Communication-efficient privacy-preserving smart metering

Sigurd Eskeland
Norwegian Computing Center
0314 Oslo, Norway
sigurd.eskeland@nr.no

ABSTRACT

The frequent reporting by smart meters may raise privacy concerns about the whereabouts of the consumers. There have been a number of privacy-preserving schemes proposed during the recent years, whereof most provide privacy-preserving aggregation of consumption values from groups of smart meters, while less provide privacy-preserving billing computations. An important aspect is transmission efficiency, since smart meter communication is usually wireless. Groups of smart meters form mesh networks, where the meters organize temporarily wireless paths where they forward messages on behalf of each other to and from the master meter or base station. Low transmission overhead is thus of high concern to reduce the amount of communication. Also of concern is resilience towards adversaries that are capable of compromising multiple meters. In this paper, we propose privacy-preserving schemes for consumption aggregation and billing that are communication-efficient and that provide $(s-1)$-resilience.

CCS CONCEPTS

• **Security and privacy → Privacy-preserving protocols**;

ACM Reference Format:
Sigurd Eskeland. 2017. Communication-efficient privacy-preserving smart metering. In *Proceedings of ECSA '17, Canterbury, United Kingdom, September 11–15, 2017,* 6 pages.
https://doi.org/10.1145/3129790.3129802

1 INTRODUCTION

Smart meters are currently being pushed into the society. This allows power companies and power authorities to continuously monitor and collect electricity consumption data of every individual household. Consumption reporting occurs at short time intervals (e.g., every hour) — in contrast to monthly-based billing. This allows power companies to implement dynamic pricing regimes, and so to charge their consumers according to variable tariffs.

The scope of such data registration may not be limited to the management of the respective individual power companies, but may for various purposes be centralized in national data hubs. In particular, such a centralization is, amongst other, justified to the public by a need to coordinate billing among several actors. In countries using billing regimes that differentiate between transmission costs (charged by the grid operator) and the electricity consumption (charged by the power supplier), such coordination is relevant. Moreover, since national electricity grids are interconnected, at least in Europe, and thus form international electricity markets, this causes a further centralization that is realized by transnational data hubs.

Smart meter employment makes it possible to establish fine-grained consumption profiles of individual private homes, and henceforth raises several privacy concerns. Realtime consumption reporting reveal if people are home or not, and likewise at what times people have been at home. Even private information such as what appliances and devices are being used, and estimates about the number of inhabitants that are present, may in some cases be deduced.

Performance is of great importance, since smart meter communication is usually wireless. Groups of smart meters form mesh network, where the meters organize temporarily wireless paths where they forward messages on behalf of each other to and from the master meter or base station. A single smart reporting therefore result in communication that involves a number of meters.

Privacy-preserving schemes address mainly the following privacy issues:

(1) Privacy-preserving aggregation of consumption values from groups of smart meters.
(2) Verifiable privacy-preserving billing computation of individual smart meters by the dot-product $b = \mathbf{c} \cdot \mathbf{r}$, where $(\mathbf{c})$ is the consumption vector and $(\mathbf{r})$ is the tariff rate vector for a given time period t (e.g., a month).

Most papers address only the first case. In this paper we address both. In Sections 2.2 and 2.4 we present two privacy-preserving schemes that sum the electricity consumption from clusters of smart meters w.r.t. time intervals. In Section 3.1, we present a verifiable privacy-preserving billing scheme for billing computation of individual smart meters, that allows the power company to verify the correctness of the billing computations.

The schemes are unique in the sense that they have lower transmission overhead in contrast to previously proposed schemes, because each smart meter does not communicate with other smart meters for privacy computation purposes, only with the head-end system (HES).

1.1 Related work

The literature contains a number of papers of privacy-preserving aggregation schemes and billing schemes. Those schemes usually use homomorphic techniques. For aggregation schemes, privacy is achieved by splitting the consumption values into shares of random

ECSA '17, September 11–15, 2017, Canterbury, United Kingdom

ACM ISBN 978-1-4503-5217-8/17/09…$15.00
https://doi.org/10.1145/3129790.3129802

values that are communicated to an associated meter that computes partial sums of received shares. Equivalently, each meter masks consumption values by a random nonce that in concert with other nonces that are sent to associated meters sum to zero. This all-to-all communication causes a high transmission overhead. Next are some relevant aggregation schemes.

Garcia et al. [6] presented a "no-leakage protocol" that has three transmission rounds and uses the homomorphic Pailler cryptosystem [13]. Each smart meter splits a consumption value into n random shares, and encrypts $n-1$ shares w.r.t. the other smart meter, respectively. These are sent to the HES, that sums the encrypted shares w.r.t. each smart meter. The encrypted sums are then sent to each smart meter, that decrypts and adds the final share, and sends the result to the HES, that than obtains the full sum. In all there are $O(n^2)$ transmissions and $n(n-1)$ encryptions. Klenze [10] presented a scheme based on [6], which is rather impractical due that it requires users to interact with the smart meters to verify that they are not being compromised.

Erkin et al. [3] presented an aggregation scheme, where each meter generates a random number w.r.t. each other smart meter. It is encrypted using the homomorphic Pailler cryptosystem and sent to the respective meter. Each meter decrypts the received message, and masks the measurement using the sum of the received encryptions. The HES multiplies the masked measurements and obtains the sum. Hence, there are $O(n^2)$ transmissions and $O(n^2)$ encryptions.

The aggregation scheme in [8] assumes a trusted dealer that provides each meter with a randomly generated secret pre-distributed key share, where all shares sum to zero. The key shares are used for masking the consumption values. The aggregator obtains homomorphically the sum by multiplying the masked values. The main disadvantage is the pre-distributed key shares, which correspond to a fixed group. Group membership updates therefore require new key share distributions for all meters. The scheme is efficient by $O(n)$ transmissions and $O(n)$ masking operations.

The scheme by Leontiadis et al. [11] is based on [8], and overcomes its disadvantage of static key shares. However, it requires a third party (a "collector") that acts as an intermediate between the meters and the aggregator.

Jung et al. [9] presented a privacy-preserving secure-sum (and a secure product) aggregation scheme. The users (or meters) form a logical ring, where a given meter SM_i compute the masking value as a modular fraction $\frac{k_{i,i+1}}{k_{i-1,i}}$ of the two Diffie Hellman-secrets $(k_{i,i+1}, k_{i-1,i})$, that it respectively shares with each of the two adjacent meters, SM_{i-1}, SM_{i+1}. This method is similar to the conference key agreement protocol proposed by Burmester et al. [1]. The masking values homomorphically sum to zero by multiplication. Since two colluding parties knowing $(k_{i,i+1}, k_{i-1,i})$, can accordingly obtain the masking value, and hence consumption value of SM_i, it is only 1-resilient. The authors propose to increase the number of shared secrets to achieve k-resilience, which affects the efficiency and complexity accordingly. A disadvantage is that these shared secrets are constant, rendering the masking values also constant. This makes the scheme susceptible to successful attacks, and it was shown to be insecure by Datta et al. [2] by means of its number-theoretical construction.

Wang et al. [15] proposed a privacy-preserving aggregation scheme and billing scheme that uses the homomorphic Pailler cryptosystem combined with verifiable secret sharing. Others billing schemes are found in [7, 12, 14].

Two survey papers on privacy-preserving schemes for smart meters and the smart grid are found in [4, 5].

2 PRIVACY-PRESERVING METER AGGREGATION

By prognosis estimation and obtaining overviews of electricity transported, consumed, and supplied by different suppliers through the electricity grid, power companies and grid operators settle production costs, carry out load balancing, detect electricity theft, etc. In this context, realtime monitoring of *individual* smart meters may not explicitly be of interest, but rather collective monitoring of consumers clustered according to their distribution in the grid structure. Privacy-preserving computations that aggregate consumption values of clusters of consumers could with advantage be used to provide privacy to the individual consumers.

In this section, we propose two privacy-preserving computation (PPC) schemes that provide privacy-preserving aggregation of consumption values for groups of smart meters. Privacy-preserving computation, also known as secure multi-party computation, refers to the general problem where a number of parties jointly compute a function in such a way that their individual input values are not disclosed to the other parties. An essential property about PPC is that such protocols must prevent that private inputs can be deduced from the messages that are sent during the execution of the protocol.

It could be noted that in the pertaining context of smart meters, only the centralized head-end system (HES) is intended to sum the reported consumption values, while each participant would compute the value of the given function in a general distributed PPC setting.

2.1 Threat model and privacy properties

The overall privacy goal is to preserve the confidentiality of individual meter consumption values, and to prevent disclosure of individual consumption values to the HES and others, while at the same time allowing computation of sums for predefined groups of smart meters.

An *honest-but-curious* adversary can be a legitimate user or a coalition of k collaborating users that do not deviate from the defined protocol, but will attempt to learn all possible information from legitimately received messages. Such coalitions could share their secret cryptographic data such keys and nonces to learn something beyond their existing knowledge.

This assumption is equivalent with an external adversary that is able to compromise k smart meters, and by such obtain the cryptographic secrets stored in those smart meters (and their consumption values). In practise, this adversary could be malware or a virus.

An honest-but-curious adversary has access to all exchanged protocol messages, which is a reasonable assumption at least considering the HES, and less than k keys:

- k-resiliency. Let S_k denote a set of associated smart meters. If less than k smart meters $\hat{S}_k \subset S_k$ of that group are compromised, privacy is preserved for the non-compromised meters $S_k \backslash \hat{S}_k$ of that group.

In other words, the k-resiliency privacy property indicates the number of meters that must be compromised (whose cryptographic secrets are obtained by the adversary) in order to compromise the privacy (i.e., obtain the consumption values) of the remaining non-compromised meters of that group, and where all exchanged messages are available. Note that the adversary is passive and does not modify messages nor keys.

The value k gives a quantitative indication of privacy in regard of multiple compromised smart meters of that group. In practise, the main concern of users is nevertheless to preserve their privacy towards the HES, which of course, is a much weaker adversary than an adversary able to compromise multiple targets.

An important thing to note is that the proposed privacy-preserving schemes do not provide explicit *security measures* in the sense of integrity, confidentiality, and entity authentication of the exchanged protocol messages. Such security measures are trivially provided by using standard cryptographic techniques.

2.2 δ_s-resilient privacy-preserving meter aggregation (PPMA$_{\delta_s}$)

PPMA facilitates periodical privacy-preserving aggregation or summation of consumption values from groups of smart meters. Each smart meter is associated to a group S_k of smart meters. The head-end system (HES) is only able to obtain the summed electricity consumption of S_k for each time interval l.

This scheme has the privacy property of δ_s-resilience, meaning that an adversary needs to compromise about $\frac{1}{\delta_s} \approx 41$ % of the smart meters in S_k, in order to disclose individual consumption values of the remaining meters, where δ_s is the so-called silver ratio. See Section 2.3.

The PPMA$_{\delta_s}$ scheme consists of the following four phases:

(1) Parameter setup. The system requires a large prime p, where $q = \frac{p-1}{2}$ is also a large prime. Select a primitive root (i.e., a generator) α to modulo p, so that the congruences $\alpha^j \equiv a \pmod p$ produce a cyclic group of residues $a \in \{1 \dots p-1\}$ for the integers $j \in \{1 \dots p-1\}$. Also, let v be a low integer that is a primitive root to modulo q.

(2) Installation. Each SM_i is represented by a Diffie-Hellman (DH) type long-term public key pair (x_i, y_i), where the private key x_i is randomly selected randomly in $\mathbb{Z}_p$, and $y_i = \alpha^{x_i} \bmod p$ is the corresponding public key.
Each $SM_i \in S_k$ is installed with the public key y_j, $i \neq j$, of each meter $SM_j \in S_k$. Due to the long-term keys, any pair of smart meters $(SM_i, SM_j \in S_k)$, share a unique static DH-secret
$$k_{i,j,0} = y_j^{x_i} = k_{j,i,0} = y_i^{x_j} = \alpha^{x_i x_j} \pmod p \quad (1)$$
that constitute initial values of the system. Hence, each smart meter manages $s-1$ DH-secrets, where $s = |S_k|$ is the group size.

(3) Privacy-preserving consumption reporting. At each time interval l, each $SM_i \in S_k$ "increments" each pairwise shared DH-value $(k_{i,j,l} \mid i, j \in S_k, i \neq j)$ according to the modular exponentiation
$$k_{i,j,l} = k_{i,j,l-1}^v \bmod p \quad (2)$$
and computes a masking value
$$m_{i,l} = \sum_{\substack{j \in S_k \\ i \neq j}} (-1)^{(j<i)} k_{i,j,l} = \sum_{\substack{j \in S_k \\ i \neq j}} (-1)^{(j<i)} k_{i,j,l-1}^v \quad (3)$$
$SM_i \in S_k$ computes and sends the masked consumption value
$$d_{i,l} = c_{i,l} + m_{i,l} \bmod p \quad (4)$$
to the HES. Security measures such as encryption is outside the scope of this paper, but should be used to ensure necessary communication security.

(4) Aggregation computation. The HES computes the aggregated consumption value c_l for all $SM_i \in S_k$ by summing
$$c_l = \sum_{j \in S_k} d_{j,l} = \sum_{j \in S_k} c_{j,l} \bmod p \quad (5)$$
which cancels out all masking values $(m_{j,l} \mid j \in S_k)$.

Performance. For each time interval, each smart must carry out $s-1$ low-exponent modular exponentiations.

2.3 Security analysis (PPMA$_{\delta_s}$)

Theorem 2.1. *δ_s-resiliency. If less than $\frac{1}{\delta_s}$ of the smart meters are compromised, it is computationally infeasible to obtain the consumption values of the non-compromised meters.*

Proof. Each smart meter $SM_i \in S_k$ is installed with the public key y_j, $i \neq j$, of each meter $SM_j \in S_k$. In conjunction with the private key $(x_i \mid SM_i \in S_k)$, the public keys $(y_j \mid SM_j \in S_k)$, $i \neq j$, constitute a unique static Diffie Hellman-secret $k_{i,j,0} = y_j^{x_i}$ (Eq. 1), which is shared by each pair of smart meters $(SM_i, SM_j \in S_k)$. Due to the Computational Diffie-Hellman problem, it is computationally infeasible to compute $k_{i,j,0}$ given the corresponding public keys (y_i, y_j).

Since each pair of smart meters in S_k shares a unique DH-secret, there are $\gamma = \binom{s}{2} = \frac{s(s-1)}{2}$ DH-secrets, which is the same as the number of ways to select two meters from that group. Any given meter computes the masking value $m_{i,l}$ based on its $s-1$ shared DH-secrets according to Eq. 2. The confidentiality of the masking values depend on the secrecy of the pertaining DH-secrets.

The masking values and the DH-secrets constitute a linear equation system S of γ unknowns and $s = |S_k|$ equations. If a smart meter is compromised by an adversary, then $s-1$ DH secrets are disclosed to that adversary. Since two meters share one DH value, s' compromised meters result in $\gamma' = \sum_{j=1}^{s'}(s-j) = s's - \frac{s'(s'+1)}{2}$ disclosed DH values, where $0 < s' < s$. This reduces S to $s - s'$ equations consisting of $\gamma - \gamma'$ unknowns. The equation system S is solvable if the number of unknowns is less than or equal to the reduced number of equations, i.e., $\gamma - \gamma' \leq s - s'$, which is
$$\gamma - \gamma' = \frac{s(s-1)}{2} - s's - \frac{s'(s'+1)}{2} \leq s - s' \quad (6)$$
which corresponds to the inequality
$$0 \leq 3s - s^2 + 2ss' + s'^2 - s' \quad (7)$$

Table 1: δ_s-resilence

s	s'	$\frac{s}{s'} \approx \delta_s$
20	8	2.500000
40	16	2.500000
60	25	2.400000
80	33	2.424242
100	41	2.439024
120	49	2.448980
140	58	2.413793
160	66	2.424242
180	74	2.432432
200	83	2.409639
300	124	2.419355
400	165	2.424242
500	207	2.415459
1000	414	2.415459
5000	2071	2.414293
10000	4142	2.414293

Table 1 lists the minimum number of compromised meters s' that are required for the inequality in Eq. 7 to be true. It also shows that the ratio $\frac{s}{s'}$ converges towards the *silver ratio*[1] $\delta_s = 1 + \sqrt{2}$.

This can be shown algebraically by simplifying Eq. 7 by removing the less significant first order terms $3s - s'$. Multiplying the remaining terms by $\frac{1}{ss'}$ yields the quadratic equation

$$\frac{s}{s'} + 2 + \frac{s'}{s} = x - 2 - \frac{1}{x} = 0$$

where $x = \frac{s}{s'}$. Multiplying by x gives the quadratic equation $x^2 - x - 1 = 0$ with solution $1 + \sqrt{2}$.

Since the equation system S is underdefined for $s' < \frac{s}{\delta_s}$, it has infinitely many solutions, and cannot be solved. Hence, Theorem 2.1 is preserved. □

Note that the initial $k_{i,j,0}$ is a long-term shared secret DH value, whereof the secret $k_{i,j,l}$, $l > 0$, is computed deterministically, without supplying additional randomness (Eq. 2). The secrecy of $k_{i,j,l}$ for any l is given by the secrecy of $k_{i,j,l'}$, $l \neq l'$.

Next is an example of an equation system that corresponds to $s = 4$ smart meters represented by 4 masking values and $\gamma = \binom{4}{2} = 6$ DH-secrets. This number is unrealistically low, but is included for the sake of illustration.

$$\begin{bmatrix} -1 & -1 & -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 & -1 & 0 \\ 0 & 1 & 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} k_{1,2} \\ k_{1,3} \\ k_{1,4} \\ k_{2,3} \\ k_{2,4} \\ k_{3,4} \end{bmatrix} = \begin{bmatrix} m_{1,l}^{S_k} \\ m_{2,l}^{S_k} \\ m_{3,l}^{S_k} \\ m_{4,l}^{S_k} \end{bmatrix} \tag{8}$$

Since the equation system is underdefined, it is not solvable as such. If for instance smart meter 1 is compromised, then the adversary would possess the three DH-secrets $k_{1,2}$, $k_{1,3}$, and $k_{1,4}$. Assuming that all masking values are correctly guessed, then the equation system is reduced to the solvable system:

$$\begin{bmatrix} -1 & -1 & 0 \\ 1 & 0 & -1 \\ 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} k_{2,3} \\ k_{2,4} \\ k_{3,4} \end{bmatrix} = \begin{bmatrix} m_{2,l}^{S_k} - k_{1,2} \\ m_{3,l}^{S_k} - k_{1,3} \\ m_{4,l}^{S_k} - k_{1,4} \end{bmatrix} \tag{9}$$

This agrees with Eq. 7, which is true for $s = 4$ and $s' = 1$.

2.4 $(s-1)$-resilient privacy-preserving meter aggregation (PPMA$_{s-1}$)

In this section, we present a multiplicative variant of the addition-oriented PPMA-δ_s presented in the previous section. It is multiplicative in the sense that the sum operation is achieved by multiplication through homomorphisms.

This scheme has the privacy property of being $(s-1)$-resilient, where an adversary need to compromise all but one associated smart meters in order to disclose individual consumption values of the remaining non-compromised meter.

The PPMA$_{s-1}$ scheme is as follows:

(1) Parameter setup. Select a large prime p, primitive root α to p^2, and a small prime v.
(2) Installation. This phase is the same as in the PPMA$_{\delta_s}$ scheme, except that the public keys y_j are computed modulo $\phi(p^2) = p(p-1)$.
(3) Privacy-preserving consumption reporting. For each time interval l, each $SM_i \in S_k$ "increments" the shared DH-secrets as $k_{i,j,l} = k_{i,j,l-1}^{v} \bmod \phi(p^2)$.
The multiplicative masking factor $m_{i,l}^*$ is computed as

$$m_{i,l}^* = \alpha^{m_{i,l}} = \prod_{\substack{j \in S_k \\ i \neq j}} \alpha^{(-1)^{(j<i)} k_{i,j,l}} \bmod p^2 \tag{10}$$

where the secret exponent $m_{i,l}$ is in agreement with Eq. 3. $SM_i \in S_k$ computes the masked consumption value

$$d_{i,l}^* = (1 + c_{i,l}p) m_{i,l}^* \bmod p^2 \tag{11}$$

(4) Aggregation computation. The HES multiplies

$$c_l' = \prod_{j \in S_k} d_{j,l}^* \bmod p^2 \tag{12}$$

and lastly obtains the total consumption $c_l = \frac{c_l' - 1}{p}$ for the group S_k.

The multiplications in Eq. 12 cause the multiplicative masking factors $m_{i,l}^*$ of $d_{i,l}^*$ to cancel out. Having the masking factors cancelled out leaves the following expansion:

$$\begin{aligned} c_l' &= \prod_{j \in S_k} (1 + pc_{j,l}) \bmod p^2 \\ &= (1 + pc_{i,l}) \cdots (1 + pc_{j,l}) \bmod p^2 \\ &= 1 + pc_{i,l} + pc_{j,l} + \ldots + p^2 c_{i,l} c_{j,l} + \ldots \bmod p^2 \\ &= 1 + p(c_{i,l} + \ldots + c_{j,l}) \bmod p^2 \\ &= 1 + p \sum_{j \in S_k} c_{j,l} = 1 + pc_l \bmod p^2 \end{aligned} \tag{13}$$

[1] https://en.wikipedia.org/wiki/Silver_ratio

where the terms containing the factor p^2 are cancelled out. Hence, this operation has a homomorphic property since the multiplication conforms to summing $c_{j,l}$.

2.5 Security analysis (PPMA$_{s-1}$)

The privacy goal is to preserve the confidentiality of each consumption value, whose privacy is preserved as long as the secrecy of the pertaining masking factor. In this section, we prove that all but one smart meters in a group need to be compromised in order to obtain consumption values from individual smart meters.

Theorem 2.2. *($s-1$)-resiliency. If less than ($s-1$) of the smart meters are compromised, it is computationally infeasible to obtain the consumption values of the non-compromised meters.*

Proof. The confidentiality of a masked consumption value depends on the secrecy of the pertaining masking factor $m^*_{i,l}$. Since the DH-secrets are shared pairwise, there are $\binom{s}{2} = \frac{s(s-1)}{2}$ DH-secrets. Any given meter computes the masking factor $m^*_{i,l}$ based on its $s-1$ shared DH-secrets according to Eq. 10. In this computation, the sum of the DH-secrets constitute the secret exponent $m_{i,l}$ of $m^*_{i,l}$. The confidentiality of the masking factors depend on the secrecy of the pertaining DH-secrets, which is preserved in agreement with the Computational Diffie-Hellman problem.

Let S_k denote a set of associated smart meters, whereof $\hat{S}_k \subset S_k$ are compromised. If an adversary compromises a set of $s-2$ smart meters $\hat{S}_k \subset S_k$, then the remaining DH-secret $k_{a,b,l}$ shared by the non-compromised meters $SM_a, SM_b \in (S_k \backslash \hat{S}_k)$ is still unknown to the adversary. Therefore, the pertaining exponent $m_{i,l}$ remains unknown to the adversary, which preserves the secrecy of the masking factor $m^*_{i,l}$. The confidentiality of the appurtenant consumption value $c_{i,l}$ masked in $d^*_{i,l}$ (Eq. 11) is thus preserved. Therefore, the PPMA$_{s-1}$ scheme is ($s-1$)-resilient, and Theorem 2.2 is preserved. □

3 PRIVACY-PRESERVING METER BILLING

In a dynamic price rate regime, power companies (PC) are able to charge each consumer according to its consumption ($\mathbf{c}$) and the tariff rate vector ($\mathbf{r}$) for a given period t (e.g., a month). The charged billing value b is the dot product $b = \mathbf{c} \cdot \mathbf{r}$.

Most smart meters produced today have bidirectional communication capabilities allowing them to receive, for instance, tariff data from the PC. A straight-forward way to preserve the privacy of the consumers, that is, to hide the consumption profile ($\mathbf{c}$) from the PC and others, would be that the PC periodically transmits tariff information to each smart meter, which computes and transmits b to the PC at the end of each period t.

From the perspective of the PC, this may be an undesired restriction for the reasons addressed in Section 2. Moreover, the PC may require means to verify the correctness of b.

In this section, we present a privacy-preserving smart meter billing (PPMB$_{s-1}$) scheme that provides the billing value b_i for each smart meter $SM_i \in S_k$ for a given time period t. The tariff vectors may therefore be distinct for two smart meters.

3.1 ($s-1$)-resilient privacy-preserving meter billing (PPMB$_{s-1}$)

The PPMB$_{s-1}$ scheme in this section is an extension of the multiplicative privacy-preserving meter aggregation (PPMA$_{s-1}$) scheme in Section 2.4 that combined produces privacy-preserving aggregation of consumption values, and privacy-preserving billing for each $SM_i \in S_k$ at the end of the billing period t.

An important property of the PPMB$_{s-1}$ scheme is *verifiability*. The HES must be able to verify that the computed billing values are correct.

The privacy goal is to prevent deduction of individual meter values in agreement with the PPMA$_{s-1}$ scheme, and to preserve the confidentiality of the billing value with regard to others than the HES. Note that the privacy-preserving scheme does not provide security in the sense of integrity, confidentiality, and entity authentication, but this is trivially provided by using standard cryptographic techniques.

Since the privacy preserving billing scheme is an extension of PPMA$_{s-1}$. The steps parameter setup, installation, and the privacy-preserving consumption reporting steps presented in Section 2.4 precede the privacy-preserving billing computation shown next:

(1) By the end of each billing period t, where $1 \leq l \leq t$, the HES transmits the tariff rate vector $\mathbf{r}_i$ pertaining to each SM_i.
(2) Each $SM_i \in S_k$ computes and transmits to HES the verification value

$$e_i = \prod_{l=1}^{t} (m^*_{i,l})^{r_{i,l}} = (\alpha^{k_{i,l}})^{r_{i,l}} \bmod p^2 \tag{14}$$

and the billing value $b'_i = \mathbf{c}_i \cdot \mathbf{r}_i$. Note that only $SM_i \in S_k$ can compute e_i since it is the only entity that knows the secret masking factors $m^*_{i,l}$.
(3) The HES computes

$$\begin{aligned} f_i &= \prod_{l=1}^{t} (d^*_{i,l})^{r_{i,l}} \bmod p^2 \\ &= \prod_{l=1}^{t} \left((1 + c_{i,l}p) m^*_{i,l}\right)^{r_{i,l}} \bmod p^2 \\ &= \prod_{l=1}^{t} (1 + c_{i,l}p)^{r_{i,l}} \alpha^{k_{i,l} r_{i,l}} \bmod p^2 \\ &= \prod_{l=1}^{t} (1 + c_{i,l} r_{i,l} p) \prod_{l=1}^{t} \alpha^{k_{i,l} r_{i,l}} \bmod p^2 \\ &= (1 + p \sum_{l=1}^{t} c_{i,l} r_{i,l}) e_i \bmod p^2 \\ &= (1 + p b_i) e_i \bmod p^2 \end{aligned} \tag{15}$$

The HES then computes the billing value

$$b_i = \frac{\frac{f_i}{e_i} - 1}{p} = \frac{\frac{(1+b_i p)e_i}{e_i} - 1}{p} = \frac{1 + b_i p - 1}{p}$$

Finally, the HES verifies $b'_i \stackrel{?}{=} b_i$. Since the privacy goal is same as for the PPMA$_{s-1}$ scheme, the same analysis applies.

Since the secret masking factors $m^*_{i,l}$ cannot be deduced from the verification value e_i and the masked consumption values $d^*_{i,l}$, the verification proves that $SM_i \in S_k$ is the legitimate originator of e_i.

If less than k smart meters $\hat{S}_k \subset S_k$ of that group are compromised, the confidentiality of the billing value is preserved for the non-compromised meters $S_k \backslash \hat{S}_k$ of that group although $\mathbf{r}_i$ is known to the adversary.

3.2 Correctness

Notice in Eq. 15 that $(1 + c_{i,l}p)^{r_{i,l}} \equiv 1 + c_{i,l}r_{i,l}p \pmod{p^2}$. This is due to the expansion of the binomial theorem:

$$\begin{aligned}(1 + c_{i,l}p)^{r_{i,l}} &= \prod_{j=0}^{r_{i,l}} \binom{r_{i,l}}{k} 1^{r_{i,l}-j}(c_{i,l}p)^j \bmod p^2 \\ &= 1 + \binom{r_{i,l}}{1} c_{i,l}p + \binom{r_{i,l}}{2} c^2_{i,l}p^2 + \ldots \bmod p^2 \\ &= 1 + r_{i,l}c_{i,l}p \bmod p^2\end{aligned} \tag{16}$$

In Eq. 15, the correctness of the products $\prod_{l=1}^{t}(1+c_{i,l}r_{i,l}p) \bmod p^2$ is in agreement with Eq. 13.

4 CONCLUSION

The awareness and attention for privacy is increasing as our society is becoming more and more digitalized. By the advent of smart meters, a number of privacy-preserving smart meter schemes have been proposed the recent years, where most provide privacy-preserving aggregation of consumption values from groups of smart meters, while privacy-preserving billing computation has only been addressed in a less degree. Due to that smart meters communicate by wireless mesh networks, low transmission overhead is of high concern to reduce the amount of communication.

In this paper, we have proposed three communication-efficient privacy-preserving schemes that provide consumption aggregation and billing computation. Two privacy-preserving aggregation schemes are presented, whereof the second provides $(s-1)$-adversarial resilience. Thus, an adversary needs to compromise all but one associated smart meters in order to disclose individual consumption values of the remaining non-compromised meter.

5 ACKNOWLEDGEMENTS

This work was partially supported by the project IoTSec – Security in IoT for Smart Grids, with number 248113/O70 part of the IKTPLUSS program funded by the Norwegian Research Council.

REFERENCES

[1] Mike Burmester and Yvo Desmedt. Efficient and secure conference-key distribution. In *Security Protocols, International Workshop, Cambridge, United Kingdom, April 10-12, 1996, Proceedings*, pages 119–129, 1996.

[2] A. Datta and M. Joye. Cryptanalysis of a privacy-preserving aggregation protocol. *IEEE Transactions on Dependable and Secure Computing*, PP(99):1–1, 2016.

[3] Zekeriya Erkin and Gene Tsudik. *Private Computation of Spatial and Temporal Power Consumption with Smart Meters*, pages 561–577. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.

[4] Mohamed Amine Ferrag, Leandros A. Maglaras, Helge Janicke, and Jianmin Jiang. A survey on privacy-preserving schemes for smart grid communications. *CoRR*, abs/1611.07722, 2016.

[5] S. Finster and I. Baumgart. Privacy-aware smart metering: A survey. *IEEE Communications Surveys Tutorials*, 16(3):1732–1745, Third 2014.

[6] Flavio D. Garcia and Bart Jacobs. *Privacy-Friendly Energy-Metering via Homomorphic Encryption*, pages 226–238. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.

[7] Marek Jawurek, Martin Johns, and Florian Kerschbaum. Plug-in privacy for smart metering billing. In *Proceedings of the 11th International Conference on Privacy Enhancing Technologies*, PETS'11, pages 192–210, Berlin, Heidelberg, 2011. Springer-Verlag.

[8] Marc Joye and Benoît Libert. *A Scalable Scheme for Privacy-Preserving Aggregation of Time-Series Data*, pages 111–125. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[9] T. Jung, X. Y. Li, and M. Wan. Collusion-tolerable privacy-preserving sum and product calculation without secure channel. *IEEE Transactions on Dependable and Secure Computing*, 12(1):45–57, Jan 2015.

[10] Tobias Klenze. Privacy strategies in smart metering. 2014.

[11] Iraklis Leontiadis, Kaoutar Elkhiyaoui, and Refik Molva. *Private and Dynamic Time-Series Data Aggregation with Trust Relaxation*, pages 305–320. Springer International Publishing, Cham, 2014.

[12] Kazuma Ohara, Yusuke Sakai, Fumiaki Yoshida, Mitsugu Iwamoto, and Kazuo Ohta. Privacy-preserving smart metering with verifiability for both billing and energy management. In *Proceedings of the 2Nd ACM Workshop on ASIA Public-key Cryptography*, ASIAPKC '14, pages 23–32, New York, NY, USA, 2014. ACM.

[13] Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding*, pages 223–238, 1999.

[14] Alfredo Rial and George Danezis. Privacy-preserving smart metering. In *Proceedings of the 10th Annual ACM Workshop on Privacy in the Electronic Society*, WPES '11, pages 49–60, New York, NY, USA, 2011. ACM.

[15] Xiao-Fen Wang, Yi Mu, and Rong-Mao Chen. An efficient privacy-preserving aggregation and billing protocol for smart grid. *Sec. and Commun. Netw.*, 9(17):4536–4547, November 2016.