An Identity-Based Encryption Scheme with Performance Optimization for Privacy Preservation in Smart Grid Communication

Ulas Baran Baloglu
Department of Computer Enginnering
Munzur University
Tunceli, Turkey
email: ulasbaloglu@gmail.com

Yakup Demir
Department of Electrical and Electronics Engineering
Firat University
Elazig, Turkey
email: ydemir@firat.edu.tr

***Abstract*—Smart grids are expected to replace existing electrical grids with advanced mechanisms and intelligent entities, which have excessive data processing and communication tasks. It is important for the sensitive consumer data, such as meter readings, to be secured at these intelligent entities. Novel digital communication mechanisms should be developed to protect privacy. Existing smart grid architectures do not have sufficient and efficient security functionalities for data transmission. In this paper, we propose an Identity-Based Encryption scheme, which is more promising than the classical form regarding performance and security. The proposed scheme focuses on the data structure of meter readings and optimizes this structure to achieve a better privacy preservation. This novel structure further improves the performance of the scheme by reducing communication overhead caused by public key creation and distribution operations, as evaluations demonstrated.**

Keywords-identity-based encryption; smart grid; privacy preservation.

I. INTRODUCTION

In the following years, smart grids are expected to replace the classical grids. Advances in information science opened a new path to the grids for transmitting power in a more efficient way than before. The electricity grids are going to be equipped with adaptation mechanisms, control technologies, data processing systems and communication mechanisms to react to various grid problems. Problems, such as power quality, will still exist in smart grids as they did in the past, but the grid structure will be more robust and efficient. The biggest problems with the transition to smart grids will be information security based including computation, data communication, and storage. Therefore, privacy and data security will play a very crucial role in the success of future smart grids.

Smart grids add the complexity of a communication layer to an electric power system, which is already a complex physical network. The introduction of this layer may create new challenges, especially regarding security. Smart meter readings may reveal some private information about daily lives and routines of its consumers. As a result, smart meters have to fulfill four essential security requirements: data authenticity, data confidentiality, data integrity and consumer privacy [1][2]. These requirements can be achieved by sender authentication, communication security, and privacy preservation techniques. Every part of a smart grid infrastructure must incorporate at least some fundamental cryptographic features to perform tasks such as data encryption and authentication [2].

There are several studies in the literature aiming to protect consumer privacy while fitting with the smart grid concept. One way of doing this is encrypting metering data before transmitting it. For this purpose, various encryption schemes are applied in this field such as ElGamal encryption system, which outperforms existing schemes based on Paillier's homomorphic cryptosystem [3]-[6]. This encryption system is secure under chosen plaintext attacks (CPA), but it is not secure under chosen ciphertext attacks (CCA) [6]. Boneh-Goh-Nissim is another homomorphic encryption technique, which has one multiplication between an arbitrary number of additions [7]. These studies are typically directed towards developing a cryptography system so that they have not paid much attention to whether they are suitable for smart grids.

Other studies prefer to perturb meter readings, which is defined as a process for adding noise to hide the true meter readings or privacy of consumers while preserving the usability [8]. There are several types of perturbation, such as adding noise (additive perturbation), k-anonymity, compressing data, differential privacy, and geometric transformation [9]-[11]. Bayes Estimate and Principal Component Analysis can also be used for perturbation purposes [12]. The main problem of perturbation techniques is the removal of noise from data, which is a difficult and computationally expensive task. Furthermore, intruders can steal perturbed data and statistically analyze it to reveal a consumption profile.

Although there exist some studies about preserving privacy in smart metering systems by applying Identity-Based Encryption [13]-[16], there are some significant differences between those studies and the proposed scheme. Our study differs from the previous studies by focusing on the data structure of the meter readings. It helps us to increase the security while preserving privacy by separating identity information from the metering data. Another contribution of this study is the performance optimization. Unlike all other previous studies, encryption is not

 ISBN: 978-1-61208-544-9

performed by using the user identities separately; instead, timestamp values of the meter readings used. Using a common timestamp value avoids a lot of key circulation inside the system, and computations can be done collectively instead of computing every key individually because all meters have the same timestamp value when the readings are completed.

The rest of this paper is organized as follows. In Section II, we explain preliminaries that are used to construct the proposed scheme. Section III describes the entities of the scheme, and in Section IV, the efficiency is evaluated. We finally conclude the paper in Section V.

II. PRELIMINARIES

In this section, we briefly outline the cryptography primitives that serve as a basis to describe the proposed privacy-preserving scheme.

A. Bilinear Pairing

Bilinear pairing is defined by a quintuple <p, G_1, G_2, e, g> [13]. In this technique, G_1 and G_2 are two cyclic groups with the same prime order denoted as p. The generator of G_1 is denoted with g, and the efficient bilinear map is defined as $e : G_1 \times G_1 \rightarrow G_2$ such that $e(g^a, h^b) = e(g, h)^{ab}$ for every g, h $\in G_1$ and a,b $\in Z^*_{(p)}$. This bilinear map is proved to be non-degeneracy and computationally polynomial [13].

B. Identity-Based Encryption for Smart Meters

Identity-Based Encryption scheme derives public keys from public identities, such as e-mail addresses instead of using certificates and it is an important alternative to certificate-based key infrastructures. Figure 1 demonstrates this scheme and how it eliminates usage of certificates. In this scheme, a consumer encrypts a meter data with a public key, for example with a meter id, and then transmits it to an aggregator. Later, the aggregator collects the private key from the private key generator to decrypt the transmitted data. In this scheme, participants can encrypt data with no prior distribution of keys, which could be a problematic issue for smart meters.

BasicIdent is an identity-based encryption algorithm, which contains four separate algorithms: setup, extract, encrypt and decrypt [13]. In this algorithm, there are two cyclic groups G_1 and G_2, and three random generators are chosen as $R_1, R_2, R_3 \in G_1$. Two hash functions are defined as $H_1 : \{0, 1\}^* \rightarrow (G_1)^*$ and $H_2 : G_2 \rightarrow \{0, 1\}^*$. A random value s is chosen to be the master key, and it is used to calculate the public key as $P_{pub} = sR_1$ where $s \in Z^*_{(p)}$.

In the proposed scheme, smart meters receive their secret keys by using their meter identification number. Public keys of smart meters are calculated as $SM_p = H_1(SM_{ID})$, and these values are used to produce secret keys $SM_s = s(SM_p)$. These keys are sent to the metering devices and the aggregator. Smart meters receive their secret keys by using their meter identification number.

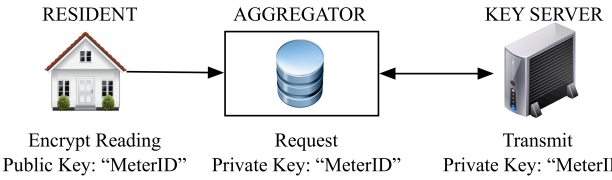

Figure 1. Identity-Based Encryption scheme.

The meter readings $(M_{ID})^t$ are signed with the pair $\Gamma(U,V)$ by first selecting a random number $k \in Z^*_{(p)}$. It is used the calculate $U = kR_1$ and $V = SM_{ID} + kH_2(ID, (M_{ID})^t, U)$. The verification is based on the value $e(R_1, V)$. If it is equal to the value of $e(P_{pub},H_1(ID))e(U,H_2(ID, (M_{ID})^t, U))$ the message is verified, otherwise it is rejected.

C. Problem Definition

The problem can be defined as transmitting smart meter readings in a secure way to a smart grid application server to be used in other smart grid applications, such as demand management systems. Each smart meter records readings at predetermined intervals t. There are 96 records in total to be transmitted per day when the value of t is chosen as 15.

For this study, we have the following assumptions:

- We assume that the internal hardware of metering devices is not accessible. This study concentrates on transmission security and data privacy.
- We assume that each metering device operates independently.
- Finally, we assume that the application server is in a safe zone. Server security mechanisms are beyond this study's interest.

III. THE PROPOSED SCHEME

The proposed privacy-preserving aggregation scheme for secure smart grid communications is based on Identity-Based Encryption [13]. However, the proposed scheme has some different aspects, as it shown in Figure 2. The scheme mainly consists of the following five entities: residents, id collector, key server, aggregator, and application server.

Residents are the consumers with smart metering devices. The scheme can also be applied with an extended-star topology by limiting the number of users per aggregator. A corrupted or modified device only reveals its individual reading and has no effect on the overall system. Unlike some other methodologies, the scheme does not need any communication between metering devices, and this will reduce communication complexity.

ID Collector collects meter readings from the residents and transmits public keys to them. After collecting the metering data, it stores consumer IDs in a hosted database and modifies the data structure by removing the ID field from the data and then adding a rowID field and data instead. This entity has two type of transmissions, as shown in Table I. The first transmission is forwarding the modified data to the aggregator. The second transmission is as a reply to the queries of the application server.

 ISBN: 978-1-61208-544-9

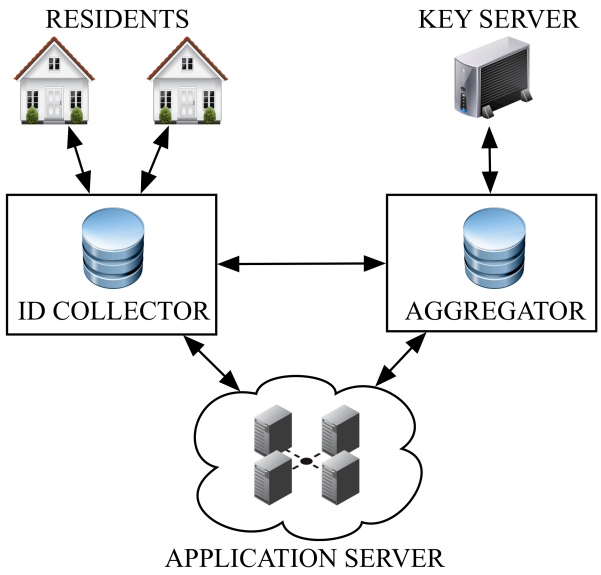

Figure 2. The proposed encyrption scheme.

The Aggregator is the entity where the decrypt operation happens. It collects meter readings and divides them into three parts as timestamp, rowID, and reading. For each data collection, only one timestamp value is used for the private key request. All meter readings are decrypted with this private key. After the decryption process, meter readings are stored in a database inside the aggregator. According to the structure of the proposed scheme, this entity has the meter readings but does not know to whom a particular reading has belonged.

Key Server is the private key generator, and it is responsible for key generation and distribution operations. Private keys need to be generated only once. According to the load, there might be more than one aggregator, and the key server in the system and additional servers can be distributed to different geographical locations. Unlike previous studies in the literature, the key server only communicates with the aggregator. Isolating the key server and limiting its accessibility provides a much better security.

Finally, an application server exists for smart grid operations, such as demand management. This server communicates with ID Collector and Aggregator entities to fetch consumption data of the residents. As it seen in Table I, the application server is the only entity, which can access a user's consumption data so that it is accepted as secure and protection of this structure is out of this study's scope.

IV. EVALUATION

In this section, we analyze the security properties and the performance of the proposed scheme.

A. Security

The proposed scheme has all security measures of Identity-Based Encryption scheme [12] since it is originated from that study. As a result, the confidentiality and integrity of the consumers' data are achieved in this study.

TABLE I. TRANSFER AND STORAGE OPERATIONS FOR THE METERING DATA

Sender	Transmission	Receiver	Storage
Residents	(timestamp, ID, Meter Reading)	ID Collector	-
ID Collector	(timestamp, rowID, Meter Reading)	Aggregator	(rowID, ID)
ID Collector	(rowID, ID)	Application Server	-
Aggregator	-	-	(timestamp, rowID, Meter Reading)
Aggregator	(timestamp, rowID, Meter Reading)	Application Server	-

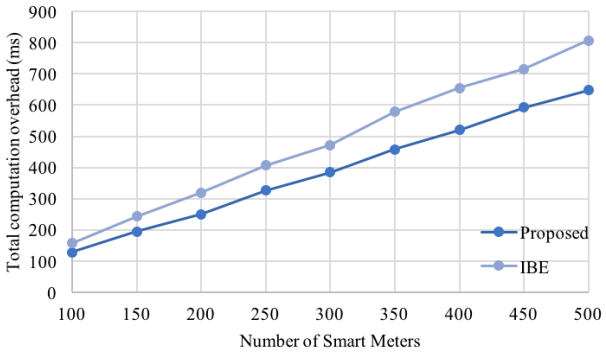

Figure 3. Total computation overhead.

Further, the proposed scheme is more secure to the CCA attacks than the classical scheme. A scheme is 'CCA-secure' if access to the decryption oracle does not give valuable information to the attacker. If an attacker somehow gains access to transmit a random message to the key server, the only information resolved will be a meter reading with no consumer information as the consumer information is stored in the ID collector entity. Hence, the privacy of the sensitive data is also achieved in the proposed scheme.

B. Performance

In this subsection, we will evaluate the proposed scheme regarding the computational performance. Figure 3 shows the total computation overhead of the proposed scheme and the traditional Identity-Based Encryption scheme. Total computation overhead is linear to the number of smart meters. The proposed scheme showed a better performance due to two reasons: one key usage for every new time interval and possibly decreased communication overhead. When the number of consumers and keys is small, both the computational and communicational overhead is low in both schemes. Total computation overhead increases with the increased number of smart meters, and this increase is much faster in the case of the traditional scheme. An increase in the number of smart meters also increase the performance losses of the traditional scheme because of the growing number of key exchanges.

It should be noted that an increase in hardware may lower the difference between two schemes but may also cause an excessive increase in the infrastructure costs.

 ISBN: 978-1-61208-544-9

V. CONCLUSION AND FUTURE WORK

In this paper, we proposed an Identity-Based Encryption scheme for privacy preservation in smart grid communication. Identity-Based Encryption scheme does not have issues, such as certificate lookup and management so that it is preferred in smart grid studies. The proposed scheme is more computationally efficient than the previous methods, and further improves the privacy and the security of the traditional key management infrastructures. The existing studies in the literature have usually been focused on the encryption algorithms themselves, but not on improving their efficiency in particular environments, such as smart grids. In this study, we concentrated on the data structure of meter readings and optimized that structure to make it more appropriate for smart metering systems. The overall performance is improved by reducing communication overhead caused by public key creation and distribution operations.

For future work, we will extend this study to analyze the communication overhead. We would also plan to optimize the computational overhead of the proposed scheme by modifying the encryption algorithm according to the developed data structure.

REFERENCES

[1] K. Sharma and L. M. Saini, "Performance analysis of smart metering for smart grid: An overview," Renewable and Sustainable Energy Reviews, vol. 49, pp. 720-735, Nov. 2014, doi:10.1016/j.rser.2015.04.170.

[2] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," Computer Networks, vol. 57, pp. 1344-1371, Jan. 2013, doi: 10.1016/j.comnet.2012.12.017

[3] N. Busom, R. Petrlic, F. Sebe, C. Sorge, and M. Valls, "Efficient smart metering based on homomorphic encryption," Computer Communications, vol. 82, pp. 95-101, May 2016, doi:10.1016/j.comcom.2015.08.016.

[4] T. E. Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in International Cryptology Conference Advances in Cryptology (CRYPTO), 1985, pp. 10-18.

[5] P. Paillier, "Public key cryptosystems based on composite degree residuosity classes," In Proceedings of Eurocrypt '99, pp. 223-238.

[6] X. Dong, J. Zhou, K. Alharbi, X. Lin, and Z. Cao, "An ElGamal-Based efficient and privacy-preserving data aggregation scheme for smart grid," Globecom 2014 Wireless Networking Symposium, pp. 4720-4725.

[7] D. Boneh, E. Goh, and K. Nissim, "Evaluating 2-dnf formulas on ciphertexts," in Proceedings of Theory of Cryptography, 2005, pp. 325–341.

[8] F. Laforet, E. Buchmann, and K. Böhm, "Individual privacy constraints on time-series data," Information Systems, vol. 54, pp. 74-91, Dec. 2015, doi:10.1016/j.is.2015.06.006.

[9] S. K. Hong, K. Gurjar, H. S. Kim, and Y. S. Moon, "A survey on privacy preserving time-series data mining," In 3rd International Conference on Intelligent Computational Systems (ICICS'2013), pp. 44-48.

[10] X. Yang, X. Ren, J. Lin, and W. Yu, "On Binary Decomposition based Privacy-preserving Aggregation Schemes in Real-time Monitoring Systems," IEEE Transactions on Parallel and Distributed Systems, 27(10), pp. 2967-2983, Jan. 2016, doi: 10.1109/TPDS.2016.2516983.

[11] P. Barbosa, A. Brito, and H. Almeida, "A Technique to provide differential privacy for appliance usage in smart metering," Information Sciences, vol.370-371, pp. 355-367, Nov. 2016, doi:10.1016/j.ins.2016.08.011

[12] Z. Huang, D. Wenliang, and B. Chen, "Deriving private information from randomized data," In Proceedings of International Conference on Management of Data, ACM SIGMOD, 2005, pp. 37-48.

[13] D. Boneh and M. K. Franklin, "Identity-Based Encyrption from the Weil Pairing," In Proceedings of 21st Annual International Cryptology Conference Advances in Cryptology (CRYPTO), Springer, 2001, pp. 213-229.

[14] J. L. Tsai and N. W. Lo, "Secure Anonymous Key Distribution Scheme for Smart Grid," IEEE Transactions on Smart Grid, 7(2), pp. 906-914, March 2016, doi: 10.1109/TSG.2015.2440658

[15] H. K. H. So, S. H. M. Kwok, E. Y. Lam, and K. S. Lui, "Zero-Configuration Identity-Based Signcryption Scheme for Smart Grid," 2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm), 2010, pp. 321-326.

[16] J. B. Hur, D. Y. Koo, and Y. J. Shin, "Privacy-Preserving Smart Metering with Authentication in a Smart Grid," Applied Sciences, vol. 5, pp. 1503-1527, Dec. 2015, doi: 10.3390/app5041503.

 ISBN: 978-1-61208-544-9