Journal of Information Hiding and Multimedia Signal Processing ©2017 ISSN 2073-4212
Ubiquitous International Volume **8**, Number **3**, May **2017**

A Provable Private Data Aggregation Scheme Based on Digital Signatures and Homomorphic Encryption for Wireless Sensor Networks

Haiyun Ma[1], Zhonglin Zhang[2], Haifeng Li[3,*], Shou-Lin Yin[4] and Chu Zhao[4]

[1]School of Electronic Information and Electrical Engineering
Tianshui Normal University
Tianshui 741001, China

[2]School of Electronic and Information Engineering
Lanzhou Jiaotong University
Lanzhou 730070, China

[3]School of Software
Dalian University of Technology
Dalian 116620, China
*Corresponding author:lihaifeng8848@mail.dlut.edu.cn

[4]Software College
Shenyang Normal University
Shenyang 110034, China

Received August, 2016; revised December, 2016

Abstract. *Data aggregation of traditional wireless sensor networks can be used for data privacy calculation, preventing denial, defending internal and external attacks, tracking and fixing mistakes, but the security and efficiency of data aggregation is low. So in this paper we propose a provable private data aggregation scheme based on digital signatures and homomorphic encryption. First, we use ElGamal encryption scheme to encrypt privacy data and add the digital signature into identity information of sensor node, which makes the data from different nodes have identifiability. Therefore, this scheme has the ability of verifying data and tracking, fixing mistakes. Second, confidentiality interference factor method is introduced into this scheme to defending interior attack. Third, we adopt a confidentiality sum algorithm with homomorphic encryption property to build confidentiality interference factor method without trusted third party. That can avoid the safety and efficiency problem resulting from trusted third party. Finally, we give the security proof and efficiency analysis for our scheme. And comparison is given to demonstrate the performance of new scheme.*
Keywords: Wireless sensor networks data aggregation, ElGamal encryption, Digital signature, Confidentiality interference factor, Confidentiality sum algorithm, Homomorphic encryption

1. **Introduction.** As we all know, wireless sensor networks[1-3] contains several sensors and a base station, which has two structures: tree form and cluster form. The nodes communicate with each other by wireless link[4]. Sensors generally are provided with power by the battery energy, its storage and computing ability is less. Base station should know the structure of the whole networks, and has fixed energy with a strong storage and computing power. This paper aims at cluster structure network.

For data collection in wireless sensor networks, data aggregation[5-7] is a general method. An ideal wireless sensor data aggregation scheme has the following characteristic: resisting the attack of external and internal sensor networks; finding the possible transmission errors in the process of data transmission; ensuring that data from the sensor nodes cannot be tampered; ensuring the privacy of data, namely the transmission data is secret for the aggregators and potential eavesdroppers.

Currently, secure data aggregation technology for wireless sensor networks mainly includes three aspects. 1) Hop-to-hop data aggregation algorithm[8,9]. Early secure data aggregation protocol adopts point-to-point security solution based on symmetric encryption mechanism. Its advantage is easy to implement. But it adopts the symmetric encryption method, that easily results in leaking key and plaintext[10]. 2) End-to-end data aggregation algorithm. In order to protect data privacy, Westhoff et al.[11] first introduced privacy homomorphism encryption algorithm into wireless sensor and proposed end-to-end data aggregation protocol. However, nodes and base station used the same key, so this scheme had a risk of leaking key. Engouang et al.[12] presented pallier based homomorphic encryption data aggregation with security measures preserving data integrity and privacy. Li et al. [13] proposed fully homomorphic encryption based on secure data aggregation in large-scale wireless sensor networks which could protect end-to-end data confidentiality and support arbitrary aggregation operations over encrypted data. In addition, by utilizing message authentication codes, this scheme could verify data integrity during data aggregation and forwarding processes so that false data could be detected as early as possible. Fan et al. [14] used an additional trusted third party to distribute confidentiality interference factor. But encryption and signature approach is complex. Othman et al. [15] proposed a novel secure data aggregation scheme based on homomorphic encryption in wireless sensor networks. The scheme adopted a symmetric-key homomorphic encryption to protect data privacy and combined it with homomorphic signature to check the aggregation data integrity. But it was difficult to defend internal attack and execute signature verification. 3) Other methods such as data aggregation algorithm based on trust management model[16], data aggregation algorithm based on privacy protection[17] and data aggregation algorithm based on authentication and access control[18,19].

Therefore, we propose a provable private data aggregation scheme based on digital signatures and homomorphic encryption for wireless sensor networks. To protect privacy of aggregation data, we use the ElGamal encryption scheme with multiplicative homomorphic feature to encrypt privacy data and add digital signature with nodes identity information and random factors into plaintext. Before aggregation operation, it needs to verify digital signature, which makes the new scheme have the ability of defending data manipulation and denial, tracking and modifying error. In addition, we introduce confidentiality interference factor into node data to defend internal attacks and avoid security and computational cost problem caused by trusted third party.

The followings are the structures of this paper. In section2, we give some preliminaries. Section3 detailed introduces the provable private data aggregation scheme based on digital signatures and homomorphic encryption. We give the security analysis in section4. There is a conclusion in section5.

2. **Preliminaries.** In this paper, we use some symbolics as shown in table1. And we briefly introduce Co-Diffie-Hellman problem, bilinear map, attack model, semantic security and homomorphic encryption.

TABLE 1. Parameters

Symbol	Explanation
G	Cyclical group
$H: 0,1^* \to G$	A hash function
q	Prime number
$Z_q^* = Z_q/0$	Reversible elements set for modular multiply
$(a\|\|b)$	object a and b linked as a whole by order
$x \leftarrow B^R$	a value randomly selected from set B for variable x

2.1. **Co-Diffie-Hellman problem.** Co-Diffie-Hellman(CDH) group is a strong cryptography tool. It can be built by using the points in elliptic curve[20]. The subgroup pairing (G_1, G_2) of CDH problem can be explained as:

- Setting $a, b, c \in Z_q^*$.
- The computational problem of CDH. Given $(g, g^a \in G_2)$ and $h \in G_1$. Computing $h^a \in G_1$.
- The judgmental problem of CDH. Given $(g, g^a \in G_2)$ and $(h, h^b \in G_1)$. If $a = b$, return "YES", the (g, g^a, h, h^b) is CDH pairing. Otherwise, return "NO".

The advantage of algorithm A solving computational problem of CDH in group pairing (G_1, G_2) is:

$$Adv_{CDA_A} = Pr[A(g, g^a, h) = h^a : a \leftarrow Z_q^R, h \leftarrow G_1^R].$$

If algorithm A satisfies $Adv_{CDH_A} \geq \varepsilon$, and the biggest running time is t. The we call the algorithm solving computational problem of CDH in group pairing (G_1, G_2).

2.2. **Bilinear map.** Assuming that G_1 and G_2 are the multiplication cyclic groups of prime order q. $a, b \in Z_q^*$. A non-degenerate computable bilinear map $e: G_1 \times G_1 \to G_2$ has the following properties[21].

- Bilinearity: for all $g, h \in G_{1'}$, we have $e(g^a, h^b) = e(g, h)^{ab}$.
- Non-degeneracy: $e(g, h) \neq 1_{G_2}$.
- Efficient computability: there is a polynomial time algorithm to compute (g, h), for any $g_1, g_2, h \in G_1, e(g_1 \cdot g_2, h) = e(g_1, h) \cdot e(g_2, h)$, we have $e(g^a, h) = e(g, h^a)$.

2.3. **Attack model.** There are two attack models for wireless sensor networks: external attackers and internal attackers.

In general, the aim of the two attack models is to get encrypted data in networks transmission. Then it obtains the original data of each node by decryption. More advanced aim is to obtain the control right of some sensor nodes or the whole wireless sensor networks, then it can read, insert, modify and even counterfeit data.

In terms of attack ability[22], attacker not only can intercept all the data in each data aggregation stage, but they can acquire the whole networks topology structure, identity information and data aggregation scheme in network initialization stage. They also have password analysis ability and enough knowledge.

2.4. **Semantic security.** Semantic security[23] can be defined that although adversary gets the corresponding ciphertext of one message, he cannot obtain any information of this message.

IND-CPA game(IND game for public key encryption under chosen-plaintext attack) has the following processes:

1. Initialization. Challenger generates system ε, adversary obtains system public key PK.

2. Challenge. Adversary outputs two messages m_0 and m_1 with same length. Challenger randomly selects $b \in 0, 1$, encrypts m_b and sends ciphertext to adversary.
3. Guess. Adversary outputs b'. If $b' = b$, then adversary wins this game.

The advantage of adversary can be defined as:

$$Adv_A = \varepsilon(\lambda)|Pr[b' = b] - 1/2|. \tag{1}$$

Where λ is security parameter to determine the key length.

Definition. IND-CPA security. Let E be an encryption algorithm. If for any polynomial time adversary, there is a negligible function $neg(\lambda)$, $\varepsilon(\lambda) \leq neg(\lambda)$. Then algorithm E has the indistinguishability under chosen-plaintext attack, or it can be called IND-CPA security.

2.5. **Homomorphic encryption.** Homomorphic encryption can operate ciphertext and ensure that the decryption result is equal to original ciphertext. So homomorphic encryption is the first choice for secure computation.

Assuming that m_1 and m_2 are plaintexts. c_1 and c_2 are the corresponding ciphertexts. $Enc()$ and $Dec()$ are the encryption and decryption function respectively. $\bigoplus$ denotes the operation symbol for the two plaintexts. $Dec(c_1 \bigoplus c_2) = m_1 \bigoplus m_2$ is the general requirement of homomorphic encryption.

3. **Provable private data aggregation scheme based on digital signatures and homomorphic encryption.** There are some different ways to construct the wireless sensor networks, such as standard aggregation protocol[24]. We suppose that aggregator is half-honest and has enough computing power. Half-honesty refers to that it is honest, but it is curious. It may make some mistakes, but it cannot commit fraud with other entities. Enough computing power refers to that it can effectively complete the digital signature verification and the aggregation decryption.

After building wireless sensor networks, aggregation scheme includes three steps: setup, encryption-signature and verification-aggregation.

1. Setup stage.

   Supposing that aggregator controls n sensor nodes $U_i(i = 1, 2, \cdots, n)$. There are two tasks in this stage.

   - Initialization.
     - Allocating a identity information $ID_i(i = 1, 2, \cdots, n)$ for each sensor node.
     - Selecting security parameter λ.
     - Selecting two big prime numbers q_1 and q_2 and computing $N = q_1 \cdot q_2$.
     - Generating N order multiplication cyclic group G.
     - Selecting generator g and u in G.
     - Calculating $h = u^{q_2}$.
     - Releasing public key $(PK = N, g, h)$, private key $(SK = q_1)$.
   - Allocating confidentiality interference factor $\pi_i(i = 1, 2, \cdots, n)$ for sensor networks.

     Generation and distribution of confidentiality interference factor is a confidentiality aggregation process. In that it does not involve the key data m_i in this operation, it does not need high security, but high algorithm efficiency is required. So it can adopt simple methods(i.e. Privacy Homomorphism) to realize this confidentiality aggregation process. The steps of generation and distribution for confidentiality interference factor based on privacy homomorphism are as follows:

– Aggregator selects an integer $r \in Z_N$ and $r^{-1} \in Z_N$.
– Each sensor node U_i selects a random integer $\pi_i \in Z_N$.
– Each sensor node U_i computes $\pi_i^* = \pi_i \cdot r^i mod N$ and sends π_i^* to aggregator.
– After receiving data π_i^*, aggregator calculates $\sum_{i=1}^n \pi_i^* r^{-i}$ and gets $\sum_{i=1}^n \pi_i^* (mod N)$. Let $\pi_0 = -\sum_{i=1}^n \pi_i (mod N)$.

2. Encryption-signature.

When sensor node U_i receives the data aggregation order, it will execute the following operation.

- Reading data $m_i \in 0, 1, 2, \cdots, q_2$ and randomly selecting a private key $x_i \in Z_{q_1}$.
- Randomly selecting $r_i \leftarrow Z_N^{*R}$, computing $C_i = g^{\pi_i m_i} h^{r_i} \in G$.
- Calculating signature $\sigma_i = H(C_i || ID_i)^{x_i}$ and $y_i = g^{x_i}$.
- Sending C_i, y_i, σ_i to aggregator.

3. Verification-aggregation.

In this stage, aggregator executes the following process:

- Aggregator receives the data $C_i, y_i, \sigma_i, i = 1, 2, \cdots, n$ from sensor node U_i.
- Randomly selecting $\delta_i \leftarrow Z_{q_1}^R$ and selecting a non-degenerate computable bilinear map $e : G \times G \to G$, verifying whether $e(\prod_{i=1}^n \sigma_i^{\delta_i}, g) = \prod_{i=1}^n e(H(C_i || ID_i)^{\delta_i}, y_i)$. If it is true, all the aggregated data pass the verifying. Otherwise, for all $i = 1, 2, \cdots, n$, it needs to check that whether $e(\sigma_i, g) = e(H(C_i || ID_i), y_i)$ is true. Then it finds i satisfying the above equation and sends error information to sensor node. When all the data pass the verifying, it does next step.
- Computing $V = g^{\pi_0} \prod_{i=1}^n C_i = g^{\pi_0} \prod_{i=1}^n g^{\pi_i m_i} h^{r_i}$.
- Computing $V^{q_1} = g^{\sum_{i=1}^n m_i q 1} = (g^{q_1})^{\sum_{i=1}^n m_i}$. Let $g_0 = g^{q_1}$, then $V^{q_1} = g_0^{\sum_{i=1}^n m_i}$.
- Calculating $\log_{g_0}^{V^{q_1}}$ and getting final aggregation result $\sum_{i=1}^n m_i$.

4. **Correctness proof of proposed scheme.**

1. Correctness of signature verification.

$$\prod_{i=1}^n e(H(C_i || ID_i)^{\delta_i}, y_i) = \prod_{i=1}^n e(H(C_i || ID_i)^{\delta_i}, g^{x_i}) \tag{2}$$

$$= \prod_{i=1}^n e(H(C_i || ID_i)^{x_i \delta_i}, g) \tag{3}$$

$$= \prod_{i=1}^n e(\sigma_i^{\delta_i}, g) \tag{4}$$

$$= e(\prod_{i=1}^n \sigma_i^{\delta_i}, g). \tag{5}$$

2. Decryption correctness of aggregation result.

Due to $V = g^{\pi_0} \prod_{i=1}^n C_i$, $C_i = g^{\pi_i m_i} h^{r_i}$, so $V = g^{\pi_0} \prod_{i=1}^n g^{\pi_i m_i} h^{r_i}$.

$$V^{q_1} = g^{\pi_0 q_1} [\prod_{i=1}^n g^{\pi_i m_i} h^{r_i}]^{q_1} \tag{6}$$

$$= g^{\pi_0 q_1} \prod_{i=1}^n g^{\pi_i m_i q_1} h^{r_i q_1} \tag{7}$$

$$= g^{\sum_{i=1}^n \pi_i q_1} g^{\sum_{i=1}^n m_i q_1} \prod_{i=1}^n h^{r_i q_1}. \tag{8}$$

Because of the function of confidentiality interference factor, $\sum_{i=0}^n \pi_i (mod N) = 0$, so

$$V^{q_1} = g^{\sum_{i=1}^n m_i q_1} h^{\sum_{i=1}^n \pi_i r_i q_1}. \tag{9}$$

But in this scheme $h = u^{q_2}$, so

$$V^{q_1} = g^{\sum_{i=1}^n m_i q_1} u^{\sum_{i=1}^n \pi_i r_i q_1 q_2}. \tag{10}$$

u is the generator of G and $N = q_1 q_2$, so

$$u^{\sum_{i=1}^{n} \pi_i r_i q_1 q_2} = u^{N \sum_{i=1}^{n} \pi_i r_i} = 1_G. \tag{11}$$

We can get $V^{q_1} = g^{\sum_{i=1}^{n} m_i q_1}$.

Let $g_0 = g^{q_1}$, we have $V^{q_1} = g_0^{\sum_{i=1}^{n} m_i}$. And the final aggregation result is:

$$\log_{g_0} V^{q_1} = \log_{g_0} g_0^{\sum_{i=1}^{n} m_i} = \sum_{i=1}^{n} m_i. \tag{12}$$

5. **Security analysis for proposed scheme.** First, assuming that adversary obtains advantage $\varepsilon(\lambda)$, λ is the security parameter. The following is IND-CPA game.

- Initialization. Challenge generates ε, adversary obtains system public key $PK = N, g, h$.
- Challenge. Adversary outputs two plaintexts m_0 and m_1 with same length. Challenger randomly selects $b \in 0, 1$ and $r, \pi \leftarrow Z_N^{*R}$ and calculates the ciphertext $C = g^{\pi m_b} h^r \in G$. Then it sends the ciphertext to adversary.
- Guess. Adversary outputs b'. If $b' = b$, then the adversary wins this game.

In the above game, if the advantage of adversary $\varepsilon(\lambda)$ cannot be ignored, then $Pr[b' = b] = \frac{1}{2} + \varepsilon(\lambda)$. The result is apparent contradiction compared with reference[25]. Therefore, this new scheme is semantic security of IND-CPA.

Second, the follow is the attack analysis from inner network. In terms of the attacker from inner network, network data can be obtained in two stages: before and after aggregating. Before aggregating, inner attacker can get encryption private key q_1, but if he wants to get data m_1, he must own interference factor π_i. So the rate of successfully acquiring data m_i is $\frac{1}{2^{|\pi_i|}}$ ($|\pi_i|$ is the binary length of π_i). After aggregating, if adversary wants to get m_i from aggregation result $V = g^{\pi_0} \prod_{i=1}^{n} C_i$, he must solve Co-Diffie-Hellman problem. Obviously, it is very difficulty. So our scheme can effectively defend the attack from inner network.

In sum, the security analysis of proposed scheme includes two aspects: semantic security of IND-CPA and attack analysis from inner network. So the security analysis is proved.

6. **Comparison of performance with different schemes.** In table2, it shows the performance comparison with different schemes. In this paper, we make comparison to Smart-Frame scheme[26], privacy-preserving DA scheme[27] with our new scheme. Where the process of data verifying is realized by digital signature, because it can provide the function of preventing repudiation and modifying error. Computational ability of wireless sensor node is small, however, computational ability of aggregator is enough. So it does not need to take verification and decryption complexity into consideration.

Supposing that n is the sensor node number in aggregation process. In our scheme, it needs to compute the encryption time including three aspects: confidentiality interference factor encryption, data encryption and data signature. Where the average computation complexity of confidentiality interference factor encryption is $o(n)$, computation complexity of data encryption and data signature is $o(1)$.

7. **Conclusions.** In order to get a better wireless sensor network data aggregation scheme, we propose a provable private data aggregation scheme based on digital signatures and homomorphic encryption. ElGamal encryption scheme is used to encrypt privacy data and we add the digital signature into identity information of sensor node, which makes the data from different nodes have identifiability. So this scheme has the ability of verifying

Table 2. Performance comparison with different schemes

Scheme	Against external attacks	Against internal attacks	Trusted third party	Data verification	Formal proof	Encryption time complexity
[25]	YES	YES	NEED	YES	YES	$o(1)$
[26]	YES	No	NEED	YES	NO	$o(n)$
This paper's method	YES	YES	NOT NEED	YES	YES	$o(n)$

data and tracking, fixing mistakes. Confidentiality interference factor method is introduced into this scheme to defending interior attack. Then a confidentiality sum algorithm with homomorphic encryption property is adopted to build confidentiality interference factor method without trusted third party. That can avoid the safety and efficiency problem resulting from trusted third party. Finally, security proof and efficiency analysis is given in this paper. And comparison is given to demonstrate the performance of new scheme. In the future, we will study more advanced homomorphic encryption methods to improve aggregation scheme in wireless sensor network.

Acknowledgment. This research is funded by the Natural Science Foundation of China No.61602080, the Ministry of Education Humanities and Social Sciences Foundation (14YJA870014);and the Natural Science Foundation of Gansu Province of China (1508RJZA076). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] Z. You, S. Chen, Y. Wang, An efficient traffic data aggregation scheme for WSN based intelligent transportation systems, *Journal of Information Hiding & Multimedia Signal Processing*, vol. 6, no. 6, pp. 1117-1129, 2015.

[2] W. F. Wang, S. J. Shih , C. Y. Yang, Study on a Computational Model of Food Intake for a Body Weight Management System, *Journal of Information Hiding & Multimedia Signal Processing*, 2015, 6, no. 3, pp. 511-522.

[3] F. C. Chang and H. C. Huang, A Survey on Intelligent Sensor Network and Its Applications, *Journal of Network Intelligence*, vol. 1, No. 1, pp. 1-15, 2016

[4] S. Lohs, R. Karnapke, J. Nolte, Link Stability in a Wireless Sensor Network C An Experimental Study *Sensor Systems and Software. Springer Berlin Heidelberg*, pp. 146-161, 2012.

[5] M. Macedo, Are there so many sons per node in a wireless sensor network data aggregation tree?, *IEEE Communications Letters* vol. 13, no. 4, pp. 245-247, 2009.

[6] B. Stelte, A. Matheus, Secure trust reputation with multi-criteria decision making for wireless sensor networks data aggregation, pp. 20-923, 2011.

[7] R. Kannan, S. S. Iyengar, Game-theoretic models for reliable path-length and energy-constrained routing with data aggregation in wireless sensor networks, *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 6, pp. 1141-1150, 2006.

[8] Y. Yang, X. Wang, S. Zhu S, et al. SDAP: a secure hop-by-Hop data aggregation protocol for sensor networks, *Acm Transactions on Information & System Security*, vol 11, no. 4, pp. 356–367, 2008.

[9] A. Saranya*1, High-Speed Pool of Aggregated Data in Multi-hop Wireless Network, *International Journal of Engineering Sciences & Research Technology*, vol. 3, no. 5, 2014

[10] J. Domingo-Ferrer, A Provably Secure Additive and Multiplicative Privacy Homomorphism, *[C]// Information Security, International Conference, ISC 2002 Sao Paulo, Brazil*, September 30 - October 2, 2002, Proceedings. pp. 471-483, 2002.

[11] D. Westhoff, J. Girao, M. AcharyaConcealed, Data Aggregation for Reverse Multicast Traffic in Sensor Networks: Encryption, Key Distribution, and Routing Adaptation, *IEEE Transactions on Mobile Computing*, vol. 5, no. 10, pp. 1417-1431, 2006.

[12] T. D. Engouang, L. Yun, Z. J. Zhang, Pallier Based Homomorphic Encrypted Data Aggregation in Wireless Sensor Networks, *Applied Mechanics & Materials*, no. 5, pp. 3017-3022, 2014.

[13] X. Li ,D. Chen , C. Li , et al., Secure Data Aggregation with Fully Homomorphic Encryption in Large-Scale Wireless Sensor Networks, *Journal of Sensors*, vol. 15, no. 7, pp. 15952-15973, 2015.

[14] C. I. Fan , S. Y. Huang ,Y. L. Lai, Privacy-Enhanced Data Aggregation Scheme Against Internal Attackers in Smart Grid, *IEEE Transactions on Industrial Informatics*, vol. 10, no. 1, pp. 666-675, 2014.

[15] S. B. Othman , A. A. Bahattab , Trad A, et al., Confidentiality and Integrity for Data Aggregation in WSN Using Homomorphic Encryption, *Wireless Personal Communications*, vol. 80, no. 2, pp. 867-889, 2014.

[16] Y. Liu , C. X. Liu , Q A. Zeng, Improved trust management based on the strength of ties for secure data aggregation in wireless sensor networks, *Telecommunication Systems*, vol. 31, pp. 1-7, 2015.

[17] F. Li, P. Li, F. Gao, et al., Privacy Protection for Wireless Sensor Networks Based on Scalable Data Aggregation, *Sensor Letters*, vol. 12, no. 6, pp. 307-312, 2014.

[18] Y. Lemieux , L. Marchand, Method and system for multi-protocol label switching , no. MPLS) based data flow aggregation in a third generation (3G) cellular telecommunication system: US, US7292575[P]. 2007.

[19] H. Bao, R. Lu, A lightweight data aggregation scheme achieving privacy preservation and data integrity with differential privacy and fault tolerance, *Peer-to-Peer Networking and Applications*, pp.1-16, 2015.

[20] B. Dan, C. Gentry, B. Lynn, et al., Aggregate and Verifiably Encrypted Signatures from Bilinear Maps, *Lecture Notes in Computer Science*, vol. 2656, no. 1, pp. 416-432, 2003.

[21] Q. Tang, H. Ma, X. Chen, Extend the Concept of Public Key Encryption with Delegated Search, *Computer Journal*, 2013, 58, no. 4, pp. 724-734.

[22] C. Castelluccia, F. Mykletun, G. Tsudik, Efficient aggregation of encrypted data in wireless sensor networks*[C]//The second annual international conference on mobile and ubiquitous systems: networking and services. IEEE*, pp. 109-117, 2005.

[23] T. Gagliardoni, A. Hlsing, C. Schaffner, Semantic security and indistinguishability in the quantum world, *arXiv preprint arXiv*:1504.05255, 2015.

[24] S. Madden, M. J. Franklin, J. M. Hellerstein, et al., TAG: a Tiny AGgregation service for ad-hoc sensor networks, *Acm Sigops Operating Systems Review*, vol. 36, no. SI, pp. 131-146, 2002.

[25] E. J. G. D. Boneh, K. Nissim, Evaluating 2-DNF Formulas on Ciphertexts *.[C]//Proceedings of Theory of Cryptography, Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA*, February 10-12, pp. 325-341, 2005.

[26] Baek J, Vu Q H, J. K. Liu, et al. A secure cloud computing based framework for big data information management of smart grid, *IEEE transactions on cloud computing*, vol. 3, no. 2, pp. 233-244, 2015.

[27] D. He, N. Kumar, J. H. Lee, Privacy-preserving data aggregation scheme against internal attackers in smart grids, *Wireless Networks*, vol. 22, no. 2, pp. 491-502, 2016.