Existential Unforgeability in Quantum Authentication From Quantum Physical Unclonable Functions Based on Random von Neumann Measurement

Soham Ghosh*, Vladlen Galetsky*, Pol Julià Farré†, Christian Deppe†, Roberto Ferrara*, Holger Boche*
*Technical University of Munich
†Technical University of Braunschweig
(Dated: October 2, 2024)

Physical Unclonable Functions (PUFs) leverage inherent, non-clonable physical randomness to generate unique input-output pairs, serving as secure fingerprints for cryptographic protocols like authentication. Quantum PUFs (QPUFs) extend this concept by using quantum states as input-output pairs, offering advantages over classical PUFs, such as challenge reusability via public channels and eliminating the need for trusted parties due to the no-cloning theorem. Recent literature introduced a generalized mathematical framework for QPUFs, demonstrating that no random unitary QPUF can achieve existential unforgeability against Quantum Polynomial Time (QPT) adversaries. Additionally, we introduce a second model where the QPUF functions as a nonunitary quantum channel, which also guarantees existential unforgeability. These are the first models in the literature to demonstrate such a high level of provable security. Finally, we show that the Quantum Phase Estimation (QPE) protocol, applied to a Haar random unitary, serves as an approximate implementation of the second type of QPUF by approximating a von Neumann measurement on the unitary's eigenbasis.

I. INTRODUCTION

A. Physical Unclonable Function (PUF):

Physical Unclonable Functions (PUF) are hardware devices with the assumption of having randomness which is inherently both physical and unclonable. This results in each PUF having a unique behaviour that produces different outputs (responses) over the same set of inputs (challenges). The assumption is a theoretical abstraction of the idea that some unpredictable manufacturing variations can create devices for which replicating their behaviour is more easily done by simply querying (collecting challenges and responses) and learning about the device rather than trying to learn about the underlying manufacturing variations (sometimes destructively). This assumption is not only valid but also cost-effective, capitalizing on the inherent unpredictability in real-world manufacturing processes. In general, the manufacturing variations can be measured as a certain amount of randomness in bits or qubits that makes the amount of queries needed to learn about the PUF device exponential in the size of the input bit or qubit space, making the PUF device highly suitable for security schemes like authentication or encryption. The queries (often called *Challenge-Response pairs* or CRPs [1]) can be stored as smaller unique fingerprints.

This assumption is not only valid but also cost-effective, capitalizing on the inherent unpredictability in real-world manufacturing processes. Manufacturing variations used to create PUFs encompass diverse examples, including gate delays within integrated circuits[2, 3] and imperfections within optical crystals[2–4].

1. *Classical PUF (CPUF):*

PUFs being a very efficient security solution have been richly studied classically for years. A full overview of various classical constructions of PUFs can be obtained here [3]. Although CPUFs are widely used today, their constructions possess three major shortcomings:

- Trusted Party: Classical bits are clonable. Thus, the party which creates and/or stores the CRPs in any security scheme becomes a trusted party posing potential threats to privacy leakage.
- Challenge reusability: Again, as classical bits are clonable, no data point in the CRPs can be reused after communication via a public channel, as this would allow an eavesdropper to simply reuse the eavesdropped responses.
- Security: Most of CPUFs constructions are heuristic, having no provable security.

2. *Quantum PUF (QPUF)*

A Quantum PUF (QPUF) can simply be thought of as a device that produces Quantum CRPs, having quantum states as data points. While the unclonability of the PUF protects the whole device in quantum and classical devices alike, in the CPUF past queries can be cloned. In contrast, the quantum no-cloning theorem ensures that even the single queries of the QPUF cannot be cloned. Moreover, performing quantum state tomography on a specific query would also require an exponential, in the size of the considered quantum system, number of identical queries. Thus the issue of *trusted party* holding a challenge and *challenge reusability* can be solved with QPUFs.

A precursor of QPUFs [5] provided such security only against classical adversaries. Recent work [1] introduced a mathematical framework that defines QPUFs with provable security also against quantum adversaries. Since then, QPUFs have seen increased interest [6–10].

In [1] it was proved that a QPUF can only be an approximation of a Haar (uniform) random unitary channel if and only if the domain and range of the QPUF channel are the same. They established three hierarchical security notions: *Quantum Exponential Unforgeability, Quantum Existential Unforgeability* and *Quantum Selective Unforgeability*, arranged in descending order of security strength. Subsequently, they explicitly proved that their model inherently lacks both exponential and existential unforgeability. However, they proved that their model does exhibit selective unforgeability, a property that is often highly suitable for numerous practical applications.

B. Our Contributions

Quantum exponential unforgeability is a security measure defined for any adversary possessing the power of querying and possessing exponentially many data points. However, this level of security can never be achieved *realistically* by any classical or quantum PUF as, if an exponential amount of queries were available, the adversary would be able to perform efficient state tomography on the PUF CRPs or process tomography on the PUF channel.

However, both Existential and Selective unforgeability are security measures against a Quantum Polynomial Time adversary, which is more plausible to be required. Since the authors in [1] proved that no Haar random unitary channel can provide Quantum Existential Unforgeability, the only way to achieve that level of security would be to introduce non-unitarity in the QPUF construction.

A simple way to construct such a non-unitary channel (quantum process) is to combine measurements with unitary evolutions. This approach is without loss of generality, as any quantum channel can be thought of as a measurement channel with a post measurement state, where some of the classical information from the measurement is lost. Thus, we modelled our QPUF using a general quantum instrument which performs a measurement on a Haar random basis [11]. The QPUF performs a von Neumann measurement on an input quantum state but the measurement basis is rotated to some random basis state using a Haar random unitary [11]. The measurement and the random rotation together constitute our QPUF and hence it is inherently a non-unitary quantum process. In short, we are proposing the idea that measurements in a QPUF can increase the security achievable in schemes using the aforementioned QPUF. Intuitively, the measurement helps because it collapses the quantum state of any adversary attempting to use the QPUF in a way that was not intended, while not affecting the quantum state of the intended users.

We prove the main result that our QPUF based on a Haar random von Neumann measurement possesses Quantum Existential Unforgeability. With this we introduce the first ever model for a QPUF that has such high level of provable security.

For the implementation of an ideal QPUF we propose two device models, each introducing its own limitation for a practical realization:

- A random measurement can be approximated by the phase estimation protocol [12] on a Haar unitary U. The problem with this model is that it assumes the device can perform CU an exponential number of times with respect to the number of input qubits.

- A random measurement can be obtained by a standard basis measurement of the target state after it has been passed through a generalized controlled NOT gate with the control basis rotated by a Haar random unitary U onto a random basis. This model assumes that the device can perform the inverse of a random unitary. Although there are known algorithms [13–18] for performing the inverse of a given unknown unitary, all of them have exponential gate cost complexity.

Such limitations would have to be addressed when designing practical realisations of QPUFs. We have discussed these limitations in details in Section IV and proposed possible research directions in order to address them.

Another model proposition of ours follows by noticing that, in the case of Selective Unforgeability [1], the security comes from the fact that the verifier uses additional randomness apart from the QPUF to select their queries for the QPUF. This weakens the security notion, as achieving perfect uniform randomness is challenging in practice and incurs additional costs. Therefore, we propose to obtain this selection of query states via measurements which are natural sources of randomness according to the laws of quantum mechanics. Namely, the verifier uses the Bell state

$$\left|\Phi^+\right\rangle \equiv \frac{1}{\sqrt{D}} \sum_{i \in \mathbb{Z}_D} |i\rangle \otimes |i\rangle \tag{1}$$

and applies the QPUF unitary U on one half of the state and leaves the other half unchanged. As a result, they obtain the state,

$$\frac{1}{\sqrt{D}} \sum_{i \in \mathbb{Z}_D} |i\rangle \otimes U\,|i\rangle \equiv |Q\rangle \tag{2}$$

The verifier stores this resulting state $|Q\rangle$ and returns the QPUF U to the prover. During verification, the verifier measures the unchanged part of the state to get the outcome i and corresponding basis state $U\,|i\rangle$ on the unmeasured half. The verifier then sends the computational basis state $|i\rangle$ to the prover, who applies their QPUF to it and returns the response. Finally, the verifier checks the match between the remaining half of the Bell state and the response using a SWAP test [19]. As shown in [19], the error probability ϵ of the SWAP test can be brought down to any desired amount by running M instances of the SWAP test circuit where $M \propto \log\left(\frac{1}{\epsilon}\right)$. Security in this model arises from the fact that, prior to measurement, even the verifier has no knowledge of which basis state will be selected. This forces the adversary to guess the correct basis state, which is a 1-dimensional subspace of the Hilbert space—a set with measure $\frac{1}{\text{dimension of the Hilbert Space}}$. Typically for n-qubits the dimension will be 2^n. As a result, the probability of the adversary guessing correctly is extremely low.

Using the additional entanglement from Bell states is efficient and not more costly than previous approaches for the following reasons:

- The verifier stores both halves of the Bell state locally, making it easier to maintain entanglement in practical applications.
- In previous models, states produced by applying Haar random unitaries are stored. Since Haar random unitaries naturally create highly entangled states, the process already involves managing such states. Therefore, our proposal does not add any extra cost in comparison.

C. Future Work

Being these new QPUF models, there are several directions for future work that needs to be investigated:

- As mentioned earlier, the methods of implementing a random measurement through a random measurement channel is problematic for a realistic implementation. Finding more realistic implementation of the random measurement QPUF is thus an important open question.
- Creating a manufacturing process that produces Haar or close-to-Haar unclonable unitaries might be impossible. We considered the Haar-unitary model as, just the simplest theoretical proof of concept showing that unforgeability can be achieved. For practical application, more realistic unitary distributions still allowing for a theoretical security proof need to be found.
- We have considered only noiseless PUFs, thus cost of dealing with noise in this QPUF still needs to be investigated.

Finally, we highlight that QPUFs are advantageous over competing schemes like '*Quantum Key Distribution* (QKD)'[20, 21] and '*Quantum Money*' [22, 23]. In contrast to our QPUF model, a fundamental requirement in Quantum Money and QKD based schemes is that the classical information about the measurement basis needs to be stored **secretly** by the verifier. This makes them a '*trusted party*' in the security scheme, opening avenues for possible privacy leakage.

II. NOTATION AND PRELIMINARIES

We denote random variables with uppercase letters (e.g. X) and for pure quantum states we follow the Dirac bra-ket (e.g. $|\psi\rangle$) notation. Lower case Greek letters (e.g. ρ) are used for labelling density operators.

The trace distance [24],[25] between two density matrices ρ and σ is denoted as $0 \leq D(\rho, \sigma) \leq 1$. The uppercase Greek letter Λ is used to denote a completely positive trace preserving (CPTP) map or quantum channel [24],[25]. The diamond norm distance [25] between two such quantum channels Λ_1 and Λ_2 is denoted as $||\Lambda_1 - \Lambda_2||_\diamond$.

negl(λ) denotes a negligible function of lambda that decays exponentially to 0 with increasing values of λ, e.g. $\frac{1}{2^\lambda}$ is a negligible function of λ.

For any integer D, we define the set $\mathbb{Z}_D$ as follows:

$$\mathbb{Z}_D \coloneqq [0, \cdots, D-1]\,. \tag{3}$$

A. Computational Security

In contrast to the information-theoretic concept of 'perfect secrecy' [26], 'computational security' [26] considers the limitations on the computational power of the adversary and also permits a negligible probability of success for the adversary in breaching the security scheme. Perfect secrecy schemes do not put any restrictions on the computational power of an adversary and also do not allow for any non-zero probability of success for the adversary in breaching the scheme, even with *unlimited computational power*! These two relaxations make computational security schemes practical and feasible. Hence, in our analysis we would also opt for this approach.

1. Computational Security Parameter

Any cryptographic scheme can be conceptualized as a sequence of problems, and breaching the scheme entails solving this sequence. The '*computational security parameter*' [26] is an integer valued parameter, denoted by the Greek letter 'λ' and often visualised as a bitstring of ones $\mathbf{1}^\lambda$, which serves to parameterize the spacial and/or time complexity of the problems within a cryptographic scheme. In most applications, such as key or token-based schemes, the security parameter can be perceived as the length of the input bitstrings to the key or token generation protocol. This parameter also characterizes the computational capabilities of both the trusted party and the adversary.

For a cryptographic scheme to achieve computational security, a fundamental requirement is that the complexity of the problems underlying the scheme should *not* belong to the *polynomial class* [26], while the computational power of both the trusted party and the adversary should fall within the *polynomial class* [26]. The general proof strategy for establishing computational security involves calculating or bounding the probability of success for the adversary in breaching the scheme as a function of the security parameter λ and demonstrating an exponential decay of this probability with the scaling of the parameter. This shows the practicality of this approach by providing a clear understanding of how security scales in relation to the scaling of resources.

B. Haar Random von Neumann Measurement Channel

For a D-dimensional Hilbert space $\mathbb{C}^D$, the computational basis $\{|i\rangle\}_{i=0}^{D-1}$ forms a complete basis set. It follows trivially that for any Haar random unitary U [11], we can obtain a complete basis set $\{U|i\rangle\}_{i=0}^{D-1}$. The measurement channel for measurement on such a basis is obtained from the quantum instrument [25],

$$\Lambda_U(\rho) = \sum_{i\in\mathbb{Z}_D} |i\rangle\langle i| \otimes \Pi_i^U \rho \Pi_i^{U\dagger}, \tag{4}$$

where the projection operators Π_i^U are defined as

$$\Pi_i^U \equiv U|i\rangle\langle i| U^\dagger. \tag{5}$$

When tracing the first system, the quantum instrument becomes a measurement channel described by the Projection Valued Measures (PVMs) [25] $\{\Pi_i^U\}$. The post-measurement state after getting a measurement outcome i becomes

$$\Pi_i^U \rho \Pi_i^{U\dagger} = U|i\rangle\langle i| U^\dagger, \tag{6}$$

where

$$p_i = \mathrm{Tr}\left[\Pi_i^U \rho\right] \tag{7}$$

is the outcome probability for a measurement outcome i.

C. Quantum Phase Estimation as an Approximate von Neumann Measurement

We highlight the preliminaries of Quantum Phase Estimation Algorithm [12] to show that it can be used as a model to approximate a Haar random von Neumann measurement. As a result, in Section III G 2 we will explain how it can be used to derive a quantum circuit based implementation for our proposed QPUF.

1. Phase Measurement

Let U be any unitary. While U is not Hermitian, it is still normal, meaning that U is unitarily diagonalizable (equivalently, its Hermitian and anti-Hermitian parts commute) and, thus, it has a spectral decomposition and defines a quantum measurement. The eigenvalues of a unitary are complex roots of unity (elements of the complex unit circle). Equivalently, we can define the measurement of the Hermitian operator H such that $U = e^{iH}$, namely the measurement of $-i\log U$. This changes the measurement outcomes (which can be done with classical processing, since the outcomes are classical values), but preserves the measurement projectors. For convenience, we choose a dimension d and we consider the measurement of the hermitian operator

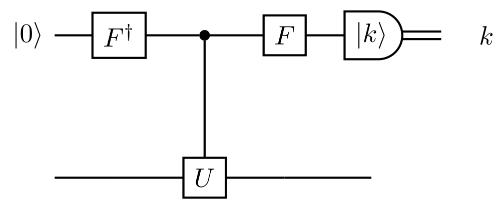
$$\phi := \frac{\log U}{i\frac{2\pi}{d}},$$

with eigenvalues fulfilling $\phi_i \in [0, d[$ when we write all the eigenvalues of U in the form $e^{i\frac{2\pi}{d}\phi}$. Below, d will become both the dimension of an ancilla system and the amount of precision we use to estimate each of the complex phases of the eigenvalues of U.

2. Phase Estimation Algorithm

Let d be the dimension of an additional quantum system $\mathbb{C}^d$, ancillary to the system of U, and let F and $F^\dagger$ be the Fourier Transform and the inverse Fourier Transform respectively in this d-dimensional system. The phase-estimation [12] circuit for U with outcomes in $\mathbb{Z}_d$ is:

$U_k =$



(8)

where CU is the controlled unitary defined as

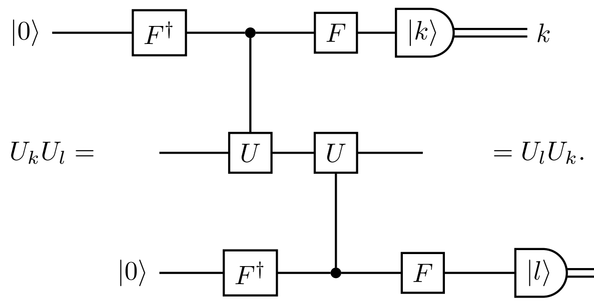
$$CU = \sum_{k\in\mathbb{Z}_d} |k\rangle\langle k| \otimes U^k.$$

Note that we are making an abuse of notation here, as we are not performing a standard controlled unitary. This circuit also corresponds to the d Kraus operators U_k of the quantum instrument

$$\Lambda_U^{QPE}(\rho) = \sum_{k\in\mathbb{Z}_d} |k\rangle\langle k| \otimes U_k \rho U_k^\dagger \tag{9}$$

produced by the circuit.

Notice, that repetitions of this algorithm always commute, independently of d or U. Indeed, all Kraus operators and, thus, also any two instances of applying Λ_U^{QPE}, commute with each other because they overlap only on the target where the various powers of U commute, as shown in the circuit below



This property will simplify later the analysis of the QPUF in Section III G 2. Notice, also, that the same argument gives that the U_k's commute with U itself, meaning U_k are also diagonal in the same basis. A consequence of this is that the conditional un-normalized states

$$U_{k_n} \dots U_{k_0} |\psi\rangle$$

and the probabilities

$$\begin{aligned} p_{k_0 \dots k_n} &= \langle\psi| U_{k_0}^\dagger \dots U_{k_n}^\dagger U_{k_n} \dots U_{k_0} |\psi\rangle \\ &= \langle\psi| \left(U_{k_n}^\dagger U_{k_n}\right) \dots \left(U_{k_0}^\dagger U_{k_0}\right) |\psi\rangle \end{aligned}$$

are all symmetric in $k_0, \dots, k_n$.

3. Phase Estimation Operators

We write the unitary U and the Fourier transform F as

$$U = \sum_{i \in \mathbb{Z}_D} e^{i\frac{2\pi}{d}\phi_i} |\phi_i\rangle\langle\phi_i| \quad F = \frac{1}{\sqrt{d}} \sum_{x,y \in \mathbb{Z}_d} e^{-i\frac{2\pi}{d}xy} |x\rangle\langle y| , \tag{10}$$

where d is the dimension of the ancillary control system which F acts on, D is the dimension of the target system which U acts on, and $|\phi_i\rangle$ are the eigenstates of U, with corresponding eigenvalue $e^{i\frac{2\pi}{d}\phi_i}$, where each $\phi_i \in [0, d[$ is *unknown.* Notice how we use d and not D to define each ϕ_i, which is due to the fact that the precision of the phase estimation is defined by the ancillary control system and not the original target system.
The explicit form of the Kraus operators in the circuit of [Eq. (8)] is

$$U_k = \frac{1}{d}\big(\langle k| F \otimes \mathbb{1}\big) CU \big(F^\dagger |0\rangle \otimes \mathbb{1}\big) \tag{11}$$

$$= \frac{1}{d} \sum_{x \in \mathbb{Z}_d} \langle k| F |x\rangle \cdot U^x = \frac{1}{d} \sum_{x \in \mathbb{Z}_d} e^{-i\frac{2\pi}{d}kx} \cdot U^x \tag{12}$$

$$= \sum_{j \in \mathbb{Z}_d} \left(\frac{1}{d} \sum_{x \in \mathbb{Z}_d} e^{i\frac{2\pi}{d}(\phi_j - k)x} \right) |\phi_j\rangle\langle\phi_j| . \tag{13}$$

When ϕ_j is an integer, the geometric series in parenthesis is the Kronecker delta δ_{k,ϕ_j}. In all other cases (in general whenever $\phi_j - k \neq 0$), we have

$$\begin{aligned} \sum_{x \in \mathbb{Z}_d} e^{i\frac{2\pi}{d}(\phi_j - k)x} &= \frac{1 - e^{i2\pi(\phi_j - k)}}{1 - e^{i\frac{2\pi}{d}(\phi_j - k)}} \qquad (14) \\ &= \frac{e^{i\pi(\phi_j - k)}}{e^{i\frac{\pi}{d}(\phi_j - k)}} \frac{\sin(\pi(\phi_j - k))}{\sin\left(\frac{\pi}{d}(\phi_j - k)\right)} . \end{aligned}$$

When divided by d, this term is an approximation of the normalized sinc function, if d is sufficiently large.

Namely, we can define (with a rescaling of the input by π for convenience)

$$\mathrm{sins}_d(x) := \begin{cases} 1 & x = 0 \\ \frac{\sin(\pi x)}{d \sin\left(\frac{\pi}{d} x\right)} & x \neq 0 \end{cases} \quad \mathrm{sinc}(x) := \begin{cases} 1 & x = 0 \\ \frac{\sin(\pi x)}{\pi x} & x \neq 0, \end{cases} \tag{15}$$

and have the following bound, coming from $\sin x \leq x$:

$$\mathrm{sins}_d(x) \geq \mathrm{sinc}(x).$$

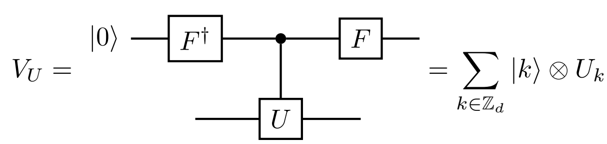
Notice that both functions are zero when x is a non-zero integer and that sins_d is symmetric just like sinc. We can finally write the Kraus operators as

$$U_k = \sum_{j \in \mathbb{Z}_D} \frac{e^{i\pi(\phi_j - k)}}{e^{i\frac{\pi}{d}(\phi_j - k)}} \mathrm{sins}_d(\phi_j - k) |\phi_j\rangle\langle\phi_j| , \tag{16}$$

which *are diagonal in the eigenbasis of* U, as we anticipated in Section II C 2. When tracing the first quantum system, the quantum instrument Λ_U becomes a measurement channel with POVM [25] elements

$$M_k := U_k^\dagger U_k = \sum_{j \in \mathbb{Z}_D} \mathrm{sins}_d^2(\phi_j - k) |\phi_j\rangle\langle\phi_j| . \tag{17}$$

Notice that, while sins_d has period $2d$, sins_d^2 has period d, which is why the sum in $\sum_k M_k = \mathbb{1}$ can be taken in any contiguous set of d integers, namely in $N, N+1, ..., N+d-1$ for any integer N. For completeness, we note that the isometry V_U before the measurement is given by



(18)

$$= \sum_{k \in \mathbb{Z}_d,\ j \in \mathbb{Z}_D} \frac{e^{i\pi(\phi_j - k)}}{e^{i\frac{\pi}{d}(\phi_j - k)}} \mathrm{sins}_d(\phi_j - k) |k\rangle \otimes |\phi_j\rangle\langle\phi_j| . \tag{19}$$

4. Phase Estimation Outcome

In the special case when each ϕ_i is an integer value, namely when the eigenvalues of U are integer powers of $e^{i\frac{2\pi}{d}}$, then the phase estimation exactly produces the measurement defined by U with preservation of the post measurement state. Thus, it becomes equal to a von Neumann measurement on the eigenbasis of U. For all other cases, the outcome will be a probabilistic and integer estimation of the quantity ϕ_i.

It can be now intuitively understood why repeated phase estimations commute. Indeed, when Λ_U^{QPE} is exactly the measurement defined by U then it is clear that different applications of Λ_U^{QPE} must commute, since they would be equivalent to different measurements of the same observable. The commutativity statement in the previous section says that commutativity holds in general even for approximate measurements.

Notice that phase estimation is a fully general model of measurements, because for any observable (Hermitian) H we can create the following unitary

$$e^{i\frac{H}{\|H\|_\infty}},$$

which has the exact same spectral projectors as H (normalization by $\|H\|_\infty$ is to guarantee that no phases loop around $\pm\pi$. Any constant above $\|H\|_\infty/\pi$ would work).

III. RESULTS

In this section, we describe our results.

A. Measurement based QPUF (MB-QPUF) scheme

The protocol can be described in the framework of standard QPUF/PUF based protocols [1], namely, it has two phases, one where the verifier collects some data from the QPUF which they use to verify the identity of the prover.

1. *Verifier's Query Phase*

The data collection of the verifier is described in the following steps:

- The verifier initialises N maximally entangled states on two $D-$dimensional systems labelled A, B, $|\Phi^+\rangle_{AB}$, where,

$$\left|\Phi^+\right\rangle_{AB} \equiv \frac{1}{\sqrt{D}} \sum_{i\in\mathbb{Z}_D} |i\rangle_A \otimes |i\rangle_B . \quad (20)$$

- Then they apply the QPUF U locally on system B of all the maximally entangled states to obtain the following states,

$$(\mathbb{I}\otimes U)\left|\Phi^+\right\rangle_{AB} = \frac{1}{\sqrt{D}} \sum_{i\in\mathbb{Z}_D} |i\rangle_A \otimes U\,|i\rangle_B \quad (21)$$

- Finally they store these states and handover the QPUF U to the prover.

2. *Prover's Verification*

The verification process occurs in the following steps:

- When the prover wishes to verify their identity, the verifier measures the system label A for all the N maximally entangled states, obtaining N measurement outcomes $\{m_i\}_{i\in\mathbb{Z}_N}$. This measurement will make the states in the other systems $\{U\,|m_i\rangle\}$.

- The verifier then sends the computational basis states corresponding to the obtained measurement outcomes m_i , $|m_i\rangle$ to the prover.

- The prover then simply receives these states and applies their QPUF on these states and sends back response states $\{|\psi\rangle_{m_i}\}$ to the verifier.

- The verifier then performs the SWAP Test [19] on all pairs $U\,|m_i\rangle$ and $|\psi\rangle_{m_i}$. If the Swap test is passed for all states, the verification is accepted or else it is rejected.

3. *Error and Security Bounds*

As shown in [19], the error probability ϵ of the SWAP test can be brought down to any desired amount by running M instances of the SWAP test circuit where $M \propto \log(\frac{1}{\epsilon})$.

Let there be M runs of the SWAP circuit for each response state. From *Theorem 2 (SWAP soundness)*, Page 12:12 of [19], it is straightforward to see that for any adversary attempting to guess the correct state for all the N states is atmost $\mathcal{O}(\frac{1}{2^{NM}})$. Choosing $\lambda = NM$ as the security parameter the probability of adversarial succeess is negligible in λ. This ensures the security of our proposed scheme.

B. Ideal QPUF

In this section we define a new model for QPUFs, namely we construct a non-unitary quantum channel which would serve as a QPUF.

1. *Hardware Requirements*

In accordance with the framework in [1], we redefine the essential hardware requirements for the Haar random von Neumann measurement channel to be considered an "*ideal QPUF*".

Definition 1 (Ideal QPUF)**.** *Any quantum instrument* Λ_U *in Eq.* (4)*, becomes an* 'ideal QPUF' *if it satisfies the following hardware requirements for some security parameter* λ*:*

- ***Unknownness:*** *The Kraus operators* $\{U|i\rangle\langle i|U^\dagger\}_{i\in\mathbb{Z}_D}$ *for the channel* Λ_U *remain unknown.*

- ***Collision-Resistance:*** *The probability of having any two post-measurement pure states* $|\psi_i\rangle$ *and* $|\psi_j\rangle$ *corresponding to different measurement outcomes* $i \neq j$ *being furthest apart in trace distance satisfies*

$$\Pr\left[D(|\psi_i\rangle\langle\psi_i|, |\psi_j\rangle\langle\psi_j|) = 1\right] \geq 1 - \mathrm{negl}(\lambda) \tag{22}$$

- ***Robustness:***
  The probability of having any two post-measurement pure states $|\psi_i\rangle$ *and* $|\psi_j\rangle$ *corresponding to the same measurement outcomes* $i = j$ *being equal satisfies*

$$\Pr\left[D(|\psi_i\rangle\langle\psi_i|, |\psi_j\rangle\langle\psi_j|) = 0\right] \geq 1 - \mathrm{negl}(\lambda). \tag{23}$$

- ***Uniqueness:***
  The probability of any two distinct QPUF instruments, Λ_{U_i} *and* Λ_{U_j}*, being furthest apart in diamond norm*

$$\Pr\left[||\Lambda_{U_i} - \Lambda_{U_j}||_\diamond = 2\right] \geq 1 - \mathrm{negl}(\lambda), \tag{24}$$

  where 2 *is the maximum value in diamond norm distance.*

C. Query structure for ideal QPUF

For any collection of input pure states $\mathcal{D} := \{|\psi_i\rangle\}$,we define the query set of the *ideal QPUF* Λ_U as

$$Q := \{|\psi_i\rangle, q_i, U|q_i\rangle\}, \tag{25}$$

where $q_i \in \mathbb{Z}_D$ is the measurement outcome correspons-ding to the i^{th} input state $|\psi_i\rangle$ and $U|q_i\rangle$ is the post-measurement state obtained after measurement through the instrument Λ_U. We denote the computational basis by $|q_i\rangle$ for the classical label q_i. As mentioned earlier Eq. (4), measuring with Λ_U yields the basis $U|q_i\rangle$ for the classical outcome q_i, instead of $|q_i\rangle$. It is evident that $|Q| = |\mathcal{D}|$. This set Q being made of the CRPs of *ideal* QPUF Λ_U provides a unique fingerprint.

D. Ideal Authentication Protocol

1. Token Generation Protocol

In Q, each state $U|q_i\rangle$ serves as a secure quantum token with the classical value q_i as its identifier, which is kept public as shown in [Fig. 1] (red). Each token in Q is sent to different authentic parties, who store them in their quantum memory. Notice that, since $U|q_i\rangle$ is a quantum state and q_i is public, there is no *trusted party* in the protocol.

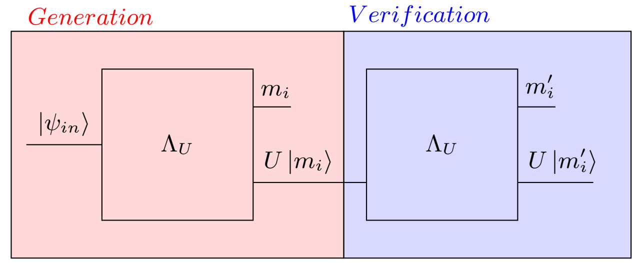


FIG. 1. Generation (in red) and verification (in blue) methods for CRPs. Verification is successful if $q_i = q_i'$ and it is otherwise failed.

2. Token Verification Protocol

Upon verification, the token state $U|q_i\rangle$ is requested back by the verifier. The state is then used as input state for the *ideal QPUF* channel, Λ_U in Definition 1, to obtain the pair of measurement outcome and post-measurement state as $(q_i', U|q_i'\rangle)$ after measurement as shown in [Fig. 1](blue). If $q_i = q_i'$, then the verification is successful and the post-measurement state $U|q_i'\rangle$ is sent back to the authentic party for a future verification. Otherwise, verification is failed/rejected.

E. Unforgeability Notion for an Ideal Quantum PUF

For any *ideal QPUF*, the concept of unforgeability lies in the difficulty of replicating its set of queries (CRPs) by any adversary having query access to it.

Let $\mathcal{A}$ be an arbitrary adversary having query database $Q_\mathcal{A}$. From Eq. (25), the structure of $Q_\mathcal{A}$ will be,

$$Q_\mathcal{A} := \{|\psi_i^\mathcal{A}\rangle, q_i^\mathcal{A}, U|q_i^\mathcal{A}\rangle\}, \tag{26}$$

where $\{|\psi_i^\mathcal{A}\rangle\}$ are input states initialised by the adversary for making a query. Then, for a security parameter λ, the adversary is termed as '*Quantum Exponential Time* (QET)' if $|Q_\mathcal{A}| = \exp(\lambda)$, and '*Quantum Polynomial Time* (QPT)' if $|Q_\mathcal{A}| = \mathrm{poly}(\lambda)$. Consider an arbitrary measurement outcome $q \notin Q_\mathcal{A}$. Based on the information gained from the query database, let the adversary produce an arbitrary pure state $|\psi_\mathcal{A}\rangle$ to pass QPUF verification for the outcome q and let the probability of passing, for the adversary, be P_q. Following [Eq. (7)], we can write it as

$$P_q = \mathrm{Tr}\left[\Pi_q^U |\psi_\mathcal{A}\rangle\langle\psi_\mathcal{A}|\right]. \tag{27}$$

Since U is a random variable, P_q is also a random variable. Considering the storage and processing capabilities of the adversary, we can now proceed to define two notions of unforgeability.

Definition 2 (Quantum Exponential Unforgeability)**.** *Let* $|Q_{\mathcal{A}}| = \exp(\lambda)$*, where* λ *is the security parameter and* $Q_{\mathcal{A}}$ *is the query database of an arbitrary adversary, denoted as* $\mathcal{A}$*. If* $\forall$ *classical measurement outcomes* $q \notin Q_{\mathcal{A}}$ *we have*

$$E[P_q] = \mathrm{negl}(\lambda), \tag{28}$$

then the QPUF is deemed exponentially unforgeable.

Definition 3 (Quantum Existential Unforgeability)**.** *Let* $|Q_{\mathcal{A}}| = \mathrm{poly}(\lambda)$*, where* λ *is the security parameter and* $Q_{\mathcal{A}}$ *is the query database of an arbitrary adversary, denoted as* $\mathcal{A}$*. If* $\forall$ *classical measurement outcomes* $q \notin Q_{\mathcal{A}}$ *we have*

$$E[P_q] = \mathrm{negl}(\lambda), \tag{29}$$

then the QPUF is deemed existentially unforgeable.

1. Comparison with standard definitions of Existential Unforgeability

Notice that there is a one-to-one correspondance between the post-measurement states and the classical outcomes. In other words, if we input any post-measurement state $U|q_i\rangle$ to the QPUF channel Λ_U we get the outcome q_i always *deterministically.* In general, the existential unforgeability condition requires correct prediction of an output given an input that is different from all inputs in the query database of an adversary. In the way we defined existential unforgeability we require the correct prediction of the input given an output. Since there is a one-to-one correspondence between inputs and outputs, (*i.e. if we consider only the set of post-measurement states and the classical outcomes corresponding to them as domain and range,* Λ_U *is invertibile for those choices of sets*) these two notions are mathematically equivalent.

F. Security Results for Ideal QPUF

The following theorems present the security results for the ideal QPUF.

Theorem 1 (No Exponential Unforgeability)**.** *No Haar random basis measurement based ideal QPUF* Λ_U *has exponential unforgeability.*

Proof. With an exponential number of queries, any adversary can conduct process tomography on an unknown quantum channel, obtaining a complete description of it. For a quantum channel on a D-dimensional Hilbert space, D^2 queries suffice for standard process tomography [24]. Since for a λ-qubit system $D = 2^\lambda$, we can then allow the adversary to make 4^λ queries and thus effectively clone the QPUF.

This completes the proof. □

Theorem 2 (Existential Unforgeability)**.** *For any Quantum Polynomial Time adversary (QPT) with query database* $Q_{\mathcal{A}}$*, the expected passing probability in an ideal QPUF verification of any classical measurement outcome* $q \notin Q_{\mathcal{A}}$ *is bounded as follows*

$$E[P_q] \leq \frac{1}{D - |Q_{\mathcal{A}}|}, \tag{30}$$

where P_q *denotes the probability of success for passing the QPUF verification for an outcome* q *and* D *is the dimension of the unitary in* Λ_U*.*

The proof of this theorem can be found in Section V A. For any λ-qubit system, the value of D would be 2^λ where λ is the security parameter. By definition of QPT, $|Q_{\mathcal{A}}| = \mathrm{poly}(\lambda)$. Hence, from Eq. (30) we have, $\forall q$,

$$E[P_q] \leq \frac{1}{2^\lambda - \mathrm{poly}(\lambda)} = \mathrm{negl}(\lambda).$$

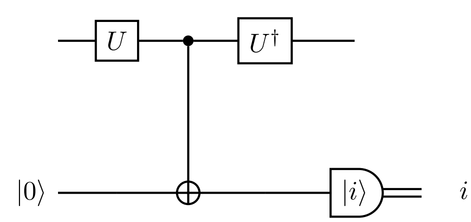
Thus, Theorem 2 implies that any Haar random basis measurement QPUF Λ_U is *existentially unforgeable.*

G. Implementations

1. Random Control-NOT based QPUF (RCNOT-QPUF)

Let us assume that, given access to a *Haar Random* unitary U, we have oracle access to its inverse, $U^\dagger$. We then have an exact implementation of the "*ideal QPUF*" as the controlled-NOT operation with randomized control followed by a standard basis measurement. The QPUF circuit with outcomes in $\mathbb{Z}_D$ can be described as:

$\Pi_i^U =$



,

where the C-NOT is defined as

$$CX = \sum_{i \in \mathbb{Z}_D} |i\rangle\langle i| \otimes X^i, \tag{31}$$

and where X is the generalised Pauli X gate defined as

$$X \equiv \sum_{i \in \mathbb{Z}_D} |i \oplus 1\rangle\langle i|. \tag{32}$$

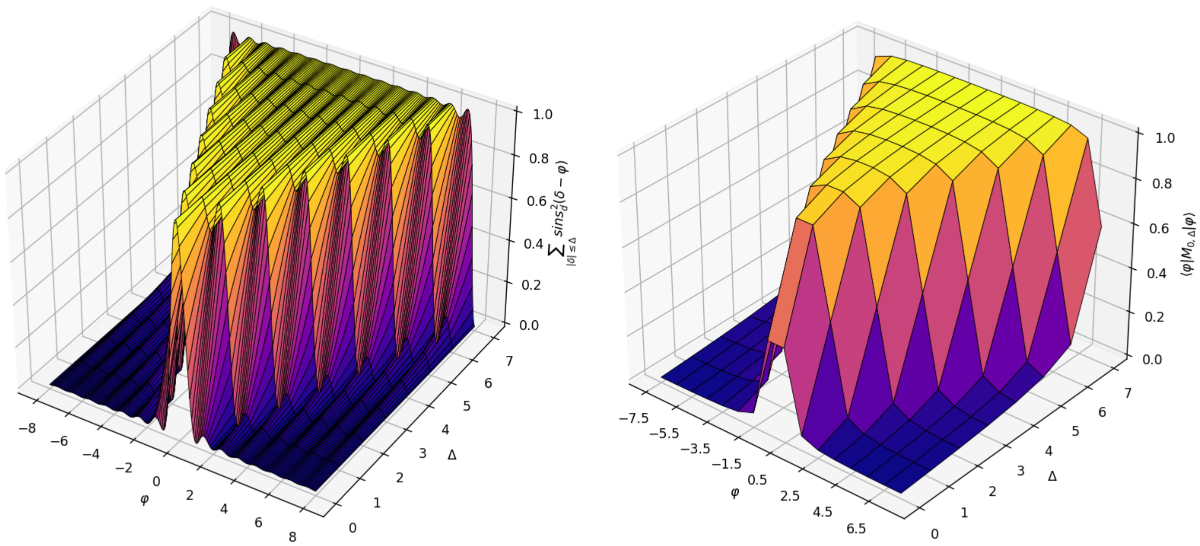


FIG. 2. Approximation of generated output state to a $sins_d^2(\delta - \phi)$: **Left)** Eigenvalue of eigenvector $|\phi\rangle$ for the verification of $M_{0,\Delta}$. **Right)** Special case where $\phi \in [-1/2, +1/2]$ for $M_{0,\Delta} = \sum_{|\delta|\leq\Delta,j} sins_d^2 |\phi\rangle\langle\phi|$. The validity of the approximation increases with larger values of Δ.

Here we also make an abuse of notation, as we did in Eq. (9). This circuit also corresponds to the D Kraus operators of the quantum instrument

$$\Lambda_U(\rho) = \sum_{i\in\mathbb{Z}_D} |i\rangle\langle i| \otimes \Pi_i^U \rho \Pi_i^{U\dagger}, \tag{33}$$

where

$$\Pi_i^U = U |i\rangle\langle i| U^\dagger. \tag{34}$$

This is exactly the Haar random von Neumann measurement channel from Eq. (4). In this implementation, a crucial assumption is that the complete quantum instrument Λ_U constitutes the QPUF, not solely the random unitary. This distinction is critical as it limits adversaries to querying Λ_U rather than the unitary U itself.

2. Phase-Estimation based QPUF (PE-QPUF)

Hardware Requirements: Since the QPE protocol approximates a von Neumann measurement, it would be an approximate implementation of the *ideal QPUF* in Definition 1. Again it is important to note the assumption that the entire quantum instrument Λ_U^{QPE} is the QPUF. We then redefine the hardware requirements as:

Definition 4 (Approximate QPUF)**.** *Any QPE channel Λ_U^{QPE} in Eq. (9) constructed with Haar random unitary U is considered an 'approximate QPUF' if it satisfies the following hardware requirements for some security parameter λ:*

- ***Unknownness:*** *The Kraus operators (Eq. (8)) $\{U_k\}_{k\in\mathbb{Z}_d}$ for the channel Λ_U^{QPE} remain unknown.*
- δ_c-***Collision-Resistance:*** $\forall\Delta; 0 \leq \Delta \leq d-1$, $\exists\delta_c; 1 \geq \delta_c > 0$ *such that for any two different measurement outcomes i, j satisfying $|i - j| \geq \Delta$, the probability of the post measurement states $|\psi_i\rangle, |\psi_j\rangle$ being different by at least δ_c in trace distance satisfies*

$$\Pr\left[D(|\psi_i\rangle\langle\psi_i|, |\psi_j\rangle\langle\psi_j|) \geq \delta_c\right] \geq 1 - \mathrm{negl}(\lambda). \tag{35}$$

- δ_r-***Robustness:*** $\forall\Delta; 0 \geq \Delta \geq d-1$, $\exists\delta_r; 1 \geq \delta_r > 0$ *such that for any two measurement outcomes i, j satisfying $|i - j| \leq \Delta$, the probability of the post measurement states $|\psi_i\rangle, |\psi_j\rangle$ being close by at least δ_r in trace distance satisfies*

$$\Pr\left[D(|\psi_i\rangle\langle\psi_i|, |\psi_j\rangle\langle\psi_j|) \leq \delta_r\right] \geq 1 - \mathrm{negl}(\lambda). \tag{36}$$

- δ_μ-***Uniqueness:*** *The probability of any two distinct QPUFs, $\Lambda_{U_i}^{QPE}$ and $\Lambda_{U_j}^{QPE}$, being distinguishable by at least an amount of $0 \leq \delta_\mu \leq 2$ in diamond norm satisfies*

$$\Pr\left[||\Lambda_{U_i}^{QPE} - \Lambda_{U_j}^{QPE}||_\diamond \geq \delta_\mu\right] \geq 1 - \mathrm{negl}(\lambda). \tag{37}$$

Notice, that for any *approximate QPUF*, if $\delta_\mu = 2$ and if $\forall\Delta > 0$; $\delta_c = 1$ and $\delta_r = 0$, we get an *ideal QPUF*.

3. Approximate Authentication Protocol:

In this section, we describe the authentication protocol with respect to the approximate implementation.

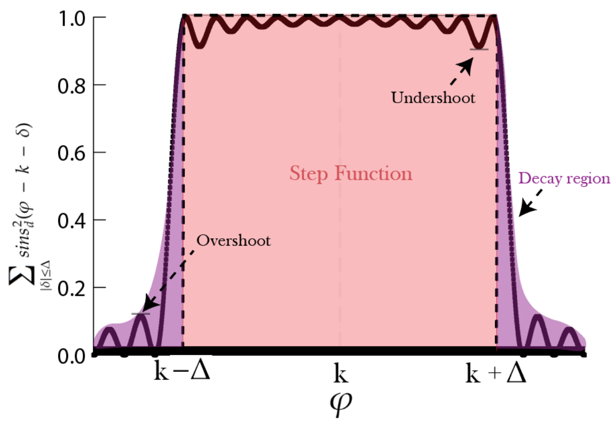
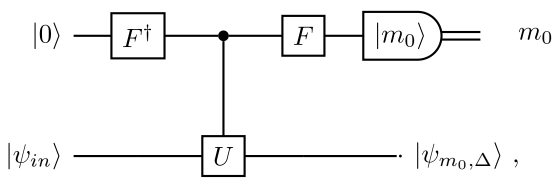


FIG. 3. Gibbs Phenomenon. Cross-section of Fig. 2 corresponding to $\Delta = 5$, showing step function approximation for the operator $M_{k,\Delta}$ demonstrating its approximate behaviour to the projector $\Pi_{k,\Delta}$ in Eq. (43).

a. ***Approximate Token Generation Protocol:*** On a general input state $|\psi_{in}\rangle$ we apply the Quantum Phase Estimation circuit [12], mentioned earlier in Section II C, with a Haar random unitary U,



to obtain a quantum token as the post-measurement state, $|\psi_{m_0,\Delta}\rangle$, and its classical verifier value as the measurement outcome m_0.

b. ***Approximate Token Verification Protocol:*** Upon verification, the token state $|\psi_{m_0,\Delta}\rangle$ is requested back by the verifier. The state is then used as input for the same circuit mentioned above, to obtain a pair of measurement outcome and post-measurement state. We consider the n-th verification to be successful when the difference between outcomes m_n and m_{n-1} (either from generation, $n-1=0$, or previous verification, $n-1 \geq 1$) is small. Since the algorithm is not exact, but provides only an estimation, we parameterize the decision boundary by an integer $0 \leq \Delta \leq \frac{d}{2}$ and say that the verification is successful when the new measurement outcome satisfies

$$|\Delta_n| := |m_n - m_{n-1}| \leq \Delta \mod d.$$

If the n^{th} verification is successful, the classical verifier value is updated from m_{n-1} to m_n in the verifier's classical memory and the post-measurement state $|\psi_{m_n,\Delta}\rangle$ is sent back to the authentic party for a further verification. Due to the commutativity of the Kraus operators in Eq. (16), the conditional probability of having an n^{th} successful verification $P_{m_{n-1},\Delta}$ can be obtained as the expectation value of the operator $M_{m_{n-1},\Delta}$ with respect to the $(n-1)^{th}$ post-measurement state $|\psi_{m_{n-1},\Delta}\rangle$,

$$P_{m_{n-1},\Delta} \equiv \langle\psi_{m_{n-1},\Delta}| M_{m_{n-1},\Delta} |\psi_{m_{n-1},\Delta}\rangle , \tag{38}$$

where for any $k \in \mathbb{Z}_d$ we define,

$$\begin{aligned} M_{k,\Delta} &\equiv \sum_{|\delta|\leq\Delta} M_{k+\delta (\mathrm{mod}\ d)} \\ &= \sum_{j\in\mathbb{Z}_D} \sum_{|\delta|\leq\Delta} \mathrm{sins}_d^2(k+\delta-\phi_j)\, |\phi_j\rangle\langle\phi_j| \qquad (39) \\ &= \sum_{j\in\mathbb{Z}_D} \tilde{1}_\Delta(k-\phi_j)\, |\phi_j\rangle\langle\phi_j| , \qquad (40) \end{aligned}$$

and where we define

$$\tilde{1}_\Delta(x) = \sum_{|\delta|\leq\Delta} \mathrm{sins}_d^2(\delta+x) = 1 - \sum_{|\delta|>\Delta} \mathrm{sins}_d^2(\delta+x), \tag{41}$$

which approximates the step function,

$$1_\Delta(x) = 1_\Delta(-x) = \begin{cases} 1 & x \in [-\Delta,\Delta] \\ 0 & x \notin [-\Delta,\Delta] \end{cases} , \tag{42}$$

as displayed in Fig. 2 for $k=0$ ($x=\phi$). Recall that the Fourier transform of such a step function is the squared sinc function. Hence, it should not be a surprise that the sins series approximates $1_\Delta(k-\phi)$, as it approximates a sinc series for large ancilla dimension d. This is known in literature as '*Gibbs Phenomenon*' [27] which is dispayed in Fig. 3.

Let

$$\Pi_{k,\Delta} \equiv \sum_{\substack{j\in\mathbb{Z}_D \\ |\phi_j - k|\leq\Delta}} |\phi_j\rangle\langle\phi_j| . \tag{43}$$

Thus, intuitively, $M_{k,\Delta}$ approximates the projector $\Pi_{k,\Delta}$, which projects the post-measurement state in a Δ neighbourhood of k as seen in Fig. 3.

Definition 5 ((d,D,Δ)-PE-QPUF)**.** *Any QPE channel Λ_U^{QPE} from Eq.* (9) *with aniclla dimension d, Haar random Unitary dimension D and decision boundary Δ satisfying the hardware requirements of* approximate QPUF *is defined as (d,D,Δ)-PE-QPUF.*

Theorem 3 (Authentic Verification Probability)**.** *For any (d,D,Δ)-PE-QPUF with $\Delta \geq 2$, the conditional probability for the n^{th} successful verification $P_{m_{n-1},\Delta}$, with m_{n-1} as the measurement outcome at the $(n-1)^{th}$ round, can be lower bounded as*

$$P_{m_{n-1},\Delta} > \left(1 - \sqrt{1 - f(\Delta)}\right)^2 , \tag{44}$$

where

$$f(\Delta) \equiv \left(1 - \frac{2}{\pi^2\left(\sqrt{\Delta}+\frac{1}{2}\right)}\right) \cdot \left(1 - \frac{2}{\pi^2(\Delta-\frac{1}{2})}\right) .$$

The proof of this theorem can be found in Section V B. From Eq. (44), for any $(2^{\alpha+\lambda}, 2^{\alpha+\lambda}, 2^{\lambda})$-PE-QPUF where $\alpha, \lambda > 1$, we have $P_{m_{n-1,\Delta}} > 1 - \text{negl}(\lambda)$. In general we observe that, with higher values of Δ, the verification probability approaches 1, whereby giving us a closer approximation to a von Neumann measurement. This is not a surprise, as increasing values of Δ reduces the precision of the phase measurement in the QPE protocol.

Definition 6. *(Verification rate) Considering N_{total} tokens sent to an authentic party, if N_{pass} pass the verification, we define the verification rate as $0 \leq v_R \leq 1$, where,*

$$v_{\text{R}} \equiv \frac{N_{\text{pass}}}{N_{\text{total}}}. \tag{45}$$

For an overall successful authentication it is then required that,

$$v_{\text{R}} \geq \left(1 - \sqrt{1 - f(\Delta)}\right)^2. \tag{46}$$

To validate our analytical predictions on Δ and v_R, we simulated the verification protocol for $(2^6, 2^6, \Delta)$-PE-QPUF and $(2^7, 2^3, \Delta)$-PE-QPUF on the IBM aer-simulator backend, with 10^3 and 10^4 states respectively, as shown in Fig. 4 (left) and Fig. 4 (right) respectively. The Haar random unitary was simulated pseudo-randomly via QR decomposition [28].

4. *Security for PE-QPUF:*

Let the adversary produce an arbitrary pure state $|\psi_{\mathcal{A}}\rangle$ to forge the QPUF verification. From Eq. (38), for any measurement outcome m, the probability of success for the adversary will be

$$P_{m,\Delta} \equiv \langle\psi_{\mathcal{A}}| M_{m,\Delta} |\psi_{\mathcal{A}}\rangle. \tag{47}$$

Since $M_{m,\Delta}$ is random, $P_{m,\Delta}$ is also a random variable.

Theorem 4 (2Δ-Existential Unforgeability)**.** *Consider a QPT adversary with query database $Q_{\mathcal{A}}$ and a $(2^{\alpha+\lambda}, 2^{\alpha+\lambda}, 2^{\lambda})$-PE-QPUF with $\alpha, \lambda > 1$. Let $m \notin Q_{\mathcal{A}}$ be any measurement outcome such that $\forall k \in Q_{\mathcal{A}}$; $|m - k| \geq 2\Delta$. The expected probability of the adversary for a successful verification of the outcome m would be bounded as follows:*

$$\begin{aligned}
&\text{E}[P_{m,\Delta}] \\
&\leq \left(1 - \frac{2}{\pi^2(\frac{\Delta}{2} - 1)}\right) \cdot \left(\frac{1}{\frac{d}{2(\Delta + \frac{\Delta}{2})} - |Q_{\mathcal{A}}|}\right) + \frac{2}{\pi^2(\frac{\Delta}{2} - 1)} \\
&= \left(1 - \frac{2}{\pi^2(2^{\lambda-1} - 1)}\right) \cdot \left(\frac{1}{\frac{2^{\alpha}}{2(1+\frac{1}{2})} - |Q_{A}|}\right) + \frac{2}{\pi^2(2^{\lambda-1} - 1)} \\
&= \text{negl}(\alpha, \lambda).
\end{aligned} \tag{48}$$

The proof of this theorem can be found in Section V C.

IV. DISCUSSION AND FUTURE WORK

We begin the discussion, by stating that in our QPUF models we do not address "man-in-the-middle" attacks, and we explain our rationale for this. We emphasize that such attacks are a distinct issue, independent of the QPUF framework, and should be treated separately, which is why they fall outside the scope of this paper. Specifically, man-in-the-middle scenarios can be viewed as arbitrarily varying channels (AVCs) established between communicating parties. As in other QPUF models [1, 5, 19],communication implicitly assumes that these AVCs have positive capacity. For instance, standard QPUF protocols are also vulnerable to "jamming" attacks, where an adversary might intercept and alter the challenge state or steal the legitimate responses, preventing successful verification or enabling false verification respectively. These issues can be addressed by studying AVCs with positive capacities and integrating them into our QPUF scheme.

Thus, omitting man-in-the-middle attacks does not detract from the validity of our proposed models. Nevertheless, incorporating such attacks would enhance the practicality of our approach, and we plan to explore this in future work.

A. Comaprison between QR-PUF and our proposed models

The (QR)-PUF model [5] faces several challenges that are absent in the model presented in [1] and also our proposed models:

- The Challenge-Response Table (CRT) consists primarily of classical strings, meaning the potential of quantum states isn't fully utilized.
- The PUF's unitary is fully known, allowing an adversary with a quantum computer to simulate it and predict the response states.
- There is a trade-off between noise resistance and unclonability in the (QR)-PUF model.
- The certifier has access to the CRT, making them a trusted party.

On the other hand, a key requirement in our models, as well as in the model from [1], is the assumption of Haar random unitaries. Since perfect Haar randomness is unattainable, this remains a potential limitation until the security of our schemes is evaluated under weaker assumptions. However, progress has been made with unitary t-designs [29], and analyzing the security of our schemes using t-designs is an interesting direction for future work.

Another promising avenue is exploring many-body quantum systems that can generate states with behavior close to Haar randomness. Investigating how such

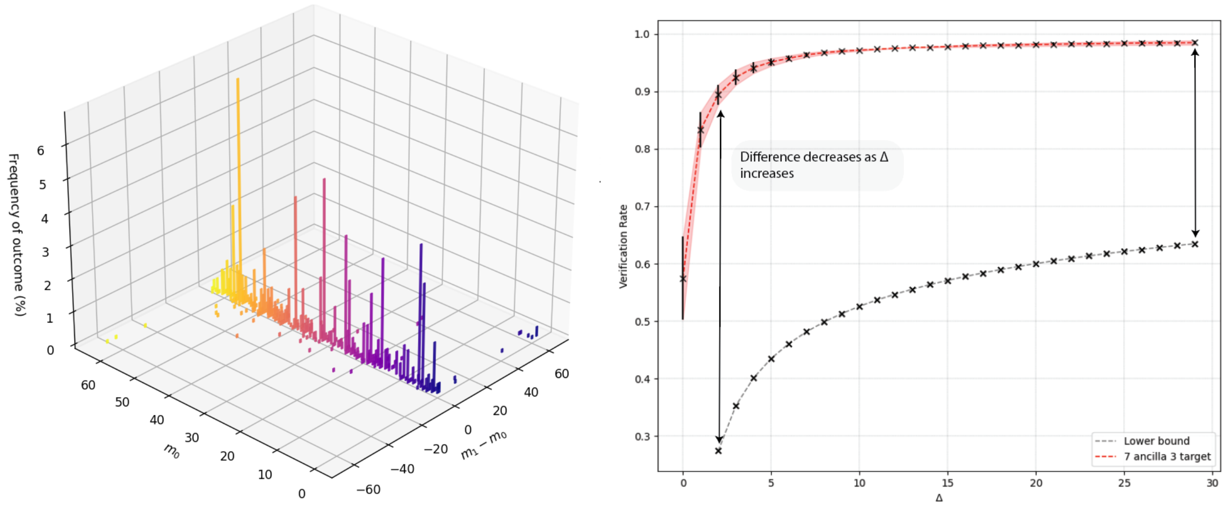


FIG. 4. On the left, a $(2^6, 2^6, \Delta)$-PE-QPUF is simulated with 10^3 quantum states. m_0 and m_1 represent measurement outcomes at generation and 1^{st} verification, respectively. As expected, high peaks of outcome frequency are observed around low values of $m_1 - m_0$ (Δ). On the right, the simulation for a $(2^7, 2^3, \Delta)$-PE-QPUF with 10^4 states compares the analytical lower bound with the verification rate from Eq. (45).The red-shaded region represents the standard deviation over 5 iterations with 10^4 states each. The difference between simulated results and the lower bound decreases with higher Δ values.

systems can be leveraged for our proposed models' security analysis will also be an important part of future research. These areas are left for future work and are beyond the scope of this paper.

B. Comparison between Hybrid PUF [10] and our proposed models

While developing our model, we noticed that the concept of combining classical elements with quantum constructions was introduced earlier through the Hybrid PUF [10]. A Hybrid PUF consists of two main components: a Classical PUF (CPUF) and a public encoder that maps the CPUF's outputs to quantum states. The key assumption in this model is that the CPUF outputs are hidden from the adversary. Security is based on the difficulty for an adversary to infer the CPUF's outputs from the encoded quantum states. However, this reliance on the secrecy of the CPUF's outputs makes the Hybrid PUF model weaker than ours, which requires no such assumption.

In the following subsections, we mention some limitations of the implementations of the '*Ideal QPUF*' and propose possible interesting future research directions.

C. Limitations for RCNOT-QPUF

This model assumes that, when provided with a Haar random unitary U, the QPUF device can carry out its inverse operation $U^\dagger$. However, the efficiency of performing such an operation remains uncertain.

Open research direction:

Attempts have been made to develop algorithms for computing the inverse of an unknown D-dimensional unitary [13–18]. None of the cited algorithms are deterministic and exact at the same time. It is also shown, in the above-mentioned references, that with the increase in precision of the implementation (*deterministic approximate case*) or increase in the probability of correct implementation (*probabilistic exact case, [14, 15]*) the gate cost complexity of the algorithms increases exponentially. Thus, although the implementations work, they are inefficient. Recently, an attempt was made for finding '*deterministic*' and '*exact*' implementation [30]. However, the introduced algorithm works only for $SU(2)$ unitaries and it remains an open problem to extend the algorithm to general dimensions and finding a closed form expression for its complexity as a function of dimension. To summarize, it is an open problem to find a computationally efficient method for inverting any unknown blackbox unitary.

D. Limitations for PE-QPUF

As the model is grounded in Quantum Phase Estimation, it inherits the *exponential overhead* issue associated with it. For any general Unitary matrix U, Quantum Phase Estimation necessitates the implementation of the gate CU $d-1$ times (for qubits, and in general scales as d), where d is the dimension of the ancilla system. For a λ qubit ancilla system, the gate CU needs to be applied $2^\lambda - 1$ times. The gate cost complexity for such implementation can be computed [24], by summing a geometric series, to be 2^λ. Other schemes, like *fast phase estimation* [31], performs phase estimation with logarithmic circuit depth, but the classical post processing remains exponentially costly. Consequently, a *trade-off* between '*implementability*' and '*security*' emerges, as efficient implementation requires smaller dimensions, while enhanced security needs larger dimensions.

Open research direction:

Since implementing $CU^{2^\lambda-1}$ is exponentially costly (gate cost complexity) in general, one can look for classes of random unitary matrices (other probability measures than the Haar measure) for which the implementation is secure and polynomially costly.

Another proposal is to convert the multiple applications of the gate U into a single application. Recall from Schrodinger's equation that any unitary U is nothing but the time evolution operator obtained by exponentiating a physical Hamiltonian, i.e., for any Hamiltonian H we can obtain an unitary U as

$$U(t) = e^{\frac{i}{\hbar}Ht}, \tag{49}$$

where the operator $U(t)$ evolves a state for a time t. β applications of U would then result into

$$U^\beta(t) = e^{\frac{i}{\hbar}\beta Ht}.$$

Consider a new Hamiltonian $H' = \beta H$. We can then obtain the operator U' by performing

$$U'(t) = e^{\frac{i}{\hbar}H't} = U^\beta(t). \tag{50}$$

If we could create all the Hamiltonians H', for integer powers β of U, we can then produce a collection of λ many gates

$$\{U^i\}_{i=0}^{\lambda-1}. \tag{51}$$

Using these gates we can implement $CU^{2^{\lambda-1}}$ with gate cost complexity λ. A possibility of creating $H' = \beta H$ is to absorb β into the coupling parameters of H by tuning them with external interactions (thermal, magnetic..). Thus, there is interesting future work in finding many body systems where such tunability is possible. For example, consider the Heisenberg-XYZ Hamiltonian

$$\hat{H} = -\frac{1}{2}\sum_{j=1}^{N}(J_{x_j}\sigma_j^x\sigma_{j+1}^x + J_{y_j}\sigma_j^y\sigma_{j+1}^y + J_{z_j}\sigma_j^z\sigma_{j+1}), \tag{52}$$

where $J_{x_j}, J_{y_j}, J_{z_j}$ are the couplings. If the couplings were random, we would have a random unitary constructed out of such a Hamiltonian. Now, if tuning the couplings with external interactions was possible, this could be a suitable candidate. It is also important to note that such an implementation is not solving the problem but rather translating '*time-complexity*' into '*energy-complexity*' as for tuning the couplings one has to access higher energy states. However, this translation of the problem from *time* to *energy* may be sometimes useful for practical purposes as relatively higher energies might be more accessible than exponentially long waiting times for token generation.

In the following section we present a comparison between the two models proposed in this paper.

E. Comparision between MB-QPUF and Ideal QPUF

In this section, we compare the two models presented in this paper. For near-term practical implementations, we argue that the MB-QPUF is more suitable than the Ideal QPUF for the following reasons:

- The MB-QPUF can be implemented efficiently with oracle access to a Haar random unitary, whereas in the proposed implementations in this paper, the Ideal QPUF requires an exponential gate cost, making it less feasible.
- Storing entangled states is not a concern for the *Ideal QPUF*, as most constructions in the literature [1, 5, 19] already involve storing highly entangled states.
- In practical scenarios, the prover typically has limited resources. The MB-QPUF does not require quantum memory on the prover's side, whereas the Ideal QPUF does. Since quantum memory is currently expensive, this is an advantage. However, this benefit is somewhat reduced by the fact that possessing a QPUF device itself can be costly in the near term.

That said, if the challenges around quantum memory are resolved and we develop an efficient implementation of the Ideal QPUF, it would offer more advantages than the MB-QPUF. This is because the Ideal QPUF is a complete device that even the verifier cannot tamper with, while in the MB-QPUF, the query process can potentially be compromised.

An efficient implementation of the *ideal QPUF* also addresses the long-standing open problem of public-key quantum money schemes [32]. Here's a brief overview of how it works:

- A public server (or mint) possesses the ideal QPUF device Λ_U.
- The mint initialises arbitrary input states and measures them using Λ_U to generate money bills $U|i\rangle$ and corresponding classical outcomes i. These classical outcomes will serve as serial numbers which are printed on the money bill. Then these money bills are distributed. In the money generation process there will be other details like what happens when two money bills have the same serial number

during production? Two money bills with the same measurement outcome are discarded. Notice, that the mint wants to print polynomially many money bills because it makes no sense if the money generation scheme has exponential complexity. However, there are exponentially many measurement outcomes possible with uniform probability on average. It is therefore trivial to show that the collision probability is negligible.

- When Alice transfers a bill to Bob, Bob sends it to the server for verification. If successful, the server returns the post-measurement state to Bob. Notice, that if the verification is passed successfully the measurement does not change the quantum state of the money bill.

V. METHODS

A. Proof of Theorem 2

Proof. (Theorem 2) We begin the proof by considering an arbitrary measurement outcome $q \notin Q_{\mathcal{A}}$, where $Q_{\mathcal{A}}$ is the query database of the adversary.

Following Eq. (27), we write the passing probability for the adversary as

$$P_q = \mathrm{Tr}\left[\Pi_q^U \left|\psi_{\mathcal{A}}\right\rangle\!\left\langle\psi_{\mathcal{A}}\right|\right], \tag{53}$$

where $|\psi_{\mathcal{A}}\rangle$ is the guess state of the adversary.

Any unitary U can be written in standard basis as

$$U = (U|0\rangle, U|1\rangle, \cdots, U|D-1\rangle). \tag{54}$$

Let us now consider the following construction for a Haar random unitary [33], which is inspired by the Gram-Schmidt orthogonalisation process [34]:

- Choose i^{th} column $U|i\rangle$ uniformly at random from $\mathbb{C}^D$.
- Choose j^{th} column $U|j\rangle$ uniformly at random from the $D-1$ dimensional orthogonal subspace of $U|i\rangle$.
- Choose k^{th} column $U|k\rangle$ uniformly at random from the $D-2$ dimensional orthogonal subspace of the subspace spanned by $U|i\rangle$ and $U|j\rangle$.
- Keep iterating until all the columns are obtained.

By exploiting the left invariance of the Haar measure, it is shown in [33] that such a construction gives a Haar random unitary. Recall the structure of the query database. $Q_{\mathcal{A}}$:

$$Q_{\mathcal{A}} := \{\left|\psi^i_{\mathcal{A}}\right\rangle, q_i, U|q_i\rangle\}_{i\in\mathbb{Z}_{|Q_{\mathcal{A}}|}},$$

where we let $\{\left|\psi^i_{\mathcal{A}}\right\rangle\}$ be the set of input states initialised by the adversary to query the QPUF. Since a quantum measurement can collapse two different states onto a same state, there can be degeneracies in $Q_{\mathcal{A}}$, i.e., for two states $\left|\psi^i_{\mathcal{A}}\right\rangle \neq \left|\psi^j_{\mathcal{A}}\right\rangle$ we may have,

$$(q_i, U|q_i\rangle) = (q_j, U|q_j\rangle).$$

Consider $Q'_{\mathcal{A}}$, with $|Q'_{\mathcal{A}}| = |Q_{\mathcal{A}}|$, having no degeneracies. It is then evident that such a case is the best case scenario for the adversary, as in such case the maximum number of different token states can be owned. Hence, the success probability, with query database $Q'_{\mathcal{A}}$, will always be greater than or equal to the one with $Q_{\mathcal{A}}$. We would now perform a calculation with $Q'_{\mathcal{A}}$ to find an upperbound on the expected success probability. Subsequently, consider $q \notin Q'_{\mathcal{A}}$. Passing the verification for such q is equivalent to guessing the state vector $U|q\rangle$. It follows from the construction of Haar random unitary above [33] that the task of guessing $U|q\rangle$ is equivalent to guessing a vector sampled uniformly at random from a $\mathbb{C}^{D-|Q'_{\mathcal{A}}|}$ dimensional subspace. Now, consider a Haar random unitary $W \in U(D - |Q'_{\mathcal{A}}|)$. By the arguments above, we have

$$U|m\rangle\!\langle m| U^\dagger \sim W|0\rangle\!\langle 0| W^\dagger, \tag{55}$$

where the symbol $\sim$ denotes *"distributed as"*.

Let us construct a random variable X as:

$$X := \mathrm{Tr}\big(W|0\rangle\!\langle 0|W^\dagger \rho_{\mathcal{A}}\big). \tag{56}$$

It follows from our arguments that

$$\begin{aligned} X &\sim P_q \\ \implies E[X] &= E[P_q]. \end{aligned} \tag{57}$$

Thus, we have

$$\begin{aligned} E[X] &= \int_W \mathrm{Tr}\big(W|0\rangle\!\langle 0|W^\dagger |\psi_{\mathcal{A}}\rangle\!\langle\psi_{\mathcal{A}}|\big) dW \\ &= \mathrm{Tr}\left(\frac{\mathbb{I}_{D-|Q'_{\mathcal{A}}|}}{D-|Q'_{\mathcal{A}}|}\cdot|\psi_{\mathcal{A}}\rangle\!\langle\psi_{\mathcal{A}}|\right) \\ &= \frac{1}{D-|Q'_{\mathcal{A}}|} \\ &= \frac{1}{D-|Q_{\mathcal{A}}|} \\ &= E[P_q]. \end{aligned} \tag{58}$$

Since we have calculated this for the best case query scenario, $Q'_{\mathcal{A}}$, we in general have

$$E[P_q] \leq \frac{1}{D-|Q_{\mathcal{A}}|}. \tag{59}$$

This completes the proof. □

B. Proof of Theorem 3

Before we begin with the proof of Theorem 3, we will first introduce two lemmas.

Lemma 1 (Lower bound for sinc series)**.** *For some decision boundary Δ, an arbitrary measurement outcome k and $\forall x$ such that $|x-k|\leq \Delta - b$, we have the following lower bound on the normalized sinc series for some arbitrary $0 \leq b < \Delta$*

$$\sum_{\substack{|\delta|\leq\Delta\\|x-k|\leq\Delta-b}} \mathrm{sinc}^2(x-k-\delta) \geq 1 - \frac{2}{\pi^2(b+\frac{1}{2})}. \tag{60}$$

Proof. Without loss of generality, we work with the measurement outcome $k=0$. Also note that, $\forall x$,

$$\sum_{|\delta|\leq\infty} \mathrm{sinc}^2(x-\delta) = 1$$
$$\implies \sum_{|\delta|\leq\Delta} \mathrm{sinc}^2(x-\delta) + \sum_{|\delta|>\Delta} \mathrm{sinc}^2(x-\delta) = 1. \tag{61}$$

Thus, we have

$$\sum_{|\delta|\leq\Delta} \mathrm{sinc}^2(x-\delta) \geq 1 - \max_x \sum_{|\delta|>\Delta} \mathrm{sinc}^2(x-\delta). \tag{62}$$

Now, for $|x|\leq \Delta - b$, we proceed to obtain

$$\max_{|x|\leq\Delta-b} \sum_{|\delta|>\Delta} \mathrm{sinc}^2(\delta-x)$$
$$= \max_{|x|\leq\Delta-b} \left(\frac{2\sin^2(\pi(x))}{\pi^2} \lim_{N\to\infty} \sum_{\delta=\Delta+1}^{N} \frac{1}{(\delta-x)^2} \right)$$

$[\because sin^2(x)$ is periodic in $\pi]$

$$\leq \max_{|x|\leq\Delta-b} \lim_{N\to\infty} \int_{\Delta+0.5}^{N+0.5} \frac{2\sin^2(\pi(x))}{\pi^2(\delta-x-0.5)^2} d\delta \tag{63}$$
$$= \max_{|x|\leq\Delta-b} \lim_{N\to\infty} \left(\frac{2\sin^2(\pi(x))}{\pi^2(\Delta+0.5-x)} - \frac{2\sin^2(\pi(x))}{\pi^2(N+0.5-x)} \right)$$
$$= \max_{|x|\leq\Delta-b} \left(\frac{2\sin^2(\pi(x))}{\pi^2(\Delta+0.5-x)} \right)$$
$$\leq \frac{2}{\pi^2(b+\frac{1}{2})}. \tag{64}$$

In [Eq. (63)] we have bounded the quadratic sum using an integral, which becomes evident from the illustration Fig. 5

$$\int_a^b \frac{dx}{(x+0.5)^2} \leq \sum_{x=a}^{b} \frac{1}{x^2} \leq \int_a^b \frac{dx}{(x-0.5)^2}. \tag{65}$$

Therefore, we have

$$\sum_{\substack{|\delta|\leq\Delta\\|x-k|\leq\Delta-b}} \mathrm{sinc}^2(x-k-\delta) \geq 1 - \frac{2}{\pi^2(b+\frac{1}{2})}. \tag{66}$$

This completes the proof. □

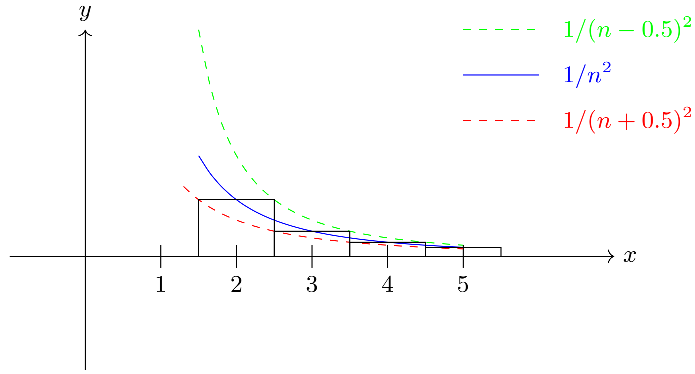


FIG. 5. Integral bound for quadratic sum.

Lemma 2 (Upper bound for normalized sinc series)**.** *For some decision boundary Δ, some arbitrary $c > 1$, an arbitrary measurement outcome k and $\forall x$ such that $|x-k|\geq \Delta + c$, we have the following upper bound on the normalized sinc series*

$$\sum_{\substack{|\delta|\leq\Delta\\|x-k|\geq\Delta+c}} \mathrm{sinc}^2(x-k-\delta) < \frac{2}{\pi^2(c-1)}. \tag{67}$$

Proof. The proof of this lemma follows along the similar lines of argument as Lemma 1. □

Now, we proceed to prove Theorem 3.

Proof. (Theorem 3) For a measurement outcome m_n at the n^{th} round, let $|\psi_{m_n,\Delta}\rangle$ denote the post-measurement state for some decision boundary Δ.

Let X be a random variable, defined as $X := [0, \cdots, d-1]$, denoting the possible measurement outcomes at the $(n-1)^{th}$ round. Let us consider an arbitrary post-measurement state at the $(n-2)^{th}$ round, which can be expressed in the eigenbasis $\{|\phi_i\rangle\}_{i=0}^{D-1}$ of the Haar random unitary U as

$$|\psi_{m_{n-2},\Delta}\rangle \equiv |\psi\rangle = \sum_{i\in\mathbb{Z}_D} c_i |\phi_i\rangle, \tag{68}$$

where c_i's are complex numbers such that $\sum_{i\in\mathbb{Z}_D}|c_i|^2 = 1$. The p.d.f. for X is then obtained as,

$$\Pr(X = m_{n-1}) = \langle\psi| M_{m_{n-1}} |\psi\rangle. \tag{69}$$

We then define another random variable $P_{X,\Delta}$ that denotes the conditional probability of having an n^{th} successful verification, conditioned on $n-1$ prior successful verifications. The values for the random variable $P_{X,\Delta}$, $\forall m_{n-1} \in \mathbb{Z}_d$ is obtained as

$$P_{m_{n-1},\Delta} = \mathrm{Tr}\left[M_{m_{n-1},\Delta} \frac{U_{m_{n-1}} |\psi\rangle\langle\psi| U^\dagger_{m_{n-1}}}{\langle\psi| M_{m_{n-1}} |\psi\rangle} \right]. \tag{70}$$

The expected conditional probability will be:

$$\begin{aligned}
\mathrm{E}[P_{X,\Delta}] &= \sum_{k\in\mathbb{Z}_d} P_{k,\Delta}\cdot \Pr(X=k)\\
&= \sum_{k\in\mathbb{Z}_d} \frac{\mathrm{Tr}\Big[M_{k,\Delta}U_k\,|\psi\rangle\langle\psi|\,U_k^\dagger\Big]}{\langle\psi|\,M_k\,|\psi\rangle}\cdot\langle\psi|\,M_k\,|\psi\rangle\\
&= \sum_{k\in\mathbb{Z}_d}\langle\psi|\,M_{k,\Delta}M_k\,|\psi\rangle\\
&= \sum_{i\in\mathbb{Z}_D}|c_i|^2\sum_{k\in\mathbb{Z}_d}\mathrm{sins}_d^2(\phi_i-k)\sum_{|\delta|\le\Delta}\mathrm{sins}_d^2(\phi_i-k-\delta)\\
&\ge \min_{\phi_i,\Delta}\left(\sum_{k\in\mathbb{Z}_d}\mathrm{sinc}^2(\phi_i-k)\sum_{|\delta|\le\Delta}\mathrm{sinc}^2(\phi_i-k-\delta)\right)\cdot 1.
\end{aligned}\tag{71}$$

The value ϕ_{i^*} that minimises [Eq. (71)] will be of the form $\phi_{i^*}=\lfloor\phi_{i^*}\rfloor+x$, where $0\le x\le 1$ and $\lfloor\phi_{i^*}\rfloor$ is some integer in $\mathbb{Z}_d$. Thus, there will always be a measurement outcome $k\in\mathbb{Z}_d$, such that $k=\lfloor\phi_{i^*}\rfloor$. We now choose some $0\le b<\Delta$ and truncate the sum in [Eq. (71)] in the following manner to obtain a lower bound as

$$\begin{aligned}
\mathrm{E}[P_{X,\Delta}] \ge& \sum_{|\delta'|\le\Delta-b}\mathrm{sinc}^2(\phi_{i^*}-\lfloor\phi_{i^*}\rfloor-\delta')\\
&\times\sum_{|\delta|\le\Delta}\mathrm{sinc}^2(\phi_{i^*}-\lfloor\phi_{i^*}\rfloor-\delta'-\delta)\\
&=\sum_{|\delta'|\le\Delta-b}\mathrm{sinc}^2(x-\delta')\sum_{|\delta|\le\Delta}\mathrm{sinc}^2(x-\delta'-\delta).
\end{aligned}\tag{72}$$

Let

$$S_{\Delta,b}(x)\equiv\sum_{|\delta'|\le\Delta-b}\mathrm{sinc}^2(x-\delta') \tag{73a}$$

$$S_{\Delta,b}(x,\delta')\equiv\sum_{|\delta|\le\Delta}\mathrm{sinc}^2(x-\delta'-\delta). \tag{73b}$$

Thus [Eq. (72)] becomes

$$\mathrm{E}[P_{X,\Delta}]\ge\sum_{|\delta'|\le\Delta-b}\mathrm{sinc}^2(x-\delta')S_{\Delta,b}(x,\delta'). \tag{74}$$

From Lemma 1 we have $\forall x,\delta'$

$$S_{\Delta,b}(x,\delta')\ge 1-\frac{2}{\pi^2\left(b+x+\frac{1}{2}\right)}. \tag{75}$$

We then have

$$\begin{aligned}
\mathrm{E}[P_{X,\Delta}] &\ge \left(1-\frac{2}{\pi^2\left(b+x+\frac{1}{2}\right)}\right)\cdot S_{\Delta,b}(x)\\
&\ge \min_x\left(1-\frac{2}{\pi^2\left(b+x+\frac{1}{2}\right)}\right)\cdot\left(\min_x S_{\Delta,b}(x)\right)\\
&= \left(1-\frac{2}{\pi^2\left(b+\frac{1}{2}\right)}\right)\cdot\left(\min_x S_{\Delta,b}(x)\right).
\end{aligned}\tag{76}$$

Again, from [Lemma 1] we have $\forall x$

$$S_{\Delta,b}(x)\ge 1-\frac{2}{\pi^2(|\Delta-\frac{1}{2}|)}. \tag{77}$$

Therefore we get

$$\mathrm{E}[P_{X,\Delta}]\ge\left(1-\frac{2}{\pi^2\left(b+\frac{1}{2}\right)}\right)\cdot\left(1-\frac{2}{\pi^2(|\Delta-\frac{1}{2}|)}\right). \tag{78}$$

Any value of $0\le b<\Delta$ in [Eq. (78)] will give us a valid lower bound. For $\Delta\ge 2$ we can then choose $b=\sqrt{\Delta}$ to obtain the final bound as

$$\mathrm{E}[P_{X,\Delta}]\ge f(\Delta), \tag{79}$$

where

$$f(\Delta)\equiv\left(1-\frac{2}{\pi^2\left(\sqrt{\Delta}+\frac{1}{2}\right)}\right)\cdot\left(1-\frac{2}{\pi^2(|\Delta-\frac{1}{2}|)}\right). \tag{80}$$

Let us now define another random variable $Q_{X,\Delta}$ as

$$Q_{X,\Delta}\equiv 1-P_{X,\Delta}. \tag{81}$$

Therefore,

$$\begin{aligned}
\mathrm{E}\left[Q_{X,\Delta}\right] &= 1-\mathrm{E}\left[P_{X,\Delta}\right]\\
&\le 1-f(\Delta).
\end{aligned}\tag{82}$$

By Markov's inequality [35], for some $a\ge 0$

$$\begin{aligned}
\Pr[Q_{X,\Delta}\ge a] &\le \frac{\mathrm{E}[Q_{X,\Delta}]}{a}\\
&\le\frac{1-f(\Delta)}{a}.
\end{aligned}\tag{83}$$

Therefore,

$$\begin{aligned}
&\Pr[Q_{X,\Delta}<a]\ge 1-\frac{1-f(\Delta)}{a}\\
\implies&\Pr[P_{X,\Delta}>1-a]\ge 1-\frac{1-f(\Delta)}{a}.
\end{aligned}\tag{84}$$

Choosing, $a=\sqrt{1-f(\Delta)}$ we have,

$$\begin{aligned}
\Pr\Big[P_{X,\Delta}>1-\sqrt{1-f(\Delta)}\Big]&\ge 1-\sqrt{1-f(\Delta)}\\
\Pr[P_{X,\Delta}>g(\Delta)]&\ge g(\Delta),
\end{aligned}\tag{85}$$

where

$$g(\Delta)\equiv 1-\sqrt{1-f(\Delta)}. \tag{86}$$

Let $V^n_{m_{n-1}}$ denote the event of successful n^{th} verification for some arbitrary measurement outcome m_{n-1} at the

$(n-1)^{th}$ round. Therefore we have

$$\begin{aligned}
&\Pr\Big[V^n_{m_{n-1}}\Big] = P_{m_{n-1},\Delta} \\
&= \Pr\big[P_{m_{n-1},\Delta} > g(\Delta)\big] \cdot \Pr\Big[V^n_{m_{n-1}} | P_{m_{n-1},\Delta} > g(\Delta)\Big] \\
&+ \Pr\big[P_{m_{n-1},\Delta} \leq g(\Delta)\big] \cdot \Pr\Big[V^n_{m_{n-1}} | P_{m_{n-1},\Delta} \leq g(\Delta)\Big] \\
&> \Pr\big[P_{m_{n-1},\Delta} > g(\Delta)\big] \cdot \Pr\Big[V^n_{m_{n-1}} | P_{m_{n-1},\Delta} > g(\Delta)\Big] \\
&= (g(\Delta))^2 \\
&= \Big(1 - \sqrt{1 - f(\Delta)}\Big)^2. \qquad (87)
\end{aligned}$$

This completes the proof. □

C. Proof of Theorem 4

Proof. (Theorem 4) Given an arbitrary adversary guess state

$$|\psi_{\mathcal{A}}\rangle = \sum_i c_i |\phi_i\rangle, \qquad (88)$$

we have, for any $m \notin Q_{\mathcal{A}}$,

$$\begin{aligned}
&P_{m,\Delta} \\
&= \langle\psi_{\mathcal{A}}| M_{m,\Delta} |\psi_{\mathcal{A}}\rangle \\
&= \sum_{i\in\mathbb{Z}_D} |c_i|^2 \sum_{|\delta|\leq\Delta} \mathrm{sins}^2_d(\phi_i - m - \delta) \\
&\leq \langle\psi_{\mathcal{A}}| \Pi_{m,\Delta+c} |\psi_{\mathcal{A}}\rangle \\
&+ \max_{|\phi_i|>2\Delta} \sum_{|\delta|\leq\Delta} \mathrm{sins}^2_d(\phi_i - m - \delta) \cdot \langle\psi_{\mathcal{A}}| (\mathbb{I} - \Pi_{m,\Delta+c}) |\psi_{\mathcal{A}}\rangle \\
&= \left(1 - \frac{2}{\pi^2(c-1)}\right) \cdot \langle\psi_{\mathcal{A}}| \Pi_{m,\Delta+c} |\psi_{\mathcal{A}}\rangle + \frac{2}{\pi^2(c-1)}, \qquad (89)
\end{aligned}$$

where in the last step we have applied [Lemma 2] with $c > 1$.

We have $\forall k \in Q_{\mathcal{A}};\ |m-k| \geq 2\Delta$. Consider any $(k', |\psi_{k'}\rangle) \in Q_{\mathcal{A}}$. Combining Eq. (89) with Theorem 3 we have

$$\begin{aligned}
&\langle\psi_{k'}| \Pi_{m,\Delta+c} |\psi_{k'}\rangle \\
&\leq 1 - \frac{\Big(1 - \sqrt{1 - f(\Delta, 1)}\Big)^2 - \frac{2}{\pi^2(c-1)}}{1 - \frac{2}{\pi^2(c-1)}} \qquad (90)
\end{aligned}$$

Let us choose $c = \frac{\Delta}{2} = 2^{\lambda-1}$. Thus, Eq. (90) becomes

$$\begin{aligned}
\langle\psi_{k'}| \Pi_{m,\Delta+\frac{\Delta}{2}} |\psi_{k'}\rangle &\leq 1 - (1 - \mathrm{negl}(\lambda)) \qquad (91) \\
&= \mathrm{negl}(\lambda).
\end{aligned}$$

This implies,

$$\mathrm{span}\{Q_{\mathcal{A}}\} \perp \mathrm{span}\{\Pi_{m,\Delta+\frac{\Delta}{2}}\}. \qquad (92)$$

Therefore, we apply [Theorem 2] with the above mentioned choice of c to obtain

$$\begin{aligned}
&\mathrm{E}[P_{m,\Delta}] \\
&\leq \left(1 - \frac{2}{\pi^2(\frac{\Delta}{2}-1)}\right) \cdot \mathrm{E}[\langle\psi_{\mathcal{A}}| \Pi_{m,\Delta+\frac{\Delta}{2}} |\psi_{\mathcal{A}}\rangle] + \frac{2}{\pi^2(\frac{\Delta}{2}-1)} \\
&\leq \left(1 - \frac{2}{\pi^2(\frac{\Delta}{2}-1)}\right) \cdot \left(\frac{1}{\frac{d}{2(\Delta+\frac{\Delta}{2})} - |Q_{\mathcal{A}}|}\right) + \frac{2}{\pi^2(\frac{\Delta}{2}-1)} \\
&= \mathrm{negl}(\lambda), \qquad (93)
\end{aligned}$$

where in the second last step we have applied Theorem 2.

This completes the proof. □

CODE AVAILABILITY

The codes for the simulations can be found in the following github repository: `https://github.com/terrordayvg/Puf_sim`.

[1] M. Arapinis, M. Delavar, M. Doosti, and E. Kashefi, Quantum **5**, 475 (2021).
[2] Y. Gao, Nature Communications (2020), 10.1038/s41928-020-0372-5.
[3] R. Maes, *Physically Unclonable Functions: Constructions, Properties and Applications* (Springer, 2013).
[4] C. S. K. Y. L. S. Y. M. Kim Min Seok Lee Gil Ju, Leem Jung Woo, Nature Communications (2022), 10.1038/s41467-021-27278-5.
[5] B. Škorić, in *Progress in Cryptology – AFRICACRYPT 2010*, edited by D. J. Bernstein and T. Lange (Springer Berlin Heidelberg, Berlin, Heidelberg, 2010) pp. 369–386.
[6] M. Doosti, N. Kumar, M. Delavar, and E. Kashefi, ACM Transactions on Quantum Computing **2** (2021), 10.1145/3484197.
[7] K. Phalak, A. A. Saki, M. Alam, R. O. Topaloglu, and S. Ghosh, IEEE Journal on Emerging and Selected Topics in Circuits and Systems **11**, 333 (2021).
[8] V. Galetsky, S. Ghosh, C. Deppe, and R. Ferrara, in *2022 IEEE Globecom Workshops (GC Wkshps)* (2022) pp. 820–825.
[9] M. Doosti, N. Kumar, E. Kashefi, and K. Chakraborty, Quantum Science and Technology **7**, 035004 (2022).
[10] K. Chakraborty, M. Doosti, Y. Ma, C. Wadhwa, M. Arapinis, and E. Kashefi, Quantum **7**, 1014 (2023).
[11] (2009).
[12] A. Y. Kitaev, Electron. Colloquium Comput. Complex. **TR96-003** (1996), arXiv:TR96-003 [quant-ph].

[13] I. S. B. Sardharwalla, T. S. Cubitt, A. W. Harrow, and N. Linden, (2016).
[14] M. Sedlá k, A. Bisio, and M. Ziman, Physical Review Letters **122** (2019), 10.1103/physrevlett.122.170502.
[15] M. T. Quintino, Q. Dong, A. Shimbo, A. Soeda, and M. Murao, Physical Review A **100** (2019), 10.1103/physreva.100.062339.
[16] M. T. Quintino, Q. Dong, A. Shimbo, A. Soeda, and M. Murao, Physical Review Letters **123** (2019), 10.1103/physrevlett.123.210502.
[17] Q. Dong, M. T. Quintino, A. Soeda, and M. Murao, Physical Review Letters **126** (2021), 10.1103/physrevlett.126.150504.
[18] M. T. Quintino and D. Ebler, Quantum **6**, 679 (2022).
[19] M. Doosti, N. Kumar, M. Delavar, and E. Kashefi, ACM Transactions on Quantum Computing **2** (2021), 10.1145/3484197.
[20] T. Metger and R. Renner, Nature Communications (2023), 10.1038/s41467-023-40920-8.
[21] T. Upadhyaya, T. van Himbeeck, J. Lin, and N. Lütkenhaus, PRX Quantum **2**, 020325 (2021).
[22] D. Gavinsky, "Quantum money with classical verification," (2012), arXiv:1109.0372 [quant-ph].
[23] S. Wiesner, SIGACT News **15**, 78–88 (1983).
[24] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th ed. (Cambridge University Press, 2010).
[25] M. Wilde, in *Quantum Information Theory* (Cambridge University Press, 2016) pp. xi–xii.
[26] J. Katz and Y. Lindell (2015) p. 43.
[27] D. Gottlieb, C.-W. Shu, A. Solomonoff, and H. Vandeven, Journal of Computational and Applied Mathematics **43**, 81 (1992).
[28] F. Mezzadri, arXiv e-prints , math-ph/0609050 (2006), arXiv:math-ph/0609050 [math-ph].
[29] J. Haferkamp, Quantum **6**, 795 (2022).
[30] S. Yoshida, A. Soeda, and M. Murao, Physical Review Letters **131** (2023), 10.1103/physrevlett.131.120602.
[31] K. M. Svore, M. B. Hastings, and M. Freedman, "Faster phase estimation," (2013), arXiv:1304.0741 [quant-ph].
[32] S. Aaronson and P. Christiano, "Quantum money from hidden subspaces," (2012), arXiv:1203.4740 [quant-ph].
[33] D. Petz and J. Reffy, "On asymptotics of large haar distributed unitary matrices," (2003), arXiv:math/0310338 [math.PR].
[34] S. Axler, *Linear algebra done right (eBook)*, 3rd ed. (Springer, Cham, 2015).
[35] W. Pleśniak, Journal of Approximation Theory **61**, 106 (1990).