QPUF: Quantum Physical Unclonable Functions for Security-by-Design of Industrial Internet-of-Things

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*—This work presents a Quantum Computing based Physical Unclonable Functions (PUF) architecture with a novel approach for PUF key generation and noise reduction in noisy Quantum systems. The motivation is to explore the potential of Quantum Computing assisted cybersecurity for Security-by-Design (SbD) of Industrial-Internet-of-Things (IIoT). Internet-of-Things (IoT) in Industry 4.0 can improve efficiency, increase automation, and facilitate intelligent decision making through the integration of edge cloud computing paradigms. However, the lack of standardization of security protocols across IIoT devices can be challenging due to the heterogeneous nature of these devices. In this context, a novel Quantum circuits based PUF design that is built on real Quantum hardware is presented. The proposed QPUF can facilitate security in IIoT by using a Quantum hardware generated PUF key as the device identity. The proposed PUF Design is built using Quantum Hadamard Gate, and Ry gates and has been experimentally demonstrated on IBM Quantum hardware systems. The proposed architecture also supports PUF key generation from Quantum hardware for security applications. Figures-of-merits (FoM) of PUF have been evaluated and presented to demonstrate the robustness of the proposed Quantum PUF for SbD of IIoT.**

***Index Terms*—Security-by-Design (SbD); Hardware Assisted Security (HAS); Industrial Internet-of-Things (IIoT); Quantum Computing; Physical Unclonable Functions (PUF).**

I. Introduction

An Cyber-Physical System (CPS) architecture consists of Sensor, communication, and Information Technology (IT) layers [1]. The sensor layer consists of various smart sensors, actuators, and control systems in an industrial environment. The Communication layer enables the flow of parametric data from physical sensors to the IT layer. The IT layer is responsible for the analysis and processing of sensor data through edge cloud computing paradigms. Decision making is done based on the analyzed data in the IT layer. It includes the enterprise level decision making systems and the commands to actuators are processed in this layer. Decision making involves improving the operational efficiency of machines, control systems and enhancing the automation [2], [3]. From a cybersecurity perspective, the trustworthiness of IIoT is pivotal since the sensors and actuators, control systems, and Programmable Logic Controllers (PLC) have diverse functionalities and characteristics. The heterogeneous nature of these devices make it more challenging to facilitate the security. The implementation of advanced cryptographic techniques to facilitate security in IIoT may involve a tradeoff between the performance and achieved cybersecurity [4], [5].

Security-by-Design (SbD) is an emerging phenomenon that works on embedding security and privacy features at the design stage of an electronic system [6], [7]. Embedding security and privacy primitives at the design phase can guarantee security right from the design stage rather than implementing security protocols at the application stage [6], [8], [9]. This work explores the scope of Quantum-assisted cybersecurity in Industrial Internet-of-Things (IIoT) applications by implementing PUF technology on Quantum Hardware.

Quantum mechanics principles like entanglement and superposition can support quantum information processing using Qubits and can be applied in the areas of IIoT, Smart Transportation [10]–[13]. Quantum entanglement facilitates information processing and sharing by entangling the quantum states of Qubits [14], [15]. Each Qubit can possibly be either in one of the two states and if there are n qubits then 2^n possible states are possible [16], [17]. Quantum PUF designs using the quantum physics prinicples like entanglement, superposition, and decoherence have been proposed in [18], [19] for security and privacy in Quantum computing applications. Quantum computing's potential in advancing computational capability to the next level surely has great potential in Industry 4.0 through PUF assisted Quantum hardware access and control. The proposed architecture aims to leverage the potential of SbD in Quantum computing for IIoT security by proposing a Quantum logic gates based PUF architecture that supports higher Challenge response pairs (CRP) and can facilitate device authentication and access control for ensuring the security of device, firmware, and network in IIoT. A conceptual overview of QPUF for SbD of I-CPS is shown in Fig. 1.

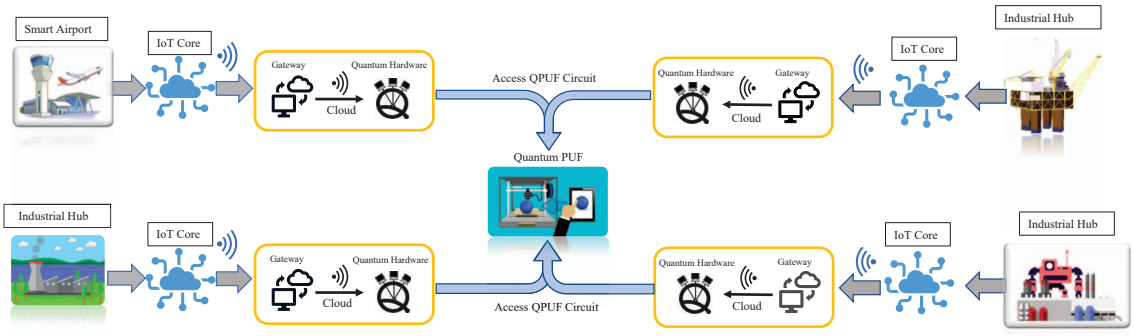


Fig. 1: QPUF for Security-by-Design (SbD) of Industrial Cyber-Physical-Systems (I-CPS).

The rest of this paper is organized as follows. Novel contributions of the proposed QPUF are illustrated in Section II. Section III illustrates the contemporary related works in IIoT security and Quantum Cybersecurity. The preliminaries and working model of the proposed QPUF architecture are discussed in section IV. QPUF Experimental validation results have been presented in section V. Finally, the conclusion and future work is discussed in Section VI.

II. State-of-the-Art Contributions

The novel contributions of the current paper include:

- A PUF built on Quantum hardware using Quantum logic.
- A noise less PUF response generation from Quantum systems through majority voting scheme.
- A robust architecture that supports higher Challenge-Response-Pair (CRP) space.
- A novel cloud computing assisted approach that can support billions of IoT devices to access QPUF and obtain cryptographic identities.
- A system that can facilitate the integration of SbD using QPUF in IIoT more efficiently than conventional PUF.

III. Related Work

This Section presents a comprehensive overview of existing PUF and Quantum-assisted hardware security schemes for IIoT. A holistic comparative analysis of our proposed QPUF with the related research is presented in Table I.

A PUF-based Blockchain named HPCchain for security and device authentication of IIoT is proposed in [20]. This work proposes a consortium Blockchain framework by using a PUF-based Blockchain consensus mechanism. The architecture of HPCchain consists of an asset, Blockchain, and Application layers. The blockchain layer works on top of the asset layer and is responsible for transaction recording and validation.

A sensor data stream integrity verification using PUF in Industrial-Cyber-Physical Systems (I-CPS) is proposed in [21]. This work proposes a PUF-based approach for secure communication between PLC nodes and sensor nodes in Industrial environments. This work claims to counter side-channel attacks by embedding smart sensors with PUF modules.

A secure Machine-to-Machine (M2M) communication mechanism in an IIoT environment using PUF has been proposed in [22]. This work proposes a PUF-based efficient authentication and session establishment protocol (PEASE) that claims to achieve device identity confidentiality with low computational power and energy overhead.

QPUF architectures based on the principles of decoherence using quantum logic gates proposed in [18] validate the potential of QPUF for Quantum computing security. This work does not experimentally validate PUF design uniqueness, reliability, diffuseness and also does not validate experimentally PUF key generation and noise reduction process. In comparison, our proposed architecture presents an approach for key extraction from the PUF design and tests the design with varying initializations for Qubits to extract large number of PUF keys. Our architecture also clearly presents a noise reduction approach using majority voting scheme to obtain the Qubit's probability.

A Pseudo PUF-based IIoT security mechanism is proposed in [23] which utilizes a weak PUF module that supports limited CRPs and a lightweight symmetric encryption module. This approach works on reducing energy overhead while improving the resiliency of the Pseudo PUF used in this paper.

In comparison, our work introduced a Quantum hardware generated cryptographic identity that is reliable, hardware generated, and can further enhance the resiliency of IoT devices in I-CPS. This design as a strong PUF can support more CRP space.

IV. Proposed QPUF Methodology

This section gives a comprehensive overview of the architecture and modeling of the proposed QPUF.

A. Architecture of QPUF

The proposed Quantum PUF design is built using Quantum Hadamard, Ry, and measurement gates. The proposed QPUF is a 5-Qubit PUF architecture, and the design can also be 7,32, and 128 Qubit based on the Quantum Hardware as in Fig. 2.

In the ideal case, super-positioned Qubits from the Hadamard gate should produce either 0 or 1 as output with equal probability. However, in a real-world scenario, the probability is expected to be biased towards either 0 or 1. This enables the QPUF design to generate a unique signature by grouping individual Qubit outputs and thereby generating a Response. Quantum gate fidelity is different in both systems as shown in Fig. 3.

TABLE I: Framework Analysis: A Comprehensive Evaluation

Research Works	Security Mechanism	Approach	Features	Platform
Barbareschi, et al. 2021 [23]	Pseudo-PUF for Industrial IoT	Weak PUF, Encryption Module	Low energy overhead	NA
Phalak, et al. 2021 [18]	Decoherence and Hadamard PUF	Qubit Decoherence	Security in Quantum Computing	Cloud
Gong, et al. 2022 [22]	PUF-based Authentication in IIoT	PUF, Fuzzy extractor	Secure Machine to Machine communication	Cloud Computing
Shan, et al. 2023 [21]	PUF-based sensor security	SRAM PUF, HMAC Algorithm	Industrial sensor data integrity	SCADA System
Qian, et al. 2023 [20]	PUF-based Blockchain for IIoT	Hybrid PUF, Consortium Blockchain	CPU & FPGA based PUF with enhanced uniqueness	NA
QPUF (Current Paper)	Quantum Computing based PUF for IIoT	QPUF based on Quantum logic gates	Quantum hardware based Reliable QPUF responses	IBM's Quantum Cloud

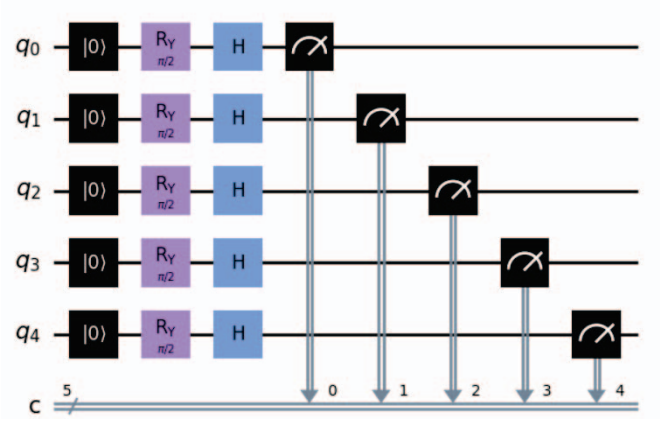
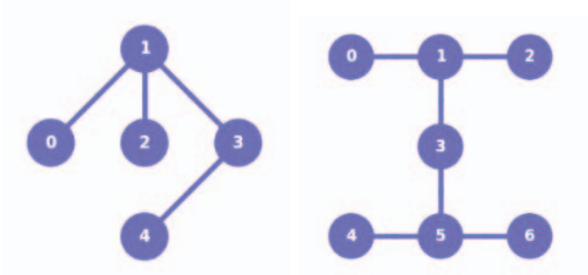


Fig. 2: Proposed Quantum Hardware QPUF Design.



(a) 5-Qubit System (b) 7-Qubit System

Fig. 3: Quantum Hardware Qubit Structures.

B. Modelling of QPUF

The QPUF initially works by initializing each Qubit as either 0 or 1. A tunable rotation gate is added to the Qubits to improve the resiliency of PUF Design to temporal variations. The Ry gate performs rotation around the Y-axis of the Bloch sphere. After applying the Ry gate, the Hadamard gate is applied to each one of the Qubits to place them in superposition. The Quantum state of individual Qubits is then measured by applying the measurement gate to all Qubits and storing these values in classical registers. The proposed QPUF Design is a five Qubit PUF design since most of the IBM Quantum devices are 5 Qubit architectures.

The resultant output of each Qubit is stored in the corresponding classical register. For instance, the measurement gate gives the result of Qubit q[0] in classical register c[0], q[1] in c[1] likewise for all qubits. For each job, the circuit is executed on hardware for 8192 shots. After obtaining the outcomes of all shots, the most occurring outcome is chosen as the Job string for that job. After executing the "n" number of jobs where n is proportional to the length of the key, a unique string is extracted from all the obtained job strings for each Qubit. Each Qubit's corresponding values from all jobs are extracted and grouped together as a string which will be the resultant PUF response. Since each job execution involves testing the circuit at different tunable rotation angles for the Ry gate and a unique initialization for Qubits, the resultant QPUF Qubit string responses will be unique. Also, each Qubit's default physical properties are different which differentiate each Qubit's response to changing Ry gate angles and initializations thereby generating unique responses. Algorithm 1 and Algorithm 2 briefly outline the details of accessing Quantum systems and building QPUF design.

Algorithm 1 Accessing Quantum System and Building PUF

Input: IBM Quantum API Token
Output: QPUF Design
1: Access IBM Quantum System
2: Obtain IBM Quantum API Token
User → API Token
3: Access Qiskit
4: Build Quantum Circuit using Quantum Logic Gates
QPUF Circuit → Hadamard, Ry, Measurement Gates
5: Choose Quantum Backend
Backend → ibmq_quito, ibmq_lima, ibmq_belem, ibmq_manila, ibmq_jakarta,..
- ibmq_quito-5 Qubit, ibmq_lima-5 Qubit, ibmq_belem-5 Qubit, ibmq_jakarta-7 Qubit

6: Execute the Circuit on the chosen backend and monitor the status of the job
- Job is being Validated, Job is Queued, Job is Actively Running, Job has successfully Run

7: Obtain the result

C. Parameters of Physical Qubits

Superconducting transmon Qubits can exchange quantum state information by operating at extremely low temperatures where these circuits can conduct electric current at extremely

Algorithm 2 Modelling of QPUF on Quantum Systems

Input: Quantum Logic Gates
Output: QPUF Signature
1: initialize Qubits (Varying Initializations)
Example:
1st Qubit → 0, 2nd Qubit →1, 3rd Qubit →1, 4th Qubit →0, 5th Qubit→0,
2: Choose unique initialization for Qubits for each job
3: Apply Ry gate to all Qubits
4: Choose unique Ry gate angle for each job
Ry Angle→pi/4, pi/2,...
Circuit→ Ry[q]
5: Apply Hadamard gate to all Qubits
Circuit→ H(Ry[q])
6: Apply Measurement Gate(M) to the superpositioned Qubits
Circuit→ M[H(Ry[q])]
7: Execute the circuit on Chosen backend and generate the result string for each job
(Jobs sets-5 sets, Each job Inputs- Initialization, Ry Gate angle
8: Extract results string from all jobs
9: Extract Qubit strings from all job strings
Final Output-Qubit strings(Responses)
10: Calculate PUF metrics
11: **if** $PUFmetrics from Qubit Strings are standardized$ **then**
12: Assign Qubits Strings as Responses
13: **end if**

low temperatures. These superconducting circuits are controlled by Josephson junctions which work by separating two conducting electrodes with a thin insulating barrier. Josephson junctions control the quantum state of a qubit by modulating the phase difference.

Individual qubits in a quantum system have default resonating frequencies and coherence and decoherence times. Different IBM Quantum systems have different parameters which can support the PUF primitive since PUF is based on the intrinsic properties of hardware and generates a unique fingerprint for each hardware. Physical qubit manufacturing frequencies are given in Table. II. These obtained Qubit frequencies are susceptible to noise and may exhibit slight variations.

V. Experimental Results

The proposed QPUF design methodology has been written in Python and executed in the Qiskit environment. IBM Quantum hardware backends:"ibmq_lima", "ibmq_quito", "ibmq_belem" have been chosen for executing the QPUF circuit. The backend systems of IBM are accessed by obtaining an API token and loading the account credentials. IBM Quantum composer platform has been used to work and execute the Quantum circuits and was run on Alienware Aurora R13 system model with 12th generation i7 processor and 16 GB RAM. "ibmq_belem", "ibmq_lima", and "ibmq_quito" quantum hardware backends have been chosen for the QPUF design execution.

We have presented the characterization and performance analysis of QPUF in Table IIIa and IIIb. The uniformity, diffuseness, and uniqueness of the resultant job string pairs from three quantum systems have been presented in Fig. 4.

QPUF implementation on ibmq_lima has produced a reliability of 60% with almost 15 matching keys of 4 sets of 25 executed jobs. The diffuseness of 40% is achieved with an average uniformity of 35.2%. ibmq_belem in comparison with ibmq_lima has somewhat lower diffuseness of 38% and uniformity of approximately 30%. ibmq_quito hardware has produced a diffuseness of 38.20% for the PUF circuit. The QPUF evaluation results of Quantum backend systems along with generated QPUF responses are given in Fig. 5.

For each job execution, a unique job string is obtained with a histogram of circuit outcomes and angles using the majority voting scheme. To reduce the noise interference and extract noise less responses, 5 sets of jobs are executed. Each job set has random qubit initialization with varying tunable rotation angles for the ry gate. Among 5 sets of jobs, each job set has a chosen qubit initialization sequence. The results of each job in all the sets are compared to obtain PUF reliability. The occurrence of the result string in all job sets are evaluated through approximation. The qubit results values inside the string in all job sets are evaluated and the maximum occurring output among all the job sets is chosen to be the final qubit's value. The length of the QPUF signature is proportional to the length of the obtained Qubit string from all the jobs. The probability of outcomes for different job sets and angles in three quantum hardware is illustrated in Fig. 6.

VI. Conclusion and Future Research

Implementing PUF technology in Quantum Computers which are noisy is a challenging task due to Qubit's nature of decoherence. The interaction of Qubit with the environment can result in its decoherence. This can be addressed by increasing the number of samples and executing a greater number of jobs. We found that the problem with the execution of jobs on IBM quantum backends is that some quantum systems tend to get faulty and require maintenance which can disrupt the execution of jobs. Also, the execution of each job goes through a queue line which might take days to complete job execution.

This work has successfully presented a novel QPUF design by implementing the Quantum logic gates-based circuit on different Quantum hardware devices and evaluated PUF metrics and generated responses from QPUF design. A novel QPUF assisted SbD approach for IIoT has been presented that can support the security of I-CPS where IIoT devices can access QPUF and obtain keys. Our proposed QPUF assisted SbD approach is scalable and secure as the access to the hardware is through the cloud and does not require IIoT devices to have a PUF module embedded physically.

Improving the accuracy of the proposed QPUF design through various noise reduction techniques can be a direction for future research. Furthermore, the proposed work could be integrated with the QKD protocol for enabling the secure exchange of PUF keys using Quantum mechanics principles.

References

[1] S. K. Ram, B. B. Das, K. Mahapatra, S. P. Mohanty, and U. Choppali, "Energy Perspectives in IoT Driven Smart Villages and Smart Cities,"

TABLE II: Frequencies of Physical Qubits in Quantum Systems.

Qubit Frequency	ibmq_lima (GHz)	ibmq_quito (GHz)	ibmq_belem (GHz)
Qubit 0	5.03	5.3	5.09
Qubit 1	5.13	5.08	5.25
Qubit 2	5.25	5.32	5.36
Qubit 3	5.3	5.16	5.17
Qubit 4	5.09	5.05	5.26

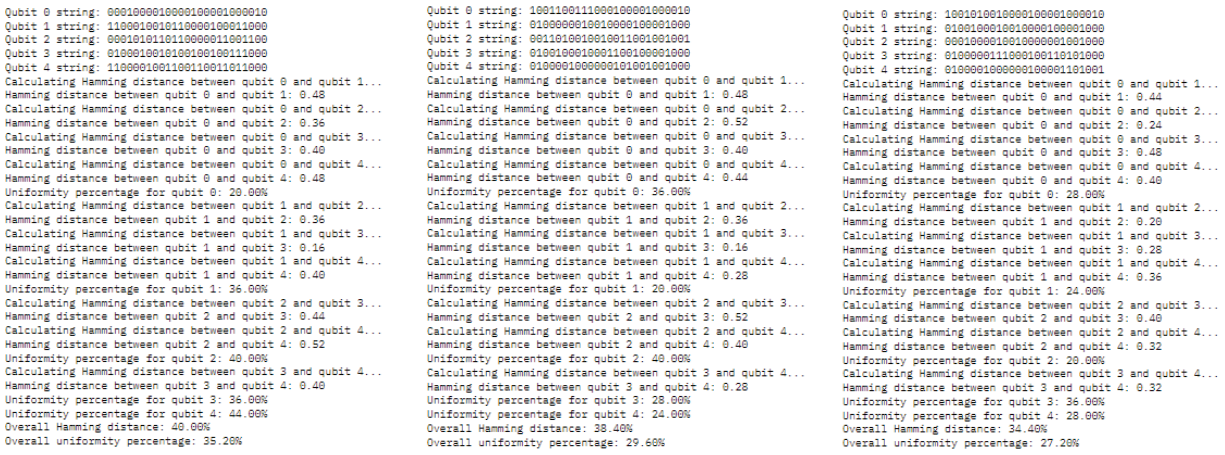
TABLE III: Performance Analysis of QPUF.

(a) Characterization of QPUF

QPUF Prameters	Specific Details
Quantum system	IBM
Working Platform	IBM Quantum experience
Environment	Qiskit
QPUF Gates	Hadamard, Ry, and Measurement Gates
Quantum Systems	Simulator, Hardware
Model	Majority Vote
Backends	ibmq_lima, ibmq_belem, ibmq_quito
Number of Jobs	25 Jobs
Number of shots	8192
Backend Architectures	5 Qubit

(b) QPUF Evaluation Results from Quantum Systems

Figure-of-Merits	ibmq_lima	ibmq_quito	ibmq_belem
Overall Hamming Distance	40%	38.40%	34.40 %
Uniformity of QPUF	35.20%	29.60%	27.60%
Uniqueness of QPUF	25.20%		
Reliability (Matching Keys)	60%	48%	-



(a) ibmq_lima (b) ibmq_quito (c) ibmq_belem

Fig. 4: QPUF Responses and Metric Evaluation for Quantum Systems.

IEEE Consumer Electronics Magazine, vol. 10, no. 3, pp. 19–28, May 2021.

[2] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, Opportunities, and Directions," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4724–4734, November 2018.

[3] A. Vakaloudis and C. O'Leary, "A framework for rapid integration of IoT Systems with industrial environments," in *Proc. IEEE 5th World Forum on Internet of Things (WF-IoT)*, April 2019.

[4] H. Sarjan, A. Ameli, and M. Ghafouri, "Cyber-Security of Industrial Internet of Things in Electric Power Systems," *IEEE Access*, vol. 10, pp. 92 390–92 409, 2022.

[5] 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, September 2021.

[6] F. Pescador and S. P. Mohanty, "Guest Editorial Security-by-Design for Electronic Systems," *IEEE Transactions on Consumer Electronics*, vol. 68, no. 1, pp. 2–4, February 2022.

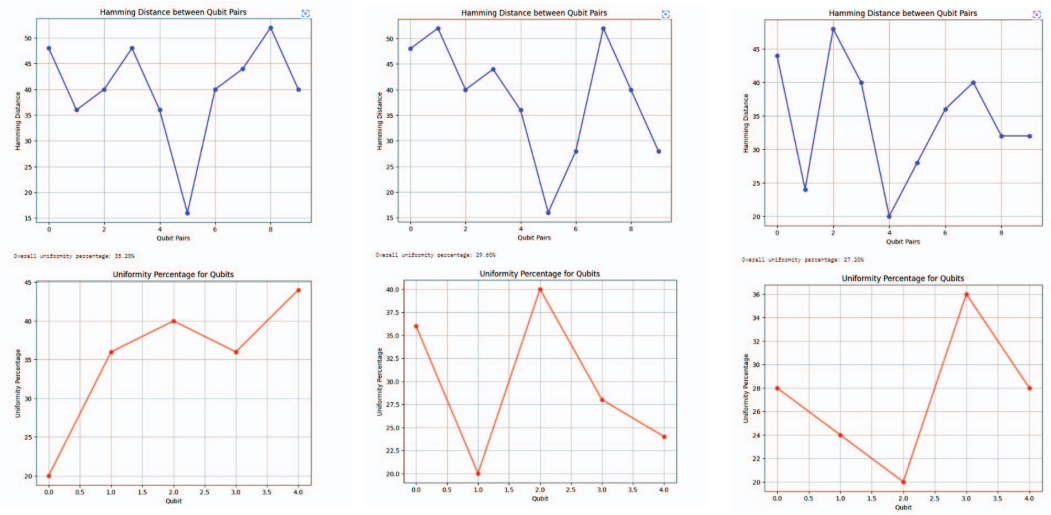
[7] V. K. V. V. Bathalapalli, S. P. Mohanty, E. Kougianos, V. Iyer, and B. Rout, "iTPM: Exploring PUF-based Keyless TPM for Security-by-Design of Smart Electronics," in *Proc. of IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2023, pp. 1–6.

[8] K. K. Rangan, J. A. Halloun, H. Oyama, S. Cherney, I. A. Assoumani, N. Jairazbhoy, H. Durand, and S. K. Ng, "Quantum Computing and Resilient Design Perspectives for Cybersecurity of Feedback Systems," *IFAC-PapersOnLine*, vol. 55, no. 7, pp. 703–708, 2022.

[9] 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)*, April 2021.

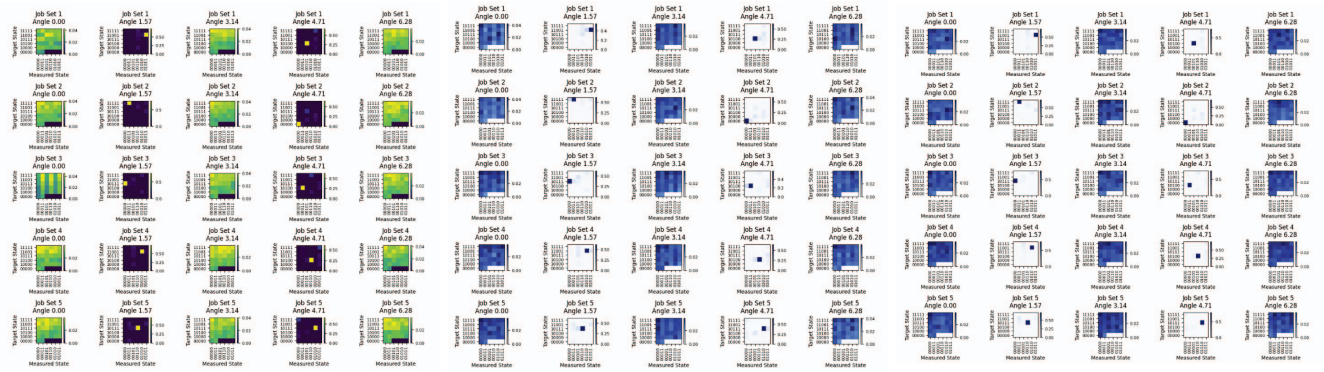
[10] T. G. Tan, J. Zhou, V. Sharma, and S. P. Mohanty, "Post-Quantum Adversarial Modeling: A User's Perspective," *Computer*, vol. 56, no. 8, pp. 58–67, Aug 2023.

[11] E. haq Shaik and N. Rangaswamy, "Implementation of Quantum Gates based Logic Circuits using IBM Qiskit," in *Proc. 5th International Con-*



(a) ibmq_lima (b) ibmq_quito (c) ibmq_belem

Fig. 5: Sample QPUF Figure-of-Metrics (FoM) for Quantum Systems.



(a) ibmq_lima (b) ibmq_quito (c) ibmq_belem

Fig. 6: QPUF Outcomes Probabilities for Varying Tunable Rotation Angles.

ference on Computing, Communication and Security (ICCCS), October 2020, pp. 1–6.

[12] T. Peham, L. Burgholzer, and R. Wille, "Equivalence Checking of Quantum Circuits With the ZX-Calculus," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 12, no. 3, pp. 662–675, September 2022.

[13] M. Bhatia and S. K. Sood, "Quantum Computing-Inspired Network Optimization for IoT Applications," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5590–5598, June 2020.

[14] H. A. Bhat, F. A. Khanday, B. K. Kaushik, F. Bashir, and K. A. Shah, "Quantum Computing: Fundamentals, Implementations and Applications," *IEEE Open Journal of Nanotechnology*, vol. 3, pp. 61–77, 2022.

[15] B. ŠKORIĆ, "Quantum readout of Physical Unclonable Functions," *International Journal of Quantum Information*, vol. 10, no. 01, p. 1250001, February 2012.

[16] E. Lella, A. Gatto, A. Pazienza, D. Romano, P. Noviello, F. Vitulano, and G. Schmid, "Cryptography in the Quantum Era," in *Proc. IEEE 15th Workshop on Low Temperature Electronics (WOLTE)*, June 2022, pp. 1–4.

[17] G. Kahanda, V. Patel, M. Parikh, M. Ippolito, M. Solanki, and S. Ahmed, "The Future Era of Quantum Computing," in *Advanced Sciences and Technologies for Security Applications*. Springer International Publishing, 2023, pp. 469–484.

[18] 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, June 2021.

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

[20] K. Qian, Y. Liu, X. He, M. Du, S. Zhang, and K. Wang, "HPCchain: A Consortium Blockchain System based on CPU-FPGA Hybrid PUF for Industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, pp. 1–11, 2023.

[21] X. Shan, H. Yu, Y. Chen, and Z. Yang, "Physical Unclonable Function Based Lightweight and Verifiable Data Stream Transmission for Industrial IoT," *IEEE Transactions on Industrial Informatics*, pp. 1–11, 2023.

[22] X. Gong, T. Feng, and M. Albettar, "PEASE: A PUF-Based Efficient Authentication and Session Establishment Protocol for Machine-to-Machine Communication in Industrial IoT," *Electronics*, vol. 11, no. 23, p. 3920, November 2022.

[23] M. Barbareschi, V. Casola, A. D. Benedictis, E. L. Montagna, and N. Mazzocca, "On the Adoption of Physically Unclonable Functions to Secure IIoT Devices," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7781–7790, November 2021.