QPUF 3.0: Sustainable Cybersecurity of Smart Grid through Security-By-Design based on Quantum-PUF and Quantum Key Distribution

Venkata K. V. V. Bathalapalli
University of North Texas
Denton, Texas, USA
vb0194@unt.edu

Saraju P. Mohanty
University of North Texas
Denton, Texas, USA
saraju.mohanty@unt.edu

Chenyun Pan
University of Texas at Arlington
Arlington, Texas, USA
chenyun.pan@uta.edu

Elias Kougianos
University of North Texas
Denton, Texas, USA
elias.kougianos@unt.edu

Abstract

The scope of Quantum computing and its information processing potential in comparison to classical computing has significantly broadened its application and research, most notably in the domain of Quantum Internet-of-Things (QIoT). This research explores the scope of Quantum Computing in enabling secure and sustainable smart grid operations through the integration of tamper-proof Quantum Physical Unclonable Functions (QPUF) primitive and Quantum Key Distribution (QKD) communication protocols. A novel framework is proposed that leverages QPUF-based intelligent device attestation and QKD-based secure communication among quantum-capable smart grid entities with quantum computing capabilities. The proposed QPUF-QKD integrated framework was evaluated using IBM and Rigetti Computing's quantum systems and simulators. Notably, QPUF evaluation on IBM and Rigetti quantum simulators achieved 100% reliability with 48.6% uniqueness, demonstrating its effectiveness and reliability across different quantum computing platforms. Additionally, the QPUF-QKD integrated framework validation and its computational time analysis presented validate its potential for Quantum Security-by-Design (QSbD) for smart grid applications.

CCS Concepts

• **Hardware → Quantum communication and cryptography**;
• **Security and privacy → Hardware-based security protocols**.

Keywords

Quantum Security-by-Design, Quantum Key Distribution (QKD) Quantum Physical Unclonable Functions (PUF), Smart Grid

GLSVLSI '25, New Orleans, LA, USA

ACM ISBN 978-x-xxxx-xxxx-x/YYYY/MM
https://doi.org/10.1145/nnnnnnn.nnnnnnn

ACM Reference Format:
Venkata K. V. V. Bathalapalli, Saraju P. Mohanty, Chenyun Pan, and Elias Kougianos. 2024. QPUF 3.0: Sustainable Cybersecurity of Smart Grid through Security-By-Design based on Quantum-PUF and Quantum Key Distribution. In *Great Lakes Symposium on VLSI 2024 (GLSVLSI '25), June 30–July 2, 2025, New Orleans, LA, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 Introduction

Quantum Physical Unclonable Functions (QPUF) serve as a security primitive that generates unique, hardware-specific fingerprints by exploiting the inherent randomness of quantum systems. A QPUF-generated fingerprint ensures the security and integrity of both communication and data associated with a quantum computer. The foundational principles behind QPUFs include the quantum no-cloning theorem, which prohibits the exact duplication or cloning of an unknown quantum state, and the Heisenberg uncertainty principle, which limits the precise measurement of a qubit's quantum state [19]. QPUF derives its uniqueness from hardware-specific quantum characteristics such as qubit coherence, decoherence times, gate fidelities, and resonant frequencies that vary across different quantum computers.

This research introduces a novel Quantum computing-assisted solution aimed at enhancing the security and sustainability of grid infrastructure and its management. The proposed approach integrates QPUF for tamper-proof device-level security and a QKD framework to enable secure communication within Supervisory Control and Data Distribution (SCADA)-driven grid infrastructure. SCADA-enabled smart grid is structured into three layers. The Physical layer comprises field-level devices such as sensors and actuators that sense and process electrical grid data. The automatic control and supervisory layer operates on top of the physical layer and consists of Programmable Logic Controllers, RTUs, and MTUs with Local and Wide Area networks. At the top, the decision control layer is responsible for centralized decision making, logic execution, and actuation processes within the grid [1].

The proposed work introduces QPUF-assisted security for smart electronic components within the electrical grid, offering unique and unclonable tamper-proof fingerprints for all the electronic devices, such as Remote and master terminal units in the SCADA.

Each of these electronic components, RTU and MTU in SCADA-Grid, will have QPUF-assisted security, enabling secure identity attestation. The communication between these entities and SCADA is further protected using QKD [14]. QPUF operates based on the foundational principles of quantum mechanics, leveraging intrinsic hardware level variations driven by micro-level process variations to generate a random bitstream of zeros and ones as a unique fingerprint. This primitive resembles classical PUFs while offering enhanced security through quantum mechanics [6]. The conceptual idea of QPUF 3.0 Quantum SbD is illustrated in Fig. 1

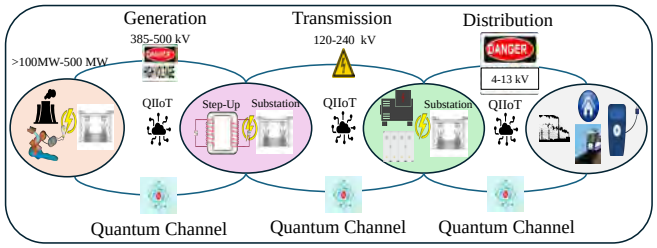


Figure 1: Conceptual Idea of QPUF 3.0 for SbD of Smart Grid

In QKD, the sender and receiver establish communication using quantum and authenticated classical channels for establishing a secure session key for information exchange. This could be performed by sending a stream of photons on a quantum channel, which could be a fiber optic communication link. The receiver captures the photons and measures each of the photons using a randomly selected basis. Then, both the sender and receiver communicate through authenticated classical channels about the chosen basis for each of the photons. The measurement values of photons that have been measured with the same basis on both sides could be the session key for communication [5, 20]. The conceptual idea of QPUF 3.0 is presented in Fig. 2.

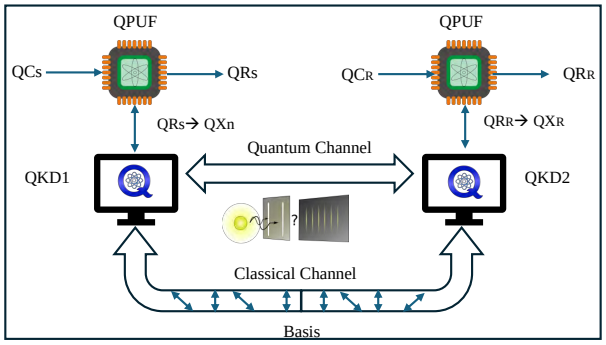


Figure 2: Proposed QPUF-QKD Integrated framework for Smart Grid

The rest of this paper is organized as follows. Section 2 discusses related research works on Quantum SbD for IoT. Section 3 presents the novel contributions of this research work. The proposed QPUF-QKD integrated framework is discussed in section 4. QPUF 3.0 Experimental validation and implementation details are presented in section 5. Finally, the conclusion and future work is discussed in Section 6.

2 Related Research

This section discusses state-of-the-art research on QKD and quantum security for IoT applications, and also discusses real-world instances of cyberattacks targeting smart grid entities in the Table. 1.

The study in [6] introduced a QPUF circuit with 8 qubits, leveraging the inherent biasing of a qubit to the 0 or 1 state through tunable Pauli X, Y, and Z rotation angles evaluated over the range of [0-2 pi]. A quantum random number generator is proposed in [13] using the Hadamard gate to induce a superposition of quantum states, along with a QPUF-based attestation protocol with a prover and verifier utilizing quantum and flash memories, respectively. The work in [22] presented a secure smart grid metering framework that integrates QKD and cryptographic-hash functions to ensure data privacy for the smart meter data and enhance secure communication among the smart grid entities. Furthermore, [2] demonstrated a real-world QKD-enabled Message Queuing and Telemetry Protocol (MQTT) for intelligent attestation of smart grid entities that was performed at Electric Power Board (EPB), Chattanooga, Tennessee, with a dedicated optical-fiber-based quantum communication channel to support secure interactions among smart grid entities.

A novel QKD framework for secure sensor data transmission in Quantum IoT applications is proposed [5], where QKD and shared secret key are employed to encrypt sensor data, enabling secure communication between sensor nodes and gateway nodes. In [8], a QKD-based communication protocol for secure power grid data exchange using both wired and wireless links addresses the challenges in key distribution and data transmission delays. To overcome the security limitations of the Message Queuing and Telemetry Protocol (MQTT) for IoT data security, a QKD-integrated MQTT-based approach to enhance data confidentiality is proposed in [11], overcoming the challenge and computational limitations in conventional cryptographic techniques, leveraging eavesdropping detection by assessing quantum state changes. A QKD-integrated fiber-optic Blockchain framework in [1] presents a sustainable approach for integrating QKD-Blockchain in SCADA driven electrical grid systems through QKD-enabled field sensors and device attestation with Blockchain smart contracts for secure communication. In [27], a hybrid symmetric-asymmetric quantum resistant encryption mechanism tailored for resource constrained IoT devices combines post-quantum cryptographic techniques with QKD for enhanced security. Table. 2 presents a brief overview of QKD-driven quantum security protocols.

3 Novel Contributions

This section highlights the novel features of the proposed Quantum Key Distribution and QPUF-enabled communication framework for SCADA-Grid, along with key research problems addressed in the paper.

Table 1: Grid Attacks [18]

Power Grid Attack	Details
PG&E Substation at Metcalf, California [26]	Attackers physically damaged fiber-optic cable and transformers through sniper-rifles
Ukraine Power Grid [10]	Hacking Control systems and modifying the Operational parameters leading to blackout
DDoS Attack in Los Angeles and Salt Lake [7]	Hackers disrupted electrical system operations and affected the real-time grid management
Ransomware attack in Johannesburg, South Africa [4]	Affecting the City's power blackout management systems and energy buying platform

Table 2: Related Works on QSbD

Research Work	Application	Primitives	Approach
Li et al. [17]	Secure Power Data transmission	QKD and Quantum Random Number Generator (QRNG)	QKD enables secure exchange of QRNG generated encryption keys
Krishna et al. [15]	patient data protection	QKD & Elliptic Curve Cryptography	BB84 with ECC based basis selection
Farooq et al. [11]	IoT data security	QKD, MQTT, ASCON-128	QKD for key exchange and ACON-128 for encryption
Xiong et al. [27]	Secure IoT enabled smart grid	Learning with Errors (LWE) and Ring-LWE	Integrating Quantum resistant algorithm with symmetric and asymmetric encryption
Parameswarath et al. [21]	Smart Meter Data Security	QKD and QRNG	Smart meter and Server establish secure communication using QKD and QRNG

3.1 Research Problems Addressed in the Current Paper

- Problem of implementing a scalable and tamper-proof attestation mechanism of resource-constrained smart grid systems.
- The absence of an intelligent communication framework for communication among quantum computing-enabled grid entities.
- Problem of sustainable Quantum sensor attestation mechanism to guarantee data integrity and protection against tampering.
- The lack of a sustainable approach for addressing noisy quantum computation, which impacts the reliability and integrity of the quantum-grid framework.
- The lack of stability in QPUF-supported security solutions for securing Quantum Internet-of-Things(QIoT) applications.

3.2 Novel Features of the Proposed Solution

- A novel quantum sensor attestation mechanism for QIoT-enabled smart grid.
- A sustainable quantum network communication protocol for secure, quantum enhanced communication among quantum grid entities
- A QKD-based communication framework for SCADA-Electrical distribution systems.
- QPUF-based QKD device attestation for sustainable and quantum hardware-driven electrical grid entity attestation.
- A QPUF architecture with a reliable challenge-response pair generation approach, tailored for noisy quantum computers.
- An integrated QPUF-QKD framework that leverages quantum mechanics to support quantum IoT.

4 Proposed QPUF-QKD Integrated Framework for Smart Grid

This section provides an overview of Quantum Key Distribution and QPUF-enabled communication within QKD-equipped devices in the SCADA-Grid infrastructure.

The proposed solution incorporates the QKD BB84 protocol for secure communication among Remote Terminal Units (RTUs) and between RTUs and MTUs within the SCADA electrical distribution system. QKD works by transmitting a stream of photons encoded in four polarization states across rectilinear and diagonal bases with Polarization angles of 0^o, 90^o, 45^o, and 135^o. These quantum states are transmitted through a quantum channel, such as a free-space optical fiber link. The QKD ensures the attestation of IEDs, RTUs, and MTUs, where each of these devices could access a quantum computer for information processing and obtain quantum hardware fingerprints or QPUF signatures. For QKD communication, along with quantum, a classical channel is also required to establish communication securely by exchanging bit-level information.

Each of the smart electronic devices or Industrial Internet-of-Things (IIoT) in the SCADA-grid framework is assumed to be

quantum-enabled and can access quantum hardware to obtain a unique quantum digital fingerprint referred to as a QPUF key. The initialization input or challenge is securely retrieved each time to uniquely generate a QPUF key for each IIoT device during attestation. QKD protocols help in securely establishing a secret session key for communication among smart grid entities. For successfully establishing the secret keys, QKD requires a quantum communication channel for transmitting the quantum states. Smart grid applications involve a myriad of tasks such as demand response management, substation protection, load shedding, etc. This research assumes all RTUs, MTUs, and servers in the smart grid have quantum capabilities and have access to quantum computers, and each node can be considered a quantum node with a unique QPUF-generated fingerprint that can further enhance the integrity in QKD communication. The smart grid nodes can establish secure communication through QKD by establishing a session based mutual authentication and data exchange using QPUF as detailed in Fig. 3.

In the proposed framework, the photon polarization bases considered for encoding qubits are as follows: 0^o and 135^o representing state 0, and 90^o and 45^o representing state 1. Alice randomly selects either a rectilinear or diagonal basis to perform encoding. These encoded qubits are then shared with Bob, where each of these qubits is measured randomly using a different basis. For example, a qubit encoded using a rectilinear basis by Alice may be measured by Bob using a diagonal basis. After the transmission, Alice and Bob compare their chosen basis for each bit without revealing the actual bit values. The final shared session key is obtained by choosing the bit positions with the matching basis on both sides.

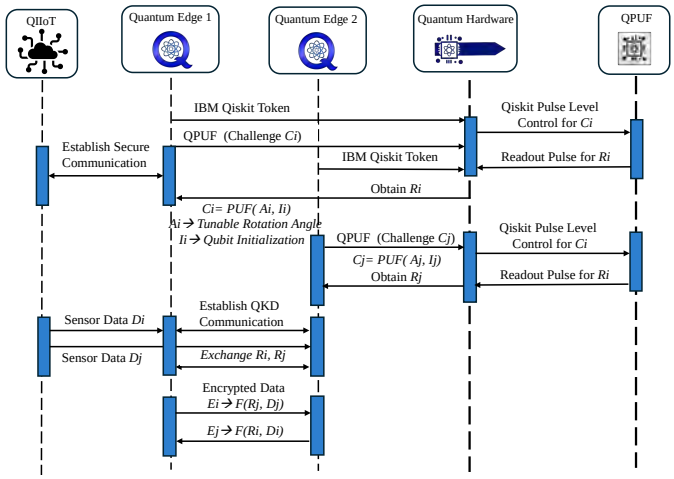


Figure 3: Proposed QPUF-QKD Integrated framework for Smart Grid

5 Experimental Results

For QPUF evaluation, this research implements the QPUF topology as presented in [3], utilizing an 8-qubit architecture, as shown in Fig.4a. The QPUF circuit comprises 8 quantum and classical registers. The circuit utilizes Hadamard, CNOT, Ry, and measurement gates to manipulate and measure the quantum states. Hadamard gate drives the qubits into superposition, while the CNOT gate establishes quantum entanglement such that the quantum state change of one qubit affects the other. The Ry gate introduces tunable rotation, inducing controlled variability in the quantum state of a qubit, which is crucial for achieving unclonability and unpredictability in QPUFs. Finally, the measurement gate performs the quantum state measurement where the qubit's state is collapsed into binary values and stored in classical registers. Furthermore, QPUF response randomness from IBM qasm_simulator was calibrated and presented in Fig. 4b.

The QPUF was deployed on IBM quantum systems, which include 127-qubit Eagle R3 processors, offering higher qubit coherence times and improved gate fidelities. The QPUF responses were calibrated by leveraging unique physical characteristics of quantum hardware, such as decoherence and coherence times, qubit resonant frequencies, gate fidelities, and readout assignment errors. The proposed QPUF topology, composed of quantum logic gates, was implemented and tested on ibm_brisbane backend and simulator using Qiskit [25], a python quantum programming framework from IBM. The reliability of QPUF on ibm_brisbane was validated by successfully regenerating 6 of the 10 QPUF responses across all three instances. As shown in Fig. 4c, the QPUF reliability evaluation demonstrates the robustness of the QPUF topology under the Noisy quantum computation on ibm_brisbane system, as shown in Fig. 5.

The QPUF was evaluated across three instances on the hardware backend, with each instance generating 10 QPUF keys. These keys were analyzed to assess their stability, intra-uniqueness, which measures their variance under different initialization parameters. Furthermore, the QPUF circuit was also deployed on Rigetti Computing's 8-qubit Quantum Virtual Machine (8q-qvm) using Pyquil [24], a Python library designed for programming on Rigetti quantum systems and simulators [12].

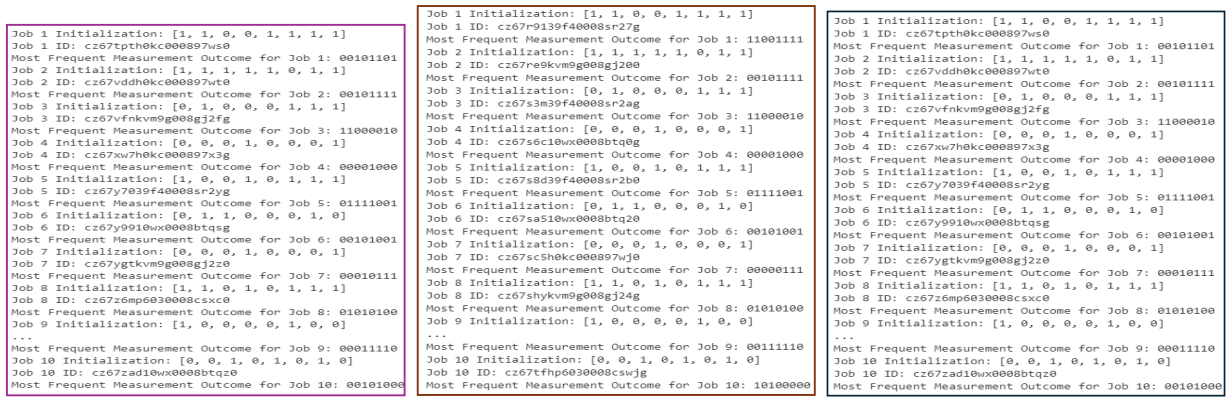
Rigetti Computing's superconducting qubit-based quantum hardware serves as an excellent platform for QPUF performance analysis alongside IBM quantum systems. Like IBM, Rigetti quantum systems utilize superconducting quantum, implemented through lithographically defined chip-based architectures. These systems support fast gate operations and offer improved qubit coherence and gate fidelity essential for fault-tolerant quantum computing [23]. The QPUF performance analysis on Rigetti's quantum virtual machine is presented in Fig. 6. An Intra-hamming distance of 50.37% was obtained across all 100 QPUF keys. Furthermore, the average uniformity of QPUF keys was observed to be 51.3% across all QPUF keys by evaluating the probability of each qubit to obtain 1 which indicates a well-balanced random response distribution.

The QKD protocol was implemented based on the available code from [16] and executed via Google Cirq, a quantum computing framework from Google [9].

The proposed QKD protocol was evaluated on Cirq's quantum simulator, where random basis was established and shared secret key was successfully generated to facilitate a secure session between Alice and Bob. To ensure confidentiality, Vernam cipher was used to perform secure encryption of QPUF key by performing XOR

(a) Proposed QPUF Topology [3] (b) QPUF Randomness (c) QPUF Stability

Figure 4: Performance Evaluation of QPUF on ibm_brisbane



```
Job 1 Initialization: [1, 1, 0, 0, 1, 1, 1, 1]
Job 1 ID: cz67tpth0kc000897ws0
Most Frequent Measurement Outcome for Job 1: 00101101
Job 2 Initialization: [1, 1, 1, 1, 1, 0, 1, 1]
Job 2 ID: cz67vddh0kc000897wt0
Most Frequent Measurement Outcome for Job 2: 00101111
Job 3 Initialization: [0, 1, 0, 0, 0, 1, 1, 1]
Job 3 ID: cz67vfnkvm9g008gj2fg
Most Frequent Measurement Outcome for Job 3: 11000010
Job 4 Initialization: [0, 0, 0, 1, 0, 0, 0, 1]
Job 4 ID: cz67xw7h0kc000897x3g
Most Frequent Measurement Outcome for Job 4: 00001000
Job 5 Initialization: [1, 0, 0, 1, 0, 1, 1, 1]
Job 5 ID: cz67y7039f40008sr2yg
Most Frequent Measurement Outcome for Job 5: 01111001
Job 6 Initialization: [0, 1, 1, 0, 0, 0, 1, 0]
Job 6 ID: cz67y9910wx0008btqsg
Most Frequent Measurement Outcome for Job 6: 00101001
Job 7 Initialization: [0, 0, 0, 1, 0, 0, 0, 1]
Job 7 ID: cz67ygtkvm9g008gj2z0
Most Frequent Measurement Outcome for Job 7: 00010111
Job 8 Initialization: [1, 1, 0, 1, 0, 1, 1, 1]
Job 8 ID: cz67z6mp6030008csxc0
Most Frequent Measurement Outcome for Job 8: 01010100
Job 9 Initialization: [1, 0, 0, 0, 0, 1, 0, 0]
...
Most Frequent Measurement Outcome for Job 9: 00011110
Job 10 Initialization: [0, 0, 1, 0, 1, 0, 1, 0]
Job 10 ID: cz67zad10wx0008btqz0
Most Frequent Measurement Outcome for Job 10: 00101000
```

(a) ibm_brisbane instane-1

```
Job 1 Initialization: [1, 1, 0, 0, 1, 1, 1, 1]
Job 1 ID: cz67r9139f40008sr27g
Most Frequent Measurement Outcome for Job 1: 11001111
Job 2 Initialization: [1, 1, 1, 1, 1, 0, 1, 1]
Job 2 ID: cz67re9kvm9g008gj200
Most Frequent Measurement Outcome for Job 2: 00101111
Job 3 Initialization: [0, 1, 0, 0, 0, 1, 1, 1]
Job 3 ID: cz67s3m39f40008sr2ag
Most Frequent Measurement Outcome for Job 3: 11000010
Job 4 Initialization: [0, 0, 0, 1, 0, 0, 0, 1]
Job 4 ID: cz67s6c10wx0008btq0g
Most Frequent Measurement Outcome for Job 4: 00001000
Job 5 Initialization: [1, 0, 0, 1, 0, 1, 1, 1]
Job 5 ID: cz67s8d39f40008sr2b0
Most Frequent Measurement Outcome for Job 5: 01111001
Job 6 Initialization: [0, 1, 1, 0, 0, 0, 1, 0]
Job 6 ID: cz67sa510wx0008btq20
Most Frequent Measurement Outcome for Job 6: 00101001
Job 7 Initialization: [0, 0, 0, 1, 0, 0, 0, 1]
Job 7 ID: cz67sc5h0kc000897wj0
Most Frequent Measurement Outcome for Job 7: 00000111
Job 8 Initialization: [1, 1, 0, 1, 0, 1, 1, 1]
Job 8 ID: cz67shykvm9g008gj24g
Most Frequent Measurement Outcome for Job 8: 01010100
Job 9 Initialization: [1, 0, 0, 0, 0, 1, 0, 0]
...
Most Frequent Measurement Outcome for Job 9: 00111110
Job 10 Initialization: [0, 0, 1, 0, 1, 0, 1, 0]
Job 10 ID: cz67tfhp6030008cswjg
Most Frequent Measurement Outcome for Job 10: 10100000
```

(b) ibm_brisbane instane-2

```
Job 1 Initialization: [1, 1, 0, 0, 1, 1, 1, 1]
Job 1 ID: cz67tpth0kc000897ws0
Most Frequent Measurement Outcome for Job 1: 00101101
Job 2 Initialization: [1, 1, 1, 1, 1, 0, 1, 1]
Job 2 ID: cz67vddh0kc000897wt0
Most Frequent Measurement Outcome for Job 2: 00101111
Job 3 Initialization: [0, 1, 0, 0, 0, 1, 1, 1]
Job 3 ID: cz67vfnkvm9g008gj2fg
Most Frequent Measurement Outcome for Job 3: 11000010
Job 4 Initialization: [0, 0, 0, 1, 0, 0, 0, 1]
Job 4 ID: cz67xw7h0kc000897x3g
Most Frequent Measurement Outcome for Job 4: 00001000
Job 5 Initialization: [1, 0, 0, 1, 0, 1, 1, 1]
Job 5 ID: cz67y7039f40008sr2yg
Most Frequent Measurement Outcome for Job 5: 01111001
Job 6 Initialization: [0, 1, 1, 0, 0, 0, 1, 0]
Job 6 ID: cz67y9910wx0008btqsg
Most Frequent Measurement Outcome for Job 6: 00101001
Job 7 Initialization: [0, 0, 0, 1, 0, 0, 0, 1]
Job 7 ID: cz67ygtkvm9g008gj2z0
Most Frequent Measurement Outcome for Job 7: 00010111
Job 8 Initialization: [1, 1, 0, 1, 0, 1, 1, 1]
Job 8 ID: cz67z6mp6030008csxc0
Most Frequent Measurement Outcome for Job 8: 01010100
Job 9 Initialization: [1, 0, 0, 0, 0, 1, 0, 0]
...
Most Frequent Measurement Outcome for Job 9: 00011110
Job 10 Initialization: [0, 0, 1, 0, 1, 0, 1, 0]
Job 10 ID: cz67zad10wx0008btqz0
Most Frequent Measurement Outcome for Job 10: 00101000
```

(c) ibm_brisbane instane-3

Figure 5: QPUF Calibration on ibm_brisbane

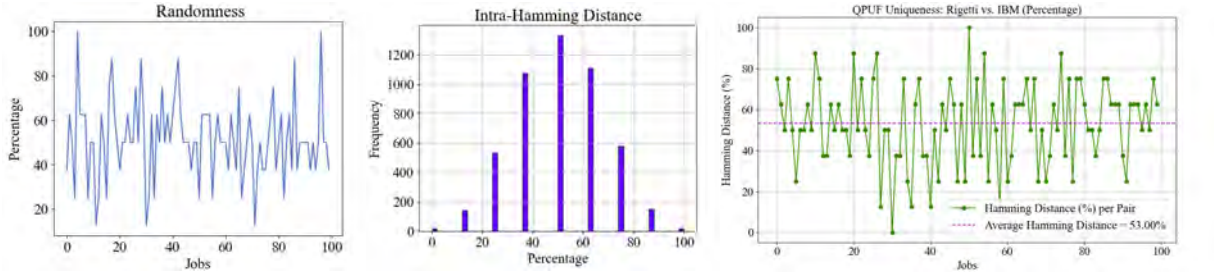


Figure 6: QPUF Performance Analysis on Rigetti's 8-Qubit Quantum Virtual Machine

operation of the secret key and QPUF key as can be seen in Fig. 7 The encrypted QPUF key was then transmitted over a quantum channel, ensuring that only the authenticated quantum-enabled smart grid edge devices could securely recover the QPUF key and establish as QPUF-secure communication session.

The QKD computational time analysis, presented in Table 3, provides the execution times for key phases in QKD: state preparation, transmission, elimination, and key encryption times during the QKD protocol. During state preparation, both Alice and Bob initialize their parameters by generating random bit sequences

Table 3: Computational Time Analysis of QKD

Phase	Time (S)
Preparation Phase	0.00153
Transmission Phase	0.04766
Elimination Phase	0.00321
Encryption and Decryption Phase	0.00057

and selecting the corresponding basis. In the transmission phase, Alice sends polarized photons to Bob via the quantum channel, while Bob measures incoming qubits using polarized filters. In the

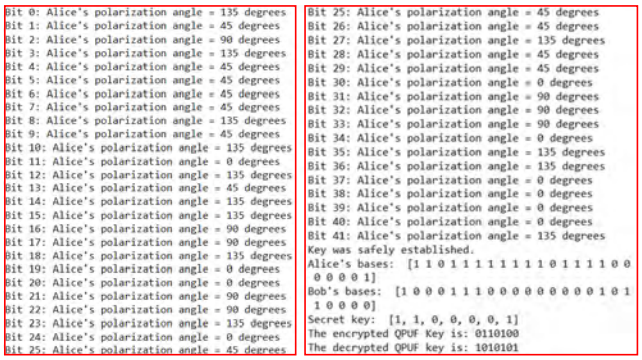


Figure 7: QKD Protocol for Secure QPUF Key Exchange

elimination stage, Alice and Bob compare their basis and discard measurements with mismatching bases to establish a shared secret key. In the final Encryption and Decryption phase, secure QPUF key exchange is performed using Vernam cipher, where the QPUF key is encrypted by applying an XOR operation with the QKD-generated session key.

6 Conclusion

This research work presents and validates a QPUF-QKD integrated framework for secure communication within SCADA-Grid infrastructures using both QPUF and QKD. The proposed framework demonstrates secure QKD communication for transmitting QPUF keys from IBM and Rigetti quantum systems. The proposed framework demonstrates secure QKD communication among smart grid entities, where each entity obtains a QPUF-generated key and can communicate through the quantum channel securely.

By deploying QPUF on Rigetti's superconducting qubit-based architecture, distinct from but similar to IBM's systems, the evaluation highlights its compatibility and consistent performance and reliability of QPUF across different quantum hardware ecosystems. Future research could extend the proposed framework to various other quantum hardware and integrate other quantum cryptography algorithms with QPUF, thereby expanding the scope of the proposed QPUF-QKD in securing emerging Quantum Internet-of-Things and Quantum Artificial Intelligence applications.

References

[1] Shubhani Aggarwal and Georges Kaddoum. 2024. Authentication of Smart Grid by Integrating QKD and Blockchain in SCADA Systems. *IEEE Transactions on Network and Service Management* 21, 5 (October 2024), 5768–5780. https://doi.org/10.1109/tnsm.2024.3423762

[2] Muneer Alshowkan, Philip G. Evans, Michael Starke, Duncan Earl, and Nicholas A. Peters. 2022. Authentication of smart grid communications using quantum key distribution. *Scientific Reports* 12, 1 (July 2022). https://doi.org/10.1038/s41598-022-16090-w

[3] Venkata K. V. V. Bathalapalli, Saraju P. Mohanty, Chenyun Pan, and Elias Kougianos. 2024. QPUF 2.0: Exploring Quantum Physical Unclonable Functions for Security-by-Design of Energy Cyber-Physical Systems. https://doi.org/10.48550/ARXIV.2410.12702

[4] BBC News. 2019. Technology Article. https://www.bbc.com/news/technology-49125853 Accessed: 2025-03-02.

[5] Basudeb Bera, Ashok Kumar Das, and Biplab Sikdar. 2025. Securing Next-Generation Quantum IoT Applications using Quantum Key Distribution. *IEEE Internet of Things Magazine* 8, 1 (January 2025), 50–56. https://doi.org/10.1109/iotm.001.2400059

[6] Franco Cirillo and Christian Esposito. 2024. Practical Evaluation of a Quantum Physical Unclonable Function and Design of an Authentication Scheme. In *Proc. IEEE International Conference on Quantum Computing and Engineering (QCE)*. IEEE, 1354–1363. https://doi.org/10.1109/qce60285.2024.00161

[7] CNBC News. 2019. DDoS Attack Caused Interruptions in Power System Operations: DOE. https://www.cnbc.com/2019/05/02/ddos-attack-caused-interruptions-in-power-system-operations-doe.html Accessed: 2025-03-02.

[8] Hua Dai, Xin Sun, Bang Lv, Hongyan Wang, and Liang Tong. 2024. Multi-Scenario Quantum Key Distribution Mechanism for Power Grid Terminals. In *Proc. 12th International Conference on Information Systems and Computing Technology (ISCTech)*. IEEE, 1–5. https://doi.org/10.1109/isctech63666.2024.10845578

[9] Cirq Developers. 2025. Cirq. https://doi.org/10.5281/ZENODO.4062499

[10] E-ISAC and SANS. 2016. *Analysis of the Cyber Attack on the Ukrainian Power Grid.* Technical Report. https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf Accessed: 2025-03-02.

[11] Sawdah Farooq, Parth Sharma, and Pyari Mohan Pradhan. 2024. Enhanced Security Framework For MQTT Protocol Based IoT Network Using Quantum Key Distribution. In *Proc. 27th International Symposium on Wireless Personal Multimedia Communications (WPMC)*. IEEE, 1–5. https://doi.org/10.1109/wpmc63271.2024.10863467

[12] Peter J Karalekas, Nikolas A Tezak, Eric C Peterson, Colm A Ryan, Marcus P da Silva, and Robert S Smith. 2020. A quantum-classical cloud platform optimized for variational hybrid algorithms. *Quantum Science and Technology* 5, 2 (apr 2020), 024003. https://doi.org/10.1088/2058-9565/ab7559

[13] Mansoor Ali Khan, Muhammad Naveed Aman, and Biplab Sikdar. 2024. Soteria: A Quantum-Based Device Attestation Technique for Internet of Things. *IEEE Internet of Things Journal* 11, 9 (May 2024), 15320–15333. https://doi.org/10.1109/jiot.2023.3346397

[14] Peng-Yong Kong. 2022. A Review of Quantum Key Distribution Protocols in the Perspective of Smart Grid Communication Security. *IEEE Systems Journal* 16, 1 (March 2022), 41–54. https://doi.org/10.1109/jsyst.2020.3024956

[15] Hosakota Vamshi Krishna and Krovi Raja Sekhar. 2024. Enhancing security in IIoT applications through efficient quantum key exchange and advanced encryption standard. *Soft Computing* 28, 3 (January 2024), 2671–2681. https://doi.org/10.1007/s00500-023-09585-9

[16] Lea318. 2024. BB84 Protocol Implementation. https://github.com/lea318/BB84. Accessed: 2025-03-08.

[17] Yuancheng Li, Pan Zhang, and Rong Huang. 2019. Lightweight Quantum Encryption for Secure Transmission of Power Data in Smart Grid. *IEEE Access* 7 (2019), 36285–36293. https://doi.org/10.1109/access.2019.2893056

[18] Lan-Huong Nguyen, Van-Linh Nguyen, Ren-Hung Hwang, Jian-Jhih Kuo, Yu-Wen Chen, Chien-Chung Huang, and Ping-I Pan. 2024. Towards Secured Smart Grid 2.0: Exploring Security Threats, Protection Models, and Challenges. *IEEE Communications Surveys and Tutorials* (2024), 1–1. https://doi.org/10.1109/comst.2024.3493630

[19] Kumar Nilesh, Christian Deppe, and Holger Boche. 2024. Quantum PUF and its Applications with Information Theoretic Analysis. In *Proc. IEEE 10th World Forum on Internet of Things (WF-IoT)*. IEEE, 1–6. https://doi.org/10.1109/wf-iot62078.2024.10811185

[20] V. Padamvathi, B. Vishnu Vardhan, and A.V.N. Krishna. 2016. Quantum Cryptography and Quantum Key Distribution Protocols: A Survey. In *Proc. IEEE 6th International Conference on Advanced Computing (IACC)*. IEEE, 556–562. https://doi.org/10.1109/iacc.2016.109

[21] Rohini Poolat Parameswarath, Chao Wang, and Biplab Sikdar. 2024. A Quantum Safe Mutual Authentication Protocol for Smart Meter Communications With Experimental Evaluation. *IEEE Transactions on Network Science and Engineering* 11, 5 (September 2024), 5058–5072. https://doi.org/10.1109/tnse.2024.3427110

[22] Kumar Prateek, Meghashrita Das, Sairaaj Surve, Soumyadev Maity, and Ruhul Amin. 2024. Q-Secure-P²-SMA: Quantum-Secure Privacy- Preserving Smart Meter Authentication for Unbreakable Security in Smart Grid. *IEEE Transactions on Network and Service Management* 21, 5 (October 2024), 5149–5163. https://doi.org/10.1109/tnsm.2024.3357103

[23] Rigetti Computing. 2025. What We Build. https://www.rigetti.com/what-we-build Accessed: 2025-04-13.

[24] Robert S. Smith, Michael J. Curtis, and William J. Zeng. 2016. A Practical Quantum Instruction Set Architecture. arXiv:1608.03355 [quant-ph]

[25] Qiskit Development Team. 2023. qiskit-ibm-runtime. https://github.com/Qiskit/qiskit-ibm-runtime. Accessed: 2025-04-15.

[26] Wikipedia contributors. 2025. Metcalf Sniper Attack. https://en.wikipedia.org/wiki/Metcalf_sniper_attack Accessed: 2025-03-02.

[27] Jian Xiong, Lu Shen, Yan Liu, and Xiaofen Fang. 2025. Enhancing IoT security in smart grids with quantum-resistant hybrid encryption. *Scientific Reports* 15, 1 (January 2025). https://doi.org/10.1038/s41598-024-84427-8