Efficient Unclonable Encryption from Pauli Eigenstates

Seyoon Ragavan
MIT
sragavan@mit.edu

July 25, 2026

Abstract

We give, to our knowledge, the first plain-model, one-time information-theoretically secure, efficient unclonable encryption scheme for one classical bit. Previous work by Bhattacharyya and Culf (Nature Physics, 2026) and Bhattacharyya, Broadbent, and Culf (arXiv:2603.08916) either only showed $1/\mathsf{poly}(\lambda)$ security loss or required inefficient encryption/decryption operations. We avoid both of these caveats; in doing so, we obtain (to our knowledge) the first plain-model construction of many-time secure $1 \to 2$ unclonable encryption for arbitrary polynomial-length messages, assuming the existence of pseudorandom function-like states (Bartusek and Goldin, arXiv:2605.27647).

The key is a uniformly random non-identity phase-free Pauli on n qubits, and bit a is encrypted as a random $(-1)^a$ eigenstate of that Pauli. Encryption and decryption use $O(n)$ single-qubit operations and $O(n)$ time classical computation; key generation uses only $O(n)$ time classical computation. The scheme is exponentially secure; we prove that the probability that both receivers recover the bit is at most $\frac{1}{2} + \frac{1}{2}\sqrt{2^n/(4^n-1)} = \frac{1}{2} + O\left(2^{-n/2}\right)$. By a lower bound due to Broadbent, Culf, and Rochette, this is the best probability bound achievable with n-qubit ciphertexts (up to the constant hidden in the $O(\cdot)$).

The main conceptual idea is to leverage, in a precise spectral sense, the balanced commutation-anticommutation structure of the Pauli group. The proof is intricate but completely elementary and makes use of standard spectral bound techniques. The main technical workhorse is a standalone linear-algebraic lemma which we present in its own section: informally, it relates the positivity of two different operators, each capturing the intuition that if the two receivers can individually decrypt unusually often then they must also disagree often.

GPT-5.6 Sol Ultra found this proof in an extended conversation with the author and drafted a preliminary version of this paper. The author is fully accountable for the correctness of this paper.

1 Introduction

Unclonable encryption [Got03, BL20] asks a quantum ciphertext sent by Alice to enforce a temporal access rule: before learning the secret key, an adversary ("the cloner") may process and split the ciphertext arbitrarily; after the key is revealed, two separated receivers ("Bob" and "Charlie") should not both be able to recover the plaintext. In this setting, the only honest party is Alice; the cloner, Bob, and Charlie are all adversarial. The baseline success probability for a one-bit message is $1/2$, since Bob and Charlie may agree in advance on a uniformly random bit. Alternatively, the cloner could forward Alice's ciphertext to Bob, who can now decrypt and leave Charlie to guess randomly. The goal is to prevent the adversaries from improving non-negligibly over these baseline strategies.

The notion originates in the study of quantum authentication and unclonable encryption [Got03, BL20] and has subsequently been investigated in oracle, computational, and information-theoretic settings

[BL20, MST21, AKL+22]. It is closely related to monogamy-of-entanglement games [TFKW13] and, more broadly, to cloning games [AKL23, PRV26]. Recent work has made tremendous progress on this deceptively simple problem, but to our knowledge, all previous results inherited at least one caveat:

- A line of works by Ananth et al. solved this problem assuming either a classical random oracle with quantum query access [AKL+22] or quantum decryption keys [AKY25].
- Bhattacharyya and Culf developed a decoupling-based approach [BC26] that worked in the plain model but incurred a security loss that was inverse-polynomial in n.
- Later, Bhattacharyya, Broadbent, and Culf [BBC26a] used a Haar-based approach in the plain model that attained negligible security loss but required inefficient encryption and decryption operations.
- Bartusek and Goldin [BG26b] solved this problem in the Haar random-oracle model.

In this paper we eliminate all of these caveats, showing that one-time, information-theoretically secure, efficient unclonable encryption exists. Our unclonable encryption scheme is as follows. Let

$$\mathcal{P}_n = \{I, X, Y, Z\}^{\otimes n}$$

denote one Hermitian, phase-free representative of every n-qubit Pauli class. The key is sampled uniformly[1] from $\Theta_n = \mathcal{P}_n \setminus \{I^{\otimes n}\}$. To encrypt a bit a, we send a random $(-1)^a$ eigenstate of the key Pauli, or equivalently the maximally mixed state on the $(-1)^a$ eigenspace of the key Pauli. The legitimate decryptor measures that Pauli. The construction is thus finite, explicit, and efficient. This construction bears some similarity to one proposed by Botteron et al. [BBC+26b], as we will discuss at the end of this introduction.

Our main theorem is stated below. The main conceptual idea behind its proof is to leverage the balanced commutation-anticommutation structure of the Pauli group, in a very precise spectral sense: if we encode this structure in a square matrix with ± 1 entries, the resulting matrix will have low spectral norm. The security proof is intricate but completely elementary and makes use of standard spectral bound techniques. The main technical workhorse is a standalone linear-algebraic lemma which we present in Section 6. (We defer it to after our main security proof to better motivate its statement.)

Main Theorem 1. *For every $n \geq 1$, the Pauli construction is perfectly correct and, against every information-theoretic splitting attack,*

$$\Pr[\text{Bob and Charlie decrypt correctly}] \leq \frac{1}{2} + \frac{1}{2}\sqrt{\frac{2^n}{4^n - 1}}.$$

In particular, the cloning advantage over the trivial $1/2$ strategy is $O(2^{-n/2})$. Encryption and decryption use $O(n)$ single-qubit operations and $O(n)$ time classical computation; key generation uses only $O(n)$ time classical computation.

Some remarks are in order. Firstly, the $O(2^{-n/2})$ cloning advantage bound is the best achievable for any perfectly correct unclonable encryption scheme with n-qubit ciphertexts [BCR25, Corollary 22]. Secondly, our proof of Main Theorem 1 also shows that we can take the key space to be any collection of non-identity Paulis of size $2^{n+\omega(\log n)}$ (rather than all $4^n - 1$ of them), and still incur a security loss of $\mathsf{negl}(n)$. See

[1] The Pauli $I^{\otimes n}$ is excluded from the key space to ensure that the key has both -1 and $+1$ eigenspaces. Strictly speaking, this restriction is not necessary; key generation could sample from all of $\mathcal{P}_n$, and in the extremely unlikely event that the key is $I^{\otimes n}$, Alice could just "give up" and send her bit in the clear. This will only incur a security loss of $O(4^{-n})$.

Theorem 5.1 for a general formulation of our security bound. Thirdly, our result can be readily upgraded via standard Haar invariance techniques [MST21, BCR25, PRV26] to give an alternate proof that the Haar scheme of [BBC26a] is secure (albeit inefficient), while also making a minor improvement to their proven security loss from $O(2^{-n/8})$ to the optimal $O(2^{-n/2})$. We present this in Section 7 for completeness.

Finally, our result can be upgraded to satisfy many-time security and encrypt arbitrary polynomial-length messages at the necessary expense of making mild computational assumptions, via the compiler of Bartusek and Goldin [BG26a] building on [AK21, HKNY24]. To our knowledge, our work is the first to obtain the following result, due to the aforementioned caveats with previous work.

Corollary 1.1 (Via [BG26a])**.** *Assuming the existence of pseudorandom function-like states and computationally bounded adversaries, there exists many-time secure* $1 \to 2$ *unclonable encryption for messages of arbitrary polynomial length in the plain model.*

Comparison with the work of [BBC+26b]. A very similar construction to ours was considered by Botteron et al. [BBC+26b], but instead of using the entire Pauli group (excluding the identity), they restricted the key space to a pairwise anticommuting subset of the Pauli group. This immediately limits the construction to security of the form $1/2 + 1/\mathsf{poly}(n)$ because the number of possible keys is at most polynomial, and whether their construction attains this security bound was posed by the authors as a conjecture. Despite having a similar encryption scheme, our techniques do not appear to imply any useful bounds on the security of their scheme.

The reason is that an essential component of our analysis is leveraging the fact that the Paulis are very balanced between commutation and anticommutation (see Section 2.2 for more discussion of this). Extending our results to cover the construction proposed by [BBC+26b] (albeit with a necessarily weaker security bound) is an interesting direction for future work.

Concurrent and independent work. Concurrently and independently to our work, Ananth and Sahai [AS26] found and posted the same result. Their construction and proof are essentially identical to ours, modulo minor differences in presentation and structure. The only substantive difference is that we give a different proof of the lemma that $\|S_B S_C\| \leq \epsilon$ (Lemma 5.5, compare with [AS26, Proposition 3.5]). Their proof uses a conditional overlap lemma and the pairwise orthogonality of the n-qubit Paulis (with respect to the Hilbert-Schmidt inner product); ours uses the Paulis' commutation-anticommutation structure.

Lean 4 formalization. To help with verifiability, we release Lean 4 code for our main proofs. In more detail, the Lean repository proves all correctness and security claims in Main Theorem 1 and Theorem 7.2, but it does not formally show the efficiency claim in Main Theorem 1. It also provides a modular interface defining unclonable encryption for a bit, allowing for other users to provide their own constructions and security proofs in Lean 4. It also does not prove Corollary 1.1 since this would also require formalizing the results of [BG26a]. The Lean code was built using Codex GPT-5.6 Sol and can be found at this GitHub repository.

Notation. All Hilbert spaces are finite-dimensional and complex. For a linear operator A, write A^* for its adjoint and $\|A\| = \sqrt{\lambda_{\max}(A^*A)}$ for its spectral norm. For self-adjoint operators A, B, the notation $A \preceq B$ means that $B - A$ is positive semidefinite. For a Hermitian A and a state ρ, we use $\langle A \rangle_\rho$ to denote the expectation value $\mathrm{Tr}\,[A\rho]$. We freely suppress identity operators and tensor symbols when their registers are clear (see Remark 1 for more detail on this). Density operators have trace one, and quantum channels

are completely positive and trace preserving. We use standard facts about Choi representations, Naimark dilation, and finite dimensional operator theory; see, for example, [NC16, Wat18].

Statement on AI use. The result was discovered by OpenAI's GPT-5.6 Sol Ultra in conversation with the author. The author asked the agents to brainstorm and pursue an array of approaches to proving the theorem. The agents eventually converged on the Pauli bit as a promising candidate encryption scheme. In the first few rounds, the agents managed to prove bounds of the form $c + o(1)$ or $c + \mathsf{negl}(n)$ for slowly improving constants $c > 1/2$, for the most part using sum-of-squares bounds based on the NPA hierarchy. The author explicitly pushed the agents to find a proof using simple spectral bounds and provided feedback on their progress. In the sixth round, the agents found a complete solution. The agents drafted the first version of this paper, after which the author significantly cleaned up and reorganized the formal presentation and added informal exposition explaining the ideas. GPT-5.6 Sol and Claude Fable 5 were both used for proofreading. Codex GPT-5.6 Sol was used to produce Lean 4 code for our proofs.

Acknowledgements. The author thanks Alexander Poremba and Vinod Vaikuntanathan for introducing him to the problem of unclonable encryption and for a wonderful collaboration on this front. The author additionally thanks Vinod Vaikuntanathan and Aparna Gupte for helpful feedback on drafts of this paper, and Prabhanjan Ananth, Eli Goldin, Yao-Ting Lin, and Amit Sahai for helpful discussions. The author's access to ChatGPT Pro and Claude Max were respectively supported by the UK AISI alignment project, and Jane Street.

2 Technical Overview

The security proof for the Pauli unclonable encryption scheme begins in Section 5.1 by applying standard transformations [BL20] to boil proving security down to the following task: let Θ denote the key space of all non-identity Paulis, and for each θ let $P_\theta, B_\theta, C_\theta$ respectively denote the corresponding Pauli, Bob's reflection, and Charlie's reflection. By "Bob's reflection", we mean that Bob outputs his guess given the secret key θ by applying the projective measurement $\{(\mathbb{I} + B_\theta)/2, (\mathbb{I} - B_\theta)/2\}$. We understand $P_\theta, B_\theta, C_\theta$ to be operators in the same Hilbert space, with the constraint that P_θ, B_ϕ, C_ψ must pairwise commute for any $\theta, \phi, \psi \in \Theta$ (which is enforced by the spatial separation of the parties). In these terms, the goal is simply to show that:

$$\Xi := \frac{1}{|\Theta|} \sum_{\theta \in \Theta} \left(\frac{\mathbb{I} + P_{\theta,\mathsf{A}}^\top B_{\theta,\mathsf{B}}}{2} \right) \left(\frac{\mathbb{I} + P_{\theta,\mathsf{A}}^\top C_{\theta,\mathsf{C}}}{2} \right) \preceq \left(\frac{1}{2} + \mathsf{negl}(n) \right) \mathbb{I}. \tag{1}$$

The subscripts $\mathsf{A}, \mathsf{B}, \mathsf{C}$ above indicate which register each of these operators acts on. Going forward, we will suppress these subscripts and understand $P_\theta, B_\theta, C_\theta$ as operators on the combined Hilbert space, carrying forward the constraint that any two of P_θ, B_ϕ, C_ψ must commute (see Remark 1 for more on this). The intuition is that the $\frac{\mathbb{I}+P_\theta^\top B_\theta}{2}$ projector checks whether Bob guesses correctly and the $\frac{\mathbb{I}+P_\theta^\top C_\theta}{2}$ projector checks whether Charlie guesses correctly. The adversaries' strategy can be encoded with the existing unitaries $\{B_\theta, C_\theta\}$ and a state ρ on this same Hilbert space. For brevity, write $\Pi_\theta = \left(\frac{\mathbb{I}+P_\theta^\top B_\theta}{2}\right)\left(\frac{\mathbb{I}+P_\theta^\top C_\theta}{2}\right)$.

It might be tempting to try and prove the stronger two-sided bound that $\|\Xi - \mathbb{I}/2\| \leq \mathsf{negl}(n)$, but this is false! If Bob always outputs 0 and Charlie always outputs 1, then their winning probability is 0 so $\langle \Xi \rangle_\rho$ will be 0. With that in mind, we pursue the one-sided objective stated in (1).

2.1 Operators and Interpretations (Section 5.2)

All techniques discussed in this overview can be interpreted as proving an inequality between three operators:

- $S_B = \frac{1}{|\Theta|}\sum_\theta P_\theta^\top B_\theta$: this is an average of reflections that check whether Bob's guess is correct. If p_B is the probability that Bob guesses correctly (averaged across θ), we have $\langle S_B\rangle_\rho = 2p_B - 1$.
- $S_C = \frac{1}{|\Theta|}\sum_\theta P_\theta^\top C_\theta$: this is defined analogously for Charlie. Let p_C denote the probability that Charlie guesses correctly.
- $D = \frac{1}{|\Theta|}\sum_\theta \frac{\mathbb{I}-B_\theta C_\theta}{2}$: this is an average of projections that check whether Bob and Charlie's guesses disagree. If $p_{\neq}$ is the probability that they disagree, we have $\langle D\rangle_\rho = p_{\neq}$.

In these terms, it is straightforward to see that:

$$\Xi = \frac{1}{2}\mathbb{I} + \frac{1}{4}(S_B + S_C) - \frac{1}{2}D. \tag{2}$$

This can either be checked with direct algebraic manipulation, or intuited by noting that $\frac{S_B+S_C}{4}$ is capturing the bias beyond $1/2$ of the sums of Bob's and Charlie's individual guessing probabilities. This overcounts cases where exactly one of Bob and Charlie guesses correctly, which we account for by subtracting off $\frac{1}{2}D$. In general, the above operational interpretations will be extremely useful for understanding the techniques which we present. At this point, one can also intuit the following bounds (which we prove rigorously in the body). The limitation of these bounds is that they can all be deduced without considering how the operators for different keys $\theta \neq \theta'$ interact with each other.

$$0 \preceq D \preceq \mathbb{I} \qquad \text{("the probability of disagreement is always between 0 and 1");} \tag{3}$$

$$D \succeq \pm\frac{S_B - S_C}{2} \qquad \text{("if Bob succeeds and Charlie does not, then their answers disagree").} \tag{4}$$

$$\tag{5}$$

2.2 Leveraging the Pauli Commutation-Anticommutation Structure (Lemma 5.5)

The main conceptual ingredient of our security analysis is to exploit the balanced commutation-anticommutation behavior of the Pauli group. In more detail, let Γ be the square matrix of dimension $4^n - 1$ with ± 1 entries that encodes the Pauli commutation structure i.e., we have $P_\theta P_\phi = \Gamma_{\theta,\phi} P_\phi P_\theta$ for all ϕ, θ. A key component of our bound will be the straightforward estimate that $\|\Gamma\| \leq 2^n$ (Lemma 3.4); this essentially follows from the fact that Γ is a submatrix of a scaled-up and column-permuted Hadamard matrix. So a feature of the all-Pauli scheme that works in our favor is that Paulis have a commutation-anticommutation pattern that has nice spectral behavior.

We view Lemma 3.4 discussed above as a spectral formulation of the notion that Γ is "balanced."[2] An example of an unbalanced Γ would be the all 1's matrix, which has larger spectral norm $4^n - 1$. Using this commutation structure alone, it is straightforward to prove that:

$$\|S_B S_C\| \leq \epsilon \qquad \text{(Lemma 5.5),} \tag{6}$$

[2] As discussed at the end of the introduction, this is quite different from the Pauli construction considered by [BBC+26b], where the proposed scheme worked with a pairwise anticommuting set of Paulis (so Γ would have 1's on the diagonal and -1's off the diagonal and have exponentially lower dimension).

where $\epsilon = \|\Gamma\| / |\Theta| = \mathsf{negl}(n)$. To see why, let us expand out $S_B S_C$:

$$S_B S_C = \frac{1}{|\Theta|^2} \sum_{\theta,\phi} P_\theta^\top B_\theta P_\phi^\top C_\phi = \frac{1}{|\Theta|^2} \sum_{\theta,\phi} C_\phi (P_\phi P_\theta)^\top B_\theta.$$

This is an average of $|\Theta|^2$ unitaries, so it is not yet clear why its spectral norm should be $\ll 1$. The trick is to commute P_ϕ and P_θ past each other, yielding:

$$S_B S_C = \frac{1}{|\Theta|^2} \sum_{\theta,\phi} \underbrace{(C_\phi P_\phi^\top)}_{:=U_\phi} \Gamma_{\phi,\theta} \underbrace{(P_\theta^\top B_\theta)}_{:=V_\theta}.$$

Now we have a *signed* average of $|\Theta|^2$ unitaries $\{U_\phi V_\theta : \phi, \theta \in \Theta\}$! This is the quadratic form of Γ applied to the matrices $\{U_\phi\}$ on the left and $\{V_\theta\}$ on the right. So the fact that Γ has low spectral norm now forces this average to destructively interfere and give us the desired negligible bound on $\|S_B S_C\|$.

2.3 Introducing a Regularized Disagreement Conditioner (Corollary 5.7)

Let us for the moment pretend that (a) S_B and S_C commute (so $S_B S_C$ is Hermitian); and (b) we have $\langle S_B S_C \rangle_\rho = \langle S_B \rangle_\rho \langle S_C \rangle_\rho$ (i.e., Bob's and Charlie's success probabilities across keys are uncorrelated in some sense). With these assumptions, (6) would admit the very clean interpretation that

$$|(2p_B - 1)(2p_C - 1)| \leq \epsilon. \tag{7}$$

In this case, the above would imply that p_B, p_C cannot simultaneously be $> 1/2 + \sqrt{\epsilon}/2$ and we would immediately be done.

What goes wrong when we account for correlations between Bob's guess and Charlie's guess? In this case, (7) need not be true. Consider the following very simple strategy: the cloner flips a coin and accordingly forwards Alice's ciphertext to either Bob or Charlie. The other receiver will guess randomly. For this strategy, we have $p_B = p_C = 3/4$, contradicting (7). The reason that Bob and Charlie still only win with probability $1/2$ is that the cases where Bob guesses incorrectly and Charlie guesses incorrectly are completely disjoint (i.e., there is a strong anticorrelation), so the two $1/4$'s add up to give a failure probability of $1/2$. So we need to somehow adapt (6) to additionally penalize strategies where Bob and Charlie disagree often.

Fortunately for us, we have an operator D that exactly captures the subspace where Bob and Charlie disagree. A concrete hope would be to prove a statement of the form:

$$\left\| S_B D^{-1} S_C \right\| \leq \mathsf{negl}(n). \tag{8}$$

In the above, D^{-1} acts as a "disagreement conditioner" that amplifies subspaces where Bob and Charlie are likely to agree but not subspaces where Bob and Charlie are likely to disagree (and therefore lose). This effectively focuses the estimate on the subspace we really need to worry about which is that where Bob and Charlie agree.

Unfortunately, (8) cannot possibly be true; D need not be invertible, as there could be a state for which Bob and Charlie agree with probability 1. However, we can prove something very close, namely:

$$\left\| S_B (D + \delta \mathbb{I})^{-1} S_C \right\| \leq \epsilon/\delta \quad \forall \delta > 0 \qquad \text{(Corollary 5.7)}. \tag{9}$$

We think of $(D + \delta\mathbb{I})^{-1}$ as a "regularized disagreement conditioner"; the $\delta\mathbb{I}$ term acts as a "regularizer" to ensure that no direction gets blown up by more than $1/\delta$ and we accordingly pay a $1/\delta$ penalty on the RHS. This penalty can be absorbed while retaining negligibility by setting $\delta = \sqrt{\epsilon}$.

The proof of (9) proceeds by taking a power series expansion of $(D + \delta\mathbb{I})^{-1}$ and bounding every term that appears using (6) (Lemma 5.5).

2.4 Linear-Algebraic Step (Section 6)

It turns out that our heuristic intuition about the relevance of (9) can actually be turned into a rigorous security proof! Recall from (2) that our task is to show that:

$$S_B + S_C - 2D \preceq \mathsf{negl}(n) \cdot \mathbb{I}. \tag{10}$$

This bears some qualitative similarity to (9); both say that "D is large relative to S_B and S_C", or more qualitatively that if Bob and Charlie individually win unusually often then they must also disagree often. In fact, we can formally show that (9) implies (10); this is the content of Theorem 6.2.

The proof uses some simple but non-obvious manipulations with 2×2 block matrices based on Schur complements; equivalently, it can be written as a matrix-valued rational sum-of-squares certificate.

3 Preliminaries

3.1 Pauli Symplectic Space

Let $V_n = \mathbb{F}_2^n \times \mathbb{F}_2^n$. For $v = (x, z) \in V_n$, let P_v be the phase-free Hermitian Pauli obtained by taking the tensor product of I, X, Y, Z prescribed by the pairs (x_i, z_i). Equivalently, one may use the phase convention $P_{(x,z)} = i^{|x \wedge z|} X^x Z^z$, where $|x \wedge z|$ is the integer number of coordinates on which $x_i = z_i = 1$. Every P_v is a reflection (meaning $P_v^2 = \mathbb{I}$).

Definition 3.1 (Pauli symplectic form)**.** *For $v = (x, z), w = (x', z') \in V_n$, we define the symplectic form to be:*

$$[v, w] = \langle x, z' \rangle + \langle z, x' \rangle \in \mathbb{F}_2.$$

Lemma 3.2 (Pauli commutation relations)**.** *For any $v, w \in V_n$, we have:*

$$P_v P_w = (-1)^{[v,w]} P_w P_v, \qquad \mathrm{Tr}\,[P_v P_w] = 2^n \mathbf{1}[v = w]. \tag{11}$$

Proof. Writing $v = (x, z)$ and $w = (x', z')$, we have:

$$P_v P_w = i^{|x \wedge z| + |x' \wedge z'|} X^x Z^z X^{x'} Z^{z'} = i^{|x \wedge z| + |x' \wedge z'|} \cdot (-1)^{\langle x', z \rangle} X^{x+x'} Z^{z+z'}.$$

(This already implies that $\mathrm{Tr}\,[P_v P_w] = 0$ unless $(x, z) = (x', z')$, in which case $P_v P_w$ is the identity since the Paulis are reflections.) By symmetry, we also have:

$$P_w P_v = i^{|x \wedge z| + |x' \wedge z'|} \cdot (-1)^{\langle x, z' \rangle} X^{x+x'} Z^{z+z'}.$$

Comparing the above two equalities implies the conclusion. □

Definition 3.3 (Symplectic character matrix)**.** *Define $\Gamma^{\mathrm{Pauli}} \in \{-1, 1\}^{(4^n-1) \times (4^n-1)}$ to be the matrix with rows and columns indexed by elements of $V_n \backslash \{(0, 0)\}$. The entry in row v and column w is $\Gamma^{\mathrm{Pauli}}_{v,w} = (-1)^{[v,w]}$.*

Lemma 3.4 (Pauli symplectic structure is spectrally balanced)**.** *We have* $\left\|\Gamma^{\mathrm{Pauli}}\right\| = 2^n$*. (We remark that we only need the upper bound of* 2^n*, but we prove tightness for completeness.)*

Proof. Unpacking $v = (x, z)$ and $w = (x', z')$, the corresponding entry of Γ^{Pauli} is $\Gamma^{\mathrm{Pauli}}_{(x,z);(x',z')} = (-1)^{\langle x,z'\rangle+\langle z,x'\rangle}$. Let us permute columns by swapping the roles of x', z' to obtain a new matrix Γ', then it suffices to show that $\|\Gamma'\| = 2^n$. We have $\Gamma'_{(x,z);(z',x')} = (-1)^{\langle x,z'\rangle+\langle z,x'\rangle}$, so it is apparent that $\frac{1}{2^n}\Gamma'$ is a submatrix of the $2^{2n} \times 2^{2n}$ normalized Hadamard matrix (removing the row and column corresponding to $(0, 0)$), which is unitary. It immediately follows that $\|\Gamma'/2^n\| \leq \|H\| = 1 \Rightarrow \|\Gamma'\| \leq 2^n$. To see that this is an equality, note that:

$$\begin{aligned}
H &= \begin{bmatrix} \frac{1}{2^n} & \frac{1}{2^n}\mathbf{1}^\top \\ \frac{1}{2^n}\mathbf{1} & \frac{1}{2^n}\Gamma' \end{bmatrix} \\
\Rightarrow 2^{2n}\mathbb{I} = (2^n H)^2 &= \begin{bmatrix} 1 & \mathbf{1}^\top \\ \mathbf{1} & \Gamma' \end{bmatrix}^2 \\
&= \begin{bmatrix} 1 & \mathbf{1}^\top \\ \mathbf{1} & \Gamma' \end{bmatrix} \begin{bmatrix} 1 & \mathbf{1}^\top \\ \mathbf{1} & \Gamma' \end{bmatrix} \\
&= \begin{bmatrix} . & . \\ . & \mathbf{1}\mathbf{1}^\top + (\Gamma')^2 \end{bmatrix} \\
\Rightarrow 2^{2n}\mathbb{I}_{2^{2n}-1} &= \mathbf{1}\mathbf{1}^\top + (\Gamma')^2.
\end{aligned}$$

So for a nonzero vector $\mathbf{v} \in \mathbf{1}^\perp \subseteq \mathbb{C}^{2^{2n}-1}$, we have $2^{2n}\mathbf{v} = (\Gamma'^2)\mathbf{v}$, forcing $\left\|\Gamma'^2\right\| \geq 2^{2n} \Rightarrow \|\Gamma'\| \geq 2^n$. □

3.2 Choi-Jamiołkowski Isomorphism

Let $\mathcal{H}_{\mathsf{A}}$ be a d-dimensional Hilbert space with an orthonormal basis denoted by $\{|1\rangle, \ldots, |d\rangle\}$. Let $|\Omega\rangle = \sum_{i\in[d]} |i\rangle \otimes |i\rangle$ be the vectorization of the identity $\mathbb{I}_d = \sum_{i\in[d]} |i\rangle\langle i|$. Then, the normalized Choi-Jamiołkowski isomorphism $J(\Phi) \in \mathrm{L}(\mathcal{H}_{\mathsf{B}} \otimes \mathcal{H}_{\mathsf{A}'})$ with respect to a CPTP map of the form $\Phi : \mathrm{L}(\mathcal{H}_{\mathsf{A}}) \to \mathrm{L}(\mathcal{H}_{\mathsf{B}})$ is defined as

$$J(\Phi) = \frac{1}{d}(\Phi_{\mathsf{A}\to\mathsf{B}} \otimes \mathbb{I}_{\mathsf{A}'})(|\Omega\rangle\langle\Omega|) = \frac{1}{d}\sum_{i,j\in[d]} \Phi(|i\rangle\langle j|) \otimes |i\rangle\langle j|\,.$$

Note that $J(\Phi)$ is a valid quantum state. We use the following well known fact (copied here from [PRV26, Corollary 2.2] while taking our different normalization convention into account).

Lemma 3.5. *Let* $\Phi : \mathrm{L}(\mathcal{H}_{\mathsf{A}}) \to \mathrm{L}(\mathcal{H}_{\mathsf{B}})$ *be any linear map. Then, for any Hermitian operators* $\mathbf{P} \in \mathrm{L}(\mathcal{H}_{\mathsf{B}})$ *and* $\mathbf{Q} \in \mathrm{L}(\mathcal{H}_{\mathsf{A}})$*, it holds that*

$$\mathrm{Tr}\left[\mathbf{P}\Phi(\mathbf{Q})\right] = d \cdot \mathrm{Tr}\left[\left(\mathbf{P} \otimes \bar{\mathbf{Q}}\right) J(\Phi)\right].$$

3.3 One-Time Secure Unclonable Encryption

Consider a key-indexed pair of states $\rho_{\theta,0}, \rho_{\theta,1}$. The plaintext $a \leftarrow \{0, 1\}$ and key θ are uniform. The cloner first applies a key-independent channel

$$\Phi : A_0 \longrightarrow B \otimes C$$

to the ciphertext. The key is then revealed, after which Bob and Charlie use arbitrary key-dependent binary POVMs $\{D^B_{\theta,a}\}_{a\in\{0,1\}}$ and $\{D^C_{\theta,a}\}_{a\in\{0,1\}}$. Their joint success probability is

$$\frac{1}{2|\Theta|}\sum_{\theta\in\Theta}\sum_{a\in\{0,1\}}\mathrm{Tr}\left[(D^B_{\theta,a}\otimes D^C_{\theta,a})\Phi(\rho_{\theta,a})\right]. \tag{12}$$

The scheme is one-time unclonably secure if this is at most $1/2+\mathsf{negl}(n)$ for every attack.

4 The Unclonable Encryption Scheme

To help highlight the important aspects of our proof, we formulate our construction in slightly more general terms than our Pauli instantiation.

Construction 1. *Fix $n\geq 1$ and put $d=2^n$. Let $\{Q_\theta:\theta\in\Theta_n\}$ be any collection of traceless Hermitian reflections of dimension 2^n. Let $M=|\Theta_n|$. We will often abuse notation and let $\Theta=\Theta_n$.*

- *Key generation: sample a uniformly random $\theta\leftarrow\Theta$.*
- *To encrypt $a\in\{0,1\}$, output*
$$\rho_{\theta,a}=\frac{1}{d}\big(\mathbb{I}+(-1)^aQ_\theta\big). \tag{13}$$
An equivalent formulation is to send a uniformly random $(-1)^a$ eigenstate of Q_θ.
- *To decrypt, measure the reflection Q_θ and output the bit whose sign $(-1)^a$ equals the measured eigenvalue.*

Lemma 4.1 (Correctness)**.** *For every $\theta\in\Theta$ and $a\in\{0,1\}$, $\rho_{\theta,a}$ is a density operator. Construction 1 is perfectly correct.*

Proof. Since Q_θ is a Hermitian reflection,

$$E_{\theta,a}=\frac{1}{2}(\mathbb{I}+(-1)^aQ_\theta)$$

is the orthogonal projector onto its $(-1)^a$ eigenspace. Tracelessness of Q_θ gives $\mathrm{Tr}\,[E_{\theta,a}]=d/2$, so $\rho_{\theta,a}=(2/d)E_{\theta,a}$ is positive semidefinite and has trace one. Measuring $\{E_{\theta,0},E_{\theta,1}\}$ on a state supported on $E_{\theta,a}$ returns a with probability one. □

4.1 The Pauli Instantiation

Our main instantiation will take $\Theta_n=V_n\backslash\{(0,0)\}$ to be the collection of all non-identity Paulis, and $Q_\theta=P_\theta$. Lemma 3.2 tells us that these are traceless Hermitian reflections and hence we get correctness.

To see the efficiency of this instantiation, let the key be $(\theta_1,\ldots,\theta_n)$ and write $S=\{i:\theta_i\neq I\}$. To encrypt, sample one-qubit eigenvalue signs $\{\sigma_j\in\{\pm1\}:j\in S\}$ uniformly subject to $\prod_{j\in S}\sigma_j=(-1)^a$, prepare the corresponding one-qubit Pauli eigenstates, and prepare the maximally mixed state on coordinates outside S. The resulting mixture is exactly the maximally mixed state in (13). Decryption measures the single-qubit Paulis on S and takes the parity of the outcomes. Sampling a nonzero Pauli label, encrypting, and decrypting all take $O(n)$ elementary operations.

5 Proof of Security

We begin by stating the general security theorem that we will prove in this section:

Theorem 5.1 (General unclonability)**.** *Consider the construction of Section 4, and assume additionally that there exists a matrix* $\Gamma \in \{-1,1\}^{|\Theta|\times|\Theta|}$ *such that:*

$$Q_\phi Q_\theta = \Gamma_{\phi,\theta} Q_\theta Q_\phi \quad \forall \theta, \phi \in \Theta. \tag{14}$$

Then for every splitting attack in the game of Section 4,

$$\Pr[\text{Bob and Charlie decrypt correctly}] \leq \frac{1}{2} + \frac{1}{2}\sqrt{\frac{\|\Gamma\|}{|\Theta|}}. \tag{15}$$

5.1 Ricochet Reduction

First, we apply some standard manipulations [BL20] based on Naimark dilation and the EPR ricochet property to reduce security to a simpler linear-algebraic task. To this end, fix an arbitrary splitting channel and arbitrary key-dependent local binary POVMs. By Naimark's dilation theorem, we may assume without loss of generality that Bob's measurement is determined by an ensemble of binary projective measurements $\{(D^B_{\theta,0}, D^B_{\theta,1}) : \theta \in \Theta\}$, and similarly for Charlie. (This was shown in [TFKW13], so we do not reproduce a proof here.) We succinctly encode these in the operators:

$$B_\theta = D^B_{\theta,0} - D^B_{\theta,1}, \qquad C_\theta = D^C_{\theta,0} - D^C_{\theta,1}.$$

It is straightforward to see that B_θ, C_θ are Hermitian and that $B_\theta^2 = C_\theta^2 = \mathbb{I}$ for all $\theta \in \Theta$. Since these reflections act on distinct receiver registers we immediately have commutation:

$$B_\theta C_\phi = C_\phi B_\theta \qquad \text{for all } \theta, \phi. \tag{16}$$

Note that there is no commutation assumption among two Bob reflections or two Charlie reflections.

The following lemma can be interpreted as switching to the following experiment: Alice and the cloner initially share n EPR pairs. The cloner then acts arbitrarily on their end of the state and forwards the results to Bob and Charlie. Bob and Charlie make their measurements as usual, and Alice measures with the projectors $\frac{1}{2}(\mathbb{I} \pm Q_\theta^\top)$. The adversaries win if all three measurement results agree. In the following, all stated operators will be over some common dimension $\tilde{d}$.

Lemma 5.2 (Winning operator)**.** *The success probability of the fixed cloning attack is* $\omega = \operatorname{Tr}[\Xi J(\Phi)]$*, where* $J(\Phi)$ *is the normalized Choi state as defined in Section 3.2, and:*

$$\Xi = \frac{1}{M}\sum_{\theta \in \Theta_n} \Pi_\theta, \qquad \Pi_\theta = \frac{1}{4}(\mathbb{I} + Q_\theta^\top B_\theta)(\mathbb{I} + Q_\theta^\top C_\theta). \tag{17}$$

Moreover, every Π_θ *is an orthogonal projection, and hence* $0 \preceq \Xi \preceq \mathbb{I}$*.*

Proof. We begin from (12) and use Lemma 3.5:

$$\omega = \frac{1}{2|\Theta|}\sum_{\theta\in\Theta}\sum_{a\in\{0,1\}} \operatorname{Tr}\left[\left(\frac{\mathbb{I} + (-1)^a B_\theta}{2}\right)\left(\frac{\mathbb{I} + (-1)^a C_\theta}{2}\right)\Phi\left(\frac{1}{d}\left(\mathbb{I} + (-1)^a Q_\theta\right)\right)\right]$$

$$
\begin{aligned}
&= \frac{1}{2|\Theta|} \sum_{\theta\in\Theta} \sum_{a\in\{0,1\}} \mathrm{Tr}\left[\left(\frac{\mathbb{I}+(-1)^a B_\theta}{2}\right)\left(\frac{\mathbb{I}+(-1)^a C_\theta}{2}\right)\left(\mathbb{I}+(-1)^a Q_\theta^\top\right) J(\Phi)\right] \\
&= \frac{1}{4|\Theta|} \sum_{\theta\in\Theta} \mathrm{Tr}\left[\left(\mathbb{I}+B_\theta C_\theta + B_\theta Q_\theta^\top + C_\theta Q_\theta^\top\right) J(\Phi)\right] \\
&= \frac{1}{|\Theta|} \sum_{\theta\in\Theta} \mathrm{Tr}\left[\Pi_\theta J(\Phi)\right] \\
&= \mathrm{Tr}\left[\Xi J(\Phi)\right],
\end{aligned}
$$

as claimed. To see the latter claims, note that $Q_\theta^\top, B_\theta, C_\theta$ are commuting reflections so it follows that $\frac{\mathbb{I}+Q_\theta^\top B_\theta}{2}, \frac{\mathbb{I}+Q_\theta^\top C_\theta}{2}$ are commuting projectors, so their product Π_θ is also a projector. The claim that their average Ξ is PSD and has all eigenvalues ≤ 1 immediately follows. □

Remark 1. *To clarify, we are abusing notation slightly: what we should really do is define $Q_\theta, B_\theta, C_\theta$ locally on Alice's, Bob's, and Charlie's registers, then define:*

$$
\begin{aligned}
\widehat{Q}_\theta &= Q_{\theta,\mathsf{A}} \otimes \mathbb{I}_\mathsf{B} \otimes \mathbb{I}_\mathsf{C} \\
\widehat{B}_\theta &= \mathbb{I}_\mathsf{A} \otimes B_{\theta,\mathsf{B}} \otimes \mathbb{I}_\mathsf{C} \\
\widehat{C}_\theta &= \mathbb{I}_\mathsf{A} \otimes \mathbb{I}_\mathsf{B} \otimes C_{\theta,\mathsf{C}},
\end{aligned}
$$

and then work with the operators $\widehat{Q}_\theta, \widehat{B}_\theta, \widehat{C}_\theta$. The abuse of notation is that we take Q_θ to mean $\widehat{Q}_\theta$, and similarly for B_θ, C_θ.

5.2 Setup

We refer the reader to Section 2.1 for an intuitive discussion of the operators defined here and their properties.

Definition 5.3. *Define the following Hermitian operators:*

$$
S_B = \frac{1}{M}\sum_\theta Q_\theta^\top B_\theta, \qquad S_C = \frac{1}{M}\sum_\theta Q_\theta^\top C_\theta, \qquad D = \frac{1}{M}\sum_\theta \frac{\mathbb{I}-B_\theta C_\theta}{2}. \tag{18}
$$

Also, define the parameter

$$
\epsilon := \epsilon_n = \frac{\|\Gamma\|}{M}.
$$

Lemma 5.4. *The winning operator satisfies*

$$
\Xi = \frac{1}{2}\mathbb{I} + \frac{1}{4}(S_B + S_C) - \frac{1}{2}D. \tag{19}
$$

Furthermore,

$$
0 \preceq D \preceq \mathbb{I}, \qquad D \succeq \frac{1}{2}(S_B - S_C), \qquad D \succeq \frac{1}{2}(S_C - S_B). \tag{20}
$$

Proof. Expanding (17) gives:

$$
\Xi = \frac{1}{M}\sum_{\theta\in\Theta} \frac{1}{4}(\mathbb{I}+Q_\theta^\top B_\theta)(\mathbb{I}+Q_\theta^\top C_\theta)
$$

$$= \frac{1}{4}\mathbb{I} + \underbrace{\frac{1}{4M}\sum_{\theta\in\Theta}(Q_\theta^\top B_\theta + Q_\theta^\top C_\theta)}_{=(S_B+S_C)/4} + \underbrace{\frac{1}{4M}\sum_{\theta\in\Theta} B_\theta C_\theta}_{=\mathbb{I}/4-D/2}$$
$$= \frac{1}{2}\mathbb{I} + \frac{1}{4}(S_B + S_C) - \frac{1}{2}D,$$

establishing the first identity. To see the positivity constraints, first note that D is an average over θ of the projector $\frac{\mathbb{I}-B_\theta C_\theta}{2}$, so $0 \preceq D \preceq \mathbb{I}$ is immediate. Secondly, for any $s \in \{\pm 1\}$ and any $\theta \in \Theta$, the projectors $\frac{1}{2}(\mathbb{I} + sQ_\theta^\top B_\theta)$ and $\frac{1}{2}(\mathbb{I} - sQ_\theta^\top C_\theta)$ commute, so we have:

$$\begin{aligned}
&0 \preceq (\mathbb{I} + sQ_\theta^\top B_\theta)(\mathbb{I} - sQ_\theta^\top C_\theta) \\
\Rightarrow\ &0 \preceq \mathbb{I} + \frac{s}{M}\sum_{\theta\in\Theta} Q_\theta^\top B_\theta - \frac{s}{M}\sum_{\theta\in\Theta} Q_\theta^\top C_\theta - \frac{1}{M}\sum_{\theta\in\Theta} B_\theta C_\theta \text{ (averaging over } \theta) \\
&= 2D + s(S_B - S_C) \\
\Rightarrow\ &\frac{s}{2}(S_C - S_B) \preceq D,
\end{aligned}$$

as desired. □

5.3 Bounds Using Pauli Commutation-Anticommutation Structure

As discussed in Section 2.2, the main property of the reflections $\{Q_\theta\}$ that we will leverage is that their commute–anticommute sign matrix $\Gamma \in \{-1, 1\}^{|\Theta|\times|\Theta|}$ has bounded norm (as we verified for the case of Paulis in Lemma 3.4). We next turn this norm estimate into a bound for $S_B S_C$:

Lemma 5.5. *We have:*

$$\|S_B S_C\| \leq \epsilon = \|\Gamma\|/M. \tag{21}$$

Proof. Recall that we can commute any of the relevant unitaries past each other, except for two Bob unitaries or two Charlie unitaries. In the case of two encoding reflections Q_θ, we can commute them but we must pay a correction factor as per (14). Bearing this in mind, we compute:

$$\begin{aligned}
S_B S_C &= \frac{1}{M^2}\sum_{\theta,\phi\in\Theta} (Q_\theta^\top B_\theta)(Q_\phi^\top C_\phi) \\
&= \frac{1}{M^2}\sum_{\theta,\phi\in\Theta} C_\phi Q_\theta^\top Q_\phi^\top B_\theta \\
&= \frac{1}{M^2}\sum_{\theta,\phi\in\Theta} C_\phi (Q_\phi Q_\theta)^\top B_\theta \\
&= \frac{1}{M^2}\sum_{\theta,\phi\in\Theta} \Gamma_{\phi,\theta} C_\phi (Q_\theta Q_\phi)^\top B_\theta \\
&= \frac{1}{M^2}\sum_{\theta,\phi\in\Theta} \Gamma_{\phi,\theta} (C_\phi Q_\phi^\top)(Q_\theta^\top B_\theta).
\end{aligned}$$

To help rewrite the above expression, let $M_C \in \mathbb{C}^{\tilde{d}\times\tilde{d}|\Theta|}$ be a block matrix with $|\Theta|$ block columns indexed by $\phi \in \Theta$. The block column corresponding to ϕ will be $C_\phi Q_\phi^\top$. Similarly define $M_B \in \mathbb{C}^{\tilde{d}|\Theta|\times\tilde{d}}$ have row

blocks indexed by $\theta \in \Theta$ and containing $Q_\theta^\top B_\theta$. Finally, let $M_\Gamma \in \mathbb{C}^{\tilde{d}|\Theta| \times \tilde{d}|\Theta|}$ be defined to be:

$$M_\Gamma := \Gamma \otimes \mathbb{I}_{\tilde{d}}.$$

In words, M_Γ has block rows and columns indexed by ϕ and θ respectively. The corresponding $\tilde{d} \times \tilde{d}$ block is $\Gamma_{\phi,\theta}$ times the identity matrix. In these terms, the outcome of the above computation can be rewritten as:

$$\begin{aligned} S_B S_C &= \frac{1}{M^2} M_C M_\Gamma M_B \\ &= \frac{1}{M^2} M_C (\Gamma \otimes \mathbb{I}_{\tilde{d}}) M_B \\ \Rightarrow \|S_B S_C\| &= \frac{1}{M^2} \left\| M_C (\Gamma \otimes \mathbb{I}_{\tilde{d}}) M_B \right\| \\ &\leq \frac{1}{M^2} \|M_C\| \cdot \|\Gamma\| \cdot \|M_B\| . \end{aligned}$$

We bound each term of the RHS above as follows:

- For any unit $|\psi\rangle$, the vector $M_B |\psi\rangle$ will be the concatenation of $Q_\theta^\top B_\theta |\psi\rangle$ for every $\theta \in \Theta$. By unitarity, each of these chunks has unit norm, so the total ℓ_2 norm will always be exactly $\sqrt{|\Theta|} = \sqrt{M}$. Consequently, we have $\|M_B\| = \sqrt{M}$.
- We may similarly obtain $\|M_C\| = \sqrt{M}$.

Putting these together yields:

$$\|S_B S_C\| \leq \frac{1}{M^2} \cdot M \cdot \|\Gamma\| = \frac{\|\Gamma\|}{M} = \epsilon,$$

as desired. □

In the next two corollaries, we build on Lemma 5.5 using power series techniques to prove a "regularized-disagreement-conditioned" version of its conclusion. See Section 2.3 for a discussion of this "regularized conditioning" idea.

Corollary 5.6. *For every integer $\ell \geq 0$, we have:*

$$\left\| S_B (\mathbb{I} - 2D)^\ell S_C \right\| \leq \epsilon. \tag{22}$$

Proof. We compute:

$$\begin{aligned} (\mathbb{I} - 2D)^\ell &= \frac{1}{M^\ell} \left(\sum_\theta B_\theta C_\theta \right)^\ell \\ &= \frac{1}{M^\ell} \sum_{\theta_1, \ldots, \theta_\ell \in \Theta} B_{\theta_1} C_{\theta_1} \ldots B_{\theta_\ell} C_{\theta_\ell} \\ &= \frac{1}{M^\ell} \sum_{\theta_1, \ldots, \theta_\ell \in \Theta} B_{\theta_1} \ldots B_{\theta_\ell} C_{\theta_1} \ldots C_{\theta_\ell} \\ \Rightarrow S_B (\mathbb{I} - 2D)^\ell S_C &= \frac{1}{M^\ell} \sum_{\theta_1, \ldots, \theta_\ell \in \Theta} S_B B_{\theta_1} \ldots B_{\theta_\ell} C_{\theta_1} \ldots C_{\theta_\ell} S_C \end{aligned}$$

$$
\begin{aligned}
\Rightarrow \left\|S_B(\mathbb{I}-2D)^\ell S_C\right\| &\leq \frac{1}{M^\ell}\sum_{\theta_1,\ldots,\theta_\ell\in\Theta}\|S_B B_{\theta_1}\ldots B_{\theta_\ell}C_{\theta_1}\ldots C_{\theta_\ell}S_C\| \quad \text{(triangle inequality)}\\
&= \frac{1}{M^\ell}\sum_{\theta_1,\ldots,\theta_\ell\in\Theta}\|C_{\theta_1}\ldots C_{\theta_\ell}S_B S_C B_{\theta_1}\ldots B_{\theta_\ell}\| \quad \text{(by commutation)}\\
&= \frac{1}{M^\ell}\sum_{\theta_1,\ldots,\theta_\ell\in\Theta}\|S_B S_C\| \quad \text{(unitaries preserve spectral norm)}\\
&\leq \epsilon \quad \text{(Lemma 5.5,)}
\end{aligned}
$$

as claimed. □

Corollary 5.7 (Bounding a "disagreement-regularized" S_BS_C)**.** *For any $\delta > 0$, we have:*

$$\left\|S_B(D+\delta\mathbb{I})^{-1}S_C\right\| \leq \epsilon/\delta. \tag{23}$$

Proof. First, note that since $D \succeq 0$ and $\delta > 0$, the inverse $(D+\delta\mathbb{I})^{-1}$ is well-defined, Hermitian, and positive-definite. The idea is to expand out $(D+\delta\mathbb{I})^{-1}$ as a power series. To this end:

$$
\begin{aligned}
D+\delta\mathbb{I} &= \frac{\mathbb{I}-(\mathbb{I}-2D)}{2}+\delta\mathbb{I}\\
&= \frac{1}{2}((1+2\delta)\mathbb{I}-(\mathbb{I}-2D))\\
&= \frac{1+2\delta}{2}\left(\mathbb{I}-\frac{\mathbb{I}-2D}{1+2\delta}\right).
\end{aligned}
$$

Remembering that $\mathbb{I}-2D$ is an average of Hermitian reflections $B_\theta C_\theta$, it follows that $\|\mathbb{I}-2D\| \leq 1 \Rightarrow \|(\mathbb{I}-2D)/(1+2\delta)\| < 1$. Therefore we can indeed compute the inverse with a power series as follows:

$$
\begin{aligned}
(D+\delta\mathbb{I})^{-1} &= \frac{2}{1+2\delta}\left(\mathbb{I}-\frac{\mathbb{I}-2D}{1+2\delta}\right)^{-1}\\
&= \frac{2}{1+2\delta}\sum_{\ell=0}^{\infty}\frac{(\mathbb{I}-2D)^\ell}{(1+2\delta)^\ell}\\
\Rightarrow \left\|S_B(D+\delta\mathbb{I})^{-1}S_C\right\| &\leq \frac{2}{1+2\delta}\sum_{\ell=0}^{\infty}\frac{\left\|S_B(\mathbb{I}-2D)^\ell S_C\right\|}{(1+2\delta)^\ell}\\
&\leq \frac{2}{1+2\delta}\sum_{\ell=0}^{\infty}\frac{\epsilon}{(1+2\delta)^\ell} \text{ (Corollary 5.6)}\\
&= \frac{2\epsilon}{1+2\delta}\cdot\frac{1}{1-\frac{1}{1+2\delta}}\\
&= \epsilon/\delta.
\end{aligned}
$$

□

5.4 Completing the Proof

The below proof makes use of Theorem 6.2, an isolated linear-algebraic lemma that we defer to Section 6.

Proof of Theorem 5.1. Lemma 5.4 gives $D \succeq \pm\frac{1}{2}(S_B - S_C)$, and Corollary 5.7 with $\delta = \sqrt{\epsilon}$ gives

$$\left\| S_B (D + \delta \mathbb{I})^{-1} S_C \right\| \leq \delta.$$

Applying Theorem 6.2 with $\gamma = \delta$ yields:

$$\frac{S_B + S_C}{2} \preceq D + \delta \mathbb{I}, \qquad \text{or equivalently} \qquad \frac{S_B + S_C}{2} - D \preceq \delta \mathbb{I}.$$

The exact game decomposition in Lemma 5.4 therefore implies

$$\Xi \preceq \left(\frac{1}{2} + \frac{\delta}{2} \right) \mathbb{I}. \tag{24}$$

Now applying Lemma 5.2 and recalling that $J(\Phi)$ is a density operator tells us that:

$$\omega = \operatorname{Tr}\left[\Xi J(\Phi)\right] \leq \frac{1}{2} + \frac{\delta}{2} = \frac{1}{2} + \frac{1}{2}\sqrt{\frac{\|\Gamma\|}{|\Theta|}},$$

establishing the theorem. □

Proof of Main Theorem 1. We instantiate the construction of Section 4 with the Pauli instantiation detailed therein. Correctness and efficiency have already been addressed. Finally, we invoke the security bound of Theorem 5.1 and use Lemma 3.4 to deduce that $\left\| \Gamma^{\text{Pauli}} \right\| \leq 2^n$. Plugging this in implies the conclusion. □

6 Key Linear-Algebraic Lemma

We isolate here the technical operator-theoretic workhorse (Theorem 6.2) of the security proof; see Section 2.4 for some motivation and Section 5 for details on how this appears in the security proof. Before that, we have a simple preliminary lemma. This is a well-known application of the Schur complement technique, but we include a proof for completeness.

Lemma 6.1 (PSD 2×2 block matrices)**.** *Let A, B, C be square Hermitian operators of the same dimension. Then:*

1. *If C is positive-definite, then $\begin{bmatrix} A & B \\ B & C \end{bmatrix}$ is PSD if and only if $A - BC^{-1}B$ is PSD.*
2. *The block matrix $\begin{bmatrix} A & B \\ B & A \end{bmatrix}$ is PSD if and only if $A - B$ and $A + B$ are both PSD.*

Proof. To prove Item 1, note that if we let $T = \begin{bmatrix} \mathbb{I} & 0 \\ C^{-1}B & \mathbb{I} \end{bmatrix}$, we have:

$$\begin{aligned} T^* \begin{bmatrix} A - BC^{-1}B & 0 \\ 0 & C \end{bmatrix} T &= \begin{bmatrix} \mathbb{I} & BC^{-1} \\ 0 & \mathbb{I} \end{bmatrix} \begin{bmatrix} A - BC^{-1}B & 0 \\ 0 & C \end{bmatrix} \begin{bmatrix} \mathbb{I} & 0 \\ C^{-1}B & \mathbb{I} \end{bmatrix} \\ &= \begin{bmatrix} \mathbb{I} & BC^{-1} \\ 0 & \mathbb{I} \end{bmatrix} \begin{bmatrix} A - BC^{-1}B & 0 \\ B & C \end{bmatrix} \end{aligned}$$

$$= \begin{bmatrix} A & B \\ B & C \end{bmatrix}.$$

Since T is invertible, it follows that $\begin{bmatrix} A & B \\ B & C \end{bmatrix}$ being PSD is equivalent to $\begin{bmatrix} A - BC^{-1}B & 0 \\ 0 & C \end{bmatrix}$ being PSD, which is in turn equivalent to $A - BC^{-1}B$ and C both being PSD. We are already assuming that C is positive-definite, so this is in turn equivalent to $A - BC^{-1}B$ being PSD.

Now we turn to Item 2. Note that $U = \frac{1}{\sqrt{2}} \begin{bmatrix} \mathbb{I} & \mathbb{I} \\ \mathbb{I} & -\mathbb{I} \end{bmatrix}$ is invertible. Conjugating by U, we have:

$$\begin{aligned} U \begin{bmatrix} A & B \\ B & A \end{bmatrix} U^* &= \frac{1}{2} \begin{bmatrix} \mathbb{I} & \mathbb{I} \\ \mathbb{I} & -\mathbb{I} \end{bmatrix} \begin{bmatrix} A & B \\ B & A \end{bmatrix} \begin{bmatrix} \mathbb{I} & \mathbb{I} \\ \mathbb{I} & -\mathbb{I} \end{bmatrix} \\ &= \frac{1}{2} \begin{bmatrix} \mathbb{I} & \mathbb{I} \\ \mathbb{I} & -\mathbb{I} \end{bmatrix} \begin{bmatrix} A+B & A-B \\ A+B & B-A \end{bmatrix} \\ &= \begin{bmatrix} A+B & 0 \\ 0 & A-B \end{bmatrix}. \end{aligned}$$

So $\begin{bmatrix} A & B \\ B & A \end{bmatrix}$ is PSD if and only if $\begin{bmatrix} A+B & 0 \\ 0 & A-B \end{bmatrix}$ is PSD, which is in turn true if and only if $A+B$ and $A-B$ are both PSD. □

Theorem 6.2 (Cloning advantage is bounded by "disagreement-regularized" $S_B S_C$)**.** *Let S_B, S_C, D be self-adjoint operators with $D \succeq \frac{S_B - S_C}{2}, \frac{S_C - S_B}{2}$. For reals $\delta, \gamma > 0$, assume the inequality:*

$$\left\| S_B (D + \delta \mathbb{I})^{-1} S_C \right\| \leq \gamma. \tag{25}$$

Then we have:

$$\frac{S_B + S_C}{2} - D \preceq \max(\delta, \gamma) \cdot \mathbb{I}. \tag{26}$$

Proof. The two positivity assumptions imply $D \succeq 0$, so $(D + \delta \mathbb{I})^{-1}$ is well-defined and positive definite. Let

$$K = S_B (D + \delta \mathbb{I})^{-1} S_C.$$

We know that $\|K\| \leq \gamma$ and therefore $\|K^*\| \leq \gamma$ also. It follows that we have:

$$\begin{aligned} \gamma &\geq \frac{1}{2} \|K + K^*\| \\ &= \frac{1}{2} \left\| S_B (D + \delta \mathbb{I})^{-1} S_C + S_C (D + \delta \mathbb{I})^{-1} S_B \right\| \\ &= \frac{1}{4} \left\| (S_B + S_C)(D + \delta \mathbb{I})^{-1} (S_B + S_C) - (S_B - S_C)(D + \delta \mathbb{I})^{-1} (S_B - S_C) \right\|, \end{aligned}$$

implying:

$$(S_B + S_C)(D + \delta \mathbb{I})^{-1} (S_B + S_C) \preceq (S_B - S_C)(D + \delta \mathbb{I})^{-1} (S_B - S_C) + 4\gamma \mathbb{I}. \tag{27}$$

Next, Item 2 of Lemma 6.1 tells us that

$$\begin{bmatrix} D & \frac{1}{2}(S_B - S_C) \\ \frac{1}{2}(S_B - S_C) & D \end{bmatrix}$$

is PSD. Consequently, we also have:

$$\begin{bmatrix} D & \frac{1}{2}(S_B - S_C) \\ \frac{1}{2}(S_B - S_C) & D + \delta\mathbb{I} \end{bmatrix} = \begin{bmatrix} D & \frac{1}{2}(S_B - S_C) \\ \frac{1}{2}(S_B - S_C) & D \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & \delta\mathbb{I} \end{bmatrix} \succeq 0.$$

Applying Item 1 of Lemma 6.1 to this matrix implies that:

$$\begin{aligned} D - \frac{1}{4}(S_B - S_C)(D + \delta\mathbb{I})^{-1}(S_B - S_C) \succeq 0 \\ \Rightarrow D + \max(\delta,\gamma)\cdot\mathbb{I} &\succeq \frac{1}{4}(S_B - S_C)(D + \delta\mathbb{I})^{-1}(S_B - S_C) + \max(\delta,\gamma)\cdot\mathbb{I} \\ &\succeq \frac{1}{4}(S_B + S_C)(D + \delta\mathbb{I})^{-1}(S_B + S_C) \text{ (plugging in (27))} \\ &\succeq \frac{1}{4}(S_B + S_C)(D + \max(\delta,\gamma)\cdot\mathbb{I})^{-1}(S_B + S_C). \end{aligned}$$

The last step above uses the fact that $D + \delta\mathbb{I} \preceq D + \max(\delta,\gamma)\cdot\mathbb{I}$ and both these operators are positive definite, so $(D + \max(\delta,\gamma)\cdot\mathbb{I})^{-1} \preceq (D + \delta\mathbb{I})^{-1}$. Now, Item 1 of Lemma 6.1 tells us that

$$\begin{bmatrix} D + \max(\delta,\gamma)\cdot\mathbb{I} & \frac{1}{2}(S_B + S_C) \\ \frac{1}{2}(S_B + S_C) & D + \max(\delta,\gamma)\cdot\mathbb{I} \end{bmatrix}$$

is PSD. Finally, Item 2 of Lemma 6.1 now tells us that $D + \max(\delta,\gamma)\cdot\mathbb{I} \succeq \frac{1}{2}(S_B + S_C)$, as desired. □

7 An Alternate Proof for the Haar Scheme

Here, we apply the techniques by [MST21, BCR25, PRV26] to show that the Haar scheme proposed by [BBC26a], though inefficient, also achieves security $1/2 + O(2^{-n/2})$. We prove this here in the interest of self-containment; we do not make any claim to originality in this section. The original proof by [BBC26a] showed security $1/2 + O(2^{-n/8})$.

Construction 2. *Fix $n \geq 1$ and put $d = 2^n$. Let $\mathfrak{U}$ be any compact subgroup of the d-dimensional unitary group.*

- *Key generation: sample U from the Haar measure on $\mathfrak{U}$.*
- *To encrypt $a \in \{0,1\}$, output*

$$\rho_{U,a} = U\left(|a\rangle\langle a| \otimes \frac{2}{d}\mathbb{I}_{d/2}\right)U^*. \tag{28}$$

- *To decrypt, apply U^* and measure the first qubit in the standard basis.*

To compare this with our scheme, note that our Pauli-based scheme in Section 4 can alternately be formulated in terms closer to Construction 2.

Lemma 7.1. *Assume Construction 1 is instantiated with the $4^n - 1$ non-identity Paulis. Then for every key $\theta \in \Theta_n$, there exists an n-qubit Clifford U_θ such that the encryption/decryption operations in Construction 2 for U_θ are identical to the encryption/decryption operations in Construction 1 for the key θ.*

Proof. The observation is that for any unitary U, we have:

$$\begin{aligned} U\left(|a\rangle\langle a| \otimes \frac{2}{d}\mathbb{I}_{d/2}\right)U^* &= U\left(\frac{\mathbb{I}+(-1)^a Z}{2} \otimes \frac{2}{d}\mathbb{I}_{d/2}\right)U^* \\ &= U\left(\frac{1}{d}\mathbb{I}_d + \frac{1}{d}(-1)^a(Z \otimes \mathbb{I}_{d/2})\right)U^* \\ &= \frac{1}{d}\left(\mathbb{I}_d + (-1)^a U(Z \otimes \mathbb{I}_{d/2})U^*\right). \end{aligned}$$

Since n-qubit Clifford group acts transitively on the non-identity Hermitian Paulis, there exists an n-qubit Clifford U_θ such that $U_\theta(Z \otimes \mathbb{I}_{d/2})U_\theta^* = P_\theta$. The conclusion follows. □

Theorem 7.2. *Let $\mathfrak{U}$ be any compact subgroup of the d-dimensional unitary group that contains the n-qubit Clifford group. Then Construction 2 instantiated with $\mathfrak{U}$ is also secure; any adversaries achieve joint cloning success probability at most*

$$\frac{1}{2} + \frac{1}{2}\sqrt{\frac{2^n}{4^n - 1}}.$$

(In particular, this holds when $\mathfrak{U}$ is the entire unitary group.)

Proof. Consider any adversary $(\mathsf{Cl}, \mathsf{B}, \mathsf{C})$ for Construction 2 instantiated with $\mathfrak{U}$, and assume that Bob and Charlie simultaneously guess correctly with probability ω. From these, we build an adversary $(\mathsf{Cl}', \mathsf{B}', \mathsf{C}')$, for Construction 1 instantiated with the Paulis. $(\mathsf{Cl}', \mathsf{B}', \mathsf{C}')$ have some unitary U hardcoded, that we will address at the end.

- Cl': when they receive the state ρ, run Cl on the state $U\rho U^*$ and forward the resulting bipartite state to B' and C'.
- B': once the Pauli key θ is revealed, reveal UU_θ as the key to B and output the guess produced by B.
- C': analogously for C.

First, note that the view of $(\mathsf{Cl}, \mathsf{B}, \mathsf{C})$ is as if Construction 2 has been instantiated with the key UU_θ; this is clear for Bob and Charlie, and the state received by Cl is:

$$U\rho U^* = U\left(U_\theta\left(|a\rangle\langle a| \otimes \frac{2}{d}\mathbb{I}_{d/2}\right)U_\theta^*\right)U^* = UU_\theta\left(|a\rangle\langle a| \otimes \frac{2}{d}\mathbb{I}_{d/2}\right)(UU_\theta)^*.$$

Bearing this in mind, we have the following chain of implications:

- Main Theorem 1 tells us that $(\mathsf{Cl}', \mathsf{B}', \mathsf{C}')$ with U hardcoded succeed with probability at most $\frac{1}{2} + \frac{1}{2}\sqrt{2^n/(4^n-1)}$.
- Equivalently, for every fixed U, $(\mathsf{Cl}, \mathsf{B}, \mathsf{C})$ succeed on the key ensemble $\{UU_\theta : \theta \leftarrow \Theta_n\}$ with probability at most $\frac{1}{2} + \frac{1}{2}\sqrt{2^n/(4^n-1)}$.
- Averaging over U now tells us that $(\mathsf{Cl}, \mathsf{B}, \mathsf{C})$ succeed on the key ensemble $\{UU_\theta : \theta \leftarrow \Theta_n, U \sim \mathrm{Haar}(\mathfrak{U})\}$ with probability at most $\frac{1}{2} + \frac{1}{2}\sqrt{2^n/(4^n-1)}$.
- Finally, Haar invariance tells us that this is exactly equivalent to $\omega \leq \frac{1}{2} + \frac{1}{2}\sqrt{2^n/(4^n-1)}$, as desired.

□

References

[AK21] Prabhanjan Ananth and Fatih Kaleoglu. Unclonable encryption, revisited. In Kobbi Nissim and Brent Waters, editors, *Theory of Cryptography - 19th International Conference, TCC 2021, Raleigh, NC, USA, November 8-11, 2021, Proceedings, Part I*, volume 13042 of *Lecture Notes in Computer Science*, pages 299–329. Springer, 2021. 3

[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*, pages 212–241, 2022. 2

[AKL23] Prabhanjan Ananth, Fatih Kaleoglu, and Qipeng Liu. Cloning games: A general framework for unclonable primitives. In Helena Handschuh and Anna Lysyanskaya, editors, *Advances in Cryptology - CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part V*, volume 14085 of *Lecture Notes in Computer Science*, pages 66–98. Springer, 2023. 2

[AKY25] Prabhanjan Ananth, Fatih Kaleoglu, and Henry Yuen. Simultaneous Haar indistinguishability with applications to unclonable cryptography. In Raghu Meka, editor, *16th Innovations in Theoretical Computer Science Conference, ITCS 2025, Columbia University, New York, NY, USA, January 7-10, 2025*, volume 325 of *LIPIcs*, pages 7:1–7:23. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2025. 2

[AS26] Prabhanjan Ananth and Amit Sahai. Unconditional unclonable encryption, 2026. 3

[BBC26a] Archishna Bhattacharyya, Anne Broadbent, and Eric Culf. The uncloneable bit exists, 2026. 2, 3, 17

[BBC+26b] Pierre Botteron, Anne Broadbent, Eric Culf, Ion Nechita, Clément Pellegrini, and Denis Rochette. Towards unconditional uncloneable encryption. *Quantum*, 10:2157, 2026. 2, 3, 5

[BC26] Archishna Bhattacharyya and Eric Culf. Uncloneable encryption from decoupling. *Nature Physics*, pages 1–4, 2026. 2

[BCR25] Anne Broadbent, Eric Culf, and Denis Rochette. Optimal untelegraphable encryption and implications for uncloneable encryption, 2025. 2, 3, 17

[BG26a] James Bartusek and Eli Goldin. A note on boosting uncloneable encryption in Microcrypt, 2026. 3

[BG26b] James Bartusek and Eli Goldin. Unclonable encryption in the Haar random oracle model. *CoRR*, abs/2603.11437, 2026. 2

[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)*, volume 158 of *LIPIcs*, pages 4:1–4:22, 2020. 1, 2, 4, 10

[Got03] Daniel Gottesman. Uncloneable encryption. *Quantum Information and Computation*, 3(6):581–602, 2003. 1

[HKNY24] Taiga Hiroka, Fuyuki Kitagawa, Ryo Nishimaki, and Takashi Yamakawa. Robust combiners and universal constructions for quantum cryptography. In *Theory of Cryptography Conference*, pages 126–158. Springer, 2024. 3

[MST21] Christian Majenz, Christian Schaffner, and Mehrdad Tahmasbi. Limitations on uncloneable encryption and simultaneous one-way-to-hiding, 2021. 2, 3, 17

[NC16] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information (10th Anniversary edition)*. Cambridge University Press, 2016. 4

[PRV26] Alexander Poremba, Seyoon Ragavan, and Vinod Vaikuntanathan. Cloning games, black holes and cryptography. In *17th Innovations in Theoretical Computer Science Conference (ITCS 2026)*, LIPIcs, 2026. 2, 3, 8, 17

[TFKW13] Marco Tomamichel, Serge Fehr, Jędrzej Kaniewski, and Stephanie Wehner. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. *New Journal of Physics*, 15(10):103002, 2013. 2, 10

[Wat18] John Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018. 4