Practical Evaluation of a Quantum Physical Unclonable Function and Design of an Authentication Scheme

Franco Cirillo
University of Salerno
Fisciano (SA), Italy
fracirillo@unisa.it

Christian Esposito
University of Salerno
Fisciano (SA), Italy
esposito@unisa.it

***Abstract*—With the increase of digital devices, the need for robust authentication mechanisms has become crucial. Traditional methods relying on cryptographic key management are susceptible to various risks, particularly the exposure of keys to interception or theft. As cyber threats evolve, the shortcomings of these methods are accentuated, necessitating more secure solutions. Physically Unclonable Functions (PUFs) have emerged as a potential alternative, utilizing inherent hardware variations for device authentication without stored secrets. However, recent studies reveal vulnerabilities in conventional PUF implementations. Simultaneously, there's a growing recognition for authentication mechanisms tailored for quantum devices. This recognition has prompted the exploration of Quantum PUFs (QPUFs), which represent a promising solution to enhance security and reliability, leveraging the unique properties of quantum mechanics. In this paper, we propose a novel approach using QPUFs for device authentication that does not require any quantum communication channel or even quantum memory. We design a quantum circuit to serve as a QPUF, evaluating metrics such as instability, randomness, and uniqueness. Additionally, we devise an authentication scheme that exploits the challenge-response paradigm, taking advantage of the distinctive properties of quantum PUFs. Furthermore, we delineate a threat model to identify and mitigate potential risks associated with the authentication process. By assessing the proposed QPUFs efficacy on real real quantum hardware provided by IBM, this research contributes to the advancement of secure authentication protocols in quantum era.**

***Index Terms*—Quantum Physical Unclonable Function (QPUF), Authentication, Quantum, Security.**

I. Introduction

Thanks to the progressive increase in the number of digital devices, the authentication has become ever more critical, yet a definitive solution remains unreachable. Traditional authentication methods rely on cryptographic key management, a process that has long been vulnerable to various risks and challenges. One of the primary vulnerabilities lies in the potential exposure of cryptographic keys, which are essential for verifying the identity of devices and ensuring the integrity of data transmission. In traditional systems, these keys are often stored centrally or distributed across different entities, making them susceptible to interception or theft by malicious actors. Moreover, the distribution of keys presents logistical challenges, particularly in large-scale systems or distributed networks, where ensuring the secure transfer and storage of keys can be complex and error-prone.

As cyber threats continue to evolve and become increasingly sophisticated, the shortcomings of traditional authentication methods are amplified. Attackers are constantly devising new techniques to exploit vulnerabilities in cryptographic systems, ranging from brute-force attacks to sophisticated cryptographic attacks. Additionally, the proliferation of interconnected devices and the rise of cloud computing have expanded the attack surface [1], exposing traditional authentication mechanisms to new vectors of exploitation.

In this rapidly evolving threat landscape, the need for strong authentication mechanisms has never been more critical. Organizations and individuals alike require robust authentication solutions that can withstand sophisticated attacks and provide assurance of identity and data integrity. Consequently, there is a growing recognition of the limitations of traditional methods and a corresponding shift towards adopting more secure and resilient authentication technologies.

Among potential solutions, Physical Unclonable Functions (PUFs) have garnered attention for their promising ability to provide device authentication without relying on stored secrets [2]. PUFs exploit the inherent physical variations present in hardware components to generate unique identifiers for each device. PUFs function on a Challenge-Response paradigm, in which a PUF is presented with a challenge, typically in the form of a random input or query. These properties cause the PUF to produce a response that is inherently tied to its specific physical structure and characteristics. This response is then compared against an expected value or stored reference to verify the authenticity of the device or to complete a cryptographic operation. However, recent studies [3]–[6] have revealed that some conventional PUF implementations suffer from security vulnerabilities, susceptibility to cloning, and vulnerability to machine learning-based attacks, casting doubts on their reliability in real-world applications.

With the advent of quantum computing, leveraging quantum principles for device authentication presents a compelling avenue, thereby highlighting an increasing necessity for authentication mechanisms applicable to quantum devices. An exemplary application that strongly demands novel authentication mechanisms is undoubtedly Quantum Federated Learning. This nascent interdisciplinary domain integrates the principles of Quantum Computing and Federated Learning, aiming to harness quantum technologies for the advancement of privacy, security, and efficacy within the learning process. However, device authentication is fundamental in Quantum Federated Learning, as it is essential for all collaborating devices within the learning algorithm to be authenticated in order to contribute to the overall model update, particularly in sensitive domains like healthcare or finance.

Quantum PUFs (QPUFs) exploit the principles of quantum mechanics to generate unique and unpredictable responses, offering heightened security compared to classical PUFs [7]. The foundational concepts of superposition and entanglement, intrinsic to quantum mechanics, underpin the inherent unpredictability and non-reproducibility of responses produced by QPUFs [8].

Today's Quantum computers are susceptible to various types of quantum errors [9]. These errors stem from diverse sources such as manufacturing imperfections, control errors, environmental interactions. All these errors are inherently leveraged by QPUFs to generate unique responses for each device.

QPUFs offer notable advantages rooted in the non-cloning theorem of quantum mechanics [10], ensuring the inherent unclonability of quantum information. Leveraging this principle, QPUFs exhibit benefits such as high entropy and resistance to cloning attacks, making them well-suited for cryptographic applications where data integrity and authenticity are paramount.

Quantum computing, while still in its nascent stages, has seen significant advancements from various stakeholders. Companies such as IBM, Google, and D-Wave are at the forefront of quantum computing research and development, with notable progress in the construction of increasingly powerful quantum processors.

In this paper, we propose a novel approach to enhance device authentication through the utilization of quantum PUFs. Our contributions are threefold:

1) firstly, we design a quantum circuit to function as a QPUF, evaluating metrics such as instability, randomness, and uniqueness to assess its efficacy.
2) Secondly, we develop an authentication scheme that leverages the challenge-response paradigm, capitalizing on the unique properties of QPUFs.
3) Ultimately, a threat model is delineated, to identify and analyze potential risks, threats, and vulnerabilities that may affect the scheme. This process helps understand potential attack scenarios and design appropriate countermeasures to mitigate or prevent such threats.

Our method aims to address the limitations of current technology, by circumventing the necessity for quantum channels and quantum memory in crafting an efficient QPUF system, which has been tested on real devices and it is repeatable. The remainder of the paper is structured as follows: in Section II we delve into the scientific background, by establishing the importance of secure authentication and introducing PUF and QPUF concepts. Section III reviews the current state of the art, while Section IV proposes a novel QPUF system, and Section V details an authentication scheme using the proposed QPUF. In Section VI potential threats are analyzed, and lastly Section VII concludes by summarizing findings and suggesting future research directions.

II. Scientific Background

A. Classical PUFs

Prior to an in-depth exploration of our methodology, we present a concise overview of the fundamental attributes of classical PUFs. These functions are digital circuits that operate based on the challenge-response model, wherein both challenges and responses are represented as bitstrings of predefined lengths. The inherent uniqueness of the mapping function, coupled with its resistance to tampering, derives from the exploitation of nanoscale imperfections introduced during the fabrication process of the circuit. Furthermore, the continued unpredictability of responses is asserted, theoretically rendering both the manipulation of physical imperfections and the successful cloning of devices unfeasible.

However, in practice, the veracity of these claims is not yet proven. Indeed, instances have been reported where successful cloning was achieved in certain implementations of PUFs [11], [12], challenging the notion of their absolute resistance to duplication. Such cases highlight the importance of ongoing research and rigorous testing to fully understand the security implications of PUF technology.

PUFs can be categorized into two main types: weak PUFs and strong PUFs. Weak PUFs are characterized by a limited number of Challenge-response pairs (CRPs), whereas strong PUFs demonstrate a CRP set that grows exponentially with the length of the challenges. Furthermore, classical PUFs can be classified as either memory-based or delay-based. Memory-based PUFs, such as those employing Static Random-Access Memory (SRAM), derive responses by exploiting nanoscale imperfections within symmetric memory cells. In contrast, delay-based PUFs ascertain responses by measuring discrepancies in signal propagation times across symmetric paths, as demonstrated by the Arbiter-PUF or Anderson-PUF, for instance.

In a classical scenario of using PUFs for authentication purposes, the process typically involves two main phases: enrollment and authentication.

1) Enrollment Phase: each PUF instance undergoes a unique initialization process. This involves capturing the inherent nanoscale imperfections within the circuitry that serve as the basis for generating its unique response to specific challenges. A CRP is generated by presenting a challenge to the PUF, typically in the form of a bitstring, and recording the corresponding response. This process is repeated multiple times to create a sufficient number of CRPs for the PUF.
2) Authentication Phase: the PUF is utilized to verify the identity of a device or the owner seeking access. A

challenge is presented to the PUF, typically generated randomly or based on a predetermined protocol. The PUF generates a response to the challenge, based on its unique characteristics encoded during the enrollment phase. The response obtained is compared to the stored challenge-response pairs in the database. If the response matches any of the stored CRPs within an acceptable error margin, authentication is successful and access is granted. Otherwise, authentication fails, indicating a potential unauthorized attempt to access the system.

Throughout both phases, security measures such as cryptographic protocols, secure communication channels, and physical protections may be implemented to safeguard against potential attacks or tampering.

B. Quantum PUFs

A QPUF represents a new paradigm within the domain of PUF, distinguished by its utilization of quantum computation to enhance security and uniqueness. Formally, a QPUF operates on the fundamental principles of quantum mechanics to exploit inherently quantum properties for the generation of unique responses to challenges. The concept of superposition and entanglement, fundamental to quantum mechanics, forms the basis for the inherent unpredictability and non-reproducibility of responses generated by QPUFs.

In a Quantum PUF, the enrollment and authentication phases closely resemble those of classical PUFs, though with a distinct quantum mechanical substructure. During the enrollment phase, quantum states of physical entities are manipulated to encode the unique characteristics of the PUF. These quantum states are measured or observed to generate CRPs, which are subsequently stored securely.

In the authentication phase, challenges are presented to the QPUF, and its quantum states are manipulated to generate responses based on its unique characteristics encoded during enrollment. The responses are obtained through quantum measurement processes that inherently introduce randomness and unpredictability. These responses are then compared against the stored CRPs to authenticate the device or the owner seeking access.

QPUFs offer distinct advantages rooted in the non-cloning theorem of quantum mechanics [10]. This theorem stipulates that an arbitrary quantum state cannot be perfectly replicated without altering the original state, thus ensuring the inherent unclonability of quantum information. Leveraging this principle, QPUFs exhibit several notable benefits, such as high entropy and resistance to cloning attacks. This property makes QPUFs particularly well-suited for cryptographic applications where data integrity and authenticity are essential. Therefore, as quantum computing technologies advance, classical cryptographic schemes may become vulnerable to quantum attacks. QPUFs, based on principles of quantum mechanics, offer a potential solution by harnessing quantum properties for secure authentication and cryptographic operations, thus future-proofing against emerging threats.

However, QPUFs also pose significant technical challenges, including the need for precise control over quantum states. Quantum computers are susceptible to different types of quantum errors [13], including gate error, decoherence or dephasing, readout error, single-qubit error, two-qubit error, and crosstalk [14]. Gate error introduces a probability of error in logical operations, while decoherence occurs as qubits interact with the environment, leading to state loss. Readout errors may result from imperfections in readout circuitry, causing bit-flips. Single-qubit errors arise from errors in single-qubit gates, such as the Hadamard gate or rotation gates, while two-qubit errors stem from errors in two qubit gates, like the CNOT gate. Additionally, crosstalk occurs when parallel gate operations on different qubits impact each other's performance. The rates of these errors vary among qubits and hardware, providing a unique signature for hardware identification.

Multiple factors contribute to errors in quantum computing systems, encompassing manufacturing imperfections, control errors, thermal gradients, environmental interactions, and microwave hygiene issues [15]. Manufacturing imperfections, such as defects, induce charge noise, thereby serving as a source of gate error. Control errors may arise from inaccurately calibrated gate pulses, resulting in under- or over-rotation of qubits.

Similar to gate delays in classical chips, which represent variability and serve as hardware signatures, gate error rates serve as representative indicators of variability in the quantum domain. For example, in IBM machines utilizing Transmon qubits, gate errors may result from trapped charge in defects, with the number of defects varying among qubits due to manufacturing variations.

In summary, QPUFs represent a promising frontier in the advancement of secure authentication and cryptographic systems, leveraging the unique properties of quantum mechanics to enhance security and reliability. However, their practical realization and integration into real-world applications require further exploration and technological advancements.

III. State of The Art

The notion of leveraging QPUF-based identification protocols was initially introduced in [16], wherein the concept of quantum read-out of PUF (QR-PUF) was delineated, and an identification protocol was devised based on this concept. Consequently, the authors of [17] introduced a novel concept of PUF, termed QPUF. According to their definition, unlike QR-PUFs and resembling classical PUFs, no entity, including both the manufacturer and the verifier, has knowledge of the unitary of QPUF. This condition guarantees the demonstrable security of QPUFs against forgery attacks. Despite the discussion of theoretical foundations, practical aspects such as application, methodology, and circuitry relevant to the authentication are not addressed.

Several implementation solutions have been explored, including [18], which employ adapted quantum readout protocols enabling PUF authentication of both classical and quantum information through classical light or single-photon-level manipulations. An other solution is depicted in [19], that presents an authentication process that involves illuminating the PUF key with a light pulse containing fewer photons than spatial degrees of freedom, followed by verifying the spatial shape of the reflected light. Nonetheless, these systems rely on specialized hardware and therefore do not tackle the broader issue associated with QPUFs, therefore there are some documented attacks [20], [21].

The paper, referred to as [22], introduces two variants of QPUFs aimed at establishing trust in public cloud-based quantum hardware, the 1-qubit gate error (Hadamard Gate-Based QPUF) and decoherence error to generate the signature. Experimental trials with the QPUFs were conducted using real quantum hardware provided by IBM. In the proposed protocol, the challenge involves a classical representation of a parameterized unitary operation executed on the quantum computer. The response is computed as the mean of multiple measurement outcomes of the qubits in the computational basis. Observations from the results indicate that distinguishing features are not readily discernible solely based on this approach. However, by modifying parameters such as rotation or the number of idle gates, the uniqueness improves. Overall, the performance of the qubit gate error based QPUF demonstrates superior stability.

These results were later analyzed in [23], demonstrating a successful machine learning attack based on a regression model. The study practically showed that it is feasible to learn the responses of the QPUF construction in [22]. The authors also discuss potential causes, explaining that the absence of entanglement between qubits and the fixed structure of the circuit contributed to the success of the attack.

This work [24] introduces a QPUF architecture featuring an innovative method for PUF key generation and noise reduction in noisy quantum systems. The proposed PUF design is constructed using Quantum Hadamard Gates and Ry gates. However, the circuit evaluates only the Hadamard gate on a single qubit, and therefore, it is subject to the same vulnerabilities identified in the previous paper, which was compromised using machine learning techniques.

The paper [25] outlines the construction of QPUFs utilizing the approximate unitary transformation design. This approach involves conducting random single-qubit XY plane measurements within the interval $[0, 2\pi]$ on the non-output qubits of a regularly structured graph state, obtained also with controlled z-gates. However, despite the presentation of results regarding uniqueness and unknownness, there is no specification regarding the devices on which the experimental tests were conducted, nor is any code provided for repeatability. Furthermore, only the basic structure of the QPUF is explained, without the mention of an authentication mechanism.

For this purpose, the authors of [26] have introduced a unified theoretical framework encompassing both classical PUFs and QR-PUFs. They offer a quantitative characterization of PUF properties, concentrating on robustness and unclonability, alongside proposing a generic identification scheme relying on both classical and quantum PUFs. Although the study may be beneficial, it solely investigates QR-PUFs, thereby necessitating the challenges and results to be inherently quantum in nature.

Paper [27] presents two identification protocols utilizing QPUFs. The first protocol enables a low-resource party to authenticate its identity to a high-resource party, while the second protocol facilitates the vice versa scenario. Unlike existing identification protocols relying on QR-PUFs, which are dependent on security against a specific set of attacks, these protocols offer demonstrable exponential security against any Quantum Polynomial-Time adversary with resource-efficient parties. However, the authentication protocols employing QPUFs necessitate a quantum memory and a quantum communication channel to execute the exchange of quantum states between the verifier and the prover.

With respect to the studies previously discussed and learning from these findings, our approach tries to make up for these shortcomings. The proposed solution avoids the use of quantum channels and quantum memory to design a generic QPUF, that is evaluated on real devices and can be repeatable. It is also proposed an authentication schema based on this construction.

IV. QPUF MECHANISM AND EXPERIMENTAL RESULTS

In this section, we describe the proposed QPUF system and provide an exposition of the empirical findings by computing the QPUF quality, then it is given an interpretation of the results.

A. QPUF circuit

The proposed QPUF circuit leverages the inherent biasing of qubits towards the 1 or 0 state to generate the response. This biasing can arise from gate errors, including those associated with X-Y-Z rotation gates, or from readout errors.

Initially, each qubit is initialized to the zero state. Subsequently, each qubit undergoes sequential rotations in every plane using X-Y-Z rotation gates, with angles parameterized within the range $[0, 2\pi]$. Next, each qubit is entangled with its predecessor or successor using Controlled-Z gates. These two steps are iterated once more to ensure entanglement across all qubits. Finally, all qubits are subjected to measurement.

Ideally, the qubits should exhibit a probability distribution spanning both the 0 and 1 states, contingent upon the parameters of the gates, i.e., the rotation angles. However, the actual probability distribution is expected to demonstrate bias towards either the zero or one state, influenced by the errors present, thereby serving as a unique device signature.

The Figure 1 shows an instance of the proposed QPUF circuit, based on 8 qubits and with random gates angles.

The resultant circuit addresses certain issues delineated in Section III, namely the requirement for entangled qubits facilitated by the utilization of CZ gates, and the necessity for a heightened challenge space achieved through the parameterization of X-Y-Z gates. Furthermore, challenges and responses of the mechanisms are not of a quantum nature, implying that

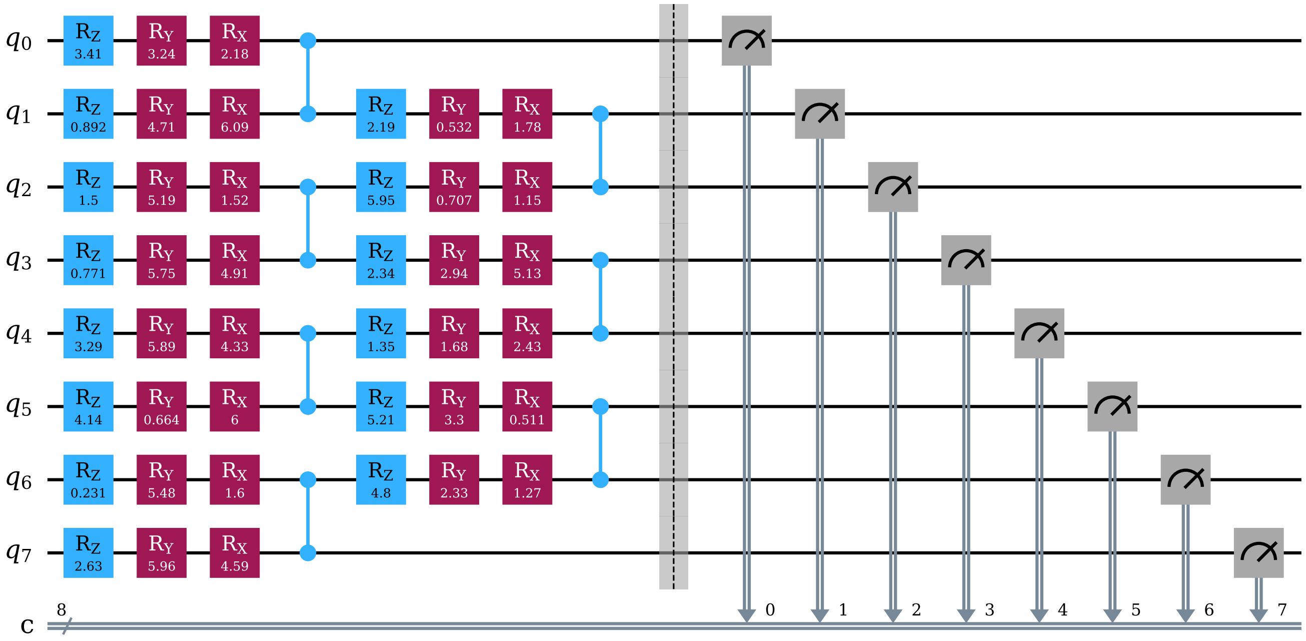

Fig. 1: Instance of 8-qubit proposed QPUF circuit based on X-Y-Z rotation gates and Controlled-Z gate.

there is no requirement for a quantum communication channel between the devices seeking authentication, nor does the verifier need to possess quantum memory to store challenges and responses. Instead, a classical memory will be sufficient for this purpose.

Utilizing the framework of this QPUF circuit, challenges appear as vectors encompassing all parameters for every individual gate within a single instance. For instance, within an 8-qubit circuit as depicted in Figure 2, a challenge is delineated by 14 angles per 3 gate types, with values falling within the range $[0, 2\pi]$. Each respective response, conversely, constitutes the outcome of measuring all qubits following the execution of the circuit a predetermined number of times. In practical terms, the response corresponds to a dictionary wherein each potential combination of qubit values is associated with its corresponding output percentage between 0 and 1, and where all values of a single response sum to 1.

B. QPUF metrics

To assess the quality of the proposed QPUF system, the following metrics have been tested:

Instability: it refers to variations and unpredictability in the QPUF responses of a single device due to factors such as manufacturing imperfections, control errors, thermal gradients and environmental interactions. These instabilities can compromise the reliability and security of QPUF-based systems.

In order to evaluate such a Instability, we can compare QPUF responses by means of Normalized Absolute Probabilistic Distance (NAPD) over every response pair. Let $r_{n,q}^{k}$ be the q-th combination of qubit results on $Q = 2^{\text{nqubits}}$, derived from the n-th challenge and the k-th device of PUF responses; the NAPD between the response of the n-th challenge with the k-th device and of the m-th challenge with the h-th device, can be defined as follows:

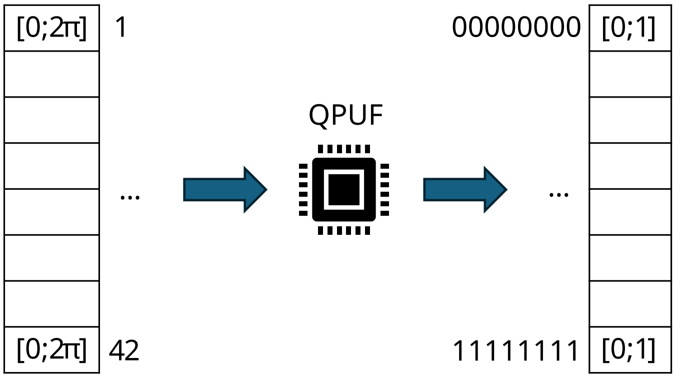

Fig. 2: QPUF maps an array of angles into an array of probabilities, one for each qubit result combination.

$$\text{NAPD}\left(r_n^k, r_m^h\right) = \frac{1}{2}\sum_{q=1}^{Q} |r_{n,q}^{k} - r_{m,q}^{h}| \tag{1}$$

The formula has been normalized by a factor of 2 because, considering the sum of the absolute differences in probabilities that individually sum to one, the range of possible values extends from 0 (identical responses) to 2 (completely opposing responses). Thus, the adjustment ensures that the range falls within 0 and 1.

Let $r_{n,i}^{k}$ denote the response corresponding to the i-th out of D executions, for the n-th out of N challenges of the k-th device. The Instability for the k-th device can be estimated as follows:

$$\text{Instability}\,(k) = \frac{1}{N}\sum_{n=1}^{N}\frac{2}{D\,(D-1)}\sum_{i=1}^{D}\sum_{j=i+1}^{D}\text{NAPD}(r_{n,i}^{k}, r_{n,j}^{k}) \tag{2}$$

For each challenge and for each distinct pair of executions on the same challenge, NAPD is computed, which is estimated by taking the average over the number of execution pairs given by the binomial coefficient $\binom{D}{2}$, and then normalized by the number of challenges, N.

Ideally, Instability in QPUFs should be minimized, approaching zero, indicating consistent responses over time.

Randomness: it refers to the stochastic nature of responses, ensuring that each response is maximally distinct from another, even when presented with similar challenges. Let r_n^k denote the response corresponding to the n-th out of N challenges of the k-th device. The Randomness for the k-th device can be estimated as follows:

$$\text{Randomness}\,(k) = \frac{2}{N\,(N-1)}\sum_{n=1}^{N}\sum_{m=n+1}^{N}\text{NAPD}(r_n^k, r_m^k) \tag{3}$$

For each distinct pair of challenges, NAPD is computed, which is estimated by taking the average over the number of challenges pairs given by the binomial coefficient $\binom{N}{2}$. Ideal Randomness values are ones as close to 1 as possible.

Uniqueness: denote that each generated output from every single device is distinct from outputs of all other devices, giving the same input. Let r_n^k denote the response corresponding to the n-th out of N challenges of the k-th out of K devices. The Uniqueness can be estimated as follows:

$$\text{Uniqueness} = \frac{2}{K\,(K-1)}\sum_{k=1}^{K}\sum_{h=k+1}^{K}\frac{1}{N}\sum_{n=1}^{N}\text{NAPD}(r_n^k, r_n^h) \tag{4}$$

For each distinct pair of devices and for each challenge, NAPD is computed, which is estimated by taking the average over the number of devices K pairs given by the binomial coefficient $\binom{K}{2}$, after being normalized by the number of challenges N. Ideal Uniqueness values are ones as close to 1 as possible.

C. Experimental results

In conducting experiments to evaluate QPUFs quality, real quantum hardware provided by IBM [28], namely ibm_brisbane, ibm_kyoto, and ibm_osaka, has been employed, leveraging the Qiskit SDK [29].

In general, the QPUF circuit described above has been employed with a qubit count of 8 and a measurement shot count of $20,000$ per circuit. Specifically, concerning Instability testing, a set of 10 challenges (N) and 5 executions each (D) were utilized. Figure 3 depicts the Instability distribution graph for all three tested devices. From the graphs, it can be observed that in all three devices, the Instability remains around 5/6%, not exceeding 7%. Furthermore, it has been observed that increasing the number of shots or the number of executions leads to a decrease in Instability values. Therefore, without limitations on the utilization of quantum computers, the results can certainly be improved.

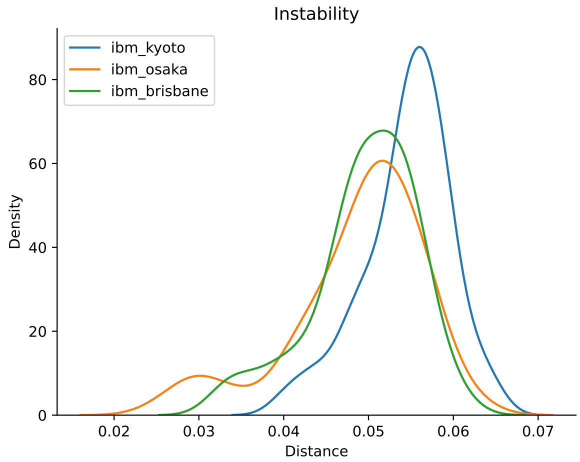

Fig. 3: Distribution of 8-qubits QPUFs Instability over $20,000$ shots, 10 challenges and 5 executions each, with ibm_kyoto, ibm_osaka and ibm_brisbane.

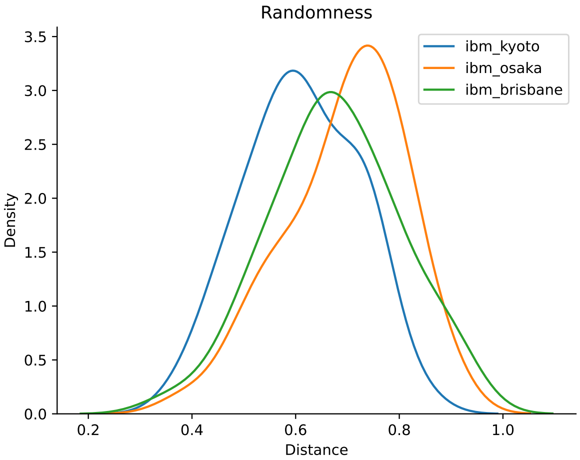

Fig. 4: Distribution of 8-qubits QPUFs Randomness over $20,000$ shots and 10 challenges, with ibm_kyoto, ibm_osaka and ibm_brisbane.

Concerning Randomness testing, the parameter N is set to 10. Figure 4 depicts the Randomness distribution graph for the three devices tested. From the graphs, it can be observed that in all three devices, the Randomness remains in the range 50-90%, with an average of 70%.

Concerning Uniqueness testing, the parameter N is set to 10 and K is 3 for the three IBM devices used. Figure 5 depicts the Uniqueness distribution graph above all three tested devices. From the graphs, it can be observed that overall the Uniqueness remains in the range 10-50%, with an average of 30%.

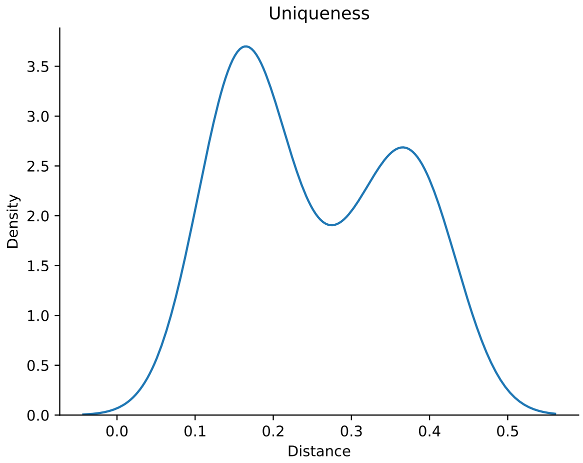

Fig. 5: Distribution of 8-qubits QPUFs Uniqueness over $20,000$ shots, 10 challenges and 3 devices.

The experiments are replicable and the source code is available on [30].

D. Interpretation and discussion of the results

To interpret the obtained results, it is essential to consider that the derived Instability values serve as an upper bound, given the continuous improvement observed by increasing the number of executions of the quantum circuit. The achieved results aimed at obtaining acceptable values rather than aiming for the best possible outcomes, primarily due to limitations in utilizing the quantum computing service. Additionally, concerning Randomness and Uniqueness, achieving the ideal value of 1 poses a significant challenge. This is because it would require each response to have a probability of 1 for only one combination of qubits and 0 for all others, and for every pair of compared responses, the combinations with a probability of 1 should be distinct. This would be the only scenario in which the NAPD would yield a normalized result of 1.

Overall, the metric graphs indicate low Instability and good Randomness of the proposed QPUF. Although the calculated Uniqueness values are satisfactory, the Uniqueness of devices utilizing the QPUF can be further enhanced by employing the authentication scheme described subsequently.

V. Device Authentication Scheme

Device authentication is a security process used to verify the identity of a device before granting it access to a network, system, or application. It ensures that only authorized devices are allowed to connect and communicate, thus enhancing overall security.

In device authentication, the device seeking access, referred to as the prover or claimant, typically presents evidence of identity to the verifying entity, referred to as the verifier. The verifier then verifies the authenticity of the presented information using authentication mechanisms. The goal of device authentication is to prevent unauthorized access and protect sensitive information from being accessed or manipulated by malicious actors.

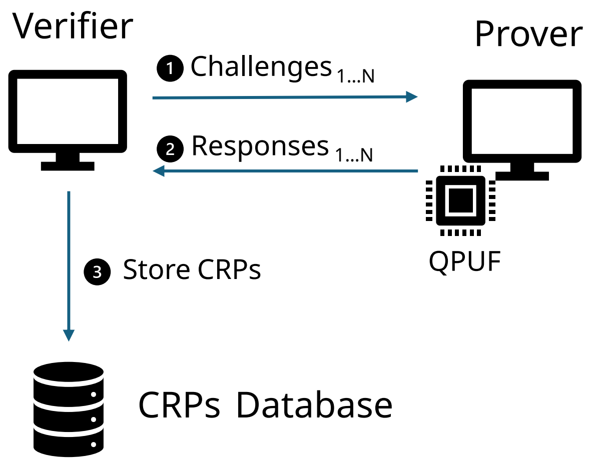

Fig. 6: Enrollment phase: after randomly generating a number N of challenges, the verifier assesses the responses using the device's QPUF within a secure environment, guaranteeing that the information remains safe from capture. Following this, the verifier stores the resulting CRPs.

The QPUF system previously described is utilized to design a device authentication protocol. Like a classical PUF authentication method, the QPUF authentication scheme proposed is composed of two different operations: an enrollment, where QPUF information is stored by the verifier, and an authentication phase, where the prover prove his identity using the device's QPUF.

A. Enrollment phase

During the enrollment phase, as in the Figure 6, the verifier randomly generates a number N of challenges and evaluates the responses using the QPUF of the device in a secure environment, ensuring that informations cannot be captured and remains safe. Subsequently, the verifier must store the resulting CRPs in a table, assigning to each challenge the value of the corresponding response, which is determined by the mean value across all execution shots of the quantum circuit.

B. Authentication phase

The enrollment phase is succeeded by the authentication phase, as depicted in Figure 7, wherein the verifier transmits m challenges, typically selected randomly, to the prover from the CRP database. These challenges are conveyed via a public classical channel to the prover, which elicits the responses to the received challenges exploiting the QPUF mechanism. Subsequently, the prover directly sends the responses to the verifier. Finally, the verifier checks whether all the received responses are similar to those stored in the local database.

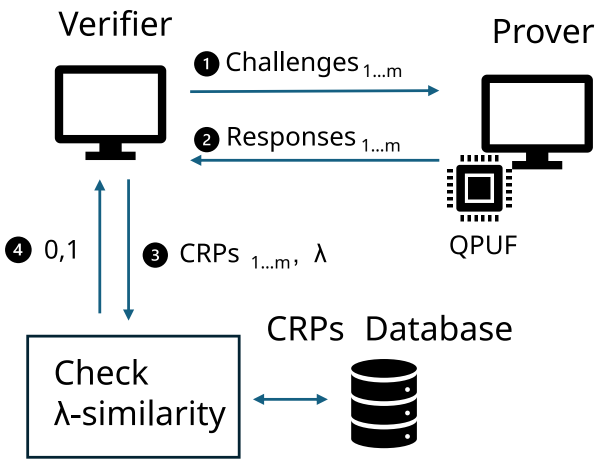

Fig. 7: Authentication phase: the verifier sends m challenges to the prover, which responds sending the responses obtained from the QPUF. The verifier then verifies whether all the received responses match those stored in the local database. If they do, the prover is authenticated. Otherwise, no information regarding the similarity of the responses is disclosed.

Upon affirmation, the prover is authenticated; otherwise, no information regarding the similarity of the responses is disclosed, and the process halts.

It is important, however, to clarify the concept of similarity. Two responses are deemed similar if their NAPD does not exceed a certain threshold parameter, λ. The parameter λ can be determined through instability analysis. In our case, based on experimental results, λ is set to 0.07, corresponding to 7%. This implies that two responses are considered similar only if their distance does not exceed 7%, as this was the maximum instability observed between pairs of responses for the same challenge and device. Furthermore, it is essential to recall that the parameter λ can be further lowered by conducting a more detailed instability analysis, thus performing multiple shots of circuit executions.

As demonstrated by the results, the uniqueness values is distinct from those of instability. This implies that, given the same challenge, the NAPD between two responses from the same device is significantly lower compared to when dealing with responses from two different devices. However, the security of the uniqueness of the QPUF can still be enhanced by increasing the parameter m, i.e., the number of challenges required for authentication, thereby reducing the probability of obtaining multiple responses similar to those of another device by an attacker.

VI. Threat model

The device authentication process is crucial for ensuring trust and security within systems by verifying the identities of devices seeking access to resources or services. In the context of quantum computing, the development of authentication protocols utilizing QPUFs presents both opportunities and challenges. The proposed protocol involve two main phases: enrollment and authentication.

However, despite the promise of QPUF-based authentication, several threats and vulnerabilities must be addressed to ensure the security of the protocol. It is essential for readers to understand the security context within which the scheme operates and its ability to mitigate potential attacks. Key components of the threat model include:

- Verifiers: They are expected to function precisely as required, accurately validating and processing authentication requests in a secure manner. Any impairment or unauthorized access to these entity could result in data leaks of CRPs database and in the possibility by an attacker to challenge repeatedly the prover's QPUF.
- Provers: While operating with integrity is expected, there is a risk of malicious compromise or manipulation by attackers. Such compromises could lead to authentication and impersonation attempts. Nonetheless, the system is designed to anticipate and mitigate such potential attacks, as with each authentication attempt by an attacker, corresponding to the submission of m responses, only a response indicating whether the authentication was successful or not is returned. Therefore, no information about the correctness of each individual response is provided; an attacker would need to guess all the responses to find out whether they are all correct. In this scenario, the security of the scheme can be enhanced by increasing the parameter m.
- Malicious Actors: They can be placed between the verifier and prover to eavesdrop on the communication and retrieve information, thereby obtaining CRPs. A data-driven learning analysis should be conducted to determine if an attacker can learn the QPUF function from the data. Nevertheless, theoretical security is provided by the fact that the circuit of the QPUFs is parameterized, and all qubits are entangled.

Mitigation strategies include employing encrypting communication channels to protect challenge-response exchanges, implementing robust response verification techniques utilizing an optimal λ parameter for similarity assessment, increasing the parameter m, ensuring the security of the CRP database through access controls and encryption, and enhancing physical protection measures for the QPUF device to prevent tampering.

Overall, while QPUF-based authentication protocols offer the potential for enhanced security, addressing the associated threats and vulnerabilities is essential to fully realise their benefits.

VII. Conclusion and future work

The escalating proliferation of digital devices has underscored the critical need for robust authentication mechanisms. Traditional methods reliant on cryptographic key management are increasingly vulnerable, necessitating more secure alternatives. PUFs have emerged as a potential solution, but recent studies have exposed vulnerabilities in conventional implementations. QPUFs are establishing themselves as a promising avenue to overcome these issues. Leveraging quantum principles, QPUFs offer heightened security and resistance to cloning attacks.

In this study, we proposed a novel approach utilizing QPUFs for device authentication, without the need for quantum communication channels or quantum memory. By designing a quantum circuit to function as a QPUF, along with developing an authentication scheme based on the challenge-response paradigm, we have laid the groundwork for a more secure authentication process. Additionally, by delineating a threat model to identify and mitigate potential risks, we ensure the robustness of the authentication mechanism against evolving cyber threats.

The results of the evaluated metrics such as instability, randomness, and uniqueness on real quantum hardware provided by IBM not only contribute to the advancement of experimental QPUFs, but also demonstrates the practical feasibility of the proposed QPUF-based authentication in real-world scenarios.

While this study provides valuable insights into the efficacy of QPUFs for device authentication, there are several avenues for future research that justify exploration.

Although we attempted to conduct experiments utilizing three IBM quantum machines to validate the scalability and performance of our proposed QPUF-based authentication scheme, limitations arose due to constraints in available resources under free-access plans. Future work could involve collaborations to conduct experiments across several quantum machines to assess the scheme's robustness and performance in diverse environments.

As quantum computing continues to advance, future experiments could explore increased complexity, leveraging a greater number of qubits and PUF challenges, in order to obtain results more in line with reality.

While our study includes a thorough threat model analysis to identify potential risks associated with the authentication process, future work could delve deeper into the security implications of QPUFs in real-world applications. This includes exploring potential vulnerabilities, devising strategies to mitigate emerging threats, and conducting comprehensive security assessments to ensure the resilience of the authentication scheme against sophisticated cyber attacks. Therefore, a data-driven learning analysis could be conducted to determine if an attacker can learn QPUFs from collected data.

Acknowledgment

This work was partially supported by the Korea Institute of Energy Technology Evaluation and Planning (KETEP) grant funded by the Korea government (MOTIE) (RS-2023-00303559, Study on developing cyber-physical attack response system and security management system to maximize real-time distributed resource availability), and by project SERICS (PE00000014) under the NRRP MUR program funded by the EU - NGEU. We acknowledge the use of IBM Quantum services for this work. The views expressed are those of the authors, and do not reflect the official policy or position of IBM or the IBM Quantum team.

References

[1] M. Masdari and M. Jalali, "A survey and taxonomy of dos attacks in cloud computing," *Security and Communication Networks*, vol. 9, no. 16, pp. 3724–3751, 2016.

[2] A. Al-Meer and S. Al-Kuwari, "Physical unclonable functions (puf) for iot devices," *ACM Computing Surveys*, vol. 55, no. 14s, pp. 1–31, 2023.

[3] N. Wisiol, B. Thapaliya, K. T. Mursi, J.-P. Seifert, and Y. Zhuang, "Neural network modeling attacks on arbiter-puf-based designs," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 2719–2731, 2022.

[4] N. Wisiol, C. Mühl, N. Pirnay, P. H. Nguyen, M. Margraf, J.-P. Seifert, M. Van Dijk, and U. Rührmair, "Splitting the interpose puf: A novel modeling attack strategy," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 97–120, 2020.

[5] T. Kroeger, W. Cheng, S. Guilley, J.-L. Danger, and N. Karimi, "Cross-puf attacks on arbiter-pufs through their power side-channel," in *2020 IEEE International Test Conference (ITC)*. IEEE, 2020, pp. 1–5.

[6] S. Duan and G. Sai, "Bti aging-based physical cloning attack on sram puf and the countermeasure," *Analog Integrated Circuits and Signal Processing*, vol. 117, no. 1, pp. 45–55, 2023.

[7] P. Ravi, A. Chattopadhyay, and S. Bhasin, "Security and quantum computing: An overview," in *2022 IEEE 23rd Latin American Test Symposium (LATS)*. IEEE, 2022, pp. 1–6.

[8] S. Chowdhury, A. Covic, R. Y. Acharya, S. Dupee, F. Ganji, and D. Forte, "Physical security in the post-quantum era: A survey on side-channel analysis, random number generators, and physically unclonable functions," *Journal of Cryptographic Engineering*, pp. 1–37, 2021.

[9] S. J. Devitt, W. J. Munro, and K. Nemoto, "Quantum error correction for beginners," *Reports on Progress in Physics*, vol. 76, no. 7, p. 076001, 2013.

[10] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[11] C. Helfmeier, C. Boit, D. Nedospasov, and J.-P. Seifert, "Cloning physically unclonable functions," in *2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, 2013, pp. 1–6.

[12] H. Cook, J. Thompson, Z. Tripp, B. Hutchings, and J. Goeders, "Cloning the unclonable: Physically cloning an fpga ring-oscillator puf," in *2022 International Conference on Field-Programmable Technology (ICFPT)*, 2022, pp. 1–10.

[13] A. Chatterjee, K. Phalak, and S. Ghosh, "Quantum error correction for dummies," in *2023 IEEE International Conference on Quantum Computing and Engineering (QCE)*. Los Alamitos, CA, USA: IEEE Computer Society, sep 2023, pp. 70–81.

[14] M. Sarovar, T. Proctor, K. Rudinger, K. Young, E. Nielsen, and R. Blume-Kohout, "Detecting crosstalk errors in quantum information processors," *Quantum*, vol. 4, p. 321, Sep. 2020.

[15] K. Phalak, A. A. Saki, M. Alam, R. O. Topaloglu, and S. Ghosh, "Quantum PUF for security and trust in quantum computing," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 11, no. 2, pp. 333–342, 2021.

[16] B. Skoric, "Quantum readout of physical unclonable functions," *Cryptology ePrint Archive*, no. 2009/369, 2009.

[17] M. Arapinis, M. Delavar, M. Doosti, and E. Kashefi, "Quantum physical unclonable functions: Possibilities and impossibilities," *Quantum*, vol. 5, p. 475, 2021.

[18] H. S. Jacinto, A. M. Smith, and N. I. Rafla, "Utilizing a fully optical and reconfigurable puf as a quantum authentication mechanism," *OSA Continuum*, vol. 4, no. 2, pp. 739–747, 2021.

[19] S. A. Goorden, M. Horstmann, A. P. Mosk, B. Škorić, and P. W. Pinkse, "Quantum-secure authentication of a physical unclonable key," *Optica*, vol. 1, no. 6, pp. 421–424, 2014.

[20] B. Skoric, "Security analysis of quantum-readout pufs in the case of challenge-estimation attacks," *Quantum Information & Computation*, vol. 16, no. 1-2, pp. 50–60, 2016.

[21] Y. Yao, M. Gao, M. Li, and J. Zhang, "Quantum cloning attacks against puf-based quantum authentication systems," *Quantum Information Processing*, vol. 15, pp. 3311–3325, 2016.

[22] K. Phalak, A. Ash-Saki, M. Alam, R. O. Topaloglu, and S. Ghosh, “Quantum puf for security and trust in quantum computing,” *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 11, no. 2, pp. 333–342, 2021.

[23] N. Pirnay, A. Pappa, and J.-P. Seifert, “Learning classical readout quantum pufs based on single-qubit gates,” *Quantum Machine Intelligence*, vol. 4, no. 2, p. 14, 2022.

[24] V. K. Bathalapalli, S. P. Mohanty, C. Pan, and E. Kougianos, “Qpuf: Quantum physical unclonable functions for security-by-design of industrial internet-of-things,” in *2023 IEEE International Symposium on Smart Electronic Systems (iSES)*. IEEE, 2023, pp. 296–301.

[25] N. Kumar, R. Mezher, and E. Kashefi, “Efficient construction of quantum physical unclonable functions with unitary t-designs,” *arXiv preprint arXiv:2101.05692*, 2021.

[26] G. Gianfelici, H. Kampermann, and D. Bruß, “Theoretical framework for physical unclonable functions, including quantum readout,” *Physical Review A*, vol. 101, no. 4, p. 042337, 2020.

[27] M. Doosti, N. Kumar, M. Delavar, and E. Kashefi, “Client-server identification protocols with quantum puf,” *ACM Transactions on Quantum Computing*, vol. 2, no. 3, pp. 1–40, 2021.

[28] IBM Quantum, https://quantum.ibm.com/, 2021.

[29] Qiskit contributors, “Qiskit: An open-source framework for quantum computing,” 2023.

[30] Franco Cirillo, https://github.com/francocirill/QPUF, 2024.