \dots, \delta_n}$ be the conditional distribution of π' on $\mathcal{U}(rn)$ given $\delta_1, \dots, \delta_n$, and define $\sigma_m^{U, \delta_1, \dots, \delta_n} = U \delta_m U^*$. Define the QECM $\mathbf{Q}^{(2)} = ([n], \mathcal{U}(rn) \times D_{rn}^n, \mu_{Haar} \times \mu, \mathbb{C}^{rn}, \{\sigma_m^{U, \delta_1, \dots, \delta_n}\}_{(U, \delta_1, \dots, \delta_n), m})$. This is again a correct QECM. Let $\mathbf{A} = (M_0, \{B_i\}_i, \{P_m^{i, U, \delta_1, \dots, \delta_n}\}_{i, U, \delta_1, \dots, \delta_n, m}, \Phi)$ be a t -to- s N -message cloning attack over $\mathcal{F}$ against $\mathbf{Q}^{(2)}$. For each $U \in \mathcal{U}(rn)$, define the 1-to- s N -message cloning attack over $\mathcal{F}$ against $\mathbf{Q}^{(1)}$ as $\mathbf{A}_U = (M_0, \{B_i\}_i, \{P_m^{i, U U_k, \delta_1^k, \dots, \delta_n^k}\}_{i, k, m}, \Phi_U)$, where $\Phi_U(\rho) = \Phi(U^{\otimes t} \rho (U^*)^{\otimes t})$. Using Haar invariance, denoting

$$C_{U, m, \delta_1, \dots, \delta_n} = \text{Tr}[(P_m^{1, U, \delta_1, \dots, \delta_n} \otimes \dots \otimes P_m^{s, U, \delta_1, \dots, \delta_n}) \Phi((U \delta_m U^*)^{\otimes t})],$$

we find that

$$\begin{aligned} \mathbf{c}_{t \rightarrow s}^N(\mathbf{Q}^{(2)}|\mathbf{A}) &= \int_{\mathcal{U}(rn)} \int_{D_{rn}^n} \frac{1}{N} \sum_{m \in M_0} C_{U, m, \delta_1, \dots, \delta_n} d\mu(\delta_1, \dots, \delta_n) dU \\ &= \int_{\mathcal{U}(rn)} \int_{D_{rn}^n} \int_{\mathcal{U}(rn)} \frac{1}{N} \sum_{m \in M_0} C_{U, m, \delta_1, \dots, \delta_n} d\pi'_{\delta_1, \dots, \delta_n}(V) d\mu(\delta_1, \dots, \delta_n) dU \\ &= \int_{\mathcal{U}(rn)} \int_{\mathcal{U}(rn) \times D_{rn}^n} \frac{1}{N} \sum_{m \in M_0} C_{UV, m, \delta_1, \dots, \delta_n} d\pi'(V, \delta_1, \dots, \delta_n) dU \\ &= \int_{\mathcal{U}(rn)} \int_K \frac{1}{N} \sum_{m \in M_0} C_{U U_k, m, \delta_1^k, \dots, \delta_n^k} d\pi(k) dU \\ &= \int_{\mathcal{U}(rn)} \mathbf{c}_{t \rightarrow s}^N(\mathbf{Q}^{(1)}|\mathbf{A}_U) dU \leq \mathbf{c}_{t \rightarrow s}^N(\mathbf{Q}^{(1)}|\mathcal{F}), \end{aligned}$$

so $\mathbf{c}_{t \rightarrow s}^N(\mathbf{Q}^{(2)}|\mathcal{F}) \leq \mathbf{c}_{t \rightarrow s}^N(\mathbf{Q}^{(1)}|\mathcal{F})$.

Next, let $G \cong \mathcal{U}(r)^n$ be the subgroup of $\mathcal{U}(rn)$ that preserves the σ_m under conjugation. Define the correct QECM

$$\mathbf{Q}^{(3)} = ([n], \mathcal{U}(rn) \times D_{rn}^n \times G, \mu_{Haar} \times \mu \times \mu_{Haar}, \mathbb{C}^{rn}, \{\sigma_m^{UV, \delta_1, \dots, \delta_n}\}_{(U, \delta_1, \dots, \delta_n, V), m}).$$

Let $\mathbf{A} = (M_0, \{B_i\}_i, \{P_m^{i, U, \delta_1, \dots, \delta_n, V}\}_{i, U, \delta_1, \dots, \delta_n, V, m}, \Phi)$ be a t -to- s N -message cloning attack over $\mathcal{F}$ against $\mathbf{Q}^{(3)}$. Then for $V \in G$, $\mathbf{A}_V = (M_0, \{B_i\}_i, \{P_m^{i, UV^*, \delta_1, \dots, \delta_n, V}\}_{i, U, \delta_1, \dots, \delta_n, V, m}, \Phi)$ is a t -to- s N -message cloning attack over $\mathcal{F}$ against $\mathbf{Q}^{(2)}$, so denoting

$$C_{U, m, \delta_1, \dots, \delta_n, V} = \text{Tr}[(P_m^{1, U, \delta_1, \dots, \delta_n, V} \otimes \dots \otimes P_m^{s, U, \delta_1, \dots, \delta_n, V}) \Phi((UV \delta_m V^* U^*)^{\otimes t})]$$

$$\begin{aligned} \mathbf{c}_{t \rightarrow s}^N(\mathbf{Q}^{(3)}|\mathbf{A}) &= \int_{\mathcal{U}(rn)} \int_{D_{rn}^n} \int_G \frac{1}{N} \sum_{m \in M_0} C_{U, m, \delta_1, \dots, \delta_n, V} dV d\mu(\delta_1, \dots, \delta_n) dU \\ &= \int_G \int_{\mathcal{U}(rn)} \int_{D_{rn}^n} \frac{1}{N} \sum_{m \in M_0} C_{UV^*, m, \delta_1, \dots, \delta_n, V} d\mu(\delta_1, \dots, \delta_n) dU dV \\ &= \int_G \mathbf{c}_{t \rightarrow s}^N(\mathbf{Q}^{(2)}|\mathbf{A}_V) dV \leq \mathbf{c}_{t \rightarrow s}^N(\mathbf{Q}^{(2)}|\mathcal{F}), \end{aligned}$$

and hence $\mathbf{c}_{t \rightarrow s}^N(\mathbf{Q}^{(3)}|\mathcal{F}) \leq \mathbf{c}_{t \rightarrow s}^N(\mathbf{Q}^{(2)}|\mathcal{F})$.

To finish, we make use of [Lemma 3](#). Fix m , and let $T : \mathbb{C}^r \rightarrow \mathbb{C}^{rn}$ be the isometry $T|i\rangle = |i + r(m-1)\rangle$. Then, for $(\delta_1, \dots, \delta_n)$ in the support of μ , δ_m is supported on the image of T . Hence we have that

$$(T^*)^{\otimes t} \int_G (V\delta_m V^*)^{\otimes t} dV T^{\otimes t} = \int_{\mathcal{U}(r)} U^{\otimes t} (T^* \delta_m T)^{\otimes t} U^{\otimes t} dU.$$

Let $\rho = T^* \delta_m T$. By [Lemma 3](#), we have that

$$\left\| \int_{\mathcal{U}(r)} (U \rho U^*)^{\otimes t} dU - \frac{I}{r^t} \right\|_{\text{Tr}} \leq 7t^2 \|\rho\|.$$

Extending outside the image of T (where all the states are 0), we find that

$$\left\| \int_G (V\delta_m V^*)^{\otimes t} dV - \sigma_m^{\otimes t} \right\|_{\text{Tr}} \leq 7t^2 \|\delta_m\|.$$

Now, let $\mathbf{A} = (M_0, \{B_i\}_i, \{P_m^{i,U}\}_{i,U,m}, \Phi)$ be a t -to- s N -message cloning attack over $\mathcal{F}$ against $\mathbf{Q}_{r,n}$. Define the t -to- s N -message cloning attack over $\mathcal{F}$ against $\mathbf{Q}^{(3)}$ $\mathbf{A}' = (M_0, \{B_i\}_i, \{P_m^{i,U}\}_{i,U,\delta_1,\dots,\delta_n,V,m}, \Phi)$. Then,

$$\begin{aligned} \mathbf{c}_{t \rightarrow s}^N(\mathbf{Q}_{r,n}|\mathbf{A}) &= \int_{\mathcal{U}(rn)} \frac{1}{N} \sum_{m \in M_0} \text{Tr}[(P_m^{1,U} \otimes \dots \otimes P_m^{s,U}) \Phi((U\sigma_m U^*)^{\otimes t})] dU \\ &= \int_G \int_{D_{rn}^n} \int_{\mathcal{U}(rn)} \frac{1}{N} \sum_{m \in M_0} \text{Tr}[(P_m^{1,U} \otimes \dots \otimes P_m^{s,U}) \Phi(\sigma_m^{UV,\delta_1,\dots,\delta_n,V})] dU d\mu(\delta_1, \dots, \delta_n) dV \\ &\quad + \int_{D_{rn}^n} \frac{1}{N} \sum_{m \in M_0} 7t^2 \|\delta_m\| d\mu(\delta_1, \dots, \delta_n) \\ &= \mathbf{c}_{t \rightarrow s}^N(\mathbf{Q}^{(3)}|\mathbf{A}') + 7t^2 \varepsilon. \end{aligned}$$

Taking suprema, we get that $\mathbf{c}_{t \rightarrow s}^N(\mathbf{Q}_{r,n}|\mathcal{F}) \leq \mathbf{c}_{t \rightarrow s}^N(\mathbf{Q}^{(3)}|\mathcal{F}) + 7t^2 \varepsilon$. $\square$

Using [Theorem 6](#) along with Corollary 3.3 from [\[MST21\]](#), we can get an approximate version of the minimality for t -to- $t+1$ -copy security uncloneable encryption.

Corollary 5. *Let $\mathbf{Q} = (M, K, \pi, H, \{\sigma_m^k\}_{k,m})$ be a correct QECCM and write $r = \dim H - |M| + 1$ and $n = |M|$. Then, if $\mathbf{c}_{t \rightarrow t+1}^N(\mathbf{Q}_{r,n}) = \frac{1}{N} + \delta$, then $\mathbf{c}_{t \rightarrow t+1}^N(\mathbf{Q}) \geq \frac{1}{N} + \frac{\delta}{56Nt^2+1}$.*

Proof. Let $\varepsilon = \max_{m \in M} \int_K \|\sigma_m^k\| d\pi(k)$. Then, by Corollary 3.3 from [\[MST21\]](#), $\mathbf{c}_{1 \rightarrow 2}^2(\mathbf{Q}) \geq \frac{1}{2} + \frac{\varepsilon}{16}$. Now, using [\[BL20, Theorem 12\]](#) as in [Corollary 3](#), $\mathbf{c}_{1 \rightarrow 2}^N(\mathbf{Q}) \geq \frac{2}{N} \mathbf{c}_{1 \rightarrow 2}^2(\mathbf{Q}) \geq \frac{1}{N} + \frac{\varepsilon}{8N}$. This also provides a lower bound for $\mathbf{c}_{t \rightarrow t+1}^N(\mathbf{Q})$ by using the strategy where the first $t-1$ players get a copy of the ciphertext state and win perfectly, and the final two players play with the 1-to-2 cloning attack. Hence, if $\varepsilon \geq \frac{\delta}{7t^2 + \frac{1}{8N}}$, then $\mathbf{c}_{t \rightarrow t+1}^N(\mathbf{Q}) \geq \frac{1}{N} + \frac{\delta}{56Nt^2+1}$.

On the other hand, we know by [Theorem 6](#) that $\mathbf{c}_{t \rightarrow t+1}^N(\mathbf{Q}) \geq \frac{1}{N} + \delta - 7t^2 \varepsilon$. Hence, we get the other case: if $\varepsilon \leq \frac{\delta}{7t^2 + \frac{1}{8N}}$, then $\mathbf{c}_{t \rightarrow t+1}^N(\mathbf{Q}) \geq \frac{1}{N} + \frac{\delta}{56Nt^2+1}$. $\square$

7.3 Implications of minimality

We can put together the results of this section with the lower bounds of [Section 6](#) to get lower bounds that hold for any QECCM.

Corollary 6. *Let $\mathcal{Q} = (M, K, \mu, H, \{\sigma_m^k\}_{k,m})$ be a correct QECCM. Then, writing $d = \dim H$,*

$$\begin{aligned} c_{1 \rightarrow 1}^N(\mathcal{Q}|\mathcal{M}) &\geq \frac{1}{N} + \frac{1}{N\sqrt{\pi(d-|M|+1)}} + O\left(\frac{1}{N(d-|M|+1)^{3/2}}\right) \\ c_{1 \rightarrow 2}^N(\mathcal{Q}) &\geq \frac{1}{N} + \frac{1}{N\sqrt{\pi(d-|M|+1)}} + O\left(\frac{1}{N(d-|M|+1)^{3/2}}\right) \\ c_{t \rightarrow t+1}^N(\mathcal{Q}) &\geq \frac{1}{N} + \frac{1}{57N^2\sqrt{\pi t^3(d-|M|+1)}} + O\left(\frac{1}{N^2(t(d-|M|+1))^{3/2}}\right). \end{aligned}$$

In particular, previous work has shown that the cloning-distinguishing value is lower-bounded as $c_{1 \rightarrow 2}^2(\mathcal{Q}) = \frac{1}{2} + \Omega\left(\frac{1}{d}\right)$ [MST21], which we strengthen to $c_{1 \rightarrow 2}^2(\mathcal{Q}) = \frac{1}{2} + \Omega\left(\frac{1}{\sqrt{d}}\right)$.

Acknowledgements

The authors would like to thank Archishna Bhattacharyya and Arthur Mehta for helpful discussions. We acknowledge the support of the Natural Sciences and Engineering Research Council of Canada (NSERC)(ALLRP-578455-2022), the Air Force Office of Scientific Research under award number FA9550-20-1-0375 and of the Canada Research Chairs Program (CRC-2023-00173).

References

- [AB24] Prabhanjan Ananth and Amit Behera. A modular approach to unclonable cryptography. In *Advances in Cryptology — CRYPTO 2024*, volume 7, pages 3–37, 2024. [doi:10.1007/978-3-031-68394-7_1](https://doi.org/10.1007/978-3-031-68394-7_1).
- [AK21] Prabhanjan Ananth and Fatih Kaleoglu. Unclonable encryption, revisited. In *Theory of Cryptography (TCC 2021)*, volume 1, pages 299–329, 2021. [doi:10.1007/978-3-030-90459-3_11](https://doi.org/10.1007/978-3-030-90459-3_11).
- [AKL⁺22] Prabhanjan Ananth, Fatih Kaleoglu, Xingjian Li, Qipeng Liu, and Mark Zhandry. On the feasibility of unclonable encryption, and more. In *Advances in Cryptology — CRYPTO 2022*, volume 2, pages 212–241, 2022. [doi:10.1007/978-3-031-15979-4_8](https://doi.org/10.1007/978-3-031-15979-4_8).
- [AKY25] Prabhanjan Ananth, Fatih Kaleoglu, and Henry Yuen. Simultaneous Haar indistinguishability with applications to unclonable cryptography. In *16th Innovations in Theoretical Computer Science Conference (ITCS 2025)*, pages 7:1–7:23, 2025. [doi:10.4230/LIPIcs.ITCS.2025.7](https://doi.org/10.4230/LIPIcs.ITCS.2025.7).
- [ALL⁺21] Scott Aaronson, Jiahui Liu, Qipeng Liu, Mark Zhandry, and Ruizhe Zhang. New approaches for quantum copy-protection. In *Advances in Cryptology — CRYPTO 2021*, volume 1, pages 526–555, 2021. [doi:10.1007/978-3-030-84242-0_19](https://doi.org/10.1007/978-3-030-84242-0_19).
- [ALP21] Prabhanjan Ananth and Rolando L La Placa. Secure software leasing. In *Advances in Cryptology — EUROCRYPT 2021*, volume 2, pages 501–530, 2021. [doi:10.1007/978-3-030-77886-6_17](https://doi.org/10.1007/978-3-030-77886-6_17).
- [BBC⁺26] Pierre Botteron, Anne Broadbent, Eric Culf, Ion Nechita, Clément Pellegrini, and Denis Rochette. Towards unconditional uncloneable encryption. *Quantum*, 10:2157, 2026. [doi:10.22331/q-2026-07-08-2157](https://doi.org/10.22331/q-2026-07-08-2157).

- [BC26] Archishna Bhattacharyya and Eric Culf. Uncloneable encryption from decoupling. *Nature Physics*, 22:315–318, 2026. doi:[10.1038/s41567-025-03154-7](https://doi.org/10.1038/s41567-025-03154-7).
- [BJL⁺21] Anne Broadbent, Stacey Jeffery, Sébastien Lord, Supartha Podder, and Aarthi Sundaram. Secure software leasing without assumptions. In *Theory of Cryptography (TCC 2021)*, volume 1, pages 90–120, 2021. doi:[10.1007/978-3-030-90459-3_4](https://doi.org/10.1007/978-3-030-90459-3_4).
- [BL20] Anne Broadbent and Sébastien Lord. Uncloneable quantum encryption via oracles. In *15th Conference on the Theory of Quantum Computation, Communication, and Cryptography (TQC 2020)*, pages 4:1–4:22, 2020. doi:[10.4230/LIPIcs.TQC.2020.4](https://doi.org/10.4230/LIPIcs.TQC.2020.4).
- [Bra08] Fernando G. S. L. Brandão. Entanglement theory and the quantum simulation of many-body physics. E-print arXiv:0810.0026 [quant-ph], 2008.
- [ÇG24a] Alper Çakan and Vipul Goyal. Unbounded leakage-resilient encryption and signatures. Cryptology ePrint Archive, Report 2024/1876, 2024.
- [ÇG24b] Alper Çakan and Vipul Goyal. Unclonable cryptography with unbounded collusions and impossibility of hyperefficient shadow tomography. In *Theory of Cryptography (TCC 2024)*, volume 3, pages 225–256, 2024. doi:[10.1007/978-3-031-78020-2_8](https://doi.org/10.1007/978-3-031-78020-2_8).
- [CG24c] Andrea Coladangelo and Sam Gunn. How to use quantum indistinguishability obfuscation. In *STOC 2024: Proceedings of the 56th ACM Symposium on Theory of Computing*, pages 1003–1008, 2024. doi:[10.1145/3618260.3649779](https://doi.org/10.1145/3618260.3649779).
- [CKNY26] Jeffrey Champion, Fuyuki Kitagawa, Ryo Nishimaki, and Takashi Yamakawa. Untelegraphable encryption and its applications. In *Theory of Cryptography — TCC 2025*, pages 3–35, 2026. doi:[10.1007/978-3-032-12296-4_1](https://doi.org/10.1007/978-3-032-12296-4_1).
- [CLLZ21] Andrea Coladangelo, Jiahui Liu, Qipeng Liu, and Mark Zhandry. Hidden cosets and applications to unclonable cryptography. In *Advances in Cryptology — CRYPTO 2021*, volume 1, pages 556–584, 2021. doi:[10.1007/978-3-030-84242-0_20](https://doi.org/10.1007/978-3-030-84242-0_20).
- [CMP24] Andrea Coladangelo, Christian Majenz, and Alexander Poremba. Quantum copy-protection of compute-and-compare programs in the quantum random oracle model. *Quantum*, 8:1330, 2024. doi:[10.22331/q-2024-05-02-1330](https://doi.org/10.22331/q-2024-05-02-1330).
- [DFSS05] Ivan Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Cryptography in the bounded quantum-storage model. In *46th Annual Symposium on Foundations of Computer Science (FOCS 2005)*, pages 449–458, 2005. doi:[10.1109/SFCS.2005.30](https://doi.org/10.1109/SFCS.2005.30).
- [Die82] Dennis Dieks. Communication by EPR devices. *Physics Letters A*, 92(6):271–272, 1982. doi:[10.1016/0375-9601\(82\)90084-6](https://doi.org/10.1016/0375-9601(82)90084-6).
- [DLMF] NIST digital library of mathematical functions. Release 1.2.4 of 2025-03-15. F. W. J. Olver, A. B. Olde Daalhuis, D. W. Lozier, B. I. Schneider, R. F. Boisvert, C. W. Clark, B. R. Miller, B. V. Saunders, H. S. Cohl, and M. A. McClain, eds. URL: <https://dlmf.nist.gov/>.
- [GZ20] Marios Georgiou and Mark Zhandry. Unclonable decryption keys. Cryptology ePrint Archive, Report 2020/877, 2020. URL: <http://eprint.iacr.org/2020/877>.

- [Haf22] Jonas Haferkamp. Random quantum circuits are approximate unitary t -designs in depth $O\left(nt^{5+o(1)}\right)$. *Quantum*, 6:795, 2022. doi:[10.22331/q-2022-09-08-795](https://doi.org/10.22331/q-2022-09-08-795).
- [JK24] Ruta Jawale and Dakshita Khurana. Unclonable non-interactive zero-knowledge. In *Advances in Cryptology — ASIACRYPT 2024*, volume 9, pages 94–128, 2024. doi:[10.1007/978-981-96-0947-5_4](https://doi.org/10.1007/978-981-96-0947-5_4).
- [KN23] Fuyuki Kitagawa and Ryo Nishimaki. One-out-of-many unclonable cryptography: definitions, constructions, and more. In *Theory of Cryptography (TCC 2023)*, volume 4, pages 246–275, 2023. doi:[10.1007/978-3-031-48624-1_10](https://doi.org/10.1007/978-3-031-48624-1_10).
- [KNY21] Fuyuki Kitagawa, Ryo Nishimaki, and Takashi Yamakawa. Secure software leasing from standard assumptions. In *Theory of Cryptography — TCC 2021*, pages 31–61, 2021. doi:[10.1007/978-3-030-90459-3_2](https://doi.org/10.1007/978-3-030-90459-3_2).
- [KT25] Srijita Kundu and Ernest Y.-Z. Tan. Device-independent uncloneable encryption. *Quantum*, 9:1582, 2025. doi:[10.22331/q-2025-01-08-1582](https://doi.org/10.22331/q-2025-01-08-1582).
- [LLQZ22] Jiahui Liu, Qipeng Liu, Luowen Qian, and Mark Zhandry. Collusion resistant copy-protection for watermarkable functionalities. In *Theory of Cryptography (TCC 2022)*, volume 1, pages 294–323, 2022. doi:[10.1007/978-3-031-22318-1_11](https://doi.org/10.1007/978-3-031-22318-1_11).
- [Mel24] Antonio Anna Mele. Introduction to Haar measure tools in quantum information: A beginner’s tutorial. *Quantum*, 8:1340, 2024. doi:[10.22331/q-2024-05-08-1340](https://doi.org/10.22331/q-2024-05-08-1340).
- [MM24] Arthur Mehta and Anne Müller. Unclonable functional encryption. E-print arXiv:2410.06029 [quant-ph], 2024.
- [MPSY24] Tony Metger, Alexander Poremba, Makrand Sinha, and Henry Yuen. Simple constructions of linear-depth t -designs and pseudorandom unitaries. In *2024 65th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2024)*, pages 485–492, 2024. doi:[10.1109/FOCS61266.2024.00038](https://doi.org/10.1109/FOCS61266.2024.00038).
- [MST21] Christian Majenz, Christian Schaffner, and Mehrdad Tahmasbi. Limitations on uncloneable encryption and simultaneous one-way-to-hiding. E-print arXiv:2103.14510 [quant-ph], 2021.
- [NZ24] Barak Nehoran and Mark Zhandry. A computational separation between quantum no-cloning and no-telegraphing. In *15th Innovations in Theoretical Computer Science Conference (ITCS 2024)*, pages 82:1–82:23, 2024. doi:[10.4230/LIPIcs.ITCS.2024.82](https://doi.org/10.4230/LIPIcs.ITCS.2024.82).
- [PRV26] Alexander Poremba, Seyoon Ragavan, and Vinod Vaikuntanathan. Cloning games, black holes and cryptography. In *17th Innovations in Theoretical Computer Science Conference (ITCS 2026)*, pages 109:1–109:21, 2026. doi:[10.4230/LIPIcs.ITCS.2026.109](https://doi.org/10.4230/LIPIcs.ITCS.2026.109).
- [Rob55] Herbert Robbins. A remark on Stirling’s formula. *The American Mathematical Monthly*, 62(1):26–29, 1955. doi:[10.2307/2308012](https://doi.org/10.2307/2308012).
- [SHH25] Thomas Schuster, Jonas Haferkamp, and Hsin-Yuan Huang. Random unitaries in extremely low depth. *Science*, 389(6755):92–96, 2025. doi:[10.1126/science.adv8590](https://doi.org/10.1126/science.adv8590).

-
- [SW22] Or Sattath and Shai Wyborski. Uncloneable decryptors from quantum copy-protection. E-print arXiv:2203.05866 [quant-ph], 2022.
- [Wer98] R. F. Werner. Optimal cloning of pure states. *Physical Review A*, 58(3):1827, 1998. [doi:10.1103/PhysRevA.58.1827](https://doi.org/10.1103/PhysRevA.58.1827).
- [WST08] Stephanie Wehner, Christian Schaffner, and Barbara M. Terhal. Cryptography from noisy storage. *Physical Review Letters*, 100(22):220502, 2008. [doi:10.1103/PhysRevLett.100.220502](https://doi.org/10.1103/PhysRevLett.100.220502).
- [WZ82] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982. [doi:10.1038/299802a0](https://doi.org/10.1038/299802a0).
- [Yan06] Dong Yang. A simple proof of monogamy of entanglement. *Physics Letters A*, 360(2):249–250, 2006. [doi:10.1016/j.physleta.2006.08.027](https://doi.org/10.1016/j.physleta.2006.08.027).