Article

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

Venkata K. V. V. Bathalapalli [1,†], Saraju P. Mohanty [2,†], Chenyun Pan [3,‡] and Elias Kougianos[4,†]

[1] Dept. of Computer Sci. and Eng., University of North Texas; vb0194@unt.edu
[2] Dept. of Computer Sci. and Eng., University of North Texas; saraju.mohanty@unt.edu
[3] Dept. of Electrical Eng., University of Texas at Arlington; chenyun.pan@uta.edu
[4] Dept. of Electrical Eng., University of North Texas; elias.kougianos@unt.edu

Abstract: This research investigates the integration of quantum hardware-assisted security into critical applications, including the Industrial Internet-of-Things (IIoT), Smart Grid, and Smart Transportation. The Quantum Physical Unclonable Functions architecture (QPUF) has emerged as a robust security paradigm, harnessing the inherent randomness of quantum hardware to generate unique and tamper-resistant cryptographic fingerprints. This work explores the potential of Quantum Computing for Security-by-Design (SbD) in the Industrial Internet-of-Things (IIoT), aiming to establish security as a fundamental and inherent feature. SbD in Quantum Computing focuses on ensuring the security and privacy of Quantum computing applications by leveraging the fundamental principles of quantum mechanics, which underpin the quantum computing infrastructure. This research presents a scalable and sustainable security framework for trusted attestation of smart industrial entities in Quantum Industrial Internet-of-Things (QIoT) applications within Industry 4.0. Central to this approach is the QPUF, which leverages quantum mechanical principles to generate unique, tamper-resistant fingerprints. The proposed QPUF circuit logic has been deployed on IBM quantum systems and simulators for validation. Experimental results demonstrate enhanced randomness and an intra-hamming distance of approximately 50% on the IBM quantum hardware, along with improved reliability despite varying error rates, coherence, and decoherence times. Furthermore, the circuit achieved 100% reliability on Google's Cirq simulator and 95% reliability on IBM's quantum simulator, highlighting the QPUF's potential in advancing quantum-centric security solutions.

Keywords: Industrial Internet-of-Things (IIoT); Quantum Security-by-Design (QSbD); Quantum Physical Unclonable Functions (QPUF)

1. Introduction

Quantum Computing is an emerging field transforming the computing paradigm, with exponentially more computational capability than classical computers. The basic unit of quantum computation is 'Qubit' which has the property to exist in a superposition of 0 and 1 simultaneously, in comparison to a Bit which can only be either 0 or 1 at any given time [1,2]. Leading companies such as IBM, Microsoft, and D-Wave Systems are providing cloud-based access to Quantum Computers, enabling the development and implementation of quantum applications and algorithms.

This research paper introduces a novel Quantum Computing-based Physical Unclonable Functions (QPUF) design, exploring the potential of Quantum Computing for enhanced security in Industrial Internet-of-Things (IIoT) applications. The proposed Quantum PUF Circuit is a novel quantum logic gates-based circuit evaluated on IBM quantum computers. It enhances security in smart electronics by enabling a quantum hardware-generated PUF key as a unique device identity. This work proposes a new QPUF topology incorporating Hadamard, CNOT, Pauli-X, and Ry gates for deployment in QPUF driven by quantum superposition, and entanglement principles. Experimental evaluation of proposed QPUF on IBM superconducting quantum hardware validates its feasibility

Citation: Lastname, F.; Lastname, F.; Lastname, F. Title. *Cryptography* **2023**, *1*, 0. https://doi.org/

Received:
Revised:
Accepted:
Published:

with key metrics evaluated to showcase its potential for the Quantum Security-by-Design (QSbD) of IIoT.

Securing an IIoT involves enhancing its resilience against malicious cyberattacks. Unauthorized access or breach in the IIoT network, which could be either an actuator executing industrial operations based on commands or a smart sensor performing data collection can compromise the security of the entire industrial environment. Ensuring the trustworthiness of these devices is essential to counter any potential cyber threats [3–5]. From a communication perspective, where IIoT communicates with an edge gateway or cloud, snipping or network traffic snooping attacks can expose secure information, enabling malicious entities to seize control and corrupt the commands. Furthermore, data security and privacy are essential and require robust regulatory mechanisms to protect sensitive information[3]. Quantum cybersecurity solutions can address the security gaps in all the above scenarios particularly, QPUF ensuring the reliability of IIoT systems at the physical layer performing various tasks such as machinery fault detection, data sensing, actuation, and relay protection. The trustworthiness of these devices at the physical layer ensuring data integrity is an essential factor for control and analysis at the business layer [6,7].

1.1. PUF Overview

PUF is a Hardware security primitive that utilizes hardware intrinsic device properties for cryptographic keys generation by utilizing device level variations to generate a unique bit stream of 0 and 1 as output which cannot be regenerated due to manufacturing process variations unique for each device [8,9]. A PUF primitive captures process variations by mapping a given challenge input to a unique binary response, typically represented as a sequence of 0s and 1s, which can serve as a key. PUFs are classified as strong and weak based on the intrinsic properties utilized to generate cryptographic keys such as variations in the power-up of a memory cell, oscillator frequency variations, and logic circuit path delays. PUF designs are classified based on the cryptographic key generation capability. PUFs that support a higher number of Challenge-Response pairs (CRP) are strong PUFs, while PUF designs that support a minimal number of CRPs are weak PUFs. SRAM and DRAM PUFs which are deployed based on variations in memory cells are weak. Whereas Arbiter and Ring Oscillator PUFs deployed based on frequency and delay variations in an IC are strong PUFs [8,10].

Once generated from the PUF module, a key will be unique for a challenge input and cannot be regenerated on another device even with the same PUF design and input. Ideally, a PUF-generated key should exhibit a hamming distance of 50%, indicating the percentage of differing bit positions among responses from a device. The ideal intra-hamming distance, which measures intra-response variations within the same device under various conditions, should range between 40-50%. Prominent PUF key evaluation metrics are summarized below [6,8]:

Diffuseness: Diffuseness of a PUF in a device represents the degree of variation in PUF responses to varying challenge inputs. It quantifies the variation in responses due to the slightest changes in challenge inputs.

Reliability: A PUF on a device should be able to generate the same response for a challenge input under varying environmental and operating conditions. Percentage of reliability represents the stability of a PUF to regenerate a response under varying conditions.

Uniqueness: Uniqueness of a PUF quantifies the variation of PUF responses when tested on different devices. It is calculated by obtaining the average inter-hamming distance of responses for a PUF on different devices. The uniqueness value is proportional to the process variation and the ideal uniqueness of a PUF should be around 50%.

Uniformity: PUF's uniformity is a measure of the probability of each bit in the PUF response key to be either 0 or 1. The ideal uniformity of a PUF should be 50%, indicating a unique distribution of 1s and 0s in a PUF response for maximum randomness and security.

1.2. Quantum Physical Unclonable Functions for Secure I-CPS

Quantum Physical Unclonable Functions (QPUF) is a primitive that generates a unique fingerprint for a quantum computer, leveraging the inherent randomness of quantum hardware driven by the principle of quantum mechanics [11,12]. A QPUF-generated response for each quantum hardware can ensure security and privacy in quantum information processing and communication. QPUF harnesses unique quantum hardware variable parameters, more specifically qubit coherence, decoherence times, and gate errors across various quantum computers [13,14].

This work explores the scope of Quantum-assisted cybersecurity in industrial IoT applications by implementing QPUF technology on Quantum Hardware. Quantum computing's potential in advancing computational capability to the next level surely has great potential in Industry 4.0. This work aims to leverage the potential of SbD in Quantum computing for IIoT security by proposing a QPUF-based device authentication and access control mechanism that ensures the security of the device, firmware, and network communication in IIoT. A conceptual overview of QPUF for SbD of I-CPS is shown in Fig. 3. Executing QPUF-based security solutions in I-CPS can improve the efficiency of industrial operations, particularly as IIoT frameworks increasingly rely on cloud computing [5]. Most of the PUF-based security solutions work by connecting physical hardware for key extraction and validation [6].This approach can reduce scalability as the number of IoT devices increases based on the application. The proposed QPUF-driven security approach establishes a robust cloud-based authentication framework among all entities in I-CPS, where a QPUF generated fingerprint ensures the reliability of both communication and data. Since current quantum computing applications are primarily cloud-based, this approach further enhances scalability in emerging quantum-driven I-CPS environments. A conceptual overview of the proposed QPUF-based secure I-CPS architecture is depicted in Fig. 1.

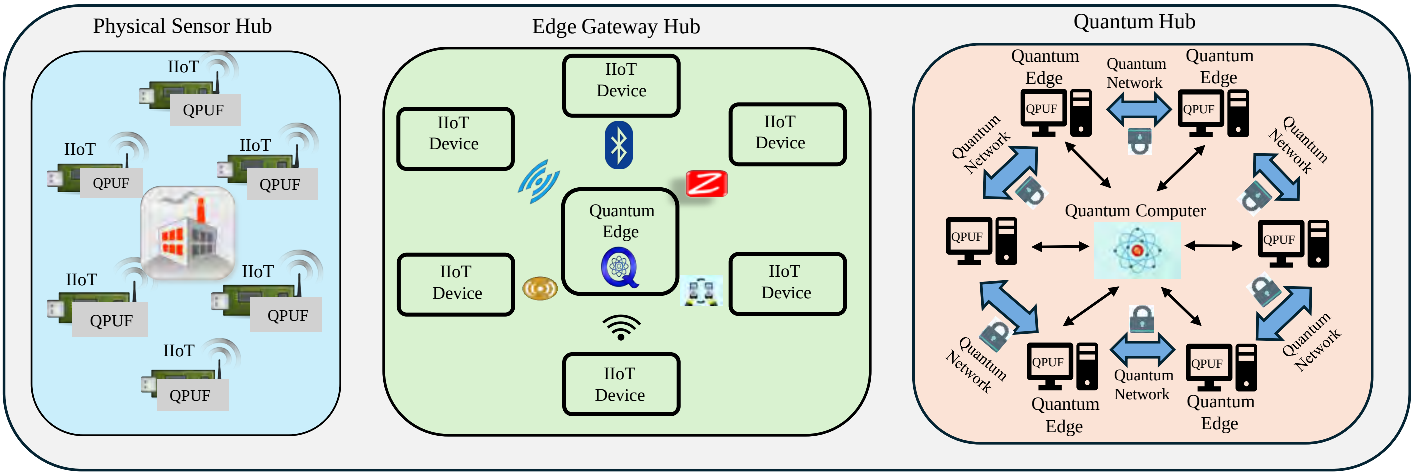


Figure 1. Conceptual Framework of QPUF for Securing Industrial Cyber-Physical Systems (I-CPS)

In I-CPS, all the smart actuators, machines, and smart sensors can be connected to the edge cloud environment for uploading sensitive parametric data related to machines, and production metrics [15]. To ensure device authenticity and integrity, quantum hardware can be accessed through the cloud to generate a unique response driven by quantum mechanics. Clusters of smart actuators and sensors can get unique quantum hardware-generated security keys from QPUF at the quantum computer ensuring secure authentication. The IIoT devices are controlled and monitored by Supervisory control and data acquisition systems (SCADA) ensuring intelligent management control, and communication among various entities in I-CPS. SCADA-based management systems include Human-Machine Interface, Remote and Master Terminal Units, and centralized command control for data sensing, communication, and decision-making tasks [5].

Quantum computing integration can further their capabilities ensuring efficient data processing, secure quantum channel-driven communication, and quantum-hardware-assisted device attestation in I-CPS. The advantage of including QPUF-based security mechanisms in Industrial environments is the easier integration of cloud computing systems in I-CPS in the present age, with the potential for even more straightforward integration with quantum chips in the future [4]. An overview of the proposed QSbD primitive for IIoT is presented in Fig. 2.

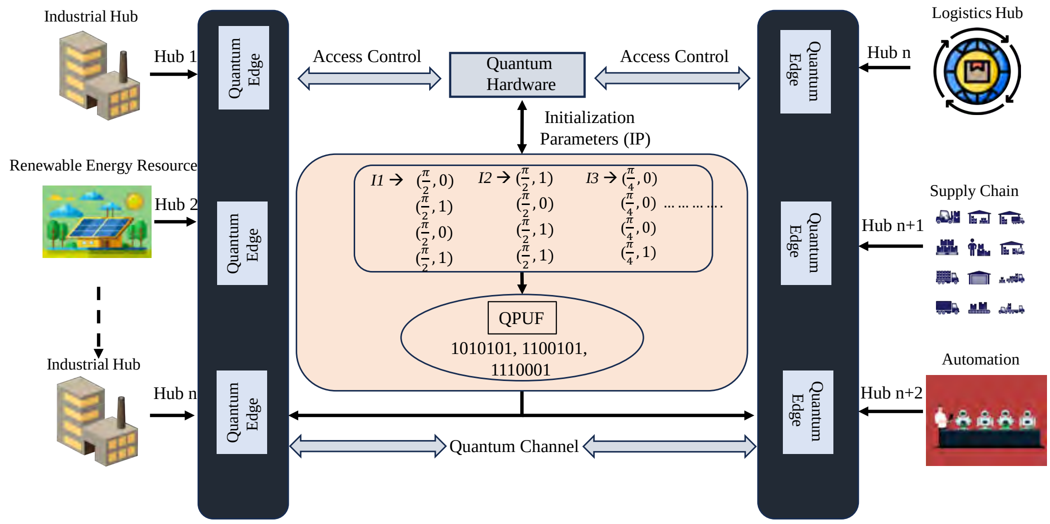


Figure 2. QPUF-driven QSbD Primitive for IIoT

The rest of this paper is organized as follows. A conceptual idea of SbD and QSbD, along with their strategies and principles is outlined in section 2. Section 3 illustrates the contemporary related works in IIoT security. Section 4 discusses the contributions of this research work. The preliminaries and working model of the proposed QPUF architecture are discussed in section 5. QPUF Experimental validation results along with challenges have been presented in section 6. Finally, the conclusion and future work is discussed in Section 7.

2. Security-by-Design in Quantum Computing

Security-by-Design (SbD) advocates security practices from the initial phase of the product development cycle rather than implementing them during the application phase to address issues affecting performance and reliability. SbD ensures the security as a fundamental feature of the product, that can sustain any attacks through intensive testing and evaluation against various possible security invasive events and vulnerabilities [16]. Privacy-by-design (PbD) is analogous to the SbD approach, focusing more on the development of a product with privacy protection mechanisms as in-built functionalities capable of ensuring the confidentiality or privacy of data processing as a default working functionality completely embedded into the design. SbD/PbD principles define and drive the security ecosystems during the design or product development stage. The examples of SbD include Windows 11 Operating System supporting Windows Hello and TPM 2.0 for secure biometric sign-in and hardware-based protection for business along with the boot process ensuring a secure startup environment allowing devices to boot up with manufacturer-trusted software [17]. With SbD, security practices integrated at the design level form a foundation that cannot be tampered with easily without changing the core design or product configuration. A comprehensive overview of Security-by-Design strategies is provided below [18] and presented in Fig. 3:

Threat Modelling is a key SbD component, performing analysis of the security vulnerabilities of a product from the adversarial perspective. This includes enabling, proactive identification, analysis, and mitigation of potential threats during the early stages of the product development cycle such as identifying critical assets such as firmware and data credentials that require protection and performing an evaluation of external threat factors including malware, and insider threats. This approach helps organizations to evaluate security practices such that they align with industry security standards such as NIST and ISO 27001. Threat modeling and risk assessment should be adopted as a bottom-up approach during product development and its deployment starting from physical hardware, network, operating systems, software, database storage, and supply chain. The working flow of threat modeling includes identifying the vulnerabilities at the hardware, firmware, and software level of the system, identifying critical system assets and data processing flow, evaluating ways of potential adversarial threats and vulnerabilities, and finally, proposing security countermeasures, such as encryption, authentication, secure boot, hardware-assisted security, and Trusted execution environment (TEE)[16].

Defense in Depth is an SbD strategy that emphasizes a layered security approach with multiple layers of primitives to protect systems, data, and networks from threats. This strategy helps in addressing single-point-failure problems and can minimize risks even if the security at one layer is compromised. A layered approach for access control and authorization can minimize adversarial access to the product's data and its resources. This includes employing runtime security agents, firewalls, and intrusion detection systems to protect the systems' access from adversaries. Additionally, multi-factor, biometric authentication, and least privilege principles ensure identity and access management. Multi-factor authentication is a layered approach for ensuring trust and authenticity of systems access and control. With MFA-based approaches, Amazon has reported a 99% drop in password-based attacks [19].

Hardware-Root-of-Trust: ensures a trustworthy execution environment for cryptographic operations, authentication, and secure boot. To ensure security right from the foundational level of the product, hardware primitives such as PUF and TPM provide various security functionalities, ensuring manufacturer-trusted firmware and software execution during system boot, cryptographic keys storage, and hardware-secure execution environment to perform computations securely. A secure cloning and hardware-tampering-resistant approach using PUF ensures reliable and efficient security using inherent silicon variations. Furthermore, hardware-centric fine-grained memory protection through TPM providing tamper-proof storage stands as a key SbD strategy [20].

Secure AI Applications advocates for security and privacy at every stage of AI model development, deployment, and operation using the principles of SbD. The training and quality of sensitive data, which includes personal, operational, and financial information could be poisoned to compromise model integrity. Furthermore, extracting medical data from AI-based healthcare models could jeopardize their applications. To address this, security should be seen as an incorporated feature of AI and ML applications such as performing adversarial training to make AI models resistant to perturbations and employing secure AI accelerators deployed with security primitives like TPM and PUF. Other possible application scenarios include applying security and privacy-enabled features for deepfake detection and mitigation using secure AI accelerators preventing unauthorized use of personalized social media through various approaches such as hardware-root-trust for watermarking and storage, and a lightweight distributed ledger for secure data access and storage. The key principles of Security-by-Design (SbD) are outlined below [20]:

Proactive not Reactive: SbD emphasizes adopting systems' security practices as a proactive approach rather than an afterthought. This includes adopting threat modeling and code scanning approaches to identify potential vulnerabilities and threats.

User-Centric: The security practices adopted should be user-friendly not fiddling with the systems operations and control while ensuring robust inbuilt security systems are in place. This could be achieved through MFA facilitating secure user access to systems applications where systems access is ensured for specified users with robust authentication that works internally while being user-centric through supportive approaches like user-chosen passwords.

Figure 3. Security-by-Design Strategies

Embedded into the Design: SbD ensures security from the very beginning of the product development and is completely embedded at the system architectural level.

Full Functionality- Positive-Sum, not Zero-Sum without trade-offs: SbD solutions should not have tradeoffs impacting the system performance and efficiency and should be mutually reinforcing without requiring to choose between security and efficiency.

End-to-End Security and Privacy for Lifecycle Protection: Security and privacy measures should be adopted to ensure integrity and reliability throughout the cycle from system development to application-level deployment.

Visibility and Transparency: Users and organizations should have a clear idea of the security practices and access control mechanisms in place. This includes transparency in the policies implemented, open security standards AI-assisted intelligent automated decision-making systems.

Respect for Users: Security and privacy policies should not overpower users restricting access rather than ensuring user consent, user-centric systems and data access control, and regulated ethical AI principles for deployment such as privacy-focused data search.

QSbD focuses on quantum computing application security and emphasizes quantum mechanics as driving principles to ensure the security, privacy, and efficiency of an application right from the development stage. This approach analogous to SbD focuses on building and deploying quantum computing algorithms and applications with security and privacy as default primitives harnessing quantum mechanical principles. Quantum's no-cloning theorem states that it is impossible to copy or clone the arbitrary unknown quantum state and Heisenberg's uncertainty principle states the impossibility of absolutely determining the position of a particle [21]. These principles serve as the driving forces for QSbD ensuring hardware-root of trust, secure and encrypted communication along with enhanced computational processing power which is exponentially more when compared with classical computing validates its potential for emerging Quantum IoT applications [22].

3. Related Research

This section briefly discusses the related prior research on QPUF and security approaches for Industrial IoT systems.

In [11], it is observed that crosstalk in superconducting transmon qubits impacts the quantum state of a qubit. Based on this observation, the QPUF signature generation process is defined using a Ramsey experiment, which determines the absolute resonant frequency of a qubit. Crosstalk introduces noise, thereby affecting the resonant frequencies of other qubits. A novel QPUF architecture that leverages quantum decoherence and entanglement to generate a unique bitstream of random zeros and ones is proposed in [21]. The evaluation of the QPUF architecture has demonstrated reliable QPUF response generation using quantum Ry, CNOT, Pauli-X, and Hadamard gates.

A novel Quantum tunneling PUF, titled Neo PUF, has been proposed, which operates by storing the PUF signature within an ultra-thin oxide layer, ensuring reliability. This PUF leverages manufacturing variations in oxide thickness to generate unique signatures [23]. The authors in [24] proposed Quantum circuit-based PUF designs that rely on tunable rotation angles for the Ry gate. However, their work does not provide an experimental demonstration of the final PUF signature generation. In contrast, our work experimentally validates the QPUF design implemented using Quantum Logic gates and explicitly defines PUF signatures through approximation. Furthermore, in this protocol, an unverified party cannot intercept communication over the quantum channel between two trusted entities [25,26]. In contrast to the previously discussed research on QPUF, the proposed work focuses on achieving enhanced reliability by leveraging quantum entanglement and superposition principles to drive the QPUF circuit. While prior studies have highlighted the need for further improvements in QPUF calibration to attain reliability, they fall short in this regard. This research introduces a novel QPUF topology that enables a scalable Challenge Response generation with improved randomness, uniqueness, and notably reliability

A novel PUF-based blockchain, named HPCchain, has been proposed in [27] for security and device authentication in IIoT. This work introduces a consortium Blockchain framework with a PUF-based consensus mechanism. The architecture of HPCchain is structured into four layers: Asset, Blockchain, Data, and Application. The Asset layer comprises PUF-embedded smart sensors, machines, and industrial actuators. The Blockchain layer operates on top of the asset layer, handling transaction recording and validation. The Data and Application layers operating above the Blockchain are responsible for analysis, processing, decision-making, and actuation.

A novel approach for sensor data stream integrity verification using PUF in Industrial-Cyber-Physical Systems (I-CPS) is proposed in [7]. This work introduces a PUF-based method to ensure secure communication between PLC nodes and sensor nodes in Industrial environments. By embedding smart sensors with PUF modules, this approach claims to mitigate side-channel attacks. A secure Machine-to-Machine (M2M) communication mechanism leveraging PUF for IIoT has been proposed in [28]. This work introduces a PUF-based Efficient Authentication and Session Establishment (PEASE) protocol, designed to achieve device identity confidentiality with minimal computational power and energy overhead. In [6], a pseudo-PUF-based IIoT security mechanism is proposed, utilizing a weak PUF module with limited Challenge-Response Pairs (CRPs) along with a lightweight symmetric encryption module. This approach focuses on reducing energy overhead while enhancing the resiliency of the Pseudo PUF. A simple Quantum random generator (QRNG) for security in IIoT applications is proposed in [4]. This work implements QRNG on both a quantum simulator and real quantum hardware, demonstrating a quantum virtual private network-based communication framework for IIoT devices and cloud systems. However, it does not provide details on the feasibility of QRNG across various hardware backends and the impact of noise on system performance. Additionally, a QIoT framework leveraging quantum entanglement for IoT sensor data attestation using Blockchain is proposed in [29]. This framework is designed for various applications such as manufacturing monitoring, logistics, and smart grid renewable energy resource management. A comprehensive analysis of the research works on QPUF and PUF based security approaches for IIoT systems is presented in Table 1.

Table 1. Related Research on PUF and QPUF-Based Security for IIoT Systems

Research Works	Security Mechanism	Approach	Platform	Features
Gong et al.[28]	PUF-based Authentication in IIoT	PUF, Fuzzy extractor	Cloud Computing	Secure Machine to Machine communication
Ahmad et al. [4]	QRNG based sensor security	Quantum hardware generated random number	IBM's Quantum Cloud	Scalable
Shan et al. [7]	PUF-based sensor security	SRAM PUF, HMAC Algorithm	SCADA System	Industrial sensor data integrity
Qian et al. [27]	PUF-based Blockchain for IIoT	Hybrid PUF, Consortium Blockchain	NA	CPU & FPGA based PUF with enhanced uniqueness
Barbareschi et al. [6]	Pseudo-PUF for Industrial IoT	Weak PUF, Encryption Module	NA	Low energy overhead
Prajwal et al. [30]	Quantum safe authentication for IIoT security	Quantum PUF, Hash function, XOR encryption	Node MCU and Scyther	No requirement of non-volatile memory
QPUF (Current Paper)	Quantum Computing based PUF for IIoT	QPUF based on Quantum logic gates	Google Cirq, IBM's Qiskit	Reliable QPUF responses from simulator exhibiting excellent uniqueness and randomness

4. Novel Contributions

This section discusses the research problems addressed in the context of SbD of IIoT systems, highlights the key contributions of the proposed research, and outlines the proposed methodology.

In IIoT systems, various wireless network communication protocols enable seamless interaction among IIoT entities. However, these entities are susceptible to numerous cyber threats and attacks. Adversarial access to even a single entity can compromise the security and integrity of the entire industrial infrastructure, potentially leading to equipment malfunctions, system outages, or tampering with control mechanisms and sensor data. The development of quantum chips has amplified interest in their potential across domains such as Artificial Intelligence, IoT, and Blockchain. However, the integration of quantum computing still presents significant challenges, particularly in interoperability and infrastructure. The proposed research aims to investigate the scope of its application, enhancing security and privacy, guided by the principles of quantum mechanics.

4.1. Research Problems Addressed in the Current Paper

- Challenge of scalable and tamper-proof attestation for IIoT devices in resource-intensive smart industries.
- Challenge of ensuring reliable communication among various entities within industrial IoT systems.
- Problem of Quantum sensor attestation and achieving tamper-proof authentication for IIoT systems.
- Problem of generating reliable QPUF responses from inherently noisy quantum computers.

The proposed research introduces a novel QSbD framework to transform IIoT systems through a sustainable, quantum hardware-assisted security framework. Central to this framework is the QPUF, which provides a robust authentication mechanism to ensure the security and integrity of both devices and data. As a unique hardware security primitive, the QPUF holds significant promise for quantum-centric security. This research presents an innovative QPUF topology that leverages quantum mechanics principles. The key contributions and novel features of the proposed research are further detailed below:

4.2. Proposed Solution and Methodology

- A QPUF CRP generation method for noisy quantum computers
- QPUF-based secure digital fingerprint for Intelligent Electronic Devices (IED), and smart industrial automation systems, and machines in IIoT.
- A novel QPUF key generation and identity attestation method for IIoT devices using noisy quantum computers.
- A robust quantum-hardware-assisted device attestation framework for SCADA-IIoT systems.
- An intelligent device and data security approach enabled by QPUF.
- An approach utilizing quantum principles of entanglement and superposition.
- A QPUF architecture implemented with Quantum CNOT, Ry, and H gates and evaluated on IBM quantum systems.

4.3. Novel Features of the Proposed Solution

- A sustainable approach for QPUF response generation with 100% reliability.
- A QPUF architecture that demonstrates significant randomness when evaluated on the IBM quantum simulator.
- A state-of-the-art solution aimed at enhancing the reliability of quantum computing for Industrial IoT frameworks.
- A sustainable method for quantum noise reduction and reliable QPUF response generation.

5. Proposed Quantum Security-by-Design (SbD) Approach for IIoT

This section gives a comprehensive overview of the architecture of QPUF in sec.5.1 and secure device attestation and communication framework for Smart Grid in sec. 5.2.

5.1. Proposed QPUF Architecture

The proposed Quantum Physical Unclonable Functions (QPUF) utilizes an 8-qubit architecture, incorporating both single and two-qubit quantum logic gates. Quantum Hadamard, Ry, and CNOT measurement gates have been employed for evaluating the QPUF. The CNOT gate entangles the first four qubits with the last four qubits, allowing the evaluation of how the superposition created by Hadamard and Ry logic gates affects the quantum state of the entangled qubits. Initially, all qubits are initialized randomly using the Pauli X-gate, followed by the application of the Ry gate, which introduces variability into their quantum states. Subsequently, the Hadamard gate is applied to all the first four qubits(control qubits) to create a superposition of quantum states, and the impact of this superposition of control qubits on target qubits is analyzed. The architecture of the proposed QPUF is presented in Fig. 4.

The performance of the QPUF is influenced by factors such as gate fidelity, Qubit decoherence and coherence times, and noise. Qubits can lose their quantum state due to interactions with the environment. These factors vary across different hardware, and the placement of qubits may differ depending on the specific architecture. Quantum hardware operates at extremely low temperatures and relies on silicon-based architecture featuring Josephson junctions which are structures consisting of a thin insulating layer sandwiched between two superconducting electrodes. microwave pulses, applied with precise timing and phase, can cause transitions between energy levels. The quantization of these energy levels results in computational basis states of 1 and 0. The QPUF circuit evaluation procedure is detailed in the Algorithm. 1 and the mathematical representation of QPUF circuit logic is presented below.

$$X|k\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} k_0 \\ k_1 \end{bmatrix} = k_0|1\rangle + k_1|0\rangle \tag{1}$$

$$\text{CNOT} \cdot (k_0|1\rangle + k_1|0\rangle) \otimes |0\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} k_0 \\ k_1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} k_0 \\ k_1 \\ k_0 \\ k_1 \end{bmatrix} \tag{2}$$

$$R_y(\theta) \begin{bmatrix} k_0 \\ k_1 \\ k_0 \\ k_1 \end{bmatrix} = \begin{bmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{bmatrix} \begin{bmatrix} k_0 \\ k_1 \end{bmatrix} \tag{3}$$

$$H \begin{bmatrix} k_0 \\ k_1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} k_0 \\ k_1 \end{bmatrix} \tag{4}$$

$$\text{QPUF state} = \text{Measurement} \cdot H \cdot R_y(\theta) \cdot \text{CNOT} \cdot X \cdot (q_0|0\rangle + q_1|1\rangle) \otimes |0\rangle \tag{5}$$

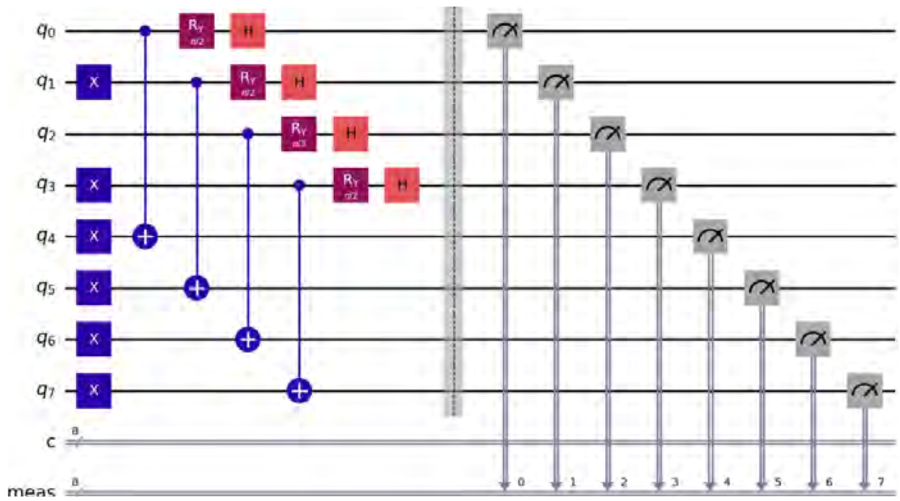


Figure 4. Proposed QPUF Architecture

5.1.1. IBM Quantum Hardware Unclonable Hardware Parameters

TI (us): T1 time, also known as the energy relaxation time, represents the duration a qubit remains excited before relaxing to the ground state. Measured in microseconds, a higher T1 value indicates greater quantum state stability. T1 time can be improved through qubit fabrication techniques and by minimizing microwave noise and crosstalk, which can disrupt qubit interactions and alter their resonant frequencies.

T2 (us): T2 Time, also known as the decoherence time, is the duration, a qubit maintains its quantum superposition before its phase relationship is lost due to the qubit's interaction with the environment, which affects the qubit's resonant frequency, noise causing crosstalk with other qubits, and magnetic field fluctuations. Unlike T1 time, which represents energy loss, T2 characterizes how long a qubit retains its phase coherence without necessarily changing its energy state.

Frequency: A qubit's natural operating frequency, or resonant frequency, typically ranges from 2-6 Hz on IBM quantum hardware. This frequency is crucial to performing quantum state calibrations and executing quantum algorithms, as microwave pulses must be precisely tuned to the qubit's resonant frequency.

Algorithm 1: QPUF Circuit Evaluation

Input: Qubits
Output: Job String

1: initialize Qubits in QPUF circuit Randomly (Varying Initializations)
Example:
Qubit 0 → 0, Qubit 1→1, Qubit 2→1, Qubit 3→0, Qubit 4→0, Qubit 5→1, Qubit 6→1, Qubit 7→0, Qubit 8→0
2: Entangle Qubits using CNOT gate
q0–>q4, q1–>q5, q2–>q6, q3–>q7
3: Apply Ry gate to control qubits with predefined angles
qc.ry(angle$_i$)–> q0, qc.ry(angle$_i$)–> q1, qc.ry(angle$_i$)–> q2, qc.ry(angle$_i$)–> q3
4: Apply Hadamard gate to control qubits to create a superposition
qc.h(q0), qc.h(q1), qc.h(q2), qc.h(q3)
5: Apply Measurement gate to measure the quantum states of qubits
6: Obtain IBM Quantum Application Programming Interface (API) token
7: Choose the quantum backend
8: Specify measurement counts for a job
9: Execute circuit
10: Obtain jobs strings which a unique job string obtained from all 8 qubits for 1024 shots
shot 1: 1010110, shot 2:0010101......

Anharmonicity Anharmonicity defines the energy level separation in a qubit, influencing its ability to selectively transition between quantum states. It plays a key role in reducing unwanted transitions and improving qubit control.

Readout Assignment Error: Readout assignment error quantifies the probability of incorrectly measuring a qubit's quantum state. For instance, if a qubit $|0\rangle$ is mistakenly read as $|1\rangle$, this contributes to readout error. Lower readout assignment error indicates higher measurement fidelity, ensuring more accurate quantum state detection. Each qubit has a distinct readout assignment error probability, which directly affects the reliability of quantum computations.

Gate Fidelity Gate Fidelity measures how accurately a quantum logic gate performs its intended operations compared to an ideal, noiseless scenario. It ranges from 0 and 1, with higher values indicating more robust and precise gate operations. Fidelity is influenced by noise, qubit fabrication inconsistencies, and calibration fluctuations. Each quantum logic gate has an associated fidelity value that reflects its ability to accurately perform operations while minimizing the effects of noise on the quantum state.

5.2. QPUF for Secure IIoT Systems

Smart sensors or industrial IoT devices can be equipped with quantum computing capabilities, enabling advanced sensing and actuation in Industry 4.0. These applications include monitoring renewable energy resource generation, controlling outages, enabling predictive maintenance, facilitating real-time industrial equipment diagnostics, and supporting autonomous control of industrial processes through IIoT sensors and actuators. The QPUF can generate a unique fingerprint for each quantum node facilitating sensor data attestation and ensuring sustainable security [29]. Each intelligent quantum electronic device can perform tasks such as fault localization, anomaly detection, and predictive maintenance. These IIoT devices can leverage quantum computing capabilities via the cloud, enabling access to the quantum hardware-generated digital fingerprints through QPUF. The QPUF-generated key for an IIoT device establishes secure communication with edge-cloud platforms for data processing, ensuring reliable and tamper-proof connectivity in the emerging quantum internet era. The workflow of the proposed QPUF-IIoT attestation mechanism is illustrated in Fig. 5.

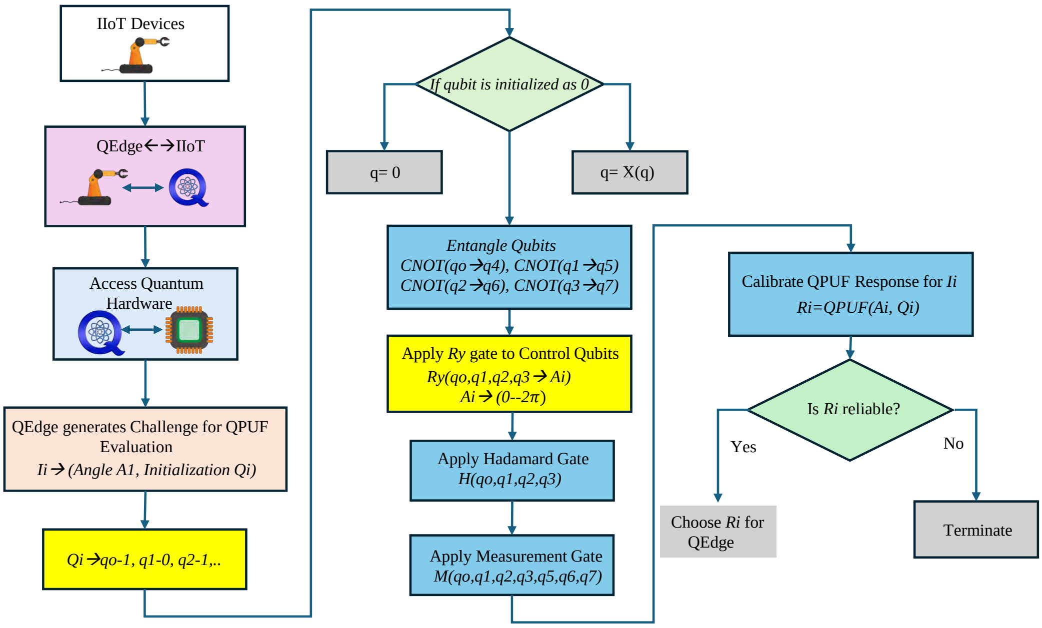


Figure 5. Working Flow of QPUF for Secure IIoT Systems

5.3. Noise Suppression Mechanism

To enhance noise suppression, after executing n jobs as an instance i on quantum hardware, additional instances i_n of jobs are evaluated with similar initialization parameters k_n on the same backend b to evaluate reliability. The final job strings obtained for all jobs j_i across all instances i_n are analyzed to compute the hamming distance H_D among them. The most frequently occurring measurement outcome across all shots s_n within a job is selected as the final job string. Among all instances, the most consistently matching final job string r_i is identified as the final QPUF reliable response key. The corresponding initialization parameters c_i used across all instances are recorded for further evaluation. The QPUF response generation and noise suppression approach is detailed in the Algorithm. 2.

6. Experimental Results

The proposed QPUF architecture is evaluated using IBM quantum systems and simulators. The IBM Qiskit's "qasm_simulator" is selected for the evaluation, with a total of 100 jobs executed on the simulator across five instances. In each job, all the qubits in the QPUF are randomly initialized using the Pauli X-Gate. For each job, 1024 measurement outcomes or shots are obtained. The most frequently occurring outcome is chosen as the QPUF response key for that job. A total of 100 jobs were executed with 100 unique qubit initializations, utilizing predefined Ry gate angles of [pi/4, pi/2, pi. 3pi/2] applied to entangled control qubits. Five instances of these 100 jobs were conducted on the "qasm_simulator" via the IBM Qiskit Run Time service [31], which enables the users to submit jobs directly to IBM's Quantum systems. For evaluation, Python programming language is used, and the Quantum PUF metric evaluation is performed on obtained results. After acquiring an Application Programming Interface (API) token from IBM, Qiskit Run Time is loaded, and the QPUF circuit is implemented and transpiled. Transpilation in Qiskit Run Time optimizes the circuit logic by considering chosen quantum backend's qubit connectivity and supported gates, thereby enhancing execution efficiency. Sampler v2 is used for executing quantum circuits in the Qiskit 1.0 version. The evaluation of the QPUF circuit on ibm_brisbane is shown in Fig. 6. Additionally, the proposed QPUF was also evaluated on the Google Cirq simulator [32] with similar qubit initialization states chosen for evaluation on qasm_simulator and tunable rotation angle of 90^o. The performance evaluation metrics for the QPUF on Cirq simulator and qasm simulators are presented in Fig. 7. The quantum computing development environment was set up on a Personal

Algorithm 2: Working Flow of Proposed QPUF Noise Suppression Mechanism

Input: Initialization Parameters k_I
Output: Most Reliable QPUF Response
initialize Qubits (Varying Initializations)
Example:
Qubit 0 → 0, Qubit 1→1, Qubit 2→1, Qubit 3→0, Qubit 4→0, Qubit 5→1, Qubit 6→1, Qubit 7→0, Qubit 8→0
Choose fixed initialization parameters for all the instances of jobs on backend b_1
Choose Ry gate to all Control qubits with a predefined set of initialization angles after entangling
Execute 5 sets of angles for all sets of initializations
Ry Angle→pi/4, pi/2...
Apply Measurement Gate(M) to measure the quantum states of all qubits
Obtain the most frequently occurring measuring outcome as job string
for For a job j_i in an instance i_1 with 1024 shots **do**
    Choose the most frequent outcome obtained from all shots as job string (10101011:5, 11001101:6..)
    Obtain the job strings for all jobs j_1 in instance i_1
end for
Extract results string from all job instances i_n
Calculate the Reliability of all job strings in instances i_n
if Job string j_i obtained is frequently occurring in all instances i_n **then**
    Choose j_i as the QPUF response r_i for backend b and initialization parameter c_i
end if

Computer equipped with a 12th Gen Intel Core i7-12700F processor (2.10 GHz), 16 GB RAM, and a 64-bit architecture. The currently deployed versions are Qiskit 1.3.2 and IBM Runtime 0.34.0. With Sampler v2, circuit submission and execution on the backend have been more efficient, exhibiting no latency and enabling noise-free quantum circuit execution. For the current evaluation, the IBM Quantum platform's open plan provides access to 3 Quantum hardware systems as of January 2025: ibm_kyiv, ibm_sherbrooke, and ibm_brisbane. The open plan allows limited Qiskit runtime usage of 10 minutes, whereas the current QPUF evaluation time for each job approximately ranges from 2 to 10 seconds, highlighting the constraints of the execution window. Once a job is submitted to a backend, a unique job address is assigned, and the circuit is executed with the specified initialization parameters.

For hardware evaluation, ibm_kyiv and ibm_brisbane were selected. These are 127-qubit quantum processors that support scalable packaging, enabling higher qubit density with improved performance. The enhanced performance is attributed to improved qubit coherence, supported by the advanced Eagle architecture, which increases reliability. Due to the limited circuit evaluation space supported by IBM, only 10 jobs were executed for QPUF evaluation on hardware backends. Each job used a unique qubit initialization sequence, where qubits were initialized using the Pauli-X gate. Following quantum entanglement, a set of tunable Ry gate rotation angles was applied to control the quantum state rotation of entangled qubits. The QPUF reliability evaluation on the IBM quantum systems and simulators is presented in the Table. 2. The QPUF evaluation on the IBM quantum simulator has shown 95% reliability with almost all the QPUF generated keys being regenerated across five instances of 100 jobs evaluated at a tunable rotation angle of pi/2. Furthermore, we conducted experimental evaluations on quantum hardware-ibm_sherbrooke, ibm_brisbane, and ibm_kyoto from IBM, and their corresponding performance metrics are presented in Fig. 8. For the hardware evaluation, only 10 evaluations were conducted per instance, with a total of three instances considered. Additionally, different tunable rotation angles were applied to the first four qubits in the circuit. While our experimental evaluation on simulators was performed at a fixed tunable rotation angle of 90^o and achieved excellent reliability and uniqueness. The corresponding evaluation on hardware at a tunable rotation angle of 90^o, although achieving high reliability, did not exhibit the same level of uniqueness.

```
# Entangle the first four qubits (control) with the last four qubi
for i in range(4):
    qc.cx(i, i + 4)

# Apply RY gates to the first four qubits (control qubits) with a
angle = 3.14 / 8  # Example: π/4
for i in range(4):
    qc.ry(angle, i)

# Apply Hadamard gates to the first four qubits (control qubits)
for i in range(4):
    qc.h(i)

# Add measurement gates to all qubits
qc.measure_all()
```

(a) QPUF Deign Logic

```
Job 1: Using Initialization [1, 1, 0, 0, 1, 1, 1, 1]
Job 1 ID: cyb666r9b62g008j6he0
Most Frequent Measurement Outcome for Job 1: 11001110
Job 2: Using Initialization [1, 1, 1, 1, 1, 0, 1, 1]
Job 2 ID: cyb66rk01rbg008jscj0
Most Frequent Measurement Outcome for Job 2: 00100111
Job 3: Using Initialization [0, 1, 0, 0, 0, 1, 1, 1]
Job 3 ID: cyb67bx9b62g008j6hj0
Most Frequent Measurement Outcome for Job 3: 11001011
Job 4: Using Initialization [0, 0, 0, 1, 0, 0, 0, 1]
Job 4 ID: cyb67gy01rbg008jscng
Most Frequent Measurement Outcome for Job 4: 00000000
Job 5: Using Initialization [1, 0, 0, 1, 0, 1, 1, 1]
Job 5 ID: cyb67pecw2k0008kf2f0
Most Frequent Measurement Outcome for Job 5: 01110000
Job 6: Using Initialization [0, 1, 1, 0, 0, 0, 1, 0]
Job 6 ID: cyb67wf01rbg008jscq0
Most Frequent Measurement Outcome for Job 6: 00101111
```

(b) QPUF Calibration

```
Job ID: cycyd9n9b62g008jdnr0
Backend: ibm_kyiv
Execution Time: 2025-01-29 02:28:22.389000-06:00
==================================================
Qubit T1 (µs)    T2 (µs)    Readout Error
==================================================
0     399.37      359.94      0.002300
1     374.24      183.66      0.003500
2     265.58      150.03      0.010400
3     222.64      142.13      0.005800
4     92.19      103.96      0.063100
5     394.79      440.38      0.012200
6     266.84      161.56      0.016000
7     423.21      317.27      0.010700
8     590.96      293.61      0.045400
9     133.12      129.96      0.017000
10    317.14      84.00      0.006300
11    145.47      45.66      0.026000
12    420.33      221.53      0.015000
13    267.32      82.99      0.013300
14    321.46      349.94      0.007600
15    380.51      75.15      0.023100
16    253.29      124.24      0.019100
17    306.17      65.21      0.095700
18    287.90      49.79      0.005300
...
123   195.11      206.25      0.090900
124   210.83      65.06      0.020200
125   156.16      139.17      0.004500
126   306.89      83.33      0.009300
```

(c) ibm_kyiv Hardware Parameters during QPUF Evaluation

```
Job ID: cyy9gjjjj6dg008gp9p0
Backend: ibm_brisbane
Execution Time: 2025-02-24 10:03:23.064000-06:00
==================================================
Qubit T1 (µs)    T2 (µs)    Readout Error
==================================================
0     237.36      65.32      0.031738
1     158.45      226.52      0.038330
2     187.96      211.99      0.009033
3     389.55      400.83      0.027832
4     186.29      172.91      0.017090
5     258.15      267.66      0.180176
6     249.92      86.20      0.018555
7     256.19      298.52      0.019043
8     110.16      139.85      0.020020
9     427.07      206.19      0.010742
10    274.78      279.91      0.018799
11    205.72      381.14      0.143555
12    364.96      215.30      0.019775
13    374.46      118.64      0.013672
14    250.79      96.97      0.030273
15    251.47      44.81      0.025146
16    235.42      19.40      0.022705
17    282.49      344.08      0.022949
18    198.93      106.76      0.015625
...
123   195.11      206.25      0.090900
124   210.83      65.06      0.020200
125   156.16      139.17      0.004500
126   306.89      83.33      0.009300
```

(d) ibm_brisbane Hardware Parameters during QPUF Evaluation

Figure 6. QPUF Circuit Evaluation: Key Hardware Parameters

6.1. Discussion and Analysis

The QPUF evaluation on IBM's qasm_simulator achieved 100% reliability. Compared to published research, this is the first QPUF design to attain 100% reliability across 5 instances of jobs, each evaluated with varying qubit initializations. The evaluation demonstrated an average intra-hamming distance and Randomness of 50%. For QPUF response extraction from ibm_kyiv, a total of 6 job instances were executed, with each job producing 1024 measurement outcomes. All job strings from the 6 instances were analyzed to determine the most frequently observed measurement outcome. Due to noise and decoherence, occasional bit flips are expected, potentially altering the response. However, by evaluating occurrences across multiple instances, the most widely observed job string is selected as the reliable response for the respective backend and initialization parameters. The evaluation confirms that the QPUF circuit achieves 100%, but its outcomes depend on the backends' unique unclonable parameters at a specific time. Since backend calibration data is updated every 2-4 hours, variations in these parameters can affect quantum state assessments.

During QPUF response computation, parameters were calibrated from the selected hardware. IBM performs periodic calibration of TI and T2 times, as well as readout errors, every few hours. In this research study, experimental evaluation demonstrated reliable QPUF response generation without bit flips or noise when the QPUF circuit was executed on hardware within a specified time, provided that the parameters remained stable within the 2-4 hours calibration window. However, fluctuations in qubits' parameter values due to calibration introduce noise, leading to instability and potential bit flips in QPUF responses. As shown in Table 2, the execution of QPUF on ibm_kyiv, and ibm_brisbane successfully regenerated a few QPUF responses without bit flips. The calibration data

Table 2. Evaluating QPUF Reliability on IBM and Google Quantum Systems

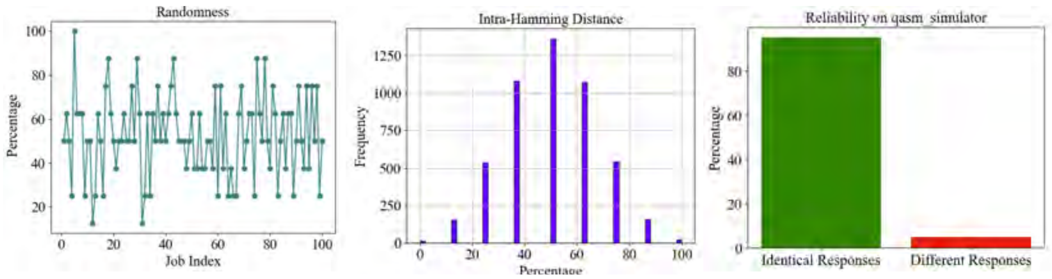
Backend	**Parameter**		**Response**	**Job ID (instance 1)**
	Ry Gate	**Initialization**		
ibm_brisbane	pi/4, pi/ 2, pi, 3pi/4	[1, 1, 1, 1, 1, 0, 1, 1]	00100111	cyy9ggay2gd00088r5s0
		[0, 1, 0, 0, 0, 1, 1, 1]	11001010	cyy9gjjjj6dg008gp9p0
ibm_kyiv	pi/4, pi/ 2, pi, 3pi/4	[0, 1, 0, 0, 0, 1, 1, 1]	11001110	cycydd5cw2k0008kp4jg
		[0, 1, 1, 0, 0, 0, 1, 0]	00101010	cycydsf7v8tg008g51p0
qasm_simulator	pi/2	[0, 0, 1, 1, 1, 0, 0, 1] .... [1, 1, 1, 0, 0, 0, 1, 0]	01011100 ... 00110111	— —
Cirq_simulator	pi/2	[0, 0, 1, 1, 1, 0, 0, 1] .... [1, 1, 1, 0, 0, 0, 1, 0]	00111010 ... 11101100	— —

presented in the figure below includes a job ID and its backend configuration parameters recorded during QPUF circuit evaluation. Additionally, it shows QPUF responses that were consistently regenerated across all five job instances executed under similar backend configuration parameters at the specified time. Our observations indicate that QPUF evaluation conducted with similar parameters exhibits consistent reliability on hardware. However, variations in these parameters across different evaluations lead to fluctuations in QPUF responses and reliability.

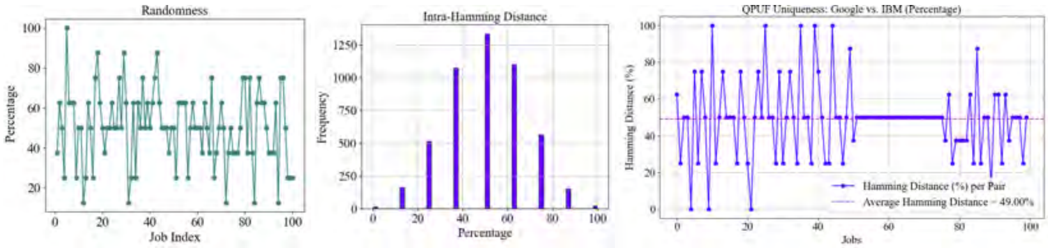
The comparative performance analysis of the proposed QPUF is an extension of the earlier architecture introduced in [13], demonstrating improved reliability, uniqueness, and randomness by introducing quantum entanglement using a quantum C-NOT gate. Additionally, a comprehensive performance analysis of QPUF with state-of-the-art research is presented in Table. 3.

6.2. Challenges in the Evaluation

The accessibility of quantum computers remains a significant issue. However, as research on noise-free quantum computing and advanced quantum chips progresses, quantum computers are expected to become more accessible for a wider range of applications, making the execution of hundreds or even thousands of jobs much easier. The noisy quantum systems may sometimes produce identical responses across different quantum hardware, potentially affecting the circuit outcomes and uniqueness. This could be attributed to very closely resonant driving frequencies that fluctuate over time and qubit crosstalk. A potential solution is to assign a unique set of qubits for each quantum job when executing QPUF. By leveraging the quantum systems with a higher number of qubits, stable driving resonant frequencies, and improved coherence times, QPUF instantiation can be further optimized.

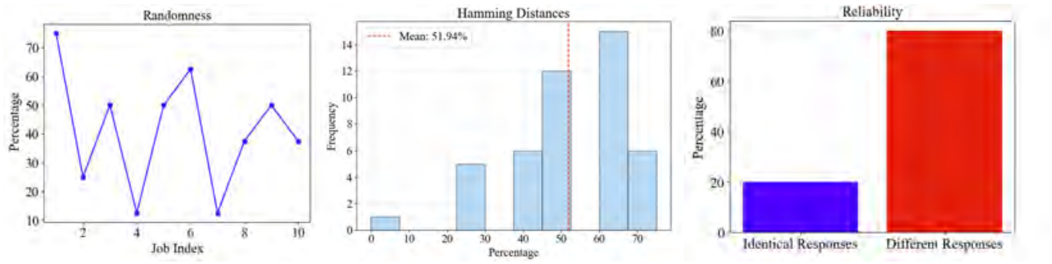


(a) QPUF Performance Evaluation on ibmq_qasm_simulator

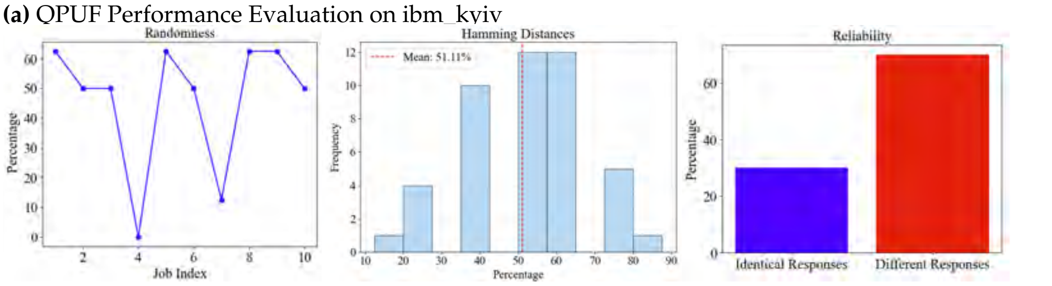


(b) QPUF Performance Evaluation on Cirq Simulator

Figure 7. QPUF Performance Evaluation



(a) QPUF Performance Evaluation on ibm_kyiv



(b) QPUF Performance Evaluation on ibm_brisbane

Figure 8. QPUF Performance Evaluation

7. Conclusion and Future Research

This research proposed and validated the QPUF Design which has been successfully tested on various quantum hardware with an effective CRP generation scheme, and performed a comprehensive evaluation of QPUF-generated keys by evaluating uniqueness, reliability, and randomness. This work has successfully proposed an approach for QPUF signature generation from a QPUF circuit built with quantum logic gates and can securely perform attestation of industrial CPS entities. Furthermore, a novel QPUF-assisted IIoT security approach has been presented, which could improve the reliability of quantum computing applications in I-CPS and validate the potential and scope for Quantum industrial Internet-of-Things (QIIoT). The QPUF evaluation on IBM and Google quantum simulators has achieved 95% and 100% reliability respectively, with a uniqueness and randomness of approximately 50%, highlighting its potential for noise-free quantum computing-assisted security, while our evaluation on hardware indicates an improved

Table 3. Comparative Performance Analysis of QPUF

Research Work	QPUF Logic	Hardware	Metrics	Challenges
Phalak et al. [24]	Hadamard Gate, Ry, and Measurement	ibmq_london, ibmq_essex, ibmq_burlington	intra-HD-13.82% (ibmq_essex), 3.94% (ibmq_london)	Low HD, No reliability, and uniqueness
Bathalapalli et.al [13]	Ry, H, and M gates	ibmq_lima, ibmq_quito, and ibmq_belem	ibmq_lima-Reliability-60%, HD-40%	Low uniqueness
Cirillo et al. [14]	Rx, Ry, Rz	ibm_osaka, ibm_brisbane, and ibm_kyoto	Average Uniqueness-30% , Average Randomness -70%	Low reliability
Topaloglu et al. [33]	Ry and Rx gates, Unitary gate and Z gates	ibmq_belem	NA	No QPUF key generation and metrics evaluation
QPUF(Current Paper)	Pauli-X, CNOT, Ry, and H gates	Qasm Simulator, Cirq Simulator, ibm_brisbane, ibm_kyiv	100% Reliability-Cirq Simulator, 50% Randomness and Intra-uniqueness, 95% Reliability-Qasm simulator	Can improve QPUF uniqueness on Hardware through noise reduction

potential for reliability and uniqueness by incorporating noise mitigation techniques. Furthermore, controlling the QUF circuit at the microwave level by carefully calibrating microwave pulses and improving the quantum hardware resiliency through improved qubit coherence and gate fidelities can further enhance the reliability of quantum hardware.

Author Contributions:

Conceptualization, Venkata K. V. V. Bathalapalli and Saraju P. Mohanty; Methodology, Venkata K. V. V. Bathalapalli, Saraju P. Mohanty and Elias Kougianos; Investigation, Chenyun Pan; Writing – original draft, Venkata K. V. V. Bathalapalli; Writing – review & editing, Saraju P. Mohanty and Elias Kougianos; Supervision, Saraju P. Mohanty and Chenyun Pan.

Acknowledgements:

A preliminary version of this work has been presented at the following conference paper [13].

1. Nanda, A.; Puthal, D.; Mohanty, S.P.; Choppali, U. A Computing Perspective of Quantum Cryptography [Energy and Security]. *IEEE Consumer Electronics Magazine* **2018**, *7*, 57–59. https://doi.org/10.1109/mce.2018.2851741.
2. Bera, B.; Das, A.K.; Sikdar, B. Securing Next-Generation Quantum IoT Applications using Quantum Key Distribution. *IEEE Internet of Things Magazine* **2025**, *8*, 50–56. https://doi.org/10.1109/iotm.001.2400059.
3. Sarjan, H.; Ameli, A.; Ghafouri, M. Cyber-Security of Industrial Internet of Things in Electric Power Systems. *IEEE Access* **2022**, *10*, 92390–92409. https://doi.org/10.1109/access.2022.3202914.
4. Ahmad, S.F.; Ferjani, M.Y.; Kasliwal, K. Enhancing Security in the Industrial IoT Sector using Quantum Computing. In Proceedings of the Proc. 28th IEEE International Conference on Electronics, Circuits, and Systems (ICECS), November 2021, pp. 1–5. https://doi.org/10.1109/icecs53924.2021.9665527.
5. Alasmary, H. RDAF-IIoT: Reliable Device-Access Framework for the Industrial Internet of Things. *Mathematics* **2023**, *11*, 2710. https://doi.org/10.3390/math11122710.
6. Barbareschi, M.; Casola, V.; Benedictis, A.D.; Montagna, E.L.; Mazzocca, N. On the Adoption of Physically Unclonable Functions to Secure IIoT Devices. *IEEE Transactions on Industrial Informatics* **2021**, *17*, 7781–7790. https://doi.org/10.1109/tii.2021.3059656.

7. Shan, X.; Yu, H.; Chen, Y.; Yang, Z. Physical Unclonable Function Based Lightweight and Verifiable Data Stream Transmission for Industrial IoT. *IEEE Transactions on Industrial Informatics* **2023**, pp. 1–11. https://doi.org/10.1109/tii.2023.3248107.
8. Joshi, S.; Mohanty, S.P.; Kougianos, E. Everything You Wanted to Know About PUFs. *IEEE Potentials* **2017**, *36*, 38–46. https://doi.org/10.1109/mpot.2015.2490261.
9. Zhang, Y.; Li, B.; Wang, Y.; Wu, J.; Yuan, P. A Blockchain-based User Remote Autentication Scheme in IoT Systems Using Physical Unclonable Functions. In Proceedings of the Proc. IEEE 5th International Conference on Signal and Image Processing (ICSIP), October 2020, pp. 1100–1105. https://doi.org/10.1109/icsip49896.2020.9339402.
10. Pudi, V.; Bodapati, S.; Kumar, S.; Chattopadhyay, A. Cyber Security Protocol for Secure Traffic Monitoring Systems using PUF-based Key Management. In Proceedings of the Proc. IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS), December 2020, pp. 103–108. https://doi.org/10.1109/ises50453.2020.00033.
11. Chwa, C.Z.; Hsia, L.A.; Merkle, L.D. Quantum Crosstalk as a Physically Unclonable Characteristic for Quantum Hardware Verification. In Proceedings of the NAECON 2023 - IEEE National Aerospace and Electronics Conference. IEEE, August 2023, pp. 309–313. https://doi.org/10.1109/naecon58068.2023.10365761.
12. Morris, J.; Abedin, A.; Xu, C.; Szefer, J. Fingerprinting Quantum Computer Equipment. In Proceedings of the Proceedings of the Great Lakes Symposium on VLSI 2023, June 2023, pp. 117–123. https://doi.org/10.1145/3583781.3590247.
13. Bathalapalli, V.K.V.V.; Mohanty, S.P.; Pan, C.; Kougianos, E. QPUF: Quantum Physical Unclonable Functions for Security-by-Design of Industrial Internet-of-Things. In Proceedings of the Proc. IEEE International Symposium on Smart Electronic Systems (iSES). IEEE, December 2023, pp. 296–301. https://doi.org/10.1109/ises58672.2023.00067.
14. Cirillo, F.; Esposito, C. Practical Evaluation of a Quantum Physical Unclonable Function and Design of an Authentication Scheme. In Proceedings of the Proc. IEEE International Conference on Quantum Computing and Engineering (QCE). IEEE, September 2024, pp. 1354–1363. https://doi.org/10.1109/qce60285.2024.00161.
15. Koroniotis, N.; Moustafa, N.; Schiliro, F.; Gauravaram, P.; Janicke, H. The SAir-IIoT Cyber Testbed as a Service: A Novel Cybertwins Architecture in IIoT-Based Smart Airports. *IEEE Transactions on Intelligent Transportation Systems* **2021**, pp. 1–14. https://doi.org/10.1109/tits.2021.3106378.
16. Murat, D.; Berkan, U.; Ali, I. An Overview of Secure by Design: Enhancing Systems Security through Systems Security Engineering and Threat Modeling. In Proceedings of the Proc. 17th International Conference on Information Security and Cryptology (ISCTürkiye). IEEE, October 2024, pp. 1–6. https://doi.org/10.1109/isctrkiye64784.2024.10779293.
17. Microsoft. Windows 11 Security Book. https://www.microsoft.com/content/dam/microsoft/final/en-us/microsoft-brand/documents/MSFT-Windows11-Security-book_Sept2023.pdf, 2023. Accessed: 2025-02-01.
18. AWS.; Institute, S. Secure by Design Whitepaper. https://d1.awsstatic.com/partner-network/AWS-SANS-Secure-by-Design-Whitepaper-2024.pdf, 2024. Accessed: 2025-02-01.
19. Services, A.W. Secure by Design: AWS Enhances Centralized Security Controls as MFA Requirements Expand, 2024. Accessed: 2025-02-04. Available at: https://aws.amazon.com/blogs/security/secure-by-design-aws-enhances-centralized-security-controls-as-mfa-requirements-expand/.
20. Bathalapalli, V.K.V.V.; Mohanty, S.P.; Kougianos, E.; Iyer, V.; Rout, B. iTPM: Exploring PUF-based Keyless TPM for Security-by-Design of Smart Electronics. In Proceedings of the IEEE Computer Society Annual Symposium on VLSI (ISVLSI). IEEE, June 2023, pp. 1–6. https://doi.org/10.1109/isvlsi59464.2023.10238586.
21. Bathalapalli, V.K.V.V.; Mohanty, S.P.; Pan, C.; Kougianos, E. QPUF 2.0: Exploring Quantum Physical Unclonable Functions for Security-by-Design of Energy Cyber-Physical Systems, 2024. https://doi.org/10.48550/ARXIV.2410.12702.
22. Nilesh, K.; Deppe, C.; Boche, H. Quantum PUF and its Applications with Information Theoretic Analysis. In Proceedings of the Proc. IEEE 10th World Forum on Internet of Things (WF-IoT). IEEE, November 2024, pp. 1–6. https://doi.org/10.1109/wf-iot62078.2024.10811185.
23. Chuang, K.K.H.; Chen, H.M.; Wu, M.Y.; Yang, E.C.S.; Hsu, C.C.H. Quantum Tunneling PUF: A Chip Fingerprint for Hardware Security. In Proceedings of the Proc. International Symposium on VLSI Technology, Systems and Applications (VLSI-TSA), April 2021, pp. 1–2. https://doi.org/10.1109/vlsi-tsa51926.2021.9440114.

24. Phalak, K.; Ash-Saki, A.; Alam, M.; Topaloglu, R.O.; Ghosh, S. Quantum PUF for Security and Trust in Quantum Computing. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems* **2021**, *11*, 333–342. https://doi.org/10.1109/jetcas.2021.3077024.
25. Rahman, M.S.; Hossam-E-Haider, M. Quantum IoT: A Quantum Approach in IoT Security Maintenance. In Proceedings of the Proc. International Conference on Robotics,Electrical and Signal Processing Techniques (ICREST), January 2019, pp. 269–272. https://doi.org/10.1109/icrest.2019.8644342.
26. Sangari, S. Providing Security in Internet of Things Using Quantum Cryptography. In *Advances in Systems Analysis, Software Engineering, and High Performance Computing*; IGI Global, 2023; pp. 245–253. https://doi.org/10.4018/978-1-6684-6697-1.ch014.
27. Qian, K.; Liu, Y.; He, X.; Du, M.; Zhang, S.; Wang, K. HPCchain: A Consortium Blockchain System based on CPU-FPGA Hybrid PUF for Industrial Internet of Things. *IEEE Transactions on Industrial Informatics* **2023**, *19*, 1–11. https://doi.org/10.1109/tii.2023.3244339.
28. Gong, X.; Feng, T.; Albettar, M. PEASE: A PUF-Based Efficient Authentication and Session Establishment Protocol for Machine-to-Machine Communication in Industrial IoT. *Electronics* **2022**, *11*, 3920. https://doi.org/10.3390/electronics11233920.
29. Sharma, A.K.; Peelam, M.S.; Chauasia, B.K.; Chamola, V. QIoTChain: Quantum IoT-blockchain fusion for advanced data protection in Industry 4.0. *IET Blockchain* **2023**, *4*, 252–262. https://doi.org/10.1049/blc2.12059.
30. Prajwal, C.P.; Mohan, A.S.; Reddy, D.N.; Nimmy, K. Quantum-Safe Authentication Protocol leveraging qPUF for Industrial Internet of Things. In Proceedings of the Proc. 15th International Conference on Computing Communication and Networking Technologies (ICCCNT). IEEE, June 2024, pp. 1–8. https://doi.org/10.1109/icccnt61001.2024.10725580.
31. Javadi-Abhari, A.; Treinish, M.; Krsulich, K.; Wood, C.J.; Lishman, J.; Gacon, J.; Martiel, S.; Nation, P.D.; Bishop, L.S.; Cross, A.W.; et al. Quantum computing with Qiskit, 2024, [arXiv:quant-ph/2405.08810]. https://doi.org/10.48550/arXiv.2405.08810.
32. Cirq Developers. *Cirq*; Zenodo, 2025. https://doi.org/10.5281/zenodo.4062499.
33. Topaloglu, R.O. Quantum Logic Locking for Security. *J* **2023**, *6*, 411–420. https://doi.org/10.3390/j6030027.