Secure and Efficient Cryptosystem for Smart Grid Using Homomorphic Encryption

Xingze He[1], Man-On Pun[2], and C.-C. Jay Kuo, *Fellow, IEEE*[1]

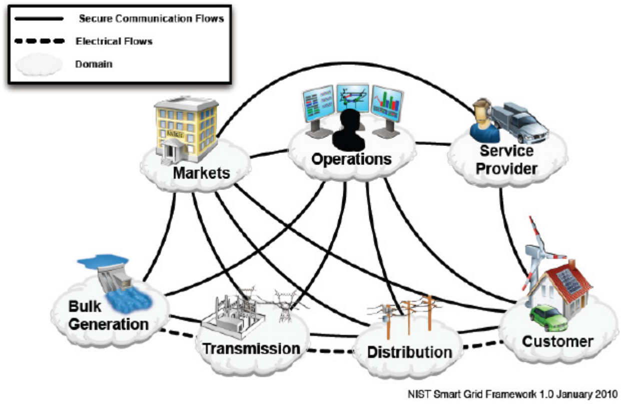
[1]Ming Hsieh Department of Electrical Engineering,University of Southern California,Los Angeles,CA
[2]Mitsubishi Electric Research Laboratories,Cambridge,MA

***Abstract*—A secure and efficient cryptography-based data exchange scheme for the smart grid based on homomorphic encryption is investigated in this work. Public key cryptography has been proposed as the main tool to ensure the security of a smart grid [1]. We first examine the shortcomings of conventional public key cryptography to motivate our current study. For the uplink communication (*i.e.* from customers to the utility) in the proposed scheme, smart meters homomorphically encrypt privacy-sensitive customer data before sending them over the grid. To prevent message forgery, a simple authentication scheme is designed sepcifically for uplink communication. For the downlink communication (*i.e.* from the utility to customers), the utility transmits the signed control messages to customers using digital signatures to ensure that messages from utilities are not tampered. For the data exchange scheme, we propose a practical cryptosystem based on a partially homomorphic encryption algorithm. The proposed solution has several appealing features such as strengthened security, high efficiency and user privacy preservation.**

***Index Terms*—Homomorphic Encryption, Public Key, Smart Grids**

I. Introduction

Empowered by the modern digital communication technology, the smart grid system has been envisaged as the next-generation power delivery system to provide reliable, economic and enviromentally friendly electricity service. While research is still in progress towards defining each key technology of smart grid,a typical smart grid is composed of seven domains as shown in Fig. 1, which are bulk generation, transmission, distribution, customers, service providers, operations, and markets [2]. In this conceptual model, customers closely interact with three domains: namely, markets, operations and service providers to boost system automation and intelligence. In this process, frequent data exchanges between different domains are essential.



NIST Smart Grid Framework 1.0 January 2010

Fig. 1. Illustration of the smart grid conceptual model [2].

Messages transmitted through the smart grid may contain sensitive data related to customers' privacy. For example, customer's daily power usage profile can be exposed to the utility as shown in Fig. 2. Through analysis, the utility can easily dectect customers' activities at home (*e.g.*, waking up and watching TV) and the number of people in a household. If these data are not properly protected, they can be exploited by adversaries to gain illegitimate advantages from targeted households and/or their business competitors. Furthermore, malicious attackers may use the data to launch large-scale attacks on the electrical grid [1], [3]. The system is particularly vulnerable when wireless transmission or a public network (*e.g.* the Internet) is used for data transmission since transmitted data can be easily intercepted.

Although information security and privacy protection have not yet been well studied in traditional utility grids, novel security schemes are demanded in smart grid to protect communication between different parties. The main objective of this research is to develop a secure data exchange scheme for smart grid.

To expedite the standardization progress, the National Institute of Standards and Technology (NIST) discussed smart grid privacy and security issues in a sequence of documents [1], [5], [6] and provided some high-level solutions. Elaboration on smart grid security attributes was provided by the Department of Energy (DOE) of the US Government in [7]. Recently, DOE allocated $20 million research funding on cybersecurity for the US electrical grid, among which $3.1 million is earmarked for the development of a centralized cryptographic key management system. Discussion in [1], [5]–[7] primarily focuses on the conceptual security architecture of a smart grid. The design detail is still lacking.

Also,some efforts have been taken to address the smart grid

Xingze He and C.-C.Jay Kuo are with the Ming Hsieh Department of Electrical Engineering,University of Southern California, Los Angeles, CA 80089, USA (e-mails:xingzehe@usc.edu; cckuo@sipi.usc.edu).

Man-On Pun is with the Mitsubishi Electric Research Laboratories(MERL), Cambridge, MA 02139, USA (e-mail: mpun@merl.com).

978-1-4577-2159-5/12/$31.00 ©2011 IEEE

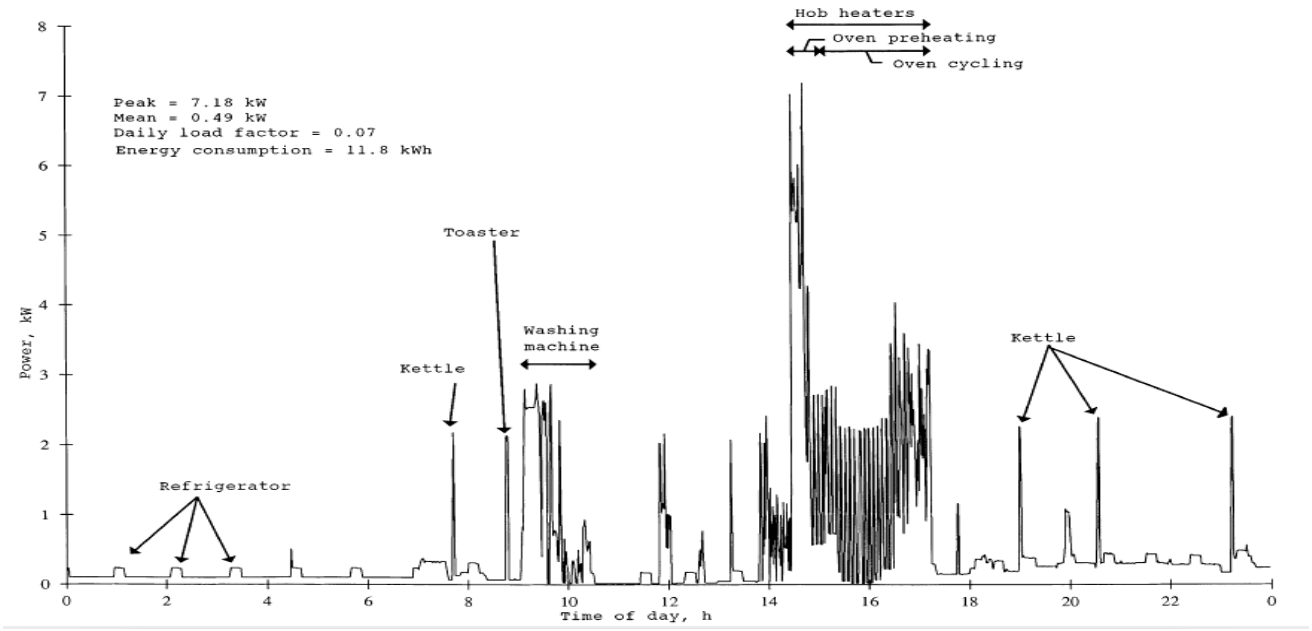


Fig. 2. Power usage to personal activity mapping [4].

security and privacy issues in the area of key management. For example, Khurana *et al.* [8] described smart grid security issues with emphasis on complexity and scalability of key management. Metke and Ekl [9] investigated smart grid security technologies, including the public key infrastructure and trusted computing. A secure information aggregation scheme for the smart grid system was proposed by Li, Luo and Liu [10] using homomorphic encryption. Although it is secure and efficient, its application is limited to information aggregation only and a more powerful homomorphic encryption scheme is needed to overcome this obstacle. Along this line, we notice a recent breakthrough in homomorphic cryptography made by Gentry [11], which offers fully homomorphic encryption using ideal lattices. Gentry's scheme supports both additive and multiplicative homomorphism and its potential is great. Despite its powerful functionalities, the complexity of Gentry's scheme is very high, and its application to a practical smart grid system is still in question.

In this work, being motivated by the above observation, we propose a secure and efficient cryptography-based data exchange scheme adopting homomorphic encryption technique. On the basis of this scheme and a partially homomorphic encryption algorithm, a practical cryptosystem is designed specifically for smart grid. The proposed cryptosystem supports an arbitrary number of additions and single multiplication on encrypted data, which differentiates this work from that in [10].

The rest of this paper is organized as follows. We first introduce two techniques adopted in our proposed scheme (*i.e.* public key cryptosystem and homomorphic encryption) in Sec. II. Then, we examine the data exchange scheme using homomorphic encryption in Sec. III. A practical cryptosystem based on a recently proposed partially homomorphic encryption is presented in Sec. IV and two applications of the proposed cryptosystem are discussed in Sec. V. Finally, concluding remarks are given in Sec. VI.

II. Public Key Cryptosystem and Homomorphic Encryption

A. Public Key Cryptosystem

In a public key cryptosystem as shown in Fig. 3, each recipient generates a pair of public and secret keys, where the public key is made open to others while the secret key is kept confidential. If someone wants to send a message to the recipient, the public key is used to encrypt the message to protect its content. Once the recipient receives the encrypted message, the secret key is used to decrypt the encrypted message so as to recover the original message. This process is called public key encryption.

The public key cryptosystem also supports the authentication of a message. That is, a message signed with a digital sigature, which is generated from sender's private key, can be verified by anyone with access to the corresponding public key. Through this verification process, the recipient can ensure sender's identity and whether the message has been tampered or not in the transmission.

Unlike the symmetric key crytosystem, the secure initial exchange of secret keys between the sender and the receiver is not required in the public key cryptosystem. Therefore, the public key cryptosystem has been widely used in large scale public networks such as the Internet. The security of this cryptosystem is generally built upon some mathematical properties such as problems of discrete logarithm and integer factorization that cannot be solved efficiently.

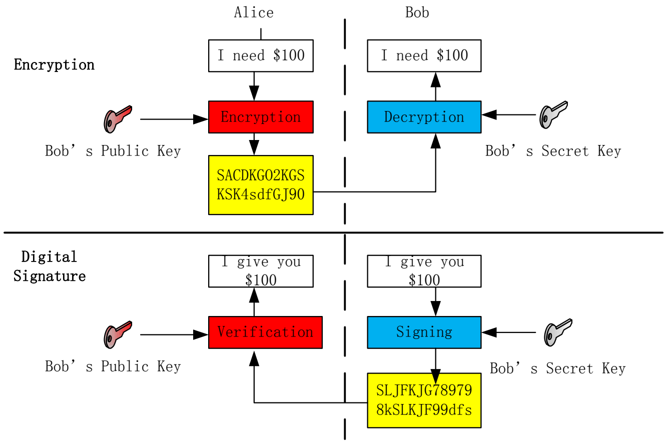


Fig. 3. Illustration of the public key cryptosystem.

B. Homomorphic Encryption

Given messages $m_1, m_2 \in Z_N$, a homomorphic encryption function $Enc()$ can be rewritten as

$$Enc_k(m_1 \circ m_2) = Enc_k(m_1) \bullet Enc_k(m_2), \qquad (1)$$

where $\circ$ and $\bullet$ are two different operators. Homomorphic encryption is a semantically secure cryptographic scheme in the sense that users can delegate the processing work on their private data (as indicated by the left-hand-side of the above equation) to others without revealing the data content (as shown by the right-hand-side of the above equation). Homomorphic encryption finds applications in secure voting, private information retrieval, etc. Once some efficient fully homomorphic encryption technique is explored, it can also be used in cloud computing.

Based on the supported functionality, homomorphic encryption schemes can be classified into two types – partially homomorphic encryption and fully homomorphic encryption. Partially homomorphic encryption has more restrictions on its supported operation (only addition, multiplication, or polynomials up to certain degrees) while fully homomorphic encryption supports both additions and multiplications. The latter is more powerful and flexible. Examples of partially homomorphic encryption schemes include: RSA [12], Pailer [13], etc. Fully homomorphic encryption schemes were better understood until recently and reported in [11], [14].However,they are still computationally too expensive to be used in practical applications today.

III. Data Exchange Scheme for Smart Grid

In the conventional public key cryptosystem, every terminal device of a two-way communication channel has to generate a pair of public and secret key for secure data exchange. In a large scale network such as the smart grid, efficient management of millions of keys is a challenging problem. Besides, the use of a key in every message reduces the efficiency of network transmission tremendously. This is especially critical in a smart grid due to its limited bandwidth and timeliness requirement.

By exploiting the fact that a smart grid system is a multi-to-one communication network (*e.g.* multiple users but one service provider) and that there exist different security and privacy requirements on the uplink and the downlink communications in a power system, we propose a highly efficient data exchange scheme without compromising system security.

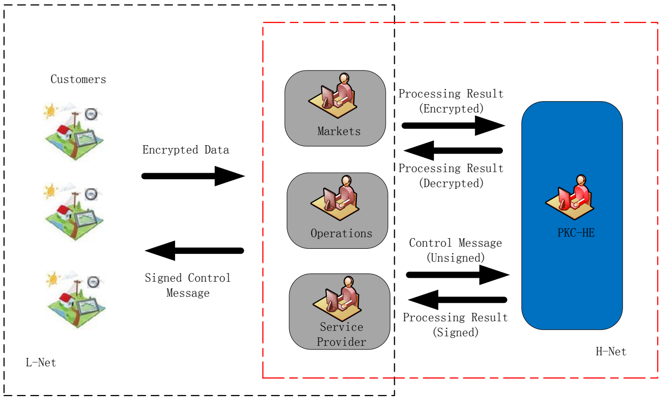

Customers
Encrypted Data
Signed Control Message
L-Net
Markets
Operations
Service Provider
Processing Result (Encrypted)
Processing Result (Decrypted)
Control Message (Unsigned)
Processing Result (Signed)
PKC-HE
H-Net

Fig. 4. Proposed data exchange scheme in Smart Grid.

The proposed data exchange scheme in smart grid is shown in Fig. 4. Being independent of the original seven domains shown in Fig. 1, another sub-system called the PKC-HE sub-system is introduced. The PKC-HE sub-system, which is the only module that has the access to the secret key, is responsible for key generation, distribution, decryption and message signing.

In the proposed data exchange scheme, operations, markets, service provider and PKC-HE form a small communication network, which is called the H-Net. Owing to the small scale of the network and infrequent communications, we still adopt the conventional public key cryposystem that protects the system to the highest degree. For the communications between customers and other domains (*i.e.* operations, markets and service providers), we called it L-Net. A secure and efficient solution is proposed by incorporating the PKC-HE sub-system.

The proposed scheme works with the following procedures.

1) Key Generation and Distribution
The proposed key generation and distribution procedure is shown in Fig. 5. The PKC-HE sub-system generates a pair of public key (PK) and secret key (SK) for the communication of L-net at time T. For key distribution, PKC-HE simply broadcasts generated public key to customers while keeping the secret key confidential. The keys will remain active for a predefined period of time before PKC-HE sub-system re-generates and distributes new keys. In contrast to a conventional public key cryptosystem where two pairs of public and private keys are generated for every point-to-point communication link, only one pair of public and private keys is needed for communications between customers and other domains (*i.e.* operations,markets,service providers)

in our proposed scheme. Please note that, additional pairs of publc and secret keys are needed for the communication in the H-Net.For instance, a network consisting of 500 customers, more than 1000 keys are needed in a conventional public key cryptosystem while less than 10 keys is enough in our proposed scheme. Thanks to the small number of keys, the generation, distribution and other management work becomes easy.

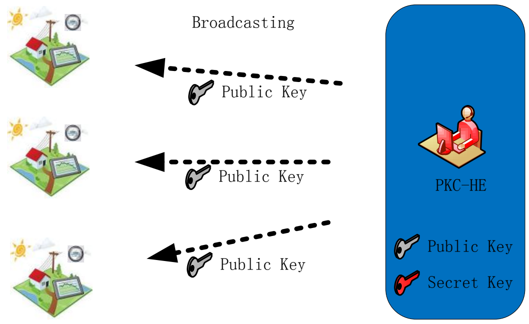


Fig. 5. Key generation and distribution procedure.

2) Uplink Communication
The operations in the proposed uplink communication are depicted in Fig. 6, where User A and User B share the same public key (PK) which is generated and distributed by PKC-HE sub-system. Before every transmission, users first homomorphically encrypt their messages under PK. Then, the encrypted messages are sent to the sepcific domain (operations, markets or service providers) through a public network (*e.g.* the Internet). Since only PKC-HE sub-system can access the private key, no one else can decrypt users' data in the transmission. To the highest extent, this custody method prevents adversaries from decrypting data in the transmission over the public network. The concern that an untrusted party (*e.g.* a third party company in the marketing domain) would leak users' data is also eliminated.

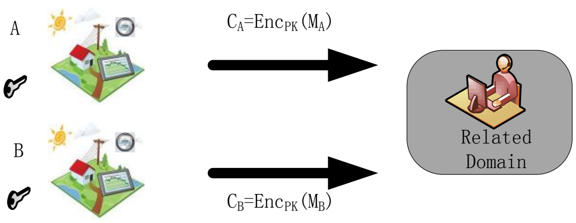
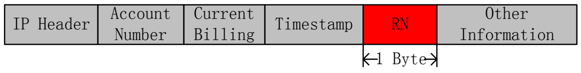


Fig. 6. Operations in the uplink communication.

To prevent data forgery, a simple authentication scheme is designed for the uplink communication. We add a byte to the output message of the smart meter as shown in Fig. 7. A random number is generated and stored in the byte right after new key's generation and distribution. After the transmission of every message, the random number is increased by 1. With the preknowledge of the initial random number, it is convinient to check whether the message has been forged or not based on the information embedded in the message. Suppose that smart meter sends power usage data in a period of T_s seconds, the initial random number generated at time t_i is N_i, the random number shown in the received message is N_p, the receiving time is t_p. Then, we can check using the following equation

$$\frac{t_p - t_i}{T_s} = N_p - N_i, \tag{2}$$

The verification of the above equation proves the correctness of the sender's identity, and vice versa. Thus, forged messages can be easily detected.



IP Header	Account Number	Current Billing	Timestamp	RN	Other Information
				1 Byte	

Fig. 7. Extended packet format.

3) Data Processing and Analysis
With the property of fully homomorphic encryption, domains such as markets, operations and service providers are able to implement any kind of calculation and processing on encrypted customers' data. The processed result is then sent back to PKC-HE sub-system, the only party who can access the secret key, for decryption as shown in Fig. 8. After decryption, PKC-HE sub-system sends the decrypted result back to domains for further analysis. Note that the communication in the H-Net is protected under the conventional public key cryptosystem.

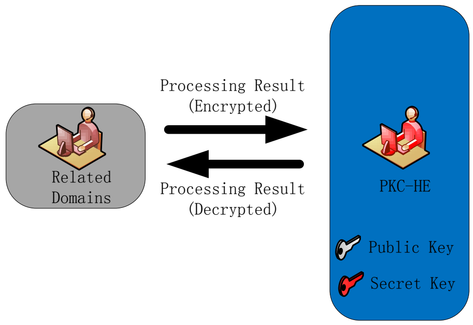
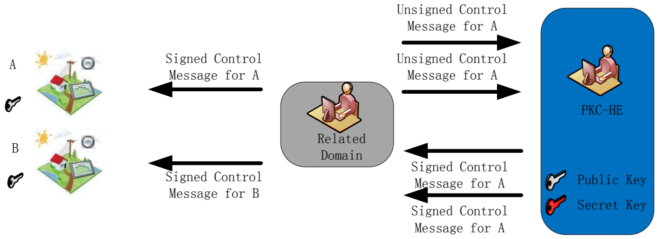


Fig. 8. Data processing and analysis.

4) Downlink Communication
Operations in the proposed downlink communication are shown in Fig. 9, where the main concern is authentication, *i.e.*, validation of the identity of the message sender. Without a proper authentication scheme, adversaries may forge and send faked control messages to users

to result in network breakdown. As shown in Fig. 9, domains such as the service providers first send control messages to PKC-HE to generate the digital sigature using the secret key. After receiving the digital signature, domains send the signed message to cutomers. With this signed message, customers can verify sender's identity using the shared public key.



Unsigned Control Message for A
A
Signed Control Message for A
Unsigned Control Message for A
PKC-HE
Related Domain
B
Signed Control Message for B
Signed Control Message for A
Public Key
Secret Key
Signed Control Message for A

Fig. 9. Operations in the downlink communication.

The efficiency of the proposed cryptosystem is evidenced by the fact that only two keys are generated while one key is broadcasted to all users for the L-Net communication. In addition, since all users share the same public key, key maintenance is efficient. For users who lost the public key, they can query it from their neighbors. Besides, key revocation is easy since it can be implemented via PKC-HE sub-system. In the proposed cryptosystem, PKC-HE is the only sub-system responsible for key generation and distribution. Other devices (such as smart meters) or systems do not have to support these functions, thereby satisfying some design requirements such as the size and complexity.

The security of the proposed cryptosystem relies on the security of the adopted public key algorithm as well as the confidentiality of the secret key. In the proposed public key cryptosystem, the introduction of PKC-HE sub-system seperates the decryption and the signing processes from others. Consequently, only PKC-HE is able to access the secret key in the whole system. The confidentiality of the secret key is high. To further strengthen system security, the system can periodically or randomly update the keys. Since all customers share the same public key, the key generation and distribution can be done efficiently.

IV. Practical Cryptosystem Using Partially Homomorphic Encryption

In the previous section, we introduced a secure and efficient data exchange scheme where the homomorphic encryption technique is used. As the best choice, fully homomorphic encryption disscussed in Sec. II is able to support any kind of processing on the encrypted data for different purposes. However, current fully homomorphic encryption algorithms in [11], [14] are computationally expensive so that they are still not practical in the real world system. Some partially homomorphic encryption schemes were proposed with lower complexity such as RSA [12] and Paillier [13]. However, most of them only support either the addition or the multiplication operation on encrypted data, which imposes some limitation on their applications.

To build a practical cryptosystem, in this section, we consider a partially homomorphic encryption algorithm recently reported by Goh [15] in the proposed data exchange scheme as described in Sec. III. It allows an arbitray number of additions and a single multiplication on the encrypted data. This property is generally enough in most applications in the context of the power grid. Some important applications in smart grid will be discussed in Sec. V.

A. Goh's Partially Homomorphic Encrytion Algorithm

Goh's partially homomorphic encryption scheme consists of the following procedures [15].

1) $KeyGen(\tau)$: Given security parameter $\tau \in Z^+$, algorithm $\Phi(\tau)$ is used to generate a tuple (q_1, q_2, G, G_1, e), where q_1, q_2 are two random τ bit primes, G,G_1 are groups of order $n = q_1 q_2$ and $e : G \times G \longrightarrow G_1$ is a bilinear map. Then two random generators $g, u \xleftarrow{R} G$ are selected. Set $h = u^{q_2} \in G$.Then, $PK = (n, G, G_1, e, g, h)$ is the public key and $SK = q_1$ is the private key.Note that,all the above operations can be computed in polynomial time in τ [15].

2) $Encrypt(PK, m)$: To encrypt a message m, a variable $r \xleftarrow{R} [0, n-1]$ is first randomly selected. Assume the message space consists of integers in set $0, 1, ..., T$ with $T < q_2$, we compute the ciphertext as follows,

$$CT = g^m h^r \in G.$$

Again, the group operations in G can be computed in polynomial time in τ.

3) $Decrypt(SK, CT)$: In order to decrypt a ciphertext CT, we directly compute the discrete logarithm of $(CT)^{q_1}$ with base $\hat{g}$, where $\hat{g} = g^{q_1}$.Because

$$(CT)^{q_1} = (g^m h^r)^{q_1} = (g^{q_1})^m \in G.$$

Since $0 \leq m \leq T$, this operation demands an expected time of $\hat{O}(\sqrt{T})$ using Pollard's lambda method [15].

This partially homomorphic algorithm can support arbitrary number of additions and a single multiplication on ciphertexts. The homomorphism is explained below [15].

- Additive Homomorphism
  Given $A = g^a h^r$ and $B = g^b h^s$, where $g, h \in G$, r and s are randomly chosen from $[0, n-1]$, the encryption of $a + b$ takes the following form:
  $$C = ABh^t = g^{a+b} h^{r+s+t} \in G \qquad (3)$$
  where $t \in Z_n$ is randomly selected.
- Multiplicative Homomorphism
  Given $A = g^a h^r$ and $B = g^b h^s$, where $g, h \in G$, r and s are randomly chosen from $[0, n-1]$, the encryption of $a \times b$ can be computed as
  $$C = e(A, B) \times h_1^t = g_1^{ab} h_1^{r'} \in G_1, \qquad (4)$$
  where $g_1 = e(g, g)$, $h_1 = e(g, h)$ and $t, r' \in Z_n$ are randomly selected.

B. Extension of Goh's Algorithm

To prevent control message forgery as discussed in Sec. III, the digital signature is introduced in the proposed cryptosystem as shown in Fig. 10. However, Goh only proposed an encryption algorithm without discussing the authentication procedure. Here, we extend Goh's encryption algorithm to support both the signing and the verification process in the downlink communication under the same pair of public and secret keys.

- Signing Process

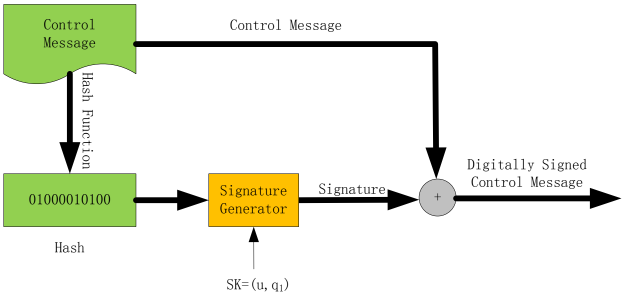


Fig. 10. Signing Process.

For a signing process, as shown in Fig. 10, a digital signature is needed. To generate a digital signature using secret key SK, we propose to select $r \xleftarrow{R} [0, n-1]$ randomly and compute

$$DS(PK, SK, m) = u^{H(m)/q_1} g^r,$$

where u and g are two public keys, q_1 is secret key,$H()$ is the hash function and m is the message to be sent. Note that group operations involved here could be computed in polynomial time of parameter τ [16].

- Verification Process

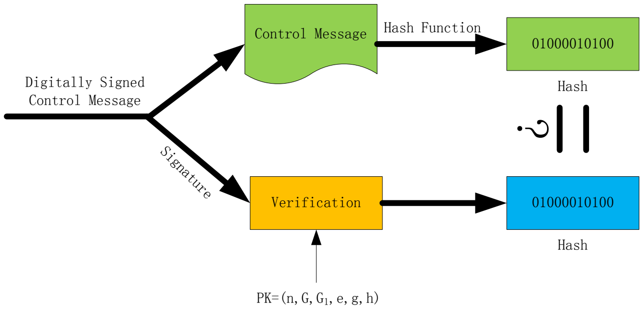


Fig. 11. Verification process.

Every control message is authenticated using the digital signature generated in the above step. Specifically, after receiving the signed message, users first verify the message.To verify a message using the public key $PK = (n, G, G_1, e, g, h)$, we compute

$$(DS)^n = (u^{m/q_1} g^r)^n = u^{q_2 m} = (u^{q_2})^m = h^m.$$

Note that m can be recovered by computing the discrete logarithm of $(DS)^n$ with base of h. As mentioned above, this operation takes expected time $\hat{O}(\sqrt{T})$ using the Pollard's lambda method. This process is depicted in Fig. 11. The same as the encryption scheme proposed by Goh, the signing and verification process is semantic secure. Increasing the frequency of key update also strengthens the security of the authentication process.

V. Applications

A. Secure and Efficient Information Aggregation

Information aggregation is an important operation in some proposed smart grid communication infrastructure (*e.g.* the wireless-wired multi-layer architecture) [3], [17]–[19]. In the network architecture as shown in Fig. 12, each neighborhood has a data collector to collect desired users data. For example, suppose that the service provider wants to know the average power consumption of the neighborhood. To do so, users send their power consumption data through an exclusive connection to the data collector. After receiving the data, the data collector calculates the mean value of power consumption and reports to the service provider. Without an effective protection technique, users data are vulnerable to interception either during the transmission or during the processing at data collector.

The proposed cryptosystem offers a secure and efficient solution to elliminate this concern since all data transmitted within the L-Net are encrypted data. Except for PKC-HE subsystem, no other units can access the original information but the encrypted data. Furthermore, the proposed cryptosystem can be used to improve the efficiency of information aggregation using in-network incremental aggregation [10].

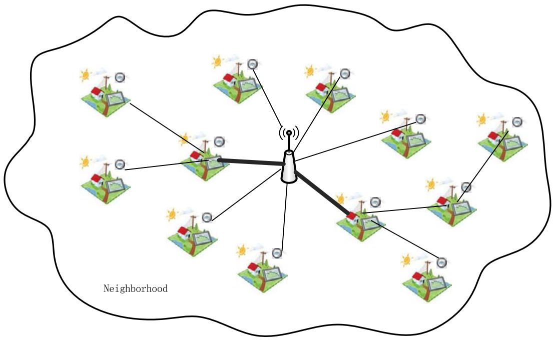


Fig. 12. Data aggregation in a smart grid.

B. Privacy Guaranteed Statistical Analysis

Besides providing secure information aggregation for a smart grid, the proposed cryptosystem offers a secure way to perform statistical analysis on encrypted data. In other words, it allows the utility or a untrusted third party to analyze the general consumer behavior based on encrypted data so that individual's privacy can be protected. In the following, we discuss two secure statistic analysis tasks – one for utilities and the other for an untrusted third party.

Accurate statistical analysis of power data helps an utility company evaluate the current grid status and plan for future power production and distribution. With the proposed cryptosystem, an utility directly processes encrypted user data and sends the processed result (in encrypted form) to PKC-HE sub-system for decryption. The processed result (in decrypted form) will be sent back to the utility for further analysis and operation.

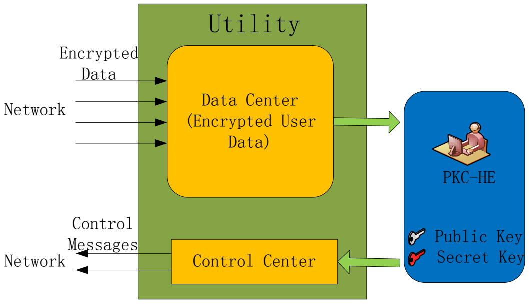


Fig. 13. Statistical analysis conducted by utilities.

In many practical cases, a third party is also interested in getting statistical knowledge of user data. For instance, a company may be interested in understanding consumers' power consumption behavior for commercial purpose. However, since the third party may be untrusted, plain user data should not be released. The third party may gather homomorphically encrypted user data from the public network and/or from utilities. By exploiting the additive and multiplicative homomorphism properties, the third party can extract useful statistical information about the underlying plain data without decrypting them. As shown in the block diagram in Fig. 14, this can be achieved as follows.

1) The third party registers in the public key infrastructure (PKI) of the conventional public key cryptosystem used in H-Net
2) The PKI authorizes the third party in the system
3) The third party gathers encrypted data by either directly collecting them from the public network or receiving them from a trusted party.
4) The third party extracts useful statistical information.Results are in encrypted form.
5) The encrypted results are sent to PKC-HE sub-system for decryption.
6) The decrypted results are sent back to the third party.

As an example, we show how to derive the mean and the variance of the underlying data below. Without loss of generality, we assume N users in a neighborhood. Given encrypted power consumption data $c_1, c_2, \cdots, c_N$, the mean and variance of the corresponding original power consumption data $m_1, m_2, \cdots, m_N$ can be computed as follows.

- Mean Value

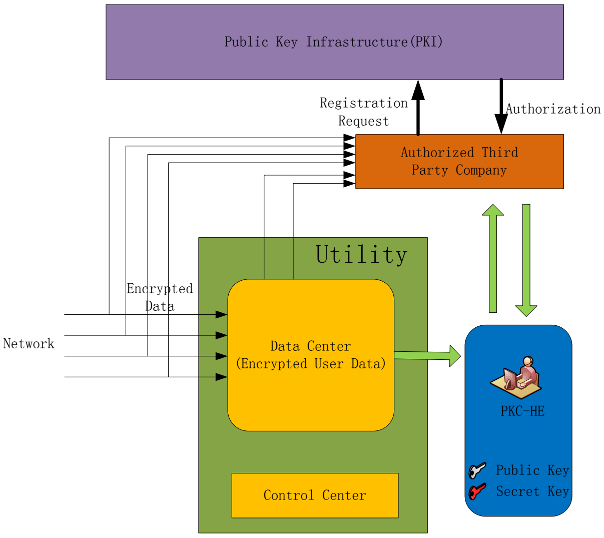


Fig. 14. Statistical analysis conducted by the third Party.

The mean of the plain data is defined as $\overline{m} = Dec_{sk}(C_{\overline{m}})$.By exploiting the additive homomorphism,the encrypted mean value $C_{\overline{m}}$ can be computed from the encrypted data as

$$C_{\overline{m}} = Enc_{pk}(\overline{m}) = \prod_{j=1}^{N} c_i \cdot h^t, \tag{5}$$

where $C_{\overline{m}}$ is the encrypted mean value. After decryption, we can get the mean value of the plain data.

- Variance
The variance of the plaintext $m_i, i = 1, .., N$ can be obtained by

$$\begin{aligned} v_m &= \frac{1}{N-1} \sum_{i=1}^{N} (m_i - \overline{m})^2 \qquad (6) \\ &= \frac{1}{N-1} \sum_{i=1}^{N} m_i^2 - \frac{N}{N-1} \overline{m}^2. \qquad (7) \end{aligned}$$

With the homomorphic property, we can obtain v_m in terms of $c_i, i = 1, ..., N$ with the following three steps.

- **STEP 1**: Calculate $C_1 = Enc_{pk}(\overline{m})$ from Eq. (5).
- **STEP 2**: Calculate $C_2 = Enc_{pk}(\sum_{i=1}^{N} m_i^2)$ by

$$\begin{aligned} C_2 &= Enc_{pk}(\sum_{i=1}^{N} m_i^2) \qquad (8) \\ &= \prod_{i=1}^{N} (e(c_i, c_i) \cdot h_1^{r_i}) \cdot h^s. \qquad (9) \end{aligned}$$

- **STEP 3**: Calculate the variance of plaintext data V_m by

$$v_m = \frac{Dec_{sk}(C_2) - NDec_{sk}(C_1)^2}{N-1} \tag{10}$$

where s and $\{r_i, i = 1, ...N\}$ are randomly chosen from $[0, n-1]$, $h = e(g, g)$, $h_1 = e(g, h)$.

VI. Conclusion

With the introduction of homomorphic encryption technique, a secure and efficient data exchange scheme was proposed for the smart grid system. Then, a practical cryptosystem was designed by adopting Goh's partially homomorphic encryption scheme and its extension. With the proposed cryptosystem, a smart grid can provide protection for both uplink and downlink communications efficiently. Moreover, the proposed cryptosystem can adjust the security level of the whole system in terms of different security requirements. Thanks to additive and multiplicative properties, all processing work at the utility side can be done on encrypted data without the need of decrypting each single message. With this feature, applications such as data aggregation and statistical analysis can be accomplished in a secure and efficient way.

References

[1] The Smart Grid Interoperability Panel-Cyber Security Working Group, NIST, *Guidelines for Smart Grid Cyber Security: Vol.1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements*. National Institute of Standards and Technology, 2010.

[2] Office of the National Coordinator for Smart Grid Interoperability, *NIST Framework and Roadmap for Smart Grid Interoperability Standards*, release 1.0 ed. National Institute of Standards and Technology, 2010.

[3] P.McDaniel and S.McLaughlin, "Security and privacy challenges in the smart grid," *Security Privacy, IEEE*, vol. 7, no. 3, pp. 75–77, 2009.

[4] E. L. Quinn, "Smart metering and privacy: Existing law and competing policies," *Available:http://www.dora.state.co.us*, p. 3, Spring 2006.

[5] The Smart Grid Interoperability Panel-Cyber Security Working Group, NIST, *Guidelines for Smart Grid Cyber Security: Vol.2, Privacy and the Smart Grid*. National Institute of Standards and Technology, 2010.

[6] The Smart Grid Interoperability Panel-Cyber Security Working Group, *Guidelines for Smart Grid Cyber Security: Vol.3, Supportive Analyses and References*. National Institute of Standards and Technology, 2010.

[7] U.S. Department of Energy Office of Electricity Delivery and Energy Reliability, *Study of Security Attributes of Smart Grid Systems-Current Cyber Security Issues*. U.S. Department of Energy Office of Electricity Delivery and Energy Reliability, 2009.

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

[9] A. R. Metke and R. L.Ekl, "Security technology for smart grid networks," *IEEE Transaction on Smart Grid*, vol. 1, no. 1, pp. 99–107, June 2010.

[10] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," Gaithersburg, MD, pp. 327–332, Oct 2010.

[11] C. Gentry, "Fully homomorphic encryption using ideal lattices," New York, NY, 2009.

[12] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–128, Feb 1978.

[13] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Theory and Application of Cryptographic Techniques*, 1999, pp. 223–238.

[14] M. van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, "Fully homomorphic encryption over the integers," in *Theory and Application of Cryptographic Techniques*, 2010, pp. 24–43.

[15] E.-J. Goh, "Encryption Schemes from Bilinear Maps," *Department of Computer Science, Stanford University*, Sep 2007.

[16] D. R. Stinson, *Cryptography: theory and practice*, 3rd ed. Chapman and hall/CRC, 2006.

[17] W.H.Sanders, "Progress towards a resilient power grid infrastructure," in *Proceedings of the IEEE Power and Energy Society General Meeting*, 2010.

[18] A. Engelen and J. Collins, "Choices for smart grid implementation," in *HICSS 10*, 2010, pp. 1–8.

[19] A. Bose, "Smart transmission grid applications and their supporting infrastructure," *IEEE Transactions on Smart Grid*, 2010.

Xingze He received the B.S.and M.S.degrees in the Department of Communication and Information System at Xi'an Jiaotong University, Xi'an, in 2007 and 2009 respectively. He is a Ph.D candidate in Ming Hsieh Department of Electrical Engineering at University of Southern California (USC). His current research interest is in the area of Smart Grids including power quality problem detection,public key cryptography and homomorphic encryption.

Man-On Pun received the BEng (Hon.) in Electronic Engineering from the Chinese University of Hong Kong in 1996, the MEng. degree in Computer Science from University of Tsukuba, Japan in 1999 and the Ph.D. degree in Electrical Engineering from the University of Southern California (USC) in 2006, respectively. He joined the Mitsubishi Electric Research Labs (MERL), Cambridge, MA as Research Scientist in 2008. Prior to MERL, he held research positions at Princeton University from 2006 to 2008 and Sony Corporation, Tokyo from 1999 to 2001. Dr. Pun received the MERL president's award in 2009 and three best paper awards from Infocom 2009, ICC 2008 and VTC-Fall 2006. He serves as Associate Editor of the IEEE Transactions on Wireless Communications.

C.-C. Jay Kuo received the B.S. degree from the National Taiwan University, Taipei, in 1980 and the M.S. and Ph.D. degrees from the Massachusetts Institute of Technology, Cambridge, in 1985 and 1987, respectively, all in Electrical Engineering. He is Director of the Signal and Image Processing Institute (SIPI) and Professor of Electrical Engineering, Computer Science and Mathematics at the University of Southern California (USC). His research interests are in the areas of digital image/video analysis and modeling, multimedia data compression, communication and networking and multimedia database management.Dr. Kuo has guided 108 students to their Ph.D. degrees and supervised 23 postdoctoral research fellows. He is a co-author of about 200 journal papers, 800 conference papers and 10 books. Dr. Kuo is a Fellow of AAAS, IEEE and SPIE. He is Editor-in-Chief for the Journal of Visual Communication and Image Representation, and Editor for 10 other international journals. Dr. Kuo received the National Science Foundation Young Investigator Award (NYI) and Presidential Faculty Fellow (PFF) Award in 1992 and 1993, respectively. He was an IEEE Signal Processing Society Distinguished Lecturer in 2006, the recipient of the Electronic Imaging Scientist of the Year Award in 2010 and the holder of the 2010-2011 Fulbright-Nokia Distinguished Chair in Information and Communications Technologies.