Analysis of Privacy-Enhancing Protocols Based on Anonymity Networks

Fábio Borges*, Leonardo A. Martucci†, Max Mühlhäuser*
*Technische Universität Darmstadt – Telecooperation Lab
64293 Darmstadt, Germany
Email: fabio.borges@cased.de, max@informatik.tu-darmstadt.de
†Linköping University – Dept. of Computer and Information Science
SE-581 83 Linköping, Sweden
Email: leonardo.martucci@liu.se

***Abstract*—In this paper, we analyze privacy-enhancing protocols for Smart Grids that are based on anonymity networks. The underlying idea behind such protocols is attributing two distinct partial identities for each consumer. One is used to send real-time information about the power consumption, and the other for transmitting the billing information. Such protocols provide sender-anonymity for the real-time information, while consolidated data is sent for billing. In this work, the privacy properties of such protocols are analyzed, and their computational efficiency is evaluated and compared using simulation to other solutions based on homomorphic encryption.**

I. Introduction

Smart Grids are the evolution of the existing power grids. Visible aspects of Smart Grids are the electronic meters, called smart meters that monitor the users' electricity consumption and the harvested data to the electricity provider. Electricity providers are empowered with a fine-granular control over their distribution network and, thus, can better manage and balance the load in their networks. Real-time measurements of power consumption also allow the introduction of flexible pricing policies, i.e., the kilowatt hour retail price may fluctuate according to the demand, being more expensive during peak hours. Two-way communication between smart meters and providers allows the real-time retail price to be communicated to users, which can decide whether or not to turn on power-demanding devices. Smart meters can be connected to the home area network, in such a way that home appliances can be remote controlled. For example, in case of brownouts, Smart Grids could assign priorities for appliances and shut non-critical devices down.

Other advantages from implementing Smart Grids are the expected reduction of the ceiling capacity and the better management of micro-generation. Flexible pricing policies are expected to reduce demand during peak hours and, therefore, reduce the amount reserve capacity and costs. Micro-generation at the end-user premises can be better managed with Smart Grids, thus increasing the ceiling capacity. Smart Grids have a positive impact for all stakeholders: providers benefit from improved control and reduced operational costs; users have means to better manage their power consumption; and the society benefits from a smarter use of resources.

However, implementing Smart Grids incur many challenges. The scope of this work is the privacy in Smart Grids and its challenges. Information collected from smart meters can be used to profile customers by inferring their habits. For instance, collected data can indicate when a customer is at home, when she eats and if she has guests or not. User profiling can of course be performed by other means (such as electronic cookies on the Internet), but Smart Grids have the potential to offer a powerful new channel for collection of personal information that was previously inaccessible.

In this paper, we present an analysis and evaluation of privacy-enhancing protocols (PEPs) for Smart Grids that are based on anonymity networks, which implement anonymous communication protocols. The goal of these networks is to dissociate item of interests, i.e., messages, from customers. However, accounting and billing services require customers to be identifiable. It is possible to discern two different information flows with distinct characteristics: one for the real-time control data that is used to manage the power grid and another for billing and accounting information, which has no real-time requirements. The former information flow is forwarded by an anonymity network, which dissociate customers from consumption data. The latter is sent directly from customers to providers (as bills are computed by the smart meters). Two distinct information flows are created using two unlikable identifiers: an identity, which is linked to a unique customer and it is used for billing, and a pseudonym. The real-time information flow is associated only to the pseudonym, which is linked to a group of users. In this paper, the privacy properties of protocols using anonymity networks are evaluated using analytic methods. We show that the two information flows are unlikable and evaluate the security and efficiency of PEPs based on an anonymity network by comparing it with a mechanism based on a general case of homomorphic encryption.

This paper is organized as follows. We introduce terms, definitions and assumptions in Section II. Section III summarizes the background information. In Section IV, we show why PEPs using anonymity networks require distinct and unlinkable identifiers and analyze it in Section V. Section VI presents our simulations results against the generalized case of homomorphic encryption and Section VII concludes the work.

978-1-4577-1703-1/12/$26.00 ©2012 IEEE

II. Requirements, Definitions and Models

In this section, we introduce the terms, definitions, scope and assumptions used in this work.

A. Terms and Definitions

In this paper, we use a slimmer version of reference model designed by the National Institute of Standards and Technology (NIST) [1], since not all actors and domains are necessary. The relevant domains for our work are:

- *Customers*: represent the end-users. They may also generate, store and manage the use of the electricity (with batteries and local generation at the customers' premises).
- *Operations*: manage the movement of electricity.
- *Service Providers*: provide services to customers.

In our analysis, Service Providers and Operations are modeled as a single domain, the *SP & O*. It simplifies our analysis without reducing the validity of the proposed solution, as the Customers' privacy requirements are the same for both Operations and Service Providers. The domains that are part of the NIST reference model but are not relevant to our paper are *Markets*, *Bulk Generation*, *Transmission* and *Distribution*.

B. Problem Definition, Scope and Assumptions

In this paper, we analyze the efficiency of privacy-enhancing protocols for Smart Grids that provide sender-anonymity for the real-time data and allow the *SP & O* to bill Customers according to a specific pricing scheme. We compare these protocols with a mechanism based on the general case of homomorphic encryption. We consider protocols based on anonymity networks and assume that every meter has two partial identities, one for each information flow, that are constructed with two unlinkable digital identifiers:

- a unique and public Customer identifier *IdC* and,
- a public group (of Customers) identifier *IdG*.

These two identifiers are further detailed in Section IV. The distribution of *IdC* and *IdG* is out of the scope of this paper and it is left for future work. We assume that both identifiers are pre-loaded in the smart meters.

The PEPs analyzed in this paper are not designed to protect smart meters against side-channel attacks or tampering. We assume that the operational system and software components running on the smart meters are trusted.

III. Background

Proposals for achieving privacy using data aggregation in Smart Grids can be divided into two categories: those implemented on the application layer and those on the network layer. In this section, we summarize these two approaches.

1) Application Layer: Proposals for privacy-enhancing metering using applications for data aggregation are based either on homomorphic encryption [2] or other cryptographic schemes [3] that can be defined as homomorphic functions. Most of the proposed schemes are constructed using homomorphic encryption. It allows mathematical operations to be computed using pieces of ciphertext. Hence, metering information from different Customers can be aggregated before being transmitted to the *SP & O*. Different cryptographic methods can be used to implement homomorphic functions.

2) Network Layer: Sender anonymity can be achieved using an anonymity network. Smart meters can establish low-latency peer-to-peer anonymity networks, such as Crowds [4] or Chameleon [5], [6]. A proposal network layer data aggregation in Smart Grids is described in [7]. Although it is not classified as a privacy-enhancing protocol, it resembles one, as some smart meters behave similarly to MIX nodes [8], i.e., they collect real-time data from other meters and aggregate data into a single packet before sending it to the *SP & O*.

IV. Generalized Ideas Behind PEPs based on Anonymity Networks

In this section, we generalize PEPs based on anonymity networks for Smart Grids. We show that anonymity networks can be used to protect privacy in Smart Grids, why it requires partial identities and also requires the agreement of cryptographic keys.

A. Information Flows and Partial Identities

The nature of information generated by a smart meter can be divided into two information flows, each with its own characteristics: one for control data and another one for billing data. Each information flow has its own requirements. On the one hand, control data may have real-time requirements, as it is needed for managing the power grid. On the other hand, billing data is needed on an arbitrary basis only, e.g., monthly. We first show that it is impossible to protect the Customer's privacy if both information flows are transmitted using a same communication channel and there is a direct connection between the Customer and the *SP & O*.

Suppose by contradiction that there is a method M that protects the personal identifiable information (PII) of a Customer. Assuming M and choosing any $x \in PII$, the *SP & O* does not know x according to the assumption of M. However, since the *SP & O* has received the billing information, it has access to x. Thus, there exist no M.

To protect the Customer's privacy, it is possible to either eliminate the direct communication between the Customer and the *SP & O* (e.g. by introducing a trusted third party) or to use two distinct communication channels. We first concentrate on the use of separation of communication channels.

Each channel has its own characteristics that are given by the nature of the information. A direct communication channel between Customers and the *SP & O* can be established for sending the billing data. As billing necessarily requires access to Customers' PII (such as a unique identification number), sender anonymity is not required in this channel. On the real-time control data channel, however, sender anonymity is desirable as PII is not required for the provision of the intended service (i.e., to manage the grid). Sender anonymity is obtained by forwarding the control data to the *SP & O* through an anonymity network. Each channel is associated to an identifier, or partial identity: *IdC* for the direct communication channel and *IdG* for forwarding the control data.

Privacy can be protected as long as *IdG* is linked to more than one *IdC* and the rate for sending control data remains higher than the one for sending the billing data. The relation between the transmission rates of the real-time control data r_c and the billing information r_b and its impact to privacy is described next. It is possible to the *SP & O* to compromise the Customers' privacy if it can link two information flows that are originated from a given Customer. If $r_c = r_b$, then the *SP & O* receives the billing information in real-time (i.e., on the same rate of the control data). Since the *SP & O* knows the relationship between the electricity price and the billing data, then the real-time power consumption information can be calculated after the billing. Thus, the *SP & O* can link the control data back to the Customer.

B. Key Agreement

Secure sessions are needed for transmitting the control data through the anonymity network. Unless session keys are predeployed, a key agreement protocol is required. The use of symmetric cryptography only can offer a better computational performance than solutions based on asymmetric cryptography. However, key management can be problematic in large scale systems, such as Smart Grids. Thus, we assume the use of the Diffie-Hellman (DH) key agreement [9]. A smart meter needs to perform one DH key agreement in order to send ciphered messages with a secret key, and another DH key agreement to receive ciphered messages with a different secret key. To improve security, the keys need to be renewed from time to time. Anonymous authentication means that the *SP & O* knows that the meter is valid, but cannot identify which meter it is. Any key agreement algorithm that does not disclose the Customer's *IdC* can be used.

Symmetric keys, which are the product of the key agreement protocol, are used to establish end-to-end secure sessions between Customers and the *SP & O*. The secure session is used to forward control data through the anonymity network. The only information that the *SP & O* obtains about its Customers is *IdG*, i.e., the group identifier. *IdG* indicates that the meter is in the set of Customers.

C. Privacy-Enhancing Protocols and Anonymity Networks

Privacy-enhancing protocols based on anonymity networks can be designed to achieve different levels of anonymity. In Smart Grids, sender anonymity is required for protecting the Customers' privacy. Taking into consideration a general anonymity network that provides sender anonymity, a protocol for forwarding the control data can establish an arbitrary number of secure sessions between a Customer and the *SP & O*, where the number of secure session established equals twice the number of runs of the key agreement protocol, and assuming that a piece of control data is not forwarded by two or more different sessions. The level of privacy is equivalent to the amount of control data information forwarded through the secure sessions. For instance, if a single secure session is used for forwarding all control data, it can be compared with the set containing the billing data, which may lead to individual matches, i.e., the level of privacy tends to zero. On the contrary, if every secure session forwards a single piece of control data only (e.g., a single packet), then the level of privacy is maximum. However, it also results in a high computational performance cost, as the number of runs of secure session established equals the number of control data packets. In our evaluation, we assume that there are concurrent secure sessions. Figure 1 shows the sequence of messages.

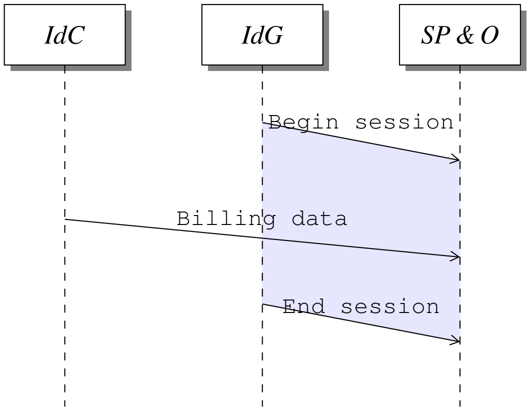

Figure 1. The sequence of messages exchanged by privacy-enhancing protocols based on network anonymity. Control data is sent using *IdG* and billing data with *IdC*.

The billing information is calculated by the smart meter, linked to *IdC* and sent to the *SP & O* through a secure session. The *SP & O* distributes the current retail price to the Customers. The total cost $Total$ is:

$$Total = \sum_{i=1}^{T} (\alpha_i \times \beta_i - \gamma_i \times \delta_i),$$

where β_i is the Consumers' buying price, δ_i is the Consumers' selling price (i.e., local generation), α_i is the electricity consumption, γ_i is the amount of locally generated electricity and T is the number of measurements used in the billing.

V. Analysis

Privacy-enhancing protocols based on anonymity networks can offer privacy to Customers and access to real-time control data to the *SP & O*, which can charge Customers according to a given pricing scheme policy. A Customer's privacy is protected because the control data information cannot be linked back to her, i.e., no adversary can establish a relationship between the *IdC* and the *IdG* sets. Figure 2 illustrates the relationship between the sets of Customers (A), *IdC* (B), *IdG* (C) and secure sessions (D).

To show that the *SP & O* cannot link a Customer (element of set A) to a secure session (element of set D), suppose by contradiction that there exists a function f from set C to set D and two distinguish secure sessions $d_i \neq d_j$ s.t. $d_i, d_j \in D$ are associated to a same *IdG*. Choosing any element $c \in C$ then $f(c) = d_i$ and $f(c) = d_j$, therefore $d_i = d_j$. The same rationale could be applied in the relationship from set C to B. Thus, there exists no function between sets A and D.

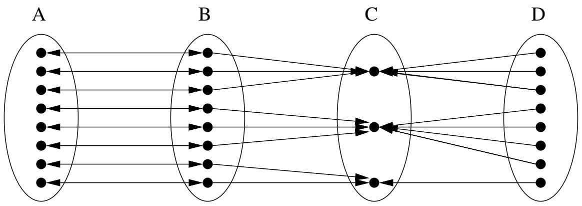

Figure 2. The relationship between the Customers' set (A), the *IdC* set (B), the *IdG* set (C), and the set of all secure sessions (D). There exists a bijective function between the sets A and B. There exists a surjective function from set B to C, and another surjective function from set D to C.

Secure sessions are unlinkable between them and a meter can establish an arbitrary number of concurrent sessions. The number of sessions observed by the *SP & O* lies in the interval:

$$|B| \leqslant |D| \leqslant \sum_{i=1}^{T} \sum_{j=1}^{|B|} \alpha_{i,j}, \tag{1}$$

where $\alpha_{i,j}$ is the electricity consumption reported by a Customer. The upper bound in Equation (1) is the total consumption observed by the *SP & O* (e.g., in Watt). Shortening the lifetime of secure sessions increases the Customers' privacy level but decreases the solution's computational performance, cf. Section IV-C. The performance of privacy-enhancing protocols based on anonymity networks is evaluated next.

VI. Simulation and Evaluation

In this section, we present the results of our performance evaluation. The evaluation was performed by means of simulation. The metric is the processing time. We compare the performance of key agreement protocols required for privacy-enhancing technologies based on anonymity networks, named identity-based key agreement (IK) with homomorphic functions (HF), which are the generalized case of homomorphic encryption. To the best of our knowledge, most homomorphic encryption schemes for Smart Grids are based on the Discrete Logarithm Problem.

Assuming a public key with modulus m and base g with a block size of r and a ciphertext $g^x u^r \mod m$ of a message x, the homomorphic property using Benaloh's method [10] is:

$$\begin{aligned} \mathcal{E}(x_1) \cdot \mathcal{E}(x_2) &= (g^{x_1} u_1^r)(g^{x_2} u_2^r) \\ &= g^{x_1+x_2}(u_1 u_2)^r \\ &= \mathcal{E}(x_1 + x_2 \mod r). \end{aligned} \tag{2}$$

Using Paillier's method [11], a public key with modulus m and base g, and the ciphertext $\mathcal{E}(x) = g^x r^m \mod m^2$ of a message x, the homomorphic property is given by:

$$\begin{aligned} \mathcal{E}(x_1) \cdot \mathcal{E}(x_2) &= (g^{x_1} r_1^m)(g^{x_2} r_2^m) \\ &= g^{x_1+x_2}(r_1 r_2)^m \\ &= \mathcal{E}(x_1 + x_2 \mod m). \end{aligned} \tag{3}$$

We can generalize the schemes (2) and (3) in

$$\overbrace{(g^{x_1} u_1^r)}^{\text{Meter}} \overbrace{(g^{x_2} u_2^r)}^{\text{Meter}} \cdots \overbrace{(g^{x_i} u_i^r)}^{\text{Meter}} \tag{4}$$

where $x_1, \ldots, x_i$ represent the measurements, and $u_1, \ldots, u_i$, g and r are pseudo-random values from Benaloh's and Paillier's methods. Equation (4) shows that in HF Customers need to execute at least 2 exponentiations and 1 multiplication for each measurement, and the *SP & O* needs $i-1$ multiplications. IK requires 4 exponentiations for Customers and 4 exponentiations for the *SP & O* for establishing a secure session.

A. Theoretical Results

In our analysis, we take into account only the most expensive operations in terms of processing time [12]. Let E be the exponentiation cost and M the multiplication cost and i is the number of measurements. The computational cost of an HF-based scheme is at least $2iE+iM$ for a Customer and $(i-1)M$ for a *SP & O*. For IK-based schemes, the computational cost is $4jE$ for a Customer and $4jE$ for a *SP & O*, where j is the number of secure sessions established.

The total cost $HF(i)$ for HF is $2iE + iM + (i-1)M$, where i is the number of measurements. And the total cost $IK(j)$ for IK is $8jE$, where j is the number of sessions. For calculating the intersection point of the curves $HF(i)$ and $IK(j)$, we assume that $i = j = t$, i.e., the number of secure sessions established is equal to the number of measurements (a secure session is used for sending one measurement only). So, $2tE + tM + (t-1)M = 8tE$ and then we have

$$t = -\frac{M}{6E - 2M}.$$

Therefore, there is no intersection for $t > 0$. Thus, the cost for *IK* is always higher than the cost for *HF* assuming that the number of secure sessions established is equal to the number of measurements. However, for $i \neq j$ these results are not necessarily true. The total cost is a function of growth rate, which has a important meaning, since it provides a better insight of the relationship between the $HF(i)$ and $IK(j)$. The growth rate of the functions $HF(i)$ and $IK(j)$ is determined by the slope of each curve. The slopes are given in function of the mean cost of a single iteration. We then have

$$\begin{cases} HF(i) = 2iE + iM + (i-1)M \approx i \times \overline{a} \\ IK(j) = 8jE \approx j \times \overline{b} \end{cases}$$

where $\overline{a}$ is the average cost of one measurement for HF and $\overline{b}$ is the average cost for establishing a secure session in IK.

In order to determine the rate between the variables i and j, where $HF(i)$ is greater than $IK(j)$, i.e.,

$$HF(i) \overset{?}{>} IK(j).$$

We prove that $HF(i) > IK(j)$ for $i = 4j$, if the modular exponentiation and multiplication costs are constant. Since $2t-1 > 0 \; \forall \; t \in \mathbb{N}^*$ and the processing time for M is greater than zero, so multiplying the inequality by M, we have

$$(2t-1)M > 0 \; \forall \; t \in \mathbb{N}^*. \tag{5}$$

Adding $2tE$ to the both sides of the Equation (5) and reordering it, we obtain

$$2tE + tM + (t-1)M > 8\left(\frac{t}{4}\right)E \; \forall \; t \in \mathbb{N}^*.$$

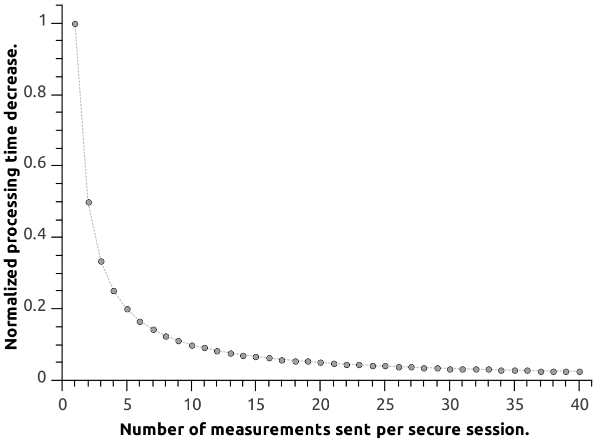

Figure 3. The processing time decreases in relation to the number of real-time measurements that are sent per secure session established. The processing time shown in the *y*-axis is normalized.

And multiplying the resulting inequality by i, we obtain

$$HF(t) > IK\left(\frac{t}{4}\right).$$

Thus, $HF(i) > IK(j)$ for $i = 4j$, i.e., there are at least 4 measurements sent for each secure session established using IK, assuming that the modular exponentiation and multiplication costs are constant. The performance of IK-based solutions increases with the number of measurements that are sent through a secure session, as shown in Figure 3.

B. Simulation Parameters

In our simulation, u, g and r, c.f. Equation (4), are 1024-bit length, and x has a length of 10 bits (where x is a measurement). The message length for the real-time measurements can be relatively short, i.e., 10 bits, as it is related to the instantaneous recording of electricity consumption characteristics. The DH parameters are 1024-bit length, with exception of the module, which is 2048-bit length.

The results obtained from our simulation differ by a factor of 10 instead of 4 from the theoretical results presented in Section VI-A because the exponentiation cost is not constant for the chosen bit lengths.

The simulator was implemented in `C` using GMP (GNU Multiple Precision) version 5 as library for multiple precision arithmetic. The simulator was running on an Intel Core(TM)2 Duo CPU T9400 2.53GHz processor with 4GB of memory. The operating system was an Ubuntu Linux with kernel version 3.0.0-12-generic for 64 bits.

C. Simulation Results

We simulated four different cases, and 10^5 measurements were generated for each case. In the 1^{st} case, we measured the Customers' processing time *HFC* using HF. In the 2^{nd} case, we measured the *SP & O*'s processing time *HFS* using HF. The 3^{rd} and 4^{th} cases are the analogous to the first two, but using IK instead of HF, where *IKC* is the processing time in the Customers' end and *IKS* is the processing time in the *SP & O*'s end. The results are presented in a box plot in Figure 4. The lower and higher quartiles are very close to median in all cases.

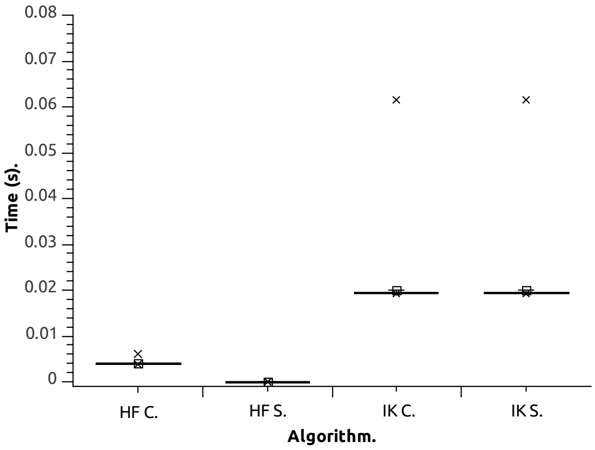

Figure 4. Box plot representing the processing time Δt required for each simulated case. Each case consists of 10^5 measurements. *HFC* and *HFS* are the Δt for Customers and *SP & O*, respectively, using HF. *IKC* and *IKS* are the Δt for Customers and *SP & O*, respectively, using IK.

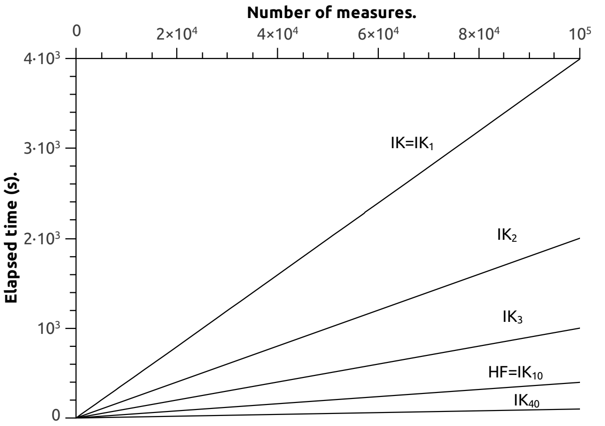

Figure 5. The family of functions IK_i is presented in this figure. It shows that $IK = IK_1$ and $HF = IK_{10}$, where IK and HF were obtained in our simulation.

The results for $\overline{a}$ and $\overline{b}$ determine the slope of the following functions:

$$\begin{cases} HF(i) = 2iE + iM + (i-1)M \approx i \times \overline{a} = i \times 0.004 \\ IK(j) = 8jE \approx j \times \overline{b} = j \times 0.04 \end{cases}.$$

To validate our findings regarding the fitting to a linear approximation, we compared the curves produced by functions $HF(i)$ and $IK(j)$ to the results obtained in the simulation. Figure 5 shows the fitting between the functions $HF(i)$ and $IK(j)$ and the HF and IK curves obtained in our simulation.

Let IK_i be a family of functions given by $IK_i = IK\left(\frac{j}{i}\right)$. It describes more than one measurement sent over a single secure session established using IK. There is a function in the family IK_i that corresponds to the function $HF(i)$, namely IK_{10}. Figure 5 shows that $IK = IK_1$ and $HF = IK_{10}$. It also shows the curves for IK_2, IK_3 and IK_{40}. The performance gain in relation to i is shown in Figure 3.

D. Comparison with Related Work

Protocols based on homomorphic encryption, e.g. [2], have a high computational cost due to modular exponentiation [12]. Using homomorphic functions for privacy protection means that every measurement requires at least 1 multiplication and 2 exponentiations. Homomorphic functions are not fair in the distribution of the computational costs for the parties involved in the protocol, as most of the computational costs falls on the Customers' side. It means that demanding cryptographic operations need to be computed using the rather limited resources of the smart meters.

Privacy-enhancing mechanisms that are based on anonymity networks may, however, leak personal information. Sending more than one measurement per secure session intuitively degrades the Customers' privacy level. These schemes also require the deployment of an anonymity network, which may increase the communication delay (round-trip time) between Customers and the *SP & O*. Peer-to-peer anonymity networks require peers to forward data, which may introduce an additional computational cost for the smart meters.

The network layer data aggregation proposed in [7] was not designed for protecting the Customers' privacy, as the *SP & O* and the aggregator can link measurements to their sources. However, if we assume that the aggregator is trusted, it is possible to modify the proposal shown in [7] to enhance Customers' privacy, in exchange for a higher computational cost for the aggregator.

VII. Conclusions

We presented an analysis and evaluation of PEPs for Smart Grids that are based on anonymity networks. These protocols protect the Customers' privacy without hampering electricity providers from obtaining real-time control data information from the metering infrastructure and allow Customers to be correctly billed.

The underlying idea is to exploit the different nature of the information flows needed in Smart Grids. We showed that each information flow needs to be associated to an identifier, or partial identity. Customers have two partial identities: *IdG*, which is used for sending real-time control data; and *IdC*, which is used only for billing. *IdC* is linked to the Customer's real identity, while *IdG* does not contain any *PII* and is a group identifier, which is related to a set of Customers. The privacy-enhancing protocol based on anonymity networks provides sender-anonymity to the Customers for the real-time control data towards the *SP & O*.

We analyzed a general privacy-enhancing protocol based on anonymity networks and compared its computational performance with a homomorphic encryption scheme. The former was generalized as a key agreement mechanism IK and the latter was abstracted as a generalized case of a homomorphic encryption scheme HF. Privacy-enhancing protocols based on anonymity networks require other security mechanisms, such as symmetric encryption, but IK is its most demanding component in terms of computational performance.

The evaluation was carried out by means of simulation. The metric used was the measured processing time. For IK, it was the time required to establish a secure session. And for HF, it was the time needed to encrypt a control data message (as secure sessions are not required to be established in the case of HF). We also analyzed the distribution of the computational load between Customers and the *SP & O*. We showed that the processing time required for IK is lower than for HF.

Privacy-enhancing protocols based on anonymity networks have three limitations. Firstly, its improved computational performance is obtained at the cost of reduced privacy protection. Increasing the amount of measurements forwarded through a secure session may have negative impact on a Customer's privacy level. Secondly, as there are no aggregation of measurements, it is possible in theory to correlate the real-time information to the billing data. Finally, the deployment of an anonymity network results increases the end-to-end delay for messages to reach the *SP & O* [6] and also incur in extra computational costs that are needed to forwarding messages. In the future, we intend to further analyze and quantify those limitations.

References

[1] *NIST Framework and Roadmap for Smart Grid Interoperability Standards. Release 1.0*, NIST Special Publications 1108, Office of the National Coordinator for Smart Grid Interoperability – National Institute of Standards and Technology (NIST), USA, Jan 2010.

[2] F. Li, B. Luo, and P. Liu, "Secure information aggregation for Smart Grids using homomorphic encryption," in *1^{st} IEEE Int Conf on Smart Grid Communications (SmartGridComm)*, Oct 2010, pp. 327–332.

[3] K. Kursawe, G. Danezis, and M. Kohlweiss, "Privacy-friendly aggregation for the Smart Grid," in *Privacy Enhancing Technologies*, ser. LNCS. Springer, 2011, vol. 6794, pp. 175–191.

[4] M. Reiter and A. Rubin, "Crowds: Anonymity for Web Transactions," in *DIMACS Technical report*, 1997, pp. 97–115.

[5] L. A. Martucci, C. Andersson, and S. Fischer-Hübner, "Chameleon and the Identity-Anonymity Paradox: Anonymity in Mobile Ad Hoc Networks," in *1^{st} Int. Workshop on Security (IWSEC)*. IPSJ, Oct 2006, pp. 123–134.

[6] L. A. Martucci, "Identity and anonymity in ad hoc networks," Ph.D. dissertation, Karlstad University, Jun 2009.

[7] A. Bartoli, J. Hernandez-Serrano, M. Soriano, M. Dohler, A. Kountouris, and D. Barthel, "Secure lossless aggregation over fading and shadowing channels for Smart Grid M2M networks," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 844–864, Dec 2011.

[8] D. Chaum, "Blind signatures for untraceable payments," in *CRYPTO*, 1982, pp. 199–203.

[9] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Information Theory*, vol. IT-22, no. 6, pp. 644–654, 1976.

[10] L. Fousse, P. Lafourcade, and M. Alnuaimi, "Benaloh's dense probabilistic encryption revisited," in *Progress in Cryptology – AFRICACRYPT 2011*, ser. LNCS. Springer, 2011, vol. 6737, pp. 348–362.

[11] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Advances in Cryptology - EUROCRYPT 1999*, ser. LNCS. Springer, 1999, vol. 1592, pp. 223–238.

[12] P. Lara, F. Borges, R. Portugal, and N. Nedjah, "Parallel modular exponentiation using load balancing without precomputation," *Journal of Computer and System Sciences*, vol. 78, no. 2, pp. 575–582, 2012.