Privacy-Preserving Power Consumption Data Measuring Protocol for Smart Grid

C.R. Xie, R.Y. Zhang
State Grid Power Corporation of Shenzhou
Zhejiang Province, P. R. China

***Abstract*—In modern smart grid, smart meter which has replaced human operators to do the power measuring work becomes very popular. However, the application of smart meter will leak power consumption data to untrusted attacker. The exposure of these data will be dangerous to users' privacy. Only privacy related problems be solved, will the power users trust smart meters. In this paper, we investigate a previous work, and find it having many disadvantages. Then we propose a corresponding measuring protocol. The comparison results between our proposed protocol and the investigated protocol show our proposed protocol works better in many aspects. The application of our proposed protocol in smart grid will surely promote the application of smart meter into smart grid and simplify the engineering project management in smart grid.**

Keywords- energy-metering; smart grid; power engineering project management

I. INTRODUCTION

The Advanced Metering Infrastructure (AMI) is a useful application in Smart Grid and it has brought many benefits [1]. The smart meter in AMI can automatically read the power consumption data and report the data to the power supplier without the participant of human operators. The replacement of human operators not only reduces the manual workload, but also increases the accuracy of sensed data. These advantages make AMI popular among power companies, both in China [2] and other foreign countries. However, the privacy issues which are in AMI are very severe. For example, in the Netherlands, because of the criticism on privacy issues from the public, the deployment plan of smart meter has been postponed [3]. According to a scholar report for AMI, privacy has become the most serious concerns on AMI, compared with other attacks, such as integrity, availability and so on [4]. Only when privacy issues are solved, will the public be welcome to the application of AMI. And only when the privacy issues are solved, can the smart grid be truly smart.

In this paper, we pay attention to a previous related work on privacy-preserving power data measuring, and find it having many disadvantages, such as more communication round and high communication overhead. Then, we propose our new protocol. The contributions can be described as follows:

1. We consider the privacy issues in AMI and propose a privacy-preserving protocol for power consumption data measuring which works better than a previous approach in many aspects.

2. Our proposed protocol requires only one communication round between the supplier and smart meters, and decreases the communication overhead which leads to better communication efficiency and less latency.

3. Our proposed protocol requires less modular exponentiation operations, compared with the previous approach and stores less secret materials, which leads to better computation and storage efficiency.

II. RELATED WORK

According to a survey on power measuring in AMI applications [5], privacy-preserving power metering approaches consist of three categories: 1) anonymization; 2) hybrid approach; and 3) non-anonymization.

The first category provides anonymization by perturbing power user's ID and power consumption data. In this type of approaches, a trusted third party [6] or additional trusted device [7] is required.

The second category is a hybrid category. The power user's ID is not anonymous while the report data are modified by an internal power supply or are masked by a specific value. The internal power supply based approaches require a rechargeable battery and some algorithms [8][9]. Therefore, the supply can obtain the total power consumption data of one meter but cannot obtain the real time-series power consumption data. The power data masking method is to add a masking value to the real power consumption data, such as secret sharing [3] and Laplacian perturbation [11].

The last category is non-anonymization approach which is based on modern cryptography. To deal with a trusted supplier, traditional encryption/decryption based approach had been proposed [12]. To deal with an untrusted supplier, aggregation based approaches had been proposed. Concatenation operation based approach was proposed in [13] which however, is not suitable for lossy network. The approach in [14] required a tree structure while the approach in [15] was not efficient in communication overhead and storage overhead.

III. PRELIMINARIES

In this section, we present the compared protocol [15] and detail the advance modular property.

A. The Compared Protocol

The compared protocol [15] involves two devices, SS which is the supplier and M which is a smart meter. The SS supplies power to Ms, and computes a total supplies data mss. The compared protocol, defined as CP, includes four steps:

Step1: Mi->SS: in each time period, each Mi picks n random numbers, the sum of which, is its reading mi. Mi uses its public key to encrypt n-1 random number except the i-th random number.

Step2: SS->Mi: SS receives n(n-1) cipher texts, and it multiplies n-1 j-th ciphertexts from each Mi. Then SS sends

j-th multiplied ciphertext to Mj.

Step3: Mi->SS: Mi uses decryption key to decrypt i-th multiplied ciphertext and adds the i-th random number to the decryped result. It sends the result to SS.

Step4: SS computes the total supplies data mss from n addition results.

B. The Modular Property

In this paper, we apply a modular property [10] into our proposed protocol.

$$(1+p)^m=\sum_{i=0}^{m}\binom{m}{i}p^i=1+mp \bmod p^2 \tag{1}$$

The above modular property can be modified into an advanced version:

$$(1+xp)^m=\sum_{i=0}^{m}\binom{m}{i}(xp)^i=1+xmp \bmod p^2 \tag{2}$$

$$\prod_{i=1}^{n}(1+x_ip)=1+\sum_{i=1}^{n}x_i\cdot p+a_0p^2+\cdots+a_{n-3}p^n \bmod p^2=1+\sum_{i=1}^{n}x_i\cdot p \bmod p^2 \tag{3}$$

IV. Privacy-Preserving Energy Metering Protocol

At the initial phase, the Certification Authority (CA) will randomly generate n secret values for each meter Mi and uses them to generate the secret value s0, for the SS.

$$s_0=-\sum_{i=1}^{n}s_i \tag{4}$$

In each time period, each Mi has its power reading, defined as mi. In addition, each Mi will generate the encryption key ki and use ki to encrypt its reading.

$$c_i=(1+pm_i)H(t)^{s_i} \bmod p^2 \tag{5}$$

Then each Mi sends the ciphertext to the SS.

In this time period, after receiving n ciphertexts, the aggregator uses s0 to generate the decryption key to decrypt the total power data from n ciphertexts.

$$V_t=H(t)^{s_0}\cdot\prod_{i=0}^{n}c_i \bmod p^2=H(t)^{s_0+\sum_{i=0}^{n}s_i}\cdot\prod_{i=0}^{n}(1+pm_i) \bmod p^2 \tag{6}$$

We apply eqn (3) and eqn (4) into eqn (6), and obtain the following equation:

$$V_t=\left(1+\sum_{i=1}^{n}m_i\cdot p\right) \bmod p^2 \tag{7}$$

According to eqn (7), we can compute the total power consumption data:

$$Sum=\sum_{i=1}^{n}m_i=\frac{1-V_t}{p} \bmod p \tag{8}$$

Hence, the aggregator can obtain the total power consumption data.

V. Performance Analysis

In this section, we mainly focus on the communication overheads. In addition, storage overhead comparison is also conduct.

A. The Rough Comparison between CP and Our Protocol

In this subsection, we compare our proposed protocol with CP. The rough comparison can be seen from Table 1. The mark √ shows which protocol works better. Table II shows our protocol works better in all the listed four items.

TABLE I .THE COMPARISON BETWEEN THE TWO PROTOCOLS.

	Communication Round	**Computation Overhead**	**Storage Overhead**	**Communication Overhead**
Our proposed protocol	√	√	√	√
CP				

In our proposed protocol, only one communication round between the aggregator and mobile users is required while that in CP three communication rounds between the SS and all the meters are required.

The computation overhead in our proposed protocol is better than that in CP for two reasons. The first is that the encryption in Paillier' Cryptosystem requires more modular exponentiation operations. And the second is that in our proposed protocol, less encryption operations is required.

The storage overhead in our proposed protocol is better than that in CP because in our proposed protocol, each Mi only needs to store one secret value while in CP, each Mi needs to store the public keys of other devices in the system.

The communication overhead in our protocol is better because with three communication rounds the message number which each Mi needs to receive/send is n+1 while in our proposed protocol, the message number which each Mi needs to send (no receiving) is 1. And, each message in two protocols is |p2|. Therefore, our protocol is better in communication overhead.

The above comparison is rough and we will compare the two protocols in detail from two aspects: communication overhead and storage overhead.

B. Communication Overhead

Table 2 and Table 3 show the communication overheads of the aggregator and mobile users, respectively.

TABLE II .THE COMMUNICATION OVERHEAD OF THE SS.

In our proposed protocol	$n\|p^2\|$
In CP	$n(n+1)\|p^2\|$

In our proposed protocol, the SS will receive one message from one meter. Therefore, the total number of received messages is n. And, the bit length of each message is determined by the modulus, which is |p2|. Therefore, the total communication overhead of the SS in our protocol is n|p2|.

In 2nd step of CP, the SS receives n(n-1) messages from n meters and sends n messages to n meters. And, in 3rd step of CP, the SS receives n messages from n meters. The number of total received/sent message is n(n+1). The bit length of each message which is determined by Paillier' Cryptosystem is also |p2|. Therefore, the total communication overhead of the SS in CP is n(n+1)|p2|.

TABLE III .THE COMMUNICATION OVERHEAD OF THE METER.

In our proposed protocol	$\|p^2\|$
In CP	$(n+1)\|p^2\|$

In our proposed protocol, each meter sends one message to the SS. Therefore, the total number of received messages is 1. The bit length of each message is |p2|. And the communication overhead of each meter in our proposed protocol is |p2|.

In 2nd step of CP, each meter sends n-1 messages to the SS. In 3rd step, each meter receives one message from the SS. In 4th step, each meter sends one messages to the SS. Therefore, the total received/sent message of each meter is n+1. The bit length of each message is |p2|. Therefore, the total communication overhead of each meter in CP is (n+1)|p2|. Table III and Table IV show our work better in communication overhead for both the SS and all the meters.

C. *Storage Overhead*

From Table 4, we can see our protocol is efficient in storage.

TABLE IV .THE STORAGE OVERHEAD.

In our proposed protocol	*SS*	1
	Each meter	1
In CP	*SS*	0
	Each meter	*n*

In our protocol, each device, both the SS and each meter, only stores one secret value. While in CP, each meter stores its privacy key and other meters' public keys. Therefore, the total storage overhead of each meter in CP is n secret materials. In CP, the SS stores nothing because only multiplication operations are required by the SS. Therefore, our proposed protocol is more efficient in storage.

VI. CONCLUSION

Smart meter has replaced human operators to do the power measuring work which not only reduces the manual workload, but also increases the accuracy of real-time power consumption data. However, privacy issues should be solved before the deployment of smart meters. In this paper, we focus on privacy-preserving power measuring in smart grid. To overcome the problems in [15], we apply a modular property into our proposed protocol. Through performance analysis, our protocol's efficiencies on storage, computation and communication are revealed. Our protocol requires one communication round which decreases the latency. The comparison results between our protocol and the previous protocol show our protocol works better. The application of our proposed protocol in smart grid will surely promote the application of smart metering into smart grid and simplify the engineering project management in smart grid.

REFERENCES

[1] Karnouskos, S., Terzidis, O., & Karnouskos, P., An advanced metering infrastructure for future energy networks. In New Technologies, Mobility and Security, Springer: Netherlands, pp. 597-606, 2007.

[2] Xiao-min, B., Jun-xia, M., & Ning-hui, Z., Functional analysis of advanced metering infrastructure in smart grid. In Power System Technology (POWERCON), 2010 International Conference on, pp. 1-4, 2010.

[3] Kursawe, K., Danezis, G., & Kohlweiss, M., Privacy-friendly aggregation for the smart-grid. In Privacy Enhancing Technologies, Springer: Berlin Heidelberg, pp. 175-191, 2011.

[4] Cleveland, F. M., Cyber security issues for advanced metering infrasttructure. In Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, pp. 1-5, 2008.

[5] Saputro, N., & Akkaya, K., On preserving user privacy in Smart Grid advanced metering infrastructure applications. Security and Communication Networks, 7(1), pp. 206-220, 2014.

[6] Molina-Markham, A., Shenoy, P., Fu, K., Cecchet, E., & Irwin, D., Private memoirs of a smart meter. In Proceedings of the 2nd ACM workshop on embedded sensing systems for energy-efficiency in building, pp. 61-66, 2010.

[7] Bohli, J. M., Sorge, C., & Ugus, O., A privacy model for smart metering. In Communications Workshops (ICC), 2010 IEEE International Conference on, pp. 1-5, 2010.

[8] Kalogridis, G., Efthymiou, C., Denic, S. Z., Lewis, T. A., & Cepeda, R., Privacy for smart meters: Towards undetectable appliance load signatures. In Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, pp. 232-237, 2010.

[9] Varodayan, D., & Khisti, A., Smart meter privacy using a rechargeable battery: Minimizing the rate of information leakage. In Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on, pp. 1932-1935, 2011.

[10] Jung, T., & Li, X. Y., Collusion-Tolerable Privacy-Preserving Sum and Product Calculation without Secure Channel. IEEE Transactions on Dependable and Secure Computing, 12(1), pp. 45-57, 2014.

[11] Acs, G., & Castelluccia, C., I have a DREAM! (Differentially private smart metering). In Information Hiding, pp. 118-132, 2011.

[12] Erkin, Z., Troncoso-Pastoriza, J. R., Lagendijk, R. L., & Perez-Gonzalez, F., Privacy-preserving data aggregation in smart metering systems: An overview. IEEE Transactions on Signal Processing Magazine, 30(2), pp.75-86, 2013.

[13] Bartoli, A., Hernández-Serrano, J., Soriano, M., Dohler, M., Kountouris, A., & Barthel, D., Secure lossless aggregation for smart grid M2M networks. In Smart Grid Communications), 2010 First IEEE International Conference on, pp. 333-338, 2010.

[14] Li, F., Luo, B., & Liu, P., Secure information aggregation for smart grids using homomorphic encryption. In Smart Grid Communications, 2010 First IEEE International Conference on, pp. 327-332, 2010.

[15] Garcia, F. D., & Jacobs, B, Privacy-friendly energy-metering via homomorphic encryption. In Security and Trust Management, Springer: Berlin Heidelbergm, pp. 226-238, 2011.