The Future of Homomorphic Cryptography in Smart Grid Applications

Maximiliane Zirm
University of Passau
Email: zirm@fim.uni-passau.de

Michael Niedermeier
University of Passau
Email: michael.niedermeier@unipassau.de

***Abstract*—On the basis of the bachelor thesis "performance comparison of cryptographic algorithms in Smart Grid applications" supervised by Dipl. Inf. Michael Niedermeier and Prof. Dr. Hermann de Meer at the chair of Computer Networks and Communications, this paper covers the analysis of the privacy ensuring capabilities of homomorphic cryptography in the Smart Grid with regard to its energy efficiency. The Paillier algorithm serves as an example and is used in two different architectural scenarios which are introduced and than compared to asymmetric and symmetric cryptography regarding their efficiency and practical applicability.**

I. Introduction

The Smart Grid is one of the most important technologies of our future, as our current power system is often unreliable and inefficient [1]. It works with detailed feedback information and two way communication between the different entities that are working together. However, due to the inherent interconnection communication, this system is a lot more vulnerable than the old power supply system [2]. With all the exchanged messages and the detailed consumer information, high security and especially privacy standards have to be ensured. But even though privacy is a very important aspect of the Smart Grid implementation, energy efficiency may not be forgotten. This paper will look at an homomorphic algorithm that can be used for privacy in the Smart Grid. It analyses its application in two scenarios for its energy efficiency, to see if homomorphic cryptography is suited to ensure a high privacy standard and keeping the energy costs at an acceptable level [2] [3].

II. Smart Grid

A. Overview

The modern solution to the problems posed by the outdated current power grid is the Smart Grid. The introduction of an intelligent power supply can guarantee more efficient energy transport and transparent energy usage information [2]. In contrast to the current system, the Smart Grid does not only transport electricity from the company to the consumer, it also depends on the exchange of data between the different participants of the network. With this two-way system and constant feedback, the power companies can e.g. dynamically adjust to rising or falling energy demand, as well as react to grid states [3]. With the transformation of the current power system to the Smart Grid, many advantages, for customers as well as providers, arise. Reliability, stability, easier integration of "green" energy and reduction of costs are just a few of them. Also, the Smart Grid offers *energy efficient* solutions for both customers and providers [4]. But with the complexity that enables these advantages, the Smart Grid also becomes vulnerable to attacks and failure. Risks to security like hacking attacks or data theft are as much a problem as *privacy* [5]. The gathered consumption data is very detailed which is dangerous when in the wrong hands, for both customers and companies. Not only can malicious attackers get valuable information about the customers from this data, but also the power company itself or third parties, like the customer's employer, can use the information for advertisement or surveillance. One way to guarantee confidential communication in the grid is the use of cryptography. Aside from the two well-known and established cryptography standards (symmetric and asymmetric cryptography), the unique properties of homomorphic algorithms, which will be further explained in Section III, can be of particular advantage in the Smart Grid. For the guarantee of privacy, the use of homomorphic algorithms in particular is encouraged, as consumer data can be encrypted and than aggregated in its encrypted state, so that only the total consumption of one area, but not the individual data is disclosed to entities other that the smart meter itself [6]. Another important aspect is to find a trade-off between security/privacy and energy efficiency which must not be forgotten while choosing the algorithms. Not only the economical aspect of saving energy has to be considered, but also the ecological side is of great importance. With the momentary state of global warming and scarcity of resources, finding an energy efficient solution for the Smart Grid is almost as important as finding one with the highest security and privacy standards [1].

B. Smart Grid Architecture

The Smart Grid architecture described in this paper uses the following terms for the different participants.

a) Smart Meters: To be able to measure this detailed amount of information and send it to the power company, a special device, the *smart meter* is necessary. Smart meters are relatively tamper-proof measuring devices which are being installed in every household integrated in the Smart Grid. They are capable of a two-way communication with the aggregator and send their information in very short time intervals (down to several seconds) [5]. In the most common smart meter models, communication goes through the Internet, either wirelessly or

using LAN [7].

b) Data Aggregator: The smart meters in this architecture are gathered in so-called *clusters*, which encapsulate households from connected areas, like e.g. all households from a city district. Each cluster is in possession of one so-called *data aggregator*. It is realized as a logically separate device, which can be physically isolated or integrated in one of the smart meters in the cluster itself. All smart meters in one cluster send their usage information to their respective data aggregator. There, the usage information is aggregated and thereby pseudonymized. This is done by extracting all personal information from the smart metering data and afterwards aggregating it on a cluster-wide level. So, the power company will only receive energy consumption information regarding the clusters, not the individual households. This helps to ensure consumers privacy while still being detailed enough to allow the Smart Grid to react to changing energy demands.

c) Power Company: The power company at the end receives the consumption data directly from the aggregators of every cluster. It has to be ensured that the company only has detailed usage data for a certain region, not for a single household but still is able to extract the billing information for each household in particular [8].

III. Homomorphic Cryptography

In the following, an overview over homomorphic cryptography in general and the Paillier scheme is given. In [9], homomorphic encryption schemes are described as "*encryption transformations mapping a set of operations on cleartext to another set of operations on ciphertext.*" This means, that it is possible to carry out operations on the ciphertext, without decrypting it first and therefore exposing the plaintext.
The notion of the existence of a **fully homomorphic** scheme was first proposed by Rivest, Adleman and Dertouzos in [10] with the introduction of the RSA public encryption scheme in 1978. A fully homomorphic scheme in this context means a turing complete scheme with a combination of homomorphic operators with which every possible process can be executed on the cipher text without decrypting it. When decrypted, it shows the same result as the same operators executed on the plaintext [10]. To find a fully homomorphic scheme has long been an important topic of cryptographic research. Only in 2009 Craig Gentry found the first fully homomorphic algorithm. He managed to create an algorithm that supports addition as well as multiplication and is turing complete [11]. Many **partially homomorphic** schemes have been found prior to this discovery. They only support a limited number of operators or can be executed only a few times consecutively. The fist partially homomorphic scheme was discovered by accident by Rivest, Shamir and Dertouzos in 1978 and is known to us as the asymmetric RSA algorithm. The fact that it is multiplicatively homomorphic, discovered shortly after its release, started the discussion about the possibility of fully homomorphic schemes [12] [10]. Most homomorphic algorithms are based on highly complex mathematical operations and are therefore computationally more complex than non-homomorphic asymmetric or symmetric algorithms, but the ability to do operations on a ciphertext offers huge possibilities for privacy applications [12].

A. Paillier Cryptosystem

One partially homomorphic algorithm which is often used for its efficiency is the Paillier scheme and its application has often been suggested for privacy purposes in the Smart Grid [13]. The three different steps of the Paillier scheme, key generation, encryption and decryption are described in the following.

1) Key Generation [14]:

- generate $n = pq$, with *p* and *q* being large prime numbers
- compute $\lambda = lcm(p-1, q-1)$
- select $g \in \mathbb{Z}^*_{n^2}$, with gcd(L($g^\lambda \ mod\ n^2$),*n*) = 1
- public key: (*n*, *g*), private key: λ

L is defined as $L(x) = \frac{x-1}{n}$, $\forall x \in \mathbb{S}_n$
$\mathbb{S}_n = \{u < n^2 \mid u = 1 \mod n\}$

2) Encryption [14]:

- Encryption with p being a plaintext $< n$ [14]
- select random *r* with $r < n$
- compute ciphertext c with $c = g^p \cdot r^n \ mod\ n^2$

3) Decryption [14]:

- check if $c \in \mathbb{Z}^*_{n^2}$, if not reject ciphertext
- decrypt ciphertext with $p = \frac{L(c^\lambda \ mod\ n^2)}{L(g^\lambda \ mod\ n^2)} \ mod\ n$

4) Homomorphic Property: The Paillier system is additive and multiplicative homomorphic. In this paper, only the additive component will be considered, which results in the following properties, with *E* being the encryption- and *D* being the decryption function:

$$D(E(p_1) \cdot E(p_2) \ mod\ n^2) = D(E(p_1) \cdot g^{p_2} \ mod\ n^2) = p_1 + p_2 \ mod\ n \quad (1)$$

$$D(E(p_1)^{p_2} \ mod\ n^2) = D(E(p_2)^{p_1} \ mod\ n^2) = p_1 \cdot p_2 \ mod\ n \quad (2)$$

$$D(E(p_1)^k \ mod\ n^2) = p_1 \cdot k \ mod\ n \ , \ k \in \mathbb{N} \quad (3)$$

5) Security & Energy Efficiency: The Paillier system is an asymmetric cryptosystem. Its security is based on the difficulty to break the computational composite residue problem and is secure against chosen-plaintext attacks. Its homomorphic property however, limits this security assumption [12] [15] .
In general the performance of asymmetric schemes is lower than the performance of symmetric schemes. Most schemes with significant homomorphic properties are considerably more complex than ordinary asymmetric schemes because of the frequent use of mathematical operations like power. [12].

IV. Assessment of homomorphic cryptography in Smart Grid environments

In the following, two different scenarios on how to use the Paillier cryptosystem (introduced in Section III) in Smart Grid applications are explained. Attacker models are being neglected in this paper.

A. Scenario 1: direct aggregation

The first scenario using the Paillier algorithm is the bold approach to use the scheme to encrypt the measurement data from each smart meter and use its additive homomorphic property to aggregate the user data at a separate aggregator, as depicted in Figure 1. Each entity in this architecture has its own set of keys, the known public key and the private key, which has to be kept secret from all entities except its owner. Communication channels are assumed to be secured by e.g. IP-Sec or SSL [16] and are neglected in this analysis.

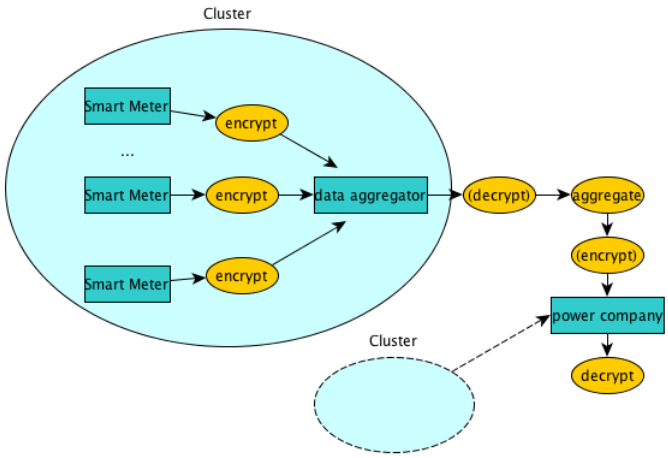

Fig. 1. Direct aggregation

In the following the usage data is described as $c(i,p)$, where i is the ID of the smart meter and p the time interval, for which the smart meter records the usage data. In this scenario, all smart meters send their usage data for p, encrypted with the public key of the power company, to the aggregator. There, the individual data is not decrypted, but aggregated, by using the homomorphic properties of the Paillier algorithm. The aggregator is now in possession of the encrypted overall consumption of the cluster for p without knowing the individual measurements of the smart meters. It then sends this encrypted data to the power company which can decrypt it with its private key. It is also possible to hierarchically set up aggregators, however this does not increase the level of privacy in the Smart Grid.

B. Scenario 2: spatial and temporal aggregation

The second and more sophisticated approach of how to make use of the privacy ensuring properties of homomorphic cryptography in Smart Grid environments is given in [13]. This relatively new idea was proposed in June 2012 and uses a slightly modified version of the Paillier system.
In this scenario, all the smart meters in one cluster share one public key and the private key also is known by all entities (smart meters as well as other participants). Additionally, there is no separate aggregation entity, but each smart meter can serve as aggregator.
[13] distinguishes between three aggregation modes: temporal, spatial and a combination of both. The usage data is described as $c(i,p)$, where i is the ID of the smart meter and p the time interval, for which the smart meter records the usage data. *Temporal aggregation* means the aggregation of the data for one smart meter in a time interval such as $\sum_p c(i,p)$. *Spatial aggregation* denotes the aggregation of the usage data of all smart meters for one measurement, such as $\sum_i c(i,p)$. A graphical display can be seen in Figure 2. *Spatio-temporal aggregation* is a combination of both approaches.

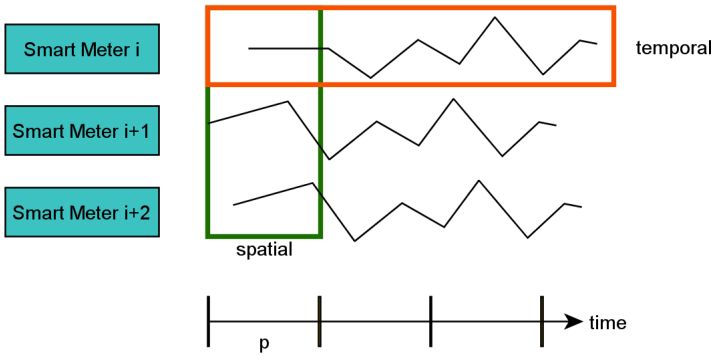

Fig. 2. Spatial and temporal aggregation as seen in [13]

The smart meters encrypt their data with a slightly modified version of the Paillier scheme. Additionally to the basic Paillier set-up in all N smart meters (described in Section III), a hash value $H(p)$ (e.g. with SHA-2) and a random number $r \in \mathbb{N}$ for every other smart meter j in the cluster is needed. Each smart meter encrypts its measurements and broadcasts (spatial) or stores (temporal) it. As an example, the encryption of the spatial aggregation proceeds as follows:

$$E(c(i,p)) = g^{(c(i,p))} \cdot h_{i,p}^{R(i,p)} \tag{4}$$

with g being the public key, $h_{i,p}$ the hash value of the smart meter for p and $R(i,p)$ computed as:

$$R_(i,p) = n + \sum_{j=1, i \neq j}^{N} r(i \to j, p) - \sum_{j=1, i \neq j}^{N} r(j \to i, p) \tag{5}$$

with n being the Paillier modulus and $r(i \to j, p)$ the random number generated in smart meter i for smart meter j in p. Even tough the private keys are publicly known within one cluster,

the individual usage data can not be decrypted, since the hash and the random number used for the encryption are not known. Only when the values are aggregated (here: all ciphertexts are multiplied) decryption is possible again, as with all the random values and hashes used, the final result of the aggregation is $E(\sum_{i=1}^{N} c(i,p))$. For the exact scheme and individual steps please refer to [13].

V. Analyzation and Conclusion

Comparing both scenarios, the second one is more flexible than the direct approach as the different modes allow to adapt to various Smart Grid architectures and privacy requirements. Another advantage is that the disclosure of the private keys is no longer a security factor, since it is not necessary to keep them secret with the modified Paillier scheme.
Both architectures can fully ensure privacy in the Smart Grid, which is critical for a full acceptance of this new technology. However, energy efficiency, as mentioned before, may not be forgotten, as it is one of the main goals of the Smart Grid and privacy should not be secured at the cost of saving energy [1]. In the context of the bachelor thesis, the direct aggregation scenario was implemented to see if it can be used efficiently in a smart metering environment. A Java based Smart Grid simulator was created to analyze the relative energy consumption and duration of different cryptographic measures, since no real Smart Grid test environment was available. Measurements with different numbers of clusters and households per cluster were taken. A Java BigInteger representing the usage data of a smart meter was encrypted, aggregated with the usage data of the other smart meters and then decrypted. The time and energy consumption of the sending of the data on the communication channels was neglected. It can be seen that encryption/decryption/aggregation processes take up to 10 times the CPU capacities and about 8 times the energy consumption of a non-homomorphic asymmetric scheme. Even tough no measurements of a real Smart Grid were available it can be assumed that this difference reflects on the performance in a real application scenario. To show the difference in efficiency the data of the results of a simulation for a smart grid with 50 clusters with 50 smart meters per cluster for Paillier and RSA without homomorphic use is shown in Table 1. RSA was chosen because an efficient implementation for Java was provided. 25 simulation runs were chosen to ensure a poignant median value. The simulation was conducted on a MacBook Pro with a 2,4 GHz Intel Core 2 Duo processor and 4 GB RAM with 1067 MHz DDR3, measuring only the encryption, deception and aggregation steps. The displayed data is the computed average of all simulation runs. The efficiency of the second scenario was not directly measured, but as the number of encryption, decryption and aggregation steps and the encryption scheme in general are about the same (depending on the use of either the only spatial and temporal or the spatio-temporal approach) and while in the second scenario the hashes and the random numbers must be computed and all nodes communicate also wit each other, less keys and actual encryption steps are needed than in the first one. So, the overall results will not deviate too much.

	RSA	Paillier
simulation runs	25	25
overall duration	47 s	283 s
single run duration	1700 ms	11000 ms
single run energy cons.	25,45 Ws	195,55 Ws

TABLE I
Statistics for the scenario with 50 clusters and 50 smart meters

As can be seen with this analysis, regarding energy efficiency, both scenarios loose to architectures which use non-homomorphic asymmetric or symmetric schemes to the extend, that usage in a Smart Grid environment can not be recommended. In [13] however, it is stated that it is already possible to implement the modified Paillier scheme with modern and powerful smart metering devices. Also, no non-homomorphic architecture can guarantee full privacy the way scenarios as those described in this paper can.
Homomorphic encryption and privacy in the Smart Grid cannot be separated and will become even more important, as the data of smart meters becomes even more detailed trough advance in technology and more and more countries decide to change their current power supply system into a Smart Grid system. Recently, the evolution of homomorphic cryptography from a theoretical concept to practically applicable algorithms became more and more rapid. Even tough the application of homomorphic cryptography in the Smart Grid is already realistic, as seen in this paper, there is still much work to do, to get full privacy without drawbacks in energy efficiency. However, with the swift development and the urgent need of a realistic solution, results can be expected within the next few years.

Acknowledgments

The author would like to thank the chair of Computer Networks and Communications at the University of Passau and her supervisor Dipl. Inf. Michael Niedermeier in particular for the great help and support received both for the bachelor thesis as well as for this paper.

References

[1] U.s. electricity blackouts skyrocketing. URL: http://edition.cnn.com/2010/TECH/innovation/08/09/smart.grid/index.html. [Online; accessed 21-November-2011].

[2] Swapna Iyer. Cyber security for smart grid, cryptography, and privacy. *International Journal of Digital Multimedia Broadcasting*, Volume 2011, 2011.

[3] Ning Lu Deborah A. Frincke Himanshu Khurana, Mark Hadley. Smart-grid security issues. *Security & Privacy, IEEE*, 8:81 – 85, Jan.-Feb. 2010.

[4] B.F. Massoud Amin, S.; Wollenberg. Toward a smart grid: power delivery for the 21st century. *Power and Energy Magazine, IEEE*, 2:34–41, 2005.

[5] Christopher Wolf Ann Cavoukian, Jules Polonetsky. Smartprivacy for the smart grid: Embedding privacy into the design of electricity conservation. Technical report, Information and Privacy Commissioner (IPC), Ontario, Canada, 2009.

[6] Flavio D. Garcia and Bart Jacobs. Privacy-friendly energy-metering via homomorphic encryption. In *STM*, pages 226–238, 2010.

[7] Saskia Jaarsma Rob van Gerwen and Rob Wilhite. Smart metering. *Leonardo Energy*, 2006.

[8] Georgios Kalogridis Costas Efthymiou. Smart grid privacy via anonymization of smart metering data. *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010.

[9] Josep Domingo-Ferrer. A provably secure additive and multiplicative privacy homomorphism. *Lecture Notes in Computer Science*, Volume 2433/2002:471–483, 2002.

[10] M. L. Dertouzos R. L. Rivest, L. Adleman. On data banks and privacy homomorphism. *Foundations of Secure Computation*, 1978.

[11] Craig Gentry. a fully homomorphic encryption scheme. Master's thesis, Stanford University, 2001.

[12] Fabien Galand Caroline Fontaine. A survey of homomorphic encryption for nonspecialists. *EURASIP Journal on Information Security*, 2007.

[13] Gene Tsudik Zekeriya Erkin. Private computation of spatial and temporal power consumption with smart meters. *Applied Cryptography and Network Security (ACNS 2012)*, 2012.

[14] Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. *Advances in Cryptology EUROCRYPT'99*, 1999.

[15] Tsuyoshi Takagi Kouichi Sakurai. On the security of a modified paillier public-key primitive. *ACISP '02 Proceedings of the 7th Australian Conference on Information Security and Privacy*, 2002.

[16] Guenter Schaefer. *Netzsicherheit - Algorithmische Grundlagen und Protokolle*. dpunkt.verlag, 2003.