Accepted As Technical Paper To Appear the 2026 IEEE Consumer Communications & Networking Conference (IEEE CCNC 2026)

Quantum-Safe and Cross-Layer Authentication and Key Agreement Protocol for Smart Grid Communications

Cong Pu† Muhammad Abdullah Bilal† Sunho Lim¶
†Department of Computer Science, Oklahoma State University, Stillwater, OK 74078, USA
¶Department of Computer Science, Texas Tech University, Lubbock, TX 79409, USA
Email: cong.pu@outlook.com, abdullah.bilal@okstate.edu, sunho.lim@ttu.edu

***Abstract*—The extensive value and importance of smart grids are evident in their transformative impact on sustainable urban development. However, the swift progression of quantum computing has made the security and privacy of smart grid communications a pressing and vital issue. Although considerable studies have been carried out on authentication and key agreement within smart grids, the predominant body of solutions either come with substantial computation, communication, and storage overheads, or are primarily single-layer schemes. More importantly, they are not designed to withstand advanced quantum attacks. In this paper, we propose a novel quantum-safe and cross-layer authentication and key agreement protocol, named QCL_{aka}, for smart grid communications that overcomes the shortcomings of existing approaches and offers advanced security and functionality features. The proposed QCL_{aka} protocol integrates lattice-based cryptography with probability physical unclonable function (Prob-PUF) to enable the local gateway and the smart meter to mutually authenticate each other and establish a secure session key. The security of the proposed QCL_{aka} protocol is assessed through formal security verification to highlight its safety in adversarial environments and its ability to withstand both well-known and advanced cyberattacks. Additionally, the experimental evaluation shows that the proposed QCL_{aka} protocol outperforms the benchmark schemes regarding the performance in security and efficiency.**

***Index Terms*—Smart grid communications, security and privacy, authentication, lattice, quantum-safe, cross-layer.**

I. Introduction

In the early 2030s, smart grids have become a pivotal component in the development of smart sustainable cities. By leveraging the Internet of Things (IoT) and modern communication systems, smart grids can intelligently regulate residential/industrial electricity consumption and effectively oversee the entire workflow of power production, transmission, and delivery [1]. In addition, the compelling financial incentives for utility companies to invest in smart grid infrastructure have become apparent. It is anticipated that global savings attributed to smart grids, in the form of reduced energy and emissions costs, are projected to increase from nearly $85 million in 2024 to an impressive $290 billion per year by 2029 [2]. With the comprehensive incorporation of machine learning and artificial intelligence techniques, it is expected that smart grids will pave the way for a future that is not only brighter and sustainable but also deeply transformative for our everyday lives.

The core of smart grids is a two-way communication system [3], where smart meters periodically collect and report time-series energy consumption data to the local gateway via open communication networks. Following this, the local gateway gathers energy usage data from every smart meter within the designated area and transmits it to the control center via relay hubs. Finally, the control center processes these data and if it is necessary, issues and sends commands back to smart meters for energy consumption adjustment, diagnostics, as well as firmware updates. In order to guarantee the security and privacy of smart grid communications, various authentication and key agreement protocols have been developed [4]. In general, authentication and key agreement serve different purposes. Dig deeper, the purpose of authentication is to verify an entity's identification, while the key agreement is the process of allowing two entities to establish a secure secret key over an insecure communication channel. When authentication and key agreement are utilized in combination, they aim to secure communication between entities, ensuring data integrity, confidentiality, and non-repudiation. As a multitude of smart meters are deployed across various sectors to gather users' electricity consumption information and intermittently report these instantaneous data to the local gateway, the importance of authentication and key agreement is self-explanatory in the context of cyber-threat environments. For instance, a criminal could study a wealthy family's electricity consumption patterns to figure out their routines, making it easier to burglarize the house when it's unoccupied. In 2015, hackers used malware to gain access to the SCADA (Supervisory Control and Data Acquisition) network, issuing malicious commands that caused power outages affecting 230,000 residents in Ukraine. In brief, to ensure secure communications and forge a trusting relationship between the smart meters and the local gateway, it's essential to implement strong and secure authentication and key agreement protocols.

Recently, several research studies focusing on authentication and key agreement [5]–[9] have been carried out for smart grids to tackle the security and privacy concerns of communications. However, these existing solutions are primarily single-layer approaches, which mainly employ either public key-based cryptographic methods or identity-based encryption techniques to meet their security requirements. While single-layer approaches can offer some level of security, they may not be robust enough to combat advanced threats within the quantum epoch. In addition, the primary drawback of recent solutions (i.e., [5]–[7]) is that they are highly resource-demanding due to the use of pairings and bilinear maps. On the other hand, identity-based encryption techniques such as [8],

[9] are either vulnerable to well-known cyberattacks (i.e., key escrow attacks, man-in-the-middle attacks, etc.) or incur high communication overhead. Recently, the rapid advancement of quantum technology has led to significant breakthroughs in computational power, enabling researchers to address previously unsolvable problems. However, every coin has two sides. Quantum computing has posed a significant challenge to current cryptographic algorithms used in various domains, including smart grid communications [10]. Therefore, it is imperative to develop quantum-safe security mechanisms to ensure the protection of critical infrastructure communications.

Motivated by the above-mentioned weaknesses and constraints in the existing approaches, in this paper, we propose a novel quantum-safe and cross-layer authentication and key agreement protocol, named QCL_{aka}, for smart grid communications. The proposed QCL_{aka} protocol leverages lattice-based cryptography [11] and probability physical unclonable function (Prob-PUF) [12] to not only facilitate two-way authenticated key exchange between the smart meter and the local gateway, but also perform well in adversarial environments without incurring high overheads. To promote collaboration and accessibility, the QCL_{aka} source code and AVISPA verification program are publicly released at https://github.com/congpu/QCLaka[1].

II. Related Work

In this section, we first classify the state-of-the-art authentication and key agreement protocols into traditional and quantum-safe approaches, and then analyze their security and performance characteristics.

Most traditional authentication and key agreement protocols for smart grids are based on physical unclonable function (PUF), elliptic curve cryptography (ECC), hashing method, and exclusive OR (XOR). In [13], the authors propose a PUF-assisted authentication and key agreement scheme for vehicle-to-grid networks, where the electric vehicle, the charging station, the utility provider authenticate each other and negotiate a session key among themselves. However, the detailed analysis revealed that their scheme is prone to cyberattacks such as ephemeral secret leakage attacks and tracing attacks. To address the issues of identity anonymity and high communication overhead, an ECC-based authentication protocol is proposed for smart grids in [14], where a secret session key is established between the smart meter and the local gateway based on Shangyong Mima2 (SM2) cryptographic algorithm (an variant of ECC). The proposed protocol shows a lower communication overhead in experiments. Nevertheless, the use of computationally intensive operations such as point addition and doubling for authentication is considered to be resource-intensive for smart meters. In [15], an authenticated key agreement protocol is proposed for smart grids where a private blockchain ledger is adopted to store residents' cryptographic information. As the electronic provider needs to frequently access the blockchain ledger for the cryptographic information of smart meters, the proposed approach suffers from high authentication latency and poor scalability.

The rise of quantum computing has driven researchers to reexamine the safety of traditional cryptographic protocols in the quantum-threat environments, and develop quantum-safe security mechanisms that can withstand potential quantum attacks. In [16], the authors propose a device-to-device authenticated key agreement protocol based on lattice-based cryptography for Internet of Things (IoT) networks. With the assistance of the edge server, two devices can mutually authenticate each other and establish a shared session key. However, the storage and communication overheads of their solution are quite excessive primarily because of the large size of the public-private keys. A lattice-based data aggregation mechanism is proposed in [17], where the local edge gateway collects and aggregates encrypted reports from smart meters. The proposed mechanism faces difficulties with the signature verification of smart meters, as the local edge gateway will verify the signature individually. The researchers in [18] propose a range query privacy preserving scheme for smart grids, where the lattice-based homomorphic encryption is utilized to defend against quantum attacks. Their scheme provides the required security and privacy features with low computational cost, however, its communication efficiency needs to be enhanced.

In summary, traditional approaches are able to provide basic security features such as authentication, anonymity, untraceability, and session key agreement. However, they lack resilience to quantum threats. On the other hand, quantum-safe mechanisms are still in the development stage. The proposed QCL_{aka} protocol is the first quantum-safe and cross-layer authentication and key agreement protocol that offers advanced security functionalities without incurring additional overheads.

III. Preliminary Background

A. Probability Physical Unclonable Function

Unlike traditional physical unclonable functions, the probability physical unclonable function (Prob-PUF) [12] leverages the stochastic nature of transistors' detrapping process to form its *challenge-response pairs* (*CRPs*). To be specific, a number of transistors in the Prob-PUF circuit are randomly selected to generate the *challenge*, and their detrapping events are simulated as the *response*. If no detrapping events are observed within the pre-set timeframe for all predetermined charging-and-sensing times, a '0' is produced. Similarly, if a transistor emits the trapped charge all predetermined charging-and-sensing times, a '1' is generated. When the detrapping events occur fewer than the predetermined number of charging-and-sensing times, a random bit (either '0' or '1') is created. Finally, the response is composed of stable bits at the client. Here, the detrapping time constant τ_e varies for each transistor because the locations and the energy of the trap within the circuit material are distributed in a random manner. Moreover, each transistor's τ_e remains constant over time. For these reasons, the τ_e has been regarded as the ''fingerprint''of a

[1]The QCL_{aka} source code and AVISPA verification program will be publicly released at https://github.com/congpu/QCLaka upon the acceptance of this manuscript.

transistor. At the server, with the τ_e of all selected transistors of the Prob-PUF circuit, the detrapping probability $P_d(t)$ at the end of pre-set timeframe can be computed according to $P_d(t) = [1 - exp(\frac{-t}{\tau_e})]$, where $exp(\cdot)$ is the exponential function. After excluding the random bits, the stable bits between the Prob-PUF output at the client and the computed value at the server can be compared for the purpose of authentication. In summary, the Prob-PUF offers two promising advantages: (i) Since the circuit transistors could generate either stable or random bits, they pose significant challenges when used for machine learning training by the adversary; and (ii) The server does not need to store a large number of CRPs, unlike traditional PUF-based approaches. Alternatively, the server only saves the τ_e of each selected transistor.

B. Lattice-based Cryptography

Lattice-based cryptography [11] that relies upon lattices has gained significant attention and development in recent years, especially in the context of post-quantum cryptography. In mathematics, lattices are composed of a consistent and repeating arrangement of points which are created by combining a set of basis vectors in higher-dimensional spaces. All lattice points further form a multi-dimensional grid which is leveraged to build cryptographic algorithms that are believed to be resistant to the Shor's groundbreaking quantum algorithm. In lattice-based cryptography, the foundation of security is the class of NP (nondeterministic polynomial time) problems such as the shortest vector (SVP), the closest vector (CVP), and the computational bilateral inhomogeneous small integer solution (CBi-ISIS) problems. The SVP and CVP problems require locating the shortest nonzero vector in a lattice and the closest lattice point to a given arbitrary point in space, respectively. Solving the SVP and CVP problems is widely recognized as extremely difficult, particularly due to their computational complexity in high-dimensional spaces, which provides the security foundation for lattice-based cryptographic mechanisms.

Given a basis $B = \{b_1, b_2, \ldots, b_n\}$ and $B \in \mathbb{R}^m$, an integer lattice Λ is defined as $\Lambda(B) = \sum_{i=1}^{n} a_i b_i$, where n is the dimension, m is the number of vectors, $\mathbb{R}^m$ is the m-dimensional Euclidean space, and $b_i \in B$ and are a set of linearly independent vectors. Further more, a module q lattice $\Lambda_q(M)$ is defined as $\Lambda_q(M) = \{v \in \mathbb{Z}^n \mid v = Mx \ (mod\ q), x \in \mathbb{Z}^m\}$, M is an $n \times m$ matrix with entries in $\mathbb{Z}_q$, x is an integer vector in $\mathbb{Z}^m$, and v is a vector in $\mathbb{Z}^n$ that is a linear combination of the columns of M modulo q.

SVP Problem Definition: Given a module q lattice $\Lambda_q(B)$, it is computationally challenging to find a significant shortest vector $v = \{v_1, v_2, \ldots, v_n\} \in \mathbb{Z}^n$ in $\Lambda_q(B)$. Mathematically, the SVP problem can be represented as

$$SVP(\Lambda_q(B)) = \min_{\forall v \in \Lambda_q(B)} ||v||$$

$$||v|| = \sqrt{v_1^2 + v_2^2 + \ldots + v_n^2}$$

CVP Problem Definition: Give a module q lattice $\Lambda_q(B)$ and a lattice point $t \in \mathbb{Z}^n$, it is computationally challenging to find the nearest lattice point $v \in \Lambda_q(B)$ to t. The CVP problem can be mathematically defined as

$$CVP(\Lambda_q(B), t) = \min_{\forall v \in \Lambda_q(B)} ||t - v||$$

CBi-ISIS Problem Definition: Given a square q-ray matrix $M \in \mathbb{Z}_q^{n \times n}$, $b \in \mathbb{Z}^+$, $e_1 = Mx$, $e_2 = y^T M \in \mathbb{Z}_q^n$, and $||x||, ||y|| \leq b$, it is computationally challenging to obtain $y^T Mx \ mod\ q \in \mathbb{Z}^n$ [19]. From the adversary $\mathcal{A}$'s perspective, the likelihood of restoring $y^T Mx \ mod\ q$ with M, b, e_1, and e_2 in hand, $Pr[\mathcal{A}(M, b, e_1, e_2) = y^T Mx]$, is nearly zero [20].

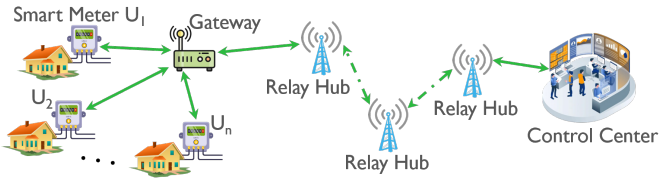

Fig. 1. System model.

IV. Security and Adversary Models & Security Requirements

A. System Model

According to the conceptual model provided by the National Institute of Standards and Technology (NIST) [21], the smart grid communication networks can be represented as a system model, as shown in Fig. 1. A smart meter U_i monitors real-time electricity usage data of appliances in the house and reports it to the local gateway intermittently. Following this, the local gateway compiles energy consumption data from all smart meters in the residential area and conveys it to the control center through relay hubs.

B. Adversary Model and Security Requirements

In the proposed adversary model, our primary emphasis is on how to ensure the security and privacy of real-time electricity usage data communication from smart meters to the local gateway. Thus, we assume that the control center, the relay hubs, and the local gateway are trusted entities. However, we consider an outside adversary $\mathcal{A}$, who possesses significant resources and computing capabilities (i.e., quantum) as indicated in the Canetti and Krawczyk (CK) adversary model [22], attempts to launch cyberattacks on the proposed system. According to the CK adversary model, the outside adversary $\mathcal{A}$ is interested in cracking, eavesdroping on, duplicating, corrupting, forging, or replaying the real-time electricity usage data to illegally access users' privacy. Additionally, because smart meters are typically installed outside the house, the adversary $\mathcal{A}$ might compromise them. Applying the CK adversary model requires us to establish the essential security features that the proposed QCL_{aka} protocol should uphold to counter the outside adversary $\mathcal{A}$'s abilities. The proposed QCL_{aka} protocol is regarded as secure within the CK adversary model if it prevents an outside adversary $\mathcal{A}$'s message cracking, sniffing, data duplication/corruption, spoofing, and replay attacks, as well as ensures perfect forward secrecy. It is worthy of mentioning that the adversary $\mathcal{A}$ might launch other cyberattacks against the

smart grid communication networks, however, they are outside the scope of this work.

V. The Proposed QCL_{aka} Protocol

In this section, we present the proposed QCL_{aka} protocol, which is composed of two parts: (i) system initialization and registration; and (ii) authentication and key agreement.

A. System Initialization and Registration

The i^{th} smart meter, U_i, goes through the following steps to register itself at the local gateway G_w.

1) The U_i chooses its real identifier UID_i, i.e., media access control address.
2) The U_i randomly selects k Prob-PUF transistors $\Gamma_i = \{\tau_{i.1}, \tau_{i.2}, \ldots, \tau_{i.k}\}$ along with their corresponding emission time constants $\Gamma_i^e = \{\tau_{i.1}^e, \tau_{i.2}^e, \ldots, \tau_{i.k}^e\}$. The U_i also determines the number of times the charging and sensing voltage pattern occurs Γ_i^{smp} and the size of sampling time window Γ_i^{ω}.
3) The U_i chooses a master random number r_i^* and calculates its initial pseudonym $PUID_i = H(UID_i \parallel r_i^*)$, where H:{0,1}^{m} is a hash function that outputs m-bit strings. It is worth mentioning that the U_i's initial (or called previous) pseudonym is used to hide its real identifier during the communication as well as verify its identification in the next communication session.
4) The U_i calculates its private key $pr_i = F\big(r_i^* \parallel P_i^{puf}(\Gamma_i)\big)$, where $F(\cdot)$ is a function that produces $pr_i \in \mathbb{Z}_q^n$ and $\|pr_i\| \leq b$. After that, the U_i computes its left and right public keys $\overleftarrow{pk_i} = pr_i^T \cdot M$ and $\overrightarrow{pk_i} = M \cdot pr_i$, respectively. Here, $M \in \mathbb{Z}_q^{n \times n}$ is a square q-ray matrix announced by the control center.
5) The U_i forms a message $msg_i^{t_{cur}^1} = \big\{UID_i, PUID_i, \{\Gamma_i, \Gamma_i^e, \Gamma_i^{\omega}\}, \overleftarrow{pk_i}, \overrightarrow{pk_i}\big\}$ and sends it to the G_w via a secure channel. Here, $t_{cur}^{...}$ is the current system time and it continuously elapses. Afterwards, the U_i deletes pr_i, $\overleftarrow{pk_i}$, $\overrightarrow{pk_i}$, and Γ_i^e for security reasons, but keeps Γ_i, Γ_i^{smp}, Γ_i^{ω}, and r_i^*.
6) After receiving $msg_i^{t_{cur}^1}$ from the U_i, the G_w stores $\big\{UID_i, PUID_i, \{\Gamma_i, \Gamma_i^e, \Gamma_i^{\omega}\}, \overleftarrow{pk_i}, \overrightarrow{pk_i}\big\}$ in the database, and replies to the U_i with a message $msg_w^{t_{cur}^2} = \{\overleftarrow{pk_w}, \overrightarrow{pk_w}\}$. If the UID_i is not linked to the utility company, the G_w will simply discard $msg_i^{t_{cur}^1}$. Here, the left and right public keys of the G_w is $\overleftarrow{pk_w} = pr_w^T \cdot M$ and $\overrightarrow{pk_w} = M \cdot pr_w$, respectively, where pr_w is the G_w's private key.

B. Authentication and Key Agreement

Through this phase, the U_i and the G_w mutually authenticate each other and negotiate a secret session key.

1) The U_i randomly generates a number $r_i^{t_{cur}^3}$ ($r_i^{t_{cur}^3} \in \mathbb{Z}_q^n$ and $\|r_i^{t_{cur}^3}\| \leq b$) and calculates its current pseudonym $PUID_i^{t_{cur}^3} = H(r_i^{t_{cur}^3} \parallel UID_i \parallel r_i^*)$. Here, $PUID_i^{t_{cur}^3}$ can also be calculated as $H(r_i^{t_{cur}^3} \parallel PUID_i)$, where $PUID_i = H(UID_i \parallel r_i^*)$.
2) The U_i recalculates its private key $pr_i = F\big(r_i^* \parallel P_i^{puf}(\Gamma_i)\big)$.
3) The U_i calculates $\gamma_{i.w} = \overleftarrow{pk_w} \cdot r_i^{t_{cur}^3}$. As $\overleftarrow{pk_w} = pr_w^T \cdot M$, $\gamma_{i.w} = pr_w^T \cdot M \cdot r_i^{t_{cur}^3}$. In addition, the U_i computes $\lambda_{i.w} = M \cdot r_i^{t_{cur}^3}$, $\mu_{i.w} = E(\gamma_{i.w}, PUID_i)$, $\nu_{i.w} = \overleftarrow{pk_w} \cdot pr_i$. Here, $E(key, data)$ is an encryption function that encrypts the *data* using the *key*, and $\nu_{i.w} = pr_w^T \cdot M \cdot pr_i$ because $\overleftarrow{pk_w} = pr_w^T \cdot M$.
4) The U_i calculates $\psi_{i.w} = H(\gamma_{i.w} \parallel PUID_i^{t_{cur}^3} \parallel t_{cur}^3 \parallel G_w \parallel \nu_{i.w})$.
5) The U_i forms a message $msg_i^{t_{cur}^3} = \{\lambda_{i.w}, \mu_{i.w}, \psi_{i.w}, t_{cur}^3\}$ and sends it to the G_w via a public channel.
6) After receiving $msg_i^{t_{cur}^3}$ from the U_i, the G_w first calculates $\gamma_{w.i} = pr_w^T \cdot \lambda_{i.w}$. Here, $\gamma_{w.i} = pr_w^T \cdot M \cdot r_i^{t_{cur}^3} = \gamma_{i.w}$. After that, the U_i recovers $PUID_i$ through $D(\gamma_{w.i}, \mu_{i.w})$, where $D(key, data)$ is a decryption function that decrypts the *data* using the *key*.
7) The G_w retrieves the U_i's $\big\{UID_i, PUID_i, \{\Gamma_i, \Gamma_i^e, \Gamma_i^{\omega}\}, \overleftarrow{pk_i}, \overrightarrow{pk_i}\big\}$ from the database, and computes $PUID_i^{t_{cur}^3} = H(r_i^{t_{cur}^3} \parallel PUID_i)$.
8) The G_w calculates $\nu_{w.i} = pr_w^T \cdot \overrightarrow{pk_i}$. Here, $\nu_{w.i} = pr_w^T \cdot M \cdot pr_i = \nu_{i.w}$.
9) The G_w computes $\psi_{w.i} = H(\gamma_{w.i} \parallel PUID_i^{t_{cur}^3} \parallel t_{cur}^3 \parallel G_w \parallel \nu_{w.i})$. If $\psi_{w.i} == \psi_{i.w}$, the identify of U_i is authenticated by the G_w. Otherwise, the G_w simply discards $msg_i^{t_{cur}^3}$.
10) The G_w selects a random number $r_w^{t_{cur}^4}$ ($r_w^{t_{cur}^4} \in \mathbb{Z}_q^n$ and $\|r_w^{t_{cur}}\| \leq b$) and calculates $\sigma_{w.i} = r_w^{t_{cur}^{4^T}} \cdot \lambda_{i.w}$. Here, $\sigma_{w.i}$ can also be calculated as $r_w^{t_{cur}^{4^T}} \cdot M \cdot r_i^{t_{cur}^3}$, where $\lambda_{i.w} = M \cdot r_i^{t_{cur}^3}$.
11) The G_w formalizes the secret session key $sk_{w.i} = H(\gamma_{w.i} \parallel \sigma_{w.i} \parallel \nu_{w.i} \parallel PUID_i^{t_{cur}^3} \parallel G_w)$.
12) The G_w computes $\eta_{w.i} = r_w^{t_{cur}^{4^T}} \cdot M$ and $\xi_{w.i} = H(G_w \parallel PUID_i^{t_{cur}^3} \parallel \nu_{w.i} \parallel t_{cur}^3 \parallel sk_{w.i})$.
13) The G_w forms a message $msg_w^{t_{cur}^4} = \{\eta_{w.i}, \xi_{w.i}\}$ and sends it to the U_i via a public channel.
14) After receiving $msg_w^{t_{cur}^4}$ from the G_w, the U_i calculates $\sigma_{i.w} = \eta_{w.i} \cdot r_i^{t_{cur}^3}$. Here, $\sigma_{i.w} = r_w^{t_{cur}^{4^T}} \cdot M \cdot r_i^{t_{cur}^3} = \sigma_{w.i}$.
15) The U_i formalizes the secret session key $sk_{i.w} = H(\gamma_{i.w} \parallel \sigma_{i.w} \parallel \nu_{i.w} \parallel PUID_i^{t_{cur}^3} \parallel G_w)$. Afterwards, the U_i checks whether $sk_{i.w} \stackrel{?}{=} sk_{w.i}$. If the verification succeeds, the U_i authenticates the G_w and accepts the secret session key $sk_{i.w}$. Otherwise, the U_i simply discards $msg_w^{t_{cur}^4}$.

As of now, the smart meter U_i and the local gateway G_w have fully authenticated each other and agreed on the secret session key $sk_{i.w}$ (or $sk_{w.i}$). Following this, they can securely communicate using the secret session key via insecure networks.

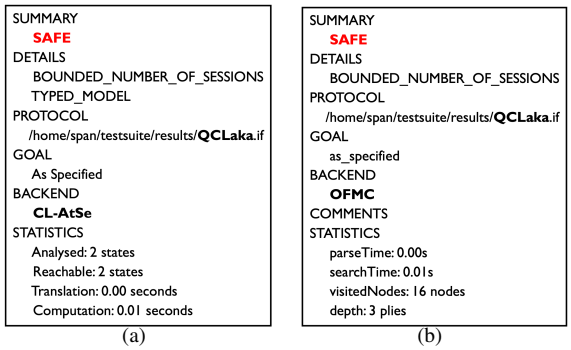

Fig. 2. Security verification results from AVISPA.

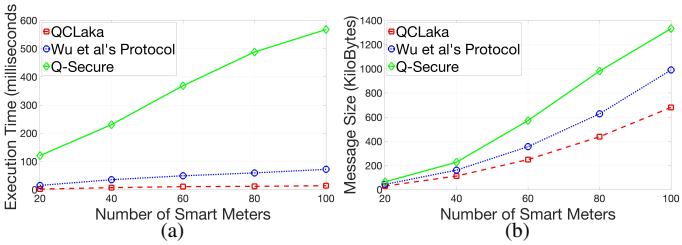

Fig. 3. The performance of execution time and communication overhead.

VI. Security and Performance Evaluation

A. Security Verification and Analysis

The security of the proposed QCL_{aka} protocol is rigorously validated using AVISPA [23], which is a tool to automatically verify the security of Internet cryptographic protocols and disclose security flaws and vulnerabilities. The protocols to be verified in the AVISPA framework need to be implemented in the HLPSL language, where three roles, such as the smart meter, the local gateway, and the CK attacker, are modeled. In the AVISPA program, Prob-PUF and lattice cryptographic operations are implemented using symbolical operations in the OFMC and CL-AtSe adversarial modules. In addition, the AVISPA program's security goals are defined as mutual authentication, session key secrecy, resistance to replay, protocol falsification, man-in-the-middle, and common cryptographic attacks. A fully-functional AVISPA environment is set up and configured within a virtual machine environment on Ubuntu 10.04. As shown in Fig. 2, the proposed QCL_{aka} protocol can be safely operating within the OFMC and CL-AtSe adversarial modules. Here, the OFMC module verifies session key confidentiality and forward secrecy through ephemeral keys, while the CL-AtSe module demonstrates QCL_{aka}'s resistance to cryptographic attacks targeting Prob-PUF and lattice cryptographic operations. In addition, the proposed QCL_{aka} protocol is not vulnerable to replay, protocol falsification, and man-in-the-middle attacks. In summary, the proposed QCL_{aka} protocol adheres to the security requirements of the CK adversary model as well as fulfills the requirements for cyberattack-safe hardness design, ensuring robust and secure communications for smart grids.

B. Performance Evaluation and Analysis

We evaluate the proposed QCL_{aka} protocol on an Apple MacBook Pro laptop (Apple M3 Pro chip; 11-Core CPU; 14-Core GPU; 18GB memory), and conduct a comprehensive

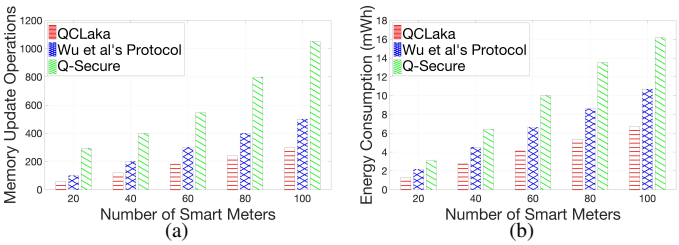

Fig. 4. The performance of memory update operations and energy consumption.

performance evaluation in terms of execution time, communication overhead, memory update operations, and energy consumption. In addition, the proposed QCL_{aka} protocol is compared with two recently proposed schemes, Wu et al.'s protocol [6] and Q-Secure [24], to show its performance efficiency and advantages. The QCL_{aka} source code and AVISPA verification program can be found at https://github.com/congpu/QCLaka.

First, in Fig. 3(a) we measure the execution time by varying the number of smart meters in the network. Overall, the proposed QCL_{aka} protocol consistently outperforms Wu et al.'s protocol and Q-Secure by requiring less time to execute the authentication algorithm. To be specific, with 100 smart meters, QCL_{aka} achieves an execution time of 14 milliseconds (ms), while Wu et al.'s protocol and Q-Secure requires 17 ms and 550 ms, respectively. This significant difference is attributed to the efficient use of Prob-PUF and lattice-based cryptographic operations in the proposed QCL_{aka} protocol, which reduce the number of computational operations required for authentication and key agreement. In contrast, Wu et al.'s protocol mainly relies on elliptic curve cryptography (ECC) which introduces additional overhead due to key generation and verification steps. Q-Secure, on the other hand, employs semi-quantum key distribution while providing quantum resistance, which adds considerable processing overhead due to the complexity of quantum operations. The proposed QCL_{aka} protocol also ensures scalability as it can maintain its performance efficiency while increasing the number of smart meters in the network.

Second, we present the result of the communication overhead for all three schemes in Fig. 3(b), showing that the proposed QCL_{aka} protocol incurs a lower communication overhead compared to the other two protocols. When the number of smart meters is set to 100, the sizes of the communication messages for QCL_{aka}, Wu et al.'s protocol, and Q-Secure are approximately 600 KB, 1000 KB, and 1400 KB, respectively. QCL_{aka} achieves a reduction in communication overhead because of optimizing the handshake process and eliminating redundant data transmissions. As the proposed QCL_{aka} protocol employs compact message formats, its communication overhead remains manageable even in high-density networks. In contrast, Wu et al.'s protocol requires multiple exchanges of cryptographic data between smart meters and the control center, leading to moderate communication overhead. Q-Secure, due to its reliance on semi-quantum key distribution, incurs the highest communication overhead. This is because it involves additional steps for quantum-secure authentication.

Third, we evaluate all three schemes' memory update operations (operations that read and write protocol variables) in Fig. 4(a). As shown in Fig. 4(a), the proposed QCL_{aka} significantly reduces the number of memory update operations compared to the other two protocols. Specifically, with 100 smart meters, QCL_{aka} protocol requires 300 memory operations, while Wu et al.'s protocol and Q-Secure need 500 and 1050, respectively. The smallest number of memory update operations is achieved through utilizing lightweight cryptographic primitives like Prob-PUF. However, Wu et al.'s protocol requires frequent memory updates due to the storage and retrieval of multiple key pairs and session keys, and Q-Secure requires extra storage and updates for quantum key distribution parameters.

Finally, we analyze the energy consumption of all three schemes in Fig. 4(b), where the proposed QCL_{aka} protocol is shown as the most energy-efficient authentication approach. For instance, with 20 smart meters, QCL_{aka} consumes only 1.312 mWh of energy, compared to 2.166 mWh for Wu et al.'s protocol and 3.067 mWh for Q-Secure. QCL_{aka}'s energy efficiency stems from its reduced communication overhead and the use of optimized cryptographic operations, which significantly reduce energy consumption. As the number of smart meters increases in the network, the energy consumption of all three schemes rises, but the energy efficiency of QCL_{aka} remains consistent. In comparison, Wu et al.'s protocol exhibits a higher energy consumption due to its reliance on ECC operations. While these ECC operations enhance security, they also introduce additional computational overhead, leading to increased energy demands. Q-Secure demonstrates the highest energy consumption among all three schemes. This is primarily due to its use of semi-quantum key distribution, which involves computationally intensive key exchanges.

VII. Conclusion

As the rise of electric vehicles continues in smart cities, the electricity demand grows. Smart grid networks are becoming ever more crucial to contemporary energy frameworks in the quantum era. However, the lack of secure and lightweight authenticated key agreement protocols poses unprecedented security and privacy challenges to power grids. In this paper, we unified lattice-based cryptography and probability physical unclonable function, and proposed a novel quantum-safe and cross-layer authentication and key agreement protocol to ensure the protection of data communication within smart grid networks. The security and performance evaluation results have confirmed that the proposed protocol provides enhanced security and privacy while also ensuring maximum performance efficiency and advantages.

References

[1] M. Khalid, "Smart grids and renewable energy systems: Perspectives and grid integration challenges," *Energy Strategy Reviews*, vol. 51, p. 101299, 2024.

[2] *Smart Grids: Optimize Energy Efficiency for a Sustainable Future*, Last accessed: Dec 3, 2024, https://www.lythouse.com/blog/smart-grid-all-you-need-to-know.

[3] B. Bera and B. Sikdar, "Securing Post-Quantum Communication for Smart Grid Applications," in *Proc. IEEE SmartGridComm*, 2024, pp. 555–561.

[4] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. Dong, and A. Martin, "Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2886–2927, 2019.

[5] Z. Liu, C. Hu, C. Ruan, P. Hu, M. Han, and J. Yu, "An Enhanced Authentication and Key Agreement Protocol for Smart Grid Communication," *IEEE Internet of Things Journal*, vol. 11, no. 12, pp. 22 413–22 428, 2024.

[6] Y. Wu, H. Guo, Y. Han, S. Li, and J. Liu, "A Security-Enhanced Authentication and Key Agreement Protocol in Smart Grid," *IEEE Transactions on Industrial Informatics*, vol. 20, no. 9, pp. 11 449–11 457, 2024.

[7] D. Kumari and K. Singh, "Lightweight Secure Authentication and Key Agreement Technique for Smart Grid," *Peer-to-Peer Networking and Applications*, vol. 17, no. 1, pp. 51–478, 2024.

[8] Y. Li, "An improved lightweight and privacy preserving authentication scheme for smart grid communication," *Journal of Systems Architecture*, vol. 152, p. 103176, 2024.

[9] G. Lian, Q. Sun, Y. Zou, Z. Gao, X. Wang, and T. Zheng, "Blockchain Identity Authentication-Based Secure Cooperative Communications for Smart Grid CPS," in *Proc. IEEE SmartIoT*, 2023, pp. 72–79.

[10] D. Monroe, "Post-Quantum Cryptography," *Communications of the ACM*, vol. 2366, no. 2, pp. 15–17, 2023.

[11] D. Micciancio and O. Regev, *Lattice-based Cryptography*. Springer, 2009.

[12] Z. Tu, Y. Xue, P. Ren, F. Hao, R. Wang, M. Li, J. Zhang, Z. Ji, and R. Huang, "A Probability-Based Strong Physical Unclonable Function With Strong Machine Learning Immunity," *IEEE Electron Device Letters*, vol. 43, no. 1, pp. 138–141, 2022.

[13] S. Yu and K. Park, "PUF-Based Robust and Anonymous Authentication and Key Establishment Scheme for V2G Networks," *IEEE Internet of Things Journal*, vol. 11, no. 9, pp. 15 450–15 464, 2024.

[14] S. Chai *et al.*, "Provably Secure and Lightweight Authentication Key Agreement Scheme for Smart Meters," *IEEE Transactions on Smart Grid*, vol. 14, no. 5, pp. 3816–3827, 2023.

[15] A. Badshah *et al.*, "LAKE-BSG: Lightweight authenticated key exchange scheme for blockchain-enabled smart grids," *Sustainable Energy Technologies and Assessments*, vol. 52, p. 102248, 2022.

[16] A. Shahidinejad and J. Abawajy, "Decentralized Lattice-Based Device-to-Device Authentication for the Edge-Enabled IoT," *IEEE Systems Journal*, vol. 17, no. 4, pp. 6623–6633, 2023.

[17] K. Fan *et al.*, "Fault Tolerant and Collusion-Resistant Lattice Based Multidimensional Privacy-Preserving Data Aggregation in Edge-Based Smart Grid," *IEEE Internet of Things Journal*, vol. 11, no. 6, pp. 9487–9504, 2024.

[18] K. Li, R. Shi, W. Guo, P. Wang, and B. Shao, "Dynamic Range Query Privacy-Preserving Scheme for Blockchain-Enhanced Smart Grid Based on Lattice," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 4, pp. 1652–1664, 2024.

[19] H. Ghaemi and D. Abbasinezhad-Mood, "Novel Blockchain-Integrated Quantum-Resilient Self-Certified Authentication Protocol for Cross-Industry Communications," *IEEE Transactions on Network Science and Engineering*, vol. 11, no. 5, pp. 4493–4502, 2024.

[20] D. Gupta, S. Ray, T. Singh, and M. Kumari, "Post-quantum lightweight identity-based two-party authenticated key exchange protocol for internet of vehicles with probable security," *Computer Communications*, vol. 181, pp. 69–79, 2022.

[21] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart Grid — The New and Improved Power Grid: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 944–980, 2011.

[22] Q. Do, B. Martini, and K. Choo, "The role of the adversary model in applied security research," *Computers & Security*, vol. 81, pp. 156–181, 2019.

[23] *Automated Validation of Internet Security Protocols and Applications*, https://people.inf.ethz.ch/basin/pubs/avispa05.pdf (Accessed: February 17, 2025).

[24] K. Prateek, M. Das, S. Surve, S. Maity, and R. Amin, "Q-Secure-P^2-SMA: Quantum-Secure Privacy-Preserving Smart Meter Authentication for Unbreakable Security in Smart Grid," *IEEE Transactions on Network and Service Management*, vol. 21, no. 5, pp. 5149–5163, 2024.