Heliyon

ELSEVIER

Received:
19 September 2018
Revised:
10 February 2019
Accepted:
1 March 2019

Cite as: Aarti Amod Agarkar, Himanshu Agrawal. LRSPPP: lightweight R-LWE-based secure and privacy-preserving scheme for prosumer side network in smart grid. Heliyon 5 (2019) e01321. doi: 10.1016/j.heliyon.2019.e01321

LRSPPP: lightweight R-LWE-based secure and privacy-preserving scheme for prosumer side network in smart grid

Aarti Amod Agarkar [a,*], **Himanshu Agrawal** [b]

[a] *Symbiosis International (Deemed) University, Lavale, Mulshi Taluka, Pune, Maharashtra, 412115, India*

[b] *Department of Computer Science and Information Technology, Symbiosis Institute of Technology, Symbiosis International (Deemed) University, Lavale, Mulshi Taluka, Pune, Maharashtra, 412115, India*

[*] Corresponding author.

E-mail address: pratibha26@gmail.com (A.A. Agarkar).

Abstract

In recent years, researchers have made tremendous progress to address an important question of how to provide security and privacy in Internet of Things systems. Privacy protection refers to safeguarding leakage of private information of the customers. In the context of Smart Grid, majority of the studies are based on addressing consumer side privacy. A recent research work has revealed that consumer side network has evolved into prosumer side network. Prosumer refers to consumer and producer, which means a dual role of a customer in the smart grid network. In this paper, we attempt to address the security and privacy issues at the prosumer side of smart grid network. Our work is different from the previous works in two ways. The paper proposes a lightweight encryption based privacy preservation scheme; Lightweight R-LWE-based Secure and Privacy-Preserving Scheme for Prosumer side network (LRSPPP). In LRSPPP, a new messaging scheme is defined which effectively minimizes the number of messages thus making it lightweight. Furthermore, the proposed privacy preservation scheme is using Learning With Errors over Rings (R-LWE) lattice

https://doi.org/10.1016/j.heliyon.2019.e01321

cryptography. There is no previous evidence of use of R-LWE based encryption for prosumer's privacy protection in smart grid. The security and performance analysis shows that the LRSPPP is superior compared to three other existing schemes.

Keywords: Computer science, Electrical engineering

1. Introduction

Security and Privacy preservation are two important research challenges in Internet of Things (IoT) applications. Customers' private information is seamlessly collected for further analytics. Smart Grid (SG) is one of the IoT applications, where customers' electricity consumption information is used for balancing production and consumption of the electricity. Nowadays, role of consumers is twofold. Consumers of electricity excels as consumers and producers which are referred as prosumers. Rathnayaka et al. (2014) introduced goal oriented Prosumer Community Groups (PCG) to manage the communication between prosumers. As shown in Fig. 1, prosumers are divided into PCGs considering prosumers behavior. Each PCG is controlled by Community Gateway (CG) which further communicates with Prosumer Community Coordinator (PCC). Clustering of these prosumers depends on the goals defined by prosumers. Goal describes the decisions of prosumers regarding profit, amount of electricity generation, sources of electricity generation, and other infrastructure related goals; such as reduction in greenhouse emission.

Given the prosumer scenario, which is primarily meant to automate and upgrade the conventional utility grid through introduction of prosumers in the network, it also

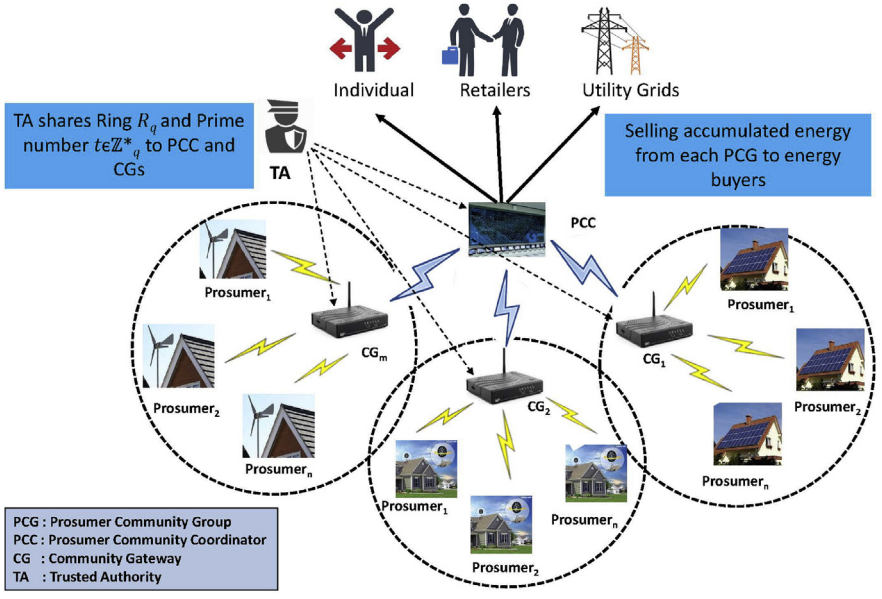

Fig. 1. Goal oriented prosumer community groups in smart grid network.

https://doi.org/10.1016/j.heliyon.2019.e01321

offers new set of cyber security challenges. As prosumer records details of its energy generation, an attacker can obtain information which defines energy generation behavior of a prosumer, thereby compromising privacy of customer. CG, which aggregates energy generation recorded by each prosumer, may be attacked by adversary to make the gateway un-available. Furthermore, an interception of a message may introduce a threat to the integrity of customer data, for instance billing data.

Considering security and privacy requirement of SG network, much of the work is done on consumer side. The proposed work focuses on security and privacy of prosumer side network. As compared to previous research studies, our work is different in two aspects. Our scheme provides lightweight solution for managing goal oriented PCGs. It limits number of messages between different parties involved in the network. The proposed scheme also guarantees the privacy of prosumers' information and satisfies security requirements of SG network. The scheme exploits Learning With Errors over Rings (R-LWE) based lattice cryptography for providing security. As per our understanding, this is the first attempt of leveraging R-LWE based cryptography on prosumer side network. The scheme is efficient in terms of communication as well as computation overhead. Our specific contributions are given as below:

- In this paper, we present an encryption based lightweight privacy preservation scheme using R-LWE lattice cryptography for prosumer side network. This is the first attempt on R-LWE based privacy protection scheme for prosumer side network.
- The proposed LRSPPP scheme is lightweight and results in reduced number of messages. Results show the merit of LRSPPP. LRSPPP shows less message communication overhead compared to ECC based lightweight scheme, RSA 512, and Elgamal scheme. Additionally, computation overheads of LRSPPP are also less compared to other three existing schemes.
- Furthermore, we conducted security analysis of the proposed scheme. Analytical results show that the proposed LRSPPP protects the privacy of the information exchanged by prosumers. The proposed scheme is also secured against Man-in-the-middle (MITM) attack, Denial of Service (DoS) and replay attack.

The paper is organized as follows. Section 2 presents related work. Section 3 focuses on basic definitions and background related to lattice cryptography, Learning With Error (LWE), NTRU and R-LWE cryptography. Section 4 presents the model of prosumer side network in smart grid. The proposed lightweight R-LWE-based secure and privacy-preserving scheme for prosumer side network is presented in Section 5. Section 6 discusses the security analysis of the proposed scheme. Results and discussion based on performance evaluation is presented in Section 7 followed by the conclusion in Section 8.

https://doi.org/10.1016/j.heliyon.2019.e01321

2. Related work

The design of security and privacy preservation schemes for SG have attracted many researchers in the recent years. In this section, the security and privacy preservation schemes are classified based on the cryptography methods employed.

First category of research work exploits homomorphic encryption algorithms where operation done on cipher text results in same operation on plain text without handling actual information. Homomorphic encryption can be further categorized as partial homomorphic encryption (PHE) and fully homomorphic encryption (FHE). Partial homomorphic encryption includes Paillier cryptosystem Paillier (1999) and ElGamal cryptosystem ElGamal (1985) based solutions. Fully homomorphic encryption scheme exhibits both additive and multiplicative homomorphism. Zhu et al. (2015) introduced an efficient privacy-preserving multidimensional aggregation scheme called PAS. The scheme is compared with an efficient and privacy-preserving aggregation scheme EPPA Lu et al. (2012) and shows marginally better performance. The disadvantage of the scheme is it defines more computation overhead at smart meter (SM) level which is practically not suitable as the computation capacity of SM is less. In the work presented in 2017, Guan and Si (2017) considered that SG has big data related to all SMs as large number of SMs are joining to SG. Privacy-preserving data aggregation scheme is invented for secret sharing and fault tolerance. Data aggregation is done using secret sharing scheme. The work considers that after every 15 minutes SM collects the data at its end, encrypt it and send to aggregator. It introduces large number of packets in the network which increases the communication overhead. Operation on cipher text at aggregator node defines more computation overhead compared to the operation on plain text. Busom et al. (2016) suggested a homomorphic encryption solution based on Elgamal encryption. The proposal is secure against a coalition composed of a misbehaving substation and some corrupted meters. Electricity consumption data from n SMs is aggregated to break the link between SM and its respective consumption data. Thus, even the substation gets compromised by attacker, the individual SM data is protected. Rahman et al. (2017) proposed a private and secure bidding protocol for incentive based demand-response systems using Elgamal Encryption and Schnorr Signature scheme. Various stages are introduced in the protocol which covers pre-processing stage, bidder registration, bidding key generation, bidding setup, bidding, bid verification, winner announcement, and incentive claim. The work is innovation but not lightweight. Also, comparison is not provided with other scheme. An incremental data aggregation scheme is presented by Hur et al. (2015). It utilizes symmetric homomorphic encryption to secure data in-between nodes. It exploits bilinear Pairings and Identity-based Sequential Aggregate Signature. SMs aggregates the energy utilization data without knowing any intermediate of final result. The scheme is facing scalability issue and require more computations if SG contains large number of SMs.

https://doi.org/10.1016/j.heliyon.2019.e01321

Tonyali et al. (2015) presented Smart-Vercauteren Scheme Perl et al. (2011) based FHE for preserving customer's privacy in SG network. The scheme is simulated in Network Simulator (NS3) for 802.11s-based mesh net-work. Compared to PHE, FHE introduces more data size and delay. The work is further extended for TCP protocol and presented the solution for packet reassembly for TCP during data aggregation process Tonyali et al. (2016). Tonyali et al. (2018) employed FHE with multiparty computation (MPC) where SM's data is concealed by encrypting it using FHE or computing its shares on randomly polynomial with MPC. The aggregated data/computed shares are aggregated by aggregator SMs in hierarchical fashion till the data reached to gateway node. The proposed protocol reduces the overhead of FHE and performance is near to Paillier cryptosystem. Zhao et al. (2014) used FHE for cloud computing security solution. Bos et al. (2017) work concentrated on forecasting of electricity requirement of customers. Authors proved that Ivakhnenko's group method of data handling is suitable for homomorphic computations and is better than neural network based forecasting approach.

The limitation of homomorphic schemes is they do not provide verifiable computing. Smart meters send the data to aggregator node and let aggregator node compute some operation on cipher text. Smart meter cannot verify that aggregator has done correct computation. To get this sort of guarantee, other solution is needed. Performance of homomorphic is another disadvantage. Cipher text in the ciphers are much larger than plain texts, and thus communication requirements typically go up. The computations on these large cipher texts are typically slower than the computations performed on plain text.

Second category covers solutions which are based on Elliptic Curve Cryptography (ECC) Hankerson and MenezesStein (2011). As the part of initial work, ECC is used for authentication and key generation purpose. Zhang et al. (2013) defined an authentication and key agreement scheme for mutual authentication between substations and smart appliances. Internal attacker resistant data aggregation scheme is presented by He et al. (2017). ECC approach is used in this scheme for better performance and provably secure aggregation scheme. Sun and Song (2017) provided a simplified approach using Password Authenticated Key Exchange (PAKE) and ECC. A trusted third party defines the parameter for ECC and initially a password is shared be-tween Community Energy Management System (CEMS) and SM as the part of initialization phase. A session key is generated between CEMS and SM. In authentication phase, CEMS and SM authenticate with each other using ECC approach. Aggregated data is encrypted using session key. The trusted party saves hash of ID of each SM and whenever SM wants to communicate with TA, SM communicates through IDs hash. The limitation here is; authors has not described about the properties of hash function. It may possible that hash of two different IDs can be same, in that case whether the TA can properly authenticate the SM. Secondly, no performance evaluation is described in the work. Vahedi

https://doi.org/10.1016/j.heliyon.2019.e01321

et al. (2017) invented a solution for data aggregation which is based on ECC and Elgamal cryptography. The research work presented an Elliptic Curve Based Data Aggregation (ECBDA) scheme to preserve the privacy of smart meter.

Majority of above protocols are based on integer factorization or discrete logarithm problem. Shor (1994) proposed algorithm to solve integer factorization problem in polynomial time. Also solution Proos and Zalka (2003) is given for elliptic curve discrete logarithm problem. This clearly indicates the need for mathematically stronger public-key cryptography. Lattices and coding based cryptography are solutions for the future.

Third category is based on Lattice Cryptography Ajtai (1996). Li et al. (2015) used R-LWE based homomorphic approach for providing support to dual-functional (mean and variance) aggregation and invented a privacy-preserving dual-functional aggregation scheme (PDA). SMs present at residential users reports consumption data based on which statistical values (mean and variance) can be calculated. PDA is secured against IND-CPA attack and also robust. It shows better performance compared to Paillier based aggregation scheme. Abdallah and Shen (2017) presented a work for providing privacy to customers' information. In this scheme, the time of day is divided into three slots and each HAN can send maximum one message in this slot. Thus number of messages in a day vary from zero to three. It is based on forecasting the future electricity demand. For providing the security, the scheme uses N-th degree truncated polynomial ring (NTRU) cryptosystem Hoffstein et al. (1998) which includes NTRU based encryption scheme and NTRU based signature scheme. The scheme provides privacy and at the same time satisfies the security requirements. In another research work, Abdallah and Shen (2016) presented lattice based homomorphic scheme.

Our work is motivated by the need to protect the SG network against future quantum attacks. In our previous work Agarkar and Agrawal (2016), we presented the lightweight privacy preserving scheme using R-LWE lattice cryptography. The scheme was developed for consumer side network of SG. The scheme showed better performance compared to RSA 512 based traditional periodic pattern scheme in terms of computation and communication overhead. It is efficient in terms of computation overhead compared to Abdallah and Shen (2014). In this paper, we presented the security and privacy for prosumer network in SG. Compared to previous research, our work is different in two aspects. The proposed scheme provides new messaging scheme for prosumer network where consumers are able to generate electricity and interested to sell the generated energy to either the electricity grid or other consumers. The scheme limits number of messages in the network which not only reduces the communication overhead of the network but also helps to secure the network against DoS attack. The scheme also guarantees privacy of prosumer's information. The scheme uses R-LWE based encryption scheme for encrypting the

https://doi.org/10.1016/j.heliyon.2019.e01321

messages between the communicating parties and also uses R-LWE based signature for verification of the messages. R-LWE reduces the space requirement as each sample from R-LWE distribution can replace n samples from standard LWE distribution; which reduces the secret key size and public key size by factor of n. It provides security against probable attacks in the network such as replay attack, DoS attack, MITM attack and also shows better performance in terms of computation and communication overhead.

3. Background

Lattice cryptography suggests cryptographic algorithms based on lattices. Such algorithms are used to build cryptographic protocols which involves routines like encryption functions, digital signature schemes and one-way hash functions. Roots of lattice cryptography can be traced to benchmark work presented by Ajtai in Ajtai and Dwork (1997, 2007) followed by several similar attempts presented in Regev (2009); Peikert (2009); Micciancio and Regev (2009); Lindner and Peikert (2011).

A lattice is set of points in hi-dimensional space and arranged in periodic manner. It can be represented as $L = \{a_1.v_1 + a_2.v_2 + ... + a_n.v_n | a_i \; is \;$ integer$\}$ for linearly independent vectors $v_1, v_2, ..., v_n$ in the real vector space R_n. Consider the lattice $a \in Z_q^{n \times m}$, which is $n \times m$ matrix (where n is small and m is large and all entries are over finite field Z_q) and s is secret matrix as, $s \in Z_q^n$, we can compute $b = a.s$. Given (a, b) it is hard to find s. This hardness is used in lattice cryptography.

3.1. Learning with error (LWE)

Hardness of lattice cryptography can be increased by introducing error values in the equation. Thus, given $(a, a.s + e)$, find where a is the lattice, s is the secret vector and e is the error vector whose entries are chosen from distribution function. LWE introduces new mathematical problems such as N-th degree truncated polynomial ring (NTRU) and Learning with errors over rings (R-LWE).

3.1.1. NTRU

NTRU is based on the algebraic structures of polynomial ring $R = Z[x]/(x^n - 1)$. Related operations are convolution multiplications and all polynomial in ring have integer coefficients where degree is at most $n - 1$. NTRU cryptosytem can be defined using three parameters (n, p, q) where n is prime, q is always larger than p, and p and q are coprime; and four sets of polynomials L_f, L_g, L_m and L_r which are a polynomial part of private key, a polynomial for generation of the public key, the message and a blinding value respectively, all of degree $n - 1$.

https://doi.org/10.1016/j.heliyon.2019.e01321

3.1.2. Ideal lattices and learning with errors over rings (R-LWE)

R-LWE distribution is pseudorandom. Here are basic elements for R- LWE. $f(x) = x^n + 1 \in Z[x]$, and n is a power of 2, which makes $f(x)$ irreducible over the rational. $R = Z[x]/ < f(x) >$ be the ring of integer polynomials modulo $f(x)$. $q = 1 \bmod 2n$ be a large public prime modulus (bounded by a polynomial in n). Let $R_q = R/ < q > = Z_q[x]/ < f(x) >$ is the ring of integer polynomials modulo both $f(x)$ and q. q^n elements of R_q and can be represented by polynomials of degree less than n. Its coefficients are from $0, ..., q - 1$.

3.2. R-LWE cryptosystem

LRSPPP uses R-LWE cryptosystem from Lyubashevsky et al. (2013) for providing security. Advantages of R-LWE can be listed as,

1. Each noisy product $b = a.s$ gives n pseudo-random values over Z_q, rather than just one scalar, yet the cost of generating is very small.
2. Polynomial multiplications required for the calculation can be done in $O(n \log n)$ time. Additionally, by employing Fast Fourier Transform the same can be done using in $O(\log n)$ with highly optimized way.
3. Each sample $(a, b) \in R_q * R_q$ from R-LWE distribution can replace n samples $(a, b) \in R_q * R_q$ from the standard LWE distribution which reduces the secret key size as well as public key size by factor of n.

3.2.1. R-LWE cryptographic scheme (Key generation, encryption, decryption)

Initially fix a ring $R = Z[x]/ < x^n + 1 >$ where n is power of 2. The cryptography scheme includes following steps:

1. Key generation: A uniformly random element $a \in R_q$ is chosen. Two random 'small' elements $s, e \in R$ are chosen where s works as private key and e works as error value. Using s and e, parameter b is calculated as,

$$b = a.s + e \tag{1}$$

The key pair $(a, b = a.s + e) \in R_q^2$. The key pair (a, b) works as the public key.

2. Encryption $(a, q, m \in 0, 1^n)$: To encrypt an n-bit message $m \in 0, 1^n$, which is an element of R by considering its bits as the 0−1 coefficients of a polynomial, 3 random elements $r, e_1, e_2 \in R$ are chosen from the error distribution $D\sigma$ and finds the pair $(u, v) \in R_q^2$ as the encryption of m.

https://doi.org/10.1016/j.heliyon.2019.e01321

$$u = \mathrm{a.r} + \mathrm{e}_1 \bmod \mathrm{q} \tag{2}$$

$$v = \mathrm{b.r} + \mathrm{e}_2 + (\mathrm{q}/2).\mathrm{m} \bmod \mathrm{q} \tag{3}$$

3. Decryption (u, v, s): Decryption algorithm finds,

$$v - u.s = (\mathrm{r.e} - \mathrm{s.e}_1 + \mathrm{e}_2) + (\mathrm{q}/2).\mathrm{m} \bmod \mathrm{q} \tag{4}$$

For an appropriate choices of parameters, $r.e - s.e_1 + e_2 \in R$ have magnitude less than $q/4$, and hence bits of m can be recovered by rounding each coefficient of $v - u.s$ to 0 or $q/2$, whichever is closest modulo q.

3.2.2. R-LWE based signature scheme (Key generation, sign, verify)

We employ the digital signature scheme introduced by Wu et al. (2012).

The scheme includes following steps:

1. Key Generation (1^n): A ring element is chosen $a \in R_q$ with a prime number $t \in Z_q^*$. Select $s, e \in D\sigma$ where s works as the secret key and e is the error value. Based on this, parameter b is computed as,

$$b = \mathrm{a.s} + \mathrm{t.e} \tag{5}$$

The pair (a, b) works as the public key.

2. Sign ($(m,\ s)$, $H(m)$): H is the collision resistant hash function $H: \{0,1\}^* \rightarrow \mathrm{R_q}$, m is the message and s is the secret key. To sign a message, select $v \in R_q$ from uniform distribution over R_q. Choose $e_1 \in D\sigma$ and compute

$$u = (\mathrm{v} + \mathrm{H(m)}).\mathrm{s} + \mathrm{t.e}_1 \tag{6}$$

Return the signature ((v, u) on m).

3. Verify ((a,b), $H(m)$, (v,u)): Based on the public key (a,b), the signed message $(m,\ (\mathrm{v}, \mathrm{u}))$ and $H(m)$, verification of the message can be performed. To verify the message check whether $(v, u) \in R_q \times R_q$ and

$$[-a.u + b.v] \bmod \mathrm{t} == -\mathrm{b.H(m)} \bmod \mathrm{t} \tag{7}$$

If both the conditions get satisfied, then the message is verified. Otherwise the message is not a valid message.

https://doi.org/10.1016/j.heliyon.2019.e01321

4. Model

System model includes details of network model, adversary model and security requirements and also covers the security goals of the LRSPPP scheme.

4.1. Network model

Fig. 1 shows a pictorial view of Prosumer Community Group network of smart grid. Prosumers are divided into prosumer community groups. PCGs communicate with each other and utility grid through community gateway. PCGs consists of prosumers which have similar electricity generation capacity. Each PCG has its defined goals which are mutually decided based on the prosumers' interest. One PCG tries to reduce energy cost where other can aim for high profit. PCC saves parameter list related to goals defined for each PCG. Our network consists of one PCC, m CGs $\{CG_1, CG_2, ..., CG_m\}$ and each community gateway coordinates n prosumers as part of its cluster. Each CG has a sufficient memory, processing power and is involved in communication with PCC and prosumers. Communication between these controllers is through inexpensive WiFi technology. PCC and CG have input parameters provided by a Trusted Authority (TA). Each prosumer has a unique ID and stored in secured way.

4.2. Adversary model and security requirements

Probable attacks in smart grid network are Denial of Service (DoS) attack, replay attack, Man-in-the-middle (MITM) attack and insider attack. An adversary refers to an attacker who can create range of attacks to the SG network. An adversary can be any node in the region of SG network. An adversary can introduce active and passive attacks. As part of a passive attack, adversary tries to listen to messages between different parties in the communication. In active attack, it can introduce replay attack or falsify intercepted messages. Additionally, the adversary may send number of messages to CG to introduce DoS attack. It may try to get electricity supply amount and benefit amount information for each prosumer. We consider all parties involved in communication are trustworthy and do not introduce any attack. In view of possible attacks, security model should provide the basic security requirements for the network such as confidentiality, message integrity, availability and provide privacy for consumers' data. Following are the details of security requirements.

- *Customer's privacy*: Individual prosumer's electricity generation data should not be revealed to any party. Only PCC and respective CG must handle it.
- *Confidentiality and Messages Integrity:* Individual prosumer's electricity generation and respective benefit amount information must be protected from the adversary. If an adversary tries to eavesdrop any message, it should not be able to

https://doi.org/10.1016/j.heliyon.2019.e01321

find actual data present in the message. Secondly, when the adversary tries to introduce replay attack, it must be detected by respective party. Finally, data present at CG must be secured, so that even if the adversary tries to access prosumer's database, the information must not be available to it.

- *Availability*: Adversary may introduce DoS attack to block access of CG. Thus, CG must be available to all parties, when required.

4.3. Security goals

Our proposed scheme achieves two major goals:

- LRSPPP assures security for all parties involved in the communication. Prosumers' privacy is preserved at the same time proposed scheme achieves integrity and confidentiality of data. It also takes care about the availability of network resources during communication.
- LRSPPP is efficient in terms of computation and communication over-head.

5. Methodology

LRSPPP consists of major two phases: Initialization phase and message exchange phase. Initialization phase is introduced for initial set up of keys between PCC, CGs and prosumers. CG informs to PCC about possible electricity supply from its PCG. Message exchange phase consists of dynamic messages required during lifetime of network such as supply change, price change and goal change. PCC computes monthly benefit share of all PCGs and inform to CGs. Further, CGs finds distribution of benefit amount among prosumers based on their performance. Fig. 2 shows messages related to initialization phase whereas Fig. 3 shows messages related to message exchange phase.

5.1. Phase I: Initialization phase

During initialization phase, public keys of PCC and CG are generated and shared with respective controllers. Other aim of this phase is to set the amount of electricity supply from PCG.

1. Public key generation:

Phase I is responsible for generation of (public key, private key) pairs for PCC and CGs. Network contains one PCC, m CGs and each CG has n prosumers under its cluster. Trusted Authority (TA) fixes a ring $R_q = Z_q[x]/ < f(x) >$, where $f(x) = x^n + 1 \in Z[x]$, and n is a power of 2, which makes $f(x)$ irreducible over the rational. R_q is the ring of integer polynomials modulo both $f(x)$ and q. q^n elements of R_q can be represented by polynomials of degree less than n. Its coefficients

https://doi.org/10.1016/j.heliyon.2019.e01321

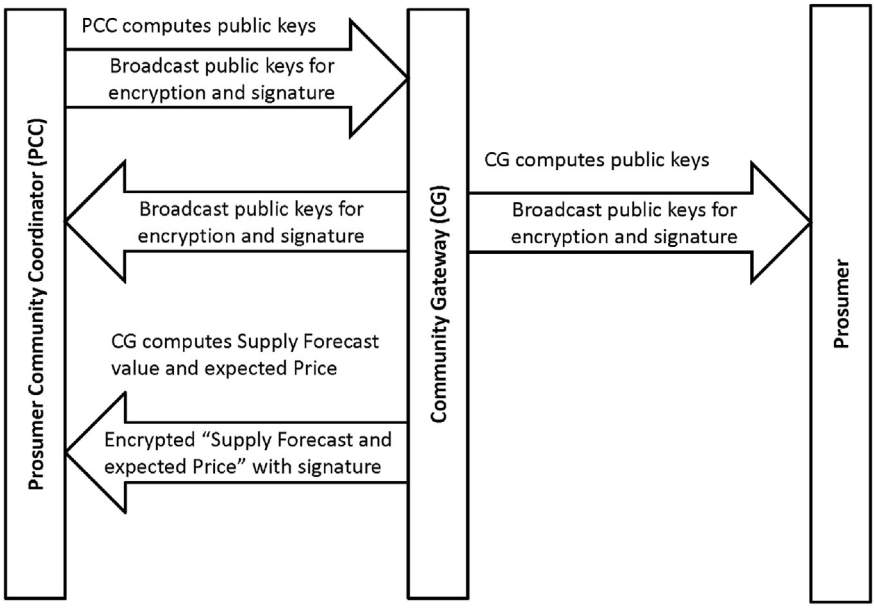

Fig. 2. LRSPPP: Initialization phase.

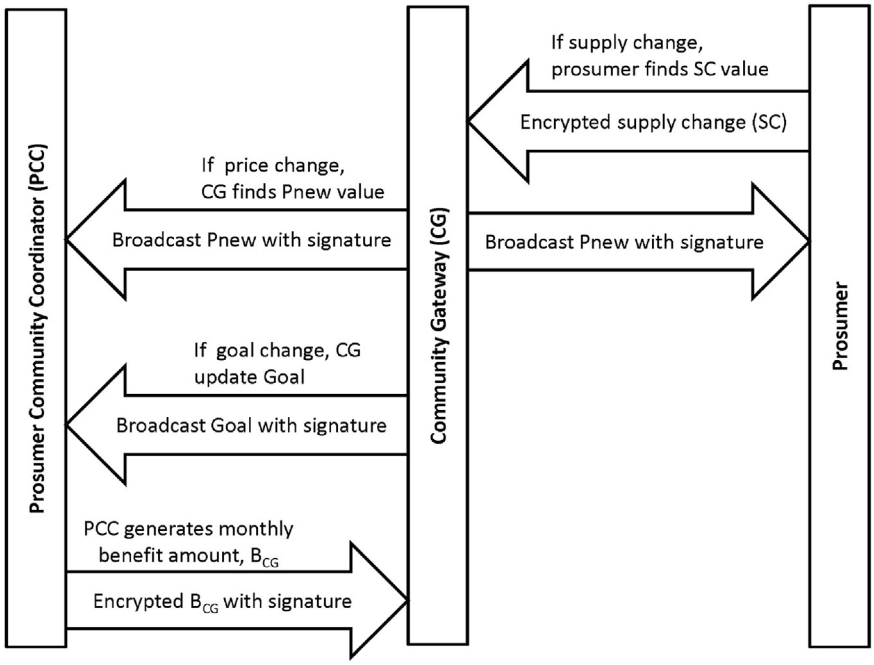

Fig. 3. LRSPPP: Message Exchange phase.

are from $0,.....,q-1$. A prime number is also fixed by TA, which is $t \in Z_q^*$. All parties are informed about the Ring and prime number and then process starts.

(a) Public key generation for encryption: LRSPPP exploits encryption scheme based on ideal lattices and learning with errors over rings (R-LWE) proposed in Lyubashevsky et al. (2013).

https://doi.org/10.1016/j.heliyon.2019.e01321

i. PCC generates a lattice $a_{PCC} \in R_q$. It chooses two small elements from error distribution D_σ, namely s_{PCC} and e_{PCC}. In this case, s_{PCC} works as private key for PCC. PCC computes

$$b_{PCC} = a_{PCC} * s_{PCC} + e_{PCC} \tag{8}$$

and consider $PK_{PCC} = (a_{PCC}, b_{PCC})$ as public key pair. PCC broadcasts public key which is available for CGs for further communication.

ii. In same fashion, all CGs generate their public keys for encryption. CG generates a lattice $a_{CG} \in R_q$. It chooses two small elements namely s_{CG} and e_{CG} from error distribution D_σ. s_{CG} works as private key. CG computes

$$b_{CG} = a_{CG} * s_{CG} + e_{CG} \tag{9}$$

and defines $PK_{CG} = (a_{CG}, b_{CG})$ as public key pair. The public key is broadcasted by CG. Prosumers and PCC collect this key at their end and save in secured way.

(b) Public key generation for signature: For signing and verification LRSPPP uses a digital signature scheme described in Wu et al. (2012). PCC and CG find private key and compute respective public key for this purpose.

i. PCC finds a lattice $c_{PCC} \in R_q$. It chooses random elements ss_{PCC} and e^*_{PCC} from D_σ error distribution. ss_{PCC} works as private key and e^*_{PCC} works as error value. PCC calculates

$$d_{PCC} = c_{PCC} * ss_{PCC} + t * e^*_{PCC} \tag{10}$$

Now, (c_{PCC}, d_{PCC}) is public key. PCC broadcasts the public key which is used for verification of messages. CG uses this key for communication with PCC.

ii. All CGs also generate keys for signing and verification. CG defines a lattice $c_{CG} \in R_q$. It generates public key (c_{CG}, d_{CG}) based on private key ss_{CG} and error value e^*_{CG}. It computes

$$d_{CG} = c_{CG} * ss_{CG} + t * e^*_{CG} \tag{11}$$

(c_{CG}, d_{CG}) is broadcasted as public key of CG. PCC and prosumers collects this key and use this key for verification of integrity of messages.

Thus, at the end of key generation step, respective parties have required public keys for secured communication with other party. PCC and CGs save their own public and private keys for encryption and signature. PCC also saves public keys of all CGs in a table where each row contains keys related to a single CG in the form of (*CG ID*, (a_{CG}, b_{CG}), (c_{CG}, d_{CG})) where PCC uses (a_{CG}, b_{CG}) key pair for encrypting a message while communicating with respective CG and (c_{CG}, d_{CG}) is used for signing the message generated for the CG. Each CG saves the public key pairs of PCC (a_{PCC}, b_{PCC}) , (c_{PCC}, d_{PCC}) for encrypting and singing the message

https://doi.org/10.1016/j.heliyon.2019.e01321

respectively, while sending the message to PCC. Prosumers under each cluster save the public key pairs of their respective CGs which are (a_{CG}, b_{CG}) and (c_{CG}, d_{CG}). Now all parties are ready for secured message exchange.

2. Supply forecast:

At CG: CG forecasts the electricity supply capacity of its PCG. It depends on the forecasted electricity supply amount of each prosumer. During electricity supply forecast process, CG sends possible electricity supply amount of PCG to PCC. As defined in Rathnayaka et al. (2014), PCC discriminates prosumers in different PCGs based on the capacity of electricity supply of each prosumer. Thus, electricity supply profile of prosumer is known to PCC and CG. Additionally, CG analyses the pattern of electricity supply of each prosumer under its cluster and forecasts the amount of electricity supply from each prosumer which is part of its cluster. CG saves this forecasted value in its database in secured way. It makes an entry in database for each prosumer as a pair; (ID_i, ES_i), where ID_i is the ID of the ith prosumer and ES_i is the predicted electricity supply amount of ith prosumer. Finally, CG computes total amount of electricity supply for its PCG. It aggregates supply value of each prosumer as,

$$Forecast_{CG} = \sum_{i=1}^{n} ES_i \tag{12}$$

CG also defines expected price per unit for the electricity supply from its PCG and sends along with the $Forecast_{CG}$ to PCC. CG first calculate hash over $Forecast_{CG}$, price and time stamp T_1. It is used to protect message from replay attack.

$$m = H(Forecast_{CG}|\mathrm{Price}|T_1) \tag{13}$$

CG chooses $X_{CG} \in R_q$ and $e_1 \leftarrow D_\sigma$ and computes

$$Y_{CG} = (X_{CG} + m)*ss_{CG} + t*e_1 \tag{14}$$

It then encrypts values of $Forecast_{CG}$ and price using public key of PCC. CG chooses $r, e_1, e_2 \in D_\sigma$. This e_1 value is different from e_1 used for signing purpose. Based on these random values, CG calculates

$$u_{CG} = a_{PCC}*r + e_1 (\mathrm{mod} q) \tag{15}$$

$$v_{CG} = b_{PCC}*r + e_2 + \lfloor q/2 \rfloor *(Forecast_{CG}|\mathrm{Price})(\mathrm{mod} q) \tag{16}$$

(u_{CG}, v_{CG}) is the cipher text of the message. Now, CG sends $(u_{CG}, v_{CG}, X_{CG}, Y_{CG})$ to PCC.

At PCC: After receiving the message, PCC decrypts the message using its private key s_{PCC} as

https://doi.org/10.1016/j.heliyon.2019.e01321

$$v_{CG} - u_{CG}{}^{*}s_{PCC} \tag{17}$$

and collects values of $Forecast_{CG}$ and Price. It verifies the received values using public key of CG i.e. it checks whether,

$$[-c_{CG}{}^{*}Y_{CG} + d_{CG}{}^{*}X_{CG}](\mathrm{mod}\, t) == -d_{CG}{}^{*}H(Forecast_{CG}|\mathrm{Price}|T_1)(\mathrm{mod}\, t) \tag{18}$$

and

$$(X_{CG}, Y_{CG}) \in R_q \tag{19}$$

If verification holds, PCC saves the $Forecast_{CG}$ and Price values from each CG in its database in the form of $(ID_{CG}, Forecast_{CG}, \mathrm{Price}, Timestamp)$, where ID_{CG} is the ID of a CG, $Forecast_{CG}$ and Price are received forecast and price values from particular CG.

PCC collects $Forecast_{CG}$ value from each CG and now can determine how much energy it can supply to buyers such as individual customers, retailers or utility grid.

After initialization phase, defined amount of electricity is supplied by CG.

5.2. Phase II: Message exchange phase

Phase II is introduced for the dynamic mechanism for electricity supply as well as price change per unit. After the initialization phase, each PCG supplies the electricity to buyers. During execution, if any change occurs in terms of electricity supply amount, price per unit or goal defined by PCG, then this situation must be handled dynamically.

1. Supply change (Prosumer → CG):

If prosumer recognizes change in possible amount of electricity supply, it informs the modified supply amount to CG. The supply change value, SC, is encrypted using public key of CG along with verification value and sent to CG. After receiving message CG make entry of updated supply amount with time stamp in its database as $(ID_i, SC_i, Timestamp)$. where ID_i is the ID of i^{th} Prosumer and SC_i is the supply change amount of i^{th} prosumer.

Prosumer finds verification value using hash function as $H(SC|T_2)$ where T_2 is time stamp. Now chooses $r, e_1, e_2 \in R$ from error distribution function. Based on these random values, prosumer computes

$$u_P = a_{CG}{}^{*}r + e_1(\mathrm{mod}\, q) \tag{20}$$

$$v_P = b_{CG}{}^{*}r + e_2 + \lfloor q/2 \rfloor {}^{*}SC\ (\mathrm{mod}\, q) \tag{21}$$

https://doi.org/10.1016/j.heliyon.2019.e01321

Prosumer sends $(u_P, v_P, H(SC|T_2))$ to respective CG. CG decrypts the message as, $v_P - u_P{*}s_{CG}$ and verifies values using hash function. It updates the electricity supply value of respective prosumer in its database.

If CG receives significant change in aggregated amount of electricity supply from all prosumers, it updates electricity forecast value and informs to PCC.

2. Price change (CG→P CC, Prosumer):

During execution of network, if CG decides to change price per unit for electricity supplied by its PCG, it records the new price value, P_{new} , in its database as $(P_{new}, Timestamp)$ and also informs this value to PCC as well as prosumers. It broadcasts the P_{new} value along with signature. PCC and prosumers decrypt the message, verify it and save this modified value in encrypted fashion.

CG defines P_{new} and finds signature value based on P_{new} and T_3 time stamp. It chooses $X_{CG} \in R_q$ and $e_1 \in D_\sigma$ and computes

$$Y_{CG} = (X_{CG} + H(P_{new}|T_3)){*}ss_{CG} + t{*}e_1 \tag{22}$$

CG broadcasts price value in plain text along with the signature. PCC and prosumers collects messages and verifies value based on signature using following equality of equations,

CG broadcasts the message $(H(P_{new}|T_3), X_{CG}, Y_{CG})$. PCC and prosumers collects messages and verifies value based on signature as,

$$[-c_{CG}{*}Y_{CG} + d_{CG}{*}X_{CG}](\mathrm{mod}\, t) == -d_{CG}{*}H(P_{new}|T_3)(\mathrm{mod}\, t) \tag{23}$$

and checks whether $(X_{CG}, Y_{CG}) \in R_q \times R_q$. If verification holds, PCC and prosumers use updated price value for further analysis.

3. Goal change (CG→PCC):

In PCG network, clustering of prosumers is done based on their goals. Mutual goals are decided for each PCG based on general characteristic of PCGs; such as number of prosumers within PCG and average sharing capacity of the PCG. These are called theoretical goals. Mutual goals are rephrased during the lifetime of the network based on characteristic behaviors and are called as realistic mutual goals. Based on energy behavior CG updates the realistic mutual goals. If at any time, CG decides to change any parameters from its defined goal list, it informs the same to PCC in secured way.

At CG: Consider CG wants to change *P1* parameter, $P1_{CG}$ from goal list, CG first calculate hash over $P1_{CG}$ and time stamp T_4. It chooses $X_{CG} \in R_q$ and e_1 from error distribution function and computes

https://doi.org/10.1016/j.heliyon.2019.e01321

$$Y_{CG} = (X_{CG} + H(P1_{CG}|T_4)*ss_{CG} + t*e_1 \tag{24}$$

It then encrypts values of $P1_{CG}$ using public key of PCC. CG chooses $r, e_1, e_2 \in R$ from error distribution function $D\sigma$. Based on these random values, CG computes u_{CG} and v_{CG} as

$$u_{CG} = a_{PCC}*r + e_1 (\text{mod } q) \tag{25}$$

$$v_{CG} = b_{PCC}*r + e_2 + \lfloor q/2 \rfloor *P1_{CG} \ (\text{mod } q) \tag{26}$$

(u_{CG}, v_{CG}) i]s the cipher text of the message. Now, CG sends $(u_{CG}, v_{CG}, X_{CG}, Y_{CG})$ to PCC.

At PCC: After receiving the message PCC decrypts the message as $v_{CG} - u_{CG}*s_{PCC}$ and collects value of $P1_{CG}$, It verifies the received values using public key of CG i.e. it checks whether,

$$[-c_{CG}*Y_{CG} + d_{CG}*X_{CG}] \ (\text{mod t}) \ == -d_{CG}*H(P1_{CG}|T_4) \ (\text{mod t}) \tag{27}$$

and $(X_{CG}, Y_{CG}) \in R_q \times R_q$. If verification holds, PCC updates the parameter from goal list of respective CG.

4. Benefit amount generation:

At the end of each month, PCC generates the benefit amount of each PCG and informs to respective CG. Benefit amount, B_{CG}, is computed as,

$\mathrm{B_{CG}}$ = Total number of electricity supply by PCG x Price per unit

B_{CG} value is sent to CG in encrypted format along with signature. Thus, CG has information about benefit amount of its PCG. The benefit message is signed by PCC's private key and encrypted using respective CG's public key.

At PCC: PCC hashes benefit value BCG with time stamp T_5. It chooses $X_{PCC} \in R_q$ and e_1 from error distribution function and computes

$$Y_{PCC} = (X_{PCC} + H(B_{CG}|T_5)*ss_{PCC} + t*e_1 \tag{28}$$

PCC encrypts the value of B_{CG} using public key of PCC. It chooses $r, e_1, e_2 \in R$ from error distribution $D\sigma$. This e_1 value is different from e_1 used for signing purpose. Based on these random values, PCC computes

$$u_{PCC} = a_{CG}*r + e_1 (\text{mod } q) \tag{29}$$

$$v_{PCC} = b_{CG}*r + e_2 + \lfloor q/2 \rfloor *B_{CG} (\text{mod } q) \tag{30}$$

(u_{PCC}, v_{PCC}) is the cipher text of the message. Now, PCC sends $(u_{PCC}, v_{PCC}, X_{PCC}, Y_{PCC})$ to CG.

https://doi.org/10.1016/j.heliyon.2019.e01321

At CG: After receiving the message, CG decrypts the message using its private key as $v_{PCC} - u_{PCC}{}^{*}s_{CG}$ and collects value of B_{CG}. It verifies the received value using public key of PCC i.e. it checks whether,

$$[-c_{PCC}{}^{*}Y_{PCC} + d_{PCC}{}^{*}X_{PCC}](\mathrm{mod}\, t) == -d_{PCC}{}^{*}H(B_{CG}|T_5)(\mathrm{mod}\, t) \tag{31}$$

and

$$(X_{PCC}, Y_{PCC}) \in R_q \times R_q \tag{32}$$

If success in validation, PCC accepts B_{CG} value.

CG compares the B_{CG} received from PCC with its record. CG calculates the distribution of benefit amount among the prosumers under its cluster based on the rank value. CG has a record of amount of electricity supplied by each prosumer. It also evaluates long-term and short-term electricity sharing for each prosumer based on which it defines rank of each prosumer. Using rank and electricity share, it finds benefit amount of each prosumer and save in the database in encrypted form. For example, if i^{th} prosumer has B_i as benefit amount, then

$$B_{CG} = \sum_{i=1}^{n} B_i \tag{33}$$

The benefit of individual prosumer is not shared to anyone in the network. Only prosumer and respective CG has its record which provides privacy for individual prosumer's information.

6. Analysis

Analysis section analyses how prosumer's privacy get preserved and how LRSPPP satisfies security requirements of SG such as confidentiality and integrity, authenticity for different parties, resource availability and accountability. Here we assume that all parties involved in communication are honest and no insider attack takes place in the network.

LRSPPP is designed considering the future requirement of smart grid network and employs the lattice cryptography solution for providing security against classical and quantum computers. In LRSPPP, the messages are securely encrypted and signed using R-LWE based schemes. The R-LWE problems can be stated as a "search problem" and a "decision problem". Let $a_i(x)$ be the set of random and known polynomials from $Z_q[x]/f(x)$ with coefficients from F_q, $e_i(x)$ be the set of small unknown polynomials relative to a bound b in the Ring $Z_q[x]/f(x)$. $s(x)$ be a small unknown polynomial relative to bound b in the Ring $Z_q[x]/f(x)$ and $b_i(x) = (a_i(x) + s(x)) + e_i(x)$. The search problem defines the task of finding $s(x)$ given the list of polynomial pairs $(a_i(x), b_i(x))$. The Decision problem states

https://doi.org/10.1016/j.heliyon.2019.e01321

that, given the list of polynomials $(a_i(x), b_i(x))$, determine whether $b_i(x)$ polynomials were constructed as $b_i(x) = (a_i(x).s(x)) + e_i(x)$ or were generated randomly from $Z_q[x]/f(x)$ with coefficient from F_q. The hardness of these problems are parameterized by the choice of quotient polynomial $f(x)$, its degree n, Field F_q and the bound b.

When the polynomial $f(x)$ is a cyclotomatic polynomial, the difficulty of solving search version of R-LWE problem is equivalent to solving shortest vector problem in an ideal lattice. Our scheme uses the Ring $R_q = Z_q[x]/f(x)$, where $f(x) = x^n + 1 \in Z[x]$, and n is a power of 2. The public and private keys are generated using this Ring. An attacker may try to find private key for decrypting the messages. But finding private key problem is equivalent to solving shortest vector problem of lattice. Trying to find private key requires finding non-zero vector from $R_q \times R_q$ field. The best known algorithm for solving this problem needs $2^{\Omega(n)}$ operations and thus it is considered as NP-Hard problem. Hence an attacker is not able to find the information sent during communication and guarantees the integrity and confidentiality of messages. Only valid receivers can decrypt the messages which proves the authenticity of communicating parties. For verification of received messages, messages are signed with private keys of the sender. Receiver verifies the messages using public keys of the sender. The signing and verification also uses R-LWE which provide guarantee regarding integrity of the messages. Here is the discussion of how LRSPPP provides privacy to customer's information and satisfies requirements of SG.

1. *Privacy preservation*: Individual prosumer's electricity supply data should not be revealed to any party. CG record individual prosumer's information in an encrypted manner in its database. CG does not disclose individual prosumer's supply amount to preserve privacy. PCC and CG share aggregated information about electricity supply and benefit amount of complete PCG in secured way using R-LWE encryption and signature scheme. Prosumers also send supply change message in encrypted manner. Also, every message is signed and verified by respective controllers. Thus an intruder cannot inject any false message. Average case hardness of R-LWE in terms of encryption and signature of messages provides a strong base for providing privacy for prosumer's information.
2. *Confidentiality and integrity of messages*: All messages in the scheme are encrypted using public key of respective controllers. Thus adversary is not able to recognize the data sent through the message, even if it listens to it. Adversary tries to impersonate a smart meter to compromise its messages, but it cannot get an ID of prosumer as the prosumer's ID is stored in a secured fashion. Thus impersonation attack is not possible. CG sends the price change message in plain text, but it also sends the signature with message. Thus, adversary can recognize what is the proposed price but it cannot inject any false price message, as it is

https://doi.org/10.1016/j.heliyon.2019.e01321

signed by the private key of CG. Again adversary cannot introduce a replay attack, as the time stamp is sent along with messages and receiver checks the same. Messages between PCC and CG are hashed and then signed using respective public keys. Thus, the scheme provides confidentiality and integrity of the messages and pro-vides security against active and passive MITM attack, and also from replay attack.

3. *Authenticity for Different Parties*: PCC and CG are authenticated by their public keys. Therefore, messages encrypted by them are authenticated. Authentication of prosumer is done through its ID.
4. *Availability of Resources*: Adversary can try to introduce a DoS attack to make PCC or CG busy so that it cannot be available for honest message handling. In LRSPPP, numbers of message transfers are limited and validity of messages is checked. If PCC or CG recognizes more input messages, in a limited time, it can detect it and block the respective malicious party.
5. *Accountability*: PCC generates monthly benefit for PCG and informs to CG. CG can verify this amount based on its database entries. Additionally, CG defines benefit amount of individual prosumer. Householder of respective prosumer can verify the monthly benefit amount based on the number of electricity units supplied and price per unit, as both values are available at prosumer.

In previous schemes such as traditional periodic pattern scheme, Busom et al.'s scheme and ECBDA scheme, each smart meter periodically sends electricity consumption data which not only reduces the lifetime of the network but also increases the chance of an attacker to recognize the knowledge regarding the electricity consumption. LRSPP reduces number of messages in the network and increases the security and privacy of prosumers individual information. Individual prosumers data is not revealed to any party except the respective CG to provide the privacy preservation. CG communicates to PCC and informs the collective amount of electricity supply from its PCG. Thus, LRSPP provides privacy to prosumer's individual information, its behavior and privacy during communication.

7. Results & discussion

The aim of our scheme is to provide the security and at the same time it should be lightweight in terms of communication and computation overhead. Communication overhead is related to messaging required between various controllers present in the communication. Computation overhead is related to the time required for execution of number of operations present in the scheme. The performance of LRSPPP is compared with traditional periodic pattern scheme Abdallah and Shen (2017), the scheme proposed by Busom et al. (2016) and Elliptic Curve Based Data Aggregation (ECBDA) scheme Vahedi et al. (2017).

https://doi.org/10.1016/j.heliyon.2019.e01321

1. *Communication overhead*: LRSPPP aims to provide lightweight solution for communication of prosumer network. It uses cluster based architecture for prosumers, CG and PCC. Messages related to initialization phase are compulsory which are sent in initial setup. Benefit amount generation message is sent for each month. Other messages such as supply change, price change and goal changes messages are sent, if required. In initial setup, if CG properly calculate electricity supply amount of CG, then in best case scenario supply change message is not introduced in the network. In smart grid, time span is divided into on-peak, mid-peak and off-peak Ontorio(http://www.ontario-hydro.com/current-rates). In worst case situation, each prosumer introduces one supply change message for the defined span. Still number of messages are limited. For experimentation, we consider one price change and one goal change message per month.

Two scenarios are considered for experimentation. In first scenario, network contains one PCC, one CG and number of prosumers varies from 10 to 100. In initialization phase, two messages are broadcasted for sharing public keys; one from PCC and other from CG. Additionally, CG sends supply forecast message to PCC. In message exchange phase, 3 messages are sent for price change, goal change and benefit amount message. In the best case situation, supply change message is not introduced in the network whereas in worst case, all prosumers send 3 supply change messages per day. Thus, for worst case situation, number of supply change messages are calculated as $30 \times 3 \times$ *Number* of Prosumers. Fig. 4 shows monthly

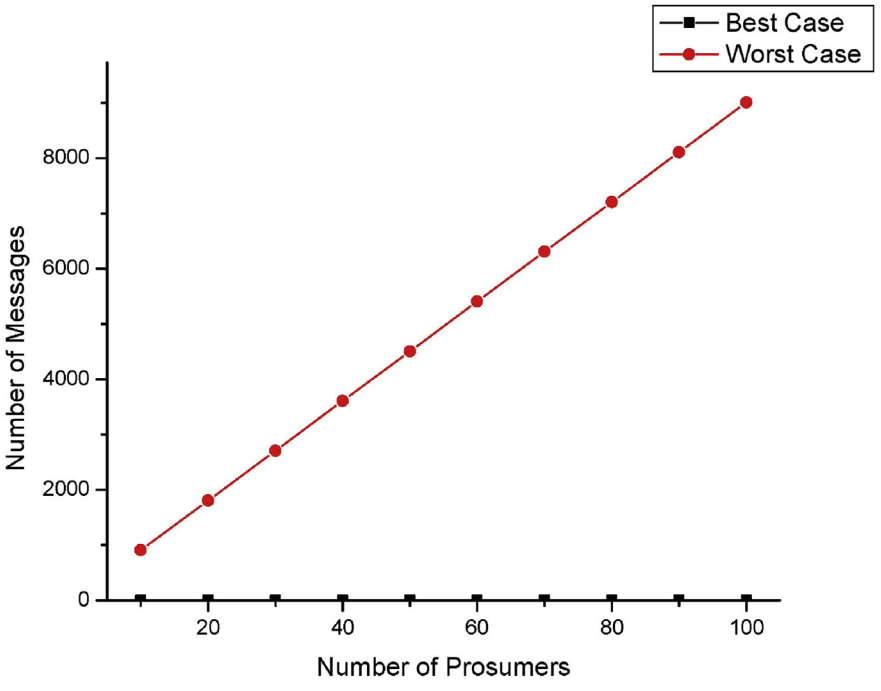

Fig. 4. Communication overhead for LRSPPP scheme.

https://doi.org/10.1016/j.heliyon.2019.e01321

communication overhead for best case and worst case situation. Practically speaking, communication overhead remains between these two limits.

Communication overhead of LRSPPP is compared with traditional periodic pattern scheme Abdallah and Shen (2017), Busom et al. (2016) scheme and ECBDA proposed by Vahedi et al. (2017). Fig. 5 shows the messaging by all these schemes for a month. In the traditional periodic pattern scheme, each smart meter sends its electricity consumption information after either 30 minutes or an hour. Considering periodicity of one hour, number of message exchange is 810**Number* of Smart Meters Abdallah and Shen (2017). Busom et al. (2016) requires maximum message transfers in the network. Four message exchange takes place for each smart meter for each periodic event. Communication overhead of ECBDA and traditional scheme are comparable. In the graph, periodicity of one hour is considered for all these three scheme. Worst case scenario of LRSPPP is considered for finding number of message transfers. Even in worst case, the proposed scheme is lightweight compared to other three scheme.

In the second scenario, we considered a network which has one PCC, CGs varies from 1 to 10 where each CG has 10 prosumers under its cluster. Fig. 6 shows the message transfers in the network. As compared to Fig. 5, there is small increase in number of messages for LRSPPP which are because of public key broadcast and supply forecast message from each CG.

2. *Computation overhead:* LRSPPP uses basic operations as R-LWE based encryption and decryption, R-LWE based signing and verification and hashing.

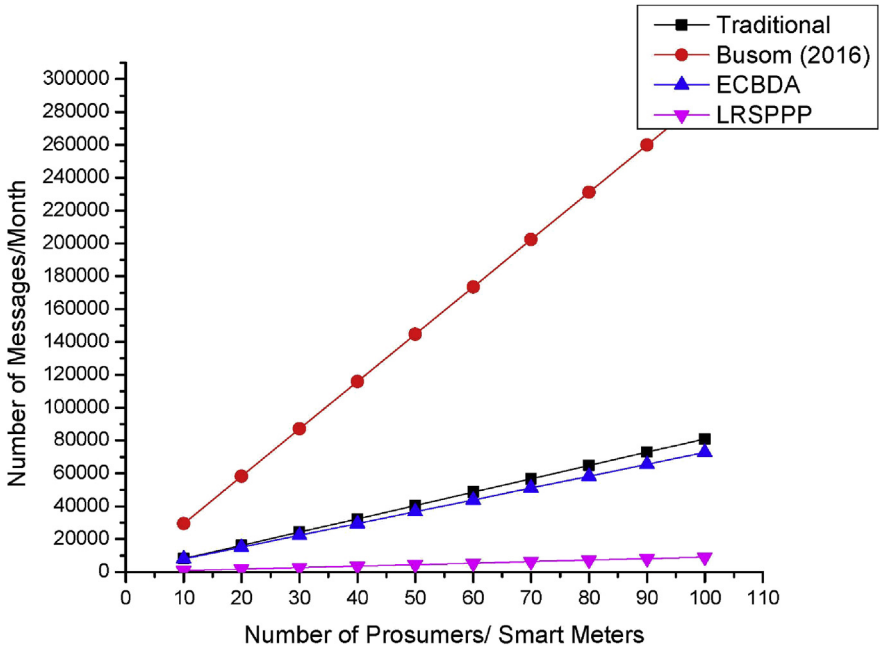

Fig. 5. Scenario 1: Communication overhead.

https://doi.org/10.1016/j.heliyon.2019.e01321

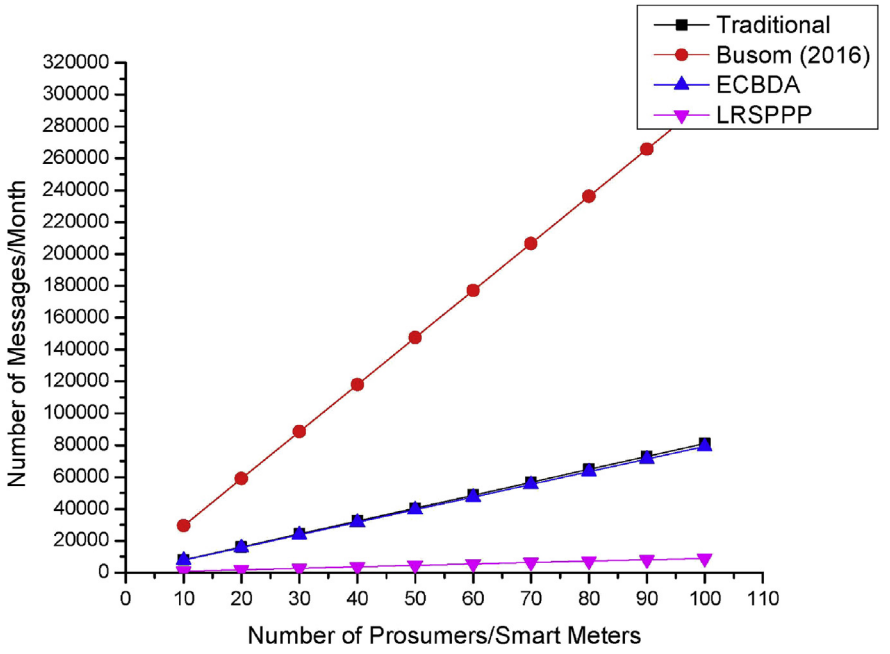

Fig. 6. Scenario 2: Communication overhead.

Consider time required for R-LWE encryption is *Te*, R-LWE decryption is *Td*, R-LWE signing is *Ts*, R-LWE verification is *Tv* and hashing is *Th.*

In initialization phase, key generation process is done by PCC and CG. Supply forecast message needs *(Te + Td + Ts + Tv)* time. Supply change message requires *(Te + Td + 2 * Th)* time. Price change message requires computation time for signing at CG as *Ts*. PCC and prosumers need price change verification time *Tv*. Goal change and benefit amount generation messages are sent by PCC for each month and requires *(Te + Td + Ts + Tv)* time each. Table 1 shows computation time for each operation at PCC, CG and prosumer.

Implementation for R-LWE operations is done for medium level security and high level security with parameters

$P1 = (n, q, \sigma) = (256, 7681, 11.31/\sqrt{2\pi})$ and

Table 1. Computation overhead at PCC, CG and prosumer.

Message	PCC	CG	Prosumer
Supply forecast	$T_d + T_v$	$T_e + T_s$	
Supply change		$T_d + T_h$	$T_e + T_h$
Price change	T_v	T_s	T_v
Goal change	$T_d + T_v$	$T_e + T_s$	
Benefit amount generation	$T_e + T_s$	$T_d + T_v$	

https://doi.org/10.1016/j.heliyon.2019.e01321

$P2 = (n, q, \sigma) = (512, 12289, 12.18/\sqrt{2\pi})$ from De Clercq et al. (2015).

Table 2 shows time required for encryption and signature scheme. Knuth-Yao algorithm is used for generating pseudorandom elements of each vector. Polynomial operations are implemented using Number Theoretic Transform (NTT) as it requires less time for execution when handling big matrices. We run both schemes on Intel Core Duo CPU with 2.10 GHz speed, 4GB RAM with 64 bit operating system. Hashing of supply change message is done using SHA-256 which requires 0.0004 ms for finding hash of the message.

The execution time for key generation, encryption and decryption of P1 parameters require 0.38 ms, 0.4 ms and 0.1 ms respectively. For P2 parameter, execution time for key generation, encryption and decryption is 0.8 ms, 0.8 ms and 0.3 ms. For digital signature, key generation, signing and verification requires 0.4 ms, 0.36 ms and 0.57 ms considering P1 parameters. For P2 parameter, 0.9 ms require for key generation whereas signing and verification requires 0.86 ms and 1.4 ms respectively.

Analysis of LRSPPP is done for two scenarios. In the first scenario, network contains one PCC, one CG and number of prosumers varies from 10 to 100. Time is required for one supply forecast message. As part of message exchange phase, considering worst case situation, each prosumer sent 3 supply change messages per day. Price change and goal change are least frequent messages. During analysis one price change and one goal change message is considered. PCC informs benefit amount for CG by a single message. Thus total computation operations performed are $3 * (Te + Td + Ts + Tv) + 90 * n * (Te + Td + 2 * Th) + (Ts + (n + 1)\, Tv)$ where n is the number of prosumers in the network. Fig. 7 shows computation overhead required for a month considering all parties in the network for R-LWE P1 and P2 parameters.

As part of second scenario, network contains one PCC and number of CGs varies from 1 to 10. Each CG has 10 prosumers in the PCG. Fig. 8 shows the computation overhead for this scenario. Little increase in computation time is recorded compared to Fig. 7.

To compare the performance of LRSPPP scheme with other schemes, we have implemented the traditional periodic pattern scheme which uses RSA 512 Hoffstein et al.

Table 2. Time requirement of cryptography algorithms.

Algorithm	Encryption	Decryption	Signing	Verification
RSA 512	0.4 ms	8.1 ms	9.43 ms	0.54 ms
EC Elgamal	4.9 ms	13.7		
R-LWE (P1)	0.4 ms	0.14 ms	0.36 ms	0.57 ms
R-LWE (P2)	0.8 ms	0.3 ms	0.86 ms	1.4 ms

$P1 = (256, 7681, 11.31/\sqrt{2\pi})$, $P2 = (512, 12289, 12.18/\sqrt{2\pi})$

https://doi.org/10.1016/j.heliyon.2019.e01321

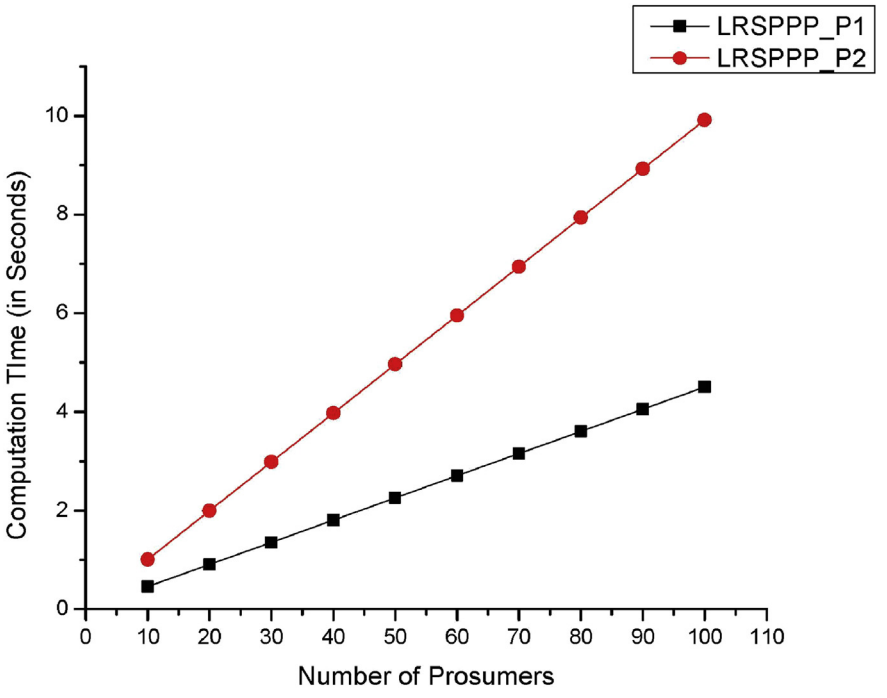

Fig. 7. Computation overhead for LRSPPP between P1 and P2: Number of prosumers varies from 10 to 100.

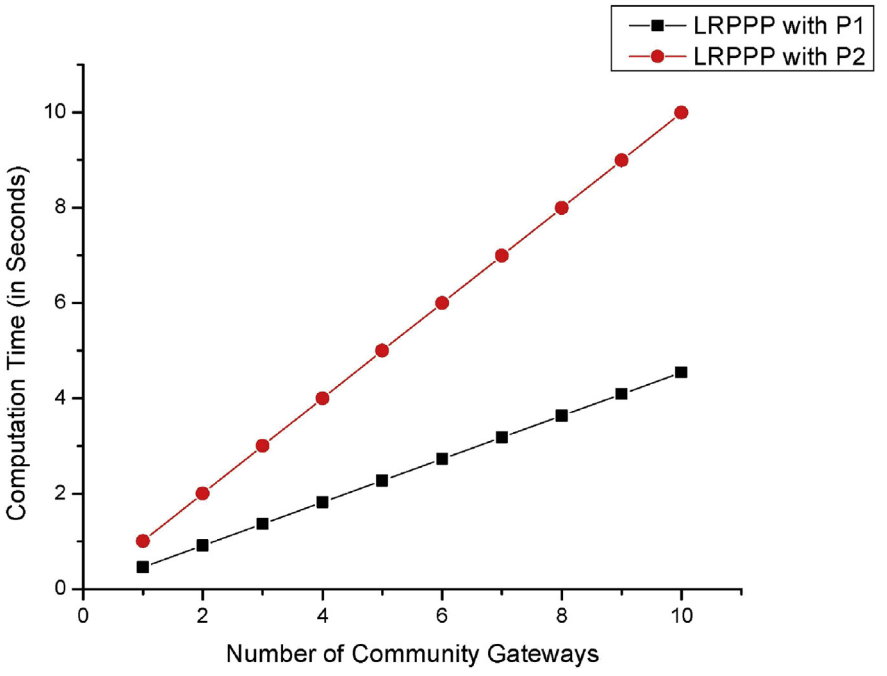

Fig. 8. Scenario 2: Computation overhead for LRSPPP between P1 and P2.

https://doi.org/10.1016/j.heliyon.2019.e01321

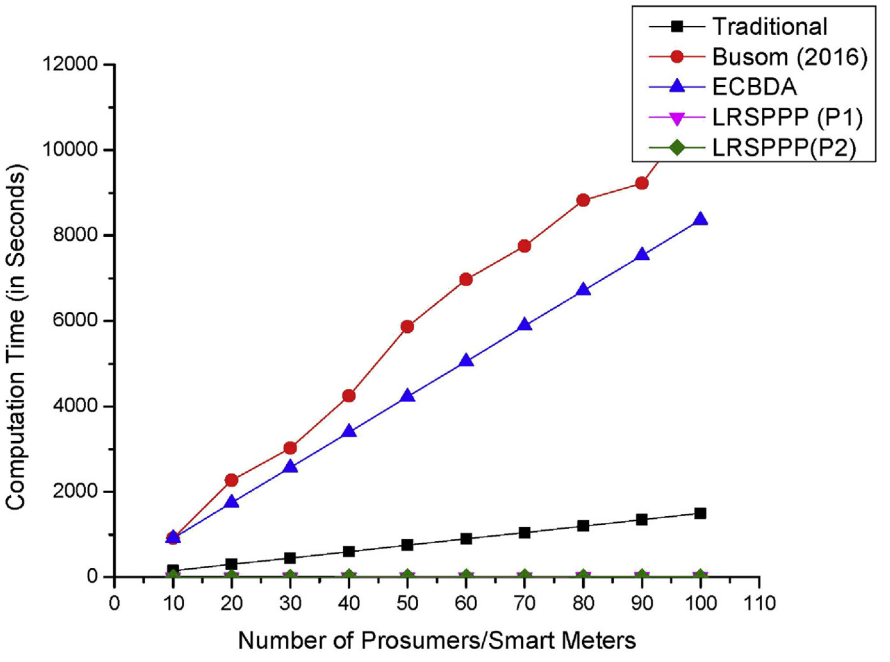

Fig. 9. Scenario 1: Computation overhead.

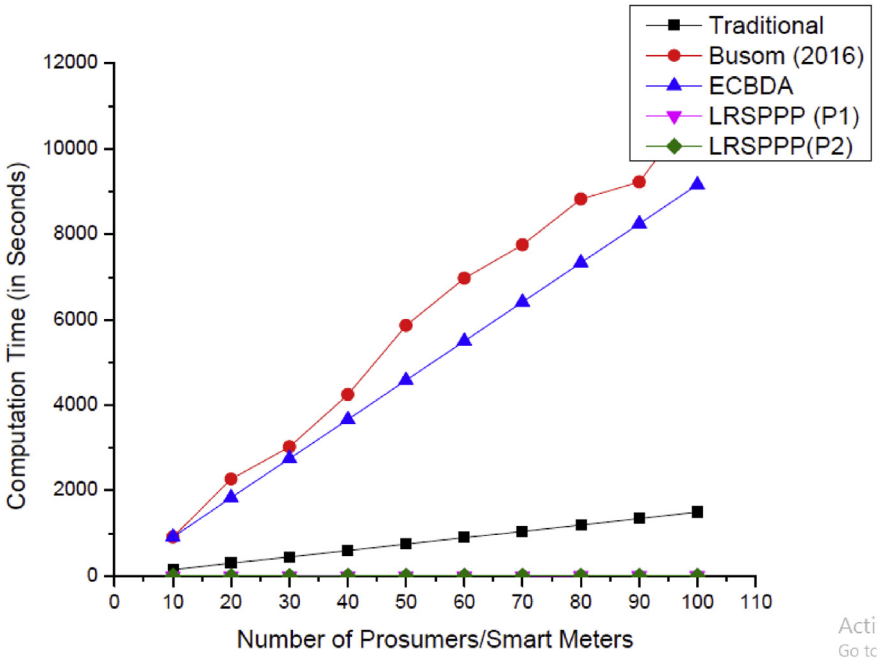

Fig. 10. Scenario 2: Computation overhead.

(1998), Busom et al. (2016) scheme and ECBDA scheme. Figs. 9 and 10 shows computation overhead of all these schemes for Scenario 1 and Scenario 2 respectively.

Traditional periodic pattern scheme employs RSA 512 for encryption, decryption, signing and verification. Encryption and decryption operations require 0.4 ms and

https://doi.org/10.1016/j.heliyon.2019.e01321

8.1 ms respectively. At the same time, signing and verification takes 9.43 ms and 0.54 ms respectively. Each smart meter sends reading after one hour, which requires all four operations. Thus computation overhead for a month is $810^* n^* (Te + Td + Ts + Tv)$ considering n as number of prosumers in the network. Busom et al. (2016) uses Elgamal cryptosystem for encrypting and decrypting messages. As the number of message exchanges in this scheme are very large, it impacts on the total time for computation. ECBDA tried to reduce the computation time by using Elliptic Curve based Elgamal encryption scheme. 4.9 ms and 13.7 ms are required for encryption and decryption process respectively. ECBDA also exploits Boneh- Lynn-Shacham (BLS) short signature scheme for signing and verification which needs 0.11 seconds for execution. Compared to these three schemes, the computation time requirement for LRSPPP is significantly less considering scenario 1 and scenario 2.

8. Conclusion

To summarize, we studied security and privacy at the prosumer side of smart grid network. A detailed discussion is presented on various encryption based privacy preservation schemes including homomorphic encryption schemes, ECC based lightweight encryption schemes, and recent developments on lattice cryptography. In this paper, R-LWE based encryption scheme is presented for privacy protection in the smart grid network. Detailed analysis is conducted and the paper concluded the superiority of LRSPPP in terms of reduced messaging overhead and computation overhead. Additionally, the proposed LRSPPP is secured against MITM and replay attacks while protecting the privacy of prosumers.

In future, our work can be extended in three directions. The proposed scheme can be extended to provide security against insider attacks. Community gateway node or prosumer community coordinator can be compromised, therefore anomaly detection under this distributed networking scenario can add further knowledge. Secondly, the proposed solution can be extended using blockchains. Smart grid network is basically a transactive energy system. Therefore, a blockchain based solution using lattice primitives can take the research work one step further. Finally, it would be interesting to test these lightweight schemes on other similar multi-layer communication networks such as Precision agriculture network, Smart Surveillance system etc.

Declarations

Author contribution statement

Aarti A. Agarkar: Conceived and designed the experiments; Performed the experiments; Analyzed and interpreted the data; Contributed reagents, materials, analysis tools or data; Wrote the paper.

https://doi.org/10.1016/j.heliyon.2019.e01321

Himanshu Agrawal: Conceived and designed the experiments; Performed the experiments; Analyzed and interpreted the data; Contributed reagents, materials, analysis tools or data.

Funding statement

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Competing interest statement

The authors declare no conflict of interest.

Additional information

No additional information is available for this paper.

References

Abdallah, A.R., Shen, X.S., 2014. A lightweight lattice-based security and privacy-preserving scheme for smart grid. In: IEEE Global Communications Conference (GLOBECOM), pp. 668−674.

Abdallah, A., Shen, X., 2016. A lightweight lattice-based homomorphic privacy-preserving data aggregation scheme for smart grid. IEEE Trans. Smart Grid 9 (1), 396−405.

Abdallah, A., Shen, X., 2017. Lightweight security and privacy preserving scheme for smart grid customer-side networks. IEEE Trans. Smart Grid 8 (3), 1064−1074.

Agarkar, A., Agrawal, H., 2016. R-LWE based lightweight privacy pre- serving scheme for Smart Grid. In: IEEE International Conference on Com- Puting, Analytics and Security Trends (CAST), pp. 410−415.

Ajtai, M., 1996. Generating hard instances of lattice problems. In: Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, New York, NY, USA, pp. 99−108. https://www.math.uni-frankfurt.de/~dmst/teaching/SS2018/Ajtai96.pdf.

Ajtai, M., Dwork, C., 1997. A public-key cryptosystem with worst- case/average-case equivalence. In: Proceedings 29th Annual ACM Symp. On Theory of Computing (STOC), El Paso, TX, USA, pp. 284−293.

Ajtai, M., Dwork, C., 2007. The first and fourth public-key cryptosys- tems with worst-case/average-case equivalence. In: Electronic Colloquium on Computational

https://doi.org/10.1016/j.heliyon.2019.e01321

Complexity. REPORT NO. 97. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.429.4440&rep=rep1&type=pdf.

Bos, J.W., Castryck, W., Iliashenko, I., Vercauteren, F., 2017. Privacy- friendly forecasting for the smart grid using homomorphic encryption and the group method of data handling. In: International Conference on Cryptol- Ogy in Africa, pp. 184−201.

Busom, N., Petrlic, R., Seb, F., Sorge, C., Valls, M., 2016. Efficient smart metering based on homomorphic encryption. Comput. Commun. 82, 95−101.

De Clercq, R., Roy, S.S., Vercauteren, F., Verbauwhede, I., 2015. Efficient Software Implementation of Ring-LWE Encryption. In: DATE 2015: Design, Automation and Test in Europe Conference and Exhibition. EDA Consortium, Grenoble, France, pp. 339−344.

ElGamal, T., 1985. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inf. Theory 31 (4), 469−472.

Guan, Z., Si, G., 2017. Achieving privacy-preserving big data aggregation with fault tolerance in smart grid. Dig. Commun. Netw. 3 (4), 242−249.

Hankerson, D., MenezesStein, A., 2011. Elliptic Curve Discrete Logarithm Problem', Encyclopedia of Cryptography and Security. Springer US, pp. 397−400.

He, D., Zeadally, S., Wang, H., Liu, Q., 2017. Lightweight data aggregation scheme against internal attackers in smart grid using elliptic curve cryptography. Wireless Commun. Mobile Comput.

Hoffstein, J., Pipher, J., Silverman, J.H., 1998. NTRU: a ring-based public key cryptosystem. In: International Algorithmic Number Theory Symposium. Springer, Berlin, Heidelberg, pp. 267−288.

Hur, J.B., Koo, D.Y., Shin, Y.J., 2015. Privacy-preserving smart metering with authentication in a smart grid. Appl. Sci. 5 (4), 1503−1527.

Li, C., Lu, R., Li, H., Chen, L., Chen, J., 2015. PDA: a privacy-preserving dual-functional aggregation scheme for smart grid communications. Secur. Commun. Netw. 8 (15), 2494−2506.

Lindner, R., Peikert, C., 2011. Better Key Sizes (And Attacks) for LWE- Based Encryption. CT-RSA, pp. 319−339.

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 Trans. Parallel Distrib. Syst. 23 (9), 1621−1631.

https://doi.org/10.1016/j.heliyon.2019.e01321

Lyubashevsky, V., Peikert, C., Regev, O., 2013. On ideal lattices and learning with errors over rings. J. Assoc. Comput. Mach. 60 (6), pp. 43:1−43:35.

Micciancio, D., Regev, O., 2009. Lattice-based Cryptography. Post Quantum Cryptography. Springer, pp. 147−191. February 2009.

Ontorio. ABC. http://www.ontario-hydro.com/current-rates.

Paillier, P., 1999. Public-key cryptosystems based on composite degree residuosity classes. In: International Conference on the Theory and Applications of Cryptographic Techniques, Berlin, Heidelberg, pp. 223−238.

Peikert, C., 2009. Public-key cryptosystems from the worst-case shortest vector problem. In: Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing, Bethesda, MD, USA, pp. 333−342.

Perl, H., Brenner, M., Smith, M., 2011. Poster: an implementation of the fully homomorphic Smart-Vercauteren crypto-system. In: Proceedings of the 18th ACM Conference on Computer and Communications Security, pp. 837−840. https://www.chi.uni-hannover.de/uploads/tx_tkpublikationen/ccsp121b.pdf.

Proos, J., Zalka, C., 2003. Shor's discrete logarithm quantum algorithm for elliptic curves. QIC 3 (4), 317−344 arXiv:quant-ph/0301141.

Rahman, M.S., Basu, A., Kiyomoto, S., Bhuiyan, M.A., 2017. Privacy friendly secure bidding for smart grid demand-response. Inf. Sci. 379, 229−240.

Rathnayaka, A.J.D., Potdar, V.M., Dillon, T., Hussain, O., Kuruppu, S., 2014. Goal-oriented prosumer community groups for the smart grid. IEEE Technol. Soc. Mag. 33 (1), 41−48.

Regev, O., 2009. On lattices, learning with errors, random linear codes, and cryptography. J. Assoc. Comput. Mach. 56 (6), 1−40.

Shor, P., 1994. Algorithms for quantum computation: discrete logarithms and factoring. In: 35th Annual Symposium on Foundations of Computer Science, pp. 124−134.

Sun, Z., Song, Z.C., 2017. Security and privacy-preserving metering service in the smart grid. Int. J. Commun. Netw. Syst. Sci. 10 (08), 307−315.

Tonyali, S., Saputro, N., Akkaya, K., 2015. Assessing the Feasibility of Fully Homomorphic Encryption for Smart Grid AMI Networks. In: IEEE Seventh International Conference on Ubiquitous and Future Networks (ICUFN), pp. 591−596.

Tonyali, S., Akkaya, K., Saputro, N., Uluagac, A.S., 2016. A reliable data aggregation mechanism with homomorphic encryption in smart grid AMI networks.

 https://doi.org/10.1016/j.heliyon.2019.e01321

In: 13th IEEE Annual Consumer Communications and Networking Conference. CCNC), pp. 550–555.

Tonyali, S., Akkaya, K., Saputro, N., Uluagac, A.S., Nojoumian, M., 2018. Privacy-preserving protocols for secure and reliable data aggregation in IoT-enabled smart metering systems. Future Gener. Comput. Syst. 78, 547–557.

Vahedi, E., Bayat, M., Pakravan, M.R., Aref, M.R., 2017. A secure ECC- based privacy preserving data aggregation scheme for smart grids. Comput. Netw. 129, 28–36.

Wu, Y., Huang, Z., Zhang, J., Wen, Q., 2012. A Lattice-Based Digital Sig- Nature from the Ring-LWE. In: IC-NIDC 2012: 3rd IEEE International Conference on Network Infrastructure and Digital Content, Beijing, China, pp. 646–651.

Zhang, L., Tang, S., Jiang, Y., Ma, Z., 2013. Robust and efficient authentication protocol based on elliptic curve cryptography for smart grids. In: Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing, pp. 2089–2093.

Zhao, F., Li, C., Liu, C.F., 2014. A cloud computing security solution based on fully homomorphic encryption. In: 16th International Conference on Advanced Communication Technology. ICACT), pp. 485–488.

Zhu, H., Liu, F., Yan, R., Li, H., 2015. PAS: an efficient privacy- preserving multi-dimensional aggregation scheme for smart grid. Int. J. Distributed Sens. Netw. 11 (10), 915795.

 https://doi.org/10.1016/j.heliyon.2019.e01321