Batten Down the Hatches: Securing Neighborhood Area Networks of Smart Grid in the Quantum Era

Chi Cheng, *Member, IEEE*, Yue Qin, Rongxing Lu, *Senior Member, IEEE*,
Tao Jiang, *Fellow, IEEE*, and Tsuyoshi Takagi

***Abstract*—On account of the recent advances in quantum computers, it becomes pressing to consider quantum-safe authentication schemes for two-way communications in neighborhood area networks of smart grid, i.e., preventing possible attacks that the quantum computers could bring to the grid. In this paper, we take a further step toward this goal by integrating the lattice-based public-key encryption and key exchange techniques to provide mutual authentication between smart meters and the neighborhood gateway. Security analysis shows that our proposed scheme is secure under attacks from both quantum and conventional computers, including the recently introduced key reuse attacks. In addition, the proposed schemes can also achieve forward security, which guarantees that the secrets leaked in the current session will not result in the leakage of secrets in former sessions. Furthermore, the proposed scheme also gives prior consideration to the smart meters with limited computation capacity and puts as little burden on them as possible. Extensive performance analysis is also conducted, and the results demonstrate the efficiency of our proposed scheme, as well as the relatively low communication and storage costs.**

***Index Terms*—Smart grid, quantum-safe, authentication, lattice, public key encryption, key exchange.**

I. Introduction

In THE face of possibly doubled energy demand by 2050 and worldwide concerns on reducing greenhouse gas emissions [1], the development of smart grid technology has become a prior in many countries and areas. As an evolution of the current grid system, the vision of smart grid is to build a smarter, greener and more efficient grid system, integrating various kinds of renewable energy, strengthening system reliability, as well as giving customers more choices to save money and energy. The recent implementations of some pilot smart grid projects have witnessed the benefits of smart grids. For example, in Illinois, USA, a smart grid project has helped to avoid 7.6 million blackouts and saved 1.4 billion dollars with the help of more than 3 million smart meters and thousands of smart switching devices installed [2]. In Singapore, the under-developing advanced metering infrastructure (AMI) is used to give commercial and industrial consumers' electricity usage data every half hour, enabling them to buy electricity at a good price, and their long term outcome is to give all consumers including individuals the choices [3]. In the AMI demonstration projects lead by State Grid Corporation of China (SGCC), 70 million smart meters have been installed, together with 656 smart substations, aiming at providing a strong and smart grid. Nevertheless, the promising features of smart gird rely heavily on two-way communication between smart meters and electricity suppliers, posing challenges on how to achieve secure two-way communications between them [4], [5].

Recent years have witnessed a substantial amount of research on smart grid security issues [6] and privacy challenges [7]–[9], as well as countermeasures [10]. Liu and Li [11] show that an attacker could modify power grid data stealthily without having the full knowledge of the network information of a power grid. The work of [12] proposes a lightweight authentication scheme for smart grid communications based on the Diffie-Hellman (DH) key exchange and hash-based message authentication code. In [13] and [14], schemes on how to aggregate information in smart grid while preserving users' privacy have been proposed. Another privacy preserving scheme proposed by Abdallah and Shen [15] is based on predicting the upcoming electricity demand, and uses the NTRU cryptosystem including the NTRU encryption [16], and NTRU signature [17] to provide lightweight security.

Despite the above research efforts, most of the above works only take into consideration the challenges from conventional computers, what would happen if there are attacks from large-scale quantum computers? Most of our secure implementations today take the DH key exchange, RSA cryptosystem, or elliptic curve cryptosystems (ECC) as the basic building blocks, of which security are based on the difficulty of certain mathematical problems such as integer factorization, the discrete logarithm problem or its elliptic curve counterpart. In 1994, Shor showed that a quantum computer can exploit quantum mechanisms to efficiently solve these problems [18]. Ever since Shor's pioneer work, numerous works have been done on quantum computers and quantum algorithms, and the

Manuscript received July 29, 2018; revised November 19, 2018 and February 13, 2019; accepted March 4, 2019. Date of publication March 8, 2019; date of current version October 30, 2019. This work was supported in part by the National Natural Science Foundation of China under Grant 61672029. Paper no. TSG-01113-2018. *(Corresponding authors: Chi Cheng; Yue Qin.)*

C. Cheng and Y. Qin are with the Hubei Key Laboratory of Intelligent Geo-Information Processing, School of Computer Science, China University of Geosciences, Wuhan 430074, China (e-mail: chengchi@cug.edu.cn; qy52hz@cug.edu.cn).

R. Lu is with the Faculty of Computer Science, University of New Brunswick, Fredericton, NB E3B 5A3, Canada.

T. Jiang is with the School of Electronics Information and Communications, Huazhong University of Science and Technology, Wuhan 430074, China.

T. Takagi is with the Department of Mathematical Informatics, University of Tokyo, Tokyo 113-8656, Japan.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2019.2903836

accompanying question is, when will the large scale quantum computers come into existence?

After two decades, the answer has become more and more optimistic. As shown in the report of National Institute of Standards and Technology (NIST) [19], some scientists believe that the obstacles we need to overcome are only engineering problems [20]. Big companies like Google, IBM, and Microsoft, as well as some startups have invested heavily on quantum computers, competing to build a machine that can beat the conventional one [21]. Just recently, IBM announced that they succeeded in building a quantum computing processor managing 16 qubits, which is open to the public for free, and another 17-qubit processor for commercial use [22].

In a word, recent advances on quantum computers [23], [24] have demonstrated the urgency to consider quantum-safe protocols, that is, secure against both conventional computers and quantum computers. In December 2016, NIST has begun the process of standardizing quantum-safe (or post-quantum) public-key cryptographic algorithms, sparkling the research interests in this area.

However, as analyzed in [25] we cannot find drop-in replacements that fits all applications, and smart grid communications have their own requirements. Therefore, we need to prepare for a rainy day, considering quantum-safe authentication schemes for Neighborhood Area Networks (NANs) of smart grid. To achieve this goal, our first challenge is to find suitable building blocks in replacements of RSA, DH or ECC. Secondly, the proposed scheme using these blocks should be secure against all the known attacks launched by the conventional computers. At the same time, special attention should be paid to forward security and recently proposed key reuse attacks against lattice-based key exchange [26]. Last but not least, the proposed scheme could be integrated to meet requirements of the smart grid, satisfying the low computation and storage resources challenges on the smart meter side. Meanwhile, the efficiency on the neighborhood gateway (NG) is also important, since there may be many smart meters connected to one NG.

Inspired by the work of [12] and recent advances in lattice-based key exchange schemes [27], [28], in this paper we make a step forward towards securing communications in the smart grid even under attacks from quantum computers. Specifically, we propose a quantum-safe authentication scheme to secure the two-way communications between smart meters and the NG. The main idea is to integrate the lattice based public key encryption and key exchange schemes to provide a quantum-safe authentication scheme for smart grid, and the challenge comes from how to make sure that "the whole is less than the sum of its parts". The contributions of our proposed scheme include:

- To our best knowledge, we are the first to provide quantum-safe mutual authentication between smart meters and the NG in smart grid, and the security analysis shows that the proposed scheme is secure even under attacks from both conventional and quantum computers. Specially, we show that the proposed scheme is immune to the newly introduced key reuse attacks against the lattice-based key exchange.
- The proposed scheme can achieve forward security, which guarantees that the secrets leaked in the current session could not affect the security of communications happened in former sessions.
- The proposed scheme is efficient even compared with schemes using Elliptic Curve Digital Signature Algorithm (ECDSA) and Elliptic Curve Diffie Hellman (ECDH), since in our implementation it takes 5.35 ms on the smart meter side, 0.18 ms on the NG side, and 5.53 ms for the whole key establishment phase. In the key establishment phase we encrypt the hash values of the public messages instead of themselves, which can significantly reduce the communication and storage costs while maintaining security in the proposed scheme. Different from DH key exchange schemes, the proposed key exchange scheme is not exactly symmetric, so that we can assign less burden on the smart meter side, while do more work on the NG side. The implementations have also shown that our proposed schemes can do well on the smart meter side.

The rest of this paper is organized as follows: In Section II, we introduce the promising solutions to resist against attacks from quantum computers. Section III depicts smart grid and our security model, as well as our design goals. The notations and the underlying hard problem are given in Section IV. We then propose our authentication scheme for smart grid in Section V, and their performance analysis in Section VII. Finally, we make the conclusions in Section VIII.

II. Related Work

The impact of quantum computers is summarized in [19] and [29], showing that symmetric encryption schemes like AES are still secure even under attacks from quantum computers and only need to increase the key size, while the public key cryptographic schemes like RSA, ECDSA, and ECDH become insecure. To resist against attacks from quantum computers, promising cryptographic solutions include the lattice-based cryptosystems, hash-based signatures, code-based cryptosystems, and multivariate polynomial-based cryptosystems, as well as schemes based on the isogenies between supersingular elliptic curves.

Due to its strong security guarantees against even large-scale quantum computers, the lattice-based cryptosystems have attracted much attention. The learning with errors (LWE) problem over lattice was first introduced by Regev in [30]. As a more efficient variant of LWE, Lyubashevsky *et al.* introduced the Ring-LWE problem, showing that it is as hard as quantumly solving some worst-case problems in ideal lattices [31]. Since then, cryptographic designs based on Ring-LWE problem has found numerous applications [32].

Key exchange schemes similar to the work of Diffie and Hellman, but their security is based on the LWE and Ring-LWE problems, have drawn significant attention in recent years. Due to the fact that they can resist large-scale quantum computers while providing forward security, which guarantees that the adversary cannot get the previous sessions keys between two parties even if one of them leak the private

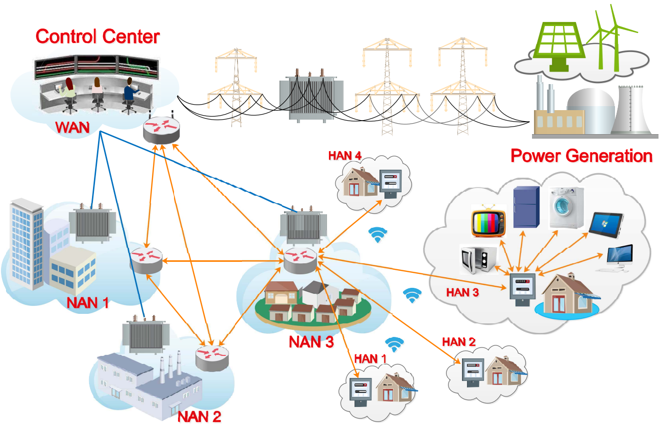


Fig. 1. The Architecture of Smart Grid.

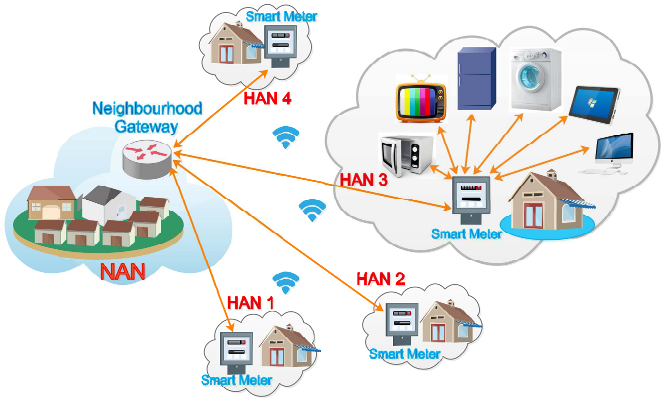


Fig. 2. The Architecture of Neighborhood Area Network.

key. Ding *et al.* [33] proposed a simple unauthenticated DH-like key exchange scheme, whose security is based on the LWE problem. Later, they proved the security of their scheme and expanded it to the Ring-LWE case. Other key exchange schemes based on the Ring-LWE problem include Fujioka *et al.* [34] and Peikert's key encapsulation mechanisms (KEMs) [35], and the work of Zhang *et al.* [36] which proposed a HMQV-like key exchange scheme and proved their security in the Bellare-Rogaway model.

Based on Peiker's work, Bos *et al.* integrated the Ring-LWE key mechanism into the Transport Layer Security (TLS) protocol in OpenSSL [27] to secure connections on the Internet. By using a more efficient reconciliation mechanism, Alkim *et al.* have proposed NewHope [28], significantly enhancing the security in [27] while reducing the communication and computation costs. Another elegant work is Frodo [37], which is based on LWE problem and believed to be practical. But all the above mentioned schemes either still use the conventional signature schemes like RSA and ECDSA for authentication or didn't provide concrete security for smart grid.

III. Models and Design Goals

A. System and Security Models

Generally, the grid consists of electricity and communication networks dealing with power generation, transmission, and distribution. As depicted in Fig. 1, a NAN is composed of several Home Area Networks (HANs). Then, a few NANs constitute a wide area network (WAN), which is connected to a power management center.

We can see from Fig. 2 that in a HAN, the smart meters collect the realtime usage data and then send it to the NG at periodic time interval. Generally, the time interval is set to be 15 minutes, or 5 minutes [38], [39]. The role of the NG is to first aggregate the data receiving from smart meters, and next forwarding them to the control center. A nice feature of smart grid is to enable two-way communications between electricity suppliers and users, which means that the NG will also receive feedbacks from the control center and then forward them to the smart meters.

In this paper, we focus on how to provide mutual authentication between smart meters and the NG under attacks from both quantum and conventional computers. We assume that the attackers have full access to the messages transmitted in the HAN and may try to attack the system with the help of quantum computers and conventional computers. It is worth noting that the quantum computers will not replace the conventional computers, but rather perform well on some tasks that are hard for conventional computers. For example, the attackers equipped with quantum computers can efficiently solve the integer factorization problem and the discrete logarithm problem as well as its elliptic curve counterpart using quantum algorithms like Shor's algorithm [19]. At the same time, the proposed scheme should also be secure under attacks from conventional computers. Generally, we classify these attacks into passive attacks and active attacks. In a passive attack, the attackers may try to get sensitive information from the messages transmitted in the HAN by means like eavesdropping, but do not modify contents of the messages. In an active attack, the attackers could modify the transmitted message, impersonate smart meters or NGs, or launch replay attacks by collecting previously received messages, and then try to replay these outdated messages to the NG or smart meters.

B. Design Goals

Our main security goal is to provide authentication for both NG and smart meters even there exist large-scale quantum computers. To be specific, our design goals are given as follows:

- The proposed scheme can provide mutual authentication even under attacks from both quantum and conventional computers. The NG and smart meters can authenticate each other, that is, the NG can make sure that the received electricity consumption reports are from the smart meters, while the smart meters can also guarantee that the feedbacks are sent from the NG. To meet this goal, the underlying hard problem of the proposed scheme should not be solved efficiently by quantum computers. Meanwhile, the proposed scheme should be secure under attacks from conventional computers including passive and active attacks.
- The proposed scheme can achieve forward security, which means that even in some cases the adversary can get

TABLE I
NOTATIONS

Notation	Definition
$\lfloor x \rceil$	The nearest integer to x
$E_k(m)$	Encryption of message m using key k
$\mathbb{Z}_q$	The integral domain modulo q
R_q	$\mathbb{Z}_q[x]/(x^n+1)$
χ	The discrete Gaussian distribution over R
ψ_k	The centered binomial distribution ψ_k of parameter k
Pub_{S_i}	The i-th smart meter's public key
Pub_{NG}	The Neighborhood Gateway's public key
ξ	The seed
G	A secure pseudorandom generator

secret information like keys used in the current session, he could not get secrets of previous sessions.

- The proposed scheme should be computationally efficient on the smart meter side, since generally the smart meters have limited computation and storage capacities. Meanwhile, due to the fact that there may be many smart meters connected to a NG, the relatively high computational efficiency should also be achieved on the NG side.

IV. Notations and the Underlying Hard Problems

In this section, we give the basic notations used in this paper, as well as the underlying hard problems, which play a central role in our security analysis.

A. Notations

First, we give definitions of some basic notations in Table I. For $x \in \mathbb{R}$, define $\lfloor x \rceil = \lfloor x + \frac{1}{2} \rfloor \in \mathbb{Z}$, here $\lfloor x \rfloor$ means the largest integer not exceeding x. Let q be an integer and $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$, which means all the elements in $\mathbb{Z}_q$ are of the form $\{0, 1, \dots, q-1\}$ and all the arithmetic operations are done modulo q. Define $R = \mathbb{Z}[x]/(x^n+1)$, where $n = 2^l$ and l is a positive integer. All the elements in R can be represented as $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ with each $a_i \in \mathbb{Z}$ for $i = 0, 1, \dots, n-1$, and all the operations are done modulo $x^n + 1$. We further define $R_q = \mathbb{Z}_q[x]/(x^n+1)$, where each element in R_q is of the form $g(x) = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}$ with each $b_i \in \mathbb{Z}_q$ for $i = 0, 1, \dots, n-1$.

In the following subsection, we introduce the LWE and Ring-LWE problems, which are essential for our design and security analysis, and regarded as securing against attacks even from quantum computers.

B. The LWE and Ring-LWE Problems

The LWE problem is to find $\mathbf{s}$ from $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$, where $\mathbf{A}$ is a matrix with elements selected from $\mathbb{Z}_q$, and $\mathbf{s}$ and $\mathbf{e}$ are all vectors with elements selected according to some distributions over $\mathbb{Z}_q$. The Ring-LWE problem is a variant of the LWE problem, which base the security on solving some worst-case problems in ideal lattices.

To introduce the Ring-LWE problem, we denote χ the discrete Gaussian distribution over R, then $x \leftarrow \chi$ means sampling x uniformly at random from R in accordance with χ. Please refer to [27] for more details on how to sample from a discrete Gaussian distribution over R.

Let $\mathcal{G}$ be an algorithm with security parameter n as its inputs, which outputs (R, R_q, q, n, χ) as defined above. The decision Ring-LWE problem is to distinguish sample pairs $(\mathbf{a}_i, \mathbf{b}_i = \mathbf{a}_i\mathbf{s} + \mathbf{e}_i)$ from samples randomly selected from $R_q \times R_q$, here $\mathbf{a}_i \leftarrow R_q$, $\mathbf{s}, \mathbf{e}_i \leftarrow \chi$. More formally, we have the following.

Definition 1: The decision Ring-LWE problem is hard relative to $\mathcal{G}$, if for any probabilistic polynomial-time (PPT) adversary $\mathcal{A}$, the advantage

$$\begin{aligned} |\Pr\big[&\mathcal{A}\big(R, R_q, q, n, \chi, \mathbf{a}_i, \mathbf{b}_i\big) = 1\big] \\ &-\Pr\big[\mathcal{A}\big(R, R_q, q, n, \chi, \mathbf{x}_i, \mathbf{y}_i\big) = 1\big]| \end{aligned}$$

is negligible. Here in each case the probability is taken over the game where $\mathcal{G}(n)$ outputs (R, R_q, q, n, χ), $\mathbf{a}_i \leftarrow R_q$, $\mathbf{s}, \mathbf{e}_i \leftarrow \chi$, and each pair $(\mathbf{x}_i, \mathbf{y}_i)$ is uniform random in $R_q \times R_q$.

V. The Quantum-Safe Authenticated Key Exchange Schemes for Smart Grid

In this section, we propose a lightweight authenticated key exchange scheme for smart grid. The proposed scheme can be divided into Initialization Phase, Key Establishment Phase, and Data Transmission Phase.

A. Initialization Phase

This phase aims at issuing NG and i-th smart meter S_i the needed information for the key establishment phase.

1) The NG chooses the Ring-LWE parameters q, n, χ such that the Ring-LWE problem is hard. For a quantum-resistant public key encryption scheme, for example the NTRU encryption scheme [16], NG generates its public and private key pairs $(\text{PU}_\text{NG}, \text{PR}_\text{NG})$. Then, NG publishes these Ring-LWE parameters q, n, χ and its public key PU_NG.
2) S_i also generates its public and private key pairs $\text{PU}_{\text{S}_\text{i}}$ and $\text{PR}_{\text{S}_\text{i}}$. And then it selects a random number Nonce_1 and its identifier $\text{ID}_{\text{S}_\text{i}}$. When registering to NG for the first time, S_i sends its public key $\text{PU}_{\text{S}_\text{i}}$ and $\text{ID}_{\text{S}_\text{i}}$ to NG via a secure channel. The NG checks whether $\text{ID}_{\text{S}_\text{i}}$ is a new identifier or not, if yes, $\text{ID}_{\text{S}_\text{i}}$ will be stored in the registration table.

After the initialization phase, S_i and NG know each other's public keys and NG maintains S_i's identifier $\text{ID}_{\text{S}_\text{i}}$. In the following phase, the smart meter S_i and NG try to share a key in a secure and authenticated way.

B. Key Establishment Phase

In this phase, we assume that $h_1()$, $h_2()$, and $h_3()$ are three cryptographically secure one-way hash functions, Nonce_1 and Nonce_2 are two nonces, and $\text{ID}_{\text{S}_\text{i}}$ and ID_NG are the identifiers of S_i and NG, respectively. We also assume that there exist a secure Pseudorandom generator (PRG) $G : \mathcal{K}_G \rightarrow \mathbb{Z}_q^n$.

The details of the Key Establishment Phase are as follows:

1) First, S_i randomly selects a seed ξ, which is then used to generate $\mathbf{a} = \mathrm{G}(\xi)$. Next, S_i chooses random parameters $\mathbf{s}$, $\mathbf{e}$ from χ and computes $\mathbf{b} = \mathbf{a} \cdot \mathbf{s} + \mathbf{e}$. After calculating $h_1(\mathrm{Nonce}_1, \mathrm{ID}_{\mathrm{S_i}}, \mathbf{b}, \xi)$, S_i uses NG's public key to encrypt $(\mathrm{Nonce}_1, \mathrm{ID}_{\mathrm{S_i}}, h_1(\mathrm{Nonce}_1, \mathrm{ID}_{\mathrm{S_i}}, \mathbf{b}, \xi))$, which is then sent to NG together with $\mathbf{b}, \xi$.

$$S_i \rightarrow NG : \mathbf{b},\ \ \xi, E_{PU_{\mathrm{NG}}}\big(\mathrm{Nonce}_1, \mathrm{ID}_{\mathrm{S_i}},\\ h_1\big(\mathrm{Nonce}_1, \mathrm{ID}_{\mathrm{S_i}}, \mathbf{b}, \xi\big)\big)$$

2) After recovering $(\mathrm{Nonce}_1, \mathrm{ID}_{\mathrm{S_i}}, h_1(\mathrm{Nonce}_1, \mathrm{ID}_{\mathrm{S_i}}, \mathbf{b}, \xi))$ with its private key, NG first makes sure that $\mathrm{ID}_{\mathrm{S_i}}$ is stored in its registration table and Nonce_1 is fresh. If so, NG calculates $h_1(\mathrm{Nonce}_1, \mathrm{ID}_{\mathrm{S_i}}, \mathbf{b}, \xi)$, and compares it with the decrypted $h_1(\mathrm{Nonce}_1, \mathrm{ID}_{\mathrm{S_i}}, \mathbf{b}, \xi)$. If this two hash values match, NG generates $\mathbf{a} = \mathrm{G}(\xi)$, then it chooses random parameters $\mathbf{s}', \mathbf{e}', \mathbf{e}''$ from χ to compute $\mathbf{b}' = \mathbf{a} \cdot \mathbf{s}' + \mathbf{e}'$. Next, NG will choose a random string $\mathbf{v} \leftarrow \{0, 1\}^{\frac{n}{4}}$ of length $\frac{n}{4}$ and computes $\mathbf{v}' = h_2(\mathbf{v})$. After that, NG encodes $\mathbf{v}'$ to get $\mathbf{k} = \mathrm{Encode}(\mathbf{v}')$. Here, the Encode function maps each bit of $\mathbf{v}'$ into four bits in $\mathbf{k}$. Specifically, if we set $\mathbf{v}' = (v'[1], v'[2], \ldots, v'[\frac{n}{4}])$, then $\mathbf{k} = (\mathbf{k}_1, \mathbf{k}_2, \mathbf{k}_3, \mathbf{k}_4)$, where each vector $\mathbf{k}_i$ is the same: $\mathbf{k}_i = (v'[1] \cdot \frac{q-1}{2}, v'[2] \cdot \frac{q-1}{2}, \ldots, v'[\frac{n}{4}] \cdot \frac{q-1}{2})$. Then, NG computes $\mathbf{c}' = \mathbf{b} \cdot \mathbf{s}' + \mathbf{e}'' + \mathbf{k}$, and $\bar{\mathbf{c}} = \mathrm{Compression}(\mathbf{c})$. We adopt the Compression function proposed in [41], in which the $\mathrm{Compression}(\mathbf{c})$ is defined as $\mathbf{c} \rightarrow \bar{\mathbf{c}} : \bar{c}[i] = \lceil (c[i] \cdot 8)/q \rfloor \bmod 8$ for $i \in [0, n-1]$.
Subsequently, NG will choose another nonce Nonce_2, and get $h_1(\mathrm{Nonce}_1,\ \mathrm{Nonce}_2,\ \mathrm{ID}_{\mathrm{NG}},\ \mathbf{b}',\ \bar{\mathbf{c}})$. Finally, NG encrypts Nonce_1, Nonce_2, $\mathrm{ID}_{\mathrm{NG}}$, $h_1(\mathrm{Nonce}_1,\ \mathrm{Nonce}_2,$ $\mathrm{ID}_{\mathrm{NG}},\ \mathbf{b}',\ \bar{\mathbf{c}})$ with S_i's public key and sends them back to S_i together with $\mathbf{b}', \bar{\mathbf{c}}$.

$$NG \rightarrow S_i : \mathbf{b}',\ \ \bar{\mathbf{c}},\ \ E_{PU_{\mathrm{S_i}}}\big(\mathrm{Nonce}_1, \mathrm{Nonce}_2,\\ \mathrm{ID}_{\mathrm{NG}}, h_1\big(\mathrm{Nonce}_1, \mathrm{Nonce}_2, \mathrm{ID}_{\mathrm{NG}}, \mathbf{b}', \bar{\mathbf{c}}\big)\big)$$

3) After receiving NG's responses, S_i decrypts the encrypted messages with its private key, and calculates $h_1(\mathrm{Nonce}_1, \mathrm{Nonce}_2, \mathrm{ID}_{\mathrm{NG}}, \mathbf{b}', \bar{\mathbf{c}})$. If the generated hash value is the same as the received $h_1(\mathrm{Nonce}_1, \mathrm{Nonce}_2, \mathrm{ID}_{\mathrm{NG}}, \mathbf{b}', \bar{\mathbf{c}})$, NG is authenticated by S_i. Then, S_i can compute $\mathbf{c}' = \mathrm{Decompression}(\bar{\mathbf{c}})$. Here the Decompression function is the inverse of the Compression function. Namely, for $i \in [0, n-1]$, we have $c'[i] = \lceil (\bar{c}[i] \cdot q)/8 \rfloor$. Thereafter, S_i will calculate $\mathbf{k}' = \mathbf{c}' - \mathbf{b}' \cdot \mathbf{s}$, and get $\mu = \mathrm{Decode}(\mathbf{k})$. The function $\mathrm{Decode}(\mathbf{k}) \rightarrow \mu$ can extract one bit from four bits. To be specific, at first we compute the sum of these four bits in $\mathbf{k}$ as $s = k_1[i] + k_2[i] + k_3[i] + k_4[i]$, $i \in [0, \frac{n}{4}]$. After that, we determine whether this sum s is greater than q, if so, we will set $\mu[i] = 0$ and $\mu[i] = 1$ otherwise. Next, the secret string is calculated as $K_{\mathrm{S_i}} = h_2(\mu, \mathrm{Nonce}_1, \mathrm{Nonce}_2)$. Finally, S_i sends the encrypted Nonce_2 and the hash values back to NG as follows.

$$S_i \rightarrow NG : E_{PU_{\mathrm{NG}}}\ \ \big(\mathrm{Nonce}_2, h_1\big(\mathrm{Nonce}_1, \mathrm{Nonce}_2, \mathrm{ID}_{\mathrm{NG}},\\ \mathbf{b}', \bar{\mathbf{c}}\big), h_3\big(K_{\mathrm{S_i}}\big)\big)$$

4) Once the correct hash value is received by the NG, it can also make sure that S_i is the valid entity. Then NG can compute the secret string $K_{\mathrm{NG}} = h_2(v', \mathrm{Nonce}_1, \mathrm{Nonce}_2)$ and $h_3(K_{\mathrm{NG}})$. Next, the latter is compared with the received $h_3(K_{\mathrm{S_i}})$ to make sure the two parties share the same key.

At the end of this phase, NG and S_i can share the same session key $K = K_{\mathrm{NG}} = K_{\mathrm{S_i}}$.

C. Data Transmission Phase

With the established key K, S_i and NG can launch an authenticated and quantum-safe two-way communication using AES-256 GCM authenticated encryption and SHA-512. Note that we can also regard the established key K as the long-term key, and then employ techniques in [38] and [39] to launch a more lightweight secure two-way communication.

In the proposed scheme, we choose the NTRU encryption algorithm as our basic building block. First as a design with concert security, the NTRU encryption is widely believed to thwart all known attacks including those from quantum computers. At the same time, other candidates for authentication still need more evaluations. On December 2008, the NTRU encryption scheme is standardized by IEEE as IEEE Std 1363.1-2008 [40]. Moreover, the elegant design of NTRU encryption makes it efficient even on resource-limited devices like smart meters. Here another question may arise, why not use the public key encryption scheme to transmit the shared key directly? The reason is, the proposed scheme can achieve forward security, which guarantees that even in case the private key is leaked in some session, the attacker cannot recover the keys in the previous sessions. Since in smart grid, the smart meters are resource-constrained and vulnerable to side channel attacks, the forward security is very important.

VI. Security Analysis

In this section, we analyze the security of the proposed scheme. First, we prove that the Key Establishment Phase is secure under passive attacks.

A. Security Under Passive Attacks

To analyze security of the key exchange scheme under passive attacks, we first give the following security game KE-GAME, which is played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$ with security parameter n:

1) Both the challenger $\mathcal{C}$ and adversary $\mathcal{A}$ run the key exchange scheme with security parameter t, resulting in a shared key K (Due to the correctness of the key exchange scheme, we assume that the two parties output the same key), and all the messages transmitted by the two parties during the execution of the scheme.

2) The challenger $\mathcal{C}$ uniformly choose a bit $\omega \in \{0,1\}$, if $\omega = 0$, $\mathcal{C}$ let $K_0 = K$; else if $\omega = 1$, $\mathcal{C}$ chooses $K_1 \in \{0,1\}^n$ randomly.
3) Upon receiving K_ω, $\mathcal{A}$ needs to output a bit ω'. If $\omega' = \omega$, we say $\mathcal{A}$ wins; otherwise $\mathcal{A}$ loses. When $\mathcal{A}$ succeeds, we denote $\text{KE-GAME}^{eav}_{n,q,\chi}(n) = 1$.

Generally, we say a key exchange protocol is secure under passive attacks, if for any probabilistic polynomial-time (PPT) adversary $\mathcal{A}$, it cannot distinguish the real shared key to a randomly selected bit string even if $\mathcal{A}$ gets the transcripts.

Definition 2: The proposed key exchange scheme is secure in the presence of eavesdropping attacks if for any PPT adversary $\mathcal{A}$, the probability that $\mathcal{A}$ can win the game KE-GAME with security parameter n is negligible. That is, the advantage

$$\text{Adv}(\mathcal{A}) = \Pr\Big[\text{KE-GAME}^{eav}_{n,q,\chi}(n) = 1\Big] - \frac{1}{2}$$

is negligible.

To prove this theorem, we introduce the following DDH-like problem given in [27].

Lemma 1: The DDH-like problem is hard with respect to $\mathcal{G}$, if for any PPT adversary $\mathcal{A}$, the advantage

$$|\Pr[\mathcal{A}(\mathbf{a},\mathbf{b},\mathbf{b}',\bar{\mathbf{c}},K_1) = 1] - \Pr[\mathcal{A}(\mathbf{a},\mathbf{b},\mathbf{b}',\bar{\mathbf{c}},K_0) = 1]|$$

is negligible. Here in each case the probability is taken over the game where $\mathcal{G}$ outputs (R, R_q, q, n, χ), and $(\mathbf{a},\mathbf{b},\mathbf{b}',\bar{\mathbf{c}})$ represents the transcript of the protocol execution, K_0 is the actual key computed by the two parties, while K_1 is a random value selected from $\{0,1\}^n$.

Theorem 1: If the decision Ring-LWE problem is hard with $\mathcal{G}$, then the proposed key exchange scheme is secure under passive attacks.

Proof: We do not need the adversary to distinguish the shared session key, instead we want it to distinguish $\text{K}_{\text{S}_\text{i}}$ (or K_{NG}) from uniformly random in R_q.

Since Pr[ω= 0] = Pr[ω= 1] = $\frac{1}{2}$, we have

$$\begin{aligned}\Pr\Big[&\text{KE-GAME}^{eav}_{n,q,\chi}(n) = 1\Big]\\ &= \frac{1}{2}Pr\Big[\text{KE-GAME}^{eav}_{n,q,\chi}(n) = 1|\omega = 1\Big]\\ &\quad + \frac{1}{2}Pr\Big[\text{KE-GAME}^{eav}_{n,q,\chi}(n) = 1|\omega = 0\Big].\end{aligned}$$

In security game $\text{KE-GAME}^{eav}_{n,q,\chi}(n)$, the adversary $\mathcal{A}$ receives $(\mathbf{a},\mathbf{b},\mathbf{b}',\bar{\mathbf{c}},k_\omega)$, where $(\mathbf{a},\mathbf{b},\mathbf{b}',\bar{\mathbf{c}})$ represents the transcript of the protocol execution, and k_ω is either the actual key computed by the parties (if ω = 0) or a random value from $\{0,1\}^n$ (if $\omega = 1$). Distinguishing between these two cases is exactly equivalent to solving the decision Ring-LWE problem. That is

$$\begin{aligned}\Pr\Big[&\text{KE-GAME}^{eav}_{n,q,\chi}(n) = 1\Big]\\ &= \frac{1}{2}\Pr\Big[\text{KE-GAME}^{eav}_{n,q,\chi}(n) = 1|\omega = 1\Big]\\ &\quad + \frac{1}{2}\Pr\Big[\text{KE-GAME}^{eav}_{n,q,\chi}(n) = 1|\omega = 0\Big]\\ &= \frac{1}{2}\Pr[\mathcal{A}(\mathbf{a},\mathbf{b},\mathbf{b}',\bar{\mathbf{c}},K_1) = 1]\\ &\quad + \frac{1}{2}(1 - Pr[\mathcal{A}(\mathbf{a},\mathbf{b},\mathbf{b}',\bar{\mathbf{c}},K_0) = 1])\\ &= \frac{1}{2} + \frac{1}{2}\Pr[\mathcal{A}(\mathbf{a},\mathbf{b},\mathbf{b}',\bar{\mathbf{c}},K_1) = 1]\\ &\quad - \frac{1}{2}\Pr[\mathcal{A}(\mathbf{a},\mathbf{b},\mathbf{b}',\bar{\mathbf{c}},K_0) = 1]\\ &\le \frac{1}{2} + \frac{1}{2}|\Pr[\mathcal{A}(\mathbf{a},\mathbf{b},\mathbf{b}',\bar{\mathbf{c}},K_1) = 1]\\ &\qquad - \Pr[\mathcal{A}(\mathbf{a},\mathbf{b},\mathbf{b}',\bar{\mathbf{c}},K_0) = 1]|\end{aligned}$$

Then, it follows that

$$\begin{aligned}\Pr\Big[&\text{KE-GAME}^{eav}_{n,q,\chi}(n) = 1\Big] - \frac{1}{2}\\ &\le \frac{1}{2}|\Pr[\mathcal{A}(\mathbf{a},\mathbf{b},\mathbf{b}',\bar{\mathbf{c}},K_1) = 1]\\ &\qquad - Pr[\mathcal{A}(\mathbf{a},\mathbf{b},\mathbf{b}',\bar{\mathbf{c}},K_0) = 1]|\end{aligned}$$

Therefore, according to Lemma 1, the probability

$$\Pr\Big[\text{KE-GAME}^{eav}_{n,q,\chi}(n) = 1\Big] - \frac{1}{2}$$

is negligible, which completes the proof. ■

B. Mutual Authentication

In step 1) of the Key Establishment Phase, since Nonce_1, $\text{ID}_{\text{S}_\text{i}}$, and $h_1(\text{Nonce}_1, \text{ID}_{\text{S}_\text{i}}, \mathbf{b}, \xi)$ are encrypted with NG's public key, only NG can recover them with its private key if the adopted public key encryption scheme is secure. Furthermore, the hash value $h_1(\text{Nonce}_1, \text{ID}_{\text{S}_\text{i}}, \mathbf{b}, \xi)$ can help NG verify whether the received $\mathbf{b}, \xi$ is correct. In Step 3 if S_i recovers the correct Nonce_2, ID_{NG}, then it can compute the hash value of $(\text{Nonce}_1, \text{Nonce}_2, \text{ID}_{\text{NG}}, \mathbf{b}', \bar{\mathbf{c}})$ with $\mathbf{b}'$, $\bar{\mathbf{c}}$ and compared it with the received $h_1(\text{Nonce}_1, \text{Nonce}_2, \text{ID}_{\text{NG}}, \mathbf{b}', \bar{\mathbf{c}})$. If the two hash values are the same, then S_i makes sure that $\mathbf{b}', \bar{\mathbf{c}}$ are correct and the messages are sent from NG.

Similarly, since $h_1(\text{Nonce}_1, \text{Nonce}_2, \text{ID}_{\text{NG}}, \mathbf{b}', \bar{\mathbf{c}})$ is encrypted with S_i's public key, only S_i can decrypt it and send it back to NG. Thus in Step 4) NG can also authenticate S_i if it can receive the correct Nonce_2, $h_1(\text{Nonce}_1, \text{Nonce}_2, \text{ID}_{\text{NG}}, \mathbf{b}', \bar{\mathbf{c}})$.

The proposed scheme achieves forward security since in the Key Establishment Phase the shared keys are generated randomly. Meanwhile, the key reuse attacks also cannot apply to the proposed scheme, due to the fact that the private information is randomly selected to generate the corresponding public key information in the Key Establishment Phase. In addition, the employment of nonces help resisting against the replay attacks. Therefore, the proposed scheme can provide mutual authentication between S_i and NG, and then establish an authenticated secure channel for the following data transmission.

VII. Performance Analysis

In this section, we give the performance analysis of the proposed authenticated communication scheme for smart grid. The proposed scheme performs computations in the ring $R_q =$

TABLE II
AVERAGE RUNNING TIME IN MILLISECONDS

Schemes	Authentication Time (ms)		Total Time (ms)
	Smart Meter	NG	
Proposed Scheme	5.35	0.18	5.53
Fouda et al's	289.19	3.79	292.98
ECDSA+ECDH	24.25	1.94	26.19

$\mathbb{Z}_q[x]/(x^n + 1)$, with the dimension $n = 1024$, the modulus $q = 12,289$. It is worth noting that in the following we use the centered binomial distribution ψ_k instead of the discrete Gaussian distribution in the Decision Ring-LWE problem to obtain the LWE secrets and the errors, since it is shown in [28] that it can provide a faster sampling rate and resist against timing attacks, while achieving even better security. For the parameter $k = 16$, the standard deviation $\sigma = \sqrt{8} \approx 2.83$, and it is shown that these parameters offer at least post-quantum security of 206 bits, and classical security of 229 bits.

We choose the NTRU encryption as the required public key encryption algorithm. There have been several other candidates for the quantum-safe public key encryption, such as the Ring-LWE encryption [31], but their concrete security is still under evaluation, and we leave their performance to future work. We choose the security set EES743EP1 to achieve at least 128-bit security against both classical and quantum attacks [40]. We also use SHAKE-128, which is an extendable-output function (XOF), and SHA-512 as the required hash function. The two both belong to the SHA-3 family with at least 128-bit post-quantum security [42].

Fouda *et al.* [12] employ RSA encryption and DH key exchange schemes to establish mutual authentication between smart meters and the NG. For comparisons in efficiency, we also implement Fouda *et al.*'s scheme by adopting 256-bit Diffie-Hellman key exchange and 3072-bit RSA encryption schemes, which can achieve 128-bit classical security. We then use the ECDSA and ECDH to implement an authentication key exchange scheme, which is widely deployed on the Internet of Things (IoT) devices. In the implementation, we use nistp256 curves for elliptic curve operations, aiming at achieving the 128-bit classical security.

A. Computation Efficiency

We implement the above schemes and evaluate their performance as shown in Table II. Our implementation is done on a Raspberry Pi 3 and a MacBook Air. The Raspberry Pi 3 is used to simulate the smart meter, which has a 64-bit ARMv8 quad core Cortex A53 processor at 1.2 GHz and a 1 GB RAM. The MacBook is equipped with an Intel Core i7 processor at 2.7 GHz and an 8 GB RAM, simulating the NG. The Raspberry Pi 3 is connected to the MacBook using IEEE 802.11ac at about 27 Mbps, and each scheme is executed 10,000 times and averaged.

The implementations of these schemes are based on liboqs, which is an open source C library for quantum-safe cryptographic algorithms and is included in the Open Quantum Safe project [43]. OQS supports Intel kernel CPU, but Raspberry Pi's CPU is ARMv8. Thus, we tailor it to make it work on Raspberry Pi. We summarize our result of the three schemes in Table II, in which the total time refer to the time spent in the Key Establishment Phase. To be specific, we also list the operating time spent on the smart meter and the NG, respectively.

TABLE III
AVERAGE RUNNING TIME IN MILLISECONDS - WITH ROLES CHANGED

Schemes	Authentication Time (ms)		Total Time (ms)
	Smart Meter	NG	
Proposed Scheme	5.63	0.18	5.81

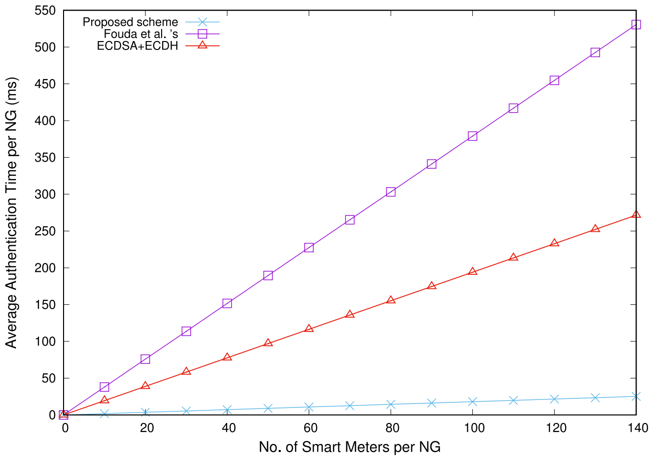


Fig. 3. Average Authentication Time per NG with Increasing Number of Smart Meters.

We can see from Table II that, the proposed scheme is roughly 54 times faster than the scheme using RSA and DH on the smart meter side, 21 times faster on NG, and almost 53 times faster for the whole key establishment phase. On the smart meter side, the proposed scheme is 4.5 times faster than the scheme using ECDSA and ECDH, and on NG the proposed scheme is roughly 10 times faster. For the whole key establishment phase, the proposed scheme is nearly 5 times faster.

Moreover, in our proposed scheme the roles the smart meter and neighborhood gateway play are not exactly symmetric, meaning that we can assign less burden on the smart meter side. In Table III, we have shown their performance if we exchange the roles of smart meter and neighborhood gateway. We can conclude from Table III that the smart meter becomes 1.05 times slower in the proposed scheme if their roles has been changed. Since in practice, the smart meters may be equipped with lower computational capacity, our design can perform better.

In Fig. 3, we show the case when one NG is in charge of a number of smart meters. Specifically, we consider the case when the number of smart meters increases from 1 to 140. We can see that as the number of smart meter increases, the average authentication time increase gradually compared with that in the Fouda *et al.*'s scheme and the case using ECDSA and ECDH. Therefore, the proposed scheme shows good potential in managing the case with more smart meters.

TABLE IV
COMMUNICATION AND STORAGE COSTS

Schemes	Communication Costs (Bytes)	Storage Costs (Bytes)	
		Smart Meter	NG
Proposed Scheme	6,938	12,383	7,391
Fouda et al's	1,216	2,370	2,434
ECDSA+ECDH	230	743	793

B. Communication and Storage Costs

Table IV surveys the communication overhead and storage cost of the above mentioned schemes. In the following we give a detailed analysis of the communication overhead and storage cost of the proposed scheme.

The communication cost in the proposed scheme includes the $\mathbf{b}$, ξ, $E_{PU_{\mathrm{NG}}}(\mathrm{Nonce}_1, \mathrm{ID}_{\mathrm{S_i}}, h_1(\mathrm{Nonce}_1, \mathrm{ID}_{\mathrm{S_i}}, \mathbf{b}, \xi))$ in step 1) of the Key Establishment Phase, $\mathbf{b}'$, $\bar{\mathbf{c}}$, $E_{PU_{S_i}}$ $(\mathrm{Nonce}_1, \mathrm{Nonce}_2, \mathrm{ID}_{\mathrm{NG}}, h_1(\mathrm{Nonce}_1, \mathrm{Nonce}_2, \mathrm{ID}_{\mathrm{NG}}, \mathbf{b}', \bar{\mathbf{c}}))$ in step 2), and $E_{PU_{NG}}(\mathrm{Nonce}_2, h_1(\mathrm{Nonce}_1, \mathrm{Nonce}_2, \mathrm{ID}_{\mathrm{NG}}, \mathbf{b}', \bar{\mathbf{c}}))$ in step 3).

In the proposed scheme, we use the NTRU public key encryption algorithm to encrypt and decrypt the data, and SHA-512 is chosen as the secure hash function. The NTRU algorithm can encrypt 106 bytes plaintexts at one time and the length of each ciphertext is $1,022$ bytes. Specifically, in the proposed scheme, encrypted data in step 1) is $2,846$ bytes, in which $\mathbf{b}, \xi$ are $1,824$ bytes and $E_{PU_{\mathrm{NG}}}(\mathrm{Nonce}_1, \mathrm{ID}_{\mathrm{S_i}}, h_1(\mathrm{Nonce}_1, \mathrm{ID}_{\mathrm{S_i}}, \mathbf{b}, \xi))$ occupies $1,022$ bytes. In step 2), $\mathbf{b}'$, $\bar{\mathbf{c}}$, $E_{PU_{\mathrm{S_i}}}(\mathrm{Nonce}_1, \mathrm{Nonce}_2, \mathrm{ID}_{\mathrm{NG}}, h_1(\mathrm{Nonce}_1, \mathrm{Nonce}_2, \mathrm{ID}_{\mathrm{NG}}, \mathbf{b}', \bar{\mathbf{c}}))$ are $3,070$ bytes and $E_{PU_{\mathrm{NG}}}(\mathrm{Nonce}_2, h_1(\mathrm{Nonce}_1, \mathrm{Nonce}_2, \mathrm{ID}_{\mathrm{NG}}, \mathbf{b}', \bar{\mathbf{c}}))$ is 1,022 bytes in step 3). Therefore, totally the communication cost of the proposed scheme is $6,938$ bytes.

In [12], all the messages are encrypted using RSA encryption. In the proposed scheme, we only encrypt the hash value of $\mathrm{Nonce}_1, \mathrm{ID}_{\mathrm{S_i}}, \mathbf{b}, \xi$ instead of themselves. The reason is that if we also try to encrypt all the data, there will be too much costs on communication and computation. For example, $\mathbf{b}, \xi$ is of $1,824$ bytes, but if we try to transmit the encryption of $\mathbf{b}, \xi$, then we need to divide it into 18 blocks for encryption, since each time NTRU algorithm can encrypt 106 bytes of plaintexts. Recalling that the length of each ciphertext is $1,022$ bytes, the total length of the ciphertext is $1022 * 18 = 18,396$ bytes. In a sum, if we choose to encrypt all the transmitted messages, then in the proposed scheme the total communication cost is $40,884$ bytes. Therefore, our proposed scheme can significantly reduce the communication cost while maintaining the same security level.

In Table IV, we also present the storage cost of the above schemes. In the proposed scheme, the smart meter's storage cost is comprised of the NTRU algorithm's key pair in the initialization phase, $\mathbf{a}$, $\mathbf{s}$, $\mathbf{e}$, $\mathbf{b}$, ξ, and $E_{PU_{\mathrm{NG}}}(\mathrm{Nonce}_1, \mathrm{ID}_{\mathrm{S_i}}, h_1(\mathrm{Nonce}_1, \mathrm{ID}_{\mathrm{S_i}}, \mathbf{b}, \xi))$ in step 1) of the key establishment phase, the encrypted data $E_{PU_{\mathrm{S_i}}}(\mathrm{Nonce}_1, \mathrm{Nonce}_2, \mathrm{ID}_{\mathrm{NG}}, h_1(\mathrm{Nonce}_1, \mathrm{Nonce}_2, \mathrm{ID}_{\mathrm{NG}}, \mathbf{b}', \bar{\mathbf{c}}))$ received from NG in step 2), and decrypted data Nonce_1, Nonce_2, $\mathrm{ID}_{\mathrm{NG}}$, $h_1(\mathrm{Nonce}_1, \mathrm{Nonce}_2, \mathrm{ID}_{\mathrm{NG}}, \mathbf{b}', \bar{\mathbf{c}})$ in step 2).

To be specific, in the proposed scheme the NTRU algorithm's key pair is of $2,147$ bytes, and $\mathbf{a}$ and $\mathbf{b}$ are of $1,792$ bytes each, while $\mathbf{s}$ and $\mathbf{e}$ both occupy $1,024$ bytes. Since the Smart Meter doesn't need to store $E_{PU_{\mathrm{NG}}}$ $(\mathrm{Nonce}_1, \mathrm{ID}_{\mathrm{S_i}}, h_1(\mathrm{Nonce}_1, \mathrm{ID}_{\mathrm{S_i}}, \mathbf{b}, \xi))$ $(1,022$ bytes) and $E_{PU_{\mathrm{S_i}}}(\mathrm{Nonce}_1, \mathrm{Nonce}_2, \mathrm{ID}_{\mathrm{NG}}, h_1(\mathrm{Nonce}_1, \mathrm{Nonce}_2, \mathrm{ID}_{\mathrm{NG}}, \mathbf{b}', \bar{\mathbf{c}}))$ $(1,022$ bytes) at the same time and the former occupies more space, we only take into account the $E_{PU_{\mathrm{S_i}}}(\mathrm{Nonce}_1, \mathrm{Nonce}_2, \mathrm{ID}_{\mathrm{NG}}, h_1(\mathrm{Nonce}_1, \mathrm{Nonce}_2, \mathrm{ID}_{\mathrm{NG}}, \mathbf{b}', \bar{\mathbf{c}}))$. Due to the fact that the $E_{PU_{\mathrm{NG}}}(\mathrm{Nonce}_2, h_1(\mathrm{Nonce}_1, \mathrm{Nonce}_2, \mathrm{ID}_{\mathrm{NG}}, \mathbf{b}', \bar{\mathbf{c}}))$ in step 3) is of $1,022$ bytes, in the proposed scheme the total storage cost of smart meter is $12,383$ bytes. On the other side, the NG's storage cost is consists of NTRU algorithm's key pair (2,147 bytes), $\mathbf{s}'$ (1,024 bytes), $\mathbf{e}'$ (1,024 bytes), $\mathbf{b}'$ (1,024 bytes), $\bar{\mathbf{c}}$ (1,024 bytes), and the encrypted data $E_{PU_{\mathrm{NG}}}(\mathrm{Nonce}_1, \mathrm{ID}_{\mathrm{S_i}}, h_1(\mathrm{Nonce}_1, \mathrm{ID}_{\mathrm{S_i}}, \mathbf{b}, \xi))$ in step 1 (1,022 bytes), decrypted data $(\mathrm{Nonce}_1, \mathrm{ID}_{\mathrm{S_i}}, h_1(\mathrm{Nonce}_1, \mathrm{ID}_{\mathrm{S_i}}, \mathbf{b}, \xi))$ (64 bytes), encrypted data $E_{PU_{\mathrm{S_i}}}(\mathrm{Nonce}_1, \mathrm{Nonce}_2, \mathrm{ID}_{\mathrm{NG}}, h_1(\mathrm{Nonce}_1, \mathrm{Nonce}_2, \mathrm{ID}_{\mathrm{NG}}, \mathbf{b}', \bar{\mathbf{c}}))$ in step 2) $(1,022$ bytes) and the encrypted data $E_{PU_{\mathrm{NG}}}$ $(\mathrm{Nonce}_2, h_1(\mathrm{Nonce}_1, \mathrm{Nonce}_2, \mathrm{ID}_{\mathrm{NG}}, \mathbf{b}', \bar{\mathbf{c}}))$ in step 4) $(1,022$ bytes), which together occupy $7,327$ bytes in the proposed scheme.

We can see that our proposed method can also significantly reduce the storage cost, since if we choose to encrypt all the transmitted data, then in the proposed scheme, the total storage cost of Smart Meter is $69,647$ bytes, meanwhile, the storage cost of the NG is $70,447$ bytes.

Therefore, from Table II, III, and IV, we can conclude that our proposed scheme is very efficient while incurring relatively low computation and communication costs.

VIII. CONCLUSION

In this paper, we have taken a step forward in designing a quantum-safe mutual authentication scheme for two-way communications in NANs of smart grid. We integrated NTRU and the lattice-based key exchange scheme to establish an authenticated secure channel. The security analysis has shown that our proposed schemes can achieve mutual authentication between NG and the smart meter. As shown by the implementations, our designed scheme is efficient and has relatively low communication and storage costs. The future work may include how to provide quantum-safe authentication for other communication networks of smart grid with strict latency.

REFERENCES

[1] A. Caille *et al.*, *Deciding the Future: Energy Policy Scenarios to 2050*, World Energy Council, London, U.K., 2007.

[2] Commonwealth Edison Company. *Delivering on Smart Grid: Five-Year Capstone Report*. Accessed: Jul. 15, 2017. [Online]. Available: https://www.comed.com/SiteCollectionDocuments/AboutUs/ComEdProgressReport2017VFinal.pdf

[3] E. Toh, "Experiences in Asia for integration of smart grids and renewables: The Singapore story," in *Proc. Int. Smart Grid Action Netw. Public Workshop*, pp. 1–19. Accessed: May 24, 2017. [Online]. Available: http://www.nedo.go.jp/content/100778185.pdf

[4] P. Mcdaniel and S. Mclaughlin, "Security and privacy challenges in the smart grid," *IEEE Security Privacy*, vol. 7, no. 3, pp. 75–77, May/Jun. 2009.

[5] N. Liu, J. Chen, L. Zhu, J. Zhang, and Y. He, "A key management scheme for secure communications of advanced metering infrastructure in smart grid," *IEEE Trans. Ind. Electron.*, vol. 60, no. 10, pp. 4746–4756, Oct. 2013.

[6] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Security Privacy*, vol. 8, no. 1, pp. 81–85, Jan./Feb. 2010.

[7] S. Li, K. Xue, Q. Yang, and P. Hong, "PPMA: Privacy-preserving multisubset data aggregation in smart grid," *IEEE Trans. Ind. Informat.*, vol. 14, no. 2, pp. 462–471, Feb. 2018.

[8] H. Shen, M. Zhang, and J. Shen, "Efficient privacy-preserving cube-data aggregation scheme for smart grids," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1369–1381, Jun. 2017.

[9] Y. Liu, W. Guo, C.-I. Fan, L. Chang, and C. Cheng, "A practical privacy-preserving data aggregation (3PDA) scheme for smart grid," *IEEE Trans. Ind. Informat.*, vol. 15, no. 3, pp. 1767–1774, Mar. 2019. doi: 10.1109/TII.2018.2809672.

[10] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1933–1954, 4th Quart., 2014.

[11] X. Liu and Z. Li, "False data attacks against AC state estimation with incomplete network information," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2239–2248, Sep. 2017.

[12] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. S. Shen, "A lightweight message authentication scheme for smart grid communications," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 675–685, Dec. 2011.

[13] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1621–1631, Sep. 2012.

[14] W. Jia, H. Zhu, Z. Cao, X. Dong, and C. Xiao, "Human-factor-aware privacy-preserving aggregation in smart grid," *IEEE Syst. J.*, vol. 8, no. 2, pp. 598–607, Jun. 2014.

[15] A. Abdallah and X. Shen, "Lightweight security and privacy preserving scheme for smart grid customer-side networks," *IEEE Trans. Smart Grid*, vol. 8, no. 3, pp. 1064–1074, May 2017.

[16] J. Hoffstein, J. Pipher and J. H. Silverman, "NTRU: A new high speed public key cryptosystem," in *Proc. Int. Algorithmic Number Theory Symp.*, 1998, pp. 267–288.

[17] J. Hoffstein, J. Pipher, and J. H. Silverman, "NSS: An NTRU lattice-based signature scheme," in *Proc. Adv. Cryptol. Eurocrypt*, 2001, pp. 211–228.

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

[19] L. Chen *et al.*, *Report on Post-Quantum Cryptography*, document NISTIR 8105, NISTIR, Gaithersburg, MD, USA. Accessed: Jun. 4, 2017. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

[20] M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?" IACR Cryptol. ePrint Archive, Rep. 2015/1075, 2015.

[21] M. H. Devoret and R. J. Schoelkopf, "Superconducting circuits for quantum information: An outlook," *Science*, vol. 339, no. 6124, pp. 1169–1174, 2013.

[22] *IBM*. Accessed: May 24, 2019. [Online]. Available: http://research.ibm.com/ibm-q/

[23] T. Monz *et al.*, "Realization of a scalable Shor algorithm," *Science*, vol. 351, no. 6277, pp. 1068–1070, 2016.

[24] N. M. Linke *et al.*, "Experimental comparison of two quantum computing architectures," *Proc. Nat. Acad. Sci.*, vol. 114, no. 13, pp. 3305–3310, 2017.

[25] L. Chen, "Cryptography standards in quantum time: New wine in an old wineskin?" *IEEE Security Privacy*, vol. 15, no. 4, pp. 51–57, Aug. 2017.

[26] J. Ding, S. Fluhrer, and S. Rv, "Complete attack on RLWE key exchange with reused keys, without signal leakage," in *Proc. Australas. Conf. Inf. Security Privacy*, 2018, pp. 467–486.

[27] J. W. Bos, C. Costello, M. Naehrig, and D. Stebila, "Post-quantum key exchange for the TLS protocol from the ring learning with errors problem," in *Proc. IEEE Symp. Security Privacy*, 2015, pp. 553–570.

[28] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, "Post-quantum key exchange—A new hope," in *Proc. USENIX Security Symp.*, 2016, pp. 327–343.

[29] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, "Securing the Internet of Things in a quantum world," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 116–120, Feb. 2017.

[30] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *J. ACM*, vol. 56, no. 6, pp. 1–40, 2009.

[31] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," in *Proc. Adv. Cryptol. (EUROCRYPT)*, 2010, pp. 1–23.

[32] R. Lindner and C. Peikert, "Better key sizes (and attacks) for LWE-based encryption," in *Proc. CT-RSA*, vol. 6558, 2011, pp. 319–339.

[33] J. Ding, X. Xie, and X. Lin, "A simple provably secure key exchange scheme based on the learning with errors problem," IACR Cryptol. ePrint Archive, Rep. 2012/688, 2012.

[34] A. Fujioka, K. Suzuki, K. Xagawa, and K. Yoneyama, "Practical and post-quantum authenticated key exchange from one-way secure key encapsulation mechanism," in *Proc. 8th ACM SIGSAC Symp. Inf. Comput. Commun. Security (ASIA CCS)*, May 2013, pp. 83–94.

[35] C. Peikert, "Lattice cryptography for the Internet," IACR Cryptol. ePrint Archive, Rep. 2014/070, 2014.

[36] J. Zhang, Z. Zhang, J. Ding, M. Snook, and Ö. Dagdelen, "Authenticated key exchange from ideal lattices," in *Proc. EUROCRYPT*, Apr. 2015, pp. 719–751.

[37] J. Bos *et al.*, "Frodo: Take off the ring! practical, quantum-secure key exchange from LWE," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2016, pp. 1006–1018.

[38] H. Li, R. Lu, L. Zhou, B. Yang, and X. Shen, "An efficient merkle-tree-based authentication scheme for smart grid," *IEEE Syst. J.*, vol. 8, no. 2, pp. 655–663, Jun. 2014.

[39] Y. Liu, C. Cheng, T. Gu, T. Jiang, and X. Li, "A lightweight authenticated communication scheme for smart grid," *IEEE Sensors J.*, vol. 16, no. 3, pp. 836–842, Feb. 2016.

[40] W. Whyte *et al.*, "IEEE P1363.1 draft 10: Draft standard for public-key cryptographic techniques based on hard problems over lattices," Cryptol. ePrint Archive, Rep. 2008/361, 2008.

[41] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe. (2016). *NewHope Without Reconciliation*. Accessed: Jun. 18, 2018. [Online]. Available: https://www.cryptojedi.org/papers/newhopesimple-20161217.pdf

[42] M. J. Dworkin, "SHA-3 standard: Permutation-based hash and extendable-output functions," Federal Inf. Process. Stand., NIST, Gaithersburg, MD, USA, Rep. 202, 2015. Accessed: Jun. 18, 2018. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf

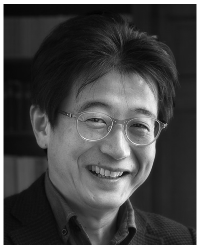
[43] *Open Quantum Safe Project*. Accessed: Jan. 3, 2017. [Online]. Available: https://openquantumsafe.org/

Chi Cheng (M'15) received the Ph.D. degree in information and communication engineering from the Huazhong University of Science and Technology, Wuhan, China, in 2013. He is currently an Associate Professor with the School of Computer Science, China University of Geosciences, Wuhan. From 2014 to 2016, he was an International Research Fellow with the Japan Society for the Promotion of Science, Institute of Mathematics for Industry, Kyushu University, Japan. His research interests focus on applied cryptography and network security.

Yue Qin received the B.S. degree in information security from the China University of Geosciences, Wuhan, China, in 2018, where she is currently pursuing the master's degree with the School of Computer Science. Her research interest focuses on applied cryptography.

Rongxing Lu (S'99–M'11–SM'15) received the Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo, Canada, in 2012. He has been an Assistant Professor with the Faculty of Computer Science, University of New Brunswick, Canada, since 2016. Before that, he was an Assistant Professor with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, from 2013 to 2016. He was a Post-Doctoral Fellow with the University of Waterloo from 2012 to 2013. His research interests include applied cryptography, privacy enhancing technologies, and IoT-big data security and privacy. He was a recipient of the most prestigious "Governor General's Gold Medal," and the 8th IEEE Communications Society Asia–Pacific Outstanding Young Researcher Award, in 2013. He currently serves as the Vice-Chair (Publication) of IEEE ComSoc CIS-TC.

Tao Jiang (M'06–SM'10–F'19) received the Ph.D. degree in information and communication engineering from the Huazhong University of Science and Technology, Wuhan, China, in 2004, where he is currently a Distinguished Professor with the School of Electronics Information and Communications. From 2004 to 2007, he worked in universities such as Brunel University and the University of Michigan–Dearborn. He has authored or co-authored over 300 technical papers in major journals and conferences and 9 books/chapters in the areas of communications and networks. He served or is serving as Symposium Technical Program Committee Membership of some major IEEE conferences, including INFOCOM, GLOBECOM, and ICC. He was invited to serve as TPC Symposium Chair for the IEEE GLOBECOM 2013 and IEEEE WCNC 2013. He is served or serving as an Associate Editor of some technical journals in communications. He is the Associate Editor-in-Chief of *China Communications*.



Tsuyoshi Takagi received the Ph.D. degree from the Technical University of Darmstadt, Germany, in 2001. He was engaged in Research on Network Security with NTT Laboratories from 1995 to 2001. He was an Assistant Professor with the Department of Science, Technical University of Darmstadt until 2005. He was a Professor with Kyushu University, Japan, until 2018. He is currently a Professor with the Graduate School of Information Science and Technology, University of Tokyo, Japan. His current research interests are information security and cryptography. He was a recipient of the DOCOMO Mobile Science Award in 2013, the IEICE Achievement Award in 2013, and the JSPS Prize in 2014. He was the Program Chair of the 7th International Conference on Post-Quantum Cryptography in 2016.