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

Venkata K. V. V. Bathalapalli, *Graduate Student Member, IEEE*, Saraju P. Mohanty, *Senior Member, IEEE*, Chenyun Pan, *Senior Member, IEEE*, and Elias Kougianos, *Senior Member, IEEE*

***Abstract*—Sustainable advancement is being made to improve the efficiency of the generation, transmission, and distribution of renewable energy resources, as well as managing them to ensure the reliable operation of the smart grid. Supervisory control and data acquisition (SCADA) enables sustainable management of grid communication flow through its real-time data sensing, processing, and actuation capabilities at various levels in the energy distribution framework. The security vulnerabilities associated with the SCADA-enabled grid infrastructure and management could jeopardize the smart grid operations. This work explores the potential of Quantum Physical Unclonable Functions (QPUF) for the security and reliability of the smart grid's energy transmission and distribution framework. Quantum computing has emerged as a formidable security solution for high-performance computing applications through its probabilistic nature of information processing. This work has a quantum hardware-assisted security mechanism based on intrinsic properties of quantum hardware driven by quantum mechanics to provide tamper-proof security for quantum computing-driven smart grid infrastructure. This work introduces a novel QPUF architecture using quantum logic gates based on quantum decoherence, entanglement, and superposition. This generates a unique bitstream for each quantum device as a fingerprint. The proposed QPUF design is evaluated on IBM and Google quantum systems and simulators. The deployment on IBM quantum (ibmq_qasm_simulator) and Google Cirq simulators has achieved 100% reliability with an average Hamming distance of 50.07%, 51% randomness.**

***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

The advancement of electrical grids is required for enhanced power quality management, outage control, customer demand forecasting, and power supply distribution. The Smart Grid evolves from the technological integration of various state-of-the-art technologies that automate the electrical distribution processes. The smart integration of electronic devices provides real time data sensing and processing capabilities that help monitor outages, power turbulence, and metering infrastructure [1]. Technological integration improves efficiency and increases reliability. The Internet-of-Things (IoT) offers communication, control, and computation capabilities to the smart grid and enhances the communication and data processing flow in grid operations [2]. The Smart Grid conceptual model by the National Institute of Standards and Technology (NIST) is depicted in Fig. 1. Along with

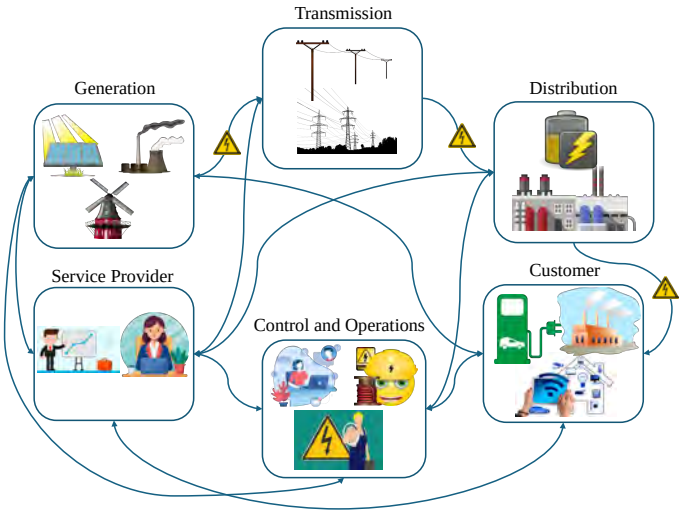



Fig. 1: NIST Smart Grid Conceptual Model [3]

the automation and advancement of energy infrastructure, generating and distributing renewable energy from various sources and managing their integration is a challenge. Optimizing the grid functions and managing the distribution of resources requires a comprehensive approach. SCADA enables the management of generation, transmission, distribution, and control of energy in a Smart Grid. Its functionalities include managing grid operations, power quality, outage control, real-time demand analysis, and customer management [4]. The salient features of a SCADA-enabled smart grid are:

- An efficient power demand response and management.
- Improved power quality with real-time power metric monitoring and control.
- A sustainable renewal energy resources distribution and management.
- A simple and lightweight bi-directional communication framework among various entities in the energy distribution and control framework.
- A sustainable approach with reduced usage of greenhouse gas emissions.
- An efficient electricity trading approach by analyzing energy usage forecast and the microgrid's distribution efficiency.
- A simple power outage control and self-healing capability with the integration of protective relays.

Venkata K. V. V. Bathalapalli and Saraju P. Mohanty are with Department of Computer Science and Engineering, University of North Texas, Denton, TX. (e-mail: vb0194@unt.edu; saraju.mohanty@unt.edu).

Chenyun Pan is with Department of Electrical Engineering, University of Texas at Arlington, Arlington, TX. (e-mail: chenyun.pan@uta.edu).

Elias Kougianos is with Department of Electrical Engineering, University of North Texas, Denton, TX. (e-mail: elias.kougianos@unt.edu).

- An intelligent energy metering infrastructure with sustainable customer data protection and privacy-enhanced communication flow.

SCADA enables secure analysis and control of communication in the grid infrastructure. It consists of Remote Terminal Units (RTUs) that monitor various energy generation metrics through electronic devices at the base stations and control the electricity transmission process. On-field electronic devices perform data sensing of various electric parameters and relay data to the control center. The control center then initiates decision making and actuation processes, ensuring quality power supply and distribution [5]. The heterogeneous nature of IoT devices and their diverse functionalities within a smart grid introduces significant security vulnerabilities. These arise from bi-directional communication flows, the integration of varied electronic components, and the handling of customers' personally identifiable information (PII). These complexities expand the attack surface with the potential for data breaches, device hijacking, and malicious command injections.

Security-by-Design (SbD) emphasizes the security of a system from the design or manufacturing stage and enhances the trust and confidentiality of the device and data as a default functionality. Prominent SbD primitives include PUF and Trusted Platform Module (TPM) and offer resource efficient security to smart electronic devices. The PUF-based approach provides a unique digital fingerprint for a smart electronic device using its inherent properties and offers reliable and tamper-proof security. The growth of semiconductor technology and the increasing market of IoT devices is estimated to reach trillions by 2030, making PUF an efficient security primitive for the sustainable application of IoT devices. Quantum computing can enhance information processing capability using the principles of quantum mechanics and has seen huge development, particularly with the advancement of superconducting quantum computing with underlying hardware built using silicon. This research proposes a novel approach for extracting a fingerprint from quantum computers based on quantum superposition, entanglement, and decoherence principles. The proposed QPUF 2.0 framework introduces a novel approach for extracting bitstream responses generated by the QPUF circuit on inherently noisy quantum computers. The QPUF leverages quantum process variations to enable secure communication among entities within a smart grid infrastructure managed via SCADA systems. A conceptual idea of Quantum secured Energy-Cyber-Physical-System infrastructure is presented in Fig. 2.

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

## II. Overview of Smart Grid

In this section, a conceptual overview of the smart grid is presented and its communication framework as defined by the National Institute of Standards and Technology (NIST) is discussed. [3].

A smart grid is an automated control system that enables efficient communication, self-healing capabilities, and effective management of distributed energy resources. The term smart grid is coined to define a technologically enhanced and efficient electrical power grid with robust control and automation of energy generation, transmission, and distribution [6]. The complexity involved in conventional power grids, where a top-down approach has a one-directional power flow from the generation subsystem to the consumer subsystem, has proven to be inefficient with increasing electricity usage demand and renewable energy resource integration and management. The bi-directional information flow increases efficiency and improves energy resource management with an advanced communication infrastructure that includes protective relays, IEDs, and circuit breakers performing data sensing, actuation, and processing in real-time [7].

Smart Substations (SS) play an important role in the electrical distribution framework. The main functionalities include voltage control, equipment monitoring, and fail-safe protection. Substations operate at AC/DC voltage and have a step-up transformer to increase the voltage to transfer power over long distances. A step-down transformer enables lowering the voltage for efficient compliance with the electrical power voltage at the customer. The SS enables fail-safe protection by monitoring the electrical system power plow, identifying any malfunctioning equipment, and issues with voltage control through the advanced SCADA-based real-time monitoring and control using protective relays. Relays play an important role in grid infrastructure management with the functionalities that include self-healing, monitoring equipment faults, and regulating voltage and current fluctuations [7].

### A. Supervisory Control and Data Acquisition (SCADA)

SCADA facilitates intelligent management and control of various critical infrastructures such as telecommunication, power plants, and industries. SCADA systems include smart electronic devices facilitating intelligent data sensing for monitoring various critical parameters, which then relay data to a centralized control system for processing and analysis through a Human Machine Interface (HMI). In electrical distribution and monitoring systems, the **Intelligent Electronic Devices** perform data sensing related to power metrics, which helps in monitoring the power quality and its transmission.

IEDs along with **Phasor Measurement Units (PMU)** have various functionalities that include protective relaying, voltage and power frequency estimation at electrical distribution lines, power equipment data processing with microseconds resolution, and voltage control. These devices also include

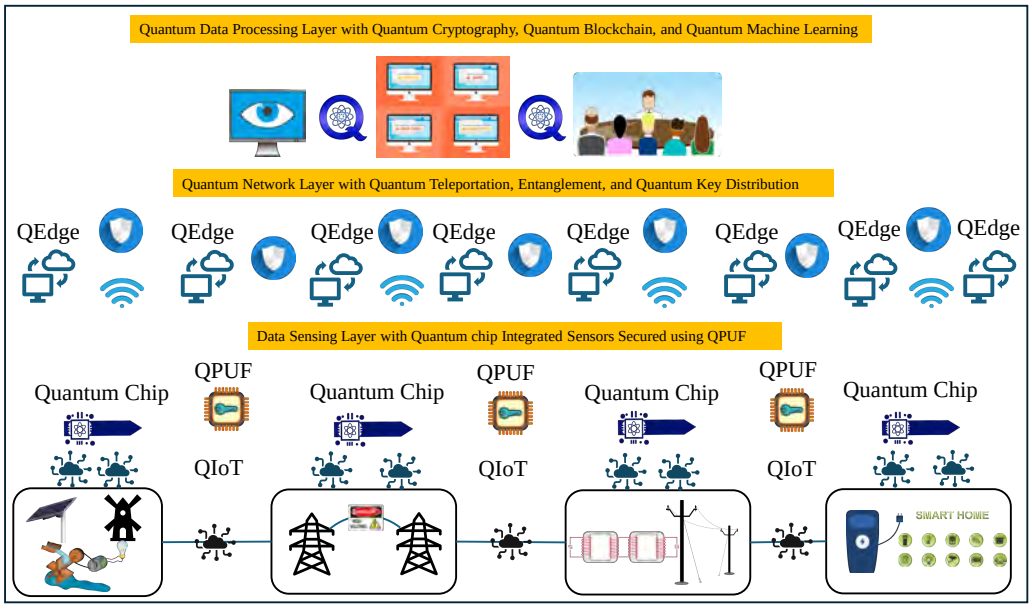



Fig. 2: Quantum Computing-Enabled Smart Grid Framework

actuators that perform operations based on commands from **Remote Terminal Unit (RTU)**, which is a gateway for controlling the sensors and actuators at a base station. IEDs are integrated microprocessor controllers for monitoring the power system equipment. IEDs consist of voltage and current sensors to obtain power metric measurements, wired, wireless, and serial communication modules to interface with RTU, power supply inputs, onboard memory, and analog-to-digital converters [8].

RTUs have communication capabilities to connect with IEDs and relays at various subsystems, enabling remote control, monitoring, and actuation. On top of RTUs, the **Master Terminal Units (MTUs)** provide high-level system control logic and communicate with RTUs and centralized command control for data analysis, processing, and storage through HMI [7], [9]. The operator/command center is part of SCADA systems and supports HMI. Communication among various RTUs and MTUs is facilitated using wired and wireless technologies such as ModBus, DNP3, and optical fiber-based infrastructure. Programmable Logic Controllers (PLC) in SCADA are centralized electrical control systems that communicate with IEDs at the physical layer through RTUs [10]. Modern RTUs can communicate with IEDs located at substations through the RS-485 serial communication protocol. RTUs receive AC measurement inputs from voltage transformers and current transformers and perform fault detection in real-time [11]. MTUs and RTUs work in a master/slave architecture where MTUs provide control logic and RTUs control IEDs. The communication and control of the power distribution framework in SCADA are presented in Fig. 3.

### *B. Smart Grid Infrastructure*

The smart grid infrastructure has bidirectional information and power flow. Smart grid monitoring includes managing grid reliability, failure protection, and power equipment monitoring in its infrastructure which are essential for ensuring power quality. Electricity generation and transmission in a smart grid can be facilitated at various sources like smart farms with advanced solar cells, electricity trading from smart homes, and electric car charging stations. Various Blockchain-based solutions for energy trading have been explored where a smart and automated way of energy trading between a user at a smart home and grid can be facilitated in real-time. Similarly, electric vehicle-grid communication facilitates energy trading from a charging station when required to reduce the load on the grid. These approaches help in demand management during extreme weather conditions which can increase electricity usage.

The *Microgrid* is an emerging smart grid subsystem with autonomy to island power generation, transmission, and distribution. The low-voltage electricity from various renewable energy resources, from solar panels at home and wind turbines at farms, can be disconnected from the macro grid and can drive the energy requirements of individual consumers without relying on the macro grid. A microgrid requires an efficient communication infrastructure with enhanced reliability and authentication protocols for ensuring the secure operation of the microgrid [10].

### *C. Cybersecurity Issues in Smart Grid*

The data processing and communication flow in the energy distribution framework is facilitated using SCADA, which has various entities with diverse communication and information processing capabilities. Providing a secure and efficient power supply framework without any security vulnerability is a challenging task due to the heterogeneity of various devices and their applications.

*Data Integrity Attacks* could arise when an adversary can intercept the communication between field sensors or IEDs and RTUs and possibly gain access to these devices and perform

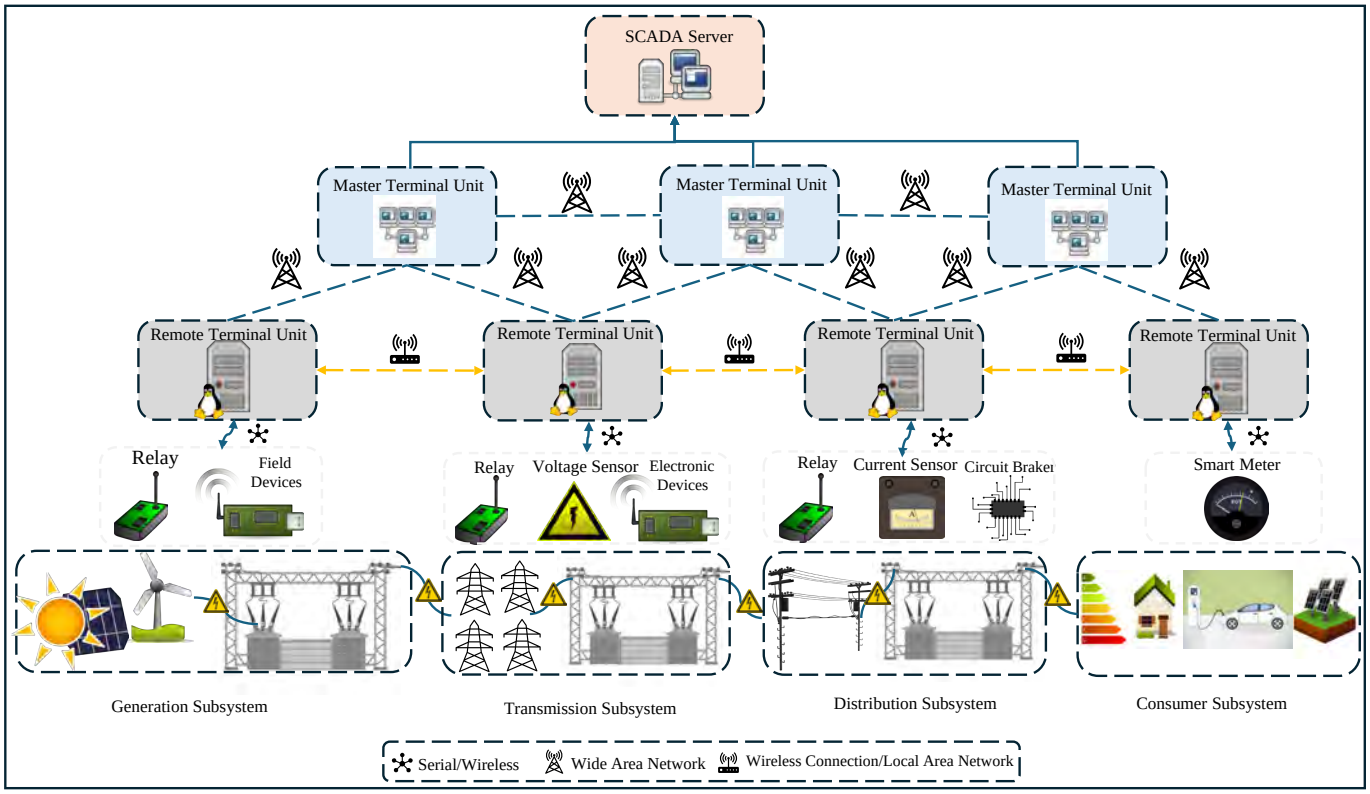



Fig. 3: Architecture of Smart Grid

sniffing and snooping attacks. The Modbus communication protocol is used for sensor data transmission between RTUs and field sensors. The lack of standard benchmarks for security metrics associated with this protocol could jeopardize the communication framework of these devices. The SCADA's control unit, receiving the sensor data, cannot validate the trustworthiness of the data or verify the identity of IEDs, which validates the requirement for a sensor integrity verification scheme [12].

*Availability* of power system resources and their reliable operations is facilitated through effective control and management of protective relays and smart electronic devices monitoring power metrics. Unauthorized access and control through spoofing and repudiation can reduce the trustworthiness of smart grid operations, where an adversary can replace a fake node with a reliable node and obtain access to communication.

*Privacy* of consumer information and its authorized secure access is a prime requirement of advanced metering infrastructure. An adversary can extract power consumption analysis data from smart meters which can be vulnerable to various cyber-attacks due to their open working environment and can pose a threat to individual consumer privacy [13].

### *D. Quantum Security-by-Design (QSbD)*

SbD focuses on a sustainable consumer-level electronic system with security built as a primitive at the design level. Adopting security practices to address the vulnerabilities and mitigate threats in smart electronics has proven to be inefficient due to the limited processing and power capabilities of smart electronic devices. Developing applications with built-in security practices is an effective way to mitigate threats. IoT applications require sustainable security both at the device and data level to counter any adversarial access that can jeopardize the integrity and authenticity of data [14]. Security-by-Design emphasizes the design and development stages combined with performing security risk analysis at various levels of application deployment and adopting security practices, ensuring sustainable security with a user-centric approach. Adopting a proactive approach to security enhances resiliency by integrating security primitives from the outset, rather than retrofitting them as reactive measures against threats and vulnerabilities in the emerging Internet-of-Everything (IoE) era. [15].

SbD works based on seven fundamental principles: 1) SbD approach should be proactive 2) Security/Privacy should be a default primitive at the design or system development stage 3) SbD should be completely embedded in the architecture enhancing resiliency of the system considering security risks 4) Facilitating end-end security 5) Full functionality with enhanced performance 6) User-centric 7) Visibility & Transparency [16].

The motivational idea of this research work can be a suitable approach for trusted authentication and secure communication in E-CPS driven by QSbD. QSbD is based on the principles of quantum mechanics, which drive the cryptographic, communication, information processing, and security functionalities in quantum computing.

The working principles of QSbD can be:

- A secure communication framework through quantum teleportation for trusted data transfer.
- A mutual device attestation technique using state-of-the-art quantum cryptography based on the principle of quantum state unclonability.
- A secure, unique device identity attestation functionality through quantum device fingerprinting using process variations.
- Information processing, storage, and attestation capabilities secured through the quantum digital signature mechanism.

### *E. Physical Unclonable Functions (PUF)*

PUF can enhance the trust and integrity of an electronic device by enabling secure digital fingerprint generation by mapping unique hardware-level properties as device fingerprints. A PUF is built based on IC technology that maps micro-manufacturing process variations to a unique cryptographic key. The unique PUF-generated identities cannot be tampered with or can be regenerated on other hardware [17] due to unclonable hardware characteristics, thereby making it a robust hardware-assisted security primitive.

A PUF has a challenge as input and response as output, where a random function maps the intrinsic hardware properties as a challenge input and generates a unique bitstream as response. A PUF on a chip, when tested with two challenge inputs $C_i$, $C_{i+1}$, will generate unique responses $R_i$, and $R_{i+1}$, respectively. The responses obtained will be unique since each challenge will work differently on the underlying hardware, resulting in unique responses ($R_i \neq R_{i+1}$). This reliability and tamper-proof hardware security primitive can also generate unique responses on different hardware with similar PUFs due to varying process variations during chip fabrication in IC development. The PUF module on device $d_1$ generating $R_1$ from $C_1$ will not be the same as $R_2$ generated from the same challenge $C_1$ on device $d_2$.

## III. Quantum Computing Background

This section provides a brief overview of quantum computing concepts, logic gates, hardware resources, and information processing capabilities.

### *A. Qubit Overview*

A Qubit is the basic unit of quantum information. Bits can exist only in one of the two states at a time, whereas a qubit can exist in the superposition of both 0 and 1 states at the same time [18]. In comparison to classical bits, qubits will have outputs with an equal probability of being 0 or 1 and are represented as follows: $|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$, $|1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$

The quantum state of a qubit is represented as $\begin{bmatrix}X\\Y\end{bmatrix}$. When the quantum state of a qubit is measured, $X^2$ is the probability of obtaining the 0 state and $Y^2$ is the probability of attaining the 1 state. Under normalization conditions, the squares of amplitudes of probabilities will be equal to 1.

$$|X|^2+|Y|^2=1.$$

The amount of information that can be represented by qubits is approximately half the number of classical bits required to represent the same information [19]. Various quantum hardware with diverse physical qubit control architectures is illustrated below:

*Superconducting Qubits* are most used in IBM quantum systems. The underlying hardware development includes the lithography process to pattern superconducting circuits made of niobium and depositing these materials on a silicon substrate. Qubit structures are created based on Josephson junctions that control the quantum state of qubits and their behavior by varying electromagnetic fields. These qubits work based on the principle of superconductivity, which defines a material working at extremely low temperatures and conducting current with zero resistance.

*Trapped Ion Qubits* work based on the internal energy of trapped ions to store, manipulate, and control the information processed by the qubits. IonQ uses trapped ion qubits in its quantum computing systems. Through a laser-based control on the ions, the qubits encoded at different energy levels inside an ion can be controlled.

*Topological Qubits* are built based on the topological states of quantum mechanics to achieve noise-free qubits. These qubits are used in Microsoft quantum systems and are controlled by manipulating their structure using chemical bonds.

*Quantum Dots:* Quantum Dots are tiny-sized semiconductor particles that carry electricity, and their energy levels are defined by the laws of quantum mechanics. These are tiny semiconductor particles where electrons are tightly packed, leading to the formation of energy levels. These energy levels can be manipulated through light or electricity.

### *B. Quantum Gates Overview*

Quantum gates are building blocks of quantum circuits and algorithms that support quantum state manipulation using various operators. In digital logic, AND, OR, NOT, and XOR gates work on bits and process the information. Analogous to digital logic, quantum logic gates work on quantum bits whose information state is a superposition of two states represented by the vectors [20], [21]. The quantum gates are either single or two qubit gates and are applied to qubits to manipulate their quantum state. When the state of a qubit is measured, it collapses to one of the two states: either 0 or 1. Fig. 4 shows the geometrical representation of a qubit's state changes when various quantum gates are applied [22]. Various single and two-qubit logic gates are:

*Pauli X-Gate:* The Pauli X-gate flips the quantum state of a qubit. If the quantum state is 1, it flips the state to 0 and vice versa. Its functionality is like a NOT gate in digital logic.

*Identity Gate:* The I-gate is similar to an identity gate or buffer, and it does not manipulate the qubit state and can

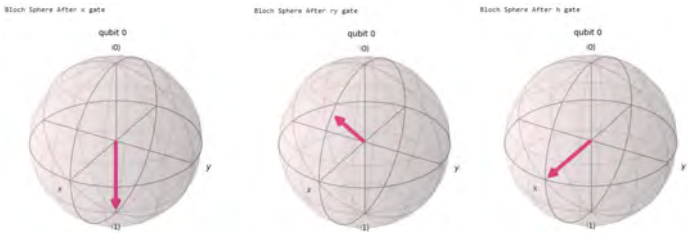


Fig. 4: Bloch Sphere Representation of Quantum State Variations of a Qubit

be used to retain the quantum state. This gate can introduce decoherence in the quantum state of a qubit by introducing a delay.

$$Igate\,|0\rangle = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = |0\rangle,$$

$$Igate\,|1\rangle = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} = |1\rangle$$

*Hadamard Gate:* The Hadamard gate is a single qubit quantum gate that manipulates the state of a qubit and places it in superposition. When the state of the superpositioned qubit is measured, it falls to either one of the two possible states, which are 0 or 1.

$$HGate = (1/\sqrt{2})\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

*RY Gate:* The RY gate is a single qubit tunable rotational quantum gate that performs qubit's state rotation around the y-axis of the Bloch Sphere. RY gate is used to place the qubit in an unknown quantum state, which can introduce more unpredictability.

*CNOT Gate*: The Controlled NOT gate is a two-qubit quantum gate that binds the quantum states of two qubits in such a way that the quantum state change of one qubit affects the other qubit. To realize CNOT, the target qubit will be driven by the control qubit's resonance frequency at the hardware level. Logically, the quantum state of the target qubit is flipped using an X-gate if the control qubit is in $|1\rangle$ state.

## IV. Related Research

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, and II.

A Quantum hardware verification approach using qubits' crosstalk was proposed in [23] using a QPUF which works on superconducting transmon qubits from IBM. Their work evaluated a QPUF design using a simple Hadamard gate application using a microwave pulse on the control qubit, and its impact on the target qubit due to crosstalk was explored. QPUF designs based on quantum logic gates using quantum superposition and decoherence phenomena were presented in [24]. Their work proposed a Hadamard gate based PUF to explore superposition phenomena and an idle gate driven design to study the impact of decoherence for realizing a unique bitstream as a PUF response. In comparison, we proposed a novel architecture in [25] based on the Hadamard gate QPUF proposed in the previous work [24] by supporting challenge-response pairs (CRP) generation and QPUF metric evaluation for various quantum systems from IBM. As an extension to [25], we proposed a framework for securing IIoT systems with a modified QPUF topology that works on leveraging quantum entanglement and superposition as driving principles for QPUF, and the obtained results have shown 100% reliability in [26].

A Quantum Readout (QR) PUF was proposed in [27], which works on a classical PUF. The PUF design is tested with challenges and responses in quantum states. The QR PUF is claimed to be more effective than a classical PUF as it is based on the no-cloning principle, which states that it is impossible to duplicate or clone the unknown quantum state of a qubit. A simple PUF-based key exchange protocol based on the quantum physical unclonability principle was presented in [28], 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 the no-cloning theorem was proposed in [29], which 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 [30], which works by storing the PUF signature inside an ultra-thin oxide and works based on manufacturing variations in an oxide. Our research on QPUF builds upon the topology presented in [31] by integrating the Quantum Key Distribution (QKD) protocol to ensure secure communication among smart grid entities, as proposed in QPUF 3.0 in [32].

Compared to the works presented in Table I, our proposed solution has several unique advantages:

1) General Hardware Compatibility: Unlike Li et al. [33] (which depends on specialized AlN photon emitters), our solution runs on standard quantum hardware without the need for exotic nanomaterials.
2) Practical Implementation: Rather than only providing theoretical limits (as in Kumar et al. [5]), we deliver an explicit circuit design and demonstrate it on real or simulated quantum devices.
3) Inherent Data Security: We eliminate the need for external encryption of CRPs (as done by Tun & Mambo et al. [40]) by using intrinsic quantum randomness and circuit design to protect keys. This reduces computational overhead on devices.
4) No Specialized Materials: In contrast to the nanoseed PUF proposed in [38], our method relies on conventional components and algorithms, simplifying manufacturing and integration.
5) Extended Functionality: Building on concepts like in [39] (which uses PUF+TRNG for simple ID), our solution supports not just fixed IDs but full dynamic challenge–response key generation and mutual device authentication in a network.

TABLE I: Classical and Quantum Hardware Security Primitives

| Research Work | Approach | Key Strengths | Weakness | Comparison with Current Work |
|---|---|---|---|---|
| Li et al. (2024) [33] | Single-photon quantum PUF | Extremely high unclonability, built-in QRNG, silicon-photonics integration | requires precise nanofabrication and specialized materials, early-stage prototype | Our solution uses standard quantum hardware rather than specialized nanomaterials. |
| Kumar et al. [34](2024) | Info-theoretic model of QPUF | Defines theoretical secret-key capacity | limits of QPUFs Purely analytical (no hardware or protocol design) | We provide a concrete architecture and experimental demonstration, not just theory. |
| Cirillo et al. (2025) [35] | Quantum PUF based on Qubit state bias | leverages inherent qubit errors, such as gate used for the entanglement, and readout errors | Designing QPUF challenges and application in cryptography | Our solution proposes scalable Challenge Response pair generation |
| Ghosh et al.(2024) [36] | Random von Neumann quantum state measurements | Claims Unforgeability using random measurement basis | NO evaluation of Uniqueness, randomness, and reliability | Our approach explicitly targets unique hardware randomness and focuses on integration with CPS architectures |
| **Classical PUF** | | | | |
| Goswami et al. (2025) [37] | Classical PUF + Quantum Entanglement | Quantum entanglement for hardware-based authentication | Authentication without quantum communication, requires secure pre-distribution or quantum channels | Our approach can obtain stronger unclonability due to quantum gate-level uniqueness |
| Ahn et al. [38] | Nanoseed PUF (optical+electrical randomness) | Vast on-demand keyspace, near-ideal randomness and uniqueness | Requires complex nanomaterials and custom algorithms; may be hard to manufacture | We achieve large key entropy without exotic materials, using conventional hardware logic. |
| Golofit et al. [39] | PUF + TRNG primitives for IoT devices | Ultra-lightweight security (XOR-based encryption, fixed-ID or variable response); no extra memory required | offers only basic ID/authentication; anonymity and advanced security require additional schemes | We support full challenge–response key generation and mutual authentication across devices. |
| Tun et al. (2024) [40] | Classical PUF + Homomorphic Encryption | Protects CRPs during transmission, resists CRP leakage and ML attacks | Heavy computational/communication overhead on IoT devices (encryption schemes) | Our design uses intrinsic quantum randomness to secure keys, avoiding expensive cryptography. |

***Related Research on Smart Grid Security:***

A novel Quantum Key Distribution (QKD) protocol for secure communication in Quantum computing applications was proposed in [41]. QKD protocol works based on the principle of Heisenberg's uncertainty principle. In this protocol, an unverified party can't intercept the communication on the Quantum channel between two trusted entities [42], [43]. In comparison to the works cited above, this work experimentally validates the QPUF design implemented using quantum Logic gates and clearly defines the QPUF signature generation process based on quantum mechanics principles that differentiate each quantum hardware.

For smart grid security and countering man-in-the-middle attacks, Quantum-Sim, a secure smart grid communication framework based on the Quantum key distribution (BB84) protocol, is proposed in [44]. A secure IoT device attestation framework using QPUF was presented in [45]. Their work proposed a QPUF mechanism based on the principles of quantum mechanics and the BB84 protocol.

A client's server handshaking protocol is validated with noisy quantum computers using a Hadamard gate-based QPUF design. A unique approach to fingerprint quantum servers executing quantum circuits from users based on the error rates of various quantum gates on different quantum devices is proposed in [46]. Using randomized benchmarking, error rates of various gates in different circuits with and without an identity gate, and their probability distributions of states are determined and evaluated in this work to identify the server.

A PUF-based approach for authenticating quantum computers is proposed in [47]. The SRAM PUF module has been used for fingerprinting quantum computers. This work is mainly based on implementing SRAM PUF at cryogenic temperatures. This work also examines the feasibility of SRAM PUFs in Quantum computers using liquid nitrogen to cool SRAM memories at -195 degrees Celsius. This work, however, can support a limited number of CRPs.

A PUF-based mutual authentication scheme for Vehicle to Grid (V2G) proposed in [48] focuses on secure communication among Vehicles, Charging Stations (CS), and Grid Servers. Bi-directional communication exists between CS and GS where CS communicates location, charging rate, duration, and energy demand forecast details with GS. Similarly, the EV shares the location details with GS for identity and attestation. For mutual authentication and security of data, an efficient and

secure authentication framework (ESAF) based on PUF was proposed in [49].

A lightweight PUF-based protocol for effective communication between smart meters and neighborhood gateways by embedding a PUF with each smart meter device was proposed in [50]. A PUF-based authentication protocol for securing communication between various substations and control centers in E-CPS was presented in [51], which proposes a PUF-based approach for securing IEDs with minimal overhead. Their work also considered an attack scenario that includes a substation with a fake IED.

SRAM PUF-based secure RTU and IED communication framework with an attestation mechanism for IEDs using SRAM PUF in [52] claims to ensure the data integrity from IEDs communicating with an RTU through a robust authentication framework. An authentication protocol for SCADA-enabled systems for Industry 4.0 was proposed in [53]. Their work envisions data flow integrity and non-repudiation by using SRAM PUF for authentication due to high entropy and hardware-generated randomness. In [54], $IED_{PUF}$ probe-based IED authentication mechanism, which is a secure hardware-software solution, is proposed. In [12], a Blockchain-integrated PUF framework for sensor authentication in the SCADA framework is proposed. The authors validated a smart contract based PUF CRP enrollment and authentication mechanism. Their work claims to address a major security issue through modeling attacks on PUF CRPs predicting PUF responses. In comparison to the above cited works on SbD in E-CPS, the proposed QPUF 2.0 presents a quantum hardware attestation framework through QPUF for the security of on-field RTUs and MTUs performing data processing.

## V. Contributions of the Current Paper

### A. Research Questions Addressed in the Current Paper

The research questions addressed through this work are:

- How to ensure security and reliability with sustainable access control and authentication in E-CPS using quantum computing?
- How can quantum computing be feasible for improving the smart grid's operational workflow?
- How to provide security for the device and ensure data integrity in the SCADA-smart grid infrastructure with heterogeneous functionalities?
- How to ensure the reliability of a QSbD solution due to the inherent noise in quantum systems and the instability in a qubit's quantum state?

### B. Challenges in Solving the Problem

The challenges involved in this research are:

- Developing a standard security solution to ensure the integrity and authenticity of various entities across the energy distribution cycle.
- Addressing scalability challenges associated with the integration of billions of smart electronic devices or IEDs into SCADA-Smart Grid, especially with noisy quantum computers.
- Exploring device fingerprint generation schemes like PUF on noisy quantum systems remains difficult due to the environmental factors that compromise the QPUF's reliability in quantum cryptographic applications.
- Limited access to quantum systems currently offered by very few companies through cloud-based access poses a significant hurdle for the emerging Quantum Chain of Things (QCT or QIoT) applications.

### C. Novel Contributions of the Current Paper

The contributions of this research work are:

- A novel quantum-hardware assisted SbD framework for a SCADA-driven electrical distribution framework.
- A QPUF design grounded in the fundamental principles of quantum mechanics, including quantum decoherence, superposition, and entanglement.
- An experimentally evaluated QPUF design achieving reliability, randomness, and uniqueness on noisy quantum computers.
- A framework that facilitates the generation of a large set of CRP, enhancing security and enabling attestation of smart grid entities through their distinct QPUF-generated fingerprints.

## VI. QPUF 2.0: A Quantum Hardware PUF based on Quantum Decoherence and Entanglement

This section discusses the proposed QPUF topology, the calibration of quantum hardware built on superconducting circuits, and the characterization of its quantum physical parameters.

### A. Quantum PUF

Quantum Physical Unclonable Functions (QPUFs) are hardware-based cryptographic primitives designed to enhance the security and reliability of quantum computing applications. Given that quantum computing systems are built on superconducting circuit architectures, QPUFs hold significant potential for securing quantum hardware and applications. In classical PUF, the challenge response pairs (CRPs) are binary valued outcomes derived from physical variations. In Quantum PUFs, the hardware level variation leads to quantum state changes, which are unclonable superpositioned states, and during the measurement, the resulting quantum state collapses to a computational 0 or 1 state with varied probabilities depending on the quantum superposition. The challenges or initialization states for QPUF include a tunable rotation angle and an initialization state for each qubit in the circuit. Each qubit, therefore, has a 0 or 1 state and a unique tunable rotation angle as a challenge input. QPUF works based on the principle of quantum mechanics, which guides the working of quantum hardware with various quantum gates performing qubits' quantum state manipulation. It is practically infeasible to rebuild or emulate a Quantum PUF design and estimate the quantum state changes of qubits on another quantum hardware as defined by the principle of *'no-cloning theorem and quantum physical unclonability'* [28]. Fig. 5 shows the difference between PUF and QPUF topologies.

TABLE II: Related Research on Smart Grid Cybersecurity

| Work | Approach | Hardware | Security Primitive | Challenges |
|---|---|---|---|---|
| Hutto, et al. (2022) [51] | IED Attestation | IC | SRAM PUF | Requires Database |
| Sharma, et al. (2021) [48] | PUF-V2G | NA | PUF-based Vehicle-to-Grid | NA |
| Gomez Rivera, et al.(2020) [52] | SPAI | IC | SRAM PUF (RTU-PLC) | PUF-AES Hardware Overhead |
| Vaidya, et al. (2022) [8] | IED Attestation | Analog-Digital circuit (ADC) | PUF-ADC | Hardware Overhead |
| Cao, et al. (2021) [55] | Authenticated Metering Infrastructure | NA | PUF-Smart Meter | No Hardware |
| Gomez Rivera, et al. (2021) [12] | PUF-Blockchain for SCADA | SRAM PUF | Smart Contract | Scalability |
| **Current Research** | QPUF for IED Attestation | Quantum Computers | Hadamard, RY, CNOT | NA |

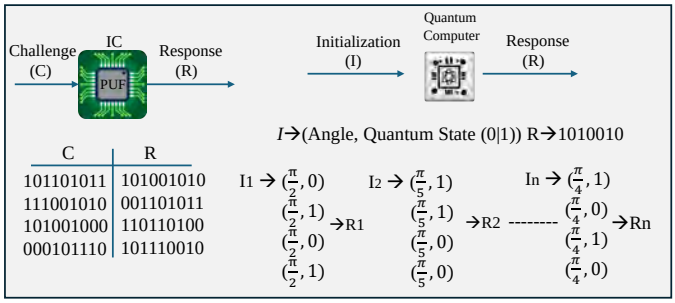



Fig. 5: PUF vs QPUF

### *B. Physical Realization of the Proposed QPUF Architecture*

The proposed QPUF circuit is an 8-qubit architecture with single and two-qubit quantum gates: Ry gate, Hadamard gate, CNOT, and idle gates. I-gate is applied to retain the quantum state or qubit's coherence for a specified time. However, the physical realization of I-gate in superconducting transmon circuits introduces decoherence, propelling the qubit to lose its quantum state or coherence. The main motivation for this research is to explore the decohering nature of superpositioned and entangled qubits and generate a unique bitstream as QPUF response from the quantum hardware.

The quantum circuit begins with the application of a Ry gate after quantum state initialization, which rotates the qubit state around the y-axis of the Bloch sphere, placing it into a new superposition with tunable probability amplitudes. This is followed by the Hadamard gate, which further enhances quantum state unpredictability by creating a balanced superposition, amplifying the probabilistic nature of the qubit state. The combined application of Ry and H gates results in a more complex and nontrivial superposition. Next, Controlled-NOT (CNOT) gates are applied to entangle pairs of qubits in the pattern Q0 $\rightarrow$ Q4, Q1 $\rightarrow$ Q5, Q2 $\rightarrow$ Q6, and Q3 $\rightarrow$ Q7. This entanglement ensures that the quantum state of each control qubit directly influences its corresponding target qubit, forming entangled pairs whose states are interdependent. These logical gate operations are physically realized in superconducting transmon architectures using precisely calibrated microwave pulses. The inherent noise and extremely cold environment-based control of superconducting quantum infrastructure often produce noise-driven results unique to each of the quantum computers due to the chip-level micro manufacturing process variations. These affect the physical qubits in such a way that the microwave pulses passing through the control lines connecting qubits can experience fluctuations, resulting in crosstalk, thereby affecting the target qubit's neighboring qubits.

Additionally, the topology of physical qubits and their location also affect the entanglement due to the requirement for entangling two distant qubits. When the circuit is programmed at the logic gate level, the compiler optimizes the circuit by inserting SWAP gates, which are essential for enabling interactions or quantum state transitions between two distant qubits. Additionally, depending on the level of optimization, during the circuit transpilation process, the error rate can be minimized. The transpilation at *optimization level 1* optimizes the circuit and thereby increases circuit fidelity by carefully arranging circuits and qubits to better align with the physical topology of the quantum device. This mapping reduces the error rates and generates circuit outcomes with high reliability. In contrast, using *optimization level 0* during job submission bypasses such optimizations, often resulting in increased bit-flip errors due to physical qubit mapping, thereby affecting and degrading the reliability.

The identity gate is a quantum gate intended to ensure no operation or idle time to retain the quantum state. However, physical qubits often experience decoherence and lose their quantum state. In this work, the objective is to perform various logic gate operations on a qubit at the logic level and further entangle its state with a qubit, and finally allow them to decohere, thereby exploring the quality of the entanglement during quantum state decoherence. Decohering the qubits at the physical level can introduce randomness that could be harnessed for unclonability. The physical realization of decoherence and other logic gate operations can result in unique quantum states due to microwave pulse interactions unique to each device, unique decoherence times for each device, and qubit connectivity where microwave level interactions could induce crosstalk.

A detailed overview of performing logic gate operations is presented in Algorithm 1.

### C. Superconducting Quantum Circuits

Superconducting quantum circuits are the most widely chosen hardware for realizing quantum circuits. Given the scalability and ease of control through microwave operability, the realization of quantum hardware is becoming simpler and easier. Superconducting circuits operate at extremely low temperatures where the electrical resistance is absent and support infinite conductivity. These circuits operate at extremely low temperatures, typically around -250 degrees Celsius. Superconducting circuits consist of Josephson junctions, inductance, and capacitance elements. These circuits conduct at extremely low temperatures, where the direction of the flowing current in the Josephson junction typically indicates the quantum state of a qubit. Mathematically, a qubit is represented as follows [56]:

$$|q\rangle = \begin{bmatrix} q0 \\ q1 \end{bmatrix} \rightarrow \mathrm{q0}|0\rangle + q1\,|1\rangle,$$
$$p|0\rangle = |qo|^2,$$
$$p|1\rangle = |q1|^2$$

A Josephson junction, typically a building block of superconducting circuits, consists of two superconducting electrodes sandwiched by a thin insulating barrier. Quantum state readout and manipulation are typically performed using microwave photons interacting with qubits. Typically, electrons form Cooper pairs, which can tunnel through the Josephson junctions based on the phase difference of the superconductors. The Josephson junctions create a harmonic energy level system for physical qubits to transition. Anharmonicity of energy states is ideal for superconducting transmon qubits realization [57]. The nonlinear inductor or Josephson junction typically leads to a non-equidistant two-energy level system where the ground state typically represents quantum state $|0\rangle$ and the excited state is represented by $|1\rangle$. Physically, the gate operations on qubits are realized using microwave pulses at a specified phase, amplitude, and frequency in resonance with the qubit's frequency to transition from the ground to the excited state [58].

### D. Unclonable Characteristics of Quantum Hardware

Quantum circuits are subjected to process variations during manufacturing processes such as fabrication, Josephson junction placement, lithography, and base metal placement. The environmental impact on these superconducting circuits, which work at extremely low temperatures, causes the physical qubits to experience decoherence and lose their quantum state. Physical qubits' quantum state is practically evaluated using the current flowing through the Josephson junctions in superconducting transmon circuits. Depending on the direction of the current as either clockwise or anticlockwise, the quantum state of the qubit is defined as either 0 or 1, respectively [59]. The physical qubit layout of various quantum hardware is shown in Fig. 6.

Physically, quantum logic gate operations are realized using microwave pulses interacting with these qubits at a specified magnitude, shape, and direction [60]. This change in microwave pulses is to obtain the desired change in the quantum state, a transition between energy levels based on an anharmonic oscillator that corresponds to the mathematical representation of the qubit's rotation around the x, y, and z-axis of the Bloch sphere [45]. Qubits' quantum state can also change due to crosstalk, which arises due to the coupling of qubits in the hardware. The application of a microwave pulse on one qubit might also affect the neighboring qubit while realizing the gate operations [24]. The quantum decoherence of entangled qubits is based on the alignment of qubits physically in the quantum hardware. The quantum entanglement of neighboring qubits and the decoherence of control qubits can decohere target qubits faster than the decoherence of distantly entangled qubits.

**Algorithm 1:** QPUF Design Calibration

1: Create a quantum circuit with 8 quantum and classical registers
2: Initialize all the qubits q[0]-q[7] randomly with 0 or 1 state for each job
- *Choose X-Gate to initialize qubit to 1 state*
  *State 1→X[q]*
- *Each qubit is initialized to state 0 by default*

3: Place qubits in an unknown quantum state by applying Ry Gate
- Angle → 0-2 pi

4: Place qubits in superposition
- Apply Hadamard Gate
  *qubits' state probabilities → 50%*

5: Perform quantum state entanglement
- Apply CNOT Gate
  *q[0]→ q[4], q[1]→ q[5], q[2]→ q[6], q[3]→ q[7]*

6: Control the qubits by applying idle gates to evaluate the impact of decoherence on the entangled qubits
- Apply I Gate
  *I[q[0]], I[q[1], I[q[2], I[q[3],*
  *I[q[4]], I[q[5], I[q[6], I[q[7]*

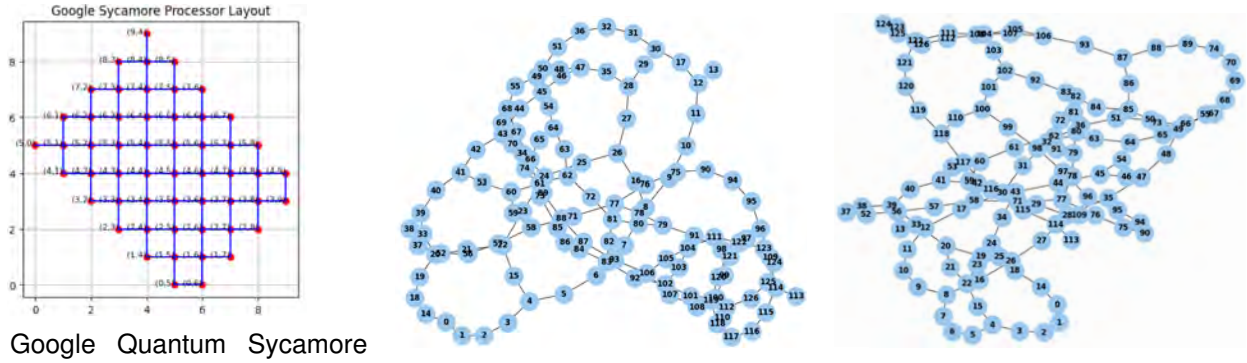
7: Perform quantum state measurement of qubits and store the result in a classical register corresponding to each qubit
*M[q[0]]→C[0], M[q[1]→C[1], M[q[2]→C[2], M[q[3]→C[3],*
*M[q[4]]→C[4], M[q[5]→C[5], M[q[6]→C[6], M[q[7]→C[7]*

### E. Physical Parameters of Quantum Circuits

QPUF signature is obtained by mapping the quantum mechanical qubit's properties to generate a unique bitstream as signature. Quantum state manipulation of a qubit is performed at a microwave pulse level by sending a microwave pulse in resonance with the qubit's driving frequency. The qubit's T1 and T2 (defined below) also impact the quantum state's stability. Furthermore, each quantum computer has a readout assignment error, and anharmonicity which impacts the quantum state of a qubit [63], [64]. Physical parameters of various quantum hardware are calibrated and presented in Table III.

*T2 Time* is the duration over which a qubit maintains phase coherence in a superposition state. A longer duration of T2 time indicates greater quantum state stability and minimal loss of information, which corresponds to higher qubit quality for quantum computation.

*T1 Time* is the energy relaxation time of a qubit to lose its quantum state from $|1\rangle$ to $|0\rangle$ when a qubit interacts with the




(a) Google Quantum Sycamore Processor (b) ibm_brisbane [61] (c) ibm_sherbrooke [62]

Fig. 6: Physical Qubit Mapping of Quantum Systems

environment. T1 can also be defined as the thermal relaxation time for a qubit to reach the ground state.

*Resonant Frequency* of a qubit can be determined using a Ramsey experiment, which measures the transition frequency between the $|0\rangle$ to $|1\rangle$ states of a superconducting qubit. The resonant frequency corresponds to the energy gap between these two quantum states.

## VII. QPUF 2.0: Proposed Quantum SbD Framework for Smart Grid

This section presents the QSbD approach using QPUFs for SCADA–Smart Grid security.

The security and reliability of SCADA-enabled critical grid operations and management are essential to counter any hardware/software-based security attacks and vulnerabilities. The data transfer from IEDs at various stages of the grid cycle to an RTU and further to an MTU for analysis needs to be secure to ensure the integrity of data. An adversary may be capable of gaining unauthorized access to an RTU and controlling the on-field IEDs and intelligent protective relays, thereby spoofing the IEDs and installing fake nodes. The fake IEDs are installed to provide a false state of the system, which could jeopardize the critical grid management and lead to blackouts. Also, software attacks could be performed to access the RTUs controlling IEDs in various subsystems, and communication could be eavesdropped on due to the unreliable communication framework. The proposed QPUF provides real-time data integrity verification from IEDs by securely attesting each IED in the grid infrastructure through QPUF. The assumptions made in this research paper are:

- All RTUs have access to quantum hardware resources and can obtain QPUF-generated responses.
- The communication between IED and RTU is secure and fool-proof such as Transport Layer Security (TLS) communication protocol.
- A QPUF evaluated on a noiseless quantum system with enhanced coherence and minimal cross-talk.

All IEDs are resource-constrained, while RTUs, MTUs, and control centers have memory and data processing capabilities. The objective is to develop a secure device attestation scheme using Quantum SbD principles.

In the proposed framework, RTUs, MTUs, and control centers of SCADA are the quantum gateways with efficient access to quantum systems. Various smart electronic devices, or IEDs, and protective relays can be controlled by RTUs. The RTUs are further controlled by MTUs for data storage, processing, and analysis, and work in a master-slave relationship. MTUs act like servers for controlling RTUs at various subsystems in the energy distribution framework. RTUs work as slaves, coordinating various field devices and protective relays at geographically distant locations in the energy cycle.

The control center is a command center with an effective human-machine interface and decision-making capability. In the proposed framework, RTUs, with reliable access to quantum systems, act as gateways for IEDs to access quantum system resources and obtain QPUF generated responses for security. A set of IEDs at a particular location can be securely controlled by an RTU at that specific substation. IEDs can be securely accessed and controlled by all the RTUs with quantum resources in the generation, transmission, and distribution subsystems. MTUs are centralized data processing control systems monitoring RTUs at different substations and energy generation sources for applications like on-field power quality metric evaluation and protective relaying, which are critical grid functionalities. Furthermore, MTUs can also authenticate RTUs and perform sensing and actuation processes for grid protection and grid equipment management. MTUs can securely establish communication with RTUs using Quantum Key Distribution (QKD).

In the proposed work, all SCADA entities, such as RTU and MTU, have access to the quantum computer or hardware for security and quantum information processing applications, as shown in Fig. 7. An IED can send the enrollment request using a unique device identifier $Dev_{IED}$ to an RTU $DRTU$, which can be the MAC address or any other device's unique address. RTUs with access to QPUF extracts a unique response for a new session key generation request from $Dev$ by sending $CDev \rightarrow Dev_{IED} \oplus DRTU$. The enrollment request is sent from IED through a secure channel encrypted with a pre-shared symmetric key and then decrypted by an RTU. RTU generates a QPUF response $RDev$ for $CDev$ from IED and assigns it as the new session key during authentication. RTU

TABLE III: Calibrated Physical Parameters of Quantum Hardware

(a) ibm_brisbane Physical Parameters (Calibrated at 2025-05-21 08:09:17)

| Qubit | T1 ($\mu$s) | T2 ($\mu$s) | Frequency (GHz) |
|---|---|---|---|
| Qubit 0 | 315.33 | 57.51 | 4.7219 |
| Qubit 1 | 407.42 | 312.70 | 4.8151 |
| Qubit 2 | 264.53 | 264.74 | 4.6097 |
| Qubit 3 | 241.02 | 241.02 | 4.8755 |
| Qubit 4 | 271.99 | 285.42 | 4.8182 |
| Qubit 5 | 99.63 | 115.64 | 4.7341 |
| Qubit 6 | 429.74 | 88.96 | 4.8763 |
| Qubit 7 | 120.23 | 113.70 | 4.9675 |
| Qubit 8 | 392.20 | 241.03 | 4.9024 |

(b) ibm_sherbrooke Physical Parameters (Calibrated at 2025-05-21 09:29:22)

| Qubit | T1 ($\mu$s) | T2 ($\mu$s) | Frequency (GHz) |
|---|---|---|---|
| Qubit 0 | 385.30 | 246.04 | 4.6357 |
| Qubit 1 | 306.36 | 398.27 | 4.7363 |
| Qubit 2 | 260.32 | 186.08 | 4.8192 |
| Qubit 3 | 266.04 | 306.35 | 4.7472 |
| Qubit 4 | 320.07 | 434.52 | 4.7879 |
| Qubit 5 | 113.88 | 308.38 | 4.8508 |
| Qubit 6 | 237.40 | 129.79 | 4.8995 |
| Qubit 7 | 277.72 | 62.61 | 4.7560 |
| Qubit 8 | 375.15 | 435.90 | 4.8126 |

also selects a random challenge input $CDev1$ for the IED and extracts $RDev1$ using QPUF and sends back the new session key $RDev$ and new QPUF challenge $CDev1$ in encrypted form to the IED. This step ensures integrity by avoiding exposure of IED's $RDev1$ from RTU and thereby RTU control groups of IED's without IED's requiring any non-volatile memory or storage capabilities. When IEDs send an attestation request, the new session key $RDev1$ is used to encrypt the sensor data and its $CDev1$ along with the timestamp of data and is encrypted and sent to RTU. RTU verifies IED by obtaining $CDev1$, extracts $RDev1$, and hashes and stores data from the IED in its secure database $CRDBR(CDRTU)$

Furthermore, each RTU can communicate with an MTU for coordination and control. MTUs can communicate with a group of RTUs at different substations and to ensure the integrity of communication between an MTU and RTU, each RTU sends its enrollment request initially to generate a new session key $SKey2 \rightarrow CRTU2_{MTU} \rightarrow QPUF \rightarrow RRTU$ for the authentication session and receives a new encrypted output from the MTU with a challenge input selected by the MTU for the RTU $CRTU2$. Finally, after attestation, the data from RTU is hashed and stored at MTU's database $CRDBR(CDMTU)$.

*Formal Security Analysis using ProVerif*

The proposed smart grid entity attestation mechanism, driven by QPUF, is formally modeled and tested using ProVerif as shown in Fig. 8, an automated tool for the formal analysis of authentication protocols validation tool [65]. ProVerif validates the confidentiality, anonymity, and resilience of the protocol against reply, and Distributed Denial-of-Service (DDoS) attacks. It also supports a wide range of cryptographic primitives like digital signatures, hash functions, and other cryptographic related operations. The proposed

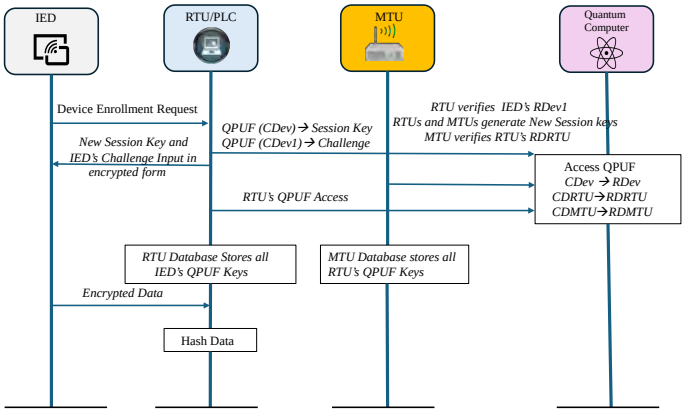



Fig. 7: Quantum PUF-Driven Smart Grid Entity Attestation Framework

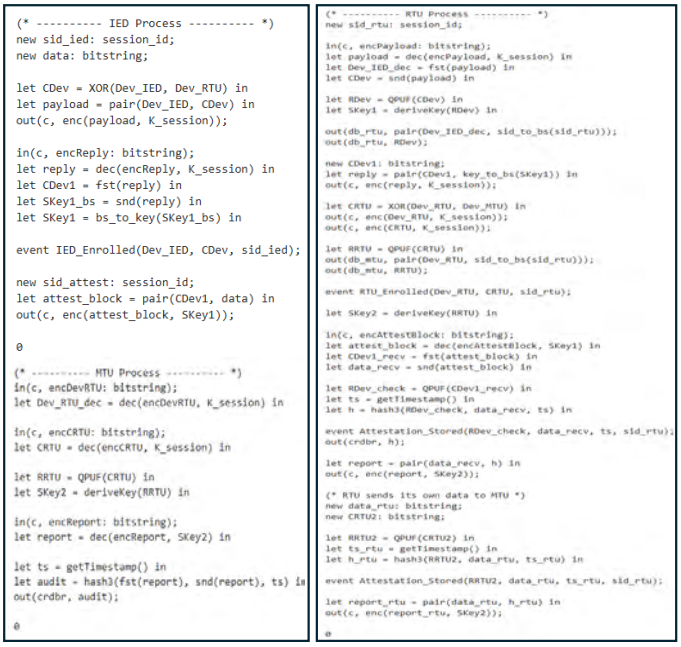
QPUF 2.0's Device enrollment, attestation, communication, and data hashing and storage phases are simulated under the Dolev-Yao attacker model [66]. The verification summary as shown in Fig. 9 indicates the protocol is secure and preserves the integrity of QPUF enhanced communication, attestation, data storage, and is resistant against eavesdropping and other attacks.

## VIII. Experimental Results

This section presents the experimental validation details of QPUF 2.0, along with its performance evaluation and analysis in detail.

### A. Experimental Setup

Experimental evaluation was performed on quantum systems and simulators from IBM and Google. IBM quantum



```
(* ---------- IED Process ---------- *)
new sid_ied: session_id;
new data: bitstring;

let CDev = XOR(Dev_IED, Dev_RTU) in
let payload = pair(Dev_IED, CDev) in
out(c, enc(payload, K_session));

in(c, encReply: bitstring);
let reply = dec(encReply, K_session) in
let CDev1 = fst(reply) in
let SKey1_bs = snd(reply) in
let SKey1 = bs_to_key(SKey1_bs) in

event IED_Enrolled(Dev_IED, CDev, sid_ied);

new sid_attest: session_id;
let attest_block = pair(CDev1, data) in
out(c, enc(attest_block, SKey1));

0
```

```
(* ---------- RTU Process ---------- *)
new sid_rtu: session_id;

in(c, encPayload: bitstring);
let payload = dec(encPayload, K_session) in
let Dev_IED_dec = fst(payload) in
let CDev = snd(payload) in

let RDev = QPUF(CDev) in
let SKey1 = deriveKey(RDev) in

out(db_rtu, pair(Dev_IED_dec, sid_to_bs(sid_rtu)));
out(db_rtu, RDev);

new CDev1: bitstring;
let reply = pair(CDev1, key_to_bs(SKey1)) in
out(c, enc(reply, K_session));

let CRTU = XOR(Dev_RTU, Dev_MTU) in
out(c, enc(Dev_RTU, K_session));
out(c, enc(CRTU, K_session));

let RRTU = QPUF(CRTU) in
out(db_mtu, pair(Dev_RTU, sid_to_bs(sid_rtu)));
out(db_mtu, RRTU);

event RTU_Enrolled(Dev_RTU, CRTU, sid_rtu);

let SKey2 = deriveKey(RRTU) in

in(c, encAttestBlock: bitstring);
let attest_block = dec(encAttestBlock, SKey1) in
let CDev1_recv = fst(attest_block) in
let data_recv = snd(attest_block) in

let RDev_check = QPUF(CDev1_recv) in
let ts = getTimestamp() in
let h = hash3(RDev_check, data_recv, ts) in

event Attestation_Stored(RDev_check, data_recv, ts, sid_rtu);
out(crdbr, h);

let report = pair(data_recv, h) in
out(c, enc(report, SKey2));

(* RTU sends its own data to MTU *)
new data_rtu: bitstring;
new CRTU2: bitstring;

let RRTU2 = QPUF(CRTU2) in
let ts_rtu = getTimestamp() in
let h_rtu = hash3(RRTU2, data_rtu, ts_rtu) in

event Attestation_Stored(RRTU2, data_rtu, ts_rtu, sid_rtu);

let report_rtu = pair(data_rtu, h_rtu) in
out(c, enc(report_rtu, SKey2));

0
```

```
(* ---------- MTU Process ---------- *)
in(c, encDevRTU: bitstring);
let Dev_RTU_dec = dec(encDevRTU, K_session) in

in(c, encCRTU: bitstring);
let CRTU = dec(encCRTU, K_session) in

let RRTU = QPUF(CRTU) in
let SKey2 = deriveKey(RRTU) in

in(c, encReport: bitstring);
let report = dec(encReport, SKey2) in

let ts = getTimestamp() in
let audit = hash3(fst(report), snd(report), ts) in
out(crdbr, audit);

0
```

Fig. 8: ProVerif Simulation of RTU, MTU and IED Processes

```
Verification summary:

Query not attacker(K_session[]) is true.

Query not attacker(QPUF(XOR(Dev_IED[],Dev_RTU[]))) is true.

Query not attacker(QPUF(XOR(Dev_RTU[],Dev_MTU[]))) is true.

Query not attacker(Dev_IED[]) is true.

Query not attacker(Dev_RTU[]) is true.

Query not attacker(Dev_MTU[]) is true.
```

Fig. 9: ProVerif Verification Summary

systems are accessible to users through an application programming interface token that is loaded each time a user accesses the quantum system. A user can access a limited number of quantum systems with an open plan and an available run time of 10 minutes. All the IBM quantum simulators are available for free access to test and execute quantum algorithms with ample run time.

For the evaluation, the proposed QPUF was implemented and tested on both quantum simulators and quantum backends. For simulator-based evaluation, IBM's qasm_simulator and Google's cirq simulators are chosen for QPUF design evaluation. Hardware evaluations were conducted on IBM's 'ibm_brisbane' and "ibm_sherbrooke" quantum backends with Eagle R3 processor supporting 127-qubits topology. The Eagle R3 is an advanced quantum processor with enhanced coherence time, facilitating complex computations. The proposed QPUF design is implemented using Python. For evaluation on IBM's backends, circuits and algorithms were implemented using Qiskit, a quantum computing framework [67] for the evaluation on IBM quantum systems. The proposed QPUF architecture uses 8 quantum and classical bits, and the design incorporates a combination of gates, including X-gate, Hadamard, CNOT, Ry, and Idle gates as shown in Fig. 10.

The QPUF evaluation is also performed on Google quantum simulator using 'Cirq', a Python framework for implementing algorithms and circuits on Google quantum systems and simulators [68]. The proposed design was evaluated on Cirq's 'cirq.simulator()', which is considered effective for flexibility and can emulate quantum hardware behavior. The circuit was evaluated for 200 initializations, similar to the evaluation performed on the IBM simulator at a tunable rotation angle of $90^o$. For evaluating QPUF's strength, certain metrics are evaluated for extracted QPUF outcomes from simulators and backends. These metrics are discussed in detail below:

The QPUF was tested under various configurations using tunable rotation angles applied via the Ry gate and different qubit initialization states (either 0 or 1) as challenge inputs. For each job or evaluation, a tunable rotation angle in the range of 0-2 pi that places each qubit in an unknown arbitrary quantum state is chosen. The QPUF then generates a unique final string as a response or measurement outcome for each execution as presented in Fig. 11.

The open plan of IBM supports a qiskit run time of 10 minutes, which allows only a limited number of circuit executions and shots for evaluation on quantum backends. A measurement outcome or shot in the quantum job execution refers to the experimental evaluation of the circuit. Each job can support 1024-8192 measurement outcomes or shots for the circuit. The QPUF response for a circuit is determined by selecting the outcome with the highest occurrence across all measurement shots. In this work, 2048 measurement shots were considered for evaluation on hardware. Therefore, a QPUF job execution implies testing the QPUF circuit with a challenge state, which includes a qubit initialization sequence and tunable rotation angle for 2048 executions.

*Randomness* of a PUF is the measure of balance in the occurrence of ones and zeros in each response. For a given QPUF response $ri$, the randomness is obtained by counting the number of ones $ki$ in $ri$ and dividing it by the total number of bits $bi$ in $ri$.

$$\text{Randomness}(ri\%) = \frac{ki}{bi} \times 100$$

*Diffuseness* of a QPUF is the extent of variation of a QPUF response with varying initialization states and angles. In the context of QPUF, Diffuseness is obtained by calculating the average intra-hamming distance of QPUF responses from a hardware or simulator with varying challenge states. To evaluate the diffuseness of QPUF on a device, the intra-hamming distance is calculated among responses $r1$ and $r2$ for initialization states with tunable angles $a1$, $a2$, and quantum state initializations $i1$, $i2$, diffuseness is defined as.

$$\text{Diffuseness } (r1,r2) = HD(\text{r1, r2});$$

The reliability of QPUF is the extent to which QPUF responses match under noisy and environmental conditions impacting the quantum systems. To evaluate reliability, the Hamming distance HD ($j1$,$j2$ ) of two instances of QPUF executions from a quantum system is calculated. The final

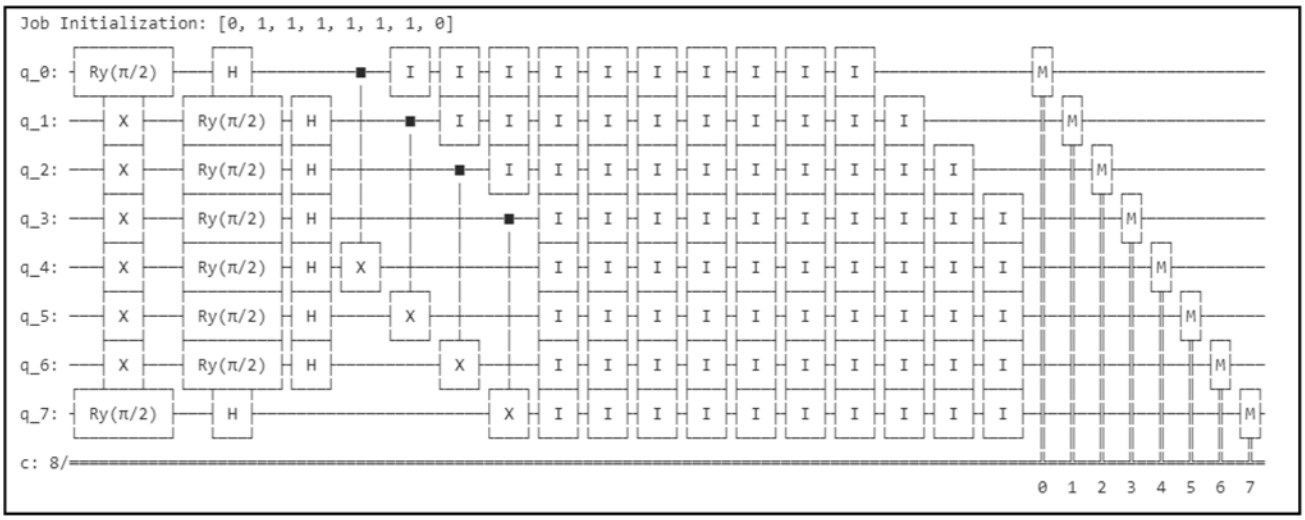



Fig. 10: Proposed QPUF Topology with X, RY, H,CNOT and Idle Gates

```
Job 1: Using Initialization [1, 0, 1, 0, 1, 0, 0, 0]
Qubit 0: Applying RY(1.57)
Qubit 1: Applying RY(1.57)
Qubit 2: Applying RY(3.14)
Qubit 3: Applying RY(3.14)
Qubit 4: Applying RY(4.71)
Qubit 5: Applying RY(4.71)
Qubit 6: Applying RY(6.28)
Qubit 7: Applying RY(6.28)
Job 1 ID: d0p9jw3t9xxg0089amgg
Most Frequent Measurement Outcome for Job 1: 10101101

Job 2: Using Initialization [1, 0, 1, 0, 1, 1, 0, 1]
Qubit 0: Applying RY(1.57)
Qubit 1: Applying RY(1.57)
Qubit 2: Applying RY(3.14)
Qubit 3: Applying RY(3.14)
Qubit 4: Applying RY(4.71)
Qubit 5: Applying RY(4.71)
Qubit 6: Applying RY(6.28)
Qubit 7: Applying RY(6.28)
Job 2 ID: d0p9jy3t9xxg0089amh0
Most Frequent Measurement Outcome for Job 2: 10001001

Job 3: Using Initialization [0, 0, 1, 1, 1, 0, 0, 1]
Qubit 0: Applying RY(1.57)
Qubit 1: Applying RY(1.57)
Qubit 2: Applying RY(3.14)
Qubit 3: Applying RY(3.14)
Qubit 4: Applying RY(4.71)
Qubit 5: Applying RY(4.71)
Qubit 6: Applying RY(6.28)
Qubit 7: Applying RY(6.28)
Job 3 ID: d0p9k0cb5pe0008ccv40
Most Frequent Measurement Outcome for Job 3: 10111100
```

Fig. 11: QPUF Evaluation on IBM quantum Backend

response (rn) from both instances, achieving 100% reliability with no varying bits, is considered reliable.

$$\text{Reliability}(\%) = 100 - \text{HD}(j1, j2)$$

$$rn = \begin{cases} 100\%, & \text{if } HD = 0, \\ 0\%, & \text{if } HD \neq 0. \end{cases} \quad (1)$$

The uniqueness of a QPUF represents the degree of variation in QPUF responses across different devices. It is evaluated by calculating the average Hamming distance between response instances $rn$, and $r_{n+1}$ obtained from hardware $s_n$ and $s_{n+1}$, respectively, and can be expressed as::

$$\text{Uniqueness } (s_n, s_{n+1}) = \text{HD } (rn, r_{n+1}) \text{x } 100$$

### *B. Pulse level Control of QPUF*

The quantum circuit logic at the higher level translates to microwave pulse level control of superconducting quantum circuits at the hardware. The microwave pulse at a specified amplitude, phase, and duration manipulates the quantum state of a qubit. The desired performance of a circuit implementation can be realized through careful calibration of microwave pulses controlling the quantum hardware. IBM's qiskit Pulse is an open-source front-end interface for IBM quantum systems. Channels in pulse level control drive microwave pulses to manipulate the quantum state of physical qubits in superconducting circuits [69]. Qiskit pulse includes various channels that facilitate qubit interaction for diverse functions, which include measurement, control, state change, and state acquisition. Various channels in the Qiskit pulse include:

*Drive Channels(Di):* This channel is connected to a qubit where a microwave pulse in resonance with the qubit's frequency can be applied to control the qubit's quantum state.

*Measurement Channel (Mi):* This channel enables microwave pulse level interaction with readout detectors to perform the qubit's state measurement after executing the quantum circuit.

*Acquire Channel(Ai):* This channel enables efficient readout of quantum state by digitizing and converting the measurement data into a suitable format.

*Control channel(Ui):* Control channels enable efficient implementation of quantum circuits by sending control signals to various components of quantum hardware.

Furthermore, Specific pulse level instructions are used to calibrate the pulse amplitude, phase, control, and delay to perform quantum state changes which include Delay, Play, ShiftPhase, ShiftFrequency, and Acquire.

- Delay instruction adds or idles the channel for a specified time while Play instruction gives the pulse output waveform of the channel.
- ShiftPhase and ShiftFrequency shifts the phase and frequency of pulse on the channel to effect a change in the qubit's state.
- Acquire instruction collects the measurement results and stores them in a classical register.

For pulse level demonstration of QPUF circuit, '**GenericBackendV2**', a customized backend with 8 qubits from qiskit-aer is chosen. It mimics the behavior of real quantum hardware while providing a pulse-level control behavior for the circuit. Fig. 12 shows the pulse schedule of the QPUF with 4 qubits. The shape and duration of each pulse represent the quantum gate operations on the qubits. The pulse schedule has 4 drive and measurement channels for the 4 qubits in the quantum circuit. The vz pulse is a virtual microwave pulse at -3.14 radians and is used to remove phase differences in the quantum state, ensuring reliable state manipulation.

### C. Testing and Validation on Simulator

The QPUF circuit evaluation on the ibmq_qasm simulator obtained an excellent 100% reliability across five instances of 200 jobs, with each job having 2048 outcomes. The QPUF metrics evaluated on the five instances of QPUF keys have shown an impressive 50% randomness and an average intra-hamming distance of 50%. Our further evaluation of QPUF at tunable rotation angles of $90^0$ and $270^o$ has shown excellent reliability and uniqueness across IBM and Google quantum simulators. The QPUF performance metrics for the circuit evaluation at $90^o$ and $270^o$ are presented in Fig. 13.

### D. Testing and Validation on Quantum Backends

For QPUF evaluation on physical backends, various evaluations were performed on ibm_sherbrooke and ibm_brisbane at different tunable rotation angles. Our preliminary evaluation was performed at a tunable rotation angle of $90^o$, which showed an impressive reliability. This could be attributed to transpilation, which is a process of optimizing the circuit's logic gates and qubit connectivity to ensure hardware compatibility. Our observation indicates that transpilation ensured reliability specifically at $90^o$. Overall, 25 evaluations were performed with 1024-2048 measurement outcomes. The circuit achieved better reliability across both backends, and their evaluation metrics are presented in Fig. 14. However, the circuit could not achieve the desired level of uniqueness across both backends, which could be attributed to circuit transpilation and logic optimization.

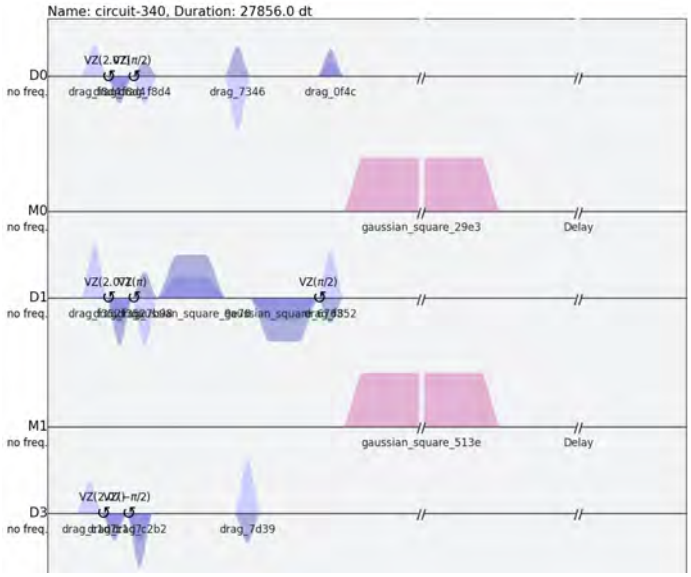
To ensure uniqueness, the circuit is extended to 16 qubits with unique initializations and tunable rotation angles as can be seen in Fig. 15. This evaluation, even with a decent level of optimization at level 1, has shown marginal bit flips affecting reliability but ensuring much better uniqueness. As can be observed from the figure, the tunable rotation angle of $90^o$ was tested on the first 8 qubits, and $180^o$ was chosen for the last 8 qubits, with each evaluation having a unique qubit initialization sequence. Overall, 2 instances of 10 jobs on ibm_sherbrooke and 5 instances of 10 evaluations on ibm_brisbane were evaluated, respectively. Our evaluation shows that ibm_sherbrooke has demonstrated approximately 100% reliability by regenerating 9 out of 10 responses. This follows with impressive randomness and intra-hamming distance. The 5 instances of evaluations on ibm_brisbane have shown marginal bit flips across different evaluations, thereby affecting reliability. Table IV presents the performance evaluation of QPUF on quantum backends and simulators. Additionally, a comparative analysis of performance and experimental designs of QPUF is presented in Table V.

### E. Analysis

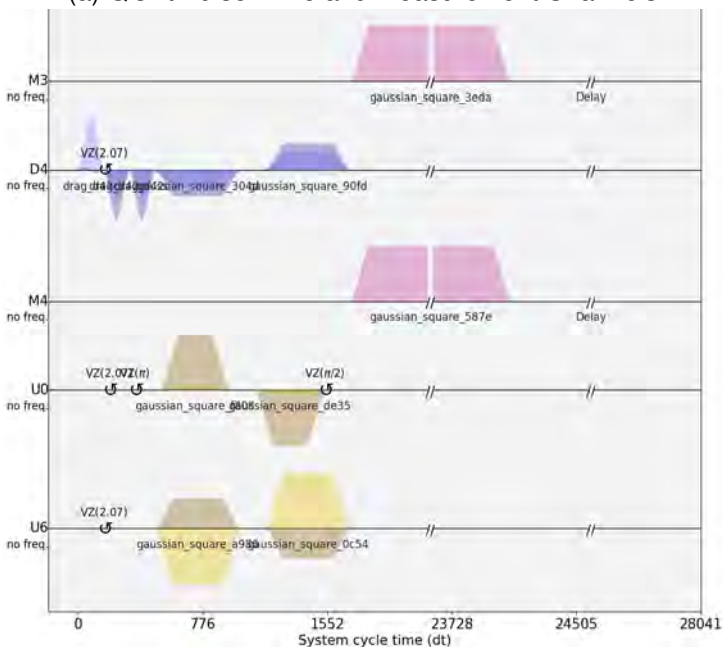
The improved qubit coherence can increase the resiliency of qubits to noise and the environment, thereby achieving better qubit coherence, which can improve the reliability of QPUF. The realization of QPUF and reliable response extraction from noisy quantum computers is a great challenge due to the very slow pace of improvement in the realization of noise-free quantum hardware. This research explored the scope of quantum mechanics principles for QSbD and presented a QPUF architecture that has shown PUF execution on Quantum hardware as a feasible approach with enhanced performance in comparison to the related research.

However, to further evaluate the robustness of the proposed QPUF, more experimental space is needed, along with increased access to noiseless quantum resources from various companies. Additionally, our evaluation of a 16-qubit QPUF circuit with transpilation and optimization at level 1 revealed multiple bitflips that affected reliability. With a further increase in the number of shots, the bit flips could be reduced, leading to deterministic outcomes. However, our circuit evaluation exhibits an average execution time of 1 second for a job with 1024 shots. A larger number of shots proportionally increases the execution time.

Furthermore, with a further increase in the evaluation space, more evaluations could be performed. Our evaluation indicates improved potential for uniqueness, particularly when the circuit undergoes optimization to match the backend. Experimental evaluation also presents a sample pulse schedule with 4 qubits exhibiting our proposed QPUF logic. We anticipate that as pulse level control to physical backends becomes more accessible, more fine-tuned pulses with better frequency and without noise could be applied. QPUF calibration parameters presented in this work have been obtained at the time of QPUF circuit execution. Since these values are recalibrated every few hours, variations occur in frequency, coherence times, and decoherence times.




(a) Qiskit Pulse Drive and Measurement Channels




(b) Qiskit Pulse Control Channels for Entangled Qubits

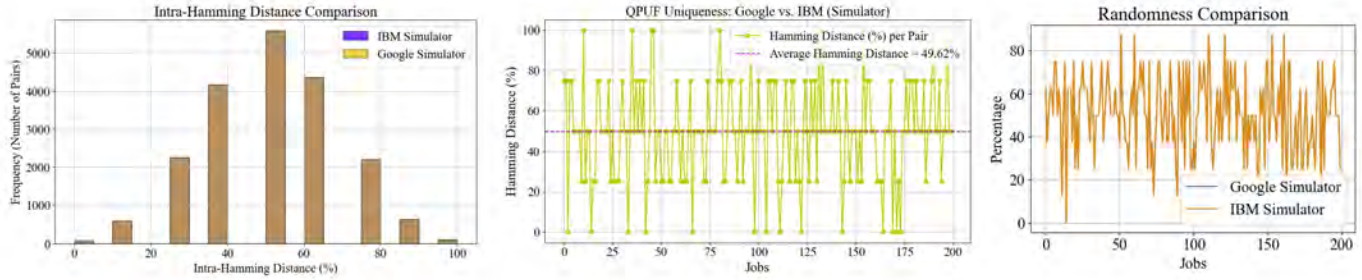
Fig. 12: Qiskit Pulse Schedule for QPUF

As physical backends become more noise-free and these parameters stabilize, the reliability of QPUF can be further improved."

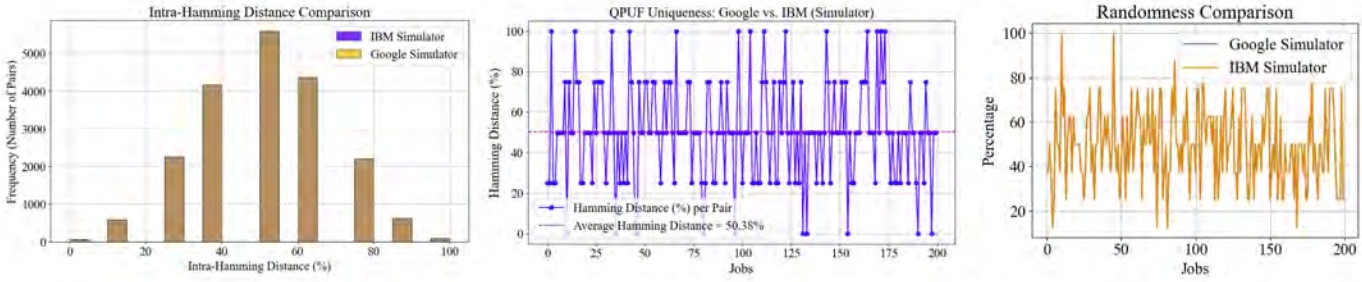
## IX. Conclusion and Future Research

This research work validated and presented a novel QSbD framework for reliable authentication of power transmission systems, ensuring the security of protective relays and intelligent electronic devices in the SCADA-Smart grid infrastructure. QPUF circuit execution demonstrates the potential for quantum-centric smart grid security with a robust authentication and communication framework. The QPUF can be a feasible security solution for the smart grid due to its capability to support high-performance computing applications with SCADA enabled energy transmission and distribution infrastructure. The QPUF measurement outcomes from quantum backends "ibm_brisbane", and "ibm_sherbrooke", and their evaluation have shown excellent diffuseness and randomness at around 50% and achieving 100% reliability across simulators. This research clearly outlines key observations for improving uniqueness and reliability further across quantum backends and clearly evaluates QPUF at various initialization parameters.

Furthermore, our experimental validation has demonstrated a QPUF CRPs generation mechanism leveraging quantum entanglement, superposition, and decoherence principles. The




(a) QPUF Evaluation on IBM and Google Quantum Simulators at $90^o$




(b) QPUF Evaluation on IBM and Google Quantum Simulators at $270^o$

Fig. 13: QPUF Performance Evaluation on Simulators

TABLE IV: QPUF Performance Evaluation

| System | Number of Qubits | Tunable Rotation Angle | Number of Jobs & Instances | Intra-Hamming Distance(%) | Randomness(%) | Reliability(%) | Uniqueness(%) |
|---|---|---|---|---|---|---|---|
| qasm_ simulator<br>Cirq Simulator (8-Qubit) | 8 | $90^o$ | 200-3 | 50.16 | 51.00<br>50.80 | 100 | 49.62 |
| qasm_ simulator<br>Cirq Simulator | | $270^o$ | | 50.16 | 49.68<br>49.68 | 100 | 50.38 |
| ibm_sherbrooke<br>ibm_brisbane | 16 | $90^o, 180^o$ | 10-2<br>10-5 | 51.81<br>52.36 | 50.62<br>48.12 | 90<br>0 | 47.50 |
| ibm_sherbrooke<br>(Optimization level=0)<br>ibm_brisbane<br>(Optimization level=0) | 8 | $90^o$ | 9-2<br><br>10-2 | 45.14<br><br>51.39 | 43.06<br><br>51.25 | 20<br><br>40 | 28 |
| ibm_brisbane<br>(Optimization level=1) | 8 | $0-360^o$ | 25-3 | 49.75 | 45.50 | 68 | - |

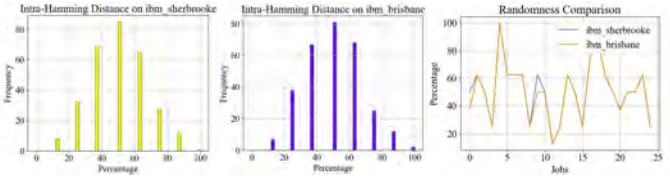



Fig. 14: QPUF Performance Evaluation of ibm_sherbrooke and ibm_brisbane at $90^o$

proposed QSbD framework can ensure the authenticity of devices and the integrity of data and communication among smart grid entities with quantum capabilities, as verified using ProVerif for validating its resilience against various attacks. Additionally, for future research, the proposed QPUF-driven security framework can be integrated with quantum cryptography protocols based on the driving principles of QSbD for enhanced security and authenticity in the emerging Quantum IoT era.

## ACKNOWLEDGEMENTS

A preliminary version of this work has been published in a conference proceeding [72] and is also available as a preprint on arXiv [31].

## REFERENCES

[1] V. C. Patil and S. Kundu, "Realizing Robust, Lightweight Strong PUFs for Securing Smart Grids," *IEEE Transactions on Consumer Electronics*, vol. 68, no. 1, pp. 5–13, February 2022.

[2] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, "Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems," *IEEE Access*, vol. 7, pp. 46 595–46 620, 2019.

[3] National Institute of Standards and Technology (NIST), "Draft smart grid framework," 2020, accessed: April 19, 2024. [Online]. Available: https://www.nist.gov/document/draft-smart-grid-framework

[4] 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.

[5] K. D. Kumar, M. A. Jawale, M. Sujith, and D. Pardeshi, "Cybersecurity Threats, Detection Methods, and Prevention Strategies in Smart Grid: Review," in *2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS)*, February 2023.

TABLE V: Quantum PUF: Experimental Evaluation and Comparative Analysis of Related Research

| Work | Quantum Hardware | Logic Gates | Quantum Principles | QPUF Metrics | Challenges |
|---|---|---|---|---|---|
| Phalak, et al. (2021) [24] | ibmq_essex and ibmq_london | H, Ry, Measurement, and I | Superposition and Decoherence | intra-HD ibmq_essex (13.82%) and ibmq_london(3.94%) | No CRP |
| Chwa, et al. (2023) [23] | IBM Falcon r5.10 and r5.11 27, ibm cairo, ibm hanoi, ibmq mumbai, and ibmq kolkata | Hadamard | Quantum Crosstalk | NA | No impact of Control on Target |
| Bathalapalli, et al. (2023) [25] | ibmq_belem, ibmq_lima, and ibmq_quito | Hadamard, Ry | Superposition | 40% Intra-HD ibmq_lima, 25% Uniqueness | Less uniqueness and Diffuseness |
| Khan, et al. (2023) [45] | 5-qubit processors | Ry and Rx gates | Entanglement | 1 state probability- q[0]-76%, q[1]-87% | No evaluation of Intra and Inter HD |
| Cirillo, et al.(2025) [35] | ibm_brisbane, ibm_kyiv, and ibm_sherbrooke | Rx, Ry, and Rz | Entanglement | Randomness-35-75%, Uniqueness-15-25% | Less randomness, uniqueness and reliability |
| Wu et al. (2024) [70] | ibm_quito, ibm_lima, ibmq_belem, ibm_perth | Bernstein–Vazirani (BV) circuits with 3, 6, and 9 qubits | CNOT gate error rates and qubit output state probabilities | Manhattan distance between circuit fingerprints (threshold = 0.035) | Reliability analysis not performed |
| Mi et al. (2021) [71] | 9 IBMQ devices (e.g., Santiago, Lima, Belem) | H and CNOT gates (via quantum state tomography) | Crosstalk and noise characterization | Fingerprinting accuracy: 99.1% (device) and 95.3% (location) | NA |
| **QPUF 2.0 (Current Paper)** | ibm_brisbane, and ibm_sherbrooke | Pauli-X, H, Ry, CNOT, and I-gate | Quantum Entanglement, Decoherence, and superposition | 50% HD, 51% Randomness | Can improve uniqueness |


[6] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—The new and improved power grid: A survey," *IEEE communications surveys and tutorials*, vol. 14, no. 4, pp. 944–980, 2011.

[7] J. Gaspar, T. Cruz, C.-T. Lam, and P. Simões, "Smart Substation Communications and Cybersecurity: A Comprehensive Survey," *IEEE Communications Surveys and Tutorials*, vol. 25, no. 4, pp. 2456–2493, 2023.

[8] G. Vaidya and T. V. Prabhakar, "Hardware based identification for Intelligent Electronic Devices," in *Proc. IEEE/ACM Seventh International Conference on Internet-of-Things Design and Implementation (IoTDI)*, 2022, pp. 82–94.

[9] D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, "A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 3, pp. 1942–1976, 2020.

[10] S. Acharya, Y. Dvorkin, H. Pandzic, and R. Karri, "Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective," *IEEE Access*, vol. 8, pp. 214 434–214 453, 2020.

[11] K. Sayed and H. Gabbar, *SCADA and smart energy grid control automation*. Elsevier, 2017, pp. 481–514.

[12] A. O. Gomez Rivera, D. K. Tosh, and U. Ghosh, "Resilient sensor authentication in SCADA by integrating physical unclonable function and blockchain," *Cluster Computing*, vol. 25, no. 3, pp. 1869–1883, November 2021.

[13] A. Akkad, G. Wills, and A. Rezazadeh, "An information security model for an IoT-enabled Smart Grid in the Saudi energy sector," *Computers and Electrical Engineering*, vol. 105, p. 108491, January 2023.

[14] S. P. Mohanty, "Security and Privacy by Design is Key in the Internet of Everything (IoE) Era," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 4–5, March 2020.

[15] 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. IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. IEEE, June 2023, pp. 1–6.

[16] 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.

[17] S. Chanda, A. K. Luhach, W. Alnumay, I. Sengupta, and D. S. Roy, "A lightweight device-level Public Key Infrastructure with DRAM based Physical Unclonable Function (PUF) for secure cyber physical systems," *Computer Communications*, vol. 190, pp. 87–98, June 2022.

[18] 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.

[19] G. T. Sridhar, A. P, and N. Tabassum, "A Review on Quantum Communication and Computing," in *Proc. 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*. IEEE, May 2023.

[20] P. N. Singh and S. Aarthi, "Quantum Circuits – An Application in Qiskit-Python," in *Proc. Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, February 2021, pp. 661–667.

[21] S. M. Ardelean and M. Udrescu, "Circuit level implementation of the reduced quantum genetic algorithm using qiskit," in *Proc. IEEE 16th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, May 2022, pp. 000 155–000 160.

[22] E. h. Shaik and N. Rangaswamy, "Implementation of quantum gates based logic circuits using ibm qiskit," in *2020 5th International Conference on Computing, Communication and Security (ICCCS)*, 2020, pp. 1–6.

[23] C. Z. Chwa, L. A. Hsia, and L. D. Merkle, "Quantum Crosstalk as a Physically Unclonable Characteristic for Quantum Hardware Verification," in *Proc. NAECON 2023 - IEEE National Aerospace and Electronics Conference*, August 2023.

[24] K. Phalak, A. Ash-Saki, M. Alam, R. O. Topaloglu, and S. Ghosh, "Quantum PUF for Security and Trust in Quantum Computing," *arXiv preprint*, 2021.

[25] 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.

[26] 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," *Cryptography*, vol. 9, no. 2, p. 34, 2025.

[27] 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

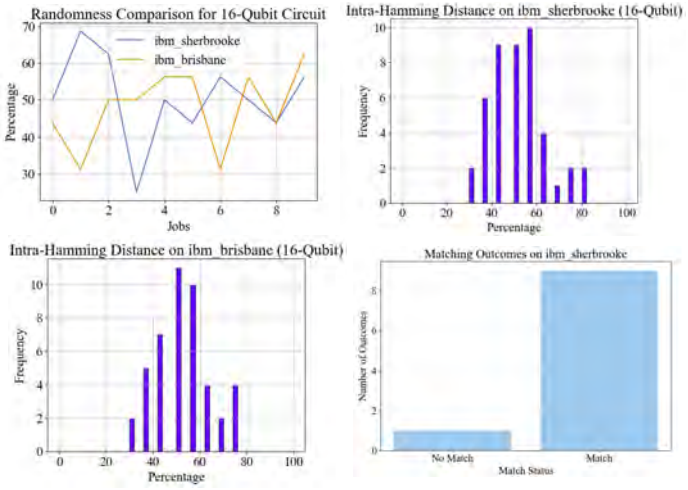
[28] B. Skoric, "Quantum readout of physical unclonable functions,"

```
Job 1: Using Initialization [1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0]
Job 1 ID: d0k6w2gfbx30008wq0q0
Most Frequent Outcome for Job 1: 1001000000010101
RY Angles Used (π/2 for 0-7, π for 8-15):
First 8 qubits: [1.57079633 1.57079633 1.57079633 1.57079633 1.57079633 1.57079633
 1.57079633 1.57079633]
Last 8 qubits: [3.14159265 3.14159265 3.14159265 3.14159265 3.14159265 3.14159265
 3.14159265 3.14159265]

Job 2: Using Initialization [1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0]
Job 2 ID: d0k6w4gfbx30008wq0rg
Most Frequent Outcome for Job 2: 1001010110010011
RY Angles Used (π/2 for 0-7, π for 8-15):
First 8 qubits: [1.57079633 1.57079633 1.57079633 1.57079633 1.57079633 1.57079633
 1.57079633 1.57079633]
Last 8 qubits: [3.14159265 3.14159265 3.14159265 3.14159265 3.14159265 3.14159265
 3.14159265 3.14159265]

Job 3: Using Initialization [0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0]
Job 3 ID: d0k6w6gcrrag008nbpag
Most Frequent Outcome for Job 3: 0110100100111100
RY Angles Used (π/2 for 0-7, π for 8-15):
First 8 qubits: [1.57079633 1.57079633 1.57079633 1.57079633 1.57079633 1.57079633
 1.57079633 1.57079633]
```

(a) QPUF Circuit Evaluation with 16 Qubits




(b) Performance Evaluation

Fig. 15: QPUF Performance Evaluation of 16-Qubit QPUF Circuit


*International Journal of Quantum Information*, vol. 10, no. 01, p. 1250001, 2012.

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

[30] 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.

[31] 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, DOI: https://doi.org/10.48550/arXiv.2410.12702.

[32] V. K. V. V. Bathalapalli, S. Mohanty, C. Pan, and E. Kougianos, "QPUF 3.0: Sustainable Cybersecurity of Smart Grid through Security-By-Design based on Quantum-PUF and Quantum Key Distribution," in *Proceedings of the Great Lakes Symposium on VLSI 2025*, ser. GLSVLSI '25. ACM, 2025, pp. 935–940.

[33] Q. Li, F. Chen, J. Su, Y. Yao, J. Kang, F. Xie, M. Li, and J. Zhang, "Quantum Physical Unclonable Function Based on Multidimensional Fingerprint Features of Single Photon Emitters in Random AlN Nanocrystals," *Advanced Functional Materials*, vol. 35, no. 9, 2024.

[34] K. Nilesh, C. Deppe, and H. Boche, "Information Theoretic Analysis of a Quantum PUF," in *Proc. IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2024, pp. 3320–3325.

[35] F. Cirillo and C. Esposito, "A QPUF-Based Scheme for Secure and Adaptable Quantum Device Attestation in NISQ Devices," in *Proc. International Conference on Quantum Communications, Networking, and Computing (QCNC)*, 2025, pp. 117–121.

[36] S. Ghosh, V. Galetsky, P. Julià Farré, C. Deppe, R. Ferrara, and H. Boche, "Existential unforgeability in quantum authentication from quantum physical unclonable functions based on random von Neumann measurement," *Physical Review Research*, vol. 6, no. 4, p. 043306, 2024.

[37] S. Goswami, M. Doosti, and E. Kashefi, "Hybrid Authentication Protocols for Advanced Quantum Networks," 2025.

[38] J. Ahn, T. Park, T. Kang, S.-G. Im, H. Seo, B.-H. Kim, S. J. Kwon, and S. J. Oh, "Nanoseed-based physically unclonable function for on-demand encryption," *Science Advances*, vol. 11, no. 17, 2025.

[39] K. Gołofit, "Security primitives for memoryless IoT devices based on Physical Unclonable Functions and True Random Number Generators," *Scientific Reports*, vol. 14, no. 1, 2024.

[40] N. W. Tun and M. Mambo, "Secure PUF-Based Authentication Systems," *Sensors*, vol. 24, no. 16, p. 5295, 2024.

[41] V. Padamvathi, B. V. Vardhan, and A. Krishna, "Quantum Cryptography and Quantum Key Distribution Protocols: A Survey," in *2016 IEEE 6th International Conference on Advanced Computing (IACC)*. IEEE, February 2016.

[42] M. S. Rahman and M. Hossam-E-Haider, "Quantum IoT: A Quantum Approach in IoT Security Maintenance," in *Proc. International Conference on Robotics,Electrical and Signal Processing Techniques (ICREST)*, January 2019.

[43] S. Sangari, "Providing Security in Internet of Things Using Quantum Cryptography," in *Advances in Systems Analysis, Software Engineering, and High Performance Computing*. IGI Global, April 2023, pp. 245–253.

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

[45] 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.

[46] J. Wu, T. Hu, and Q. Li, "Q-ID: Lightweight Quantum Network Server Identification through Fingerprinting," *IEEE Network*, pp. 1–1, 2024.

[47] J. Morris, A. Abedin, C. Xu, and J. Szefer, "Fingerprinting quantum computer equipment," in *Proceedings of the Great Lakes Symposium on VLSI 2023*, June 2023, pp. 117–123.

[48] G. Sharma, A. M. Joshi, and S. P. Mohanty, "An Efficient Physically Unclonable Function based Authentication Scheme for V2G Network," in *Proc. IEEE International Symposium on Smart Electronic Systems (iSES)*, December 2021.

[49] P. J. Mehta, B. L. Parne, and S. J. Patel, "ESAF: An Efficient and Secure Authentication Framework for V2G Network," in *Proc. 16th International Conference on COMmunication Systems and NETworkS (COMSNETS)*, January 2024.

[50] M. Kaveh, D. Martín, and M. R. Mosavi, "A Lightweight Authentication Scheme for V2G Communications: A PUF-Based Approach Ensuring Cyber/Physical Security and Identity/Location Privacy," *Electronics*, vol. 9, no. 9, p. 1479, September 2020.

[51] K. Hutto, S. Paul, B. Newberg, V. Boyapati, Y. Vunnam, S. Grijalva, and V. Mooney, "PUF-Based Two-Factor Authentication Protocol for Securing the Power Grid Against Insider Threat," in *Proc. IEEE Kansas Power and Energy Conference (KPEC)*. IEEE, April 2022.

[52] A. O. Gomez Rivera, D. K. Tosh, J. C. Acosta, and L. Njilla, "Achieving Sensor Identification and Data Flow Integrity in Critical Cyber-Physical Infrastructures," in *2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, November 2020.

[53] A. O. Gomez Rivera, E. M. White, and D. K. Tosh, "Robust Authentication and Data Flow Integrity for P2P SCADA Infrastructures," in *Proc. IEEE 46th Conference on Local Computer Networks (LCN)*. IEEE, October 2021.

[54] V. D. Jadhav, N. N. Moudhgalya, T. Sen, and T. V. Prabhakar, "IED$_{\text{PUF}}$ Probe: A PUF-Based Hardware Fingerprint Extraction Equipment for IEDs," in *2023 IEEE Physical Assurance and Inspection of Electronics (PAINE)*, 2023, pp. 1–7.

[55] Y.-N. Cao, Y. Wang, Y. Ding, H. Zheng, Z. Guan, and H. Wang, "A PUF-based Lightweight Authenticated Metering Data Collection Scheme with Privacy Protection in Smart Grid," in *2021 IEEE Intl Conf on Parallel and Distributed Processing with Applications, Big Data and Cloud Computing, Sustainable Computing and Communications, Social*

*Computing and Networking (ISPA/BDCloud/SocialCom/SustainCom)*, 2021, pp. 876–883.
[56] J. C. Bardin, D. Sank, O. Naaman, and E. Jeffrey, "Quantum Computing: An Introduction for Microwave Engineers," *IEEE Microwave Magazine*, vol. 21, no. 8, pp. 24–44, August 2020.
[57] H.-L. Huang, D. Wu, D. Fan, and X. Zhu, "Superconducting quantum computing: A review," *arXiv preprint*, 2020.
[58] M. Kjaergaard, M. E. Schwartz, J. Braumüller, P. Krantz, J. I.-J. Wang, S. Gustavsson, and W. D. Oliver, "Superconducting Qubits: Current State of Play," *Annual Review of Condensed Matter Physics*, vol. 11, no. 1, pp. 369–395, March 2020.
[59] K. N. Smith and P. Gokhale, "Trustworthy Quantum Computation through Quantum Physical Unclonable Functions," 2023.
[60] B. T. Torosov and N. V. Vitanov, "Qubit Control on IBM's Quantum Computing Devices," in *Proc. IEEE John Vincent Atanasoff International Symposium on Modern Computing (JVA)*, July 2023.
[61] "IBM Quantum," https://quantum.ibm.com/services/resources?system=ibm_brisbane, accessed on May 25, 2025.
[62] IBM Quantum, "IBM Quantum Backend: ibm_sherbrooke," https://quantum.ibm.com/services/resources?system=ibm_sherbrooke, 2025, accessed: 2025-05-24.
[63] 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
[64] R. Youssef, "Measuring and Simulating T1 and T2 for Qubits," Fermi National Accelerator Lab. (FNAL), Batavia, IL, United States, Tech. Rep., August 2020. [Online]. Available: https://www.osti.gov/biblio/1656632
[65] B. Blanchet, V. Cheval, D. Smyth, and M. Sylvestre, "ProVerif 2.00: Automatic Cryptographic Protocol Verifier, User Manual and Tutorial," May 2018, version 2.00, vol. 16, pp. 5–16, Inria. [Online]. Available: https://proverif.inria.fr
[66] I. Cervesato, "The Dolev-Yao intruder is the most powerful attacker," in *16th Annual Symposium on Logic in Computer Science—LICS*, vol. 1. Citeseer, 2001, pp. 1–2.
[67] 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
[68] C. Developers, "Cirq: A Python framework for creating, editing, and invoking Noisy Intermediate Scale Quantum (NISQ) circuits," 2024, accessed: Sep. 15, 2024. [Online]. Available: https://github.com/quantumlib/Cirq
[69] T. Alexander, N. Kanazawa, D. J. Egger, L. Capelluto, C. J. Wood, A. Javadi-Abhari, and D. C McKay, "Qiskit pulse: programming quantum computers through the cloud with pulses," *Quantum Science and Technology*, vol. 5, no. 4, p. 044006, August 2020.
[70] J. Wu, T. Hu, and Q. Li, "Detecting Fraudulent Services on Quantum Cloud Platforms via Dynamic Fingerprinting," in *Proceedings of the 43rd IEEE/ACM International Conference on Computer-Aided Design*, ser. ICCAD '24. ACM, October 2024, pp. 1–8.
[71] 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*, ser. HASP '21. New York, NY, USA: Association for Computing Machinery, 2022. [Online]. Available: https://doi.org/10.1145/3505253.3505261
[72] 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," in *Proceedings of the Workshop on Quantum Solutions for Technology Resilience and Infrastructure Development Enhancement (QSTRIDE), 26th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*. IEEE, 2025, accepted on 22 Apr 2025.

**Vishnu Bathalapalli** (Student Member, IEEE) is a Doctoral Student in the Department of Computer Science and Engineering at the University of North Texas, Denton, under the guidance of Dr. Saraju P. Mohanty in the Smart Electronic Systems Laboratory (SESL). He earned his Bachelor of Technology (B.Tech) in Electronics and Communication Engineering from Sri Venkateswara University, Tirupati, India. His research advances Security-by-Design (SbD) principles, ensuring robust data and device security within Healthcare and Energy Cyber-Physical Systems (CPS). He addresses security challenges from the design phase using hardware-assisted security primitives, including Physical Unclonable Functions (PUFs), Trusted Platform Modules (TPMs), Quantum PUFs, and Blockchain. A major focus of his work is Quantum Security-by-Design (QSbD), employing quantum-centric and quantum-hardware-based methods to enhance the trustworthiness of emerging Quantum Internet-of-Things (QIoT) applications. He has co-authored over 15 peer-reviewed journal and conference publications.

**Saraju P. Mohanty** (Senior Member, IEEE) received the bachelor's degree (Honors) in electrical engineering from the Orissa University of Agriculture and Technology, Bhubaneswar, in 1995, the master's degree in Systems Science and Automation from the Indian Institute of Science, Bengaluru, in 1999, and the Ph.D. degree in Computer Science and Engineering from the University of South Florida, Tampa, in 2003. He is a Professor with the University of North Texas. His research is in "Smart Electronic Systems" which has been funded by National Science Foundations (NSF), Semiconductor Research Corporation (SRC), U.S. Air Force, IUSSTF, and Mission Innovation. He has authored 550 research articles, 5 books, and 10 granted and pending patents. His Google Scholar h-index is 58 and i10-index is 269 with 15,000 citations. He is regarded as a visionary researcher on Smart Cities technology in which his research deals with security and energy aware, and AI/ML-integrated smart components. He introduced the Secure Digital Camera (SDC) in 2004 with built-in security features designed using Hardware Assisted Security (HAS) or Security by Design (SbD) principle.

He is widely credited as the designer for the first digital watermarking chip in 2004 and first the low-power digital watermarking chip in 2006. He is a recipient of 19 best paper awards, Fulbright Specialist Award in 2021, IEEE Consumer Electronics Society Outstanding Service Award in 2020, the IEEE-CS-TCVLSI Distinguished Leadership Award in 2018, and the PROSE Award for Best Textbook in Physical Sciences and Mathematics category in 2016. He has delivered 30 keynotesand served on 15 panels at various International Conferences. He has been serving on the editorial board of several peer-reviewed international transactions/journals, including IEEE Transactions on Big Data (TBD), IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), IEEE Transactions on Consumer Electronics (TCE), and ACM Journal on Emerging Technologies in Computing Systems (JETC). He has been the Editor-in-Chief (EiC) of the IEEE Consumer Electronics Magazine (MCE) during 2016-2021. He served as the Chair of Technical Committee on Very Large Scale Integration (TCVLSI), IEEE Computer Society (IEEE-CS) during 2014-2018 and on the Board of Governors of the IEEE Consumer Electronics Society during 2019-2021. He serves on the steering, organizing, and program committees of several international conferences. He is the steering committee chair/vice-chair for the IEEE International Symposium on Smart Electronic Systems (IEEE-iSES), the IEEE-CS Symposium on VLSI (ISVLSI), and the OITS International Conference on Information Technology (OCIT). He has supervised 3 post-doctoral researchers, 17 Ph.D. dissertations, 28 M.S. theses, and 28 undergraduate projects

**Chenyun Pan** (Senior Member, IEEE) received a B.S. degree in microelectronics from Shanghai Jiao Tong University, Shanghai, China, in 2010 and a Ph.D. in ECE from Georgia Institute of Technology in 2015. He is currently an Assistant Professor at the Department of Electrical Engineering, The University of Texas at Arlington. His research interests include device-, circuit-, and system-level modeling and optimization for energy-efficient Boolean and non-Boolean computing systems based on various emerging device and interconnect technologies. He has published over 70 peer-reviewed IEEE journal and conference papers. He is the recipient of two Best Paper awards in the IEEE International Symposium on Quality Electronic Design and IEEE Conference on IC Design and Technology, Research Spotlight Award in the School of ECE at Georgia Tech, and early career research program award from US Department of Energy.

**Elias Kougianos** (Senior Member, IEEE) received a BSEE from the University of Patras, Greece in 1985 and an MSEE in 1987, an MS in Physics in 1988 and a Ph.D. in EE in 1997, all from Louisiana State University. From 1988 through 1998 he was with Texas Instruments, Inc., in Houston and Dallas, TX. In 1998 he joined Avant! Corp. (now Synopsys) in Phoenix, AZ as a Senior Applications engineer and in 2000 he joined Cadence Design Systems, Inc., in Dallas, TX as a Senior Architect in Analog/Mixed-Signal Custom IC design. He has been at UNT since 2004. He is a Professor in the Department of Electrical Engineering, at the University of North Texas (UNT), Denton, TX. His research interests are in the area of Analog/Mixed-Signal/RF IC design and simulation and in the development of VLSI architectures for multimedia applications. He is an author of over 200 peer-reviewed journal and conference publications.