Trade-off between Service Granularity and User Privacy in Smart Meter Operation

Junggab Son*, Donghyun Kim*, Sejin Lee‡, Heekuck Oh†§, Alade Tokuta*, and Hayk Melikyan*,
* Department of Mathematics and Physics, North Carolina Central University, Durham, NC 27707, USA
E-mail: {json, donghyun.kim, atokuta, gmelikyan}@nccu.edu
† Department of Computer Science and Engineering, Hanyang University, ERICA Campus, South Korea
E-mail: hkoh@hanyang.ac.kr
‡ Department of Mechanical and Automotive Engineering, Kongju National University, South Korea
E-mail: sejiny3@kongju.ac.kr
§ Corresponding Author.

***Abstract*—The term "smart grid" refers to the next generation power supply system. A smart meter, an essential component of the grid system, is installed at each housing unit and acts as an agent for the unit. While the smart meter is a key enabler of great opportunities and conveniences in smart grid, it is susceptible to various cyber-security attacks, especially privacy invasion from electricity providers. Trusted third party (TTP) and homomorphic encryption are two favorite tools to deal with this issue in the literature. Unfortunately, the use of TTP does not completely eliminate the privacy risk. On the other hand, the use of homomorphic encryption makes it harder for the providers to support various services whose demand can be highly diversified. In this paper, we introduce a drastically new approach to deal with the consumer privacy issue in smart grid. Our key idea is let each consumer to determine the frequency of the measurement report. In this way, each consumer can responsibly make a trade-off between the level of privacy preservation with the quality of the services it will receive.**

***Index Terms*—Smart grid, smart meter, user privacy, service granularity.**

I. Introduction

A smart grid refers an automated modernized version of the old electrical power supply network. The grid collects real-time information about its status as well as the behavior of power suppliers and consumers connected to the grid and uses the information to improve the overall reliability, efficiency, sustainability, and the economics of the distribution and production of electricity [1]. One salient feature of the smart grid compared to the conventional power supply network is the existence of a two-way real-time communication network connecting the *electricity providers (EPs)* and the consumers. Using this network, the smart grid is able to improve the existing power supply system as well as provide a rich set of new services, which were previously not available [2], [3]. Many experts believe that the benefit of the smart grid will be magnified in the future as we will more rely on irregular and unpredictable power supplies, especially renewable energy sources such as sunlight and wind.

It is also expected that the advent of the smart grid will benefit each individual. The system can provide a real-time quote of electricity unit price and such information will help the consumer to adjust their power consumption pattern more cost effectively. It is known that the unit price of electricity generated by a renewable energy source during night time is much cheaper than the counterpart generated by fossil fuel during peak day time. Therefore, a customer can save lots of money by setting a dishwasher at home up so that it will be operated during late night. On the other hand, an EP can monitor the electricity usage of each consumer and notify the consumer if any abnormal usage pattern of electricity is detected.

One key enabler of the smart grid is the *smart meter (SM)* installed at each housing unit to manage the power usage as well as meter the usage and report it to the electricity provider automatically [4]. Unfortunately, many existing studies show the smart meter can be a security breach susceptible to be attacked or misused, which raises a great security and privacy concern over the whole smart grid. As a result, many efforts are made to improve the security and reliability of the smart meter and related communication protocols. In the earlier days, most researches focused on protecting SM from various physical attacks, especially, SM manipulation launched by a customer to reduce the bill and by an eavesdropper who wants to invade the privacy of the customer. Applying a *tamper proof memory (TPM)* is used to be one promising way to defend SM against such attacks.

Unfortunately, it is recently found that even with TPM at each SM, the privacy of a customer cannot be protected from the EPs who can observe the real-time electricity usage of the customer, which is useful to commit various crimes. Due to the reason, a *data aggregator (DA)* based approach is introduced in the literature. In this approach, the SM of each household regularly generates two different types of messages. In detail, the SM generates a message with a metering data encrypted by the symmetric key of the SM (shared with the EP) and sends it to the EP for billing purpose less frequently (e.g. one time per month). Since the frequency of the meter information is very low, the provider cannot invade the privacy of the customer seriously. At the same time, the SM creates a message with a real-time metering data encrypted by a secret key shared with DA and sends it to DA with much higher frequency. Then, DA combines the messages from the area and sends one single merged metering message to the EP. As a result, the EP cannot obtain the information about each individual customer, but can obtain the real-time electricity usage of the group which can be still useful to improve the efficiency of the power supply system.

However, some recent report pointed out the possibility of information leakage from at DA and proposed to use a TPM for the DA [5]. While this can protect the attack from outside, this approach cannot prevent privacy intrusion by the EP since the DA is merely a hardware under the control of the EP. For instance, the EP can obtain the real-time meterage (meter reading) from the DA when the DA is merging the metering information from each household. Also, the cost of a TPM is very high, which makes this approach minimally attractive. To solve this issue, several approaches utilizing a homomorphic encryption have been proposed [6]. In this strategy, each SM only sends a message including a real-time metering information encrypted by a homomorphic encryption key to the DA, the DA aggregates the messages from the SMs, and forwards the resulting message to the EP throughout a secure channel between them. While this approach can protect the privacy of each user efficiently, it becomes very difficult for the EP to provide an adequate service to meet the unique need of each customer which is a unique feature of smart grid since the EP cannot access the real-time electricity of each customer.

Alternatively, in [18], the authors proposed a solution which uses a *trust third party (TTP)* as a DA. In this approach, each SM sends the real-time metering information encrypted by the symmetric key shared by each SM and the TTP. Then, the TTP decrypts the message from the SMs, aggregates them, and sends the merged meter information to the EP. At the end of a session, the TTP also sums up the meterage of each individual customer and sends it to the EP along with the pseudonym of the customer for billing. The EP can link the pseudonym with the actual identification of the user, and thus send the bill to the correct customer.

Motivation and Contribution. In this paper, we propose a new secure smart metering framework. Its design is based on our observation that the existing systems assuming each SM with TPM along with the homomorphic encryption scheme in which the DA merges encrypted messages from each household cannot be completely secure. This is because the SM and the DA can be under the control of the EP. Furthermore, the aggregation strategy will diminish one main merit of the smart grid, providing various user-specific services. When it compared with the existing systems, the proposed framework has the following desirable properties.

(a) **Less overhead**: there is no need of a secure DA equipped with TPM for aggregation. At the same time, there is no need for a TTP to be involved in the transmission of each message from each SM to an EP, since this is somehow excessive and unrealistic.

(b) **Less assumption**: In some existing systems, a SM with a TPM has been assumed for security. However, in practice, it is still possible for the part of SM which is under the control of EP not to follow the protocol. For instance, EP can launch various attacks against the customer such as sending meterage more frequently or sending unencrypted data. The proposed work assumes the part of SM under the control of EP is not secure, but is still able to preserve the privacy of the user.

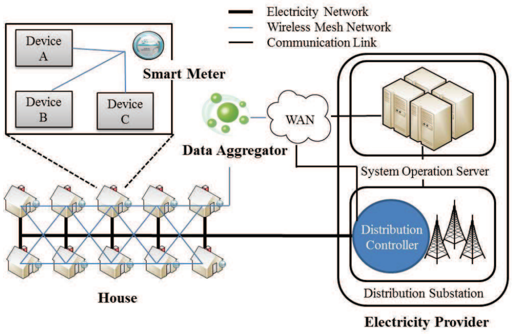

Fig. 1: System model.

(c) **User specific service granularity**: the metering the usage of electricity for each household by an EP is possible only after a certain customer specific number of encrypted meterage message is received by the EP. In this way, each customer adjusts the level of service granularity by sacrificing the level of privacy.

(d) **Conditional privacy revocation**: Our system provides a conditional privacy to the customer and any billing dispute can be resolved by the assist of TTP.

The rest of this paper is organized as follows. Section II defines some terms and presents related work. Some preliminaries are given in Section III. Our main contribution, a new security framework for SM with user adjustable service granularity is presented in Section IV. The security and efficiency analysis of the proposed scheme is in Section V. Finally, we conclude this paper in Section VI.

II. Background and Related Work

Fig. 1 shows the smart grid system and its main components including SM, DA and EP.

- **Smart meter** (SM): SM is a metering device attached at each housing unit, and enables the two-way communication between each consumer and the EP. It also make real-time energy metering possible. A customer consumes electricity at home by using various appliances. SM meters the power being used in a real-time manner and provide it to the customer and the EP. Using this data, the customer can actively manage its power consumption. Meanwhile, the EP can charge the cost for the electricity usage as well as provide various services to the customer.
- **Data aggregator** (DA): In many existing work, DAs are introduced and located between SM and the EP. A DA collects meterage messages from the SMs and forward them to the EP. To protects user privacy, DA

usually aggregates metering data from multiple SMs and forwards the merged data to the EP.

- **Electricity provider** (EP): EP consists of distribution substation, electricity distribution network, data network, and a system operation server. It meters electric charge in real-time and determines power supply quantity by analyzing data transmitted through DA. The EP should know the sum of the current electricity consumption of all customers and the sum of electricity consumption values of an individual customer over a given time interval.

A metering data consists of two types, high-frequency and low-frequency metering data [7]. Low-frequency metering data is the quantity of consumed data that is transmitted to the service provider by SM in long time interval. This data is for account management or billing purposes. High-frequency metering data is read by a SM and is transmitted to the service provider often enough. The service provider uses it to determine amount of electricity providing or to analyze a usage patterns depending on time, user, region and so on. Studies on smart grid security mostly focused on SM, which is the core element of smart grid.

The security issues of SM can be classified into three kinds; which are internal attack [8], external attack [9] and privacy protection [10]. Data falsifying by user and data manipulation by EP are internal attacks. In smart grid environment, power consumption data is stored in SM and the information is provided to user through network. If a user attempts to pay electric charge less than it has consumed, user can falsify the data stored in SM by hacking it. Meanwhile, EP levies electric charge based on data transmitted from SM. EP can also manipulate data by transmitting incorrect price information so that user would pay more.

Since SM is installed outside houses in general, it is exposed to potential attacker [9]. An attacker can attack SM in various ways. The most powerful but simple attack is accessing the stored data in SM by physical access. For instance, an attacker can attack the firmware of SM and set up it in a form, which can be controlled by the attacker. An attacker can also obtain meaningful data by detecting and analyzing the electric signal of the memory chip. It is also possible to generate data falsified by internally stored key by having SM infected with malicious code. Because SM location is not safe while it is the key element of the system, studies to make physically safe SM are ongoing. A representative scheme proposed by such studies is installing TPM and handling important data and arithmetic calculation within it.

The living pattern of a household can be learned by analyzing data collected by a SM [11], [12]. It is possible to speculate appliances used in home by knowing power consumptions of home appliances. An SM has lot of information including SM ID, information of home appliance connected to SM and electric charge levying information. If such information would be exposed, it can lead to infringement of user privacy. Since such sensitive data are being handled in SM, the top priority task in SM is the issue of data privacy.

As mentioned before, the leakage of internal information in smart system can be prevented by installing TPM [5], [13], [14]. The privacy infringement by power consumption analysis can be protected by having the data transmitted to EP through DA. SMs send their meterage to the DA depending on given time interval, and then DA aggregates these messages and sends it to EP. Since a meterage that is sent to EP is not individual usage but aggregated usage of group of SMs. Although this method can preserve consumer's privacy from EP, cannot preserve consumer's privacy from DA. The remaining problem is that encrypted data is transmitted to DA to protect transmission section. DA is not a reliable entity, it only combines data. If encrypted data would be transmitted to DA, DA could not aggregate data; therefore, certain measure enabling data aggregation is required. Some previous works use TTP as DA to solve privacy problem of DAs [18]. TTP has the role of aggregating meterages that is encrypted with shared secret key between SMs and TTP. SMs send their meterage to the TTP after encrypting with shared secret key. Then TTP decrypts those messages and send aggregated meterage to the EP. Another role of TTP is to calculate individual meterage for each SM. At the end of session, the TTP sums up a stored meterage for each SM, and sends it to EP for billing process. In point of privacy, it is better method than using just DAs, but is worse in terms of TTP has to manage all of metering data that is sent to EP. It is unrealistic because TTP cannot deploy as much as the number of DA and there is so much metering data that TTP has to aggregate.

Schemes applying a homomorphic encryption have been proposed to resolve this issue [15]–[17]. If homomorphic encryption is used, the calculation result of two ciphertexts is same as the calculation result of two plaintexts. For instance, when there are two data m_1 and m_2 and corresponding ciphertexts $E(m_1)$ and $E(m_2)$, if $m_3 = m_1 + m_2$, then $E(m_3) = E(m_1) + E(m_2)$. SMs send encrypted meterage to protect from various attacks in transmission section. Since homomorphic encryption can aggregate encrypted data without decrypting it, metering operation can protect data leakage in aggregation process of DA. The transmission and aggregation process can be protected in this way.

III. Preliminaries

A. Problem Statement

The real-time electricity usage of each customer collected by SM should not be used against the customer's good and only for the public benefit such as efficient system operation and effective power distribution. Clearly, the usage information should be safely handled because they include information which can infringe user privacy. The existing TPM scheme and homomorphic encryption scheme introduced in Section II can resolve most SM-related security issues. However, still there is an issue that the party who manages SM and metering data is EP. An EP can infringe privacy by manipulating the transmission cycle of low-frequency metering data. Low-frequency metering data is used for electric charge payment and that include power consumption of certain period. This data would not be aggregated with other metering data and that would be encrypted by user personal key before transmission to EP. Consequently, if the low-frequency metering data cycle decreases, it is possible to guess the appliances being used in real-time by analyzing the data. It is also important not to involve TTP too much frequently into the protocol, e.g. involving them in every message transmission, since it is not practical. Finally, existing strategy implicitly assumes the service granularity of all users are same, which is not necessarily true. An EP can provide a higher quality service if they has real-time information like electricity usage of a customer, which is against the privacy of the customer. Therefore, it is reasonable for each customer to determine the level of trade-off between the level of privacy and the degree of service granularity.

B. System model

Unlike as system model shown in Fig. 1, our system model consist of three different entities; TTP, EP, and SMs.

- *Trust third party (TTP)*: When a session begins, the TTP generates a session secret for each user. The TTP sends this secret value to users with its signature. In addition, the TTP stores session secret to revoke user in case of abnormality.
- *Electricity provider (EP)*: This entity has the same role as system model shown in Fig. 1.
- *Smart Meter (SM)*: We assume that a SM consist of two components. First is $SM-TPM$, which managed by user. $SM-TPM$ has role of measuring usage and sends encrypted meterage to EP at every time interval that setted by user. $SM-TPM$ applied TPM to protect inappropriate access of EP. Second is $SM-Controller$, which managed by EP. It has role of verify a meterage that measured by $SM-TPM$ and sends verified meterage to EP.

In addition, the system model in this paper uses only high-frequency metering data; while existing system model uses both high-frequency metering data and low-frequency metering data for data metering. Since the metering data does not need to aggregate, there is no DA in our system model. Instead, user can control a time interval that sending frequency of meterage. Additionally, we assume that all of the external communication from SM is protected by secure channel.

C. Design Goal

The proposed scheme is designed under the consideration of following properties.

- Privacy Preservation: The EP cannot infer user's active devices through analyzing metering data.
- Service granularity: A user can control the level of service granularity and user privacy.
- Conditional anonymity: SM operation must provide conditional anonymity to protect privacy of users while enabling authorities to identify misbehaving SMs. A conditional anonymity in SM operation is similar, but it has a crucial difference with conditional anonymity in other environment. In case if illegal action occurs, SM operation scheme can not only trace who made abnormality but also can restore metering data. It makes EP to charge for usage even if user made abnormality to avoid billing payment.

TABLE I: Notations

Notation	Description
U_i	User(SM)
ID_i	ID of U_i
pk_i, sk_i	Public/private key pair of U_i
t	Timestamp
c_{i-j}	meterage (meter reading) of U_i in certain time period j
$E_k\{m\}$	Encrypt m using key k

IV. The New SM Operation Framework Supporting User-defined Service Granularity Control

In this section, we introduce our new framework to operate SM which allows each user to make the trade-off between the level of user privacy and the degree of service granularity. Table I shows the notations used in this paper.

A. Setup

First of all, TTP, EP and client generate a public/private key pairs (pk_t, sk_t), (pk_e, sk_e), (pk_i, sk_i), repectively. TTP generates random large prime p_i and sends it to U_i with ID_i, t and also the signature of those values. p_i is used as period secret.

We define session as time interval of meterage which is set by EP, and period as time interval of meterage which is set by user. A period consists of one or more sessions. A user has to send encrypted meterage to the EP at the end of each session, and a user has to send meterage to the EP at the end of each period. EP can obtain users actual meterage after period, while stores encrypted meterage of every session. The encrypted meterage of session carries an important meaning in two ways. It can protect user privacy and enable controlling service granularity by user as well as it can prevent users misbehavior such as loss of money caused by user that does not send period secret. In this case, EP can solve this through receiving period secret of the user from TTP.

B. Metering Data Encryption and Verification

To make service granularity possible, we added SGF (Service Granularity Function) in $SM-TPM$. A User can control service granularity and user privacy through setting up the period of SGF in $SM-TPM$. Like with the recent state-of-art schemes, we use TPM for SMs. Therefore, SGF cannot be controlled by EP as well as other attacker.

Fig. 2 illustrates the proposed smart metering operation during a user configured period. At the start of period, $SM-TPM$ generates random large prime q_i and computes $N_i = p_i \cdot q_i$. This N_i is used for all sessions in a period. After a session ends, $SM-TPM$ sends encrypted meterage to the EP. Since meterage has to be hide for privacy reason and $SM-Controller$ is EP side devices, an effective solution

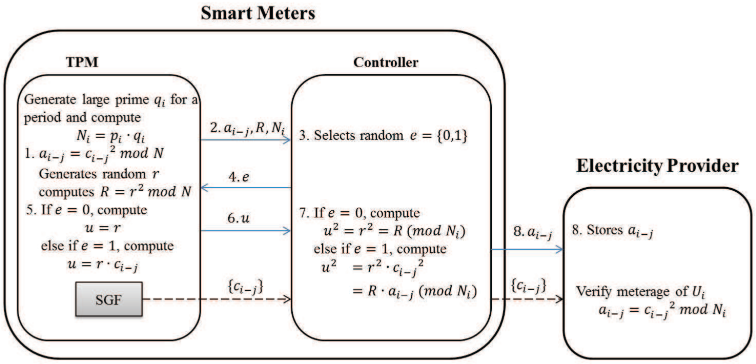

Fig. 2: Proposed Smart Metering Operation.

that satisfies both conditions is needed. Therefore, we use Zero-knoledge Proof [19] to verify meterage is valid without exposure.

$SM-TPM$ computes $a_{i-j} = c_{i-j}^2$ mod N_i. Where, j is session number in a period. Next, It generates random number r and computes $R = r^2$ mod N_i. Then, $SM-TPM$ sends a_{i-j}, R, N_i to the $SM-controller$. Here, If $SM-controller$ cannot trust N_i which is generated by U_i, $SM-controller$ can request TTP's signature on N_i. Here, If $SM-controller$ cannot trust N_i which is generated by U_i, $SM-controller$ can request verification of N_i. Then TTP sends verification result as follow: If $N_i mod p_i = 0$ return true, else false. Now, $SM-controller$ can trust N_i as revocable session secret.

After receiving the message, $SM-controller$ selects random number $e = 0, 1$ and sends it back to the $SM-TPM$. $SM-TPM$ computes u based on e. If $e = 0$, $SM-TPM$ computes $u = r$; else if $e = 1$, $SM-TPM$ computes $u = r \cdot c_{i-j}$; otherwise return false. $SM-TPM$ sends u to the $SM-controller$. $SM-controller$ verifies u, based on e. If $e = 0$, $SM-controller$ compares $u^2 = r^2$ with R; else if $e = 1$, $SM-controller$ compares $u^2 = r^2 \cdot c_{i-j}^2$ with $R \cdot a_{i-j}$; where R and a_{i-j} was received in previous process. If two values are same, it passes verification process. If not, user made an abnormality. $SM-controller$ repeats this verification process to reduce probability that a user pass the process without actual meterage. Then, $SM-TPM$ sends ID, timestamp, encrypted meterage and its signature to $SM-Controller$; $ID_i, t, E_{p_i}\{c_{i-j}\}, (ID_i, ||t||E_{p_i}\{c_{i-j}\})^{sk_i}$. $SM-Controller$ sends it with verified information; a_{i-j}, t_c, N_i. The EP can store this received information.

After user configured period expires, SGF in the SM sends period secret p_i to EP. Then EP can calculate the meterage of specific period using p_i from stored meterage information. EP decrypts c_{i-j} and computes $a_{i-j} = c_{i-j} mod N_i$. If a_{i-j} is same as stored a_{i-j}, user sent valid meterage; otherwise EP performs user revocation process.

C. *Conditional Anonymity*

In our scheme, user can hide meterage by ignoring a session secret transmission. In this case, EP can claim user's abnormality to the TTP. The TTP which is also a revocation authority gives notice to user about its abnormality. If user does not respond to TTP's notice, TTP can revoke the user and sends session secret p_i to EP to restore a session meterage. Using p_i EP can calculate meterage of certain period.

V. Analysis of Proposed Scheme

A. *Security Analysis*

In our scheme, we follow the previous works and assume that SMs are based on TPM. Generally SMs are installed outside houses and easily exposed to potential attackers. So SMs must be designed in such a way that it can be secure from various physical attacks. And we assume that symmetric key can be used to protect each transmission section. Additionally in our scheme, there is another security issue that U_i can use illegal session secret instead of received from TTP. We verify that our scheme is secure from this security issue through following proof.

Theorem 1. *EP can detect U_i's misbehavior that use illegal session secret instead of received from TTP.*

Proof: A period secret is made by TTP. When a user uses an illegal period secret, it cannot pass verification process between $SM-Controller$ and TTP. $SM-Controller$ sends $SM-TPM$'s period secret to TTP, invalid period secret is hard to pass $N_i mod p_i = 0$ and $N_i \neq p_i$. Therefore, it is hard that user uses illegal period secret instead of p_i. ■

B. *Anonymity Analysis*

In the proposed scheme, SM consists of $SM-TPM$ and $SM-controller$. $SM-TPM$ allows only user's access, while $SM-controller$ allows only EP's access. Temper resist memory is applied to $SM-TPM$ to protect its operation and storage. A user stores session secret which is sent from TTP, meterage, and time interval of session to the $SM-TTP$. EP cannot operate $SM-TPM$ and obtain any information that is stored in $SM-TPM$ through hacking. Our scheme can modulate a level of user privacy by controlling time interval. EP cannot receive a meterage without fixed time interval. Therefore, our scheme can provide the user desired level of privacy. In addition, we verify our scheme can revoke user in case of abnormality.

Theorem 2. *TTP can help EP to revoke abnormal user and restore meterage.*

Proof: First, EP has ID of each SMs in the system model. The U_i that did not send session secret for a long time can be target of revocation. Before revocation, TTP warns U_i that it can be revoked. After that, TTP sends stored $(ID_i, t, p_i)^{sk_t}$ to EP. After confirming signature of TTP, EP can restore meterage of U_i. Our protocol based on the difficulty of extracting modular square roots when the factorization of n_i is unknown. When TTP sends one of the factorization of n_i, EP can easily break the difficulty we used in protocol. Therefore, our scheme can revoke an abnormal user with restore it's meterage. ■

C. Computational Overhead

Homomorphic encryption scheme used in previous works that are based on public key cryptography [17]. Homomorphic encryption has advantage of protecting data during computation, but has disadvantage of computational overhead. While data aggregation process is not much burden for DA, the encryption process of high frequency metering data can be a burden for SM. SM has role of measuring all the usage inside a house and sending metering data to the EP. It can be advantage to reduce computational complexity of SM. In the proposed scheme, we use modular arithmetic that has less computational overhead than homomorphic encryption. SM needs one modular and zero knowledge proof to send meterage. Therefore our scheme is more realistic than previous schemes which are based on homomorphic encryption. Especially, our scheme has high efficiency when time interval of session is very short.

VI. Conclusion

In this paper, we introduce a new SM operation framework in smart grid. To preserve the privacy of each user, our drastically new framework does not have strong assumptions such as completely secure SM and the existence of secure DA. It also does not require the TTP involved in sever communication from each SM to EP. On the other hand, it allows each user to determine how to trade-off between the level of privacy and the degree of service granularity, which has not been considered before. As a result, the proposed framework is ideal for smart meter operation to meet diverse user needs.

Acknowledgment

This research was supported in part by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (NIPA-2014-H0301-14-1015) supervised by the NIPA(National IT Industry Promotion Agency). This research was supported in part by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (NIPA-2014-H0301-14-1044) supervised by the NIPA(National IT Industry Promotion Agency). This work was supported in part by the NRF (National Research Foundation of Korea) grant funded by the Korea government MEST (Ministry of Education, Science and Technology) (No. NRF-2012R1A1A2009152). This work was supported in part by the NRF (National Research Foundation of Korea) grant funded by the Korea government MEST (Ministry of Education, Science and Technology) (No. NRF-2012R1A2A2A01046986). This work was supported in part by US National Science Foundation (NSF) CREST No. HRD-0833184 and by US Army Research Office (ARO) No. W911NF-0810510.

References

[1] U.S. Department of Energy. "Smart Grid / Department of Energy". Retrieved 2012-06-18.

[2] National Institute of Standards and Technology (NIST), "NIST Framework and Roadmap for Smart Grid Interoperability Standards," Release 2.0, Feb. 2012.

[3] The National Energy Technology Laboratory (NETL), "Understanding the Benefits of Smart Grid," June 2010.

[4] A. H. Rosenfeld, D. A. Bulleit, and R. A. Peddie, "Smart meters and Spot Pricing: Experiments and Potential," *IEEE Technology and Society Magazine*, vol. 5, no. 1, pp. 23-28, Mar. 1986

[5] H. Simo Fhom, N. Kuntze, C. Rudolph, and M. Cupelli, "A User-Centric Privacy Manager for Future Energy Systems," *International Conference on Power System Technology*, pp. 1-7, 2010

[6] F. D. Garcia, and B. Jacobs, "Privacy-Friendly Energy-Metering via Homomorphic Encryption," *Proceedings of the 6th international conference on Security and Trust Management*, pp. 226-238, 2010.

[7] C. Efthymiou, and G. Kalogridis, "Smart Grid Privacy via Anonymization of Smart Metering Data," *The 1st IEEE International Conference on Smarg Grid Communications*, pp. 238-243, 2010

[8] R. C. Park, "Advanced metering Infrastructure Security Considerations," *Sandia report*, ref. SAND2007-7327, Dec. 2007

[9] J. McCullough, "AMI Security Considerations," *Elster*, ref. WP42-1007B, 2010.

[10] E. L. Quinn, "Privacy and the New Energy Infrastructure," *Social Science Research Network (SSRN)*, Feb. 2009

[11] F. Siddiqui, S. Zeadally, C. Alcaraz, S. Galvao, "Smart Grid Privacy: Issues and Solutions," *The 21st International Conference on Computer Communications and Networks (ICCCN)*, 2012

[12] P. McDaniel, S. McLaughlin, "Security and privacy Challenges in the Smart Grid," *IEEE Security& Privacy*, vol. 7, issue. 3, pp. 75-77, 2009

[13] N. Kuntze, C. Rudolph, M. Cupelli, J. Liu, and A. Monti, "Trust Infrastructures for Future Energy Networks," *IEEE Power and Energy Society General Meeting*, pp. 1-7, 2010

[14] A. J. Paverd, and A. P. Martin, "Hardware Security for Device Authentication in the Smart Grid," *The 1st International Workshop on Smart Grid Security (SmartGridSec)*, pp. 72-84, 2012

[15] F. Li, B. Luo, and P. Liu, "Secure Information Aggregation for Smart Grids Using Homomorphic Encryption," *The 1st IEEE International Conference on Smarg Grid Communications*, pp. 327-332, 2010

[16] D. Seo, H. Lee, and A. Perring, "Secure and Efficient Capability-based Power management in the Smart Grid," *IEEE International Symosium in Parallel and distributed Processing with applications Workshops*, pp. 119-126, 2011

[17] N. Saputro, K. Akkaya, "Performance evaluation of Smart Grid Data Aggregation via Homomorphic Encryption," *IEEE Wireless Communications and Networking Conference*, pp. 2945-2950, 2012.

[18] J. M. Bohli, C. Sorge, and O. Ugus, "A Privacy Model for Smart Metering," *IEEE International Conference on Communications Workshops (ICC)*, pp. 1-5, 2010.

[19] A. Fiat, Adi Shamir, "How to Prove Yourself: Practical Solutions to Identification and Signature Problems," *Advances in Cryptology-CRYPTO' 86*, pp. 186-194, 1987.