Received 23 January 2024; revised 25 February 2024; accepted 28 February 2024. Date of publication 1 March 2024; date of current version 21 March 2024.

Digital Object Identifier 10.1109/OJCOMS.2024.3372524

Securing Synchrophasors Using Data Provenance in the Quantum Era

KASHIF JAVED[1], MANSOOR ALI KHAN[2] (Member, IEEE), MUKHTAR ULLAH[1] (Senior Member, IEEE), MUHAMMAD NAVEED AMAN[3] (Senior Member, IEEE), AND BIPLAB SIKDAR[2] (Senior Member, IEEE)

[1]Department of Electrical Engineering, National University of Computer and Emerging Sciences, Islamabad 44000, Pakistan
[2]Department of Electrical and Computer Engineering, National University of Singapore, Singapore
[3]School of Computing, University of Nebraska-Lincoln, Lincoln, NE 68588, USA

CORRESPONDING AUTHOR: M. N. AMAN (e-mail: naveed.aman@unl.edu)

This work was supported by the National Research Foundation, Singapore, and A*STAR under its Quantum Engineering Programme (National QuantumSafe Network) under Grant NRF2021-QEP2-04-P01.

ABSTRACT Trust in the fidelity of synchrophasor measurements is crucial for the correct operation of modern power grids. While most of the existing research on data provenance focuses on the Internet of Things, there is a significant need for effective malicious data detection in power systems. Current methods either fail to detect malicious data modifications or require certain Phasor Measurement Units (PMUs) to be physically secured. To solve these issues, this paper presents a new protocol to establish data provenance in synchrophasor networks. The proposed protocol is based on Physically Unclonable Functions (PUFs) and harnesses the principles of quantum unreality and uncertainty. It aims not only to verify the source of data but also to provide robust protection against data tampering. The proposed protocol serves the purpose of devising new protocols to protect our critical infrastructure sectors in the quantum era. Security and performance analyses, along with experiments conducted on IBM's Qiskit platform, demonstrate that the protocol offers a strong defense against cyberattacks while maintaining a lightweight profile. In particular, the proposed protocol has a worst-case computational complexity of $O(1)$, an execution time per packet bounded by the time required to compute a cryptographically secure hash, and an upper bound for the per packet communication overhead of 256-bits. In terms of storage overhead, the proposed protocol requires each PMU to store the output of a cryptographically secure hash function, while the PDC needs to store one challenge-response pair (CRP) for each PMU.

INDEX TERMS Data provenance, synchrophasors, quantum channels.

I. INTRODUCTION

Monitoring and control of power systems are crucial components in the overall design and operation of the smart grid. Monitoring power grids in real-time is a crucial mechanism that requires a mathematical representation of the status of an interconnected power system. Synchrophasor technology offers new opportunities for the monitoring and control of electric power systems. Bevrani et al. [1] introduced the concept of using GPS for synchronized phasor measurement. Phasor Measurement Units (PMUs) deliver highly accurate synchrophasor data, time-stamped and synchronized with Coordinated Universal Time (UTC). PMUs enable time-stamped synchrophasor measurements of the power grid up to 100 times quicker than typical SCADA systems. These measurements can be utilized for power grid situational awareness, state estimation, and system analysis [2]. PMUs, deployed in various geographic locations, transmit measured synchrophasors to a Phasor Data Concentrator (PDC) center (Fig. 1). The PDC receives data from each PMU and time-aligns it based on the corresponding time stamp. This data is then used by the PDC to monitor, analyze, and control the entire grid system. Synchrophasor networks' dependability is determined by the authenticity and integrity of the data produced by PMUs.

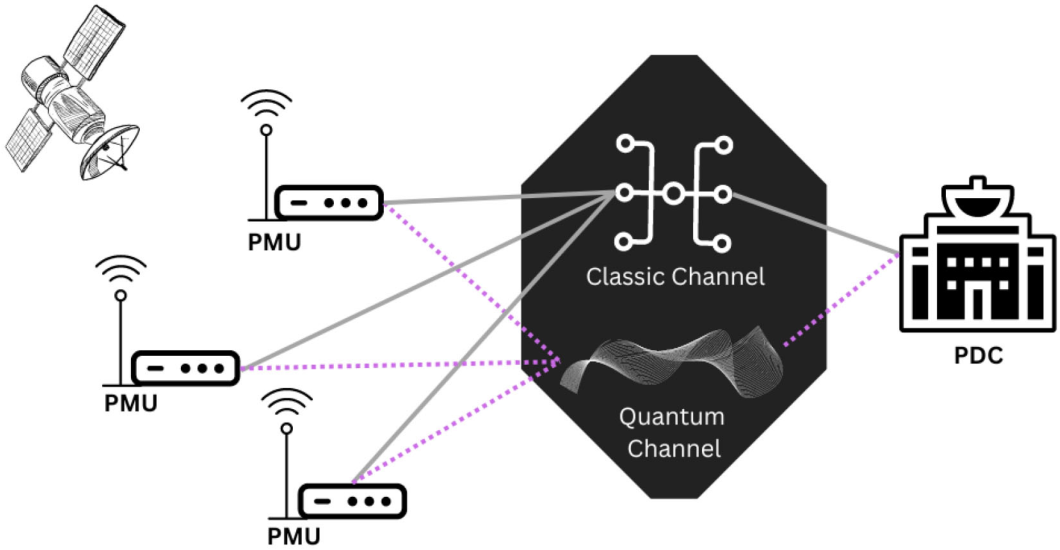


FIGURE 1. Network model.

The IEEE C37.118, IEC 61859, and IEC 62351 standards outline the requirements for synchrophasor measurement and data communication protocols. However, the system is susceptible to man-in-the-middle (MITM) attacks, data spoofing attacks, Denial-of-Service (DoS) attacks, time synchronization attacks, false data injection attacks, and eavesdropping attacks due to the absence of a transmission protocol and the streaming of data to multiple hierarchical structures. Leased lines, privately owned Synchronous Optical Networks (SONETs), and wireless links can connect PMUs to PDCs [3]. Before being sent to the control center, data is transmitted to multiple hierarchical structures, including PDCs and Super PDCs. PMUs are susceptible to cyberattacks as a component of Wide Area Measurement Systems (WAMS) due to their integration with the critical infrastructure of the smart grid and precise state estimation data. Data provenance establishes confidence in the origin and creation process of the data. Examining data provenance, which confirms whether the PMU indeed collected the data at the specified location and time, not only enables a user to assure data integrity but also provides non-repudiation. However, the majority of existing synchrophasor data security techniques emphasize data integrity over provenance, leaving PMUs vulnerable to proxy attacks. In such attacks, the adversary constructs a clone of the compromised PMU by extracting PMU device secrets through physical attacks.

Existing work on securing synchrophasors mostly focuses on detecting data tampering, particularly through bad data detection. Malicious data modifications in power systems may be regarded as "bad data," a term traditionally applied to measurements from faulty equipment. Estimators of the state of a power system employ poor data detection strategies based on a statistical analysis of measurement residuals. Techniques such as using an L2-norm or the Largest Normalized Residual (LNR) detect outliers and poor measurements [4], [5], [6]. However, these techniques presume that erroneous data is the result of measurement or transmission errors, and most bad data detection methods assume that the measurement residuals are independent. An adversary can exploit this assumption by introducing structured interactions among bad data, causing bad data detectors to fail against data tampering attacks. Other methods to detect malicious data modification in synchrophasors require a subset of PMUs to be secure, which may not be realistic.

To solve the above issues, this paper proposes a lightweight data provenance protocol for securing synchrophasor data using Physically Unclonable Functions (PUFs) and quantum mechanics. Utilizing the inherent random variations in the physical (sub-)microstructure of an integrated circuit (IC), PUFs enable us to provide a unique hardware fingerprint for each PMU. Moreover, the power of quantum unreality and uncertainty is exploited to protect any type of data tampering. Note that, unlike other data networks, synchrophasors send their data in plain text without the use of any cryptographic primitives. Therefore, the proposed protocol is exclusively designed for synchrophasor networks for two major reasons: (i) PMUs have limited computational processing power combined with high-intensity traffic makes conventional cryptographic primitives unsuitable [7], and (ii) a critical assumption behind any attack model for synchrophasors is that the adversary is capable of breaking the encryption of PMU packets [8], [9]. Given these two unique characteristics of synchrophasors, the major contributions of this paper are as follows:

i. Application of quantum unreality and uncertainty principles to protect synchrophasor data from malicious modifications.
ii. Development of a novel PUF-based data provenance protocol to provide authenticity and integrity of synchrophasor data.

iii. Formal security analysis and extensive experimentation to validate the proposed protocol.
iv. Optimization of a quantum-based method that effectively addresses the limitations of traditional data provenance techniques, utilizing principles of quantum mechanics to enhance security against quantum attacks and to augment scalability and flexibility in synchrophasor networks/environments.

The rest of the paper is organized as follows: Section II presents a discussion on existing related work, while Section III provides the necessary background to understand the proposed protocol. The proposed network model and assumptions are presented in Section IV, and the threat model is discussed in Section V. The proposed protocol is presented in Section VI, followed by its security analysis in Section VII. Experiments are discussed in Section VIII, performance analysis in Section IX, and the paper concludes in Section X.

II. LITERATURE REVIEW

Most of the existing work on data provenance is concentrated in the Internet of Things (IoT) domain and can be divided into three categories: security-primitives-based, hardware-based, and techniques using wireless channel characteristics. Security-primitives-based techniques employ filters, hash chains, blockchains, or zero-knowledge proofs (ZKP). For instance, [10] proposed a data provenance technique for IoT devices using Bloom filters and attribute-based encryption. However, this technique requires devices to store provenance information, which is vulnerable to manipulation through physical attacks. Another approach [11] transmits provenance information across multiple IoT devices using an identity-based hash chain, but it is susceptible to impersonation attacks due to its reliance on the device identities of IoT devices. The use of non-interactive zero-knowledge proofs (NI-ZKPs) for data provenance is proposed in [12], although ZKP techniques can be computationally complex. In [13], an algorithm for data provenance compression is proposed, but this solution remains computationally intensive. Recent blockchain-based data provenance techniques, such as [14], [15], [16], [17] increase the computational burden.

Hardware-based data provenance solutions, like those employing Trusted Platform Modules (TPMs), are discussed in [18], [19], [20]. However, such techniques may require specialized hardware that may not be available or practical for the majority of devices. The first description of executing a data injection attack against power system state estimation was by [21], showing that an adversary with knowledge of a power system's configuration can introduce arbitrary errors into the state variables by tricking a flawed data detector. Reference [22] discusses the minimal number of measurements an adversary must alter to influence the state model. Security indices for state estimators are presented in [23], demonstrating their use in quantifying the effort required for a successful data modification attack. Reference [24] examines defending against data manipulation attacks from the operator's perspective, identifying a minimal set of measurements for system observability. Reference [25] developed metrics to assess the economic impact of data integrity attacks on power grids, illustrating that such attacks can lead operators to make erroneous decisions, resulting in significant economic and physical damage. In [26], the authors demonstrate that a power system may defend itself against data injection assaults by protecting a small subset of measurements. They identified that the selection of such subsets is a complex combinatorial problem that can be solved with an agreed strategy.

The majority of extant research on data tampering attacks is based on the premise that a subset of PMUs can be protected and made completely secure. However, given the large number of PMUs and their diverse locations, this assumption is implausible. Moreover, the existing techniques for data provenance in the IoT are either based on computationally complex cryptographic primitives or require additional secure hardware. Traditional or classical cryptographic techniques, such as hardware-accelerated cryptographic algorithms (e.g., Speck and Simon) and PUFs, play a significant role in securing IoT devices [27], [28]. While Speck and Simon offer computational efficiency, they may not withstand the emerging quantum threats, as they are not inherently designed to resist quantum computing attacks like Post-Quantum Cryptography (PQC) transition algorithms [29]. Specifically, the vulnerability of Speck and Simon to quantum attacks is primarily due to Shor's algorithm [30], which can efficiently factorize large numbers and compute discrete logarithms in polynomial time on a quantum computer. This capability could potentially break the Rivest-Shamir-Adleman (RSA) encryption through an index-calculus attack [31], [32].

The above discussion shows that the existing security mechanisms for data provenance suffer from the following problems:

i. Rely on computationally expensive cryptographic primitives that may not be suitable for high traffic intensity and real-time applications in synchrophasors.
ii. Rely on stringent assumptions such as completely secure PMUs.
iii. Rely on advanced TPMs, which may not be available on PMUs due to their higher cost. Moreover, when using TPMs, there is an inherent delay when switching between the normal mode of operation and the secure execution environment, typically called the switching cost [33]. Thus, TPMs may not be suitable given the high switching time and frequent updates, leading to significantly higher latency in synchrophasors [34].
iv. Vulnerable to quantum-capable actors.

This paper solves these issues as follows: The proposed protocol

i. only uses a cryptographically secure hash function, and instead of using any computationally expensive cryptographic primitives, it leverages the power of quantum unreality and uncertainty to provide data integrity guarantees.

ii. does not make any stringent assumptions regarding the PMUs, except for the availability of PUFs on each PMU. Note that PUFs have extremely low power consumption, silicon area, and manufacturing costs, making them suitable for large-scale production in synchrophasor networks.

iii. uses quantum encoding to mitigate quantum threats.

III. BACKGROUND

A. QUANTUM UNREALITY AND UNCERTAINTY

In classical communication and authentication schemes, passwords, biometrics, and cryptographic protocols are used as secret keys to guarantee security. The security of these schemes is based on the mathematical computational complexity of certain tasks, such as factoring large numbers in the RSA encryption algorithm or finding collisions in hash functions (Secure Hash Algorithms: SHA-256 and SHA-3) [35]. Consequently, classical authentication is considered computationally secure, meaning it relies on the assumption that certain computational problems are difficult to solve using classical resources. On the other hand, quantum cryptography utilizes the laws of physics, as opposed to mathematical assumptions, to enable the secure exchange of a secret key between two parties. It is considered more robust because, unlike mathematical assumptions that can unravel with the advent of stronger computing power, the laws of physics cannot be broken. This makes quantum cryptography potentially more secure against MITM attacks due to the principles of quantum physics. Quantum physics is known as a probabilistic theory, meaning randomness is built into it. Superposition and entanglement are powerful features of quantum computing that make it vastly different from classical computing. These unique properties enable quantum computers to perform certain tasks or calculations much faster and more effectively than classical computers, a phenomenon referred to as "Quantum Supremacy" [36].

Quantum mechanics, the bedrock of modern physics, introduces fascinating concepts of unreality and uncertainty at the subatomic level. Particles in the quantum realm, such as photons and electrons, do not exist in definite states until measured [37]. These concepts form the basis for a wide array of quantum technologies, including quantum computing, quantum cryptography, and quantum key distribution, all of which ensure secure information exchange. The proposed data provenance protocol leverages quantum unreality and uncertainty in securing synchrophasor data. Therefore, understanding these concepts is vital before delving into the proposed technique.

1) *Quantum Unreality (Superposition):* In the classical world, objects exist in definite states. For example, a coin has either heads or tails. However, in the quantum realm, particles such as atoms, photons, or electrons can exist in a state of superposition, meaning they can be in multiple states simultaneously, as illustrated in Fig. 2. Consider an electron's spin; it can be in a superposition of both "up" and "down" states until measured, at which point it collapses into one of the two states. This bizarre phenomenon implies that quantum entities do not have well-defined properties until they are observed or measured [38]. In a similar vein, a quantum bit, or qubit, is the fundamental unit of quantum information. It possesses the remarkable ability to exist in a superposition of both 0 and 1 until a measurement is conducted, at which juncture it adopts one of these binary states. This inherent multiplicity of states or configurations introduces a significant degree of unpredictability, which can be utilized for various purposes, such as the creation of distinctive quantum states or identifiers for devices. It also underpins parallel processing tasks, exemplified by algorithms like Shor's algorithm for integer factorization and Grover's algorithm for searching, which utilize quantum superposition for enhanced computational capabilities [30], [39].

2) *Quantum Uncertainty (Heisenberg Uncertainty Principle):* Uncertainty or indeterminacy is another peculiar feature of quantum systems. The Heisenberg uncertainty principle, a key concept in quantum mechanics, posits a fundamental limitation on the precision with which specific pairs of physical properties can be simultaneously known. These pairs, also known as complementary variables (e.g., a particle's position and momentum, energy and time), cannot be precisely known concurrently due to this inherent limitation [40]. For instance, accurately measuring the position of a quantum particle like an electron makes its momentum uncertain, and vice versa. This intrinsic uncertainty arises from the wave-particle duality of quantum objects. Consequently, this means that quantum uncertainty refers to the inherent probabilistic nature of quantum systems. In other words, it implies that when certain quantum properties are measured, uncertainty is introduced into complementary properties. This uncertainty has practical implications for data integrity and cybersecurity. For example, quantum uncertainty can be harnessed to generate true random numbers, crucial for encryption and security protocols. Specifically, PMUs are devices employed in power systems to gauge electrical waveforms at various points and provide synchronized data to PDCs for monitoring and control purposes.

B. QUANTUM UNREALITY AND UNCERTAINTY FOR SYNCHROPHASOR TECHNOLOGY

Now, let's delve into how the power of quantum unreality and uncertainty can be harnessed to protect synchrophasor data from any malicious modification.

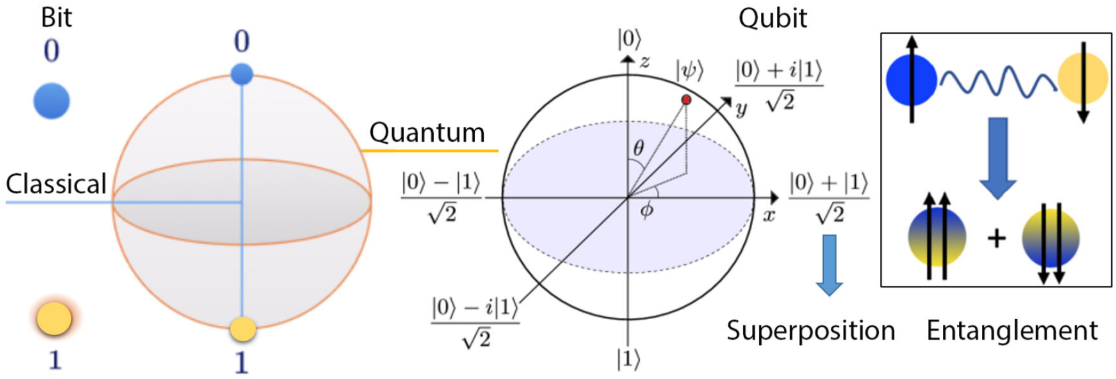

Bit
0
0
Classical
Quantum
1
1
Qubit
$|0\rangle$
z
$|\psi\rangle$
$\frac{|0\rangle + i|1\rangle}{\sqrt{2}}$
y
θ
$\frac{|0\rangle - |1\rangle}{\sqrt{2}}$
ϕ
x
$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$
$\frac{|0\rangle - i|1\rangle}{\sqrt{2}}$
$|1\rangle$
+
Superposition
Entanglement

FIGURE 2. Classical digital (bits) and Quantum (qubit) computing.

Source Verification: Quantum unreality allows for the creation of PUFs that generate unique identifiers for PMUs and data sources [41]. These PUFs exploit the quantum uncertainty principle to generate random, unpredictable values. When synchrophasor data is tagged with these quantum-derived identifiers, any tampering attempt would disrupt the superposition state or introduce uncertainty, instantly revealing unauthorized modifications.

Physically Unclonable Functions: To establish a root of trust, TPMs and PUFs are commonly utilized in hardware and hybrid-based attestation methods [42], [43], [44], [45]. A TPM, serving as a secure crypto-processor, stores and protects encryption keys, passwords, and other sensitive data, including digital certificates [19]. However, it relies on cryptographic keys and certificates pre-stored within the module's non-volatile memory. This indicates that TPM chips are standalone modules, necessitating additional hardware, which in turn, occupies more physical space, potentially increases costs, power consumption, and the overall complexity of device design and manufacturing. Such a design introduces a vector for sophisticated physical or side-channel attacks aimed at extracting sensitive information [34]. In contrast, PUFs inherently generate cryptographic keys based on the unique physical characteristics of the device, where random variations in the IC fabrication process create an intractable physical system [46]. This facilitates a novel challenge-response mechanism, where keys do not need to be stored in non-volatile memory, thereby reducing the risk of key extraction attacks. Consequently, PUFs can be implemented using existing hardware components (like SRAM, flash memory, etc.), eliminating the need for additional specialized hardware [47]. Thus, PUFs offer advantages over TPMs in terms of unclonability, tamper evidence, cost-effectiveness, scalability, flexibility, and intrinsic key generation and management [48], [49]. These features make PUFs highly suitable for secure hardware authentication, especially in applications where cost, physical security, ease of integration, and resistance to tampering are critical, as is the case with our prototype.

Fundamentally, PUF is characterized by a challenge-response-pair (CRP), i.e., $R = P(C)$, where R is a PUF's response to a challenge C [44]. Each PUF responds differently to an identical challenge, indicating its uniqueness. Environmental factors such as temperature and voltage may influence the performance of a PUF when presented with the same challenge. Using fuzzy extractors or error correction codes (ECC) algorithms, we can circumvent this issue and obtain PUF responses stable enough for security applications [50]. PUFs eliminate the need for PMUs to retain secret keys in their memory, thereby protecting them from physical attacks. In the context of PUF security, PUFs are typically categorized into weak, strong, and controlled types, each with unique merits and limitations [45], [51]. Weak PUFs are suited for key generation within a limited CRP range, offering consistency but possessing limited security capabilities due to their predictability. Strong PUFs excel in generating a vast array of CRPs and maintain stability under varying conditions, making them ideal for authentication. However, an adversary with access to a large number of CRPs can facilitate the creation of a malicious clone using machine learning techniques [49], [52]. Such attacks can lead to alterations in functionality, including CRP leakage to adversaries or the modification of PUF inputs to generate false responses. Controlled PUFs represent an evolution in PUF design, incorporating strong PUFs at their core but enhancing them with control logic [53]. This control mechanism regulates challenges from being freely applied to the PUF circuit, thereby obstructing intermediate response readout, effectively thwarting machine learning attacks [54].

Considering the aforementioned aspects, in this paper, we propose the use of an ideal controlled strong PUF (CPUF) due to vulnerabilities observed in other PUF types. For example, delay-based PUFs, including both strong arbiter PUFs (A-PUF) and weak ring oscillator PUFs (RO-PUF), have been susceptible to machine learning attacks using Logistic Regression (LR), QuickSort (QS), and Support Vector Machines (SVMs) [55], [56], [57]. To resist machine learning attacks and detect any possible invasive attacks, different research groups have implemented further countermeasures. These involve integrating additional software functionalities, such as hashing, non-linear functions, and ephemeral CRP tables, or incorporating hardware solutions like XOR gates, CMOS, and other logic circuits [58], [59], [60], [61], [62], [63], [64]. For instance, [65], [66], [67] developed an obfuscated challenge-response protocol that utilizes a PUF chip, a random number generator (RNG), and a control block to safeguard against machine learning attacks, circumventing the need for traditional cryptographic techniques. Furthermore, in the realm of security applications, the hybrid PUF-finite state machine (PUF-FSM) emerges as a robust example of a strong CPUF, eliminating the need for error correction logic and related computation, particularly favored for its resilience against fault attacks or reliability-based attacks [68], [69]. Thus, all of these interventions make it more challenging for adversaries to develop a numerical model that effectively emulates PUF operations.

Quantum Key Distribution (QKD): QKD protocols use the uncertainty principle to create unbreakable encryption keys. By encoding synchrophasor data using quantum states and transmitting them over quantum channels, any eavesdropping attempts would disturb the quantum states, revealing the intrusion. This ensures data integrity and confidentiality. For example, the BB84 protocol utilizes uncertainty in measuring the polarization of photons to detect interception or tampering during key distribution [70].

Quantum Entanglement: Enabled by superposition and entanglement, quantum entanglement can be employed to verify data integrity [71]. Entangled particles can be used to synchronize remote PMUs or data sources. Any alteration in the data would disrupt the entanglement, making tampering evident.

In summary, quantum unreality and uncertainty provide a unique set of tools for protecting synchrophasor technology. By exploiting superposition, uncertainty, and entanglement, we can create secure identification, encryption, and synchronization mechanisms highly resistant to any type of data tampering. This ensures the trustworthiness of synchrophasor measurements in the quantum era. Therefore, by incorporating quantum unreality and uncertainty into the protocol, we not only bolster the trustworthiness of synchrophasor measurements but also offer a robust defense against cyberattacks.

IV. NETWORK MODEL & ASSUMPTIONS

The network model considered in this paper is illustrated in Fig. 1. A set of PMUs at various power buses are connected to the PDC through the Internet. We assume that each PMU has an optic fiber connection, which it can use as a quantum channel to exchange messages with the PDC.

We make the following assumptions in this paper:

i. The assumed packet format is IEEE C37.118.2. The sizes of the different fields in a typical PMU packet are displayed in Table 1.

ii. PMUs transmit their data to a single PDC using the UDP-only communication technique. The process of encapsulation and decapsulation is carried out using the standard TCP/IP protocol suite.

TABLE 1. Data packet format for a PMU [72].

#	Field	Size (bytes)
1	SYNC	2
2	FRAMESIZE	2
3	**IDCODE**	2
4	SOC	4
5	FRASEC	4
6	STAT	2
7	PHASORS	4/8 per phasor
8	FREQ	2/4
9	DFREQ	2/4
10	**ANALOG**	2/4 per value
11	DIGITAL	2 per value
12	CHK	2

iii. PMUs have limited memory and processing power and therefore, cannot sustain high traffic intensity applications with computationally complex cryptography.

iv. Each PMU is equipped with a controlled strong PUF (hybrid PUF-FSM) that forms a System-on-Chip (SoC). The PUF is assumed to be useless and destroyed if separated from the PMU [41].

v. The PDC is considered physically secure and trustworthy [73].

V. THREAT MODEL

We assume an adversary possesses capabilities according to the Dolev-Yao (DY) model, i.e., an adversary $\mathcal{A}$ possesses the ability to intercept and monitor all network communication, engage in malicious alteration or insertion of packets, replicate previously transmitted packets, and impersonate other nodes within the classic channels of the Internet. The PMUs and other network elements, such as routers and communication lines, could potentially be compromised. Nevertheless, the PDC is widely regarded as the reliable and reputable entity. Moreover, we also assume a CK-adversary model [74]. In addition to the capabilities under the DY model, a CK-adversary is able to reveal the session state, private, and session keys under the CK-adversary model. We further assume that an adversary may obtain physical access to a PMU and subject it to physical attacks to extract stored secrets.

The set of queries listed below can be used to model these attacks:

- $\texttt{Send}S(S, \texttt{m0,r0,m1})$: $\mathcal{A}$ sends a message $\texttt{m0}$ to the PDC S in an attempt to impersonate a legitimate PMU. The PDC then replies with $\texttt{m1}$.
- $\texttt{Send}ID(ID, \texttt{m0,r0})$: $\mathcal{A}$ sends a message $\texttt{m0}$ to the PMU in an attempt to impersonate a PDC. The PMU responds with $\texttt{r0}$.
- $\texttt{Monitor}(ID, S)$: $\mathcal{A}$ observes and eavesdrop the wireless channel between PMU ID and PDC S.
- $\texttt{Drop}(\mathcal{A})$: $\mathcal{A}$ drops packets between the PMU and PDC. The objective is to disrupt the synchronization between entities by selectively dropping packets.
- $\texttt{Reveal}(ID)$: $\mathcal{A}$ uses a physical attack to extract the secrets stored in a PMU's memory.

An adversary $\mathcal{A}$ can invoke Send$S$, SendID, Monitor, and Drop any polynomial number of times. Note that any attempt to physically alter a PMU makes it useless. Therefore, Reveal can be called by $\mathcal{A}$ only once. The adversary's objective is to tamper with the synchrophasor data sent from a PMU to the PDC, intending to cause power blackouts by affecting the power system state estimator.

In addition to the conventional threat model, in this paper, we assume that the adversary has a quantum computer with the ability to break traditional cryptographic algorithms such as the public key infrastructure using Shor's algorithm. Similarly, the adversary can use Grover's algorithm to enhance the potential risks by achieving a quadratic acceleration in scanning unsorted databases, which could have implications for symmetric key encryption.

VI. PROPOSED PROTOCOL

To manage CRPs (C_i, R_i) for each PMU at the PDC, we assume the protocol proposed in [75]. Therefore, the PDC needs to store only one CRP for each PMU. The initial CRP is obtained by the PDC using a time-based one-time password algorithm (TOTP) [76] and an operator using a password. The proposed protocol for establishing data provenance of synchrophasors is shown in Fig. 3. The steps are as follows:

1) The PDC sends a random challenge C_i to the PMU U_1.
2) The PMU starts to send synchrophasors to the PDC, and for each data packet sent, the PMU saves a hash digest by calculating the hash chain of each packet. Considering a cryptographically secure hash function H, the hash chain is given by:

$$\sigma = \mathtt{H}(\cdots \mathtt{H}(\mathtt{H}(P_1)\|P_2)\cdots\|P_n), \tag{1}$$

where n is the maximum allowed number of packets that can be transferred from the PMU to the PDC before verification. Note that n depends on the maximum verification delay that can be tolerated at the PDC. For example, consider a PMU with a sampling rate of 50 samples per second and transmitting 10 samples per data packet. If the PDC can tolerate a maximum verification delay of 1 second, then $n \le 5$.
3) Once the PMU has sent n data packets, it uses the challenge C_i to excite its PUF and obtain the response R_i. The PMU then uses the bits in R_i to send σ over the quantum channel. Assuming R_i and σ to have the same length, for each bit in R_i, encode the corresponding bit in σ as follows:
    a) If the current R_i bit is a 0, then encode the corresponding bit in σ using the H-V basis.
    b) If the current R_i bit is a 1, then encode the corresponding bit in σ using ±45 basis.

For example, if $R_i = 010011\cdots$ and $\sigma = 110010$, the above encoding procedure is illustrated as follows:

$$|\updownarrow\rangle_1^{H-V}|\text{⤡}\rangle_1^{\pm 45^o}|\leftrightarrow\rangle_0^{H-V}|\leftrightarrow\rangle_0^{H-V}|\text{⤡}\rangle_1^{\pm 45^o}|\text{⤢}\rangle_0^{\pm 45^o}$$

where $|\updownarrow\rangle_b^{H-V}$ represents encoding of a digit b in H-V basis while $|\text{⤡}\rangle_1^{\pm 45^o}$ and $|\text{⤢}\rangle_0^{\pm 45^o}$ represent the encoding of digits 1 and 0 in the ±45 basis, respectively. The experimental validation is shown in Section VIII.

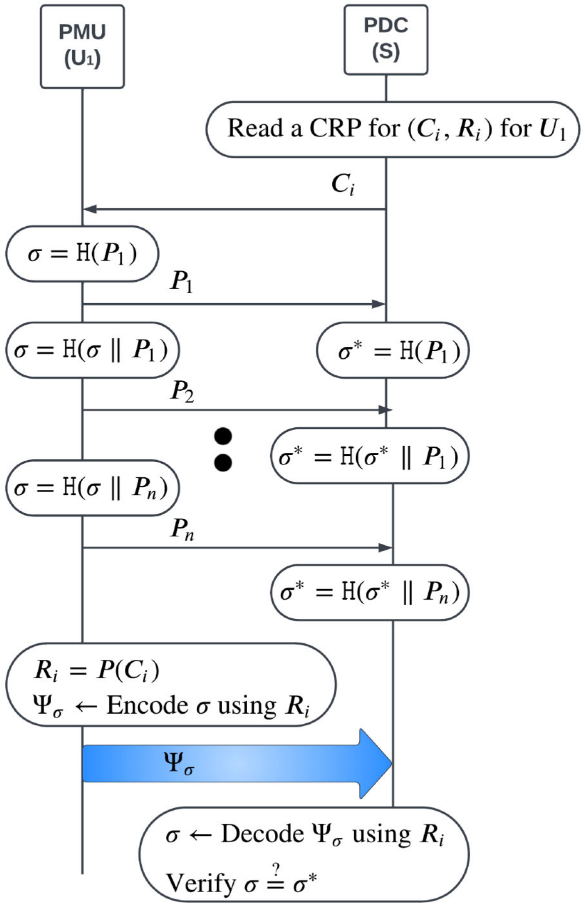

PMU
(U_1)
PDC
(S)
Read a CRP for (C_i, R_i) for U_1
C_i
$\sigma = \mathtt{H}(P_1)$
P_1
$\sigma = \mathtt{H}(\sigma \| P_1)$
$\sigma^* = \mathtt{H}(P_1)$
P_2
$\sigma^* = \mathtt{H}(\sigma^* \| P_1)$
$\sigma = \mathtt{H}(\sigma \| P_n)$
P_n
$\sigma^* = \mathtt{H}(\sigma^* \| P_n)$
$R_i = P(C_i)$
$\Psi_\sigma \leftarrow$ Encode σ using R_i
Ψ_σ
$\sigma \leftarrow$ Decode Ψ_σ using R_i
Verify $\sigma \overset{?}{=} \sigma^*$

FIGURE 3. Proposed Protocol.

Note that the proposed protocol is based on the assumption of secure storage at the PDC. However, this assumption can be relaxed by using PUF based authentication protocols that utilize ephemeral CRP tables [77].

VII. SECURITY ANALYSIS

Lemma 1: A PUF's behavior cannot be predicted.

Proof: Exciting a PUF with a challenge of length l_C produces a response of length l_R, i.e., $\{0,1\}^{l_C} \to \{0,1\}^{l_R}$. Let us model the security of a PUF with a security game $\mathcal{G}_{Sec}^{PUF}$ between an adversary $\mathcal{A}$ and challenger $\mathcal{L}$:

i. $\mathcal{A}$ chooses a set of random challenges $\mathbf{C}$ and sends them to $\mathcal{L}$.
ii. $\mathcal{L}$ chooses a random challenge $C^* \notin \mathbf{C}$ and shares it with $\mathcal{A}$.
iii. $\mathcal{A}$ sends its guess for the response to C^*, $R^\star$ to $\mathcal{C}$.
iv. $\mathcal{C}$ uses C^* to excite the PUF to get R^*. $\mathcal{A}$ wins the game if $R^\star = R^*$.

Given the unclonability attribute of PUFs, the advantage of the adversary to win this game is negligible and given by $\boldsymbol{\alpha}_{\mathcal{G}_{Sec}^{PUF}} = \mathtt{Pr}[R^{\star} = R^{*}] = \frac{1}{2^{l_R}} \approx 0$. ■

Additionally, in the controlled strong PUF (PUF-FSM), each CRP is utilized only once to avoid the risk of replay-based attacks and MITM attacks [44], [46]. This is particularly relevant for the authentication process using the strong hybrid PUF-FSM, where the set of CRPs can also be periodically refreshed for enhanced security. To counteract side-channel attacks, which exploit timing and power consumption, the PUF-FSM incorporates a pseudo-random permutation through an integrated RNG [64], [78]. This approach obstructs precise power trace measurements during response evaluations, enhancing the PUF's defense against combined modeling and side-channel attacks, thereby validating its robustness.

Lemma 2: The basis used for encoding a qubit cannot be revealed by measuring it.

Proof: Let us model this by a security game $\mathcal{G}_{Sec}^{qubit}$ between an adversary $\mathcal{A}$ and challenger $\mathcal{L}$:

i. $\mathcal{A}$ chooses a set of random bits $\mathbf{q_D}$ and a set of bits $\mathbf{q_B}$ to $\mathcal{L}$.

ii. $\mathcal{L}$ uses $\mathbf{q_B}$ to encode the bits in $\mathbf{q_D}$ as follows: for each bit in $\mathbf{q}_B$, encode the corresponding bit in $\mathbf{q}_D$ as follows:

   - If the current $\mathbf{q}_B$ bit is a 0, then encode the corresponding bit in $\mathbf{q}_D$ using the H-V basis.
   - If the current $\mathbf{q}_B$ bit is a 1, then encode the corresponding bit in $\mathbf{q}_D$ using ±45 basis.

   The resulting polarized photons are sent to $\mathcal{A}$.

iii. $\mathcal{L}$ choose a set of random bits $\mathbf{q}_B^*$ to encode the bits in $\mathbf{q_D}$ and sends the resulting polarized photons to $\mathcal{A}$.

iv. $\mathcal{A}$ sends its guess of $\mathbf{q}_B^*$ denoted by $\mathbf{q}_B^{\star}$ to $\mathcal{L}$.

v. $\mathcal{A}$ wins the game if $\mathbf{q}_B^* = \mathbf{q}_B^{\star}$.

To win this game, $\mathcal{A}$ needs to copy the photon polarization states exactly as they are. However, given quantum unreality and uncertainty, it is impossible to copy an unknown quantum state [37]. $\mathcal{A}$'s best strategy would be to measure all photons in the same basis, i.e., either all in the H-V basis or all in the $\pm 45^{o}$ basis. This strategy results in a random collapse of each photon with a 50-50 probability within the wrong basis, i.e., if the photon was polarized using the H-V basis but measured in the $\pm 45^{o}$ basis, it will randomly collapse into either $|\nwsearrow\rangle$ or $|\neswarrow\rangle$, and vice versa. Therefore, if the length of $\mathbf{q}_B$ is l_B bits, then the advantage of the adversary winning this game is given by $\boldsymbol{\alpha}_{\mathcal{G}_{Sec}^{qubit}} = \frac{1}{4^{l_B/2}} = \frac{1}{2^{l_B}} \approx 0 \quad \forall \quad l_B \geq 10$. ■

Theorem 1 (Data Provenance): If a PDC successfully verifies σ in the proposed protocol, then the source of the data is indeed true.

Proof: The adversary $\mathcal{A}$ aims to tamper with the data sent to the PDC. Let us model the security of the proposed protocol with a security game $\mathcal{G}_{Sec}^{Prov}$ between an adversary $\mathcal{A}$ and challenger $\mathcal{L}$:

i. $\mathcal{L}$ initiates the proposed protocol between a PMU U^* and a PDC.

ii. $\mathcal{A}$ uses $\mathtt{Send}ID$, $\mathtt{Send}S$, $\mathtt{Drop}$, and $\mathtt{Monitor}$ to query the PMU U_1 and PDC a polynomial number of times.

iii. $\mathcal{A}$ attempts to impersonate the PMU by invoking the $\mathtt{Send}S$ oracle and sending invalid data.

iv. $\mathcal{A}$ wins this game if the PDC accepts the tampered data sent by $\mathcal{A}$.

To win this game, the $\mathcal{A}$ must be able to encode each bit of the hash digest σ using the correct basis, i.e., H-V or ±45°. To do this, $\mathcal{A}$ needs to obtain R_i. However, by Lemma 1, the only option for $\mathcal{A}$ is to randomly guess R_i. Therefore, the adversary's advantage in winning this game is negligible, i.e., $\boldsymbol{\alpha}_{\mathcal{G}_{Sec}^{Prov}} = \boldsymbol{\alpha}_{\mathcal{G}_{Sec}^{PUF}} \approx 0$.

The $\mathcal{A}$ can also win this game if he/she can copy the photon polarization states exactly as they are. However, by Lemma 2, the adversary's advantage in this case is also negligible, i.e., $\boldsymbol{\alpha}_{\mathcal{G}_{Sec}^{Prov}} = \boldsymbol{\alpha}_{\mathcal{G}_{Sec}^{qubit}} \approx 0 \quad \forall \quad l_B \geq 10$. ■

Lemma 3: The proposed protocol is secure against man-in-the-middle attacks.

Proof: The fact that an adversary cannot tamper with the data sent from the PMUs is established in Theorem 1. However, an adversary can still cause all the packets in a window to be discarded by the PDC, typically called a grey-hole attack. In this attack, an adversary measures Ψ_{σ} which causes the photons carrying σ to collapse. However, thanks to quantum mechanics, eavesdropping is immediately detected by the sender or the recipient [79]; hence, a grey hole attack can easily be detected in the proposed protocol. Therefore, the maximum impact that an adversary can have is a loss of information worth one window of packets before being detected. However, synchrophasor networks have inherent redundancy which makes them resilient against the loss of just one window worth of packets [80]. Note that, although an adversary may cause a loss of one window of packets, given the fact that PMUs use UDP at the transmission layer, discarded packets are not retransmitted, avoiding any extra loss of resources through retransmission attacks [81]. This also makes it apparent that DoS attacks won't be fruitful either. ■

VIII. EXPERIMENTAL VALIDATION

As described in Step 3 of the proposed model (Section VI), following the PMU's successful transmission of n data packets, it proceeds to stimulate its PUF using the challenge C_i, resulting in the acquisition of the response R_i. Subsequently, the PMU employs the bits contained in R_i to transmit σ over the quantum channel (Fig. 1). Assuming R_i and σ share the same length, each bit in R_i is encoded into σ using an angle or tensor encoding pattern. The angle encoding scheme utilizes the phase or rotation property of a qubit to represent information [82]. This encoding employs rotation gates to represent classical information. The general mathematical form is:

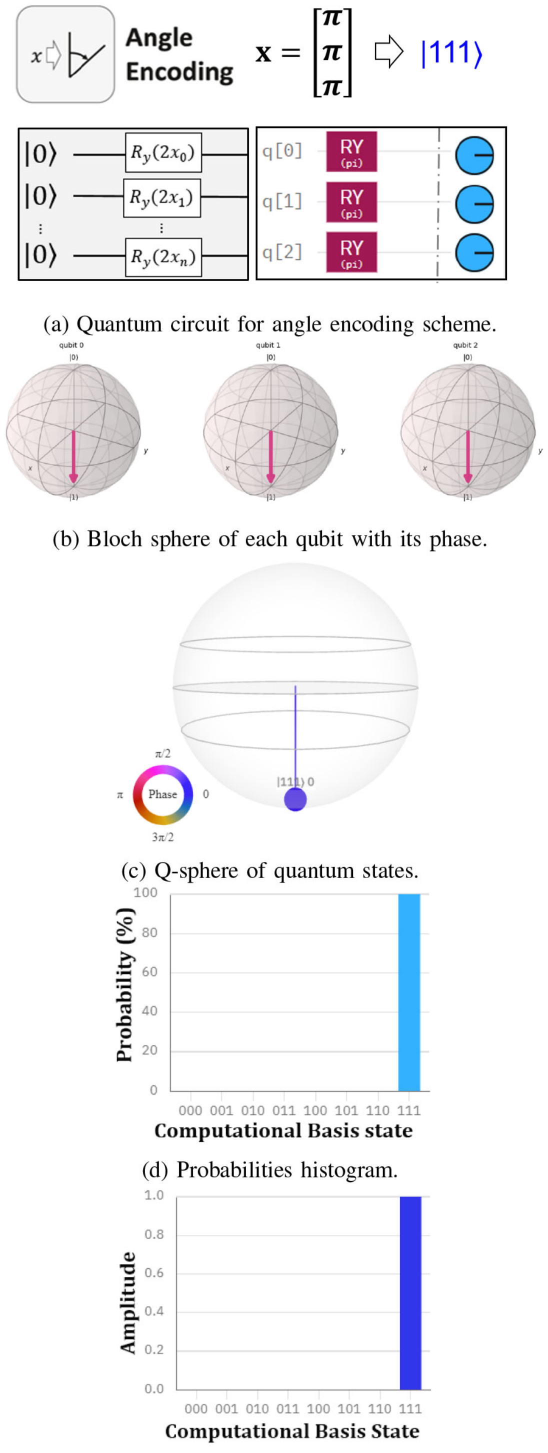
$$|x\rangle = \bigotimes_{i}^{N} R(x_i)\left|0^N\right\rangle, \ \ or$$
$$|x\rangle = \bigotimes_{i=1}^{N} \cos(x_i)|0\rangle + \sin(x_i)|1\rangle, \qquad (2)$$

where $\bigotimes$ is the tensor product operation over N qubits, R can be any Pauli gate R_x, R_y, R_z for x, y, and z--axes rotation to encode N features into the rotation angles of n-qubits. For instance, in Fig. 4, the data point $\mathbf{x} = (\pi, \pi, \pi)$ has been encoded as $|\boldsymbol{\psi}\rangle = |111\rangle$. From Fig. 4(a), it can be noticed that we have also introduced an R_y gate, which is a single-qubit gate that rotates the qubit state around the y-axis of the Bloch sphere by a given angle. Consider a rotation operator gate $R_{\text{y}}(\theta)$; then θ-angle rotation around the y-axis is expressed by:

$$\text{y} = \cos\left(\frac{\theta}{2}\right), \ \ or$$
$$\theta = 2\arccos(\text{y}) = 2\cos^{-1}(0) = \pi \ \text{radians}, \qquad (3)$$

where the R_{y} gate implements $\exp^{(-i\frac{\theta}{2}\text{y})}$ on the Bloch sphere, causing the qubit state to be rotated by the specified angle around the y-axis. In fact, on decomposition, this gate is $U3(\theta, \varphi, \lambda)$, i.e., the general U gate is a single-qubit rotation powerful gate that allows for any arbitrary rotations of a single qubit. By selecting appropriate values for 3 Euler angles: $[U(\theta, \varphi, \lambda)]$, we can rotate the qubit state to any point on the Bloch sphere. The role of these rotational gates allows us to adjust the amplitudes of the $|0\rangle$ and $|1\rangle$ states, which in turn affects the probabilities of measuring these states.

In Fig. 4(a), classical 3-dimensional data points are encoded using 3-qubits ($q[0]$, $q[1]$, and $q[2]$) by introducing three R_Y rotational gates. The combination of these gates encodes given classical information into the angle and amplitudes of quantum states. Bloch sphere and Q-sphere visualizations are shown in Fig. 4(b) and (c), respectively. It is essential to emphasize that the Q-sphere differs from the Bloch sphere or phase disk, which represents a single qubit [37]. In Fig. 4(b), the Bloch sphere represents the amplitudes of the individual qubits, each with its respective phase angle of π radians. On the other hand, the Q-sphere (Fig. 4(c)) mainly visualizes the relative phase relationships between different states, i.e., in this case, all states have the same phase of 0° relative to each other (marked in blue). The Q-sphere offers a global perspective of a multi-qubit state based on a computational basis. The size of each node is indicative of the state's probability, while color corresponds to the phase of individual basis states. The Q-sphere aids in comprehending the behavior of qubit registers (multi-qubit states) when subjected to quantum circuits. It's more revelatory to take a holistic view of the quantum state as a whole. The phase disk at the endpoint of each qubit, as illustrated in Fig. 4(a), provides a local view of the quantum state of each qubit at the conclusion of the computation. It is anticipated that the probability of measuring the $|1\rangle$ state for qubits $q[0]$, $q[1]$, and $q[2]$ will be 100%, which is further depicted in Fig. 4(d) histogram. In Fig. 4(e), the statevector plot illustrates the amplitude of the quantum state $|\boldsymbol{\psi}\rangle = |111\rangle$.



(a) Quantum circuit for angle encoding scheme.

(b) Bloch sphere of each qubit with its phase.

(c) Q-sphere of quantum states.

(d) Probabilities histogram.

(e) Statevector histogram.

FIGURE 4. **Quantum Information Mapping and Analysis.**

Considering our proposed model, if we take $R_i = 010011$ and use an angle embedding scheme to encode its corresponding bit into the quantum state $|\psi_\sigma\rangle$ as $\sigma = 110010$, following the two provided conditions below:

i. If the current R_i bit is 0, encode the corresponding bit in σ using the H-V basis.
ii. If the current R_i bit is 1, encode the corresponding bit in σ using ±45 basis.

The encoding procedure outlined above is depicted in Fig. 5. In Fig. 5(a), the quantum circuit holds the combination of Hadamard (H) and rotational (R) gates. The H-gate induces a non-trivial superposition in the qubit, and when measured, it equally likely collapses to either $|0\rangle$ or $|1\rangle$ [37]. For instance, if the current bit in R_i is '0', the H-gate is applied, commonly used for encoding information in the horizontal-vertical (H-V) basis. When applied to a qubit initialized in the $|0\rangle$ state, it transforms it into an equal superposition of $|\updownarrow\rangle$ and $|\leftrightarrow\rangle$, expressed as:

$$H|0\rangle = \frac{|\updownarrow\rangle + |\leftrightarrow\rangle}{\sqrt{2}}$$

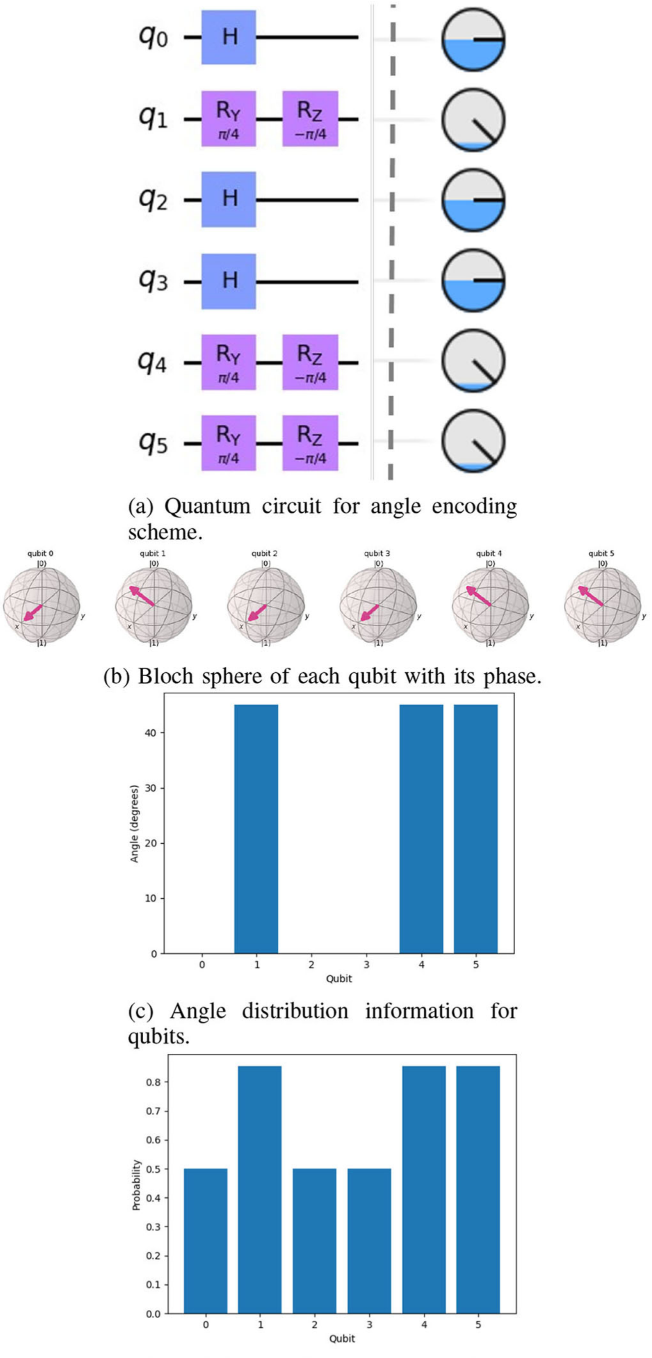
Thereby, the H-gate transforms the basis states $|0\rangle$ and $|1\rangle$ into the H-V basis states $|\updownarrow\rangle$ and $|\leftrightarrow\rangle$, respectively. The Pauli gates R_y and R_z are single-qubit rotational gates that rotate the qubit state around the y or z-axis of the Bloch sphere by a given angle, respectively [35]. For example, when the current bit in R_i is '1', a combination of rotational gates is applied. The R_y gate with a rotation angle of $\pi/4$ $(+45°)$ around the y-axis is applied, followed by an R_z gate with a rotation angle of $-\pi/4$ $(-45°)$ around the z-axis. This combination of gates transforms the basis states $|0\rangle$ and $|1\rangle$ into the ±45° basis states (i.e., $| \nwsearrow\ or\ \neswarrow\rangle$), corresponding to ±45° rotations from the standard $|0\rangle$ and $|1\rangle$ states. Fig. 5(b), illustrates that the qubit states are in:

$$|\updownarrow\rangle_1^{H-V}|\nwsearrow\rangle_1^{\pm45^o}|\leftrightarrow\rangle_0^{H-V}|\leftrightarrow\rangle_0^{H-V}|\nwsearrow\rangle_1^{\pm45^o}|\neswarrow\rangle_0^{\pm45^o},$$

where $|\updownarrow\rangle_b^{H-V}$ represents the encoding of a digit b in H-V basis, while $|\nwsearrow\rangle_1^{\pm45^o}$ and $|\neswarrow\rangle_0^{\pm45^o}$ represent the encoding of digits 1 and 0 in the ±45 basis, respectively. Moreover, the phase disk at the end of each qubit in the quantum circuit (Fig. 5(a)) provides a local view of the individual quantum state at the end of the computation, where the probability that the measured states of encoded qubits $q_0, q_1, \ldots, q_5$ will be in the $|0\rangle$ state is expected to be as follows:

$$\begin{aligned}
&\text{Qubit 0:} && \text{Probability} = 0.5000, && \text{Angle} = \pm 0^\circ\\
&\text{Qubit 1:} && \text{Probability} = 0.8536, && \text{Angle} = \pm 45^\circ\\
&\text{Qubit 2:} && \text{Probability} = 0.5000, && \text{Angle} = \pm 0^\circ\\
&\text{Qubit 3:} && \text{Probability} = 0.5000, && \text{Angle} = \pm 0^\circ\\
&\text{Qubit 4:} && \text{Probability} = 0.8536, && \text{Angle} = \pm 45^\circ\\
&\text{Qubit 5:} && \text{Probability} = 0.8536, && \text{Angle} = \pm 45^\circ.
\end{aligned}$$

The above probabilities with angle distribution information/statistics are further plotted in Fig. 5(c) and (d), respectively. In summary, the H-gate is used to encode bits in the H-V basis because it provides a superposition of $|\updownarrow\rangle$ and $|\leftrightarrow\rangle$, allowing information to be encoded probabilistically in both basis states. This is useful for quantum algorithms and quantum information processing in synchrophasor technology. On the other hand, the combination of R_y and R_z gates is used to encode bits in the ±45° basis because it allows for a controlled rotation of the qubit state to achieve the desired angle. This is particularly useful when encoding information that needs to be distinguished at ±45° angles,



(a) Quantum circuit for angle encoding scheme.

(b) Bloch sphere of each qubit with its phase.

(c) Angle distribution information for qubits.

(d) Probabilities distribution for qubits.

FIGURE 5. Quantum Information Mapping and Analysis: classical data mapping into quantum bits (qubits) using angle encoding.

which may be required in certain quantum algorithms or quantum communication protocols. Overall, the choice of gates in the encoding procedure depends on the specific quantum basis or angle representation required for the application or algorithm being implemented. In our case, the protocol is designed to support encoding in both the H-V basis and the ±45° basis.

Besides, quantum encoding allows for a more efficient representation of data. For example, angle encoding uses the phase or rotation property of a qubit to represent information, which can encode multiple states within a single qubit. This leads to a significant reduction in resource requirements compared to the classical binary encoding used in traditional methods [35], [82]. It is pertinent to note that the angle or tensor product encoding technique processes one data point at a time, as opposed to encoding entire datasets like basis or amplitude encoding [37]. Consequently, it necessitates N qubits, specifically 1 qubit per data point. Nevertheless, there exists another variant known as *dense angle encoding*, which requires only half of the qubits to encode the same volume of data points. Angle encoding patterns prove particularly advantageous in image processing, where they employ the angle parameter of a qubit to represent color information. This technique is employed for creating flexible representations of quantum images, allowing distinct angle levels to encode RGB information, combined with tensor products for location information (x-axis, y-axis, or z-axis) to depict an image [83]. Furthermore, this encoding method finds applications in quantum neural networks, quantum machine learning models, parameterized quantum circuits, and for optimizing performance or reducing error rates in quantum circuits for diverse applications [84], [85].

IX. PERFORMANCE ANALYSIS

This section demonstrates the feasibility of the proposed protocol with real-time applications in synchrophasors. All the results that are presented in this section represent the additional overhead incurred by the proposed protocol in comparison to a conventional synchrophasor network that does not use any kind of security primitive or protocol.

A. COMPUTATIONAL COMPLEXITY

The proposed protocol exclusively relies on a cryptographically secure hash and abstains from employing other cryptographic primitives. The worst-case time complexity of secure hash functions is typically assessed based on the number of operations directly proportional to the length of the hash, denoted as $O(m)$, where m signifies the length of the hash output. This implies that utilizing a fixed-length output for cryptographically secure hash results in constant computational complexity. In the proposed protocol, each packet transmitted from the PMU to the PDC triggers the computation of a single secure hash, as depicted in Fig. 3. Assuming a 256-bit cryptographically secure hash, the worst-case running time becomes $O(256) \approx O(1)$. Thus, we assert that the proposed protocol exhibits significant lightweight characteristics in comparison to conventional/traditional data integrity measures employed in cryptography. For example, the computational complexity of a message authentication code (MAC) is $O(M)$ for each packet, where M represents the message size. This stands in stark contrast to the $O(1)$ complexity per packet achieved by the proposed protocol. It's also worth noting that, typically, $M \gg m$.

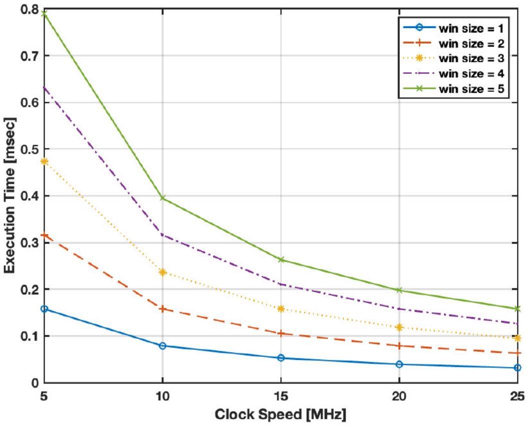


FIGURE 6. Execution time overhead of the proposed technique using SHA-256 based on various clock speeds.

B. EXECUTION TIME

Given the time-critical nature of synchrophasors, evaluating any security protocol designed for these networks must prioritize execution time. In this context, we examine the MSP-430 16-bit microcontroller [86]. For each data packet that the PMU sends to the PDC in the proposed protocol, the only additional operation is computing one cryptographically secure hash for each packet. Assuming a conversion resolution of 20 bits for modern PMUs [87], the execution time for computing an SHA-256-based hash is illustrated in Fig. 6. The data presented in Fig. 6 indicates that the execution time overhead for computing an SHA-256 hash on an MSP-430 16-bit microcontroller remains below 0.8 milliseconds across various clock speeds, with a downward trend as clock speed increases. Specifically, at a clock speed of 25 MHz, the execution time overhead for all window sizes converges to just above 0.1 milliseconds, demonstrating the protocol's minimal impact on execution time and its viability for time-sensitive synchrophasor networks. Consequently, the proposed protocol emerges as a suitable choice for time-critical applications in synchrophasor networks.

To further investigate the merit of the proposed technique compared to other conventional cryptographic primitives such as AES 128 and the more recent lightweight block ciphers Speck and Simon [86], Fig. 7 presents a comparative analysis of execution times for various cryptographic algorithms at different clock speeds on the MSP-430 16-bit microcontroller. The proposed technique consistently requires less execution time than existing lightweight techniques. For example, at a clock speed of 10 MHz, the proposed method's execution time is approximately

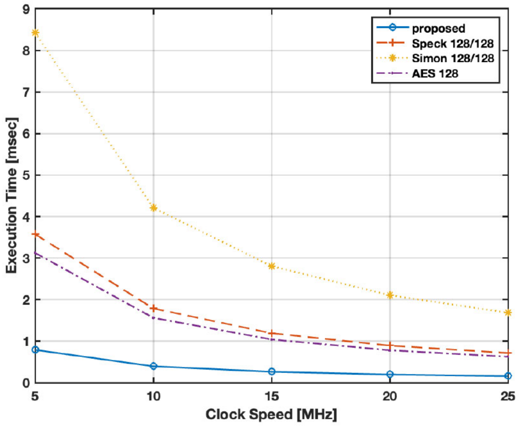


FIGURE 7. Comparison of execution times.

0.5 milliseconds, compared to the 2 milliseconds for Speck, 4.2 milliseconds for Simon, and slightly over 1.5 milliseconds for AES 128. This efficiency is mirrored on both the PMU and PDC sides as the number of hash operations required is identical.

C. COMMUNICATION OVERHEAD

The communication overhead associated with encryption-based signature systems, such as RSA, typically ranges from 128 to 256 bytes. In contrast, our proposed scheme introduces a minimal additional load by sending an extra 256 bits for each window of packets, facilitated by a 256-bit cryptographically secure hash function. Let's consider a PMU with a sampling rate of 50 samples per second, transmitting 10 samples per data packet. Assuming a maximum verification delay of 1 second that the PDC can tolerate, then the window size (n) is limited to ≤ 5. Accordingly, this results in a mere 256 bits of additional overhead for each window of n packets, leading to a per-packet communication overhead of $256/n$ bits. Compared to traditional MAC-based schemes, which typically incur a 256-bit overhead for each data packet, the proposed scheme adds an incremental 256 bits per window, resulting in a substantially lower per-packet overhead when considering windows containing multiple packets. This reduced overhead demonstrates the protocol's efficiency in handling the high-frequency traffic characteristic of synchrophasor systems.

D. STORAGE OVERHEAD

In the proposed protocol, the maximum data storage requirement for each PMU is equivalent to the output length of the employed cryptographically secure hash function. Given an output length of 256 bits, the storage demand for each PMU is notably modest, especially when compared to the storage capacities of typical PMUs, which can store from a few megabytes up to tens of megabytes. On the PDC side, storage needs are minimal, with the PDC only required to store one CRP for each PMU [75] and a 256-bit hash value.

X. CONCLUSION

This paper introduced a pioneering data provenance protocol tailored for synchrophasor networks in the quantum era. Central to the protocol's design is the integration of PUFs and quantum mechanics. PUFs play a crucial role in authenticating data sources, while quantum mechanics, through its principles of unreality and uncertainty, offers robust protection against data tampering. A security evaluation of the proposed protocol indicates its capability to deliver impeccable security, remarkably without relying on any computationally complex cryptographic primitives. Additionally, implementation tests on IBM's Qiskit platform confirm its practicality and efficiency, requiring minimal quantum gates. This marks a significant advancement in securing synchrophasor networks by leveraging the potential of quantum computing. Furthermore, a performance analysis unequivocally confirms that compared to typical synchrophasor communications (i.e., without using any security primitives), the proposed protocol maintains a worst case computational complexity of $O(1)$, an additional execution time bounded by the time required to compute a cryptographically secure hash on a given platform, an upper bound of per packet communication overhead of 256-bits, and additional storage requirements of one CRP at the PMU while one CRP per PMU at the PDC. These benchmarks make the proposed protocol a promising solution for real-world implementations.

Looking forward, future research directions should concentrate on addressing potential threats associated with the use of PUFs, with a particular emphasis on developing robust defense strategies to safeguard against man-in-the-middle and various forms of side-channel attacks, including invasive, semi-invasive, and non-invasive attacks. Particularly, the vulnerability of security credentials, identities, and secret keys stored in the PDC to hardware and software exploits poses a critical challenge. It is imperative for researchers to propose innovative and reliable hybrid-controlled strong PUF [59], [88], [89], [90], or Quantum-based PUF (QPUF) solutions [91] to mitigate such attacks, further strengthening the security of synchrophasor networks in the quantum era.

ACKNOWLEDGMENT

The authors acknowledge the IBM open-source Qiskit-SDK.

REFERENCES

[1] H. Bevrani, M. Watanabe, and Y. Mitani, *Power System Monitoring and Control*. Hoboken, NJ, USA: Wiley, 2014.

[2] "About NASPI—North American synchrophasor initiative." 2024. [Online]. Available: https://www.naspi.org/

[3] C. Tu, X. He, X. Liu, and P. Li, "Cyber-attacks in PMU-based power network and countermeasures," *IEEE Access*, vol. 6, pp. 65594–65603, 2018.

[4] E. Handschin, F. Schweppe, J. Kohlas, and A. Fiechter, "Bad data analysis for power system state estimation," *IEEE Trans. Power App. Syst.*, vol. 94, no. 2, pp. 329–337, Mar. 1975.

[5] M. Baran and A. Abur, "Power system state estimation," in *Wiley Encyclopedia of Electrical and Electronics Engineering*, New York, NY, USA: Wiley, 1999.

[6] Y. Deng and S. Shukla, "Vulnerabilities and countermeasures: A survey on the cyber security issues in the transmission subsystem of a smart grid," *J. Cyber Secur. Mobility*, vol. 1, no. 2, pp. 251–276, 2012.

[7] B. Appasani and D. K. Mohanta, "A review on synchrophasor communication system: Communication technologies, standards and applications," *Prot. Control Mod. Power Syst.* vol. 3, p. 37, Dec. 2018.

[8] H. Yang, S. Liang, X. Luo, D. Tang, H. Li, and X. Shen, "PIPC: Privacy-and integrity-preserving clustering analysis for load profiling in smart grids," *IEEE Internet Things J.*, vol. 9, no. 13, pp. 10851–10861, Jul. 2022.

[9] A. Rashid, M. N. Aman, M. Ullah, and B. Sikdar, "Detecting data tampering in synchrophasors using power flow entropy," in *Proc. IEEE Innovat. Smart Grid Technol. Asia (ISGT Asia)*, Singapore, 2018, pp. 850–855.

[10] M. S. Siddiqui, A. Rahman, and A. Nadeem, "Secure data provenance in IoT network using bloom filters," *Procedia Comput. Sci.*, vol. 163, pp. 190–197, Jan. 2020.

[11] S. Suhail et al., "Data trustworthiness in IoT," in *Proc. ICOIN*, 2018, pp. 414–419.

[12] J. L. C. Sanchez, J. B. Bernabe, and A. F. Skarmeta, "Towards privacy preserving data provenance for the Internet of Things," in *Proc. IEEE WF-IoT*, Singapore, 2018, pp. 41–46.

[13] Z. Liu and Y. Wu, "An index-based provenance compression scheme for identifying malicious nodes in multihop IoT network," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4061–4071, May 2020.

[14] U. Javaid, M. N. Aman, and B. Sikdar, "BlockPro: Blockchain based data provenance and integrity for secure IoT environments," in *Proc. ACM BlockSys*, 2018, pp. 13–18.

[15] N. Baracaldo, L. A. D. Bathen, R. O. Ozugha, R. Engel, S. Tata, and H. Ludwig, "Securing data provenance in Internet of Things (IoT) systems," in *Proc. Int. Conf. Service Orient. Comput.*, Cham, Switzerland, 2016, pp. 92–98.

[16] S. Ali et al., "Secure data provenance in cloud-centric Internet of Things via blockchain smart contracts," in *Proc. IEEE SmartWorld, Ubiquitous Intell.*, Guangzhou, China, 2018, pp. 991–998.

[17] M. Sigwart et al., "Blockchain-based data provenance for the Internet of Things," in *Proc. ACM Int. Conf. Internet Things*, New York, NY, USA, 2019, pp. 1–8.

[18] M. Elkhodr, B. Alsinglawi, and M. Alshehri, "Data provenance in the Internet of Things," in *Proc. WAINA*, 2018, pp. 727–731.

[19] W. Arthur, D. Challener, and K. Goldman, *A Practical Guide to TPM 2.0: Using the New Trusted Platform Module in the New Age of Security*. Berkeley, CA, USA: Apress, 2015.

[20] "Trusted computing." Trust. Comput. Group. 2023. [Online]. Available: https://trustedcomputinggroup.org/trusted-computing/

[21] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. ACM Conf. Comput. Commun. Secur.*, Chicago IL, USA, 2009, pp. 21–32.

[22] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.

[23] H. Sandberg, A. Teixeira, and K. Johansson, "On security indices for state estimators in power networks," in *Proc. 1st Workshop Secure Control Syst.*, Stockholm, Sweden, 2010, pp. 1–6.

[24] R. B. Bobba, K. M. Rogers, Q. Wang, and H. Khurana, "Detecting false data injection attacks on DC state estimation," in *Proc. 1st Workshop Secure Control Syst.*, 2010, pp. 1–9.

[25] A. Giani, R. Bent, M. Hinrichs, M. McQueen, and K. Poolla, "Metrics for assessment of smart grid data integrity attacks," in *Proc. IEEE Power Energy Soc. Gener. Meet.*, 2012, pp. 1–8.

[26] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 326–333, Jun. 2011.

[27] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "The SIMON and SPECK lightweight block ciphers," in *Proc. 52nd Annu. Design Autom. Conf. (DAC)*, San Francisco, CA, USA, 2015, pp. 1–6.

[28] J.-L. Danger, "Physically unclonable functions: Principle, advantages and limitations," in *Proc. Int. Conf. Adv. Technol. Commun. (ATC)*, 2019, p. 32.

[29] O. S. Althobaiti and M. Dohler, "Cybersecurity challenges associated with the Internet of Things in a post-quantum world," *IEEE Access*, vol. 8, pp. 157356–157381, 2020.

[30] P. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, 1994, pp. 124–134.

[31] R. L. Rivest, A. Shamir, and L. Adleman, "On digital signatures and public-key cryptosystems," Lab. Comput. Sci., Cambridge, MA, USA, Rep. MIT/LCS/TR-212, 1978.

[32] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *Soc. Ind. Appl. Math. Rev.*, vol. 41, no. 2, pp. 303–332, Jan. 1999.

[33] N. Aaraj, A. Raghunathan, and N. K. Jha, "Analysis and design of a hardware/software trusted platform module for embedded systems," *ACM Trans. Embed. Comput. Syst.* vol. 8, no. 1, pp. 1–31, 2009.

[34] D. Moghimi et al., "TPM-Fail: TPM meets timing and lattice attacks," in *Proc. 29th USENIX Secur. Symp.*, 2020, pp. 2057–2073. [Online]. Available: https://www.usenix.org/conference/usenixsecurity20/presentation/moghimi

[35] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th ed. Cambridge, U.K.: Cambridge Univ. Press, 2010.

[36] A. Khrennikov, "Roots of quantum computing supremacy: Superposition, entanglement, or complementarity?" *Eur. Phys. J. Spec. Topics*, vol. 230, no. 4, pp. 1053–1057, Jun. 2021.

[37] R. S. Sutor, *Dancing With Qubits*. Birmingham, U.K.: Packt Publ., 2019.

[38] D. Castelvecchi and E. Gibney, "'Spooky' quantum-entanglement experiments win physics nobel," *Nature*, vol. 610, no. 7931, pp. 241–242, 2022.

[39] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th Annu. ACM Symp. Theory Comput.*, New York, NY, USA, 1996, pp. 212–219.

[40] X. Yunlong, S. Kuntal, Y. Siren, and G. Gilad, "Uncertainty principle of quantum processes," *Phys. Rev. Res.*, vol. 3, no. 2, Apr. 2021, Art. no. 023077.

[41] M. Kirkpatrick et al., "System on chip and method for cryptography using a physically unclonable function," U.S. Patent 8 750 502 B2, Mar. 2014.

[42] B. Kuang, A. Fu, W. Susilo, S. Yu, and Y. Gao, "A survey of remote attestation in Internet of Things: Attacks, countermeasures, and prospects," *Comput. Secur.*, vol. 112, Jan. 2022, Art. no. 102498.

[43] A. Lioy and G. Ramunno, "Trusted computing," in *Handbook of Information and Communication Security*, P. Stavroulakis and M. Stamp, Eds. Berlin, Germany: Springer, 2010.

[44] Y. Gao, S. F. Al-Sarawi, and D. Abbott, "Physical unclonable functions," *Nat. Electron.*, vol. 3, pp. 81–91, Feb. 2020.

[45] A. Al-Meer and S. Al-Kuwari, "Physical unclonable functions (PUF) for IoT devices," *ACM Comput. Surveys*, vol. 55, no. 14, pp. 1–31, Jul. 2023.

[46] H. Ning, F. Farha, A. Ullah, and L. Mao, "Physical unclonable function: Architectures, applications and challenges for dependable security," *IET Circuits, Devices Syst.*, vol. 14, no. 4, pp. 407–424, 2020.

[47] D. Li, H. Guo, and J. Xu, "Enhancing TPM security by integrating SRAM PUFs technology," in *Proc. 2nd ACM Int. Workshop Cyber Phys. Syst. Secur.*, 2016, pp. 82–93.

[48] R. Johnson, J. Mueller, Y. Saadatazadeh, and J. Y. Ci Kim, *Trusted Platform Module and Privacy: Promises and Limitations*, Univ. Auckland, Auckland, New Zealand, 2005.

[49] U. Rührmair, S. Devadas, and F. Koushanfar, "Security based on physical unclonability and disorder," in *Introduction to Hardware Security and Trust*, New York, NY, USA: Springer, 2012, pp. 65–102.

[50] P. Gope, A. K. Das, N. Kumar, and Y. Cheng, "Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks," *IEEE Trans. Indust. Inform.*, vol. 15, no. 9, pp. 4957–4968, Sep. 2019.

[51] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug. 2014.

[52] U. Rührmair and J. Sölter, "PUF modeling attacks: An introduction and overview," in *Proc. Conf. Design, Autom. Test Eur. (DATE)*, 2014, pp. 1–6.

[53] B. Gassend, D. Clarke, M. Van Dijk, and S. Devadas, "Controlled physical random functions," in *Proc. 18th Annu. Comput. Secur. Appl. Conf.*, 2002, pp. 149–160.

[54] B. Gassend, M. Van Dijk, D. Clarke, E. Torlak, S. Devadas, and P. Tuyls, "Controlled physical random functions and applications," *ACM Trans. Inf. Syst. Secur. (TISSEC)*, vol. 10, no. 3, pp. 1–22, 2008.

[55] U. Rührmair et al., "PUF modeling attacks on simulated and silicon data," *IEEE Trans. Inf. Forensics Security*, vol. 8, pp. 1876–1891, 2013.

[56] A. Vijayakumar, V. Patil, C. B. Prado, and S. Kundu, "Machine learning resistant strong PUF: Possible or a pipe dream?" in *Proc. IEEE Int. Symp. Hardw. Orient. Security Trust (HOST)*, 2016, pp. 19–24.

[57] U. Rührmair and M. van Dijk, "PUFs in security protocols: Attack models and security evaluations," in *Proc. IEEE Symp. Security Privacy*, 2013, pp. 286–300.

[58] S. W. Lee et al., "Designing secure PUF-based authentication protocols for constrained environments," *Sci. Rep.*, vol. 13, Dec. 2023, Art. no. 21702.

[59] X. Xi, G. Li, Y. Wang, and M. Orshansky, "A provably secure strong PUF based on LWE: Construction and implementation," *IEEE Trans. Comput.*, vol. 72, no. 2, pp. 346–359, Feb. 2023.

[60] A. Venkatesh and A. Sanyal, "A machine learning resistant strong PUF using subthreshold voltage divider array in 65nm CMOS," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, 2019, pp. 1–5.

[61] Y. Gao et al., "Emerging physical unclonable functions with nanotechnology," *IEEE Access*, vol. 4, pp. 61–80, 2016.

[62] G. Li, Khalid T. Mursi, and Y. Zhuang, "Lightweight strategy for XOR PUFs as security primitives for resource-constrained IoT devices," 2022, *arXiv:2210.01749*.

[63] J. Yao et al., "Design and evaluate recomposited OR-AND-XOR-PUF," *IEEE Trans. Emerg. Topics Comput.*, vol. 10, no. 2, pp. 662–677, Jun. 2022.

[64] C. Gu et al., "A modeling attack resistant deception technique for securing lightweight-PUF-based authentication," *IEEE Trans. Comput. Aided Design Integr. Circuits Syst.*, vol. 40, no. 6, pp. 1183–1196, Jun. 2021.

[65] Y. Gao et al., "Obfuscated challenge-response: A secure lightweight authentication mechanism for PUF-based pervasive devices," in *Proc. IEEE Int. Conf. Pervas. Comput. Commun. Workshops (PerCom Workshops)*, 2016, pp. 1–6.

[66] J. Zhang and C. Shen, "Set-based obfuscation for strong PUFs against machine learning attacks," *IEEE Trans. Circuits Syst.*, vol. 68, no. 1, pp. 288–300, Jan. 2021.

[67] Y. Gao et al., "Systematically evaluation of challenge obfuscated APUFs," 2022, *arXiv:2203.15316*.

[68] Y. Gao, H. Ma, S. F. Al-Sarawi, D. Abbott, and D. C. Ranasinghe, "PUF-FSM: A controlled strong PUF," *IEEE Trans. Comput. Aided Design Integr. Circuits Syst.*, vol. 37, no. 5, pp. 1104–1108, May 2018.

[69] J. Zhang, Y. Lin, Y. Lyu, and G. Qu, "A PUF-FSM binding scheme for FPGA IP protection and pay-per-device licensing," *IEEE Trans. Inf. Forensics Security*, vol. 10, pp. 1137–1150, 2015.

[70] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst., Signal Process.*, 1984, pp. 175–179.

[71] "Nobel prize in physics 2022." 2022. [Online]. Available: https://www.nobelprize.org/prizes/physics/2022/summary/

[72] *Synchrophasor Data Transfer for Power Systems*, IEEE Standard C37.118.2, 2011.

[73] S. You, Y. Su, Y. Liu, and Y. Liu, "Wide-area monitoring and anomaly analysis based on synchrophasor measurement," in *New Technologies for Power System Operation and Analysis*. H. Jiang, Y. Zhang, and E. Muljadi, Eds. Waltham, MA, USA: Acad. Press, 2021, pp. 143–161.

[74] R. Canetti and H. Krawczyk, "Universally composable notions of key exchange and secure channels," in *Proc. EUROCRYPT*, Amsterdam, The Netherlands, 2002, pp. 337–351.

[75] M. N. Aman, M. H. Basheer, and B. Sikdar, "Data provenance for IoT with light weight authentication and privacy preservation," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10441–10457, Dec. 2019.

[76] "TOTP: Time-based one-time password algorithm," Internet Eng. Task Force, RFC 6238, 2011.

[77] K. Lounis and M. Zulkernine, "More lessons: Analysis of PUF-based authentication protocols for IoT," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2021/1509, 2021.

[78] A. Mahmoud, U. Rührmair, M. Majzoobi, and F. Koushanfar, "Combined modeling and side channel attacks on strong PUFs," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2013/632, 2013.

[79] A. Pourbabak, T. Chen, and W. Su, "Emerging data encryption methods applicable to energy Internet," in *The Energy Internet*, W. Su and A. Q. Huang, Eds. Sawston, U.K.: Woodhead Publ., 2019, pp. 181–199.

[80] J. Cavitt, S. Wallace, and X. Zhao, "Detecting cyber attacks with packet loss resilience for power systems," *Sustain. Comput. Informat. Syst.*, vol. 34, Apr. 2022, Art. no. 100629.

[81] S. D. Nguyen, M. Mimura, and H. Tanaka, "Abusing TCP retransmission for DoS attack inside virtual network," in *Proc. Int. Workshop Inf. Secur. Appl.*, Cham, Switzerland, 2018, pp. 199–211.

[82] M. Weigold, J. Barzen, F. Leymann, and M. Salm, "Encoding patterns for quantum algorithms," *Inst. Eng. Technol. Quantum Commun.*, vol. 2, no. 4, pp. 141–152, 2021.

[83] F. Yan, A. M. Iliyasu, and S. E. Venegas-Andraca, "A survey of quantum image representations," *Quantum Inf. Process.*, vol. 15, no. 1, pp. 1–35, Jan. 2016.

[84] R. LaRose and B. Coyle, "Robust data encodings for quantum classifiers," *Phys. Rev. A*, vol. 102, no. 3, Sep. 2020, Art. no. 032420.

[85] M. Beisel et al., "Patterns for quantum error handling," in *Proc. 14th Int. Conf. Pervas. Patterns Appl.*, 2022, pp. 22–30.

[86] R. Beaulieu et al., "SIMON and SPECK: Block ciphers for the Internet of Things," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2015/585, 2015.

[87] "Phasor measurement unit data sheet," Vizimax Inc., Longueuil, QC, Canada, 2017. [Online]. Available: https://blob.opal-rt.com/medias/L00161_0917.pdf.

[88] S. R. Sahoo, K. S. Kumar, and K. Mahapatra, "A novel current controlled configurable RO PUF with improved security metrics," *Integration*, vol. 58, pp. 401–410, Jun. 2017.

[89] L. Santiago de Araújo et al., "Design of robust, high-entropy strong PUFs via weightless neural network," *J. Hardw. Syst. Secur.*, vol. 3, pp. 235–249, 2019.

[90] C. Jin, W. Burleson, M. van Dijk, and U. Rührmair, "Programmable access-controlled and generic erasable PUF design and its applications," *J. Cryptogr. Eng.*, vol. 12, pp. 413–432, Mar. 2022.

[91] M. A. Khan, M. N. Aman, and B. Sikdar, "Soteria: A quantum-based device attestation technique for the Internet of Things," *IEEE Internet Things J.*, early access, Dec. 25, 2023, doi: 10.1109/JIOT.2023.3346397.

KASHIF JAVED received the B.Sc. degree in telecommunication engineering and the M.Sc. degree in electrical engineering from the National University of Computer and Emerging Sciences, Pakistan, in 2012 and 2016, respectively, where he is also currently pursuing the Ph.D. degree. His research interests include cyberphysical systems security.

MANSOOR ALI KHAN (Member, IEEE) received the B.Sc. degree in computer systems engineering from KPK UET Peshawar, Pakistan, in 2006, the M.Engg. degree in electrical and electronics engineering from Seoul, South Korea, in 2014, and the Ph.D. degree in physics (nanotechnology) from the University of Sydney, NSW, Australia, in 2018. He is a Research Fellow with the National University of Singapore, Singapore. He was a Research Assistant with ETRI-Samsung, South Korea, and a Postdoctoral Researcher with UNSW, Sydney, Australia. He also possesses special skills in chip design, fabrication, and material characterization for competitive/failure analysis, and performance optimization of commercial devices. His research interests include nanotechnology, quantum materials, quantum computation, and the quantum Internet.

MUKHTAR ULLAH (Senior Member, IEEE) received the B.Sc. degree in electrical engineering from KPK UET Peshawar, Pakistan, in 1998, the M.Sc. degree in control engineering from the University of Manchester, U.K., in 2001, and the Ph.D. degree in electrical engineering from the University of Rostock, Germany, in 2008. He is a Professor with the National University of Computer and Emerging Sciences, Islamabad, Pakistan. His research interests include cyberphysical systems, stochastic models, and cybersecurity.

MUHAMMAD NAVEED AMAN (Senior Member, IEEE) received the B.Sc. degree in computer systems engineering from KPK UET, Peshawar, Pakistan, in 2006, the M.Sc. degree in computer engineering from the Center for Advanced Studies in Engineering, Islamabad, Pakistan, in 2008, and the M.Engg. degree in industrial and management engineering and the Ph.D. degree in electrical engineering from the Rensselaer Polytechnic Institute, Troy, NY, USA, in 2012. He is an Assistant Professor with the University of Nebraska-Lincoln. His research interests include IoT and network security, hardware systems security and privacy, wireless and mobile networks, and stochastic modelling.

BIPLAB SIKDAR (Senior Member, IEEE) received the B.Tech. degree in electronics and communication engineering from North Eastern Hill University, Shillong, India, in 1996, the M.Tech. degree in electrical engineering from the Indian Institute of Technology, Kanpur, India, in 1998, and the Ph.D. degree in electrical engineering from the Rensselaer Polytechnic Institute, Troy, NY, USA, in 2001. He was on the faculty of Rensselaer Polytechnic Institute from 2001 to 2013, first as an Assistant and then as an Associate Professor. He is currently a Professor with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore. His research interests include wireless network, and security for IoT and cyber physical systems.