QPUF 2.0: Exploring Quantum Physical Unclonable Functions for Security-by-Design of Energy Cyber-Physical Systems

Venkata K. V. V. Bathalapalli
Dept. of Computer Science and Engineering
University of North Texas.
Email: vb0194@unt.edu

Saraju P. Mohanty
Dept. of Computer Science and Engineering
University of North Texas.
Email: saraju.mohanty@unt.edu

Chenyun Pan
Dept. of Electrical Engineering
University of Texas at Arlington.
Email: chenyun.pan@uta.edu

Elias Kougianos
Dept. of Electrical Engineering
University of North Texas.
Email: elias.kougianos@unt.edu

***Abstract*—The Smart Grid concept evolved from the idea of intelligent and secure management of electrical grid infrastructure components and their communication through sustainable integration with the state-of-the-art technologies. This research focuses on emerging quantum computing-assisted security and its application in the Smart Grid. The robustness of electrical grid is increasing every day through advancements in grid infrastructure management which include outage control, relay protection, reliable distribution, renewable energy resource integration, and energy trading. Quantum Computing emerges as a formidable solution for application in the smart grid due to its processing capability and scale. Its application and scope are evolving every day with the recent developments in Quantum Chips which could pave the way for emerging Quantum-Chain-of-Things (QCoT). This research focuses on providing robust security in smart grids through Quantum Physical Unclonable Functions (QPUF) primitive, a quantum-hardware assisted security approach driven by micro manufacturing quantum process variations for generating a quantum digital fingerprint driven by quantum mechanics principles. The QPUF experimental evaluation in this research was performed to uniquely fingerprint various electrical grid entities providing a sustainable and secure flow of communication. Experimental evaluation shows a robust and reliable extraction of quantum digital fingerprints from noisy IBM quantum systems. The evaluation shows an impressive 86% keys achieving 100% reliability.**

***Index Terms*—Cyber-Physical Systems (CPS); Smart Grid; Cybersecurity; System Security; Security-by-Design (SbD); Physical Unclonable Functions (PUF); Quantum Physical Unclonable Functions (QPUF)**

I. Introduction

Substantial improvement is being made to improve the efficiency in generation, transmission, and distribution of renewable energy resources and their management ensuring reliable operation of the smart grid. Supervisory control and data acquisition (SCADA) provides intelligent control and management of electrical grid infrastructure entities and their communication by supporting real-time data sensing, actuation, and processing capabilities [1]. The adoption of SCADA-based intelligent grid management systems poses security threats at various levels of electrical grid operational and distributional frameworks due to the heterogeneity of various smart sensors, actuators, and the modernized grid infrastructure with diverse network communication protocols. These cyber threats affect grid operational framework through trojans, snooping, and various other attacks which could jeopardize the reliability of electrical grid operations. This research focuses on ensuring the reliability of grid communication and operational entities supported by Quantum Computing through quantum hardware-assisted security primitive QPUF. Quantum Computing and its potential make it a suitable player for addressing increasing electrical grid operational and communication data processing and security issues with its exponential capability in information processing and communication. This work presents QPUF as a solution for ensuring grid reliability as it harnesses the inherent randomness of quantum hardware to uniquely generate a cryptographic key for attesting various entities in grid distribution and operational framework [2], [3]. The conceptual idea of proposed QPUF 2.0 is depicted in Fig. 1.

Quantum Security-by-Design (QSbD) focuses on the security for emerging Artificial Intelligence, Blockchain, and Machine Learning based quantum applications using the principles of quantum mechanics. Physical Unclonable Functions (PUF) facilitate security at the hardware level by mapping inherent properties of devices to a unique binary bitstream as a hardware driven digital fingerprint. The properties and characteristics of each hardware are unique due to inherent micro-manufacturing variations at various stages. Exploring PUF on quantum hardware has been an emerging research area due to its potential and scope in Quantum hardware which have underlying architecture built based on silicon. Quantum systems are

built based on superconducting circuits can support QPUF for security applications. Even though the quantum systems are noisy, the emerging trend of noiseless quantum systems validates the potential for QPUF-based security and its application [4]. Specifically, the deployment of quantum logic gates-based QPUF topologies on varying quantum hardware architectures facilitates the generation of quantum bitstrings

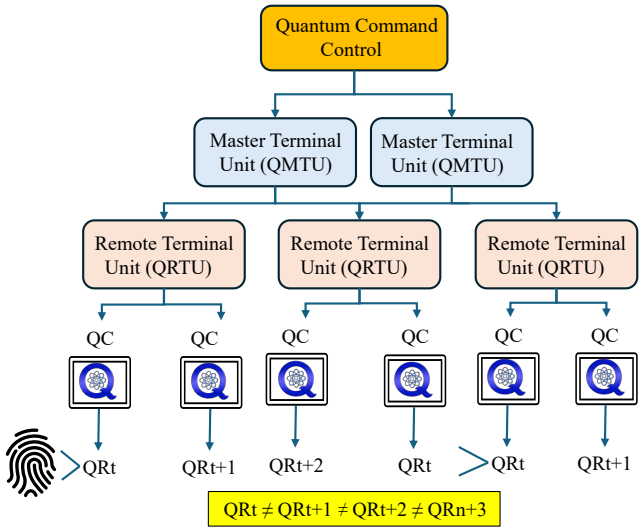


Fig. 1: QPUF 2.0 Framework for Secure Smart Grid

systems operate and control various smart grid domains ranging from distribution to electric utility data management, grid equipment monitoring, relay for protection, transmission and generation subsystems. SCADA enables smart control of the electricity and communication flow from transmission systems to customers with high reliability. These systems monitor the electricity generation, transmission, and distribution processes at various levels and have smart devices to monitor and regulate the electricity flow. To enable the security of various components deployed for applications in the smart grid, this research work focuses on a novel concept of QSbD which defines designing electrical subsystems infrastructure with QPUF based security as a default feature enhancing reliability of the grid operations. The underlying tamper proof QPUF built on quantum systems can protect the smart quantum electronic devices at the grid thereby ensuring security at various levels of electrical distribution framework and secures SCADA enabled grid access control and management.

The rest of this paper is organized as follows. Section II discusses related research on Quantum SbD and smart grid cybersecurity. Novel contributions of the proposed work are presented in section III. The architectural overview of the proposed QPUF 2.0 is discussed in section IV. QPUF Experimental validation results are presented in section V and finally, the conclusion and future research directions are discussed in Section VI.

II. Related Work

This section gives a comprehensive overview of state-of-the-art research on Quantum PUF and smart grid cybersecurity. Also, a comprehensive review of QPUF and smart grid SbD solutions is presented in Tables I.

A quantum hardware attestation approach using QPUF that uses qubit cross talk as a characteristic which is unique for each hardware is proposed in [5]. Their work was evaluated using superconducting transmon qubits from IBM. Their experimental evaluation include a simple Hadamard gate realization using microwave pulse on entangled control qubit to realize its impact on the target qubit. QPUF topologies based on quantum superposition and decoherence phenomena are presented in [6]. Their QPUF evaluation include evaluating the impact of decoherence driven by idle gates and the impact of Hadamard gate driven superposition for QPUF. In comparison, to the above cited work, a novel approach for reliable QPUF extraction using Hadamard gate based topology proposed in [6] is presented in [7] which is a robust QPUF response bit string extraction approach from various quantum hardware from IBM.

A Quantum Readout (QR) PUF was proposed in [8] which is based on classical PUF in silicon chips. The PUF topology is evaluated with challenges response pairs (CRP) in quantum states. The QR PUF is claimed to be more effective than a classical PUF as it is driven by the no-cloning principle which states that it is impossible to duplicate or clone the unknown arbitrary quantum state of a qubit. A simple PUF-based key exchange protocol based on the quantum physical unclonability principle was presented in [9] which proposes a PUF-based quantum BB84 key exchange protocol with CRP being converted to qubits. A QPUF multi-factor authentication algorithm based on the principle of no-cloning theorem was proposed in [10]. This work also includes an enrollment authentication mechanism through QPUF using QTOKSim, a quantum token-based authentication simulator.

A novel Quantum tunneling PUF titled Neo PUF has been proposed in [11] which works by storing the PUF signature inside ultra-thin oxide. This PUF works based on manufacturing variations in oxide. For QSbD in smart grid, a smart grid communication framework through Quantum key distribution (BB84) is proposed in [12] to counter man-in-the-middle-attacks. [13] presents a secure device attestation framework for Internet-of-Things (IoT) devices. Their work is based on QPUF driven by the principles of quantum mechanics and the QKD.

III. Novel Contributions

The novel features of the proposed QPUF 2.0 are summarized below:

- A quantum-hardware centric QSbD approach for secure attestation of SCADA-driven electrical distribution framework entities.
- A state-of-the-art Quantum Security-by-Design (QSbD) solution providing security as a default feature or primitive for SCADA-Smart Grid framework.

TABLE I: Related Research on Quantum PUF

Work	Evaluation Systems	Architecture	QPUF Parameters	Evaluation Metrics
Chwa, et al. (2023) [5]	IBM Falcon r5.10 and r5.11 27, ibm cairo, ibm hanoi, ibmq mumbai, and ibmq kolkata	Hadamard	Quantum Crosstalk	NA
Phalak, et al. (2021) [6]	ibmq_essex and ibmq_london	H, Ry, Measurement, and I	Superposition and Decoherence	intra-HD ibmq_essex (13.82%) and ibmq_london(3.94%)
Khan, et al. (2023) [13]	5-qubit processors	Ry and Rx gates	Entanglement	1 state probability- q[0]-76%, q[1]-87%
Bathalapalli, et al. (2023) [7]	ibmq_belem, ibmq_lima, and ibmq_quito	Hadamard, Ry	Superposition	40% Intra-HD ibmq_lima, 25% Uniqueness s
QPUF 2.0 (Current Paper)	ibm_osaka, ibm_kyoto, and ibm_sherbrooke	H, Ry, CNOT, and I-gate	Quantum Entanglement, Decoherence, and superposition	50% HD, 51% Randomness

- A QPUF-based attestation approach for IEDs, protective relays, and smart equipment monitoring devices in SCADA.
- A QPUF topology driven by the quantum mechanics principles of Decoherence, Entanglement, and Superposition.
- A reliable QPUF calibration and evaluation on noisy quantum computers from IBM
- A secure QPUF random bitstream generation approach based on unique initialization parameters as challenges and supports higher QPUF-based cryptographic keys or responses generation.
- A simple QPUF driven device attestation framework for Remote Terminal Units (RTUs), Mater Terminal Units (MTU's), and Phasor Measurement Units (PMUs) in SCADA-grid systems.

IV. Proposed QPUF Methodology

The proposed architecture is an 8-qubit topology evaluated with various single and two-qubit logic gates. The ry gate is a tunable rotational angle gate that is applied to induce variations in the quantum states of qubits. This gate can induce variations and reduce quantum state predictability. The ry gate is applied to all the 8 qubits in the proposed architecture followed by H-gate, a single-qubit gate that is applied on qubits to place them in a super positioned state. Finally, CNOT gate, a two-qubit logic gate is applied on qubits to entangle their quantum states in such a way that the quantum state changes of one qubit affects the other qubit. In the proposed architecture, the first four qubits are entangled with the last four in such a way that the first four qubits are control qubits that drive the quantum state changes of the last four which are target qubits. Finally, I-gate is applied on control qubits which ideally works on retaining the quantum state for a fixed time but in physical evaluation on qubits introduces decoherence propelling it to lose its quantum state due to environmental interactions. The main motivation of the proposed QPUF topology is to explore the decohering nature of control qubits on the target qubits. Finally, the measurement gate is applied to all the qubits to read the quantum states which are stored in classical registers corresponding to the qubits in circuit. Finally obtained bitstream of random 1s and 0s are considered as QPUF response. The architecture of proposed QPUF design is shown in Fig. 2

The current evaluation of QPUF was performed on IBM's superconducting quantum systems with a unique API token to access and run quantum algorithms on quantum machines. The proposed QPUF topology was evaluated on IBM quantum systems where a circuit is run based on an initialization parameter (challenge). Each job is run for a specified number of times or shots before generating the result. The IBM's quantum system access and QPUF evaluation steps are outlined in the Algorithm. 1.

In the proposed SCADA-Smart grid security framework, all the Remote Terminal Units(RTUs), Mater Terminal Units(MTUs), and control centers have access to quantum computers and are considered quantum edge devices or gateways. All smart electronic electronics, including Intelligent Electronic Devices (IED) and relays, are controlled by Quantum RTUs (QRTUs). Furthermore, on top of QRTUs, QMTUs, and quantum control centers perform information processing, decision making, analysis, and work in a master-slave relationship.

The control center is the centralized quantum command computer with an effective human-machine interface and decision-making capability. In the proposed framework, QRTUs act as edge gateways for IEDs to relay the data, establish communication, process data, and obtain QPUF-generated responses through QRTUs for security. A group of IEDs at a particular geographical location can be securely accessed by a QRTU at the specific substation level for attestation and communication. IEDs can be securely accessed and controlled by all the QRTUs in the generation, transmission, and distribution subsystems of the SCADA controlled electrical distribution framework. QMTUs can also authenticate QRTUs and perform sensing and actuation processes for grid protection and equipment management. Quantum Key Distribution (QKD) can be deployed to ensure sustainable and intelligent communication, and attestation of QPUF entities in SCADA-Grid systems. The proposed QPUF enabled secure grid infrastructure is further explained holistically in our archived

article [2].

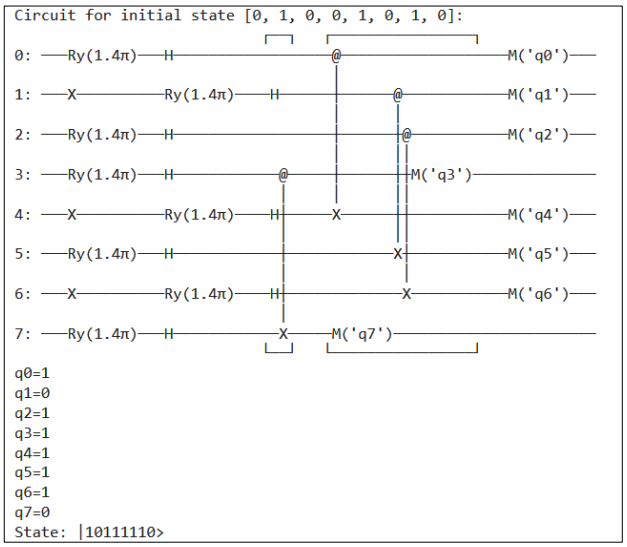


Fig. 2: QPUF Architecture based on Quantum Logic Gates

Algorithm 1 QPUF Evaluation Steps

Input: IBM Quantum API Token
Output: QPUF Design

1: Access IBM Quantum Learning
2: Obtain IBM Quantum API Token
User → API Token
3: Access Qiskit Lab
4: Choose a random Qubit Initialization
q0-1→Apply X-Gate, q1-0,... q2-1→X-gate
5: QPUF Circuit Gates → Hadamard, Pauli-X, Pauli-Y, CNOT, Measurement Gates
6: Choose Ry gate for all qubits–angle 0–2pi
Job 1–pi/4, Job 2–pi/6, job 3-pi/7..
7: Apply Hadamard Gate to all qubits
8: Entangle Qubits as follows:
qo–q4, q1–q5, q2–q6, q3–q7
9: Apply I-gate to Control qubits
10: Choose Quantum Systems or Simulators
IBM Quantum System → 127 Qubits→Eagle R3 architecture
- ibm_kyoto, ibm_osaka, ibm_sherbrooke, ibm_kyoto
- Simulator →ibmq_qasm_simulator

11: Execute the Circuit on the chosen backend and monitor the status of the job
12: Obtain the result

V. Experimental Results

Experimental evaluation of proposed QPUF was performed on IBM quantum systems. IBM quantum resources are accessible through 'Qiskit' [14], a python-based programming framework to access and deploy quantum algorithms and circuits on IBM quantum systems. The open plan of IBM supports 10 minutes of qiskit runtime with access to limited number of quantum hardware. For the evaluation on simulator, 'ibmq_qasm_simulator' was chosen and for hardware evaluation, "ibm_osaka" 'ibm_kyoto' and "ibm_sherbrooke" with Eagle R3 processor supporting 127-qubits are chosen. Eagle R3 is an advanced processor from IBM supporting more than 100 qubits with improved qubit coherence and gate fidelities. The Eagle R3 architecture has improved wiring for quantum state readout, signal routing thereby reducing cross talk and decoherence. The proposed QPUF topology is an 8-qubit architecture with 8 quantum and classical registers respectively. The architecture consists of single and two-qubit quantum logical gates which include Hadamard, Ry, CNOT, and Idle gates. Overall, the circuit is evaluated for 100 jobs on the simulator with each job undergoing 2048 measurements and obtaining 2048 outputs. For each job execution, a unique Ry gate angle is chosen in the range of 0-2pi to uniquely place a qubit in an unknown quantum state. For initialization, all the qubits are randomly initialized as either 0 or 1. These qubits initializations and tunable rotation angles act as unique initialization parameters or challenges for the circuit that produces a random string of zeros and ones which stored in the classical registers as response after applying the measurement gates and performing quantum state readout measurement as shown in Fig. 3. 100% reliability is achieved for QPUF on qasm simulator at tunable rotation angle of 90 degrees.

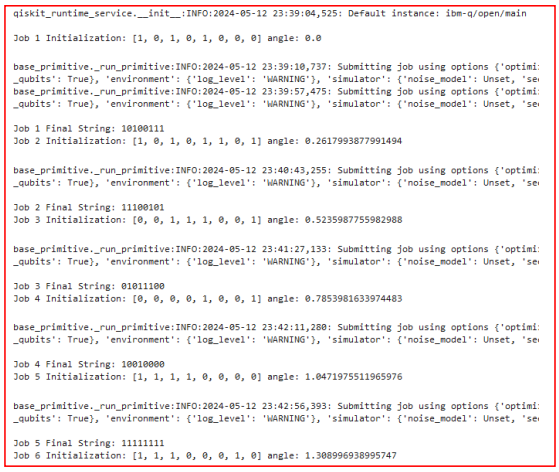
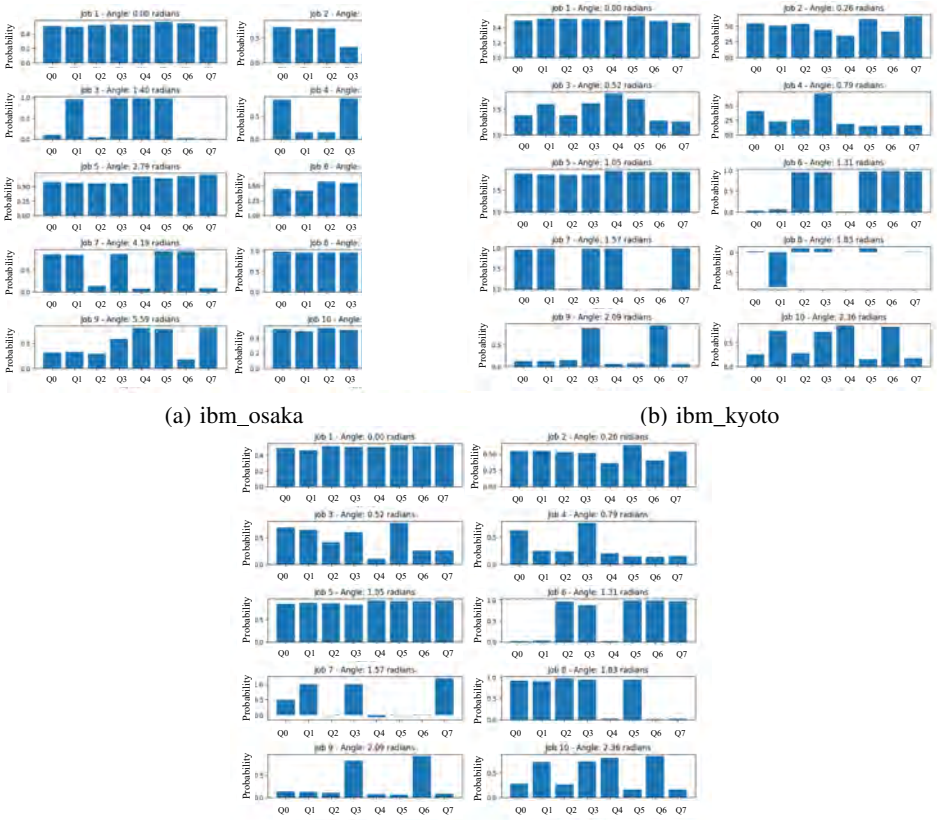


Fig. 3: Executing QPUF circuit on IBM quantum system and extracting QPUF responses

The QPUF metrics evaluated on the obtained job execution outcomes are defined and presented below:
Randomness of a PUF response is a measure of the balance in the occurrence of ones and zeros. For QPUF response, balance in the count of number of zeros and ones indicates a very unpredictable and stable QPUF response.
Diffuseness of a QPUF is the extent of variation in responses to changing initialization parameters indicating a minute fluctuation in challenge prompting a change in the obtained response or measurement string.
The reliability of QPUF is the evaluation of QPUF circuit stability to varying environmental and noise conditions by regenerating the same response for a challenge or initialization



(a) ibm_osaka (b) ibm_kyoto

(c) ibm_sherbrooke

Fig. 4: Qubit's State Probabilities for the QPUF Circuit from Various Quantum Systems

input respectively under varying conditions.

The uniqueness of a QPUF is the degree of variation of QPUF responses based on varying quantum hardware architectures, qubit mapping, coherence times and gate fidelities which are unique for each hardware.

The QPUF metrics evaluated for IBM quantum simulator is presented in Fig. 5. QPUF response is obtained by harnessing inherent manufacturing variations during design and fabrication that affect how each qubit in the hardware has unique decoherence and coherence times, gate fidelities, and resonant frequencies. T2 time indicates the quantum state retaining capability of a qubit with higher T2 times indicating better stability. T1 time or energy relaxation time indicates the time taken to reach the ground state. Each qubit is physically mapped uniquely in each hardware with different driving resonant frequencies. These frequencies acts as qubit drivers which each microwave pulse calibrated to operate on the qubit at that frequency to drive the quantum state changes. At the time of QPUF evaluation, the calibrated physical parameters of qubits on various IBM quantum hardware are presented in Table II.

VI. Conclusion and Future Research

This research presented a novel Quantum SbD framework for trusted attestation of smart devices in SCADA-Smart Grid systems. The proposed QSbD framework ensures the security and reliability of various Intelligent electronic devices with quantum computing assisted capabilities through Quantum PUF guided by the quantum mechanics principles. Our evaluation has shown an impressive randomness of 50% and reliability of QPUF key extraction with 90% of keys being regenerated successfully. The proposed QPUF topology supports QPUF challenge response pairs generation supporting device attestation and secure communication for emerging Quantum-Energy-Cyber-Physical Systems (QE-CPS).

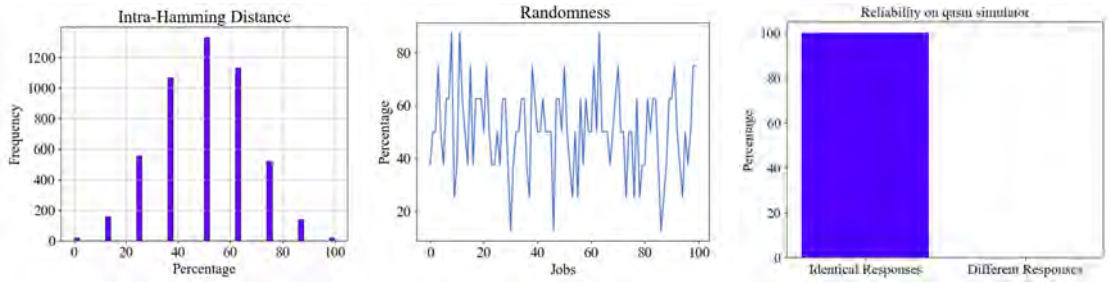
As a direction for future research, exploring the potential of QPUF in resource constrained healthcare-CPS could be a potential area as the application and adoption of quantum computing in H-CPS is increasing. Furthermore, integrating Quantum cryptography with QPUF could be another area to explore for enhanced security, privacy, and authenticity in the emerging Quantum Chain-of-Things (QCoT) era.

Acknowledgement

A preprint version of this work has been provided at [2].

References

[1] L. Cardwell and A. Shebanow, "The efficacy and challenges of SCADA and smart grid integration," *Journal of Cyber Security and Information Systems*, vol. 1, no. 3, pp. 1–7, 2016.



(a) QPUF Evaluation Results from IBM Simulator (ibmq_qasm_simulator)-100 Jobs

Fig. 5: QPUF Performance Evaluation Metrics

TABLE II: Calibrated Physical Parameters of Quantum Hardware

(a) ibm_osaka (**Calibrated at 5:30 PM on 6/19/24**)

Qubit	**T1 (us)**	**T2(us)**	**Frequency (GHz)**
Qubit 0	403.80	238.66	4.718
Qubit 1	320.35	363.44	4.800
Qubit 2	228.67	191.89	4.833
Qubit 3	350.98	198.82	4.661
Qubit 4	43.980	83.540	4.907
Qubit 5	161.30	68.470	4.720
Qubit 6	334.10	39.520	4.635
Qubit 7	269.28	9.0700	4.717

(b) ibm_kyoto (**Calibrated at 1:20 AM on 6/21/24**)

Qubit	**T1 (us)**	**T2(us)**	**Frequency (GHz)**
Qubit 0	184.74	30.200	4.908
Qubit 1	195.10	71.180	4.856
Qubit 2	247.98	51.490	4.733
Qubit 3	94.890	47.870	4.820
Qubit 4	417.88	67.250	4.854
Qubit 5	189.22	331.44	4.728
Qubit 6	213.21	263.22	4.783
Qubit 7	329.81	126.10	4.944

(c) ibm_sherbrooke (**Calibrated at 1:30 AM on 6/21/24**)

Qubit	**T1 (us)**	**T2(us)**	**Frequency (GHz)**
Qubit 0	375.14	172.24	4.636
Qubit 1	351.25	70.130	4.736
Qubit 2	237.88	150.08	4.819
Qubit 3	370.71	163.46	4.747
Qubit 4	120.26	199.60	4.788
Qubit 5	104.23	161.77	4.851
Qubit 6	312.87	186.59	4.900
Qubit 7	120.79	221.67	4.756

[2] 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," 2024. [Online]. Available: https://arxiv.org/abs/2410.12702

[3] L. A. Hsia, "Physically Unclonable Characteristics for Verification of Transmon-based Quantum Computers," Ph.D. dissertation, Air Force Institute of Technology, September 2021, theses Diss., Accessed: Sep. 15, 2024. [Online]. Available: https://scholar.afit.edu/etd/5073

[4] M. Arapinis, M. Delavar, M. Doosti, and E. Kashefi, "Quantum Physical Unclonable Functions: Possibilities and Impossibilities," *Quantum*, vol. 5, p. 475, June 2021.

[5] C. Z. Chwa, L. A. Hsia, and L. D. Merkle, "Quantum Crosstalk as a Physically Unclonable Characteristic for Quantum Hardware Verification," in *Proceedings of the IEEE National Aerospace and Electronics Conference*, 2023, pp. 309–313.

[6] 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.

[7] V. K. V. V. Bathalapalli, S. P. Mohanty, C. Pan, and E. Kougianos, "QPUF: Quantum Physical Unclonable Functions for Security-by-Design of Industrial Internet-of-Things," in *Proc. IEEE International Symposium on Smart Electronic Systems (iSES)*, 2023, pp. 296–301.

[8] B. Skoric, "Quantum readout of Physical Unclonable Functions: Remote authentication without trusted readers and authenticated Quantum Key Exchange without initial shared secrets," Cryptology ePrint Archive, Paper 2009/369, 2009, https://eprint.iacr.org/2009/369. [Online]. Available: https://eprint.iacr.org/2009/369

[9] B. Skoric , "Quantum readout of physical unclonable functions," *International Journal of Quantum Information*, vol. 10, no. 01, p. 1250001, 2012.

[10] V. Galetsky, S. Ghosh, C. Deppe, and R. Ferrara, "Comparison of Quantum PUF models," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, 2022, pp. 820–825.

[11] K. K.-H. Chuang, H.-M. Chen, M.-Y. Wu, E. C.-S. Yang, and C. C.-H. Hsu, "Quantum Tunneling PUF: A Chip Fingerprint for Hardware Security," in *Proc. International Symposium on VLSI Technology, Systems and Applications (VLSI-TSA)*, 2021, pp. 1–2.

[12] W. Lardier, Q. Varo, and J. Yan, "Quantum-Sim: An Open-Source Co-Simulation Platform for Quantum Key Distribution-Based Smart Grid Communications," in *Proc. IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2019, pp. 1–6.

[13] M. A. Khan, M. N. Aman, and B. Sikdar, "Soteria: A Quantum-Based Device Attestation Technique for Internet of Things," *IEEE Internet of Things Journal*, vol. 11, no. 9, pp. 15 320–15 333, 2024.

[14] A. Javadi-Abhari, M. Treinish, K. Krsulich, C. J. Wood, J. Lishman, J. Gacon, S. Martiel, P. D. Nation, L. S. Bishop, A. W. Cross, B. R. Johnson, and J. M. Gambetta, "Quantum computing with Qiskit," 2024. [Online]. Available: https://arxiv.org/abs/2405.08810