Quantum Science and Technology

PAPER

On the connection between quantum pseudorandomness and quantum hardware assumptions

Mina Doosti[1,*], **Niraj Kumar**[1], **Elham Kashefi**[1,2] and **Kaushik Chakraborty**[1,*]

[1] School of Informatics, 10 Crichton St., University of Edinburgh, United Kingdom
[2] CNRS, LIP6, Sorbonne Université, 4 place Jussieu, 75005 Paris, France
[*] Authors to whom any correspondence should be addressed.

E-mail: m.doosti@sms.ed.ac.uk and kchakrab@exseed.ed.ac.uk

Keywords: quantum pseudorandomness, quamtum hardware assumptions, quantum PUF, pseudorandom unitaries

OPEN ACCESS

RECEIVED
15 November 2021

REVISED
30 March 2022

ACCEPTED FOR PUBLICATION
13 April 2022

PUBLISHED
29 April 2022

Abstract

This paper, for the first time, addresses the questions related to the connections between quantum pseudorandomness and quantum hardware assumptions, specifically quantum physical unclonable functions (qPUFs). Our results show that efficient pseudorandom quantum states (PRS) are sufficient to construct the challenge set for universally unforgeable qPUFs, improving the previous existing constructions based on the Haar-random states. We also show that both the qPUFs and the quantum pseudorandom unitaries (PRUs) can be constructed from each other, providing new ways to obtain PRS from the hardware assumptions. Moreover, we provide a sufficient condition (in terms of the diamond norm) that a set of unitaries should have to be a PRU in order to construct a universally unforgeable qPUF, giving yet another novel insight into the properties of the PRUs. Later, as an application of our results, we show that the efficiency of an existing qPUF-based client–server identification protocol can be improved without losing the security requirements of the protocol.

1. Introduction

Pseudorandomness is one of the most fundamental concepts in the domain of cryptography and complexity theory. In contrast to true randomness, it captures the notion of primitives that behaves randomly to the computationally-bounded observers [1–3]. The pseudorandom objects like pseudorandom number generators (PRGs) and pseudorandom functions (PRFs) play a crucial role in designing classical symmetric key cryptography protocols for secure communication [4–8]. These pseudorandom objects can be designed by exploiting the algebraic properties of the families of keyed functions like the keyed hash functions or from some hardware assumptions like the physical unclonable functions (PUFs). In the classical world, the relationship between PUF and pseudorandomness is well-studied [9]. Similar to classical pseudorandomness, recently Ji *et al* [10] introduced the concept of quantum pseudorandomness such as pseudorandom quantum states (PRSs) and pseudorandom unitaries (PRUs) as families of states or unitary transformations that are indistinguishable from Haar measure (true random measure) to any quantum computationally-bounded observers. On the other hand, similar to the classical PUFs, recently, we have the concept of the quantum PUFs [11]. However, unlike the classical case, the relation between the quantum pseudorandomness and the quantum PUFs is not well-explored. The existing PRS schemes are constructed under computational assumptions such as quantum-secure PRF (qPRFs) or quantum secure one-way functions [10, 12]. An interesting question that arises is whether quantum pseudorandomness can be achieved under a different set of assumptions? In this paper, to the best of our knowledge, for the first time, we show the construction of quantum PRUs from quantum PUFs and vice-versa.

Quantum PRs are an ensemble of a keyed family of quantum states $\{|\phi_k\rangle\}_{k\in\mathcal{K}}$ that can be generated efficiently [10]. The pseudorandomness comes from the property that for any polynomial-time quantum adversary, any polynomial number of copies of the states that are sampled from the ensemble $\{|\phi_k\rangle\}_{k\in\mathcal{K}}$ is indistinguishable from the same number of copies of Haar-random states. Similarly, PRUs are an ensemble

of a keyed family of unitaries $\{U_k\}_{k\in\mathcal{K}}$ that can be implemented efficiently [10]. Analogous to the PRS, the pseudorandomness of the PRUs implies that with oracle access to the unitary, no polynomial-time quantum adversary can distinguish between the unitaries that are sampled from $\{U_k\}_{k\in\mathcal{K}}$ and the Haar-measure unitaries.

A PUF is designed to be a cost-efficient, and low resource hardware device that provides a unique physically defined digital fingerprint [13, 14]. Corresponding to a challenge it produces a unique response that acts as an identifier. In the case of classical PUFs, the uniqueness comes from the unique physical variations that occur naturally during the manufacturing process of the device. Such subtle physical variations of the hardware components during the manufacturing process can be easily measured but are infeasible to reproduce in practice. It is well known in the classical setting that theoretically, PUFs can be considered PRFs. However, in practice, most of the classical PUFs are vulnerable to machine learning-based attacks [15–17]. Due to this shortcoming, there is a significant interest in designing quantum PUFs that utilise quantum mechanical properties (qPUFs), where both the challenges and responses are quantum states [11, 18, 19]. Quantum challenges and responses feature an additional property that they cannot be cloned by the laws of quantum mechanics [20], in contrast to the classical case.

In general, a qPUF is modelled as a completely positive trace preserving (CPTP) map, which maps an input challenge state to a unique response state. In addition, a qPUF must also be unique i.e. two distinct qPUFs must generate different responses to any given challenge with high probability (*uniqueness* property), and it must be unforgeable by any bounded (quantum or classical) adversary trying to clone the device (*unforgeability property*). In [11], Arapinis *et al* developed a formal security notion for the qPUFs and provided a qPUF construction based on Haar-random unitaries with the challenge states also being drawn from the Haar-random state, to satisfy the unforgeability property. Moreover, in the same paper, the authors design a generic quantum emulation-based attack for forging any qPUF and proved that their generic construction is unforgeable against any polynomial-time quantum adversary. This construction, although secure, is not practical due to the Haar-random requirement on the unitaries and the states. The reason for this is the fact that sampling from Haar measure requires exponential resources [21] and hence is experimentally challenging [22]. The construction of the unitary qPUF itself was partially improved by the result of Kumar *et al* [23] where they constructed a qPUF based on unitary t-designs which are efficiently built. However, they still require the challenges to be drawn from the Haar-random set of states to prove the unforgeability property. Further, we emphasise that, unlike the classical PUFs, the literature on qPUFs is not yet mature, and we have only very few candidate designs for qPUFs as mentioned above.

In this work, we make substantial progress in the above inefficient requirement of the challenges being chosen from the Haar measure. Specifically, we show that PRS can help reduce the challenger's overhead significantly in choosing the challenge states—from inefficient Haar-random states to efficient PRS. We further show that PRUs can be used as a viable candidate for qPUFs. This result provides yet another novel and efficient technique for constructing qPUFs. Moreover, here we also investigate, whether qPUFs can be used as PRUs. Similar to the qPUF, PRU is also a relatively new concept, and to the best of our knowledge, there are no concrete designs for the PRUs. Our investigation in this paper helps establish a close connection between these two new fields, i.e., qPUFs and quantum pseudorandomness. This relation gives us novel insights into designing both qPUFs and the PRUs. We are optimistic that the connections that we foster here would benefit both communities and the advances in one field would help to enrich the advances in the other. In the next subsection, we give a brief outline of our results.

1.1. Result overview

In this paper, we first address the inefficiency issue of the qPUF design in [11, 23] and prove the security against quantum polynomial-time (QPT) adversaries even if the challenge states are sampled from a set of PRSs.

Theorem 1 (informal). *Any unitary qPUF satisfies unforgeability with the challenges that are selected from a PRSs family (instead of Haar random states) against QPT adversaries.*

Here we also show that the PRUs can be used as qPUFs. Moreover, we establish a connection between a unitary family of qPUFs, with a specific practical requirement, and PRUs.

Theorem 2 (informal). *Any PRU family can be a unitary qPUF family.*

Theorem 3 (informal). *A family of practically unknown unitaries (UUs) is also a PRU family. Hence any unitary qPUF family that satisfies practical unknownness, is also a PRU family.*

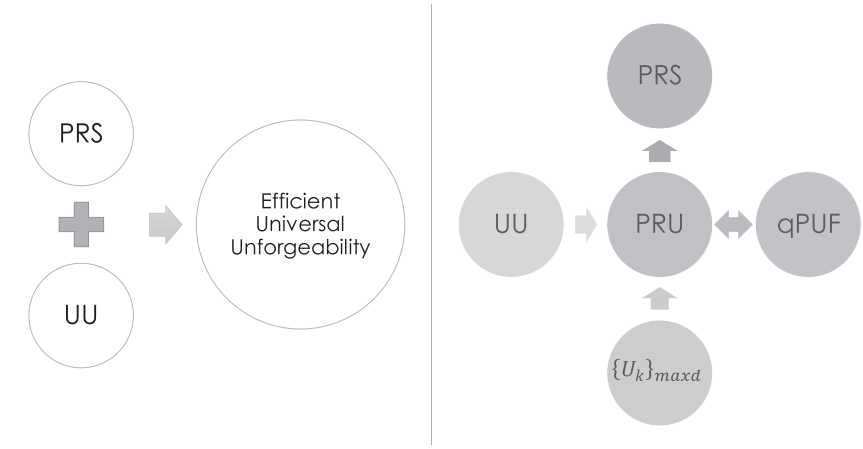

Figure 1. Demographic summary of the results. The left hand figure demonstrates theorem 9 stating that the universal unforgeability of UUs can be achieved efficiently using PRS. The right figure depicts the relationship between UUs, qPUFs, PRUs and families of almost maximally-distanced unitaries ($\{U_k\}_{\max d}$) proved in the theorems 10, 11, 12, and 13. It also shows that they can be used as generators for PRSs.

Later, we give a novel construction of PRUs from the family of qPUFs by exploring yet another hardware requirement which is their uniqueness property. The following result can also be applied to any unitary family with almost-maximal uniqueness, not only qPUFs.

Theorem 4 (informal). *Any family of unitary transformation of over d-dimensional Hilbert space satisfying the almost-maximal uniqueness in the diamond norm is also a PRU family for sufficiently large d. Hence any PUF family satisfying this degree of uniqueness, is also a PRU.*

The demographic summary of the above theorems can be found in figure 1. We finish our paper with a secure and efficient qPUF-based client verification protocol using our result from theorem 1.

Theorem 5 (informal). *The qPUF-based identification protocols in [24] can achieve the same security guarantee against QPT adversary if the Haar-random states are replaced with PRS.*

1.2. Notations

Here we provide some of the widely-used notations in this paper.

- PRG: pseudorandom generator.
- PRF: pseudorandom function.
- qPRF: quantum-secure pseudorandom function.
- PRS: pseudorandom state.
- PRU: pseudorandom unitary.
- qPUF: quantum physical unclonable function.
- QPT: quantum polynomial-time.
- UU: unknown unitary transformation.
- CRP: challenge response pair.
- BQP: bounded quantum polynomial.
- CPTP: completely positive trace preserving.
- $F(.,.)$: Uhlmann's fidelity.
- μ: Haar measure.
- λ: security parameter.

2. Preliminaries

This section presents the various ingredients required for our results and proofs.

2.1. Quantum pseudorandomness

Pseudorandomness is a central concept in modern cryptography which has also been extended to the quantum regime. Here we mention different notions that have been defined or extended into the quantum world namely, PRSs, qPRFs and their quantum analogue, namely quantum PRUs.

2.1.1. Pseudorandom quantum states

Definition 1 [PRSs [10]]. Let $\mathcal{H}$ be a Hilbert space and $\mathcal{K}$ the key space. $\mathcal{H}$ and $\mathcal{K}$ depend on the security parameter λ. A keyed family of quantum states $\{|\phi_k\rangle \in S(\mathcal{H})\}_{k\in\mathcal{K}}$ is *pseudorandom*, if the following two conditions hold:

- **Efficient generation.** There is an efficient quantum algorithm G which generates the state $|\phi_k\rangle$ on input k. That is, for all $k \in \mathcal{K}$, $G(k) = |\phi_k\rangle$.
- **Pseudorandomness.** Any polynomially many copies of $|\phi_k\rangle$ with the same random $k \in \mathcal{K}$ is computationally indistinguishable from the same number of copies of a Haar random state. More precisely, for any efficient quantum algorithm $\mathcal{A}$ and any $m \in \text{poly}(\lambda)$,

$$|\Pr_{k\leftarrow\mathcal{K}}[\mathcal{A}(|\phi_k\rangle^{\otimes m}) = 1] - \Pr_{|\psi\rangle\leftarrow\mu}[\mathcal{A}(|\psi\rangle^{\otimes m}) = 1]| = \text{negl}(\lambda), \tag{1}$$

  where μ is the Haar measure on $S(\mathcal{H})$.

2.1.2. Quantum-secure pseudorandom function

qPRFs are families of functions that look like truly random functions to QPT adversaries. Formally, qPRF are defined as follows:

Definition 2 [qPRFs [10]]. Let $\mathcal{K}, \mathcal{X}, \mathcal{Y}$ be the keyspace, the domain and range, all implicitly depending on the security parameter λ. A keyed family of functions $\{\text{PRF}_k : \mathcal{X} \to \mathcal{Y}\}_{k\in\mathcal{K}}$ is a qPRF if for any polynomial-time quantum oracle algorithm $\mathcal{A}$, PRF_k with a random $k \leftarrow \mathcal{K}$ is indistinguishable from a truly random function $f \leftarrow \mathcal{Y}^{\mathcal{X}}$ in the sense that:

$$|\Pr_{k\leftarrow\mathcal{K}}[\mathcal{A}^{\text{PRF}_k}(1^\lambda) = 1] - \Pr_{f\leftarrow\mathcal{Y}^{\mathcal{X}}}[\mathcal{A}^{f}(1^\lambda) = 1]| = \text{negl}(\lambda). \tag{2}$$

2.1.3. PRUs operators

These are unitary equivalent of PRFs defined as follows.

Definition 3 [PRU operators [10]]. A family of unitary operators $\{U_k \in \mathcal{U}(\mathcal{H})\}_{k\in\mathcal{K}}$ is a PRU if two conditions hold:

- **Efficient computation.** There is an efficient quantum algorithm Q such that for all k and any state $|\psi\rangle \in S(\mathcal{H}), Q(k, |\psi\rangle) = U_k|\psi\rangle$.
- **Pseudorandomness.** U_k with a random key k is computationally indistinguishable from a Haar random unitary operator. More precisely, for any efficient quantum algorithm $\mathcal{A}$ that makes at most polynomially many queries to the oracle:

$$|\Pr_{k\leftarrow\mathcal{K}}[\mathcal{A}^{U_k}(1^\lambda) = 1] - \Pr_{U\leftarrow\mu}[\mathcal{A}^{U}(1^\lambda) = 1]| = \text{negl}(\lambda), \tag{3}$$

  where μ is the Haar measure on $S(\mathcal{H})$. Note that here we focus on the pseudorandomness condition of the PRU definition.

2.1.4. UU transformations

We also mention a relevant notion to PRU, called a family of UUs defined in [11], that can also be interpreted as single-shot pseudorandomness.

Definition 4 (UU transformation [11]). We say a family of unitary transformations U^u, over a d-dimensional Hilbert space $\mathcal{H}^d$ is called UUs if for all QPT adversaries $\mathcal{A}$ the probability of estimating the output of U^u on any state $|\psi\rangle \in \mathcal{H}^d$ selected uniformly from Haar measure, is at most negligibly higher than the probability of estimating the output of a Haar random unitary operator on that state:

$$|\Pr_{U\leftarrow U^u}[F(\mathcal{A}(|\psi\rangle), U|\psi\rangle) \geqslant \delta(\lambda)] - \Pr_{U_\mu\leftarrow\mu}[F(\mathcal{A}(|\psi\rangle), U_\mu|\psi\rangle) \geqslant \delta(\lambda)]| = \text{negl}(\lambda), \tag{4}$$

where $\delta(\lambda)$ is any non-negligible function in the security parameter.

We note that this definition characterises a notion of *single-shot* indistinguishability from the family of Haar-random unitaries. Thus the adversary has only a single black-box query access to the unitary, but can have some existing prior information from the family that can be used for estimating the output. The definition intuitively states that a family of unitary is unknown when no such useful information exist about the family prior to the query access.

2.2. Quantum adversarial model and security definitions

Strong notions of the security for quantum cryptographic proposals require cryptanalysis against adversaries which also possess quantum capabilities of varying degrees [25–27]. The strongest of such notions is achieved by assuming no restrictions on the adversary's computational power and resources. This security model, also known as security against *unbounded adversary*, is usually too strong to be achieved by most cryptographic primitives such as qPUFs. It has been shown in [11], that unitary qPUFs cannot remain secure against an unbounded adversary. Thus the standard security model that we also use in this paper is the notion of security against efficient quantum adversaries, or in other words, QPT adversaries. We define such an adversary in the context of qPUFs. A QPT adversary with query access to qPUF is defined as an adversary that can query the qPUF oracle with polynomially many (in the security parameter) arbitrary challenges and has a polynomial sized quantum register to store the quantum CRPs. The QPT adversary is also allowed to run any efficient quantum algorithm. The security of most qPUF-based cryptographic protocols relies on the unforgeability property of qPUF.

Here we follow the same definitions of *universal* unforgeability (also called *selective unforgeability* in the context of quantum PUFs) defined in [11, 28] and restate them as follows:

Game 1 *[Universal unforgeability]. Let* Gen, $\mathrm{U}_{\mathcal{E}}$ *and* $\mathcal{T}$ *be the generation, evaluation and test algorithms of the quantum primitive* $\mathcal{E}$ *respectively. We define the following game G running between an adversary* $\mathcal{A}$ *and a challenger* $\mathcal{C}$*:*

Setup phase. *The challenger* $\mathcal{C}$ *runs* $\mathrm{Gen}(\lambda)$ *and reveals to the adversary* $\mathcal{A}$*, the domain and range Hilbert space of* $\mathrm{U}_{\mathcal{E}}$ *respectively denoted by* $\mathcal{H}_{in}$ *and* $\mathcal{H}_{out}$

Learning phase. *For* $i = 1 : k$.

- $\mathcal{A}$ *issues arbitrary query* $\rho_i \in \mathcal{S}(\mathcal{H}_{in})$ *to* $\mathcal{C}$*;*
- $\mathcal{C}$ *generates* $\rho_i^{\mathrm{out}} = \mathrm{U}_{\mathcal{E}}\rho_i\mathrm{U}_{\mathcal{E}}^{\dagger}$ *and sends* ρ_i^{out}*, to* $\mathcal{A}$*;*

Challenge phase. $\mathcal{C}$ *chooses a quantum state* ρ^* *at random from the uniform distribution (Haar) over the Hilbert space* $\mathcal{H}_{in}$ *and sends* ρ^* *to* $\mathcal{A}$*. The challenger can generate arbitrary copies of* ρ^*.

Guess phase.

- $\mathcal{A}$ *generates the forgery* ω *and sends it to* $\mathcal{C}$*;*
- $\mathcal{C}$ *runs the test algorithm* $b \leftarrow \mathcal{T}((\rho*^{\mathrm{out}})^{\otimes\kappa_1}, \omega)$ *where* $b \in \{0, 1\}$ *and outputs b. The adversary wins the game if* $b = 1$.

Definition 5 (Quantum universal unforgeability). A primitive provides quantum universal unforgeability if the success probability of any QPT adversary $\mathcal{A}$ in winning the game 1 is negligible in the security parameter λ

$$\Pr[1 \leftarrow G(\lambda, \mathcal{A})] = \mathrm{negl}(\lambda). \tag{5}$$

Throughout the paper we widely use the result from [11, 28] implying that UU transformations as formalized by definition 4, can satisfy the notion of universal unforgeability:

Theorem 6 ([28]). *Primitives with their evaluation algorithm being an UU transformation are universally unforgeable.*

2.3. Quantum equality tests

Distinguishing two unknown quantum states is a central ingredient in quantum information processing. This task is often referred to as the 'state discrimination task'. The celebrated Holevo–Helstrom bound [29] relates the optimal distinguishability of two unknown states with the trace distance between the density matrices. This implies that unless the states are the same (up to a global factor), it is impossible to deterministically distinguish the two states. An important application of state discrimination is the task of equality testing [30–32]. This is an extremely simple task but a building block for lots of complicated quantum protocols. The objective of equality testing, one that we consider in our work, is to test whether two *unknown* quantum states are the same. This is a well-studied topic and we describe the optimal quantum protocols for equality testing.

2.3.1. SWAP test

Given a single copy of two unknown quantum states ρ and σ, is there a simple test to optimally determine whether the two states are equal or not? This question was answered in affirmative by Buhrman *et al* [30] when they provided a test called the SWAP test. This test was initially used by the authors to prove an exponential separation between classical and quantum resources in the simultaneous message passing model. Since then it has been used as a standard tool in the design of various quantum algorithms [33, 34]. A SWAP test circuit takes as an input the two unknown quantum states ρ and σ and attaches an ancilla $|0\rangle$. A Hadamard gate is applied to the ancilla followed by the control-SWAP gate and again a Hadamard on the

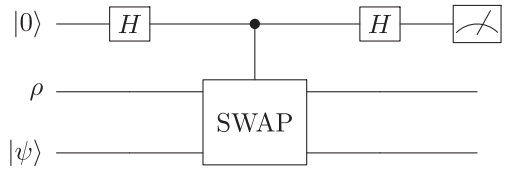

Figure 2. The SWAP test circuit.

ancilla qubit. Finally, the ancilla is measured in the computational basis and we conclude that the two states are equal if the measurement outcome is '0' (labelled accept). Figure 2 illustrates this test in the special case when the state σ is a pure state and shown by $|\psi\rangle$.

It can be shown that the probability the SWAP test accepts the states ρ and σ is [35],

$$\Pr[\text{SWAP accept}] = \frac{1}{2} + \frac{1}{2}\,\text{Tr}(\rho\sigma). \tag{6}$$

In the special case of when at least one of the states (let us say σ) is a pure state $\sigma = |\psi\rangle\langle\psi|$, the probability of acceptance is,

$$\Pr[\text{SWAP accept}] = \frac{1}{2} + \frac{1}{2}|\langle\psi|\rho|\psi\rangle| = \frac{1}{2} + \frac{1}{2}F(\rho, |\psi\rangle\langle\psi|). \tag{7}$$

Thus when at-least one of the two states is a pure state, the acceptance probability is related to the fidelity between the states. This implies when the states are the same, the probability of acceptance is 1. However, when the states are different then if the SWAP test accepts the states, this implies an error. Thus the error in the SWAP test when the states are different (also called the one-sided error) is the accept probability of the SWAP test while the states are not equal. This error can, however, be brought down to any desired error $\epsilon > 0$ by running multiple instances of the SWAP test circuit. The number of instances required to bring down the error probability to a desired ϵ is,

$$\begin{aligned}\Pr[\text{SWAP error}] = \prod_{j=1}^{M} \Pr[\text{SWAP accept}]_j = (\frac{1}{2} + \frac{1}{2}F)^M = \epsilon \\ \Rightarrow M(\log(1+F) - 1) = \log(\epsilon) \Rightarrow M \approx \mathcal{O}(\log(1/\epsilon))\end{aligned},$$

where $F = F(\rho, |\psi\rangle\langle\psi|) = \langle\psi|\rho|\psi\rangle$ and we use the fact that fidelity is independent of ϵ.

2.3.2. GSWAP test

The above SWAP test is optimal in equality testing (in a single instance) of two unknown quantum states when one has a single copy of the two states. However, there are certain quantum protocols where one has access to multiple copies of one unknown state $|\psi\rangle$ and only a single copy of the other unknown state ρ and the objective is to provide an optimal equality testing circuit. Considering this scenario, Chabaud *et al* [36] provided an efficient construction of such a circuit, generalised SWAP (GSWAP) test circuit. A GSWAP circuit takes as an input a single copy of ρ, M copies of $|\psi\rangle$ and $\lceil \log M + 1 \rceil$ copies of the ancilla qubit $|0\rangle$. The generalised circuit is then run on the inputs, and the ancilla qubits are measured in the computational bases. Figure 3 is a generic illustration of such a circuit. For more details on the circuit refer to the original work [36]. It can be shown that the probability the GWAP circuit accepts two quantum states ρ and $|\psi\rangle$ is,

$$\Pr[\text{GSWAP accept}] = \frac{1}{M+1} + \frac{M}{M+1}\langle\psi|\rho|\psi\rangle = \frac{1}{M+1} + \frac{M}{M+1}F, \tag{8}$$

where $F = F(\rho, |\psi\rangle\langle\psi|)$. We note that in the special case of $M = 1$, the GSWAP test reduces to the SWAP test. Also in a single instance, GSWAP provides a better equality test compared to the SWAP test since it reduces the one-sided error probability. In the limit $M \to \infty$, we obtain the optimal acceptance probability of $\Pr[\text{accept}] = F = |\langle\psi|\rho|\psi\rangle|$. Another important feature of GSWAP is that it can achieve any desired success probability $\epsilon(\geqslant F)$ in just a single instance which is impossible to achieve using SWAP circuit. However, the number of copies required is exponentially more than the number of instances that the SWAP circuit has to run to achieve the same error probability,

$$\begin{aligned}\Pr[\text{GSWAP error}] = \Pr[\text{GSWAP accept}] = \frac{1}{M+1} + \frac{M}{M+1}F = \epsilon \\ \Rightarrow M \approx \mathcal{O}(1/\epsilon)\end{aligned}. \tag{9}$$

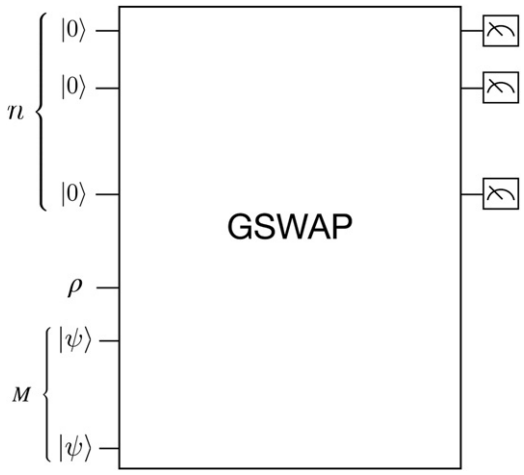

Figure 3. GSWAP: a generalisation of the SWAP test with a single copy of ρ and M copies of $|\psi\rangle$. The circuit also inputs $n = \lceil \log M + 1 \rceil$ ancilla qubits in the state $|0\rangle$. At the end of the circuit, the ancilla states are measured in the computational basis.

Hence one decides the use of either SWAP test or GSWAP test depending on the specific application.

2.4. Quantum physical unclonable functions

A quantum physical unclonable function, or qPUF, is a secure hardware cryptographic device that is, by assumption, hard to clone or reproduce and utilises properties of quantum mechanics [11]. Similar to a classical PUF [37], a qPUF is assessed via CRPs. However, in contrast to a classical PUF where the CRPs are classical states, the qPUF CRPs are quantum states. We use the definition of qPUF introduced in [11] for the purpose of this paper.

A qPUF manufacturing process involves a quantum generation algorithm, 'qGen', which takes as an input a security parameter λ and generates a PUF with a unique identifier **id**,

$$\text{qPUF}_{\mathbf{id}} \leftarrow \text{qGen}(\lambda.) \tag{10}$$

Next we define the mapping provided by $\text{qPUF}_{\mathbf{id}}$ which takes any input quantum state $\rho_{\text{in}} \in \mathcal{S}(\mathcal{H}^{d_{\text{in}}})$ to the output state $\rho_{\text{out}} \in \mathcal{S}(\mathcal{H}^{d_{\text{out}}})$. Here $\mathcal{H}^{d_{\text{in}}}$ and $\mathcal{H}^{d_{\text{out}}}$ are the input and output Hilbert spaces respectively corresponding to the mapping that $\text{qPUF}_{\mathbf{id}}$ provides. This process is captured by the 'qEval' algorithm which takes as an input a unique $\text{qPUF}_{\mathbf{id}}$ device and the state ρ_{in} and produces the state ρ_{out},

$$\rho_{\text{out}} \leftarrow \text{qEval}(\text{qPUF}_{\mathbf{id}}, \rho_{\text{in}}). \tag{11}$$

A qPUF needs to satisfy a few requirements. The first property, $\boldsymbol{\delta_{\text{r}}}$**-robustness** [11], ensures that if the qPUF is queried separately with two input quantum states ρ_{in} and σ_{in} that are δ_{r}-indistinguishable to each other, then the output quantum states ρ_{out} and σ_{out} must also be δ_{r}-indistinguishable. The second property, $\boldsymbol{\delta_{\text{c}}}$**-collision resistance** [11], ensures that if the same qPUF is queried separately with two input quantum states ρ_{in} and σ_{in} that are δ_{c}-distinguishable, then the output states ρ_{out} and σ_{out} must also be δ_{c}-distinguishable with an overwhelmingly high probability. Here, the distinguishability is defined with respect to fidelity such that two quantum states ρ and σ are δ-distinguishable if $0 \leqslant F(\rho, \sigma) \leqslant 1 - \delta$, where $F(\rho, \sigma)$ is the Uhlmann's fidelity. Alternatively, other distance measures such as trace norm, Euclidean norm (any Schatten p-norm) can also be used to define security requirements for qPUF.

The last requirement, which we will use in this paper is the $\boldsymbol{\delta_{\text{u}}}$**-uniqueness** [11]. This property ensures that the generation process of qPUF can generate sufficiently distinguishable qPUFs. This is captured by modelling each qPUF as a quantum operation characterised by a CPTP map that takes the input quantum states in $\mathcal{H}^{d_{\text{in}}}$ to output states in $\mathcal{H}^{d_{\text{out}}}$. We say that two such maps Λ_i^{qPUF} and Λ_j^{qPUF} are δ_{u} distinguishable if

$$\Pr[\|\Lambda_i^{\text{qPUF}} - \Lambda_j^{\text{qPUF}}\|_\diamond \geqslant \delta_u[i \neq j]] \geqslant 1 - \epsilon(\lambda), \tag{12}$$

where $\| \cdot \|_\diamond$ is the diamond norm distance measure for the distinguishability of two quantum operations, and $\epsilon(\lambda)$ is a negligible function in the security parameter λ.

The diamond norm is a distance metric for any two CPTP quantum operations Λ_1, Λ_2. It is defined as,

$$\|\Lambda_1 - \Lambda_2\|_\diamond = \max_\rho(\|(\Lambda_1 \otimes \mathbb{I})[\rho] - (\Lambda_2 \otimes \mathbb{I})[\rho]\|_1). \tag{13}$$

Operationally it quantifies the maximum probability of distinguishing operation Λ_1 from Λ_2 in a single-use.

It has been shown in [11] that unitary maps and ϵ-close to unitary channels, under certain additional conditions, can be considered as a qPUF. We restate the following theorem from [11]:

Theorem 7 (from [11]). *Let $\mathcal{E}(\rho)$ be a completely positive and trace-preserving (CPT) map described as follows:*

$$\mathcal{E}(\rho) = (1 - \epsilon)U\rho U^\dagger + \epsilon\tilde{\mathcal{E}}(\rho), \tag{14}$$

where U is a unitary transformation, $\tilde{\mathcal{E}}$ is an arbitrary (non-negligibly) contractive channel and $0 \leqslant \epsilon \leqslant 1$. Then $\mathcal{E}(\rho)$ is a $(\lambda, \delta_r, \delta_c)$-qPUF for any λ, δ_r, and δ_c and with the same dimension of domain and range Hilbert space, if and only if $\epsilon = \text{negl}(\lambda)$.

This is because the properties of robustness and collision resistance can be satisfied by an almost unitary map as a subclass of all CPTP qPUFs. The uniqueness property on the other hand, is quite challenging and [11, 23] showed that one can achieve uniqueness if one samples a unitary from a Haar random set of unitaries. Further [23], numerically showed that one can achieve uniqueness if one sample the unitary from a unitary t-design set. In this work, we show that one can achieve this property by sampling from a PRU set. Here we consider the qPUF construction to be a unitary matrix $U \in \mathbb{C}^{d\times d}$, where $d = d_{\text{in}} = d_{\text{out}}$.

A crucial security feature of the qPUF device is its unforgeability property. The unforgeability for qPUFs as a quantum primitive is captured by definition 5.

It has also been shown in [11] that even though qPUFs cannot satisfy a general existential unforgeability, which is a strong notion for capturing the unpredictability of such hardware, all unitary qPUFs that satisfy the notion of unknownness can satisfy the notion of universal unforgeability. This general possibility result is the consequence of the following theorem proved against any QPT adversary:

Theorem 8 (restated from [11]). *For any unitary qPUF characterised, and any non-zero acceptance threshold δ in the fidelity, the success probability of any QPT adversary $\mathcal{A}$ in the universal unforgeability game is bounded as follows:*

$$\Pr[1 \leftarrow G(\lambda, \mathcal{A})] \leqslant \frac{\tilde{d} + 1}{d}, \tag{15}$$

where d is the dimension of the domain Hilbert space, and $0 \leqslant \tilde{d} \leqslant d - 1$ is the dimension of the largest subspace of $\mathcal{H}^d$ that the adversary can span in the learning phase of the game 1.

This possibility result, has been later used in [24] to prove security of qPUF-based identification protocols.

3. Efficient unforgeability with PRS

In this section, we investigate the problem of *universal unforgeability* with efficiently producible PRSs. As specified in the game 1, the challenge states need to be picked at random from Haar measure by the challenger. This is an important condition for the unforgeability of UU transformations. Nevertheless, producing Haar random state is a challenging and resource-intensive task. Hence to take the first step towards the realization of universally unforgeable schemes, we attempt to replace this condition with its computational equivalent, i.e. the notion of PRS, introduced in the preliminary. We first relax this condition by defining a variation of the universal unforgeability game, namely *efficient universal unforgeability* where the challenger picks the challenge states from a pseudorandom family of quantum states. Then we formally prove that UUs satisfy this notion of unforgeability. Furthermore, we discuss how such PRSs can be efficiently generated using classical PRFs.

We define the *efficient universal unforgeability* as bellow:

Definition 6 (Efficient quantum universal unforgeability). Let game G_{eqUnf} be same as game 1 except that in the challenge phase, the challenge states are being picked from PRS family of states with a generation algorithm $G(k)$ with a key $k \in \mathcal{K}$, realised in the setup phase. A primitive provides efficient quantum

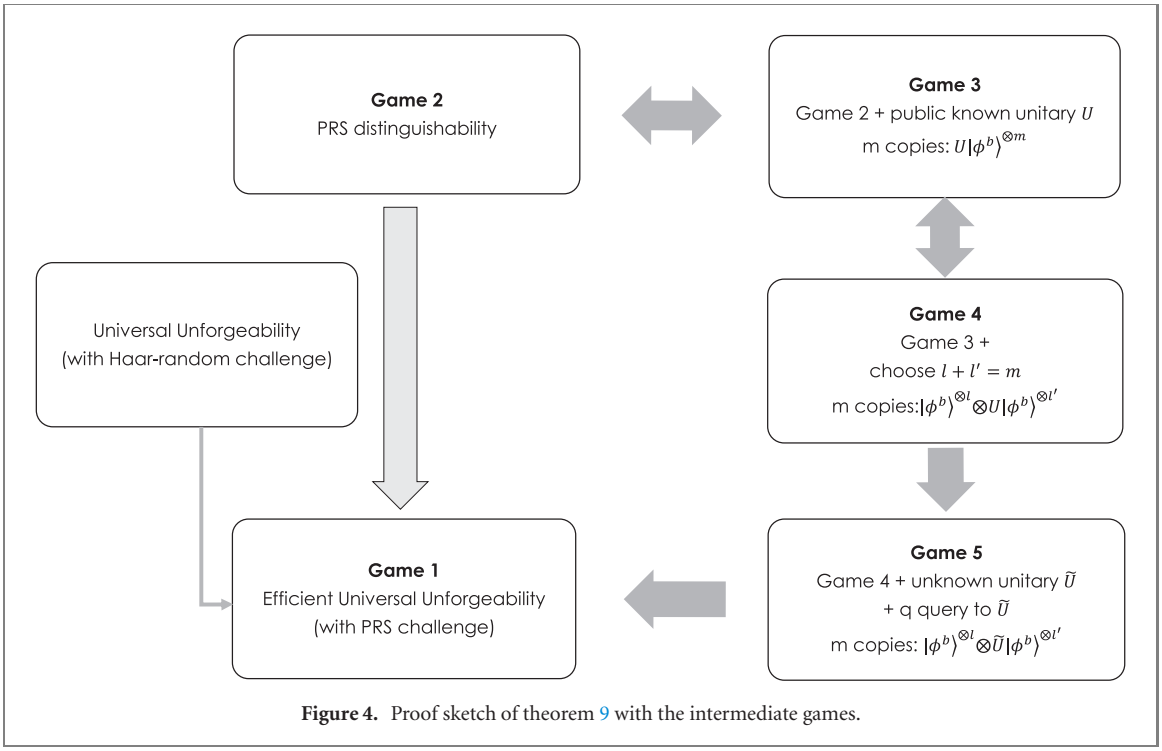

Figure 4. Proof sketch of theorem 9 with the intermediate games.

universal unforgeability if the success probability of any QPT adversary $\mathcal{A}$ in winning the G_{eqUnf} is negligible in the security parameter λ,

$$\Pr[1 \leftarrow G_{\text{eqUnf}}(\lambda, \mathcal{A})] = \text{negl}(\lambda). \tag{16}$$

Now, for simplicity in the proof, we also define the pseudorandomness property of the PRS with a game as formalized in the following:

Game 2 *[PRS distinguishability game]. Let $\mathcal{H}$ be a Hilbert space and $\mathcal{K}$ the key space. The dimension of $\mathcal{H}$ and size of $\mathcal{K}$ depend on the security parameter λ. Let $\{|\phi_k\rangle \in S(\mathcal{H})\}_{k\in\mathcal{K}}$ be a keyed family of quantum states with efficient generation algorithm $G(k) = |\phi_k\rangle$ on input k. We define the following distinguishability game between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$:*

Setup phase. *The challenger $\mathcal{C}$ selects $k \xleftarrow{\$} \mathcal{K}$ and $b \xleftarrow{\$} \{0, 1\}$ at random.*

Challenge phase.

- *If $b = 0$ (PRS world): $\mathcal{C}$ prepares m copies of $|\phi^0\rangle = |\phi_k\rangle$ by running $G(k)$.*
- *If $b = 1$ (random world): $\mathcal{C}$ prepares m copies of a Haar-random state $|\phi^1\rangle = |\psi\rangle$.*
- *$\mathcal{C}$ sends $|\phi^b\rangle^{\otimes m}$ to $\mathcal{A}$.*

Guess phase. *$\mathcal{A}$ guesses b.*

Now we establish our main result regarding the efficient unforgeability of UU primitives.

Theorem 9. *Any unitary transformation* U *selected from an UU family according to definition 4, satisfies efficient universal unforgeability against QPT adversaries.*

Proof. We prove by contraposition in a game-based setting. We want to show that starting from the assumption of pseudorandomness of PRS in the efficient universal unforgeability game, if there exists a QPT adversary who succeeds to win this game, with non-negligible probability, there will also exist an adversary who can efficiently distinguish between PRS and Haar random states, which is in contrast with the initial assumption and as a result show a contradiction. First, we need to specify the following games:

- Game 1: this is the universal unforgeability game as specified in game 1, with the only difference that the challenge state $\rho^* = |\phi_{k^*}\rangle\langle\phi_{k^*}|$ is chosen from a PRS family.
- Game 2: this is the PRS distinguishability game as specified in game 2.
- Game 3: this is a variation of game 2 where $\mathcal{C}$ in addition to initial resources, has also access to a publicly known and implementable unitary U. In the challenge phase, $\mathcal{C}$ does the following: Generates m copies of $|\phi^0\rangle = |\phi_k\rangle$ using $G(k)$, or m copies of Haar random states $|\phi^1\rangle = |\psi\rangle$ depending of b,

then on each copies applies the public unitary U and sends $(U|\phi^b\rangle)^{\otimes m}$ to $\mathcal{A}$. The rest of the game is similar to game 2.

- Game 4: this game is similar to game 3, except that $\mathcal{C}$ publicly chooses an l and $l^{'}$ such that $l + l' = m$ and sends l copies of the generated state and l' copies of the state after applying the unitary U, i.e. sends $|\phi^b\rangle^{\otimes l} \otimes (U|\phi^b\rangle)^{\otimes l'}$ to $\mathcal{A}$.
- Game 5: this game is similar to game 4 except the public unitary has been replaced by an UU $\tilde{U}$ of the same dimension. Hence in this game, similar to game 1, we also assume a learning phase for $\mathcal{A}$ before the challenge phase. The learning phase is as follows: $\mathcal{A}$ issues $q = \text{poly}(\lambda)$ queries $\{\rho_i\}_{i=1}^q$ to $\mathcal{C}$, on each query $\mathcal{C}$ generates $\rho_i^{\text{out}} = \tilde{U}\rho_i\tilde{U}^\dagger$ by applying the unitary on the query state and sends ρ_i^{out} to $\mathcal{A}$. Then the rest of the game is similar to game 4 and at the end of the challenge phase $\mathcal{A}$ receives $|\phi^b\rangle^{\otimes l} \otimes (\tilde{U}|\phi^b\rangle)^{\otimes l'}$

Figure 4 illustrates the sketch of the proof. We first show that game 2, game 3 and game 4 are equivalent. We note that unitary transformations are distance invariant and hence they also preserve the distribution of states, as a result applying a unitary to the state will not affect the distribution and the distinguishability of the quantum states, and as a result game 2 and 3 are equivalent. Furthermore, in game 4, since the unitary is public, $\mathcal{A}$ can either apply U on the first l copies $|\phi^b\rangle^{\otimes l}$ and end up with m copies of $(U|\phi^b\rangle)^{\otimes m}$ or alternatively apply $U^\dagger$ on the next $l^{'}$ copies $(U|\phi^b\rangle)^{\otimes l'}$ and get m copies of $|\phi^b\rangle^{\otimes m}$, and hence be reduced to either game 2 or game 3. As a result, we have

$$\text{Game } 2 \equiv \text{Game } 3 \equiv \text{Game } 4. \tag{17}$$

Now we show that game 4 implies game 5 i.e. if an adversary wins the distinguishability in game 5 with a probability p, she will also win in game 4 with the same probability.

The proof is straightforward as highlighted here. Let $\mathcal{A}$ be an adversary who wins game 5, which means after the learning phase leading to a polynomial-size database of the input–outputs of the UU $\tilde{U}$, and receiving $|\phi^b\rangle^{\otimes l} \otimes (\tilde{U}|\phi^b\rangle)^{\otimes l'}$, they can guess b with non-negligible probability better than random guess:

$$\Pr_{|\phi^b\rangle}[b \leftarrow \mathcal{A}(|\phi^b\rangle^{\otimes l} \otimes (\tilde{U}|\phi^b\rangle)^{\otimes l'})] = \frac{1}{2} + \text{nonnegl}(\lambda). \tag{18}$$

Now let us assume an adversary $\mathcal{A}'$ who plays the game 4 and has to guess b by receiving the state $|\phi^b\rangle^{\otimes l} \otimes (U|\phi^b\rangle)^{\otimes l'}$ can guess b with same l and l' where U is a public unitary. Now $\mathcal{A}'$ can run $\mathcal{A}$ as a subroutine and $\mathcal{A}'$ sends to $\mathcal{A}$ the response to the same learning phase states from U. Since U is public $\mathcal{A}'$ can run it locally and produce the required queries. Then $\mathcal{A}'$ also sends the state $|\phi^b\rangle^{\otimes l} \otimes (U|\phi^b\rangle)^{\otimes l'}$ to $\mathcal{A}$ and since $\mathcal{A}$ guesses the b with a probability non-negligibly better than half, so does $\mathcal{A}'$. As a result, we have shown that:

$$\text{Game } 4 \Rightarrow \text{Game } 5. \tag{19}$$

Finally, we show that game 5 implies game 1. By contradiction, we assume there exist an adversary $\mathcal{A}$ who wins the unforgeability game with non-negligible probability. Let $\tilde{U}$ be the UU and $\mathcal{A}$'s forgery state be $|\omega\rangle$ and let the challenge state of game 1 be a PRS state $|\phi_k\rangle$. We have:

$$\begin{aligned}\Pr[1 \leftarrow G_{\text{eqUnf}}(\lambda, \mathcal{A})] &= \Pr_k[1 \leftarrow \mathcal{T}(|\omega\rangle, (\tilde{U}|\phi_k\rangle)^{\otimes\kappa})] \\ &= \Pr_k[F(|\omega\rangle, \tilde{U}|\phi_k\rangle) = \text{nonnegl}(\lambda)] \\ &= \text{nonnegl}(\lambda).\end{aligned} \tag{20}$$

Now we construct an adversary $\mathcal{A}'$ playing an instance of game 5 where $l = 1$ and $l' = m - 1$. In the learning phase $\mathcal{A}$ interacts with the UU $\tilde{U}$ with the same learning phase states required for $\mathcal{A}$ and sends the query states $\{\rho_i^{\text{out}}\}_{i=1}^q$ together with the challenge state $|\phi^b\rangle$ to $\mathcal{A}$. Then $\mathcal{A}$ produces the forgery $|\omega\rangle$ as their guess for $\tilde{U}|\phi^b\rangle$. Now $\mathcal{A}'$ verifies $|\omega\rangle$ with the same test algorithm $\mathcal{T}$ where $\kappa = m - 1$, since $\mathcal{A}'$ has $m - 1$ copies of $\tilde{U}|\phi^b\rangle$ to check with. Then $\mathcal{A}'$ outputs the same b as outputted by the $\mathcal{T}$. The success probability of $\mathcal{A}'$ is as follows. If $b = 0$, the state is a PRS and the contradiction assumption is satisfied. Hence $\mathcal{A}$'s forgery state will pass the test algorithm with high probability. On the other hand if $b = 1$, the state has been picked from Haar measure and as a result of theorem 6, the success probability of $\mathcal{A}$ winning the forgery game and producing a state to pass the test is negligible. Since guessing b in game 5 with probability better than random guess is equivalent to the difference between the success probability of $\mathcal{A}'$ in winning

the game in the two different scenarios, we have:

$$\begin{aligned}
&|\Pr_{k\leftarrow\mathcal{K}}[\mathcal{A}'(|\phi_k\rangle\otimes(\tilde{U}|\phi_k\rangle)^{\otimes m-1})=1]-\Pr_{|\psi\rangle\leftarrow\mu}[\mathcal{A}'(|\psi\rangle\otimes(\tilde{U}|\psi\rangle)^{\otimes m-1})=1]|\\
&=|\Pr_{k\leftarrow\mathcal{K}}[\mathcal{A}(|\phi_k\rangle)=1]-\Pr_{|\psi\rangle\leftarrow\mu}[\mathcal{A}(|\psi\rangle)=1]| \qquad .\\
&=\text{nonnegl}(\lambda)-\text{negl}(\lambda)=\text{nonnegl}(\lambda)
\end{aligned} \tag{21}$$

Here, as a specific example, we can consider the GSWAP to be the equality test and, we show how this check can efficiently be performed to show the gap and hence the implication of the two later games. Let us denote the adversary's purified forgery state as $|\omega_b\rangle$. According to equation (8), the probability of the GSWAP accepting this state given $m-1$ copies of reference state $\tilde{U}|\phi^b\rangle$, has the following relation with the fidelity of the forgery state:

$$\Pr[\text{GSWAP accept}]=\frac{1}{m}+\frac{m-1}{m}F(\tilde{U}|\phi^b\rangle,|\omega_b\rangle). \tag{22}$$

Assuming $\mathcal{A}$ wins the unforgeability game for PRS state with non-negligible probability implies that this fidelity is a non-negligible value in the security parameter, hence $F(\tilde{U}|\phi^0\rangle,|\omega_0\rangle)=\delta=\text{nonnegl}(\lambda)$. On the other hand, for Haar-random state this fidelity is always a negligible value and we have that $F(\tilde{U}|\phi^1\rangle,|\omega_1\rangle)=\text{negl}(\lambda)$. As a result the difference between $\mathcal{A}$'s success probability in the two cases is as follows:

$$\begin{aligned}
&|\Pr_{k\leftarrow\mathcal{K}}[\mathcal{A}'(|\phi_k\rangle\otimes(\tilde{U}|\phi_k\rangle)^{\otimes m-1})=1]-\Pr_{|\psi\rangle\leftarrow\mu}[\mathcal{A}'(|\psi\rangle\otimes(\tilde{U}|\psi\rangle)^{\otimes m-1})=1]|\\
&=\frac{1}{m}+\frac{m-1}{m}F(\tilde{U}|\phi^0\rangle,|\omega_0\rangle)-\frac{1}{m}+\frac{m-1}{m}F(\tilde{U}|\phi^1\rangle,|\omega_1\rangle) \qquad .\\
&=\frac{m-1}{m}(\delta-\text{negl}(\lambda))\approx\frac{m-1}{m}\delta=\text{non negl}(\lambda)
\end{aligned} \tag{23}$$

As a result, we have shown that there exist a non-negligible gap and hence $\mathcal{A}'$ can also win the game 5. In conclusion, we have shown the following relation:

$$\text{Game 2}\equiv\text{Game 3}\equiv\text{Game 4}\Rightarrow\text{Game 5}\Rightarrow\text{Game 1}. \tag{24}$$

This means that an adversary winning the unforgeability game, with the challenge being picked from a PRS family, can also distinguish the PRS states from Haar random state which is a contradiction and it concludes the proof. □

We have formally shown that PRS states are enough to achieve quantum universal unforgeability. The next question is that how such states can be constructed. Ji *et al* [10] propose several constructions for generating a PRS family using classical qPRFs. Hence they show that PRS can be constructed under the assumption that quantum-secure one-way function exists. Another similar notion called asymptotically random state has also been introduced in [38]. In both works, first, oracle access to a classical random function is given to efficiently construct a PRS that is indistinguishable to Haar random states even for exponential adversaries. Then by relying on the existence of quantum-secure one-way function they replace the random function with a post-quantum secure PRF to achieve security against polynomial adversaries. With this approach, one can construct computationally secure n-qubit PRS which is also desired for unforgeability security property. Nevertheless, as discussed in [12], these methods are not scalable and also an n-qubit PRS generator cannot necessarily be used to produce a random state for k-qubit where $k<n$. For these reasons, in [12] the authors introduce a scalable construction for PRS which, unlike prior works, relies on randomising the amplitudes of the states instead of the phase. The authors use Gaussian sampling methods to efficiently achieve PRS.

4. From pseudorandom unitaries to UUs

We prove that a family of unitaries satisfying the computational assumption of PRU, is also a family of UU transformation. As a result of this implication, efficient constructions such as PRU or t-design can also satisfy the notion of universal unforgeability. Moreover, this result establishes for the first time, a link between a computational assumption of PRU with a hardware assumption such as unknownness.

Theorem 10. *A family of PRU, $\mathcal{U}=\{U_k\}_{k\in\mathcal{K}}$ is also a family of UU with respect to definition 4.*

Proof. We prove this by contradiction. Let $\mathcal{U}$ be a family of PRU but not a family of UU which means that there is a QPT adversary $\mathcal{A}$ who can estimate the output of a randomly picked $U\leftarrow\mathcal{U}$ where $\mathcal{U}$ is a UU, on

a state $|\psi\rangle$, non-negligibly better than the output of a $U \leftarrow \mu$ picked from a Haar-random unitaries μ over a d-dimensional Hilbert space. Thus for $\mathcal{A}$ the following holds:

$$\begin{aligned} &|\Pr_{U\leftarrow\mathcal{U}}\left[F(\mathcal{A}(|\psi\rangle), U|\psi\rangle) \geqslant \text{nonnegl}(\lambda)\right] - \Pr_{U_\mu\leftarrow\mu}[F(\mathcal{A}(|\psi\rangle), U_\mu|\psi\rangle) \geqslant \text{nonnegl}(\lambda)]| \\ &= \text{nonnegl}(\lambda). \end{aligned} \tag{25}$$

Let $\mathcal{A}$' be a QPT adversary who aims to break the pseudorandomness property of $\mathcal{U}$ using $\mathcal{A}$, and works as follows:

$\mathcal{A}$' picks $|\psi\rangle$ as one of her chosen inputs in the learning phase of the pseudorandomness game. Then $\mathcal{A}$' also runs $\mathcal{A}$ internally on $|\psi\rangle$.

From the previous equation we know that $\mathcal{A}$ can estimate the output of $U|\psi\rangle$ better than $U_\mu|\psi\rangle$ where U_μ is a Haar random unitary, by a non-negligible value. Also by definition, we know that the probability that any QPT algorithm estimates the output of any Haar randomly given unitary, is negligible, as the response maps to any random state in the Hilbert space $\mathcal{H}^d$ with exponential distribution [39, 40]. Thus the equation implies that:

$$|\Pr_{U\leftarrow\mathcal{U}}[F(\mathcal{A}(|\psi\rangle), U|\psi\rangle) \geqslant \text{nonnegl}(\lambda)]| = \text{nonnegl}(\lambda). \tag{26}$$

This means that $\mathcal{A}$ can estimate the output with non-negligible fidelity if the U had been picked from the family. Now $\mathcal{A}$' runs a quantum equality test on the $U|\psi\rangle$ obtained in the learning phase and $\mathcal{A}(|\psi\rangle)$. In the case where U is picked from the PRU family, the estimated output and the real output have non-negligible fidelity and the test returns equality with a non-negligible probability. Otherwise, the test shows that they are not equal and $\mathcal{A}$' can conclude that the unitary has been picked from Haar unitaries. Thus for $\mathcal{A}$' we have:

$$\Pr_{U\leftarrow\mathcal{U}}[\mathcal{A}'^{U}(1^\lambda) = 1] - \Pr_{U_\mu\leftarrow\mu}[\mathcal{A}'^{U_\mu}(1^\lambda) = 1] = \text{nonnegl}(\lambda). \tag{27}$$

Therefore we conclude the contradiction. □

We have shown that PRU implies UUs and followed by the results of [11] for unforgeability of UU, we conclude that PRU makes a set of universally unforgeable unitaries. Now we show that PRU can also be considered as a PUF family. In order to do that we need to show that the PUF requirements discussed in preliminary section 2.4 are satisfied. Since the δ_r-robustness and δ_c-collision resistance are trivially satisfied by the unitarity, we only need to argue the δ_u-uniqueness requirement.

Theorem 11. *Let $\mathcal{U} \in U(d) = \{U_k\}_{k\in\mathcal{K}}$ be a family of PRU and universally-unforgeable unitary matrices. Then there exist a $\delta_u = \text{non-negl}(\lambda) = n\text{on-negl}(\text{polylog}(d))$ such that $\mathcal{U}$ satisfies δ_u-uniqueness.*

Proof. We prove by contraposition and we assume that a non-negligible δ_u to satisfy the δ_u-uniqueness does not exist. This means that for any two unitary U_i and U_j picked uniformly at random from $\mathcal{U}$, the two unitary are ζ-close in the diamond norm with a high probability. Otherwise if there exist a minimum $\zeta_{\min} = \text{non-negl}(\lambda)$ distance in diamond norm between any two unitaries we have already shown the δ_u exists. Hence we assume that we have the following condition:

$$\Pr[\|(U_i - U_j)_{i\neq j}\|_\diamond \leqslant \zeta] \geqslant 1 - \epsilon(\lambda), \tag{28}$$

where both ζ and $\epsilon(\lambda)$ are negligible function in the security parameter. Now we assume an adversary $\mathcal{A}$ wants to distinguish between $\mathcal{U}$ and the set of Haar-random unitaries. By assumption, we have that all the unitaries in $\mathcal{U}$ are universally unforgeable. So now we let the $\mathcal{A}$ play the PRU game (similar to game 2) while running the universal unforgeability game as a distinguishing subroutine. Let $\mathcal{C}$ be the honest party picking at random a bit $b \in \{0, 1\}$ where if $b = 0$, a unitary U is picked at random from $\mathcal{U}$ and we are in the PRU world and otherwise U is picked from μ that denotes the set of Haar-random unitary matrices. Then $\mathcal{A}$ gets polynomial oracle access to the U and after the interaction, needs to guess b. Now, since there exist an efficient public generation algorithm Q for the PRU set, we let the adversary sample another unitary U' from Q locally and uniformly at random. According to the contraposition assumption give in equation (28), if $b = 0$, with a high probability these two unitaries are ζ-close in the diamond norm, i.e. $\| (U - U') \|_\diamond \leqslant \zeta$. Given this promise, the adversary performs the following strategy: $\mathcal{A}$ locally plays the universal unforgeability game on the U, by picking a state $|\psi\rangle$ uniformly at random from Haar measure and querying it to $\mathcal{C}$ as a part of the polynomial oracle interaction with U. $\mathcal{A}$ will receive $U|\psi\rangle$ and can ask for multiple copies of it so long as the total number of queries to the oracle remains polynomial. Now we also rely on the fact that since PRU has the efficient computation property, meaning that $\mathcal{A}$ can locally compute the $U'|\psi\rangle$ to get multiple copies. Now $\mathcal{A}$'s strategy to win the unforgeability game is to output $U'|\psi\rangle$ as the forgery for $|\psi\rangle$.

Again in the case of $b = 0$, since the two unitaries are negligibly close in the diamond norm with a high probability we have the following:

$$\Pr[\|(U - U')\|_\diamond \leqslant \zeta] \geqslant 1 - \epsilon \Rightarrow \Pr[F(U|\psi\rangle, U'|\psi\rangle) \geqslant 1 - \zeta] \geqslant 1 - \epsilon. \tag{29}$$

This holds since the diamond norm is defined as a maximum over all of the density matrices, hence if the two unitaries are very close in the diamond norm, their output over a random state is also very close on average. Thus, the adversary can run a local efficient verification test (for instance a GSWAP test) between $U'|\psi\rangle$ and $U|\psi\rangle$ and use the output of the test as a distinguisher between pseudorandom and Haar-random world. If $b = 0$, we have:

$$\Pr[F(U|\psi\rangle, U'|\psi\rangle) \geqslant 1 - \zeta] \geqslant 1 - \epsilon \Rightarrow \Pr[1 \leftarrow G(\lambda, \mathcal{A})] = \text{nonnegl}(\lambda). \tag{30}$$

Hence $\mathcal{A}$ will win the game with a high probability. However, in the case of $b = 1$ where U is a Haar-random unitary, we can use lemma 16 in [41], that states for a fixed state $|\phi\rangle \in \mathcal{H}^d$ and a Haar-random state $|\psi\rangle \leftarrow \mu$, and any $\epsilon > 0$ we have:

$$\Pr_{|\psi\rangle \leftarrow \mu}[|\langle\phi|\psi\rangle|^2 \geqslant \epsilon] \leqslant e^{-\epsilon d}. \tag{31}$$

This implies that taking the $U'|\psi\rangle = |\phi\rangle$ to be the fixed state, we denote that since U is a Haar-random unitary then $U|\psi\rangle$ is also a Haar-random state and hence the probability that the fidelity $F(U|\psi\rangle, U'|\psi\rangle)$ is a non-negligible value (with respect to polylog(d)) like $1 - \zeta$ is exponentially low. Hence in case $b = 1$, the probability that the adversary's state passes the verification is exponentially low. Hence using this strategy, there will be always a distinguisher that can distinguish between $\mathcal{U}$ and Haar-random unitaries i.e.:

$$\Pr_{U \leftarrow \mathcal{U}}[\mathcal{A}'^{U}(1^\lambda) = 1] - \Pr_{U_\mu \leftarrow \mu}[\mathcal{A}'^{U_\mu}(1^\lambda) = 1] = \text{nonnegl}(\lambda). \tag{32}$$

But this is in contrast with the assumption that $\mathcal{U}$ is a PRU. Hence we have reached a contradiction and the proof is complete. □

5. Pseudorandom unitaries and states from hardware assumptions

As discussed earlier PRSs can be constructed under the assumption of qPRF or quantum one-way functions. Given the relationship that we have explored in the previous section between the unforgeability of qPUF and quantum pseudorandomness, here we ask whether it is possible to construct PRSs under a different set of assumptions? In this section, we discuss how one can achieve PRU and PRS under hardware assumptions on a family of unitary transformations. These hardware assumptions are generally discussed in the context of quantum PUFs, nevertheless, our results can be in general applied to any sets of unitaries with the given properties as long as they can be assumed on a hardware level.

Let $\mathcal{U} \subseteq U(d) = \{U_i\}_{i=1}^K$ be a family of unitaries with certain specific assumption that is given by their physical nature. We want to use the above family as a PRU family or generators for PRS. As shown in [10], if $\mathcal{U}$ is a PRU then it is also a generators for PRS i.e. $G(k) = U_k|0\rangle = |\phi_k\rangle$. To this end, we investigate the properties of a qPUF family that can be used to achieve pseudorandomness. In the last section, we have shown that PRU implies the notion of UU assumption, or in other words single-shot unknownness. Now we explore the relation of PRU and another notion of unknownness called *practical unknownness* by Kumar *et al* [23]. This definition is a more suited definition for t-design unitary sets constructions and is defined as follows:

Definition 7 (ϵ, t, d**-practical unkownness** [23]). We say a unitary transformations U, from a set $\mathcal{U} \subseteq U(d)$ is (ϵ, t, d)-practically unknown if provided a bounded number $t \leqslant \text{poly}(\log_2 d)$ of queries $U\rho U^\dagger$, for any $\rho \in \mathcal{H}^d$, the probability that any poly$(\log_2 d)$-time adversary can perfectly distinguish U from a Haar distributed unitary is upper bounded by $1/2(1 + 0.5\epsilon)$. Here $0 < \epsilon < 1$, t are functions of $\log_2 d$, and $\lim_{\log_2(d) \to \infty} \epsilon = 0$.

For the sake of our proof, we need a variation of this definition which is for any polynomial number of queries in the security parameter:

Definition 8 (ϵ, d**-practical unkownnness**). We say a unitary transformations U, from a set $\mathcal{U} \subseteq U(d)$ is (ϵ, d)-practically unknown if it is (ϵ, t, d)-practically unknown for any $t = \text{poly}(\lambda) = \text{poly}(\log d)$.

Now we show that the assumption of ϵ, d-practical unkownness implies PRU.

Theorem 12. *A family of* (ϵ, d)*-practically UUs where* $\epsilon = \text{negl}(\lambda)$ *is a PRU family.*

Proof. We prove this by contraposition. Let $\mathcal{U} = \{U_k\}_{i=1}^{\mathcal{K}} \subseteq U(d)$ be a (ϵ, d)-practically unknown family, that is not a PRU. This means that there exists a QPT adversary $\mathcal{A}$ for which we have the following after some $q = \text{poly}(\lambda) = \text{poly}(\log(d))$ queries to the unitary oracle:

$$|\Pr_{k\leftarrow\mathcal{K}}[\mathcal{A}^{U_k}(1^\lambda) = 1] - \Pr_{U\leftarrow\mu}[\mathcal{A}^{U}(1^\lambda) = 1]| = \delta = \text{nonnegl}(\lambda). \tag{33}$$

Equivalently, we can say that if a unitary is randomly picked from either of the sets $\mathcal{U}$ or a set of Haar-random distributed unitaries with a random bit b, the advantage of the adversary in guessing bit b is a non-negligible function δ greater than $\frac{1}{2}$. Now if such adversary exists, there exists also an adversary $\mathcal{A}'$ that querying the same q states, can distinguish the $U_k \in \mathcal{U}$ from a Haar-random unitary with the following probability:

$$\Pr[\text{distinguish } U_k] \geqslant \frac{1}{2} + \delta. \tag{34}$$

On the other hand, if $\mathcal{U}$ is (ϵ, d)-practically unknown this probability is equal to $\frac{1}{2}(1 + 0.5\epsilon)$ where $\frac{\epsilon}{4}$ is a negligible function while as δ is non-negligible. Hence we reach a contradiction and the proof is complete. □

We have shown that given the hardware assumption of practical unknownness, over a set of unitary transformations such as unitary qPUFs, one can get PRU and as a result generate PRS by applying random elements of the set on the computational basis state. Now, we want to look at another property of a family of qPUFs and see whether pseudorandomness can be achieved under other related assumptions of such families. One of the main requirements on a qPUF family is the uniqueness property that ensures any two qPUFs in the family are sufficiently distinguishable in the diamond norm. The uniqueness property is formally defined in preliminary section 2.4, equation (12). In what follows we show a family of unknown and maximally distinguishable unitary matrices, such as unitary qPUFs, also form a family of PRU and are a generator for PRS.

Theorem 13. *Let $\mathcal{U}_\mathcal{K} = \{U_k\}_{k=1}^{\mathcal{K}} \subseteq U(d)$ be a family of unitary transformation selected at random from a distribution $\chi_\mathcal{U}$ such that they satisfy almost maximal uniqueness i.e. for any randomly picked pairs of unitary matrices from $\mathcal{U}_\mathcal{K}$, we have $\|(U_i - U_j)_{i\neq j}\|_\diamond = 2 - \epsilon$ where $\epsilon = \text{negl}(\lambda)$, then for a sufficiently large $\mathcal{K}$ and d, the $\mathcal{U}_\mathcal{K}$ is also a PRU.*

Proof. We first show that if the maximum uniqueness is on average satisfied for any pairs of unitary matrices of $\mathcal{U}_\mathcal{K}$, then the distribution $\chi_\mathcal{U}$ converges to Haar measure in the limits of large d. The first part of our proof is in the spirit of a proof given in [23] for proving uniqueness of Haar-random unitaries. We attempt to prove the other direction for a specific degree of uniqueness which is $2 - \epsilon$ where the maximum of the diamond norm is 2. We have,

$$\|(U_i - U_j)_{i\neq j}\|_\diamond = 2 - \epsilon = 2\sqrt{1 - \delta(U_i^\dagger U_j)^2}. \tag{35}$$

Where the $\delta(M) = \min_{|\phi\rangle} |\langle\phi|M|\phi\rangle|$ is the minimum of absolute value over the numerical range of the operator M. From the above equation we have:

$$\delta(U_i^\dagger U_j)^2 = \epsilon - \frac{\epsilon^2}{4} \approx 0. \tag{36}$$

Since the diamond norm is unitary invariant, we can multiply all the unitaries of the family by a fixed unitary matrix which results in the set including the identity matrix $\mathcal{I}$, hence the above equation can be rewritten as:

$$\delta(U_k')^2 = \epsilon - \frac{\epsilon^2}{4}, \tag{37}$$

where the set of unitary matrices U' is equivalent to the initial set up to a unitary transformation. Now let $\{e^{i\theta_1}, \ldots, e^{i\theta_d}\}$ be the eigenvalues of U_k'. The eigenvalues of a unitary matrix lie on a unit circle $\mathbb{S}^1 \subset \mathcal{C}$. As shown in the lemma 1.1 of [23], the following relation exist between the distribution of the eigenvalues of a general unitary matrix in an arc of size θ, and the function $\delta(U)$:

$$\delta(U_k')^2 = \frac{1}{2} + \frac{1}{2}\cos\theta. \tag{38}$$

Where $\theta = \theta_j - \theta_k$ for pairs of eigenvalues $\{e^{i\theta_j}, e^{i\theta_k}\}$. From the above equation we have:

$$\theta = \theta_j - \theta_k = \arccos\left(-1 + 2\epsilon - \frac{\epsilon^2}{2}\right) \approx \pi - \sqrt{\epsilon} + \dots. \tag{39}$$

Now we can use theorem 19. Let N_θ be a random variable that represents the number of eigenvalues in an arc of size θ. Then we have the expectation value of this random variable for the given distribution where the $\theta = \pi - \epsilon'$, and $\epsilon' = \text{negl}(\lambda)$, to be

$$\mathbb{E}_d[N_\theta] = \frac{d \times \theta}{2\pi} = \frac{d}{2} - \frac{\epsilon' d}{2\pi}, \tag{40}$$

which is close to half of the total number of eigenvalues since the second term is always smaller than 1. This means that in the limit of large d, every diameter of the unit circle divide the circle into two areas that each on average includes half of the eigenvalues. Also the variance of the random variable N_θ will be:

$$\text{Var}(N_\theta) = \frac{1}{\pi^2}\left(\log(d) + 1 + \gamma + \log|2\,\sin\left(\frac{\pi - \epsilon'}{2}\right)|\right) + o(1) \approx \frac{\log(d)}{\pi^2} + c' + o(1), \tag{41}$$

where $\gamma \approx 0.577$ and $c' < 1$. Next we calculate the probability that for our given distribution, there are more than half of the eigenvalues in each half of the circle denoted by an arc or size $\pi - \epsilon'$. Using the Chernoff bound we have:

$$\Pr[N_{\pi-\epsilon'} - \mathbb{E}_d[N_{\pi-\epsilon'}]| > x\mathbb{E}_d[N_{\pi-\epsilon'}]] \leqslant e^{-\frac{x^2}{2+x}\mathbb{E}_d[N_{\pi-\epsilon'}]}. \tag{42}$$

Here we want the $x\mathbb{E}_d[N_{\pi-\epsilon'}]$ to be equal to $\frac{d}{2}$, so we have $x = \frac{d/2}{d/2 - \mathrm{d}\epsilon'/2\pi} = \frac{1}{1-\epsilon'/\pi}$ and since the x is a small value the above inequality can be used. Substituting this into the above equation we will have:

$$\Pr\left[N_{\pi-\epsilon'} - \mathbb{E}_d[N_{\pi-\epsilon'}]| > \frac{d}{2}\right] \leqslant e^{-\frac{\left(\frac{1}{1-\epsilon'/\pi}\right)^2}{2+\frac{1}{1-\epsilon'/\pi}} \times (d/2 - \epsilon' d/2\pi)} \approx e^{-d/6}, \tag{43}$$

since ϵ' is negligible. This shows that with a very high probability, on every half of the unit circle, there exist half of the eigenvalues of the random matrix from our specified distribution. We conclude eigenvalues of a random unitary from the distribution $\chi_{\mathcal{U}}$ are uniformly distributed on the unit circle. Let us denote this uniform distribution on $\mathbb{S}^1$ by ν. In order to compare the distribution of $\chi_{\mathcal{U}}$ with the Haar measure, we use the empirical spectral measure introduces in the appendix A. We denote the empirical spectral distance of $\chi_{\mathcal{U}}$ as $\tilde{\mu}_\chi$ and for Haar measure we denote it as $\tilde{\mu}_{\text{H}}$. Since we have shown that the eigenvalues of matrices from $\chi_{\mathcal{U}}$ are distributed uniformly on $\mathbb{S}^1$, it is easy to see that $\mathbb{E}(\tilde{\mu}_\chi) = \nu$ and in the limit of large d we have the convergence in probability $\tilde{\mu} \xrightarrow{d\to\infty} \nu$. Now we use the theorem 18 (appendix A) that implies the convergence of the empirical spectral measure of the set of unitaries picked from Haar measure to ν, in the limit of large d. Having the these two convergence and the properties of the limit we can conclude that the empirical spectral measure for $\chi_{\mathcal{U}}$ converges to the one for Haar measure. Then we look at Kolmogorov distance of the eigenvalues of these two distributions. We rely on the result given in [42] that shows the Kolmogorov distance between the distributions of eigenvalues of random unitary matrices is given by $d_{\text{K}}(\mu, \nu) = \sup_{0\leqslant\theta<2\pi}|\frac{N_\theta}{d} - \frac{\theta}{2\pi}|$ and specifically for Haar measure it is bounded by

$$d_{\text{K}}(\mu_{\text{H}}, \nu) \leqslant c\frac{\log(d)}{d}. \tag{44}$$

Where $c > 0$ is a universal constant. Given the fact that for the specific value of θ for the distribution of $\chi_{\mathcal{U}}$ the Kolmogorov distance $d_{\text{K}}(\mu_\chi, \nu)$ is of the order $\frac{1}{d}$ which is negligible and using the triangle inequality for the Kolmogorov distance we have

$$\begin{aligned} d_{\text{K}}(\mu_{\text{H}}, \mu_\chi) &\leqslant d_{\text{K}}(\mu_{\text{H}}, \nu) + d_K(\nu, \mu_\chi) \\ &\leqslant c\frac{\log(d)}{d} + \text{negl}(\lambda) \\ &\leqslant \text{negl}(\lambda) \end{aligned} \quad . \tag{45}$$

Thus the distribution of the eigenvalues of the random matrices of $\chi_{\mathcal{U}}$ is negligibly close to the Haar measure. Also for any randomly picked matrix from each of these distributions, the eigenvalues are fixed. As a result, the convergence between the distribution of the eigenvalues of matrices leads to the fact that in the limit of large d, $\chi_{\mathcal{U}}$ converges to the Haar measure on the unitary set.

Finally, we show that a polynomial time quantum adversary given a polynomial query to each UU U_k cannot distinguish any member of this family from Haar measure. This is straightforward since the two distributions are asymptotically close. Thus we have:

$$|\Pr_{k\leftarrow\mathcal{K}}[\mathcal{A}^{U_k}(1^\lambda)=1]-\Pr_{U\leftarrow\mu}[\mathcal{A}^{U}(1^\lambda)=1]|=\text{negl}(\lambda). \tag{46}$$

And we have shown that the set $\mathcal{U}_\mathcal{K}$ is a PRU. □

6. Efficient quantum identification protocols using quantum pseudorandomness

We discuss the application of some of our previously established results, in order to achieve an efficient quantum identification protocol. *Identification* (also called entity authentication), is a method to prove the identity of one party called *prover* to another party called *verifier*. In the quantum setting, either the verifier or the prover or both have some quantum capabilities and the properties of quantum mechanics are used to enhance the security of such protocols against powerful quantum adversaries. Here we focus on two quantum identification protocols, proposed in [24]. These identification protocols are based on quantum PUFs and use their unforgeability property to achieve exponential security against QPT adversary (polynomial time in the learning phase, and unbounded during the quantum communication) in a polynomial number of rounds. Even though these protocols are resource-efficient in many aspects, one of the main practical challenges in implementing these protocols is the fact that in order to use the unforgeability property of quantum PUFs, the challenge states needs to be sampled at random from Haar measure. As a result, relying on theorem 9, we show that these protocols can still achieve exponential security using PRS. This brings us one step closer to the practical implementations of quantum identification protocols with exponential security against powerful quantum adversaries and can lead to promising solutions to the problem of untrusted manufacturers. Furthermore, using theorem 10, we show that PRU can also be used as an alternative to hardware assumptions in order to run these identification protocols.

First, we briefly mention the two protocols. The full description of both protocols can be found in appendix B.

6.1. Identification protocol with high-resource verifier

In this qPUF-based protocol, the verifier uses a database of the challenge-responses of the qPUF in order to identify a party who has access to the qPUF device. Since the verifier needs to run a quantum verification algorithm to check the response-state received by the prover, this protocol is referred to as *high-resource verifier*. The protocol has three phases: *setup phase*, *identification phase* and *verification phase*.

In the *setup phase* the verifier who has physical access to the qPUF device samples some quantum challenges at random from the Haar measure and records the response state of the qPUF on a quantum database. Then publicly sends the qPUF over to the prover. At this stage, polynomial access to the qPUF device has been assumed for the adversary i.e. the quantum adversary can query the qPUF with a polynomial number of arbitrary quantum states attempting to learn the behaviour of the underlying unitary transformation.

In the *identification phase*, the verifier picks one of the challenges in the database at random and sends them to the prover over a public quantum channel, while an adversary has full control over the channel. Then the prover who acquires the qPUF obtains the correct response to the challenge states and sends it back through the same public quantum channel.

Finally, in the *verification phase*, the verifier needs to verify the challenge state to confirm the identity of the other party. To this end, the verifier needs to run a quantum verification or test algorithm on the received response, and the M copies of the correct response that is stored in the database. In [24] the protocol has been proposed and analysed with both SWAP and GSWAP test as the verification algorithm.

The following theorem states the security or soundness of the above protocol with both of the tests:

Theorem 14 (Theorems 2 and 4 in [24]). *Let qPUF be a selectively unforgeable*[3] *unitary PUF over $\mathcal{H}^d$. The success probability of the adversary to pass the SWAP-test or GSWAP-test verification of the high resource verifier protocol is at most ϵ, given that there are N different CRPs, each with M copies. The ϵ is bounded as follows for each verification:*

$$\Pr[Ver\ accept_{\mathcal{A}}]\leqslant\epsilon \qquad \epsilon_{SWAP}\approx\mathcal{O}\left(\frac{1}{2^{NM}}\right) \qquad \epsilon_{GSWAP}\approx\mathcal{O}\left(\frac{1}{(M+1)^N}\right). \tag{47}$$

[3] Universally unforgeable in our terminology.

We now introduce a computationally efficient variation of this protocol which we denote as *efficient hr-verifier identification protocol*, by replacing the qPUF with any general universally unforgeable pseudorandom unitary and the Haar-random challenges with PRSs as follows:

(a) *Setup phase*:
1. Verifier has access to a PRU family $\mathcal{U} \subseteq U(d) = \{U_i\}_{i=1}^{\mathcal{K}}$.
2. Verifier samples at random $k \xleftarrow{\$} \mathcal{K}$ and selects U_k.
3. Verifier has also access to a family of PRS $\{|\phi_{k'}\rangle \in S(\mathcal{H}^d)\}_{k' \in \mathcal{K}'}$ and randomly picks $Q \in \mathcal{O}(\text{poly log } d)$ of them as the challenge states.
4. Verifier queries the U_k individually with each challenge $|\phi_{k'}\rangle$ a total of M number of times to obtain M copies of the response state $|\phi_{k'}^r\rangle$ and stores them in their local database S.
5. The verifier transfers the U_k to prover or securely sends the key k.

(c) *Verification phase*:
1. Verifier runs a quantum equality test algorithm on the received response from Bob and the M copies of the correct response that she has in the database. This algorithm is run for all the R CRP pairs.
2. Verifier outputs '1' implying successful identification if the test algorithm returns '1' on all CRPs. Otherwise, outputs '0'.

We note that the protocol assumes that the adversary has only query access to the unitary U_k from a PRU family as it is also assumed in the definition 3. The following theorem which is a corollary of the previous results shows that the *efficient hr-verifier identification protocol* is also exponentially secure against QPT adversary with the same security bounds.

Theorem 15. *Let $U_k \in \mathcal{U}$ be unitary randomly selected from a PRU family $\mathcal{U} \subseteq U(d)$. The success probability of the adversary to pass the SWAP-test or GSWAP-test verification of the* efficient hr-verifier protocol *is at most ϵ, given that there are N different CRPs, each with M copies. The ϵ is bounded as follows for each verification:*

$$\Pr[\textit{Ver accept}_{\mathcal{A}}] \leqslant \epsilon \qquad \epsilon_{SWAP} \approx \mathcal{O}\left(\frac{1}{2^{NM}}\right) \qquad \epsilon_{GSWAP} \approx \mathcal{O}\left(\frac{1}{(M+1)^N}\right). \tag{48}$$

Proof. First, we use theorem 10 that shows $\mathcal{U}$ is also an UU family. Then we use theorem 9 that states any UU unitary satisfies efficient universal unforgeability which is the universal unforgeability given the states are picked from the PRS family. These two results suggest that the U_k within the protocol satisfies the same notion of universal unforgeability that qPUF satisfies in the original protocol. Now we can directly use the result of [24] using the SWAP and GSWAP test which will result in the same security bound in the number of rounds and copies of challenge-response pairs. □

6.2. Identification protocol with low-resource verifier

The second identification protocol also introduced in [24], enables a weak verifier to identify a quantum server prover in the network. The main idea behind this protocol is to delegate the equality testing to the prover so that the verifier can only run a classical verification algorithm. While it might seem this delegation could damage the security, it has been shown that the unforgeability property of qPUF combined with some trapification techniques used in the protocol leads to yet another exponentially secure qPUF-based identification protocol. In addition to enabling the clients to identify quantum servers on the clouds, this protocol has the advantage of one-way quantum communication compared to the previous protocol. We give a brief description of the protocol here. The complete protocol can be found in appendix B.2.

The *setup phase* is similar to the previous protocol, except that in addition to the challenge-response pairs, the verifier also generates some trap states. These trap states need to be orthogonal to the challenge subspace.

In the *identification phase*, the verifier sends two quantum states in every communication rounds. One of the states is the challenge state and the other one is either the correct response or the trap states with no overlap with the correct response. The verifier selects the correct or trap response at random with probability $1/2$.[4] In other words in N rounds, around $N/2$ positions are the states sent with their correct responses.

In the *verification phase*, the prover generates the valid response for every challenge by interacting them with the qPUF device and then runs a SWAP-test on the response produced by the qPUF and the other state sent by the verifier. The prover then sends the classical output of the test to the verifier who receives a classical $S_N = s_1, \ldots, s_N$ where $s_i \in \{0, 1\}$. Finally, the verifier runs a classical verification algorithm on this

[4] It has been shown that this probability can be generalised to arbitrary distribution.

string that checks the expected result for the positions with the valid responses and also the statistics of the remaining positions.

The protocol has been proven secure against both collective and coherent attacks with the following bound which we restate from the original paper:

Theorem 16 (Theorems 6, 7 and 8 in [24]). *Let qPUF be a universally unforgeable unitary PUF over $\mathcal{H}^d$. The success probability of any QPT adversary $\mathcal{A}$ (using coherent or collective strategy) to pass the verification of the low resource verifier protocol is at most ϵ, in N rounds. The ϵ is of the order $\mathcal{O}(\frac{1}{2^N})$*

$$\Pr[\textit{Ver accept}_{\mathcal{A}}] \leqslant \epsilon \qquad \epsilon \approx \mathcal{O}\left(\frac{1}{2^N}\right). \tag{49}$$

Similar to the previous protocol, we introduce an efficient version of this protocol by replacing the Haar-random states with PRS and the qPUF with an UU selected from a PRU family. We denote this protocol as *efficient lr-verifier identification protocol* and it is described as follows:

(a) *Setup phase*:
1. Verifier has access to a PRU family $\mathcal{U} \subseteq U(d) = \{U_i\}_{i=1}^{\mathcal{K}}$.
2. Verifier samples at random $k \xleftarrow{\$} \mathcal{K}$ and selects U_k.
3. Verifier has also access to a family of PRS $\{|\phi_{k'}\rangle \in S(\mathcal{H}^d)\}_{k' \in \mathcal{K}'}$ and randomly picks $Q \in \mathcal{O}(\text{poly log } d)$ of them as the challenge states.
4. Verifier queries the U_k individually with each challenge $|\phi_{k'}\rangle$ a total of M number of times to obtain M copies of the response state $|\phi^r_{k'}\rangle$ and stores them in their local database S.
5. Verifier selects states $|\phi^{\perp}\rangle$ orthogonal to the selected challenge's subspace and queries the U_k with them to obtain the trap states labelled as $|\phi^{\text{trap}}\rangle$. The unitary property ensures that $\langle\phi^{\text{trap}}|\phi^r_{k'}\rangle = 0$.
6. The verifier transfers the U_k to prover or securely sends the key k.

(b) *Identification phase*:
1. Verifier randomly selects a subset $N \subseteq \mathcal{K}'$ different challenges from the database, and sends the state $|\phi_i\rangle$ over a public quantum channel to prover.
2. Verifier randomly selects $N/2$ positions, marks them $b = 1$ and sends the valid response states $|\phi^1_i\rangle = |\phi^r_i\rangle$ to prover. On the remaining $N/2$ positions, marked as $b = 0$, verifier sends the trap states $|\phi^0_i\rangle = |\phi^{\text{trap}}_i\rangle$.

Again using the previous proof techniques presented in [24] and our results, we show that the *efficient lr-verifier identification protocol* satisfies exponential security against QPT adversary both under the coherent and collective attack models.

Theorem 17. *Let $U_k \in \mathcal{U}$ be unitary randomly selected from a PRU family $\mathcal{U} \subseteq U(d)$. The success probability of a QPT adversary $\mathcal{A}$ to pass the verification of the* efficient lr-verifier protocol *is at most ϵ, in N rounds. The ϵ is bounded as follows:*

$$\Pr[\text{Ver accept}_{\mathcal{A}}] \leqslant \epsilon \quad \epsilon \approx \mathcal{O}\left(\frac{1}{2^N}\right). \tag{50}$$

Proof. First, we specify that we can directly use the result of the theorem (6) in [24] which bounds the success probability of classical adversary in passing the classical verification algorithm. Then the success probability against a quantum adversary with the collective and coherent attack is defined as the advantage of the quantum adversary over that classical adversary in guessing the trap states, using all the side information obtained from the U_k in the learning phase. Using theorem 10 we have that $\mathcal{U}$ is also an UU family. Then we use theorem 9 that states any UU unitary satisfies efficient universal unforgeability which is the universal unforgeability given the states are picked from the PRS family. Next, the conditions of theorems (7) and (8) in [24] are satisfied and we can directly use those results that state the success probability of such adversaries in guessing the traps is bounded as follows:

$$\Pr[b \leftarrow \Lambda_{\mathcal{A}}] \leqslant \frac{1}{2} + \mathcal{O}(2^{-N}). \tag{51}$$

Where $\Lambda_{\mathcal{A}}$ denotes any map that $\mathcal{A}$ uses to distinguish the traps states. Finally, putting all the above results together we have

$$\Pr[\text{Ver accept}_{\mathcal{A}}] \leqslant \epsilon = \Pr[\text{Ver accept}_{\text{Classical Adv}}] + \mathcal{O}(2^{-N}) \approx \mathcal{O}(2^{-N}). \tag{52}$$

This concludes the soundness proof of *efficient lr-verifier protocol*. □

7. Conclusion and discussion

We have explored the relationship between quantum pseudorandomness and quantum hardware assumptions such as quantum physical unclonability. Since one of the main cryptographic properties of qPUFs is the notion of universal unforgeability, we have inspected whether quantum pseudorandomness would be enough as a challenge sampling requirement, to achieve this level of unforgeability. We have formally proved that the answer to this question is positive. This result can improve the practicality of qPUF-based constructions and protocols since it will replace the requirement of Haar-randomness on the challenge states, which is resourceful and experimentally challenging.

We have also established the link between the notions of UU and PRU. We proved that any family of PRU is also a family of UUs and, hence they could be a potential candidate for the construction of qPUF devices. This result can be a complement to the result of [23] where they show t-designs can also satisfy a similar notion, namely practical unknownness, which leads to an efficient proposal for constructing quantum PUFs.

Then we also looked at the problem of generating PRSs from hardware assumptions. Our results show that different physical assumptions that were proposed in the context of PUFs, such as uniqueness or practical unknownness, can also imply quantum pseudorandomness. This is of theoretical interest as it shows an alternative way for achieving quantum pseudorandomness which is different from current approaches based on post-quantum and computational assumptions. Apart from the cryptography perspective, having a different set of assumptions for PRS and PRU can find potential applications in physics [43]. Another interesting future direction would be to further explore the relationship between unclonability and quantum pseudorandomness that has been initially proposed in [10], relying upon our new results.

Finally, to show the consequence of our result in the practicality of qPUF-based protocols, we have revisited the qPUF-based identification protocols proposed in [24] using PRS and we have shown that this more efficient version of these protocols can achieve the same security guarantee as they were initially proposed.

An important note that needs to be emphasised regarding these protocols is that they assume during the transition stage (5) in the setup phase, the adversary has only query access to the device. If the PRU is realised by hardware assumptions such as practical unknownness as showed in theorem 12, then this requirement is satisfied by assumption. Otherwise, the unitary circuit of the U_k selected from the PRU needs to be obfuscated or hidden from the adversary [44, 45]. This problem mainly arises if the PRU is built from classical PRF and hence the underlying circuit is publicly known. Another alternative way to go around this problem is that only the key index of the selected unitary is sent in a secure way to the other party who is running the selected unitary locally. Thus the above protocol works naturally with hardware assumptions that imply the unitary transformation is unknown. Nevertheless, using PRU constructions with known unitary circuits has the advantage that removes the quantum memory requirements to store the response pairs, as one can presumably compute the response state having access to the circuit and only store the related classical parameters.

Yet another interesting future direction would be to establish concrete bounds on the randomness and pseudorandomness of unitary families given different degrees of uniqueness or distinguishability (not negligibly close to perfect distinguishability), in terms of the diamond norm. This is also related to the study of t-design unitaries and the toolkit from random matrix theory, which we used in this paper can be potentially beneficial and powerful tools for this study.

Acknowledgments

We acknowledge the UK Engineering and Physical Sciences Research Council grant EP/N003829/1 and as well as Innovate UK funded project called AirQKD : product of a UK industry pipeline, Grant Number 106178.

Data availability statement

No new data were created or analysed in this study.

Competing interests

The authors declare no competing interest.

Appendix A. Haar measure group and properties of random matrices

A Haar measure is a non-zero measure on any locally compact group G such that $\mu : G \to [0, \infty)$ such that for all $X \subset G$ and $x \in G$ we have the following translation invariance property for $\mu(X) = \int_{x\in G} \mathrm{d}\mu(x)$:

$$\mu(xX) = \mu(Xx) = \mu(X). \tag{53}$$

In particular, the Haar measure $\mathrm{d}\mu(U)$ can be defined for a unitary group $U(d)$. Sampling unitaries from Haar measure on $U(d)$ is equivalent to geometrically uniform sampling from unitary groups of a certain dimension. In practice, however, sampling from the Haar measure requires exponential (in d) resources [21].

In this work, we are interested in characterising the properties of the eigenvalues of Haar-random unitary matrices and their distributions. To this end, we introduce the following important results from the random matrix theory. The first result that we need, is known as *Weyl density formula* or *Weyl integration formula*, and is stated as follows:

Lemma 1 (Weyl integration formula on $\mathbb{U}(n)$ [46]). *Let $\{e^{i\theta_j}\}_{j=1}^n$ be the eigenvalues of $n \times n$ random unitary matrix. The unordered eigenvalues of a random unitary matrix have the following eigenvalue density*

$$\frac{1}{n!(2\pi)^n} \prod_{1\leqslant j<k\leqslant n} |e^{i\theta_j} - e^{i\theta_k}|^2, \tag{54}$$

with respect to $\mathrm{d}\theta_1 \ldots \mathrm{d}\theta_n$ on $(2\pi)^n$. That is, for any $g : \mathbb{U}(n) \to R$ with

$$g(U) = g(VUV^*) \quad \text{for any } U, V \in \mathbb{U}(n),$$

(i.e., g is a class function), if U is Haar-distributed on $\mathbb{U}(n)$, then

$$\mathbb{E}[g(U)] = \frac{1}{n!(2\pi)^n} \int_{[0,2\pi)^n} \tilde{g}(\theta_1, \ldots, \theta_n) \prod_{1\leqslant j<k\leqslant n} |e^{i\theta_j} - e^{i\theta_k}|^2 \mathrm{d}\theta_1 \ldots \mathrm{d}\theta_n, \tag{55}$$

where $\tilde{g} : [0, 2\pi)^n \to \mathbb{R}$ is the (necessarily symmetric) expression of $g(U)$ as a function of the eigenvalues of U.

As discussed in [46], one consequence of the above lemma is that the eigenvalues of random unitary matrices want to spread out. For any given pair of eigenvalues labelled by (j, k), $|\mathrm{e}^{\mathrm{i}\theta_j} - \mathrm{e}^{\mathrm{i}\theta_k}|^2$ is zero if $\theta_j = \theta_k$, and is 4 if $\theta_j = \theta_k + \pi$ (and in that neighbourhood if they are roughly antipodal). This produces the effect alternatively known as 'eigenvalue repulsion'.

Another important tool in the study of the eigenvalues of random matrices is the *empirical spectral measure* defined as,

$$\tilde{\mu} = \frac{1}{n} \sum_{j=1}^{n} \delta_{\mathrm{e}^{\mathrm{i}\theta_j}}, \tag{56}$$

where $\mathrm{e}^{\mathrm{i}\theta_j}$ are the eigenvalues of the unitary matrix and δ is the probability distribution function over the eigenvalues. The empirical spectral measure is a probability measure to encode the ensemble of eigenvalues which puts equal mass at each of the eigenvalues of U. This encoding is very useful for representing the spreading of the eigenvalues on the complex unit circle denoted by $\mathbb{S}^1 \subseteq \mathbb{C}$.

Next, we need the following important theorem by Diaconis–Shashahani [47], that shows the convergence of the eigenvalues of the Haar-random matrices to the uniform distribution over the unit circle:

Theorem 18. *Let U be uniformly chosen from Haar-measure in $U(d)$, Let ν be the uniform distribution on $\mathbb{S}^1$. Then as $d \to \infty$, the $\tilde{\mu}_U$ converges, weakly in probability, to ν:*

$$\tilde{\mu}_U d\infty \to \nu. \tag{57}$$

Finally, we use the following result by Wieand [48]:

Theorem 19. *Let U be a unitary matrix chosen from Haar measure in $U(d)$, and let $\{e^{i\theta_1}, \ldots, e^{i\theta_d}\}$ be the eigenvalues of U. Fix a finite number of intervals on the unit circle $I_1 = (e^{i\theta_{1j}}, e^{i\theta_{1l}}), \ldots, I_m = (e^{i\theta_{mj}}, e^{i\theta_{ml}})$. Define*

the random variables $N_{\theta_1}, \ldots, N_{\theta_m}$ to be the number of eigenvalues in each arc defined by the intervals. In the limit of large d, the mean and variance of N_{θ_k} are as follows:

$$\mathbb{E}_d[N_{\theta_k}] = \frac{d(\theta_{kj} - \theta_{kl})}{2\pi}, \tag{58}$$

and

$$\mathrm{Var}(N_{\theta_k}) = \frac{1}{\pi^2}\left(\log(d) + 1 + \gamma + \log|2\,\sin\left(\frac{\theta_{kj} - \theta_{kl}}{2}\right)|\right) + o(1), \tag{59}$$

where $\gamma \approx 0.577$ is the Euler's constant.

This theorem, gives a concrete formula for calculating the expectation value and variance of the random variable that represents the number of eigenvalues of a random unitary matrix, in each arc of the unit circle and hence can be used to study the distribution of eigenvalues of random matrices.

Appendix B. qPUF-based identification protocols

In this appendix we give the full description of the qPUF-based identification protocols introduced in [24] which we briefly describes in section 6.

B.1. Identification with high-resource verifier

This protocol, is run between the Alice, the verifier, and Bob, the prover and it is divided into three sequential phases,

(a) *Setup phase*:
1. Alice has the qPUF device.
2. She randomly picks $K \in \mathcal{O}(\mathrm{poly}\log D)$ classical strings $\phi_i \in \{0,1\}^{\log D}$.
3. Alice selects and applies a Haar-random state generator operation denoted by the channel $\mathcal{E}$ to locally create the corresponding quantum states in $\mathcal{H}^D$: $\phi_i \xrightarrow{\mathcal{E}} |\phi_i^c\rangle, \quad \forall i \in [K]$.
4. She queries the qPUF individually with each challenge $|\phi_i^c\rangle$ a total of M number of times to obtain M copies of the response state $|\phi_i^r\rangle$ and stores them in their local database $S \equiv \{|\phi_i^c\rangle, |\phi_i^r\rangle^{\otimes M}\}_{i=1}^K$.
5. Alice publicly transfers the qPUF to Bob.

(b) *Identification phase*:
1. Alice uniformly selects a challenge labelled ($i \xleftarrow{\$} [K]$), and sends the state $|\phi_i^c\rangle$ over a public quantum channel to Bob.
2. Bob generates the output $|\phi_i^p\rangle$ by querying the challenge received from Alice to the qPUF device.
3. The output state $|\phi_i^p\rangle$ is sent to Alice over a public quantum channel.
4. This procedure is repeated with the same or different states a total of $R \leqslant K$ times.

(c) *Verification phase*:
1. Alice runs a quantum equality test algorithm on the received response from Bob and the M copies of the correct response that she has in the database. This algorithm is run for all the R CRP pairs.
2. She outputs '1' implying successful identification if the test algorithm returns '1' on all CRPs. Otherwise, she outputs '0'.

The quantum verification algorithm run by Alice can be both SWAP or GSWAP tests described in the preliminary section.

B.2. Identification with low-resource verifier

This protocol is run between Alice, the verifier, and Bob, the prover in three sequential phases,
Low-resource verifier qPUF-based protocol

(a) *Setup phase*:
1. Alice has the qPUF device.
2. Alice randomly picks $K \in \mathcal{O}(\mathrm{poly}\log D)$ classical strings $\phi_i \in \{0,1\}^{\log D}$.
3. Alice selects and applies a Haar-random state generator operation denoted by the channel $\mathcal{E}$ to locally create the corresponding quantum states in $\mathcal{H}^D$: $\phi_i \xrightarrow{\mathcal{E}} |\phi_i^c\rangle, \quad \forall i \in [K]$.
4. Alice queries the qPUF individually with each quantum challenge $|\phi_i^c\rangle$ to obtain the response state $|\phi_i^r\rangle$.

Algorithm 1. `cVer` algorithm.

Description: Let $S_N = \{0,1\}^N$ be the input N-bit string. Let $P = \{i_k\}_{k=1}^{N/2}$ be the set of indices showing the rounds of the protocol where $b = 1$. Algorithm consists of two tests, `test1` and `test2` as follows:

```
test1:
forall i in P do
    if s_i = 0 then
        count ← count + 1;
    end
end
if count = N/2 then
    return 1;
else
    return 0;
end
```

```
test2:
if test1 = 0 then
    return 0;
else
    forall i not in P do
        if s_i = 1 then
            count ← count + 1;
        end
    end
    if |count − δ N/2| ⩽ δ_er then
        return 1;
    else
        return 0;
    end
end
```

5. Alice creates states $|\phi_i^{\perp}\rangle$ orthogonal to $|\phi_i^c\rangle$ and queries the qPUF device with them to obtain the trap states labelled as $|\phi_i^{\text{trap}}\rangle$. The unitary property of qPUF device ensures that $\langle\phi_i^{\text{trap}}|\phi_i^r\rangle = 0$.
6. She creates a local database $S \equiv \{|\phi_i^c\rangle, \{|\phi_i^r\rangle, |\phi_i^{\text{trap}}\rangle\}\}$ for all $i \in [K]$. Thus the S registers stores the challenge state $|\phi_i^p\rangle$ and the corresponding valid response state and the trap state which is orthogonal to the response state.
7. Alice publicly transfers the qPUF to Bob.

(b) *Identification phase*:

1. Alice randomly selects a subset $N \subseteq K$ different challenges $|\phi_i^c\rangle$ and sends them over a public channel to Bob.
2. She randomly selects $N/2$ positions, marks them $b = 1$ and sends the valid response states $|\phi_i^1\rangle = |\phi_i^r\rangle$ to Bob. On the remaining $N/2$ positions, marked as $b = 0$, she sends the trap states $|\phi_i^0\rangle = |\phi_i^{\text{trap}}\rangle$.

(c) *Verification phase*:

1. Bob queries the qPUF device with the challenge states received from Alice to generate the response states $|\phi_i^p\rangle$ for all $i \in [N]$.
2. He performs a quantum equality test algorithm by performing a SWAP test between $|\phi_i^p\rangle$ and the response state $|\phi_i^b\rangle$ received from Alice. This algorithm is repeated for all the N distinct challenges.
3. Bob labels the outcome of N instances of the SWAP test algorithm by $s_i \in \{0,1\}$ and sends them over a classical channel to Alice.
4. Alice runs a classical verification algorithm $\texttt{cVer}(s_1, \ldots, s_N)$ and outputs '1' implying that Bob's qPUF device has been successfully identified. She outputs '0' otherwise.

The classical verification algorithm, `cVer`, receives an N-bit binary string S_N as input. The algorithm is divided into two tests as is as follows (algorithm 1):

ORCID iDs

Mina Doosti https://orcid.org/0000-0003-0920-335X
Kaushik Chakraborty https://orcid.org/0000-0002-6425-0418

References

[1] Yao A C 1982 Theory and application of trapdoor functions *23rd Annual Symp. Foundations of Computer Science (SFCS)* (Piscataway, NJ: IEEE) pp 80–91
[2] Shamir A 1983 On the generation of cryptographically strong pseudorandom sequences *ACM Trans. Comput. Syst.* **1** 38–44
[3] Blum M and Micali S 1984 How to generate cryptographically strong sequences of pseudorandom bits *SIAM J. Comput.* **13** 850–64
[4] Goldreich O, Goldwasser S and Micali S 1986 How to construct random functions *J. ACM* **33** 792–807
[5] HÅstad J, Impagliazzo R, Levin L A and Luby M 1999 A pseudorandom generator from any one-way function *SIAM J. Comput.* **28** 1364–96
[6] Goldreich O, Goldwasser S and Micali S 1984 On the cryptographic applications of random functions *Workshop on the Theory and Application of Cryptographic Techniques* (Berlin: Springer) pp 276–88
[7] Luby M and Rackoff C 1988 How to construct pseudorandom permutations from pseudorandom functions *SIAM J. Comput.* **17** 373–86
[8] Rompel J 1990 One-way functions are necessary and sufficient for secure signatures *Proc. 22nd Annual ACM Symp. Theory of Computing* pp 387–94
[9] Rührmair U, Sölter J and Sehnke F 2009 On the foundations of physical unclonable functions *IACR Cryptol. ePrint Arch.: Report 2009:277*
[10] Ji Z, Liu Y-K and Song F 2018 Pseudorandom quantum states *Annual Int. Cryptology Conf.* (Berlin: Springer) pp 126–52
[11] Arapinis M, Delavar M, Doosti M and Kashefi E 2021 Quantum physical unclonable functions: possibilities and impossibilities *Quantum* **5** 475
[12] Brakerski Z and Shmueli O 2020 Scalable pseudorandom quantum states *Annual Int. Cryptology Conf.* (Berlin: Springer) pp 417–40
[13] Delvaux J 2017 Security analysis of PUF-based key generation and entity authentication *PhD Dissertation* Shanghai Jiao Tong University, China
[14] Herder C, Yu M-D, Koushanfar F and Devadas S 2014 Physical unclonable functions and applications: a tutorial *Proc. IEEE* **102** 1126–41
[15] Ganji F, Tajik S, Fäßler F and Seifert J-P 2016 Strong machine learning attack against PUFs with no mathematical model *Int. Conf. Cryptographic Hardware and Embedded Systems* (Berlin: Springer) pp 391–411
[16] Rührmair U, Sehnke F, Sölter J, Dror G, Devadas S and Schmidhuber J 2010 Modeling attacks on physical unclonable functions *Proc. 17th ACM Conf. Computer and Communications Security* pp 237–49
[17] Khalafalla M and Gebotys C 2019 PUFs deep attacks: enhanced modeling attacks using deep learning techniques to break the security of double arbiter PUFs *2019 Design, Automation & Test in Europe Conf. Exhibition (DATE)* (Piscataway, NJ: IEEE) pp 204–9
[18] Gianfelici G, Kampermann H and Bruß D 2020 Theoretical framework for physical unclonable functions, including quantum readout *Phys. Rev.* A **101** 042337
[19] Nikolopoulos G M and Diamanti E 2017 Continuous-variable quantum authentication of physical unclonable keys *Sci. Rep.* **7** 46047
[20] Wootters W K and Zurek W H 1982 A single quantum cannot be cloned *Nature* **299** 802–3
[21] Knill E 1995 Approximation by quantum circuits (arXiv:quant-ph/9508006)
[22] Carolan J *et al* 2015 Universal linear optics *Science* **349** 711–6
[23] Kumar N, Mezher R and Kashefi E 2021 Efficient construction of quantum physical unclonable functions with unitary t-designs (arXiv:2101.05692)
[24] Doosti M, Kumar N, Delavar M and Kashefi E 2021 Client-server identification protocols with quantum puf *ACM Trans. Quantum Comput.* **2** 1–40
[25] Boneh D, Dagdelen Ö, Fischlin M, Lehmann A, Schaffner C and Zhandry M 2011 Random oracles in a quantum world *Int. Conf. Theory and Application of Cryptology and Information Security* (Berlin: Springer) pp 41–69
[26] Mosca M 2018 Cybersecurity in an era with quantum computers: will we be ready? *IEEE Secur. Priv.* **16** 38–41
[27] Song F 2014 A note on quantum security for post-quantum cryptography *Int. Workshop on Post-Quantum Cryptography* (Berlin: Springer) pp 246–65
[28] Doosti M, Delavar M, Kashefi E and Arapinis M 2021 A unified framework for quantum unforgeability (arXiv:2103.13994)
[29] Holevo A S 1973 Bounds for the quantity of information transmitted by a quantum communication channel *Probl. Pereda. Inf.* **9** 3–11 http://mi.mathnet.ru/eng/ppi/v9/i3/p3
[30] Buhrman H, Cleve R, Watrous J and De Wolf R 2001 Quantum fingerprinting *Phys. Rev. Lett.* **87** 167902
[31] Barenco A, Berthiaume A, Deutsch D, Ekert A, Jozsa R and Macchiavello C 1997 Stabilization of quantum computations by symmetrization *SIAM J. Comput.* **26** 1541–57
[32] Xu F, Arrazola J M, Wei K, Wang W, Palacios-Avila P, Feng C, Sajeed S, Lütkenhaus N and Lo H-K 2015 Experimental quantum fingerprinting with weak coherent pulses *Nat. Commun.* **6** 8735
[33] Buhrman H, Cleve R, Massar S and De Wolf R 2010 Nonlocality and communication complexity *Rev. Mod. Phys.* **82** 665
[34] Kumar N, Diamanti E and Kerenidis I 2017 Efficient quantum communications with coherent state fingerprints over multiple channels *Phys. Rev.* A **95** 032337
[35] Kobayashi H, Matsumoto K and Yamakami T 2003 Quantum Merlin–Arthur proof systems: are multiple Merlins more helpful to Arthur? *Int. Symp. Algorithms and Computation* (Berlin: Springer) pp 189–98
[36] Chabaud U, Diamanti E, Markham D, Kashefi E and Antoine J 2018 Optimal quantum-programmable projective measurement with linear optics *Phys. Rev.* A **98** 062318
[37] Armknecht F, Moriyama D, Sadeghi A-R and Yung M 2016 Towards a unified security model for physically unclonable functions *Cryptographers' Track at the RSA Conf.* (Berlin: Springer) pp 271–87

[38] Brakerski Z and Shmueli O 2019 (pseudo) random quantum states with binary phase *Theory of Cryptography Conf.* (Berlin: Springer) pp 229–50
[39] Dankert C, Cleve R, Joseph E and Livine E 2009 Exact and approximate unitary two-designs and their application to fidelity estimation *Phys. Rev.* A **80** 012304
[40] Nielsen M A and Chuang I L 2010 *Quantum Computation and Quantum Information* 10th edn (Cambridge: Cambridge University Press)
[41] Kretschmer W 2021 Quantum pseudorandomness and classical complexity (arXiv:2103.09320)
[42] Meckes E S and Meckes M W 2019 A sharp rate of convergence for the empirical spectral measure of a random unitary matrix *J. Math. Sci.* **238** 530–6
[43] Bouland A, Fefferman B and Vazirani U 2019 Computational pseudorandomness, the wormhole growth paradox, and constraints on the AdS/CFT duality (arXiv:1910.14646)
[44] Alagic G and Fefferman B 2016 On quantum obfuscation (arXiv:1602.01771)
[45] Brakerski Z and Henry Y 2020 Quantum garbled circuits (arXiv:2006.01085)
[46] Meckes E S 2019 *The Random Matrix Theory of the Classical Compact Groups* vol 218 (Cambridge: Cambridge University Press)
[47] Diaconis P and Shahshahani M 1994 On the eigenvalues of random matrices *J. Appl. Probab.* **31** 49–62
[48] Wieand K 2002 Eigenvalue distributions of random unitary matrices *Probab. Theory Relat. Fields* **123** 202–24