JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Survey on Smart Grid Networks and Security using Lattice-Based Cryptography

Chandrashekhar Diwakar[1,3] and Nasheem Khan[2,3]*

[1]Department of Mathematics, Govt. Degree College, Mant, Mathura (U. P.)- 281202, India

[2]Department of Mathematics, Babu Shivnath Agrawal College, Mathura (U. P.)- 281004, India

[3]Dr. Bimrao Ambedkar University, Agra (U. P.)- 282004, India

Abstract: A smart grid network (SGN) is an advanced electrical grid system based on information and communication technology. The system uses digital technology, sensors, and two-way communication to manage electricity flow from generation to consumption, enabling real-time monitoring, efficiency, reliability, and seamless integration of renewable and electric vehicles. In the present time, SG network systems are vulnerable to cyber security attacks because these systems use sensors as well as the internet during two-way communication. So, there is a critical need of cryptosystems that can ensure the security of two-way smart grid communication. There are numerous authentication protocols proposed by researchers to protect smart grid networks (SGNs) from cyber security attacks. But, most of them are based on prime factorization and discrete logarithmic problems, which are vulnerable to quantum computing attacks. The researchers have found that lattice-based cryptographic primitives are important candidates to form cryptosystems that are hard to break even on quantum computers. The aim of this article is to find out lattice-based cryptosystems that are suitable to design the cryptographic protocols secure against quantum computing attacks. This survey provides an overview of lattice-based cryptosystems and their applications in securing SG networks.

Key words: Smart-Grid Networks (SGNs), Post-quantum cryptography, Lattice-based cryptography (LBC), Security, Privacy.

I. INTRODUCTION

Conventional power grid systems are the traditional, centralized electrical networks that deliver power from large, often fossil-fuel-based, power plants to consumers through a one-way flow, relying on older technologies with limited monitoring and communication, making them less efficient and reliable than modern smart grids. The SGNs [1, 2] are believed to be the extension of the conventional power grid systems. The smart grid is an inventive bi-directional power system based on information and communication technology that computes the total amount of power generated as well as consumed. The primary motivation for implementing SGNs is to ensure the prosperity of future generations, not only by regulating green energy sources but also by forming a sustainable economy [3]. It realizes real-time retrospect, optimized scheduling, and excellent governance of the power system through smart communication networks and computer technology sensors. In comparison of conventional power grid systems, the SGNs produce a wide overview of operations, networked data transmission, vulnerability scanning, enhanced scheduling decision process, self regulation, and optimized machine-network coordination. The grid utilizes the widespread use of distributed intelligence and broadband communications, as well as the integration of automated control systems. In this way, it ensures market transactions and interactions on the grid are in real-time and benefit from seamless connectivity.

1.1 Vulnerabilities in Smart Grid Infrastructures

The evolution of conventional power grids into IoT-enabled SGNs has significantly increased their exposure to cyber threats, particularly because communication across these networks often occurs over public infrastructures. Attackers may exploit these communication channels to impersonate users, manipulate smart meter (SM) readings, or deliberately disrupt grid operations through denial-of-service (DoS) attacks. Prior research has extensively examined the security vulnerabilities inherent in SGN environments [4]. Alongside security challenges, protecting user privacy has become a pressing concern, especially in consumer-facing network segments such as Home Area Networks (HANs), Building Area Networks (BANs), and Industrial Area Networks (IANs) [2]. Exposure of sensitive information, including detailed electricity usage patterns, can have serious implications for individual and organizational privacy. Even access to coarse-grained daily consumption data may allow adversaries to infer occupancy status or identify commonly used electrical devices using simple analytical methods. The integration of IoT technologies throughout SGNs results in the continuous generation of large volumes of data across power generation, transmission, and consumption stages. This data proliferation amplifies privacy risks, particularly for industrial

entities. For instance, unauthorized access to industrial energy usage and production information may be exploited for corporate espionage or competitive advantage. Consequently, safeguarding consumer privacy, most notably by ensuring the confidentiality of data exchanged among smart meters within Neighbourhood Area Networks (NANs),must be treated as a primary requirement in current SGNs deployments.

1.2 Motivation and Contribution

This work is driven by the objective of reviewing recent progress in SGNs, particularly from the perspective of emerging security and privacy challenges. Conventional power grids operate on a centralized generation model in which electricity is produced at power stations, regulated through voltage adjustments, and distributed to consumers via a unidirectional flow. While functional, this approach lacks the adaptability required for modern energy management and efficient utilization. Smart Grid Networks address these shortcomings by introducing bidirectional communication and intelligent control mechanisms, enabling improved coordination between energy generation, distribution, and consumption while supporting environmentally sustainable power usage. Despite these benefits, SGNs remain exposed to various security and privacy threats, as highlighted in earlier studies [4]. Interruptions in power generation or communication channels can destabilize grid operations, leading to widespread disruptions and significant socio-economic consequences. To mitigate such risks, the National Institute of Standards and Technology (NIST) has established security and privacy guidelines for SGNs based on the PAA principles of privacy, authenticity, and availability [5].

Although numerous solutions have been proposed to strengthen SGNs security and protect user privacy, a large portion of existing work relies on traditional public-key cryptographic techniques grounded in integer factorization and discrete logarithm assumptions. The advent of practical quantum computing threatens these foundations, rendering conventional cryptographic approaches increasingly inadequate for securing IoT-enabled SGN infrastructures [6].In response, this article concentrates on post-quantum security and privacy-preserving mechanisms built upon lattice-based cryptography [7]. The study aims to analyze recent advancements in lattice-based cryptosystems that offer resilience against both present-day attacks and future quantum adversaries, thereby enabling secure and trustworthy SGN deployments.

II. SMART GRID NETWORK TECHNOLOGY

2.1Smart-Grid Networks

The increasing digitalization of power-grid systems has led to the development of advanced Smart Grid Networks (SGNs) (Figure 1) built on IoT technologies [1, 2]. These networks incorporate smart meters, intelligent communication environments, and sustainable on-demand power generation. The SGN architecture is organized into several communication layers, namely home area networks (HANs), building area networks (BANs), industrial area networks (IANs), neighbourhood area networks (NANs), field area networks (FANs), vehicle-to-grid (V2G) interfaces, and wide area networks (WANs).

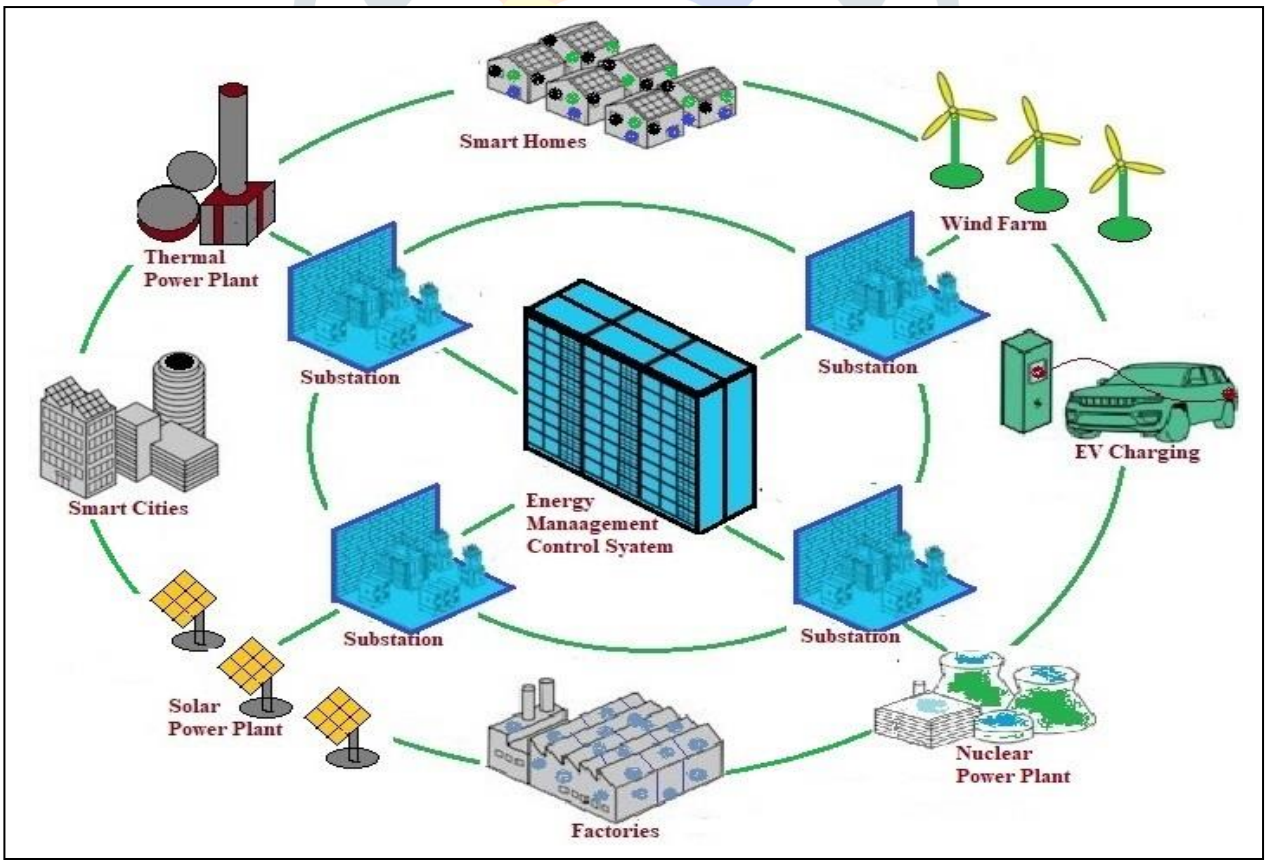

figure 1: Smart grid network

2.2 Smart Grid Networks Structure

The National Institute of Standards and Technology set up a new design of the power-grid systems, which is known as SGNs. In comparison with traditional power-grid systems, the SGNs are totally unified, rapid, elegant, and two-way communication

frameworks. The SGNs frameworks are designed with the association of numerous power appliances to initiate an interactive and concurrent adaptive configuration and strong power management abilities, for example, "Advanced Metering Infrastructure" [8] and "on-demand" ability to react. The power-grid layers of the SGNs architecture comprise of four phases such as: power-production, power-dissemination grid, power-dispensation grid, and power utilization. The SGNs are divided into the structures such as the SGN model, SGN layers, and SGN systems to accomplish the SGNs effectiveness.

2.3 Smart Grid Networks Advantages

Conventional power grid systems have long faced numerous operational and structural challenges, including limited support for diverse energy sources such as renewable, high infrastructure costs, and rigid control mechanisms. Traditional approaches to electricity generation and distribution often result in substantial maintenance expenses, delayed demand-response actions, elevated greenhouse gas emissions, and extended blackout durations. To address these shortcomings, Smart Grid Networks (SGNs) have emerged as a robust, adaptive, and scalable alternative that enables seamless integration of renewable and non-renewable energy resources. In addition to improving flexibility, SGNs enhance grid resilience through fault-tolerant mechanisms, reduction of transmission losses, and support for lower carbon emissions. Overall, SGN infrastructures deliver significant performance improvements over legacy grid systems. This subsection highlights the advantages of SGNs across three major dimensions—reliability enhancement, efficiency improvement, and environmental sustainability as reported in earlier studies [9].

- **Reliability Enhancements:** SGNs improve service reliability by reducing the frequency and impact of power outages while ensuring electricity availability based on real-time consumer demand. Intelligent monitoring and automated control allow utility providers to respond promptly to usage fluctuations and deliver improved service quality. In scenarios where demand requirements are not met, utilities may be required to compensate customers, making SGN deployment beneficial for both consumers and service providers.
- **Efficiency Improvement:** Operational efficiency in SGNs is achieved through reduced power losses and optimized energy utilization. Dynamic pricing strategies encourage consumers to shift usage to off-peak hours, while vehicle-to-grid (V2G) systems help minimize unnecessary electricity production. Secure SGNs also play a role in limiting power theft, a major cause of energy loss in many regions. The incorporation of renewable energy sources further decreases reliance on conventional power plants and supports scalable power distribution. Moreover, SGNs enable accurate aggregation of consumption data, real-time grid monitoring, and timely transmission of alerts to control centers during faults or cyber incidents.
- **Environmental Sustainability:** A defining benefit of SGNs lies in their environmentally conscious architecture, which integrates distributed generation with renewable energy resources to meet varying power demands. By promoting efficient energy usage and reducing emissions, SGNs enhance consumer satisfaction while simultaneously improving the operational profitability of utility providers [10].

III. SECURITY AND PRIVACY ISSUES IN SGNs

The serious security and privacy challenges in Smart Grid Networks (SGNs) [1, 2] arise primarily from the IoT-enabled wireless communication infrastructure and the extensive exchange of information between aggregators and smart meters (SMs). These characteristics expose SGNs to a wide range of cyber threats, including man-in-the-middle (MITM) attacks, replay attacks, denial-of-service (DoS) attacks, and insider attacks. [11] A MITM attack [12] is an active threat in which an adversary eavesdrops on ongoing communications, intercepts sensitive data, and may modify the transmitted information before forwarding it to the intended receiver. Replay attacks [5] involve capturing legitimate communication messages and retransmitting them multiple times, thereby disrupting normal system operations. For instance, repeated transmission of a single entity's resource-demand messages to control centers (CCs) can cause erroneous prioritization, leading to resource imbalance, potential blackouts, and significant economic and infrastructural losses in affected regions. DoS [13] attacks target network availability by overwhelming SGN communication channels with excessive traffic, thereby preventing legitimate users from accessing essential services. Furthermore, insecure wireless channels facilitate insider and resource-theft attacks [14], where adversaries gain unauthorized access to SMs, intermediate CCs, or other network entities to exploit shared resources, ultimately compromising system reliability and security.

3.1 Security Goals in SGNs

NIST outlines a comprehensive set of security requirements for Smart Grid Networks (SGNs) grounded in the PAA [1, 4] security model: privacy, authenticity, and accessibility, which are fundamental to secure power-system infrastructures.

- **Privacy:** Privacy or confidentiality focuses on preventing unauthorized [5] access to private and proprietary information by applying strict access-control and privacy-preserving mechanisms. Any form of data leakage undermines confidentiality and can have serious consequences for both individual consumers and organizations. For example, exposure of household energy consumption patterns may reveal sensitive lifestyle information, while disclosure of industrial energy usage can allow adversaries to estimate production levels and business performance using straightforward analytical techniques [14].
- **Authenticity:** Authenticity ensures that information exchanged within the SGN remains trustworthy, accurate, and resistant to unauthorized modification, while also supporting authentication and non-repudiation. Since SGNs rely on bidirectional communication to exchange demand-response signals among various entities, maintaining data integrity is critical for grid stability. Both passive and active man-in-the-middle (MITM) attacks threaten this property by enabling adversaries to alter, inject, or replay messages [10]. Such attacks may distort demand forecasts and negatively affect overall grid operation.

- **Accessibility:** Accessibility represents the ability of the system to provide uninterrupted and timely access to information and services. Failure to access data at any point in the SGN can lead to severe operational disruptions or even system-wide collapse [15, 16]. Data aggregation from smart meters (SMs) and substations typically depends on multiple gateways and intermediate nodes; therefore, denial-of-service (DoS) attacks targeting these components can significantly impair communication efficiency and grid reliability.

Beyond the PAA triad, secure data storage [17] mechanisms are employed to protect sensitive information throughout the SGNs. Additionally, scalability is recognized as a vital security requirement, referring to the ability of communication protocols and technologies to support secure operation in large-scale, distributed, and heterogeneous smart-grid environments.

3.2 Privacy-Preservation Goals in SGNs

The National Institute of Standards and Technology (NIST) identifies four key privacy dimensions to safeguard user privacy during data collection, transmission, and information sharing in smart grid networks (SGNs) [18]. The foremost of these is the protection of personal information, which includes an individual's physical, cultural, economic, and social identifiers. Personal privacy involves securing sensitive personal data such as biometric indicators, health-related information, and medical records. Another important aspect is behavioural privacy, which ensures that an individual's daily activities and usage patterns are not exposed. Communication privacy further addresses the prohibition of unauthorized monitoring or tracking of communication exchanges. Among these dimensions, the protection of personal information is considered the most critical when designing privacy-preserving mechanisms for SGNs [19].

In SGN environments, smart meters (SMs) collect electricity consumption data from smart appliances (SAs) within home-area and industrial-area networks (HANs/IANs) and transmit aggregated readings to building-area networks (BANs) [11]. These consumption records are highly sensitive, as they reflect users' daily routines and lifestyle behaviours. If such data are disclosed, adversaries may infer household activities, predict future behaviour, and identify the number and types of appliances in use, enabling surveillance, targeted marketing, and consumer profiling.

As a result, unauthorized sharing of energy usage information can seriously undermine personal privacy, reduce user trust, and hinder the adoption of SGNs. These concerns highlight the importance of making privacy protection a fundamental design objective in smart grid systems.

IV. LATTICE-BASED CRYPTOGRAPHY

During the mid-1990s, Peter Shor [20] revealed that quantum computing techniques are capable of efficiently solving the integer factorization and discrete logarithm problems, which underpin many classical cryptographic systems. As a consequence, cryptographic algorithms relying on these mathematical assumptions are expected to become insecure in the presence of practical quantum computers [21]. This potential risk has accelerated the search for alternative cryptographic solutions and highlighted the importance of post-quantum cryptography (PQC).To address these challenges, the National Institute of Standards and Technology (NIST) has identified and shortlisted multiple PQC schemes. Among those schemes, lattice-based cryptographic approaches built upon computationally hard lattice problems are widely recognized as strong contenders for resisting quantum-enabled attacks [21, 22]. This section therefore, introduces the fundamental concepts of lattices and their hardness assumptions, which are essential for the development of secure PQC systems.

4.1 Lattices

Lattices are mathematical structures composed of infinitely many discrete points positioned in a uniform n-dimensional arrangement, creating a symmetric geometric pattern (Figure 2). Although their geometric layout appears simple, lattices exhibit complex combinatorial properties that have made them a subject of extensive mathematical study and a foundation for innovative computational techniques. The advent of quantum computing has challenged the long-term security of traditional cryptographic systems, prompting the exploration of alternative constructions capable of withstanding quantum attacks. In this context, LBC has gained prominence as a viable solution for post-quantum security. By relying on computationally intractable lattice problems, numerous cryptographic primitives, including encryption schemes, key exchange mechanisms, authentication protocols, and digital signature algorithms, have been developed to address emerging security demands [23, 24].The intrinsic structure of lattices enables strong resistance to quantum adversaries while supporting efficient and practical implementations. As a result, lattice-based approaches are widely considered strong candidates for achieving long-term, quantum-resilient security [25]. Formally, lattices are defined as follows:

Definition: Consider a set $B = \{u_1, u_2, \dots \dots \dots, u_n\}$ consisting of n linearly independent vectors in R^n. The lattice L associated with B consists of all vectors obtained by taking integer linear combinations of these vectors, that is

$$L = \{ \sum_{i=1}^{n} c_i u_i : c_i \text{is an integer for all } i\}.$$

The set B is known as a generating basis of the lattice L, and the number of vectors in any such basis is fixed for a given lattice. This quantity, denoted by dim (L), represents the dimension of the lattice.

It is important to note that a lattice may be generated by many different bases, all yielding the same point set. These bases are not equivalent in terms of geometric quality; some are composed of shorter vectors that are close to being orthogonal. The existence of multiple, geometrically diverse bases for the same lattice forms the foundation of several lattice-based cryptographic schemes, as it leads to computational problems that are hard to solve efficiently. The primary goal of cryptography is to construct security mechanisms that remain resilient against adversarial efforts aimed at compromising protected systems. One of the central problems in this domain is enabling confidential communication between legitimate participants who seek to exchange information without disclosure. This objective is typically achieved by establishing a shared secret key, which allows messages to be encrypted and securely transmitted. Consequently, contemporary cryptographic research concentrates on developing cryptographic primitives whose underlying problems are computationally infeasible to solve in practice. Identifying suitable hard problems for cryptographic design, however, presents a significant challenge. If the complexity classes P, and NP were shown to be equivalent, many cryptographic assumptions would be invalidated, as attackers

could potentially derive secret keys efficiently using nondeterministic algorithms. Conversely, the widely accepted assumption that $P \neq NP$ [24] supports the existence of problems that are computationally difficult to solve, thereby ensuring that adversaries have only a negligible chance of successfully breaking cryptographic schemes.

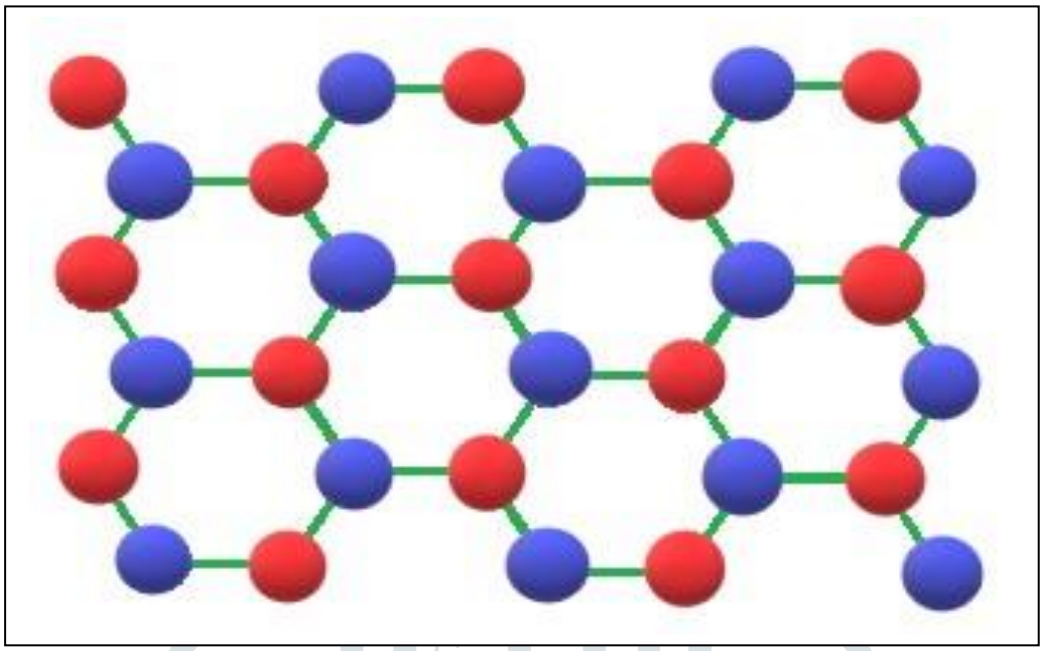

figure 2: The hexagonal honeycomb lattice

As a result, cryptographic constructions are typically grounded in mathematical problems that demonstrate hardness in both worst-case and average-case settings. Many classical cryptographic algorithms rely on the computational difficulty of number-theoretic problems such as integer factorization. However, advances in quantum computing threaten the security of these approaches, as sufficiently powerful quantum machines could solve such problems efficiently. To mitigate this risk, lattice-based cryptosystems have emerged as a promising alternative. These systems are built upon geometric structures formed by point lattices [22] generated from basis vectors and benefit from a strong connection between worst-case and average-case complexity. Owing to these properties, LBC has gained substantial attention as a foundation for future secure communication systems. The formal introduction of this paradigm by Goldreich et al. [26] in 1997 marked an important step toward developing cryptographic techniques capable of withstanding both classical and quantum adversaries.

4.1.1 Lattice Hard Assumptions

Ajtai [38] established that efficiently approximating core lattice problems are computationally infeasible, providing strong evidence of their inherent hardness. His work introduced lattice-based one-way functions, which are straightforward to compute but extremely difficult to reverse due to the randomness embedded in their inputs. Because of this asymmetry, these functions are well-suited for constructing fundamental cryptographic primitives such as digital signature algorithms, secret-key encryption schemes, and pseudorandom generators. Ajtai's results marked a turning point in cryptographic research by demonstrating that lattice problems could serve as a reliable security foundation. This insight encouraged further investigation into lattice-based constructions, including collision-resistant hash functions and a broad class of lattice-based cryptographic schemes [27]. The present section briefly outlines the principal lattice problems that underpin the development of lattice-based cryptosystems. Two problems are especially central: the Shortest Vector Problem (SVP) [28] and the Closest Vector Problem (CVP) [29].

(i) Shortest Vector Problem: Let $u \in L\backslash\{0\}$ be an arbitrary vector. Then, one has to find a non-zero vector in the lattice L such that $\|v\| \leq \|u\|$.

(ii) Closest Vector Problem: Let $u \notin L$ be any arbitrary vector. Then, one has to find a vector $v \in L$ such that $\|v - u\| \leq \|v - w\|$ for all $w \in L$.

The assumed difficulty of these problems forms the cornerstone of security for lattice-based cryptographic mechanisms. In lattice-based cryptographic constructions, a parameter γ is used to denote approximate variants of NP-hard lattice problems. As an example, the approximate shortest vector problem, denoted by SVP_γ, seeks a lattice vector whose Euclidean length is bounded by γtimes the length of the shortest nonzero vector in the lattice. Although these problems may be expressed using different norm definitions, the Euclidean norm is most commonly employed due to its analytical convenience and widespread acceptance. It is formally given by $\|x\| = \sqrt{\sum_{i=1}^{n} x_i^2}$.

4.2 p- Ary Lattices

An integer lattice L is said to be a p-ary lattice if L is a subgroup of Z_p^n where$Z_p^n \subseteq Z^n$ for some integer modulus p.

4.2.1 p-Ary Lattice Hard Problems:

(i) Small Integer Solution (SIS) Problem [30]: Let$N \in Z_p^{n\times m}$be a given integer modular matrix with integer modulo p and let $s \in R^+$ be a positive real constant. Then, it is computationally impractical to find anon-zero vector $v \in Z^m\backslash\{0\}$ such that$N.v = 0(modp)$and $\|v\| \leq s$.

(ii) Inhomogeneous Small Integer Solution (ISIS) Problem [30]: Let$N \in Z_p^{n\times m}$ be a given integer modular matrix with integer modulo p and $s \in R^+$ be a real positive constant. Then, for an arbitrary vector $u \in Z_p^n$ it is computationally impractical to find a non-zero vector $v \in Z^m\backslash\{0\}$which satisfy the condition $N.v = u(modp)$ and $\|v\| \leq s$.

(iii) Bi-Lateral Small Integer Solution (Bi-SIS) [30]: Let$N \in Z_p^{n\times n}$be a modular square matrix of rank r with integer modulo p, and $s \in R^+$ be a real positive constant. Then, it is computationally impractical to find two non-zero vectors$v, w \in Z^n\backslash\{0\}$which satisfy the condition

$$N \cdot v = 0(modp) \text{ for all } \|v\| \leq s \text{ and } w^T \cdot N = 0^T(modp) \text{ for all} \|w\| \leq s.$$

(iv) Bi-lateral Inhomogeneous Small Integer Solution [30] Problem: Let$N \in Z_p^{n\times n}$be a modular square matrix of rank r with integer modulo p and $s \in R^+$ be a real positive constant. Then for any two vectors $y, z \in Z^n$, it is computationally impractical to find two non-zero vectors $v, w \in Z^n\backslash\{0\}$ which satisfy the condition

$$N \cdot v = y(modp) \text{ for all } \|v\| \leq s \text{ and } w^T \cdot N = z^T(modp) \text{ for all } \|w\| \leq s.$$

(v) Computational Bi-ISIS Problem [30]: Let$N \in Z_p^{n\times n}$be a random modular square matrix of rank r and let $v, w \in Z^n\backslash\{0\}$are any two vectors. Then for all $\|v\| \leq s$ and $\|w\| \leq s$ it is computationally impracticable to find $w^T \cdot Nv(modp)$.

4.3 Lattice-Based Cryptographic Algorithms Based on Hardness of Lattices Problems

In terms of computational efficiency, traditional public-key cryptographic schemes such as RSA, ECC, and ElGamal generally require $O(k^3)$ time complexity to support encryption and decryption at a security level of k bits. By comparison, lattice-based cryptographic schemes can achieve similar security guarantees with a lower computational cost of approximately$O(k^2)$. This improvement is largely due to the fact that lattice-based operations are dominated by matrix arithmetic and basic linear algebraic computations, which are relatively efficient and easy to implement. Although LBC offers these practical advantages, its security analysis is still an active area of research and has not yet reached the same level of maturity as cryptosystems grounded in integer factorization or discrete logarithm assumptions.

Some lattice-based cryptographic constructions derived from different underlying lattice hardness problems are as follows:

(i) LLL- basis reduction algorithm (1982) proposed by Lenstra, Lenstra, and Lovasz [31].
(ii) Ajtai's Dwork [22] cryptosystem (1996) proposed by Ajtai, which is related to average/worst-case complexity of a lattice problem.
(iii) GGH [26] cryptosystem (1997) proposed by Goldreich, Goldwasser, and Halevi, an encryption and decryption scheme related to the solution of CVP.
(iv) NTRU [32] algorithm (1999) proposed by Hoffstein, Pipher, and Silverman, defined as an expression of quotients of polynomial rings.
(v) Learning with errors (LWE) (2009) algorithm proposed by O. Regev [33],a special class of hard problems that is SIVP and SIS hard assumptions of lattice mathematical structures.
(vi) Verbauwhede et al. [34] proposed an efficient software implementation of RLWE encryption(2014).

Overall, addressing the security challenges posed by quantum computing has become a major focus of current research, particularly in the context of Smart Grid Networks (SGNs). This survey has examined security solutions that rely on the computational hardness of lattice problems such as SVP, CVP, LWE, RLWE and related formulations discussed earlier. These hardness assumptions serve as the core building blocks for many proposed schemes. Looking forward, continued research into stronger, quantum-resilient security and privacy mechanisms will be essential for protecting IoT-enabled smart systems, which are expected to underpin next-generation technologies.

V. LATTICE-BASED SCHEMES FOR SGNs

As illustrated, lattice problems are notably difficult. The most well-known approach either takes an infinite amount of time or yields poor approximation ratios. LBC emerged with the belief that lattice problems are sufficiently challenging to resist conventional cryptographic attacks. In a post-quantum world, LBC remains a promising candidate as it is likely to withstand quantum attacks as well. While lattice problems seem to be natural candidates for quantum algorithms, no known quantum algorithms have surpassed the best-known classical cryptographic methods for solving lattice problems at the moment. Although lattice problems possess a periodic structure and a Fourier transform, they are not believed to be NP-hard for typical approximation factors.

Consequently, lattice problems can be extensively used in quantum algorithms and are closely connected to the concept of lattice duality. Despite attempts to solve lattice problems using quantum algorithms since Shor's discovery of the quantum factoring algorithm in the mid-1990s, there has been little or no success. The main obstacle lies in the fact that the periodicity-finding technique employed in Shor's factoring algorithm and related quantum algorithms does not seem to be effective for solving lattice problems. Thus, LBC remains a strong candidate for the post-quantum era due to its resilience against quantum attacks and the difficulty of solving lattice problems with quantum algorithms. Some lattice-based cryptographic schemes for SGNs are as follows:

- Lightweight security and privacy-preserving scheme for smart grid customer-side networks [7].
- A lightweight lattice-based security and privacy-preserving scheme for smart grid [35].
- A lightweight lattice-based homomorphic privacy-preserving data aggregation scheme for smart grid [36].
- Lattice-based cryptosystem for secure communication in a smart grid environment [37].
- Lightweight lattice-based homomorphic privacy-preserving aggregation scheme for home area networks [38].
- lightweight RLWE-based secure and privacy-preserving scheme for the consumer side network in smart grid [39].
- A lattice-based privacy preserving multi-functional and multi-dimensional data aggregation scheme for smart grid [40].
- A mutual authentication and key agreement protocol for a smart grid environment using lattice [41].
- A privacy-preserving dual-functional aggregation scheme for smart grid communications [42].

- The secure lattice-based data aggregation scheme in residential networks for smart grid [43].
- At the crossroads of lattice-based and homomorphic encryption to secure data aggregation in smart grid [44].

VI. CONCLUSION

The advent of quantum computing introduces significant future security risks, as quantum algorithms are expected to compromise modular arithmetic-based cryptographic schemes within polynomial time. These concerns have accelerated research efforts in the area of post-quantum cryptography (PQC). Accordingly, this work presents a review of existing studies in PQC, with particular emphasis on LBC, which is founded on the computational hardness of lattice problems. In addition, the paper surveys encryption and decryption techniques, key agreement mechanisms, authentication frameworks, and digital signature schemes specifically designed for SGNs. Furthermore, this study reviews emerging PQC primitives, NIST-recommended algorithms, open-source PQC tools and libraries, and ongoing industrial initiatives leveraging quantum-resistant technologies.

Future research should focus on advancing lattice-based cryptography by exploring new mathematical constructions and improving theoretical understanding. As IoT-driven SGNs continue to evolve, customized cryptographic solutions will be required to address emerging security and privacy challenges posed by quantum adversaries. In-depth performance evaluations—particularly with respect to efficiency, scalability, and resource consumption—are essential when comparing lattice-based methods with traditional cryptographic approaches. Beyond lattice-based techniques, further examination of alternative PQC primitives and the practical deployment of NIST-selected algorithms is necessary. Continued assessment of open-source implementations, industrial developments, and standardization efforts will be critical for identifying strengths and limitations. Ultimately, integrating quantum-resistant cryptographic technologies into critical infrastructures such as SGNs will be vital to ensuring long-term security in the post-quantum era.

VII. REFERENCES

1. Fang X., Misra S., Xue G., Yang D. 2011. Smart grid–the new and improved power grid: A survey. IEEE Commun Surv Tutor, 14(4):944-980.
2. Abdallah A., Shen X. 2018. Security and privacy in smart grid. Springer.
3. Wang W., Yi X., Khanna M. 2011. A survey on the communication architectures in smart grid. Comput Netw, 55(15):3604-3629.
4. Fan Z., Kulkarni P., Gormus S., et al. 2012. Smart grid communications: Overview of research challenges, solutions, and standardization activities. IEEE Commun Surv Tutor, 15(1):21-38.
5. Chen P. Y., Cheng S. M., Chen K. C. 2012. Smart attacks in smart grid communication networks. IEEE Commun Mag, 50(8):24-29.
6. Gupta D. S. 2023. Pilike: Post-quantum identity-based lightweight authenticated key exchange protocol for IIoT environments. IEEE Syst J.
7. Abdallah A., Shen X. 2015. Lightweight security and privacy preserving scheme for smart grid customer-side networks. IEEE Trans Smart Grid, 8(3):1064-1074.
8. Shengjie X., Qian Y., Rose Qingyang H. 2017. Astudy on communication network reliability for advanced metering infrastructure in smart grid. IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech). IEEE; 127-132.
9. Fan C. I., Huang S. Y., Lai Y. L. 2013. Privacy-enhanced data aggregation scheme against internal attackers in smart grid. IEEE Trans Industr Inform., 10(1):666-675.
10. Liu J., Xiao Y., Li S., Liang W., Chen C. L. P. 2012. Cyber security and privacy issues in smart grids. IEEE Commun Surv Tutor., 14(4):981-997.
11. Agarkar A., Agrawal H. 2019. A review and vision on authentication and privacy preservation schemes in smart grid network. Secur Priv, 2(2): e62.
12. Yang Y, McLaughlin K, Littler T, et al.Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in smart grid SCADAsystems. 2012.
13. Lan T., Wang W., Huang G. M. 2017. False data injection attack in smart grid topology control: Vulnerability and countermeasure. IEEE Power & Energy Society General Meeting. IEEE; 1-5.
14. Yan Y,Qian Y, Sharif H, Tipper D. 2012. A survey on cyber security for smart grid communications. IEEE Commun Surv Tutor, 14(4):998-1010.
15. Bou-Harb E., Fachkha C., Pourzandi M., Debbabi M., Assi C. 2013. Communication security for smart grid distribution networks. IEEE Commun Mag., 51(1):42-49.
16. Erkin Z., Troncoso-Pastoriza J. R., Lagendijk R. L., Pérez-González F. 2013. Privacy-preserving data aggregation in smart metering systems: An overview. IEEE Signal Process Mag., 30(2):75-86.
17. Alaba F. A., Othman M., Hashem I. A. T., Alotaibi F. 2017. Internet of things security: A survey. J Netw Comput Appl., 88:10-28.
18. NIST Smart Grid. 2010. Introduction to NISTIR 7628 guidelines for smart grid cyber security. Guideline., 1-20.
19. Guo H., Yongdong W., Chen H., Ma M. 2011. A batch authentication protocol for V2G communications. 2011 4th IFIP International Conference on New Technologies, Mobility and Security. IEEE;1-5.
20. Shor P. W. 1999. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Rev., 41(2):303-332.
21. Micciancio D., Goldwasser S. 2002. Complexity of Lattice Problems: A Cryptographic Perspective. Vol 671. Springer Science & Business Media.
22. Ajtai M. 1996. Generating hard instances of lattice problems. Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing. ACM: 99-108.

23. Van Tilborg H. C. A., Jajodia S. 2014. Encyclopedia of Cryptography and Security. Springer Science & Business Media.
24. Hoffstein J, Pipher J, Silverman J. H. 2008. An Introduction to Mathematical Cryptography. Vol 1. Springer.
25. Chaudhary R., Aujla G. S., Kumar N., Zeadally S. 2018. Lattice-based public-key cryptosystem for internet of things environment: Challenges and solutions. IEEE Internet Things J., 6(3):4897-4909.
26. Goldreich O, Goldwasser S, Halevi S. 1997. Public-key cryptosystems from lattice reduction problems. Annual International Cryptology Conference. Springer: 112-131.
27. Goldreich O., Goldwasser S., Halevi S. 1996. Collision-free hashing from lattice problems. IACR Cryptol ePrint Arch., 1996:9.
28. Khot S. 2005. Hardness of approximating the shortest vector problem in lattices. J ACM., 52(5):789-808.
29. Ajtai M., Dwork C. 1997. Apublic-key cryptosystem with worst-case/average-case equivalence. Proceedings of the twenty-ninth annual ACM symposiumon Theory of computing., 284-293.
30. Wang S. B., Zhu Y., Ma D., Feng R. Q. 2014. Lattice-based key exchange on small integer solution problem. SCIENCE CHINA Inf Sci., 57(11):1-12.
31. Lenstra A. K., Lenstra H. W., Lovász L. 1982. Factoring polynomials with rational coefficients. Math Ann., 261:515-534.
32. Hoffstein J., Lieman D., Pipher J., Silverman J. H. 1999. NTRU: A public key cryptosystem. NTRU Cryptosystems, Inc.
33. Regev O. 2009. On lattices, learning with errors, random linear codes, and cryptography. J ACM., 56(6):1-40.
34. Verbauwhede, Clercq R. D., Roy S. S., Vercauteren F. Ingrid. 2014. Efficient Software Implementation of Ring-LWE Encryption". Cryptology ePrint Archive.
35. Abdallah A. R., Shen X. S. 2014. A lightweight lattice-based security and privacy-preserving scheme for smart grid. IEEE Global Communications Conference.IEEE; 2014:668-674.
36. Abdallah A., Shen X. S. 2016. A lightweight lattice-based homomorphic privacy-preserving data aggregation scheme for smart grid. IEEE Trans Smart Grid., 9(1):396-405.
37. Chaudhary R., Aujla G. S., Kumar N., Das A. K., Saxena N., Rodrigues J. J. P. C. 2018. LACSYS: Lattice-based cryptosystem for secure communication in smart grid environment. 2018 IEEE International Conference on Communications (ICC). IEEE;2018:1-6.
38. Abdallah A. R., Shen X. S. 2014. Light weight lattice-based homomorphic privacy-preserving aggregation scheme for home area networks. Sixth international conference on wireless communications and signal processing (WCSP). IEEE; 2014:1-6.
39. Agarkar A. A., Agrawal H. 2019. LRSPPP: Light weight RLWE-based secure and privacy-preserving scheme for prosumer side network in smart grid. Heliyon., 5(3):e01321.
40. Darzi S., Akhbari B., Khodaiemehr H. 2022. LPM2DA: a lattice-based privacy-preserving multi-functional and multi-dimensional data aggregation scheme for smart grid. Clust Comput., 25(1):263-278.
41. Gupta D. S. 2022. Amutual authentication and key agreement protocol for smart grid environment using lattice. Proceedings of the International Conference on Computational Intelligence and Sustainable Technologies. Springer; 2022:239-248.
42. Li C., Rongxing L., Li H., Chen L., Chen J. 2015. PDA: a privacy-preserving dual-functional aggregation scheme for smart grid communications. Sec. Commun. Networks., 8(15):2494-2506.
43. Qian J., Cao Z., Mengjie L., Chen X., Shen J., Liu J. 2021. The secure lattice-based data aggregation scheme in residential networks for smart grid. IEEE Internet Things J., 9:2153-2164.
44. Romdhane R. B., Hammami H., Hamdi M., Kim T. H. 209. At the cross roads of lattice-based and homomorphic encryption to secure data aggregation in smart grid. 15th International Wireless Communications &Mobile Computing Conference (IWCMC). IEEE; 2019:1067-1072.