A QPUF-Based Scheme for Secure and Adaptable Quantum Device Attestation in NISQ Devices

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

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

***Abstract*—The rapid advancement of quantum computing has introduced a critical need for secure quantum device attestation to ensure that devices involved in computations are authentic.**

Existing solutions for quantum device attestation often rely on quantum memory or lack adaptability across diverse quantum computing platforms. To address these limitations, we propose a novel Quantum Physical Unclonable Function (QPUF)-based device attestation scheme that leverages the inherent noise of Noisy Intermediate-Scale Quantum (NISQ). Unlike existing methods, our approach eliminates the need for quantum memory and is compatible with various quantum hardware technologies.

The proposed method uses a custom quantum circuit as a QPUF, combined with a challenge-response-based protocol, to establish secure and efficient quantum device attestation. We evaluated our approach on IBM quantum hardware, analyzing key metrics such as instability, randomness, and uniqueness of the QPUFs. Experimental results validate the feasibility of the proposed method and demonstrate its practical advantages for real-world quantum service provision.

***Index Terms*—Quantum Physical Unclonable Function (QPUF), Device attestation, Quantum device fingerprint.**

I. Introduction

The rise of quantum computing marks a new technological frontier with profound implications for computation and data security. However, as quantum computing systems evolve, the need for reliable and secure device attestation mechanisms has become a critical concern. Attestation ensures that quantum devices participating in computations or data exchanges are genuine, uncompromised, and authorized [1]. This is particularly important in scenarios where clients request computational tasks to quantum service providers, as they must be assured that the device executing their requested computations matches the one specified or agreed upon. Without robust attestation mechanisms, a quantum service provider could potentially substitute the requested high-performance quantum device with a cheaper, less capable system.

Despite advancements in device security, quantum device attestation faces unique challenges that extend beyond classical paradigms. Unlike classical systems, quantum computers are characterized by their underlying physical implementations, which vary significantly across providers and platforms. This diversity in hardware architecture accentuates the difficulty of developing a universal attestation mechanism capable of reliably verifying devices from heterogeneous providers. Traditional attestation methods face significant limitations in the quantum domain due to their reliance on securely storing cryptographic keys or certificates.

In this context, Quantum Physical Unclonable Functions (QPUFs) [2] offer a promising solution for quantum device attestation by exploiting the inherent errors and imperfections of NISQ devices [3]. These quantum errors and imperfections are harnessed to generate unique and unpredictable responses tied to the specific characteristics of the quantum hardware. Using the Challenge-Response paradigm, a challenge is presented to the quantum device, and the device generates a response based on its unique quantum errors. This response can then be used to authenticate the device [4] and verify its integrity within a secure system.

The key contributions of our work are as follows:

1) We design a quantum circuit that functions as a QPUF, capable of extracting the unique characteristics of a quantum device. The circuit is evaluated on real IBM hardware based on critical metrics such as uniqueness, instability, and randomness to demonstrate its effectiveness in generating robust challenge-response pairs.
2) We develop an attestation scheme based on the QPUF's challenge-response paradigm and the use of an attestation service. This scheme leverages the unique properties of quantum devices to perform secure attestation, not needing any quantum memory.
3) We discuss about parameter optimization and security consideration to enhance the reliability of the method.

II. Background

QPUFs rely on inherently quantum properties, such as superposition and entanglement, to generate unique and unpredictable responses to challenges, ensuring that QPUFs are fundamentally unclonable and highly resistant to tampering.

The operation of QPUFs parallels that of classical PUFs, with two main phases:

1) Enrollment Phase: quantum states of the physical system are manipulated to encode the unique characteristics of the QPUF. The quantum states are measured to generate CRPs, which are securely stored.
2) Verification Phase: a challenge is applied to the QPUF, and its quantum states are manipulated to produce a response. This response is measured using quantum processes that inherently introduce unpredictability. The

resulting response is then compared against the stored CRPs. If a match is found within an acceptable margin of error, authentication is successful.

A defining feature of QPUFs is their reliance on the quantum no-cloning theorem, which states that arbitrary quantum states cannot be perfectly duplicated without altering the original ones. This principle ensures the intrinsic unclonability of QPUFs, offering high entropy and robust resistance to cloning attacks. As advancements in quantum computing threaten classical cryptographic schemes, QPUFs provide a future-proof solution for secure authentication and encryption.

Despite their promise, QPUFs present significant challenges, due to the need for precise control of quantum states. Quantum systems are prone to various errors [5], such as gate errors, which arise from calibration imperfections leading to inaccuracies in logical operations; decoherence and dephasing, where environmental interactions cause loss of quantum state fidelity; readout errors, resulting in bit-flip inaccuracies during measurement; single-qubit and two-qubit errors, affecting gates like Hadamard and CNOT; and crosstalk, where interference between parallel gate operations degrades performance. These error rates, which vary across qubits and hardware, can serve as unique hardware identifiers. However, their practical deployment in real-world applications will require continued research and technological improvements.

III. Related work

The concept of QPUFs for identification protocols was first introduced in [6] with the Quantum Read-Out of PUF mechanism and in [7] with QPUF, addressing only the theory.

To address security and trust in quantum systems, the work in [8] proposes two QPUF variants, but [9] later revealed vulnerabilities in this QPUF construction through a successful machine learning attack, showing that the fixed circuit structure and lack of qubit entanglement made it feasible to predict QPUF responses, raising concerns about its security. The work in [10] evaluates only single-qubit operations, remaining vulnerable to the same machine learning attacks identified. In another approach, [11] describes the construction of QPUFs using approximate unitary transformations, but lacks of a defined attestation mechanism.

The work in [12] introduces a method that leverages quantum crosstalk. However, its effectiveness as a reliable feature for PUFs remains uncertain, as noted in [13]. The study in [14] demonstrates that qubit frequency is unique to each device, making it suitable for creating QC fingerprints. However, this method lacks the parametrizability needed to generate multiple challenges. Similar challenges are discussed in [15], where the robustness of fingerprinting against frequency manipulation is questioned. Other methods, proposed in [16], [17], rely on quantum memory and secure quantum channels, utilizing protocols like BB84, increasing the complexity. The final response string generated by the circuit proposed in [18] does not capture the differences between quantum computers, limiting its utility for fingerprinting. Fingerprinting methods in [19], [20] use static device characteristics, but a dishonest provider could detect probing circuits and spoof results, undermining reliability. To overcome all these challenges, we propose a generic QPUF that eliminates reliance on quantum memory and channels, ensuring compatibility with real quantum devices. Additionally, we introduce a practical attestation scheme to enhance security and usability.

IV. QPUF implementation and evaluation

To leverage the unique characteristics of each quantum device for device attestation, we proposed a QPUF circuit and presented an analysis of the empirical findings by evaluating the QPUF quality, followed by an interpretation of the results.

A. QPUF circuit

The proposed QPUF circuit exploits the natural bias of qubits towards the $|0\rangle$ or $|1\rangle$ state to generate a response. This bias arises from imperfections such as single gate errors, including those in X-Y-Z rotation gates, multiple qubit errors, such as gate used for the entanglement, and readout errors.

Initially the circuit doesn't explicitly reset the state to the $|0\rangle$ state, with the aim of exploiting the associated noise of each qubit. Each qubit then undergoes sequential rotations along the X, Y, and Z planes using rotation gates, with angles parameterized within the range $[0, 2\pi]$. Following this, each qubit is entangled with its neighboring qubits using Controlled-Z (CZ) gates. These two steps are repeated once more to ensure full entanglement across the qubit array and an other X rotation is applied to every qubits, to exploit the entanglement. Finally, all qubits are measured. In an ideal scenario, the qubits would exhibit a uniform probability distribution over the $|0\rangle$ and $|1\rangle$ states, dictated by the rotation gate parameters. However, due to imperfections, the actual probability distribution of each qubit is expected to exhibit a bias towards either the $|0\rangle$ or $|1\rangle$ state. This bias acts as a unique signature of the quantum device. Figure 1 illustrates an instance of the proposed QPUF

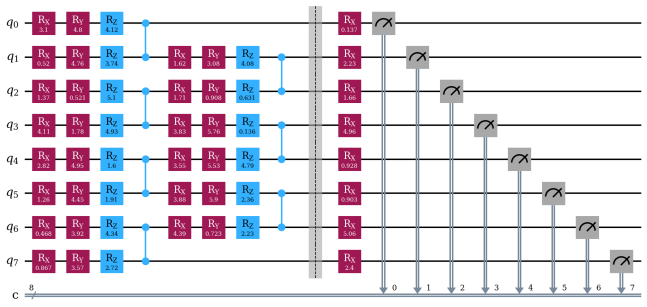


Fig. 1: QPUF circuit proposed with 8-qubit and based on X-Y-Z rotation gates and Controlled-Z gate.

circuit, built with 8 qubits and gates parametrized by random angles. Within the framework of this QPUF circuit, challenges are represented as vectors comprising all gate parameters in a given instance of the circuit. For example, in the 8-qubit circuit depicted in Figure 2, a challenge is defined by 50 angles, with each angle taking a value in the range $[0, 2\pi]$. The response

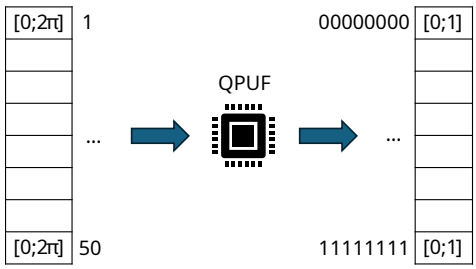


Fig. 2: QPUF mapping of challenge-response.

is represented as a dictionary where each possible qubit state combination is assigned a probability value between 0 and 1, with all probabilities in a single response summing to 1.

B. QPUF metrics

The following metrics have been evaluated:

Instability: This metric captures the variations and unpredictability in the QPUF responses of a single device. To quantify Instability, QPUF responses can be compared using the Normalized Absolute Probabilistic Distance (NAPD) metric for each pair of responses. Let $r^k_{n,q}$ represent the q-th combination of qubit results from the n-th challenge on the k-th device, where $Q = 2^{\text{nqubits}}$. The NAPD between the responses of the n-th challenge on the k-th device and the m-th challenge on the h-th device is defined as:

$$\text{NAPD}\left(r^k_n, r^h_m\right) = \frac{1}{2}\sum_{q=1}^{Q} |r^k_{n,q} - r^h_{m,q}| \tag{1}$$

Here, the normalization factor of $1/2$ ensures that the NAPD ranges from 0 (identical responses) to 1 (completely opposite responses). This adjustment accounts for the absolute differences in probabilities, which individually sum to 1.

Let $r^k_{n,i}$ denote the response corresponding to the i-th out of D executions of the n-th challenge on the k-th device. The Instability of the k-th device can then be estimated as:

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

For each challenge and each distinct pair of executions of the same challenge, the NAPD is computed. This is averaged over all pairs, determined by the binomial coefficient $\binom{D}{2}$, and normalized by the number of challenges N.

Ideally, the Instability of QPUFs should approach zero, reflecting consistent and reliable responses over repeated trials.

Randomness: This metric evaluates the stochastic nature of the responses, ensuring that they are highly distinct across challenges, even when the challenges are similar. Let r^k_n denote the response of the n-th challenge on the k-th device. The Randomness of the k-th device is estimated as:

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

The NAPD is calculated for every distinct pair of challenges, and the result is averaged over all pairs, given by $\binom{N}{2}$.

Ideal Randomness values are as close to 1 as possible, indicating maximally distinct responses across challenges.

Uniqueness: This metric measures the distinctiveness of the responses generated by different devices when presented with the same challenge. Let r^k_n represent the response of the n-th challenge on the k-th device. The Uniqueness is estimated as:

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

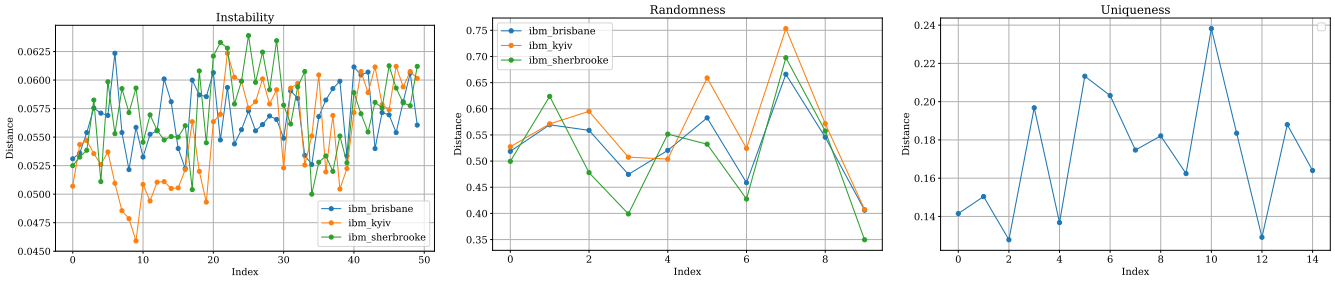
For each distinct pair of devices and for each challenge, the NAPD is computed. The result is averaged over all device pairs, determined by $\binom{K}{2}$, and normalized by the number of challenges N. High Uniqueness values indicate greater differentiation between device responses. However, extremely high values, approaching 1, may suggest unreliable device computations, as the responses would be excessively divergent.

C. Experimental results

In the experiments conducted to evaluate the quality of QPUFs, real quantum hardware provided by IBM was utilized, specifically the devices `ibm_brisbane`, `ibm_kyiv`, and `ibm_sherbrooke`. The QPUF circuit described earlier was implemented with 8 qubits, and each circuit execution involved 20,000 measurement shots. For Instability testing, a set of 5 challenges ($N = 5$) and 5 executions per challenge ($D = 5$) were used. Figure 3a shows the distribution of Instability for the three tested devices, where index means the i-th iteration among $5 * \binom{5}{2}$ iterations. From the graphs, it can be observed that Instability values across all three devices hover around 5%, with a maximum value not exceeding 7%. Additionally, increasing the number of measurement shots or executions leads to a reduction in Instability. This indicates that, without constraints on the usage of quantum hardware, the results can be further improved. For Randomness testing, the number of challenges was set to $N = 5$. Figure 3b illustrates the distribution of Randomness for the three devices among $\binom{5}{2}$ iterations. The graphs indicate that Randomness values for all three devices fall within the range of 35–75%, with an average of approximately 55%. For Uniqueness testing, the number of challenges was set to $N = 5$, and the number of devices was $K = 3$. Figure 3c shows the distribution of Uniqueness across the three tested devices for $3 * 5$ iterations. From the graphs, it can be observed that the Uniqueness values range between 15–25%, not going below 12%.

D. Interpretation and discussion of the results

To interpret the obtained results, it is essential to note that the derived Instability values represent an upper bound, as continuous improvement was observed with an increased number of quantum circuit executions. The results aimed at achieving acceptable performance, rather than optimizing for the best possible outcomes, primarily due to limitations in the use of the quantum computing service. Additionally, achieving



(a) Distribution QPUF Instability over 5 challenges, and 5 executions per challenge.

(b) Distribution QPUF Randomness over 5 challenges.

(c) Distribution of QPUF Uniqueness over 5 challenges, and 3 devices.

Fig. 3: Distributions of 8-qubit QPUF properties over 20,000 shots: (a) Instability, (b) Randomness, and (c) Uniqueness.

an ideal value of 1 for Randomness and Uniqueness presents a significant challenge, because this requires that the compared responses should be completely different, but It cannot happen because the circuit and the challenges are the same.

Overall, the metric graphs indicate low Instability and good Randomness for the proposed QPUF. Although the calculated Uniqueness values are satisfactory, as they do not overlap with the Instability values, the Uniqueness of devices utilizing the QPUF can be made more reliable by using multiple challenges and employing the device attestation scheme proposed.

V. Quantum Device Attestation Scheme

The proposed framework introduces a novel method for quantum device attestation using QPUFs to verify the authenticity of quantum hardware. Quantum PUFs act as unique, hardware-based cryptographic fingerprints, ensuring the device's identity is unforgeable. The framework involves three main actors: the Quantum Provider (supplies quantum computing services), the Client (uses the services), and the Attestation Service (manages device registration, monitoring, and attestation). It operates in two phases: Enrollment and Attestation.

A. Enrollment Phase

During the Enrollment phase, in Figure 4, the Quantum Provider initiates a request to the Attestation Service to register a specific quantum device by sending its identifier. The Attestation Service generates a series of N random challenges to test the device's unique Quantum PUF. The Provider executes the required circuits with these challenges and returns the corresponding responses, which are saved as CRPs. To prevent the Provider from caching or precomputing responses, the Attestation Service introduces randomness in the timing of these requests, spreading them over unpredictable intervals. This ensures the Provider cannot identify enrollment-related requests or store a large set of precomputed responses, making the process secure and infeasible to manipulate. The unique Quantum PUF responses are securely stored for future verification in the Attestation phase.

B. Attestation Phase

In the Attestation Phase, the goal is to verify that the requested quantum computations are being executed on the authentic quantum device, enrolled with the Attestation Service. The process begins when the Client requests attestation for a specific quantum device, sending the identifier of the quantum computer. The Attestation Service responds by selecting n random challenges not already used for previous attestations. The Client then sends these challenges to the Quantum Provider, which executes them on the claimed quantum device and returns the corresponding n responses. The Client forwards these responses, along with the original challenges and the identifier of the quantum computer, to the Attestation Service. The Attestation Service compares the received responses to the baseline responses generated during the enrollment phase. It calculates the average distance between the observed responses and the expected responses stored during enrollment. If this average distance is below a predefined threshold, λ, the attestation is deemed successful, confirming that the computations were executed on the authentic quantum device.

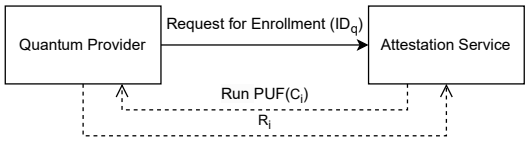


Fig. 4: Enrollment phase initiated by Quantum Provider to enroll its quantum computers.

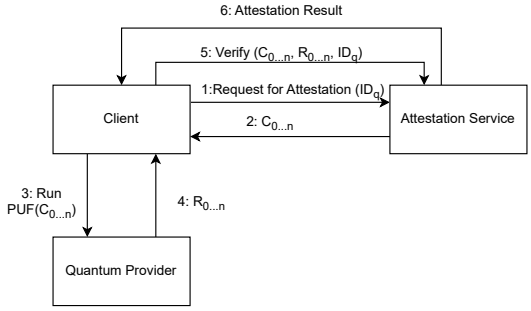


Fig. 5: Attestation phase requested by the Client to verify the authenticity of the quantum computers claimed.

C. Security Considerations

As evidenced by the results, the Uniqueness values are clearly distinct from their corresponding Instability values for each device. This indicates that, for the same challenge, the NAPD between two responses from the same device is consistently lower than that observed between responses from different devices. Nevertheless, a larger n helps mitigate the influence of potential outliers, thereby enhancing the overall robustness of the system. The concept of the threshold λ warrants clarification. This parameter should be determined through an analysis of Instability and Uniqueness, with the goal of minimizing false positives and false negatives. The method involves maximizing the separation between the Instability and Uniqueness values to define λ. In this study, experimental results indicate that λ is set to 0.09, as the maximum Instability value is 0.07, and the minimum Uniqueness value is 0.12. This threshold means that two devices are considered identical only if their average NAPD across all tested challenges does not exceed 0.09. Additionally, the value of λ can be further refined by performing a more detailed Instability analysis, which could involve increasing the number of measurement shots for each circuit execution. The schema ensures security by preventing the Quantum Provider from substituting stored responses for requested challenges during the attestation phase. The randomization of the challenge execution during enrollment makes it infeasible for the Provider to accurately precompute or cache results. Additionally, the reliance on Quantum PUFs adds an extra layer of security, as the quantum-specific hardware responses are inherently tied to the physical properties of the device and are practically impossible to clone or forge. This framework not only guarantees that the requested quantum computations are performed on the intended device but also mitigates the risk of service degradation or fraud by the Provider.

VI. Conclusion

This study introduces a QPUF-based approach for quantum device attestation, eliminating the need for quantum memory and ensuring adaptability across different quantum technologies. A specialized quantum circuit functions as a QPUF, supporting a challenge-response attestation scheme for secure service provision. Experiments on IBM's quantum hardware assessed instability, randomness, and uniqueness, validating the method's feasibility. However, due to resource limitations, tests were restricted to three devices, highlighting the need for future research across multiple quantum platforms to evaluate scalability and robustness.

Acknowledgment

This research was funded by the NGIsargasso project (Europe Horizon Grant No. 101092887), Open Call 4 FRQ-GAN4AD project. 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] O. Arias, F. Rahman, M. Tehranipoor, and Y. Jin, "Device attestation: Past, present, and future," in *2018 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2018, pp. 473–478.

[2] 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.

[3] 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.

[4] F. Cirillo and C. Esposito, "Practical evaluation of a quantum physical unclonable function and design of an authentication scheme," in *2024 IEEE International Conference on Quantum Computing and Engineering (QCE)*, vol. 01, 2024, pp. 1354–1363.

[5] 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.

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

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

[8] 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.

[9] 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.

[10] 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.

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

[12] A. Mi, S. Deng, and J. Szefer, "Short paper: Device-and locality-specific fingerprinting of shared nisq quantum computers," in *Proceedings of the 10th International Workshop on Hardware and Architectural Support for Security and Privacy*, 2021, pp. 1–6.

[13] C. Z. Chwa, L. A. Hsia, and L. D. Merkle, "Quantum crosstalk as a physically unclonable characteristic for quantum hardware verification," in *NAECON 2023-IEEE National Aerospace and Electronics Conference*. IEEE, 2023, pp. 309–313.

[14] K. N. Smith, J. Viszlai, L. M. Seifert, J. M. Baker, J. Szefer, and F. T. Chong, "Fast fingerprinting of cloud-based nisq quantum computers," in *2023 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 2023, pp. 1–12.

[15] K. N. Smith and P. Gokhale, "Trustworthy Quantum Computation through Quantum Physical Unclonable Functions," Nov. 2023, arXiv:2311.07094 [quant-ph]. [Online]. Available: http://arxiv.org/abs/2311.07094

[16] M. A. Khan, M. N. Aman, and B. Sikdar, "Soteria: A Quantum-Based Device Attestation Technique for the Internet of Things," *IEEE Internet of Things Journal*, pp. 1–1, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/10373567/

[17] J. Laeuchli and R. Trujillo-Rasua, "Software-based remote memory attestation using quantum entanglement," *Quantum Information Processing*, vol. 23, no. 6, p. 208, 2024.

[18] V. K. V. V. Bathalapalli, S. P. Mohanty, C. Pan, and E. Kougianos, "QPUF 2.0: Exploring Quantum Physical Unclonable Functions for Security-by-Design of Energy Cyber-Physical Systems," Oct. 2024, arXiv:2410.12702. [Online]. Available: http://arxiv.org/abs/2410.12702

[19] J. Wu, T. Hu, and Q. Li, "Detecting Fraudulent Services on Quantum Cloud Platforms via Dynamic Fingerprinting," Aug. 2024, arXiv:2408.11203. [Online]. Available: http://arxiv.org/abs/2408.11203

[20] ——, "Q-id: Lightweight quantum network server identification through fingerprinting," *IEEE Network*, 2024.