2024 International Conference on Intelligent and Innovative Computing Applications (ICONIC)
7th-9th November 2024, Pearle Beach Resort & Spa, Flic en Flac, Mauritius
https://doi.org/10.59200/ICONIC.2024.021

Lightweight Scheme for Security and Privacy in Smart Grids Applications

Philani Khumalo*, Mohohlo Samuel Tsoeu and Katleho Moloi
Electronic Engineering Department, Steve Biko Campus,
Durban University of Technology, South Africa
philanipk@gmail.com*

Abstract
In the evolving landscape of smart grid technology, the need for robust, efficient, and scalable security solutions is paramount. This paper presents a lightweight cryptographic scheme based on the Nth Degree Truncated Polynomial Ring (NTRU) designed to enhance security and privacy in smart grid applications. Unlike traditional cryptographic methods that may be computationally intensive and resource-consuming, our proposed NTRU-based scheme offers a quantum-resistant solution with minimal overhead, making it ideal for deployment in resource-constrained environments such as smart meters and distributed sensors. The scheme provides strong protection against various cyber threats, ensuring data confidentiality, integrity and authenticity while maintaining high operational efficiency. Through comprehensive analysis and comparison with existing schemes, we demonstrate the effectiveness of our approach in balancing security with the practical demands of smart grid infrastructure. Our findings indicate that the NTRU-based scheme not only meets the stringent security requirements of smart grids but also preserves user privacy, making it a viable solution for future-proofing smart grid communications against emerging threats.

Keywords*:* AMR, smart grid; group authentication, smart meter, communication, protocol security and privacy

1. Introduction

The transformation of traditional power grids into smart grids (SGs) represents a pivotal shift in the way electricity is generated, distributed, and consumed. SGs leverage digital technologies and advanced communication systems to create a more efficient, reliable, and sustainable energy infrastructure. These grids incorporate features such as real-time monitoring, automated control systems, and Advanced Metering Infrastructure (AMI), which collectively enable better management of electricity demand, improved integration of renewable energy sources, and enhanced grid resilience. A typical SG architecture is shown in Figure 1.

However, the integration of these sophisticated technologies introduces a range of security threats that must be addressed for effective secure operation of SGs. The data collected by SGs including precise information about consumers' electricity usage patterns can reveal sensitive personal information. This raises significant privacy concerns, as unauthorised access or misuse of this data could compromise consumer privacy. In addition to privacy issues, SGs are susceptible to various security threats. The increased connectivity and reliance on digital systems make them vulnerable to cyber-attacks that could disrupt services, steal sensitive information, or even cause physical damage to infrastructure. Ensuring the integrity and reliability of the grid is paramount to preventing outages and maintaining continuous service. Effective access control mechanisms are also essential to ensure that only authorised personnel and systems can interact with critical infrastructure and data (Aweya & Al Sindi, 2013) and (Lévesque & Tipper, 2016).

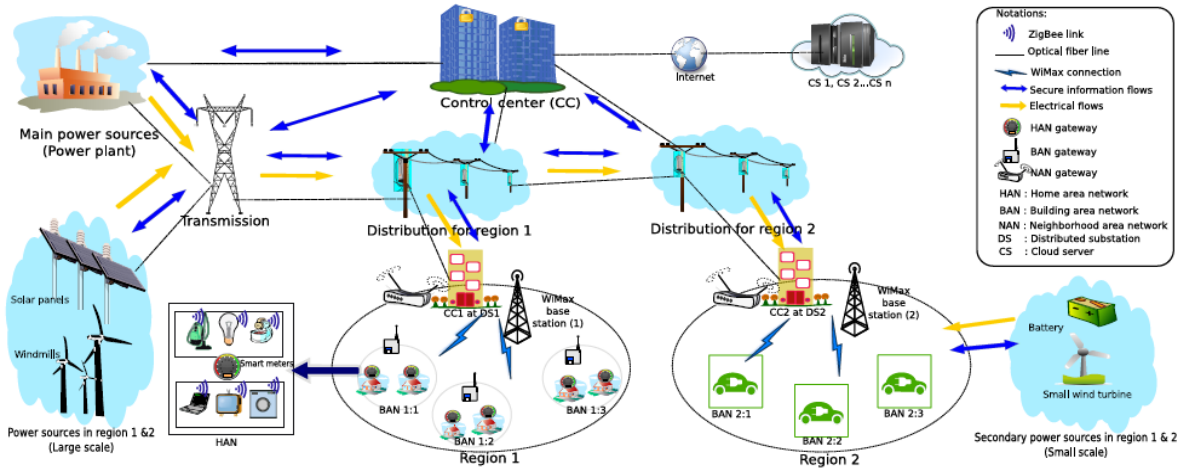

Figure 1. A Typical Smart Grid

2. Time synchronisation in Smart Grids

The power grid's increasing reliance on high-precision timing has made timing synchronisation the foundation for a robust system. The current voltage, angle of the phases, and power angle of a power system are time-reliant, highlighting the criticality of precise timing for stable and safe power grid operation. Relay protection, remote terminal units, energy management systems, digital power technique online precision systems, and wide area measurement systems all require highly accurate and synchronised timing information (Hasan et al., 2018). Global Position System (GPS) timing synchronisation has already been extensively used in various domains. Security and privacy concerns in time synchronisation such as signal jamming, spoofing and denial-of-service attacks are security threats on SG operations, grid stability and integrity investigated. We also explore the implications of compromised time synchronisation on SGs components, such as AMI and grid control systems (Moussa et al., 2016). and (Zhang, et al., 2013). The diagram in Figure 2 illustrates a Man-in-the-Middle (MiTM) attack.

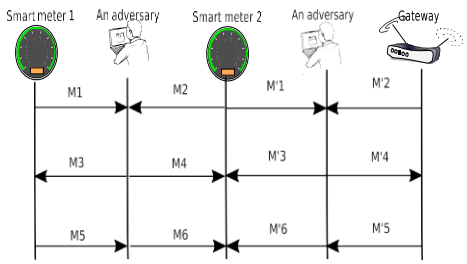

Figure 2: MiTM attack.

Cryptographic mechanisms, authentication protocols, and anti-jamming techniques to enhance the security are proposed. The effectiveness and limitations of these solutions are evaluated based on previous research identifying research gaps and real-world implementations. Additionally, alternative synchronisation sources, redundancy strategies, and backup systems are examined as means to mitigate the impact of security breaches (Han et al., 2013).

By integrating Information Communication Technology (ICT) technologies, a two-way communication channel is established, allowing for interactions between end users and utility operators. This mutual interaction results in enhanced operations and management of the SG system. This is achieved through more efficient real-time monitoring and control of electricity generation, distribution, and consumption within the system. The main objectives are as follows:

- **Integration of Renewable Generation**: Incorporate renewable energy generated by specific homes and isolated units into the power grid.
- **Real-time energy Monitoring**: Real-time monitoring of power consumption, effective billing, and accurate measurements.
- **Optimal Balancing of Demand and Energy Consumption**: Achieve optimal balance between the demand for power and the energy consumption by end users.
- **Effective Interaction between Utility and End Customers**: Interaction between utility operators and end customers, enabling seamless communication and collaboration.
- **Security Measures**: Guarding against and mitigating malicious attacks and other security threats to ensure the integrity and safety of the SG.

- **Autonomy in Management**: Provide a certain degree of autonomy in management to enhance the reliability of the SG operations.
- **Maximising Efficiency**: Efficiency of assets used within the SG system, optimising resource utilisation, and minimising wastage.

Duplex communication facilitates the utility operator's ability to remotely acquire energy consumption data from smart meters (SMs). However, this capability raises concerns about end-user privacy, as it may violate their privacy in terms of their habits and activities (Behrendt & Fodero, 2006; Zhao et al. 2018; Zhou et al. 2011).

3. Secure Time synchronisation

Secure time synchronisation is crucial for ensuring accurate and reliable communication. Figure 4 shows how time can be compromised by spoofing.

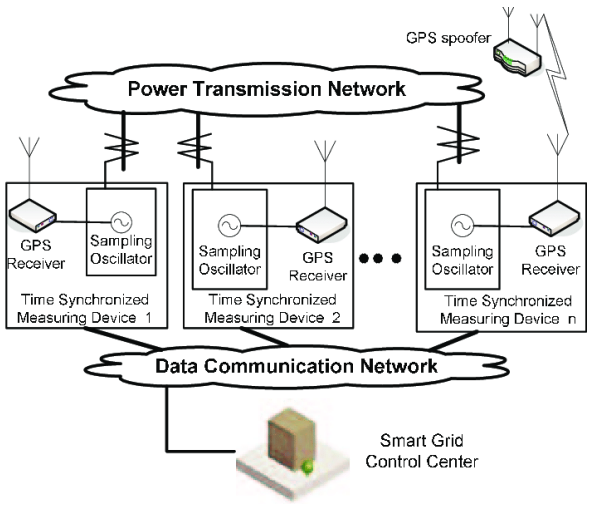

Figure 3: Time Synchronisation Spoofing**.**

To enhance the security of time synchronisation, the following measures can be taken:

- **Encryption**: Introduce encryption mechanisms to protect the time synchronisation signals transmitted between GPS and ground stations. To prevents tampering with the synchronised data.
- **Authentication**: Use secure authentication protocols to protect the identity and integrity of the time synchronisation process.
- **Secure Time Transfer Protocols**: Protocols such as Network Time Protocol over Secure Socket Layer or Transport Layer Security, to establish encrypted and authenticated channels for time synchronisation.

It is important to approach time synchronisation security holistically, considering both technical and physical security measures. The specific implementation details will depend on the time system and infrastructure in use (Ye, 2011) and (Meloni & Atzori, 2017).

4. Cryptographic approach

Cryptographic methods, offers a potential solution to address privacy threats in the SG. Numerous studies have investigated these methods and commonly classify them into three categories: public key, symmetric key, and unkeyed primitives.

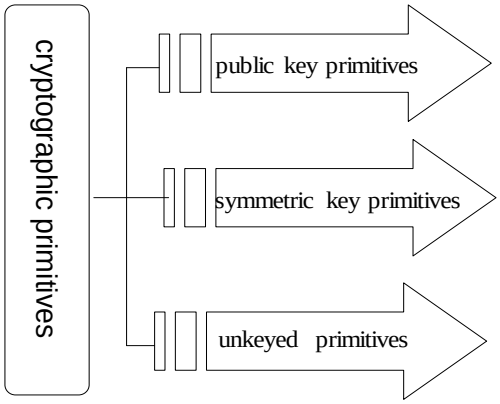

Figure 4: Classification of Cryptographic Primitives

The taxonomy of cryptographic primitives is illustrated in Figure 5. Within the category of public key, asymmetric cryptography is employed, which utilises both public keys. It is essential to maintain the privacy of the private key while securely distributing the public key through protected channels. Symmetric key primitives, also known as private key primitives, involve the use of the one key by both parties, the sender and receiver. This is why they are referred to as symmetric key primitives or private key cryptography, as the key used is symmetrical in nature. Unkeyed primitives rely on hash functions and random sequences.

A. Privacy preservation and cryptographic approaches

To preserve privacy in SGs, techniques such as data aggregation, anonymisation, and perturbation are widely implemented. These techniques are often combined with multi-party computation or homomorphic ciphering and deciphering to ensure total privacy preservation while meeting security requirements.

In multi-party computation-based approaches, individual entities collaboratively generate cryptographic operations using their private data but not sharing content with other entities. Homomorphic encryption-based techniques allow mathematical operations on ciphered text, enabling entities to execute computations except for accessing the information contents.

Anonymisation techniques replace true entity information with pseudonyms, making it difficult to link an individual's real name to power usage-related data. Hybrid methods, which blend more than one primary techniques, result in even stronger privacy preservation techniques. Time perturbation techniques fall into this category. Extensive research has been conducted on privacy-preserving schemes in SG environments. A lightweight security and privacy data aggregation scheme utilising bilinear pairing and one-time masking methods is proposed by (Alharbi & Lin, 2012). This scheme conceals an entity's identity while maintaining lightweight aggregation. Several entities are involved, including multiple Home Area Networks (HANs) within the equivalent Building Area Network (BAN), the BAN-Gateway, and Control Centre (CC). The scheme comprises three phases:

a) At the initial stage, the CC calculates the necessary bilinear and two hash functions. It retains one key as the master private key and distributes the other as the public key. The HANs and the BAN-Gateway register with the CC and are given private keys to set up static communication keys.
b) The data aggregation phase involves authentic HANs receiving time-stamped request data from the BAN-Gateway.
c) Through the aggregation phase, specific HANs aggregate energy consumption messages and mask them using their assigned static key and a one-time mask. The masked messages are sent to the BAN-Gateway, which performs verifications and validations before securely sending the messages to the CC. The CC verifies and authenticates the received messages. This scheme effectively prevents security vulnerabilities but may present challenges in key management.

In the paper by Abdallah and Shen (2018), a homomorphic scheme is proposed, where a spanning tree protocol is shaped to secure customer utilisation data. The collector serves as the root node, and all communications between nodes are encrypted. The aggregation route links all the SMs in the designated area, with energy consumption data being aggregated upward along the tree structure. Intermediary SMs cannot read the message contents, ensuring complete confidentiality. However, this scheme lacks proper message auditing, making data forgery possible.

Similarly, the privacy and security preserving aggregation Endpoint Protection Platform EPPA scheme proposed by Lu et al. (2012) employs homomorphic algorithm using identity-based signatures. These keys are then shared non-interactively among the entities involved. It is important to note that this scheme generates new session keys within the same session after each timeout period. Table 1 provides a list of similar schemes.

Table 1: Privacy preservation and cryptographic schemes

Endpoint Protection Platform (EPPA) scheme	Abdallah and Shen (2017); Gope and Sikdar (2018); Li (2014); He et al. (2017)
Multi-party Computation-Based Schemes	Elgamal (1985); Huang et al. (2011); Melchor et al. (2008); Thoma et al. (2013).
Anonymity Based Schemes	Efthymiou and Kalogridis (2010); Cheung et al. (2011); Hajy Mahdizadeh et al. (2013); Mustafa (2017)
Hybrid Based Schemes	Diao et al. (2015); Hwang et al. (2011); Mustafa et al. (2019); Ullah et al. (2017)
Identity and Attributes Based Schemes	Katti et al. (2013); Li et al. (2014); Saxena and Soh (2003).
Ciphertext-Policy Attribute-Based Encryption (CP-ABE)	Ma et al. (2014); Shelke and Kenny (2018).

These references delve into different approaches and techniques for privacy-preserving aggregation in SG environments.

4. Lightweight Scheme for Smart Grid

A. Privacy and Security

Based on the preceding the literature survey, it is proposed to analyse a lightweight aggregation on data approach that ensures both privacy and confidentiality. The focus of this approach is on forecasting power consumption demands for a specific neighbourhood. Given that most attacks tend to occur during data transmission across the ICT subsystem, our approach aims to limit such attacks by forecasting power consumption demands and only establishing connections with the CC when changes are necessary. Our goal is to design a scheme that satisfies all privacy objectives, is robust and lightweight. Additionally, we aim to minimise both communication and computational overheads.

NTRU, known for its quantum-resistant encryption, can be adapted to enhance privacy in SGs applications through several mechanisms:

- **Data Confidentiality**: NTRU encrypts data to ensure only authorised users can access it, and its quantum resistance safeguards against future threats from quantum computing.
- **Anonymity and Pseudonymity**: NTRU supports anonymous communication by using pseudonyms, preventing user data from being traced back to individuals.
- **Data Integrity and Authenticity**: NTRU can generate digital signatures and provide authenticated encryption, ensuring data is both confidential and unaltered.
- **Secure Multi-Party Computation (SMPC)**: NTRU allows multiple parties to collaboratively compute functions without revealing private inputs, preserving user privacy.
- **Obfuscation Techniques**: By integrating with homomorphic encryption, NTRU enables operations on encrypted data without decryption, protecting privacy during data processing and aggregation in SGs.

Figure 5 illustrates the BANs scheme connect to the CC via the accessible NAN. A specific inhabited area, in SGs and has several *BANs*= {*BAN_ (1,) BAN_2, BAN_m*}. The BANs is not link direct to the *CC*, instead via an accessible *NAN* grid. The NAN simply transmits data to BANs and CCs.

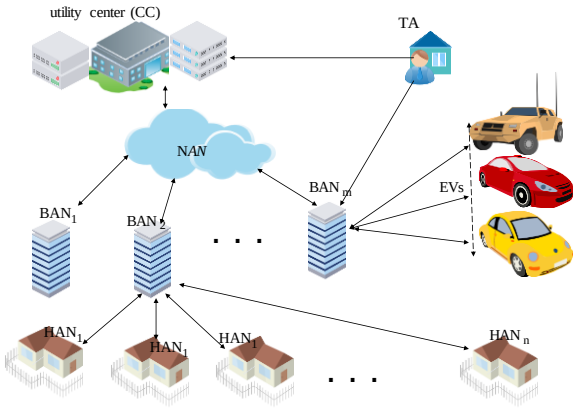

Figure 5: Time scheme's model illustration

The BANs are presumed to be non-computational resources constrained. The BAN It interconnects several HANs on the network,

$$HANs = \{HAN_1, HAN_2, \ldots HAN_n\}. \quad (1)$$

A typical HAN represents a solo house and will hence include various domestic electrical appliances. A TA assigns IDs to each SM.

B. Model requirements and design objectives

To safeguard against potential threats from attackers or adversaries, we must ensure the privacy of end users' personal information. Unauthorised access to customers' personal data, energy consumption details, and usage trends must be strictly prohibited. To further enhance end users' privacy, the actual IDs will not be disclosed to the CCs; this information will remain confidential and only accessible to the BANs. The integrity and confidentiality of messages are of utmost importance. We must protect the customer's energy usage details, trends, and related billing information from any attempts of malicious actions. Our priority is to ensure total data integrity and to promptly detect any suspicious activities in real-time. It is crucial to ensure the availability and accessibility of all key entities, especially the BAN servers, throughout the system. By doing so, we will effectively shield the system from potential denial-of-service (DoS) attacks, ensuring continuous and uninterrupted service.

1) **Design Objectives**

The proposed scheme aims to achieve the following objectives:

- Minimise of computational loads.
- Reduction or complete avoidance of communications overheads.
- Preservation of consumers' privacy.

To achieve our objectives, we will use NTRU, for ciphering and deciphering. The NTRU uses lattice-based cryptography for session data encryption and decryption. NTRU consists of two algorithms, namely NTRUEncrypt and NTRUSign (Zhang et al., 2019), and (So et al., 2010).

NTRUEncrypt is primarily employed as a lattice-based encryption algorithm for its public-key cryptosystem. It is based on the shortest vector problem in a lattice and mainly relies on the assumed difficulty of factoring certain polynomials in a truncated polynomial ring into a quotient of two polynomials with very small coefficients. By leveraging NTRU and its lattice-based cryptographic techniques, our scheme aims to achieve efficient computational processes, minimal communications overhead, and utmost privacy for consumers' data. The NTRU cryptosystem can be presented as follows:

If n is a power of 2; and Φ has n liner factors

$\Phi = rn + 1, R = Z[x]/\Phi, q(q = 1 \bmod 2n)$:

$$\Phi = \prod_{i<n} \Phi_i = \prod_{i<n}(x - \Phi_i)\ mod \quad \text{q} \tag{2}$$

$$R_q = \frac{R}{qR} = Z[r]_q / \Phi \tag{3}$$

where $R_q^x \in R_q$.

Referring to two equations 2 and 3, q is a prime number.

2) **Key generation**

The key creation technique is as follows:

For $n, q \in Z, p \in R_q^x$, $\sigma \in R.$; if we sample the value f' from a distinct Gaussian function $D_{Z^n,\sigma}$, where $\sigma > Poly(n) * q^{0.5+\varepsilon}$, for any value of $\varepsilon > 0$, we have:

$$(sk, pk) \cup R \times R_q^x \tag{4}$$

A secret key can be produced as follows:

$$f = p * f' + 1 \tag{5}$$

In the above equation $(f\ mod\ \ q) \in R_q^x$, and $f = 1\ mod\ \ p$. The secret value will range from g to $D_{Z^n,\sigma}$, subject to $(g\ mod\ \ q) \in R_q^x$.

We can then retrieve the secret key $sk = f$ and public key $pk = h$, where.

$$h = pg/f \in R_q^x \tag{6}$$

3) **Encryption**

Having a message M , a sender S generates dollar.

$$s, \varepsilon \leftarrow \overline{Y_\varepsilon} \tag{7}$$

and ciphertext as:

$$C = hs + p\varepsilon + M \in R_q \tag{8}$$

4) **Decryption**

Upon obtaining C the receiver R decode the data using the private key f as follows:

$$C' = f.C \in R_q \tag{9}$$

$$M = C'\ mod\ \ p \tag{10}$$

The NTRUSign, also known as the NTRU Signature Algorithm, is a digital signature system that follows public-key cryptography principles. It works by mapping a message to a random point in a 2N-dimensional space, where N is one of the parameters unique to NTRUSign. It then addresses the closest vector problem in a lattice similar to the one used in NTRUEncrypt.The NTRUSign employs the Goldreish Goldwasser-Halevi signature scheme.

In the NTRUSign scheme, we use the following parameters:

- *N*: Prime dimension.
- *q*: Modulus.
- *d*: Key size.
- *NB*: Authentication bound perimeter.

By using these parameters, NTRUSign enables secure digital signature generation and verification, providing an efficient and reliable method for ensuring the authenticity and integrity of messages. Also given two polynomials f, g which are both invertible modulo q, such that their coefficients $d + 1$ equal $1, d$, -1 and the remaining 0, we then have;

$$h = f^{-1} * g(mod \quad \text{q}) \tag{11}$$

Compute polynomial (F, G) such that:

$$f * G - g * F = q \quad (12)$$

5) **Key Generation**

For user i we choose a random polynomial $r_i \in R_q$ such that:

$$f_i = f * r_i, g_i = g * r_i \quad (13)$$
$$F_i = F * r_i^{-1} \quad (14)$$
$$G_i = G * r_i^{-1} \quad (15)$$

Ultimately the output is:

$$Sk_i = (f_i, g_i, F_i G_i) \quad (16)$$

6) **Signing in Process**

Upon S hashing a message M, to create a random vector (m_1, m_2) $(mod \quad q)$, and substituting m_1, m_2 in the following:

$$G_i * m_1 - F_i \circ m_2 = A_i + q * B_i \quad (17)$$

$$-g_i \cdot m_1 + f_i * m_2 = a_i + q * b_i \quad (18)$$

The signature on the message M is:

$$s_i = f_i * B_i + F_i b_i (mod \quad q) \quad (19)$$

7) **Signature Verification**

The verifying entity V also hashes the received message M to create (m_1, m_2) then calculates:

$$t_i = s_i * h (mod \quad q) \quad (20)$$

Subject to the following:

$$\|s_i = m_1\|^2 + \|t_i - m_2\|^2 \leq NB \quad (21)$$

Proposed Scheme

There are two phases to this concept. The first step is focused on initialisation, which ensures connectivity amongst the various entities involved in energy supply. The second phase involves message exchanges within the scope of a BAN.

1) **Phase 1**

The key steps are as follows:

a) Key generation

The TA will encryption and signing in keys for both CC and BAN as follows:

For the CC's secret key f_{cc} we have;

$$f_{cc} = p * f'_{cc} + 1 \text{ , } f_{cc} \mod q \in R_q^x \quad (22)$$

$$f_{cc} = 1 \bmod p \quad (23)$$

The TA also samples g_{cc} from the function $D_{Z^n,\sigma}$ such to satisfy:

$$g_{cc} \, mod \quad q \in R_q^x \quad (24)$$

After which it calculates:

$$h_{cc} p g_{cc} / f_{cc} \in R_q^x \quad (25)$$

Thus h_{cc} is the CCá public key whereas f_{cc} is the private key.

Similarly, for the BAN gateway its keys are computed as follows:

$$f_{bam} = p * f'_{ban} + 1 \quad (26)$$

Once again:

$$f_{cc} \, mod \quad q \in R_q^x \text{ and } f_{ban} = 1 \bmod p$$

The TA also samples g_{ban} from the function $D_{Z^n,\sigma}$ such to satisfy:

$$g_{ban} \, mod \quad q \in R_q^x \quad (27)$$

After which it calculates:

$$h_{ban} p g_{ban} / f_{ban} \in R_q^x \quad (28)$$

Thus h_{ban} is the CCá public key whereas f_{ban} is the private key.

b) **Signing Keys**

The TA a pair of polynomial f, g invertible module q. They both satisfy $d + 1$ of their roots equal 1, d roots equal -1 and the remainder equal 0. The public key for all end users is calculated according to:

$$h = f^{-1} * g (mod \, q) \quad (29)$$

It then computes (F, G), in which:

$$f * G - g * F = q \quad (30)$$

In order to generate the signing key for CC, it selects $r_{cc} \in R_q$ and setting:

$$f_{ccs} = f * r_{cc}, g_{ccs} = g * r_{cc} \quad (31)$$

It further computes,

$$F_{cc} = F * r_{cc}^{-1}, G_{cc} = G * r_{cc}^{-1} \quad (32)$$

Thus the CC's signing keys will be:

$$Sk_{cc} = (f_{cc}, g_{ccs}, F_{cc}, G_{cc}) \quad (33)$$

Correspondingly, the signing key for the BAN gateway is computed by first selecting $r_{ban} \in R_q$:

This is followed by:

$$f_{bans} = f * r_{ban}, g_{bans} = g * r_{ban} \quad (34)$$

and then,

$$F_{ban} = F * r_{ban}^{-1}, G_{ban} = G * r_{ban}^{-1} \quad (35)$$

Thus the BAN 's signing keys will be:

$$Sk_{ban} = (f_{ban}, g_{bans}, F_{ban}, G_{ban}) \quad (36)$$

2) **Generation of IDs**

Each SM is assigned an ID, $ID_1, ID_2, \ldots ID_n$. At regular intervals corresponding pseudo-IDs are generated according to,

$$ID_{new} = h(ID_{old}) \quad (37)$$

where h is a hash function.

3) **Electricity Demand Forecast**

This is in line with the forecasting function $g()$ and for each HAN, the forecasted demand is;

$$x_i = g(HAN_i) \quad (38)$$

Thus, for each cluster, the BAN aggregates the forecasted demands as follows,

$$x = \sum(x_1, x_2, \ldots, x_n) + \varepsilon \quad (39)$$

Where ε denotes a backup. Note that the backup is mainly derived from EVs;

$$C_{EV} = \sum C_i, 1 \leq i \leq N_{EV-expected} \quad (40)$$

Thus, we have:

$$\varepsilon = r * C_{EV} \quad (41)$$

subject to $0 < r < 1$ a scaling factor.

Note that during the initialisation phase, the BAN determines the ideal number of EVs necessary to work as energy buffers based on:

$$min \quad N_{EV}(m) \quad (42)$$

Subject to:

$$\varepsilon(m) \leq \sum_i C_i(m), i \in \{1, \ldots, N_{current}(m)\} \quad (43)$$

$$N_{EV}(m) \leq N_{current}(m), N_{current}(m) \in \{1, ., N_{max}\}$$

$$m \in \{1, \ldots, 100\} \quad (44)$$

4) **Power Consumption Agreement**

It is important to note that x is regarded as the aggregated demand per BAN by the CC. The CC is not aware of each individual HAN requirements in this regard. Instead, it deals with the collective demand from the BAN without specific knowledge of individual HAN demands.

5) **The Agreement Request Message**

This represents an agreement between the BAN and the CC. The process begins with the BAN sending an agreement request message, denoted as m_a to the CC. This request includes the requested amount x in encrypted form, where x is hashed to yield a secure representation $(x_1, x_2)(mod\ q)$.

$$G_{ban} * S_1 - F_{ban} * S_2 = A_{ban3} + qB_{ban3} \quad (45)$$

$$-g_{bans} * S_1 + f_{bans} * S_2 = a_{ban3} + q * b_{ban3} \quad (46)$$

Thus, the signature is:

$$S = s_{ban3} = f_{bans} * B_{ban3} + F_{ban} * b_{ban3}(mod\ q) \quad (47)$$

This will yield S and s_{ban3}. Consequently the BAN computes,

$$m_5 = S \| s_{ban3} \| T_{s_5} \| k_5 \quad (48)$$

After encrypting m_5 the BAN sets $s_5, \varsigma \leftarrow \overline{\gamma_\alpha}$ and also uses h_{cc} to generate:

$$m_b = h_{cc} s_5 + p\varsigma_5 + m_5 \in R_q \quad (49)$$

At the CC, f_{cc} is used to decrypt m_b. $ban3$s is also verified, so is the validity of the time stamp.

If needed, the BAN can adjust the requested power using the following algorithm:

Table 2: BAN Algorithm

1.	**BAN Electricity Share Adjustment Procedure**
2.	x : **The xed demand for BAN**
3.	y : **The current actual demand for BAN**
4.	z : **The EV remaining capacity**
5.	$\beta : \beta = \|x - y\|$: **The dierence between x and y**
6.	**If** $(x > y \,\&\, \beta < z)$ **then;**
7.	$\beta \leftarrow EV_{battery}$
8.	**else if** $(x < y\beta\text{^} > z)$ **then**
9.	$B - z \leftarrow CC$
10.	**else if** $(x < y \,\&\, \beta > z)$ **then**
11.	$\phi - z \rightarrow CC$
12.	**end if**

6) **Protocol Evaluation**

The scheme's analysis consists of two main parts: an assessment of its security and an evaluation of its performance.

D. Security Analysis

The proposed approach aims to protect end users' privacy, associated data (especially billing), and entities while also offering adequate guarantees of confidentiality, integrity, availability, authenticity, and responsibility. We shall now compare these elements to the scheme's capabilities.

1) *Preservation of individual end-user privacy*

The scheme takes extensive measures to maintain privacy regarding an individual's private information. This includes concealing the end user's ID, location, and power consumption patterns. Despite the possibility of the CC being a target for attacks by adversaries, it does not possess the end user's details in this scheme. Only the BAN has access to this information. Furthermore, the CC cannot derive precise individual power consumption invoices because the BAN provides such information in aggregated form for all linked users. Furthermore, all messages, including those from the BAN to the CC, are encrypted, and only the CC has the necessary decryption key. Messages sent from HANs to the BAN are also encrypted.

2) *Guaranteed messages' confidentiality*

The CC and BAN preserve confidentiality by exchanging public keys. The same applies to messages sent between HANs and BAN gateways. The TA assigns IDs to SMs to prevent MiTM attacks while also concealing the SMs' true identity. Furthermore, the use of signing signatures makes it harder to decrypt intercepted messages, as only an authority with the appropriate signatures may do so.

3) *Integrity of exchanged messages*:

To protect the integrity of communications transferred between the CC and BANs, they must be hashed and signed using a private key. SMs integrate energy consumption-related communications with their individual IDs, hash the resulting data, and send it to BANs. The BANs can validate the details of the SMs because they have the necessary information in their databases. The database information is secure because the stored data is encrypted using a private key known only to the TA.

4) *Authentication guarantees*:

Public keys are used to authenticate entities such as the CC and BAN. By encrypting, formulating, and encrypting the messages, the entities authenticate their messages.

5) *Resource availability*:

BAN gateways are protected against DoS attacks. The number of connections to a given BAN is strictly limited, and any unauthorised attempts will be immediately detected.

6) *Accountability*

Individuals have the option to validate and verify their bills at the local BAN, as it possesses the necessary information, including prices. Additionally, the expected volume of message exchanges between customers and BANs is relatively low, making it challenging for adversaries to intercept messages. The NTRU cryptosystem offers an added safeguard against

adversaries gaining any knowledge from intercepted data. In essence, the scheme effectively upholds customer privacy.

E. Performance Evaluation

The scheme's effectiveness is assessed in the following subsections.

1) *Communication overheads*:
When creating protocols and schemes that involve communication, it is critical to consider the levels of communication overhead. Communication overhead is defined as the extra data bits in headers, message trailer flags, and other elements that aid in addressing flow control, error correction, and receiver-side delineation. In the proposed protocol design, relatively few messages are transmitted between the various parties. This is due in part to message aggregation before being delivered as multi-party communications, as well as BANs' lack of active participation during the initialisation phase.

However, during the negotiation of the power-share agreement, only two messages are exchanged by both the CC and BAN. In the second phase, HANs only send demand messages if there is a sudden change in demand or power tariffs.

Figure 6 illustrates the communication overheads, including a comparison with traditional approaches, for different numbers of connections per BAN. The proposed scheme demonstrates a reduction in the number of exchanged messages and, consequently, communication overhead compared to traditional approaches.

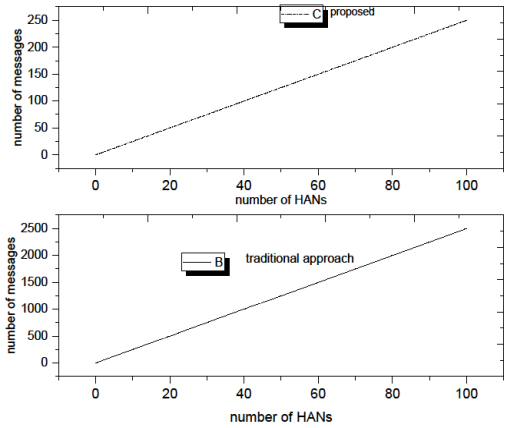

Figure 6: Comparisons of communication overheads (c) Proposed (b) Traditional

To further investigate the communication overhead loads, we explore different scenarios with varying numbers of demand messages in the following five cases:

- **Case I:** In this scenario, some of the HANs send one power demand message over a 24-hour period, while the rest do not send any requests at all.
- **Case II:** Each HAN sends one power demand message per 24-hour period.
- **Case III:** In this case, some HANs send two power demand messages each, some send one message, and the others do not send any messages over a 24-hour period.
- **Case IV:** Each HAN sends two power demand messages per 24-hour period.
- **Case V:** Each HAN sends three power demand messages per day.

Figure 7 illustrates the fluctuations in communication overhead within the proposed system, accounting for the five previously described scenarios. The data represents the number of messages exchanged among approximately 350 domain clusters, with each cluster comprising 120 HANs.

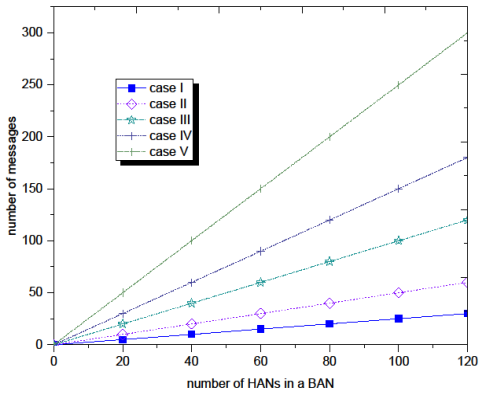

Figure 7: Communication overhead considering for various scenario cases

1) *Computational complexity*:
In simpler terms, computational overhead represents the extra burden or cost imposed on the system's resources to execute the intended functions and meet the targeted goals of the scheme effectively. Managing and minimising this overhead is crucial for optimising the scheme's performance and ensuring its overall effectiveness. In this scenario, the computational times for four essential operations are taken into consideration: signing (T_S), verification (T_V), encryption (T_E), and decryption (T_D).

During the initialisation phase, both the CC and the BAN perform a single ciphering operation and a single decryption. Additionally, they execute a one-time signing and verification process. This equates to a computational time of:

$$C_1 = 2 \times [T_E + T_D + T_S + T_V] \quad (50)$$

In the upcoming phase (Phase II), a HAN is expected to engage in message exchanges to request additional power allocations. During this process, the HAN will perform a single encryption operation on the request message, which will subsequently be decrypted by the associated entity on the receiving end. This equates to $T_E + T_D$ per data message. The likely that tariffs might change and hence necessitates communication between CC and BAN, thus the computation time is $2x\ T_s + T_v$.

If the number of $HANs$ is m, the total calculation time becomes,

$$m(T_E + T_D) + (2T_S + (m+1)T_V) \quad (51)$$

In the next phase, i.e., billing, the message is sent to CC from ^{BAN} this requiring one encryption, one decryption, one sign and one authentication process.

Using the method by (Line, M. B., et al., 2011).

$$C_{proposed} = 90 \times [T_E + T_D + T_S + T_V] \quad (52)$$

$$C_{traditioal} = 810 \times [T_E + T_D + T_S + T_V] \quad (53)$$

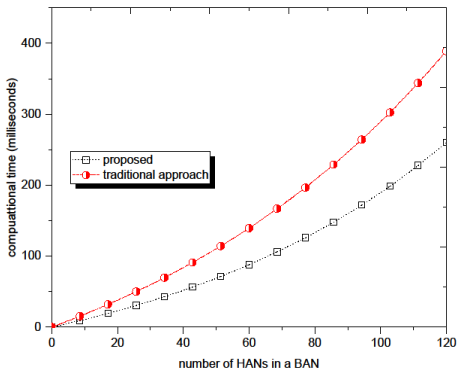

Figure 8: Computation overhead: Traditional vs. proposed scheme

Figure 8 illustrates the aggregate computational times of our proposed scheme. The graph shows that as of the number of HANs increases that results in increases in computational time. However, when compared to alternative approaches, the increase in computational time for our proposed scheme is significantly lower. This demonstrates that our scheme can execute quickly, even with limited computational resources, and it falls within the expected time frame for a fully-fledged SG network. Next, we analyse a worst-case scenario in which every entity in a cluster domain sends the maximum possible number of power demand messages. The computational times for this worst-case scenario are shown in Figure 9.

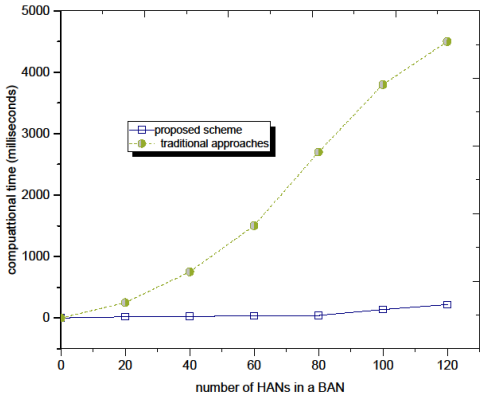

Figure 9: Computational times: Traditional vs. proposed

Once more, we compare the total computational times of the proposed scheme with those of traditional approach schemes. The proposed scheme significantly reduces computational overhead, resulting in much lower computational times compared to the traditional approaches.

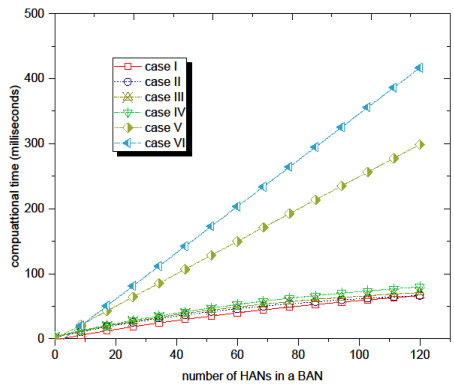

Figure 10: Computation Overheads Comparisons

There are five case scenarios (Case I, Case II, Case III, Case IV, and Case VI) that involve different numbers of power demand messages being sent by different entities over a 24-hour period. The scenarios are as follows:

- **Case I**: Some entities transmit a single power demand message throughout a 24-hour period, whereas others do not send any et al.
- **Case II**: Each entity sends a single power demand notification every 24 hours.
- In **Case III**, some entities send two power demand signals, others send one, while some do not transmit any over the 24-hour period.
- **Case IV**: Each entity sends a few power demand messages every 24 hours.
- **In Case VI**, each HAN transmits as many power demand alerts as possible within 24 hours.

Despite this increase in computational complexity, the proposed scheme guarantees privacy, while it simultaneously minimises computational and communication overhead levels.

1. Comparison of NTRU and Other Security Schemes and Analysis in Smart Grid Applications

In the context of Smart Grid applications, the selection of a suitable cryptographic scheme is crucial for ensuring secure, efficient, and scalable operations. Below is a comparison of NTRU (Nth Degree Truncated Polynomial Ring) with other common security schemes used in SGs, such as RSA (Rivest-Shamir-Adelman), ECC (Elliptic Curve Cryptography), and AES (Advanced Encryption Standard).

1. NTRU (Nth Degree Truncated Polynomial Ring)

- *Security:*

NTRU is based on the hardness of lattice problems, making it resistant to both classical and quantum attacks. This gives it a long-term advantage, particularly as quantum computing becomes more feasible. Unlike RSA and ECC, which are vulnerable to quantum attacks, NTRU is considered secure against quantum adversaries.

- *Performance:*

NTRU offers efficient encryption and decryption operations with relatively low computational overhead, making it suitable for real-time Smart Grid applications.

NTRU typically has larger key sizes compared to ECC but smaller than RSA. However, it compensates for this with faster operations.

- *Scalability:*

NTRU is lightweight enough to be implemented in resource-constrained devices like SMs and sensors, which are common in SGs.

2. RSA (Rivest-Shamir-Adleman)

- *Security:*

RSA's security is based on the difficulty of factoring large integers, a problem that is solvable in polynomial time by quantum computers using Shor's algorithm, making RSA vulnerable to future quantum attacks.

- *Performance:*

RSA requires more computational power and time, especially for key generation and encryption/decryption processes, which can be a bottleneck in SGs.

RSA keys are significantly larger than those of ECC and NTRU, leading to higher storage and transmission costs.

- *Scalability:*

Due to its heavy computational requirements, RSA is less suitable for deployment in resource-constrained environments typical of SGs.

3. ECC (Elliptic Curve Cryptography)

- *Security:*

ECC offers strong security with much smaller key sizes compared to RSA, making it more efficient. However, it is still vulnerable to quantum attacks, though less so than RSA.

- *Performance:*

ECC provides high security with smaller key sizes, which results in faster computations and lower power consumption compared to RSA. This efficiency makes ECC suitable for many Smart Grid applications.

ECC keys are much smaller than those required for equivalent security levels in RSA, making it ideal for environments where bandwidth and storage are limited.

- *Scalability:*

ECC's efficiency and lower resource demands make it highly scalable and suitable for a wide range of devices within SGs.

4. AES (Advanced Encryption Standard)

- *Security:*

AES is a symmetric encryption algorithm, meaning the same key is used for both encryption and decryption. It is highly secure and efficient for bulk data encryption.

- *Performance:*

AES is very fast and efficient, making it ideal for real-time applications in SGs. However, it requires secure key management, which can be challenging in distributed systems.

- *Scalability:*

While AES is efficient, managing keys securely in a distributed Smart Grid environment can be complex, particularly because it requires a different key management system compared to public-key schemes like NTRU, RSA, or ECC.

7. Conclusion

The privacy and security issues in SGs, along with secure time synchronisation, were investigated, highlighting various attack scenarios that can compromise the privacy and security of end users. Ensuring privacy in SGs and maintaining time synchronisation protocols are critical requirements. Based on a literature survey, a lightweight data aggregation scheme is proposed. This scheme focuses on forecasting power consumption demands for specific neighbourhoods and aims to mitigate attacks occurring during data transmission across the ICT subsystem. The scheme ensures privacy and confidentiality, aiming to satisfy all privacy objectives while being robust and lightweight. Additionally, it strives to minimise both communication and computational overheads. Ensuring secure time synchronisation enhances the robustness of this protocol, as some adversaries exploit time synchronisation to inject malware. Securing time synchronisation inhibits and protects against data spoofing and cryptanalysis. Simulations have demonstrated the effectiveness of the proposed protocol. NTRU is more efficient and offers post-quantum security, making it a better choice for future-proofing SGs against quantum threats. RSA, while widely used, is less suitable due to its computational demands and vulnerability to quantum attacks. Both NTRU and ECC are efficient and scalable, but NTRU has the advantage of being quantum-resistant. ECC, with its smaller key sizes, remains very efficient and is currently more widely adopted, but its future security is a concern in the quantum era. While AES is extremely efficient for symmetric encryption, NTRU provides a public-key option with quantum resistance. AES is often used in combination with public-key schemes like NTRU for secure key exchange followed by symmetric encryption.

8. References

Abdallah, A., & Shen, X. (2017). Lightweight security and privacy preserving scheme for smart grid customer-side networks. *IEEE Transactions on Smart Grid, 8*(3), 1064-1074. https://doi.org/10.1109/TSG.2015.2463742

Abdallah, A., & Shen, X. S. (2018). A lightweight lattice-based homomorphic privacy-preserving data aggregation scheme for smart grid. *IEEE Transactions on Smart Grid, 9*(1), 396-405. https://doi.org/10.1109/TSG.2016.2553647

Alharbi, R., & Lin, X. (2012). LPDA: A lightweight privacy-preserving data aggregation scheme for smart grid. In *2012 International Conference on Wireless Communications and Signal Processing (WCSP)* (pp. 1-6). IEEE. https://doi.org/10.1109/WCSP.2012.6542880

Aweya, J., & Al Sindi, N. (2013). Role of time synchronization in power system automation and smart grids. In *2013 IEEE International Conference on Industrial Technology (ICIT)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICIT.2013.6505864

Behrendt, K., & Fodero, K. (2006). *The perfect time: An examination of time-synchronization techniques.* Schweitzer Engineering Laboratories, Inc.

Cheung, J. C. L., Chim, T. W., Yiu, S. M., Li, V. O. K., & Hui, L. C. K. (2011). Credential-based privacy-preserving power request scheme for smart grid network. In *2011 IEEE Global Telecommunications Conference - GLOBECOM 2011* (pp. 1-5). IEEE. https://doi.org/10.1109/GLOCOM.2011.6134566

Diao, F., Zhang, F., & Cheng, X. (2015). A privacy-preserving smart metering scheme using linkable anonymous credential. *IEEE Transactions on Smart Grid, 6*(1), 461-467. https://doi.org/10.1109/TSG.2014.2358225

Efthymiou, C., & Kalogridis, G. (2010). Smart grid privacy via anonymization of smart metering data. In *2010 First IEEE International Conference on Smart Grid Communications* (pp. 238-243). IEEE.

https://doi.org/10.1109/SMARTGRID.2010.5622050

Elgamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, *31*(4), 469-472. https://doi.org/10.1109/TIT.1985.1057074

Gope, P., & Sikdar, B. (2018). An efficient data aggregation scheme for privacy-friendly dynamic pricing-based billing and demand-response management in smart grids. *IEEE Internet of Things Journal*, *5*(4), 3126-3135. https://doi.org/10.1109/JIOT.2018.2833863

Hajy Mahdizadeh Zargar, S., & Yaghmaee, M. H. (2013). An efficient privacy-preserving scheme of high frequency reports for secure smart grid communications. In *ICCKE 2013* (pp. 368-373). IEEE. https://doi.org/10.1109/ICCKE.2013.6682824

Han, C., Zhang, W., Liu, X., & Jiang, C. (2013). Time synchronization and performance of BeiDou satellite clocks in orbit. *International Journal of Navigation and Observation*, *2013*, 1-9. https://doi.org/10.1155/2013/718083

Hasan, K. F., Feng, Y., & Tian, Y. (2018). GNSS time synchronization in vehicular ad-hoc networks: Benefits and feasibility. *IEEE Transactions on Intelligent Transportation Systems*, *19*(12), 3915-3924. https://doi.org/10.1109/TITS.2018.2793303

He, D., Kumar, N., Zeadally, S., Vinel, A., & Yang, L. T. (2017). Efficient and privacy-preserving data aggregation scheme for smart grid against internal adversaries. *IEEE Transactions on Smart Grid*, *8*(5), 2411-2419. https://doi.org/10.1109/TSG.2017.2720159

Huang, Y., Lin, C., & Leu, F. (2011). Verification of a batch of bad signatures by using the matrix-detection algorithm. In *2011 First International Conference on Data Compression, Communications and Processing* (pp. 299-306). IEEE. https://doi.org/10.1109/CCP.2011.46

Hwang, J. Y., Lee, S., Chung, B., Cho, H. S., & Nyang, D. (2011). Short group signatures with controllable linkability. In *2011 Workshop on Lightweight Security & Privacy: Devices, Protocols, and Applications* (pp. 44-52). IEEE. https://doi.org/10.110

Katti, R. S., Sule, R., & Kavasseri, R. G. (2013). WiP abstract: Multicast authentication in the smart grid with one-time signatures from sigma-protocols. In *2013 ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)* (p. 239). IEEE.

Lévesque, M., & Tipper, D. (2016). A survey of clock synchronization over packet-switched networks. *IEEE Communications Surveys & Tutorials*, *18*(4), 2926-2947. https://doi.org/10.1109/COMST.2016.2582499

Li, H., Lin, X., Yang, H., Liang, X., Lu, R., & Shen, X. (2014). EPPDR: An efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid. *IEEE Transactions on Parallel and Distributed Systems*, *25*(8), 2053-2064. https://doi.org/10.1109/TPDS.2013.124

Li, Y. et al. (2014). Study on the remote communication technology in the construction of power user electric energy data acquire system. In *2014 China International Conference on Electricity Distribution (CICED)* (pp. 43-46). IEEE. https://doi.org/10.1109/CICED.2014.6991660

Line, M. B., Tøndel, I. A., & Jaatun, M. G. (2011). Cyber security challenges in smart grids. In *2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies* (pp. 1-8). IEEE. https://doi.org/10.1109/ISGTEurope.2011.6162695

Lu, R., Liang, X., Li, X., Lin, X., & Shen, X. (2012). EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications. *IEEE Transactions on Parallel and Distributed Systems*, *23*(9), 1621-1631. https://doi.org/10.1109/TPDS.2012.86

Ma, T., Jiang, Y., Wen, H., Wu, B., Guo, X., & Chen, Z. (2014). Physical layer assist mutual authentication scheme for smart meter system. In *2014 IEEE Conference on Communications and Network Security* (pp. 494-495). https://doi.org/10.1109/CNS.2014.6997521

Melchor, C. A., Castagnos, G., & Gaborit, P. (2008). Lattice-based homomorphic encryption of vector spaces. In *2008*

IEEE International Symposium on Information Theory (pp. 1858-1862). IEEE. https://doi.org/10.1109/ISIT.2008.4595310

Meloni, A., & Atzori, L. (2017). The role of satellite communications in the smart grid. *IEEE Wireless Communications*, *24*(2), 50-56. https://doi.org/10.1109/MWC.2017.1600378

Moussa, B., Debbabi, M., & Assi, C. (2016). Security assessment of time synchronization mechanisms for the smart grid. *IEEE Communications Surveys & Tutorials*, *18*(3), 1952-1973. https://doi.org/10.1109/COMST.2016.2539167

Mustafa, M. A., Cleemput, S., Aly, A., & Abidin, A. (2017). An MPC-based protocol for secure and privacy-reserving smart metering. In *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)* (pp. 1-6). IEEE. https://doi.org/10.1109/ISGTEurope.2017.8260202

Mustafa, M. A., Cleemput, S., Aly, A., & Abidin, A. (2019). A secure and privacy-preserving protocol for smart metering operational data collection. *IEEE Transactions on Smart Grid*, *10*(6), 6481-6490. https://doi.org/10.1109/TSG.2019.2906016

Saxena, A., & Soh, B. (2003). A new paradigm for group cryptosystems using quick keys. In *The 11th IEEE International Conference on Networks, 2003. ICON2003* (pp. 385-389). IEEE. https://doi.org/10.1109/ICON.2003.1266221

Shelke, V. M., & Kenny, J. (2018). Data security in cloud computing using hierarchical CP-ABE scheme with scalability and flexibility. In *2018 International Conference on Smart City and Emerging Technology (ICSCET)* (pp. 1-5). IEEE. https://doi.org/10.1109/ICSCET.2018.8537272

So, H. K., Kwok, S. H. M., Lam, E. Y., & Lui, K. (2010). Zero-configuration identity-based signcryption scheme for smart grid. In *2010 First IEEE International Conference on Smart Grid Communications* (pp. 321-326). IEEE. https://doi.org/10.1109/SMARTGRID.2010.5622061

Thoma, C., Cui, T., & Franchetti, F. (2013). Privacy preserving smart metering system-based retail level electricity market. In *2013 IEEE Power & Energy Society General Meeting* (pp. 1-5). IEEE. https://doi.org/10.1109/PESMG.2013.6672616

Ullah, S., Khan, E., Ullah, S., & Ali, W. (2017). A light-weight secret key-based privacy-preserving technique for home area networks in smart grid. In *2017 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD)* (pp. 895-899). IEEE. https://doi.org/10.1109/FSKD.2017.8393395

Ye, S. (2011). Beidou time synchronization receiver for smart grid. *Energy Procedia*, *12*, 37-42. https://doi.org/10.1016/j.egypro.2011.10.007

Zhang, Y., Li, J., & Yan, H. (2019). Constant size ciphertext distributed CP-ABE scheme with privacy protection and fully hiding access structure. *IEEE Access*, *7*, 47982-47990. https://doi.org/10.1109/ACCESS.2019.2909272

Zhang, Z., He, L., & Wei, X. (2013). Time synchronization attack in smart grid: Impact and analysis. *IEEE Transactions on Smart Grid*, *4*(1), 87-98. https://doi.org/10.1109/TSG.2012.2217507

Zhao, Y., Cao, J., & Li, Y. (2018). An improved timing synchronization method for eliminating large doppler shift in LEO satellite system. In *2018 IEEE 18th International Conference on Communication Technology (ICCT)* (pp. 1030-1035). IEEE. https://doi.org/10.1109/ICCT.2018.8600084

Zhou, S., Liu, X., Li, Z., & Zhou, W. (2011). Orbit determination and time synchronization for a GEO/IGSO satellite navigation constellation with regional tracking network. *Science China Physics, Mechanics, and Astronomy*, *54*, 1089-1097. https://doi.org/10.1007/s11433-011-4395-5