An Efficient Privacy Preserving Scheme of High Frequency Reports for Secure Smart Grid Communications

Samaneh Hajy Mahdizadeh Zargar
Dept. Computer Engineering, Mashhad Branch,
Islamic Azad University
Mashhad, Iran
smahdizadeh@wali.um.ac.ir

Mohammad.H Yaghmaee
Dept. Computer Engineering, Mashhad Branch,
Islamic Azad University
Mashhad, Iran
yaghmaee@ieee.org

Abstract—**Smart grid is a new approach that significantly increases the efficiency of the entire electrical delivery system. The smart grid uses information technologies to improve how electricity travels from power plants to consumers, Allows consumers to interact with the grid and Integrates new and improved technologies into the operation of the grid. These techniques lead to some threats for the privacy of users. Since smart grid networks prepare detailed information and manage them to achieve a reliable network, such management might reveal users personal habits and behavior. The smart grid increases automation, continuity and coordination between consumers, suppliers and transmission network in long distance or local distribution networks. The development of a schema which is able to both satisfy requirements of the smart grid and guarantees the security of users has became a vast researchable area which is required a serious attention of the smart grid researchers and developers. The moving to a smart gird will depend to Meeting this challenge.**

We provide, via group signature, and efficient schema in order to preserve the users' privacy. In the proposed schema SGGS, the data with high frequency are collected through the smart meters which have less computational overload, higher speed and so much less communication overhead than the previous schemas. In the schema SGGS, the group signature is used to make pseudonym and temporary short signature. The data confidentiality will be guaranteed through the random confidential keys, also the requirements, limitations and properties of the smart grid will be considered. In this case while the schema SGGS in having a high level of security, the cryptography overhead which is used to send the confidential data is much less than the previous schemas. Also we propose one batch verification schemes which double the efficiency of our schema

Keywords; Smart Grid; Privacy preserving; Group signature; batch verification.

I. INTRODUCTION

The August 2003 electrical blackout in North America affected over 100 power plants and paralyzed the lives of tens of millions of people. Investigations revealed that the failure was due to load imbalance and lack of effective real-time diagnosis. Recently, the concept of smart grid has emerged and has been recognized as the next generation of power grids [6]. Smart grid is a new approach that significantly increases the efficiency of the entire electrical delivery system and Not only does it increase reliability, but also reduces energy consumption in the delivery process and reduce greenhouse gas emissions. The smart grid combines the traditional grid and information and control technologies. It allows decentralized two-way transmission, reliability and efficiency driven response, and aims to provide improved reliability and security. Smart meters are important components of a smart grid. A smart meter records high frequency power consumption. And with its report, the control center collects real-time information from the grid. Because of high complexity and integration, cyber security is a challenge in smart grids. All the data transmitted in the grid must be authenticated and secured against malicious modification. Privacy and confidentiality are primary concerns from the customers' point of view as power consumption information may reveal their physical activities. Data confidentiality can be achieved by a simple end to end encryption. To preserve user privacy, there are several proposed methods such as using aggregation gateway by homomorphic encryption techniques or data anonymization and obfuscation techniques. For example, some have described privacy as consisting of four dimensions: 1) Privacy of personal information. This is the most commonly thought-of dimension. Personal information is any information relating to an individual, who can be identified, directly or indirectly. 2) Privacy of the person. This is the right to control the integrity of one's own body. It covers such things as physical requirements, health problems, and required medical devices. 3) Privacy of personal behavior. This is the right of individuals to keep any knowledge of their activities, and their choices, from being shared with others. 4) Privacy of personal communications. This is the right to communicate without undue surveillance, monitoring, or censorship for instance, frequent meter readings may provide a detailed timeline of activities occurring inside a metered location and could also lead to knowledge about specific equipment usage or other internal home/business processes. Some failure to address privacy issues in the smart grid will not be accepted by regulators and customers.

The remainder of this paper is organized as follows. We discuss the related work in Section 2 and in Section 3, we introduce our system model. In Section 4 we recall the bilinear pairings, Paillier cryptosystem, Short signature and Short Group Signatures with Controllable Linkability as the preliminaries, then we present proposed Efficient signing and Batch Verifier for CLGS in section 5 and our SGGS scheme in Section 6, followed by performance evaluation in Section 7. Finally, we draw our conclusions in Section8.

II. RELATED WORKS

We categorize previous researches into two fields, the first group works on adopting privacy-preserving data

978-1-4799-2093-8/13/$31.00 ©2013 IEEE

aggregation techniques, and the second group focuses on data anonymization and obfuscation techniques [1].

A. Adopting privacy-preserving data aggregation techniques

Most technologies in Secure Information aggregation use homomorphic encryption, such as: [2] which describe protocols for secure communication with smart meters and for fraud detection (leakage) in a privacy-preserving manner. Using a combination of Paillier's additive homomorphic encryption and additive secret sharing, a secure and efficient power management mechanism leveraging a homomorphic data aggregation and capability-based power distribution model is proposed in [3]. And an in-network aggregation model proposed in [4] is based on homomorphic encryption. In [5] a bihomomorphic method is additively homomorphic in key and ciphertext space. In [6], an efficient and privacy-preserving aggregation scheme, named EPPA, is proposed. EPPA uses a super-increasing sequence to structure multi-dimensional data and encrypt the structured data by the homomorphic Paillier cryptosystem technique. EPPA also adopts the batch verification technique to reduce authentication cost.

B. Data anonymization and obfuscation techniques

One method for Data anonymization is to hide owner ID such as [7] that provides a 3rd party escrow mechanism for authenticated anonymous meter readings which are difficult to associate with a particular smart meter or customer. Or the idea in [8], a customer generates a set of credentials by himself and asks the control center to blindly sign them. When the customer needs to request more power later on, he presents the signed credential to the control center as proof of his identity. Some of them use obfuscation techniques by moderating the home's load signature in order to hide appliance usage information, for example using a rechargeable battery [9].

III. System model

We mainly focus on how to report energy usage data to the control center in smart grid communications without the compromising consumer's privacy. In specific, we consider smart meters in residential area as a group of users, which communicate to the local gateway (GW) connected with the smart grid control center. The GW is a powerful workshop, which mainly performs two functions: aggregation and relaying. The GW will perform process of the aggregation and relaying, and also perform some authentication operations to guarantee the data's authenticity and integrity. Each group has a group manager GM as a trusted authority for managing group members join and revocation as shown in Fig.1

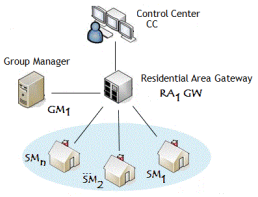

Figure 1. System model

We consider two security parameters: 1) Confidentiality and privacy preserving. 2) Authentication and Data Integrity. Since privacy preserving data aggregation techniques ensure tradeoffs between privacy and data collection requirements, we present data anonymization using group signature. Group signatures offer the expected support in terms of anonymity.

IV. Preliminaries

A. Bilinear Maps

Let $\mathbb{G}_1$, and $\mathbb{G}_2$ be multiplicative groups of prime order p and $e: \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$ be a bilinear map which satisfies the following properties: 1) Bilinear: $e(g^a, h^b) = e(g, h)^{ab}$ for all $g \in \mathbb{G}_1$, $h \in \mathbb{G}_2$ and $a, b \in \mathbb{z}_p$. 2) Non-degenerate: There exists $h \in \mathbb{G}_2$ such that $e(g, h) \neq 1$. 3) Computable: There exists an efficient algorithm to compute $e(g, h)$ for all $g \in \mathbb{G}_1$, $h \in \mathbb{G}_2$.

B. Paillier Cryptosystem

The Paillier cryptosystem, named after and invented by Pascal Paillier in 1999, is a probabilistic asymmetric algorithm for public key cryptography. The Paillier Cryptosystem is comprised of three algorithms: key generation, encryption and decryption.

Key Generation: Given the security parameter κ1, two large prime numbers p1, q1 are first chosen, where |p1| =|q1| = κ1. Then, the RSA modulus n = p1q1 and λ = lcm(p1 − 1, q1 − 1) are computed. Define a function L(u) = $\frac{u-1}{n}$, after choosing a generator $g \in \mathbb{Z}^*_{n^2}$, $\mu = (L(g^\lambda \bmod n^2))^{-1} \bmod n$ is further calculated. Then, the public key is pk = (n, g), and the corresponding private key is sk = (λ, μ).

Encryption: Given a messagem $\epsilon\, \mathbb{Z}_n$ choose a random Number $r \in \mathbb{Z}^*_n$, and the ciphertext can be calculated as $c = E(m) = g^m r^n \bmod n^2$.

Decryption: Given the ciphertext $c = \mathbb{Z}^*_{n^2}$, the corresponding message can be recovered as $m = D(c) = L(c^{\lambda \bmod n^2})\, \mu \bmod n$.

Note that, the Paillier Cryptosystem is provably secure against chosen plaintext attack, and the correctness and security can be referred to [14].

C. Short Signature

We used the short signature schema 'BBSig' for signing message [15]. The schema includes four algorithms which are BSSetup, BSJoin, BSSig, BSVfy:

BSSetUp : The master node picks random generators $g_1 \in \mathbb{G}_1$, $g_2 \in \mathbb{G}_2$ and computes $z \leftarrow e(g_1, g_2) \in \mathbb{G}_T$. Then it generates $mpk = (g_1, g_2, z)$ as master public key.

BSJoin: For given mpk, every node $i = 1, \ldots, m$ picks random number $s_i \in \mathbb{z}_p^\times$, and computes $spk_i \leftarrow g_2^{s_i} \in \mathbb{G}_2$. The public key is$spk_i$ and the secret key is s_i.

BSSig: For given master public key $mpk = (g_1, g_2, z)$, secret key s_i and message $m_i \in \mathbb{z}_p$, it outputs signature $\sigma_i \leftarrow g_1^{1/(s_i + m_i)} \in \mathbb{G}_1$.

BSVfy: For given mpk and $SPK = spk_i$ it verify signature (σ_i, m_i) using by 'small exponents test'. If $e(\sigma_i, spk_i g_2^{m_i}) = e(g_1, g_2)$ then output 1, and otherwise 0.

978-1-4799-2093-8/13/$31.00 ©2013 IEEE

D. Short Group Signatures with Controllable Linkability Linkability (CLGS)

A group signature scheme is a method that allows a member of a group to anonymously sign a message on behalf of the group. The concept was first introduced by David Chaum and Eugene van Heyst in 1991.After this a number of different Group signatures have been proposed, like [10] as the first practical and coalition-resistant group signature scheme. In [11] Boneh, Boyen, and Shacham (BBS) proposed an efficient GS scheme that yields a short signature with bilinear pairings. They also informally presented methods to achieve nonframeability and to revoke users by updating keys. In [12] Hwang et.al present a Group Signatures scheme with Controllable Linkability for Dynamic Membership and referred to CLGS, A group signature scheme supporting controllable anonymity linking [13]. A CLGS scheme consists of the following algorithms:

SetUp: For given a security parameter 1^{λ}, it proceeds as follows: It generates a tuple of groups of prime order p, $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$ and a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ It picks random $h_1 \xleftarrow{R} \mathbb{G}_2$ and $g, g_1, g_2, u \xleftarrow{R} \mathbb{G}_1$, and $\eta, \xi, \theta \xleftarrow{R} \mathbb{Z}_p^*$. It then computes $w = u^{\eta}$, $d = u^{\xi}$, $U = h_1^{\xi}$ and $h_\theta = h_1^{\theta}$. Let $H : \{0,1\}^* \rightarrow \mathbb{Z}_p^*$ be a cryptographic hash function. A group public key is:

$$gpk = (\boldsymbol{e}, g, h_1, h_\theta, \boldsymbol{H}, g_1, g_2, u, w, d) \quad (1)$$

And the master issuing key, $mik = \theta$, the master opening key, $mok = (\eta, \xi)$, and the master linking key, $mlk = U$. The group public key, more concretely the parameters g_1, g_2, u, w, d will be updated per revocation.

UserJoin: Two algorithms, UserJoin (run by a joining user) and Issue (run by the Issuer) interactively performs a protocol to generate a user signing key:

$$USK[i] = \left(x_i, y_i, z_i, A_i = (g_1 g_2^{-y_i} w^{-z_i})^{\frac{1}{\theta + x_i}}\right) \quad (2)$$

Here, $z_i \in \mathbb{Z}_p^*$ is privately selected by UserJoin and $x_i, y_i \in \mathbb{Z}_p^*$ are selected by Issue. Refer to [13].

GSig: For given gpk, a user key $usk[i] = (x, y, z, A)$ corresponding to gpk, and a message M, proceeds as follows: It picks $\alpha \xleftarrow{R} \mathbb{Z}_p^*$ and computes $\gamma = x\alpha - z \bmod p$, $D_1 \leftarrow u^{\alpha}$, $D_2 \leftarrow Aw^{\alpha}$, and $D_3 \leftarrow g^y d^{\alpha}$. It also picks $r_\alpha, r_\gamma, r_x, r_y \xleftarrow{R} \mathbb{Z}_p^*$ and computes:

$$R_1 \leftarrow u^{r_\alpha} \quad , \quad R_3 \leftarrow g^{r_y} d^{r_\alpha} \quad (3)$$

$$R_2 \leftarrow e(D_2, h_1)^{r_x}\, e(w, h_\theta)^{-r_\alpha}\, e(w, h_1)^{-r_\gamma}\, e(g_2, h_1)^{r_y}$$

It then computes $c = H(M, D_1, D_2, D_3, R_1, R_2, R_3)$ and $s_\alpha \leftarrow r_\alpha + c\alpha$, $s_x \leftarrow r_x + cx$, $s_\gamma \leftarrow r_\gamma + c\gamma$ and $s_y \leftarrow r_y + cy \bmod p$. Finally, output a signature:

$$\sigma = (D_1, D_2, D_3, c, S_\alpha, S_x, S_\gamma, S_y) \quad (4)$$

GVfy: For given gpk, (M, σ), it computes

$$R_1 \leftarrow u^{s_\alpha} D_1^{-c} \qquad R_3 \leftarrow g^{s_y} d^{s_\alpha} D_3^{-c} \quad (5)$$

$$R_2 \leftarrow e(D_2, h_1)^{s_x}\, e(w, h_\theta)^{-s_\alpha}\, e(w, h_1)^{-s_\gamma}\, e(g_2, h_1)^{s_y}\, (e(D_2, h_\theta)/e(g_1, h_1))^{c}$$

If $c = H(M, D_1, D_2, D_3, R_1, R_2, R_3)$ then output 1, and otherwise, 0.

Link: For two given pairs of messages, (M_0, σ_0) and (M_1, σ_1) , and the master linking key, $mlk = U$, it first checks if the signatures are valid. If so, it computes $B_1 \leftarrow e(D_{0,3}, h_1)/e(D_{0,1}, U)$ and, $B_2 \leftarrow e(D_{1,3}, h_1)/e(D_{1,1}, U)$. If $B_1 = B_2$ then it outputs 1 and otherwise, 0.

V. Proposed Efficient Signing and Batch Verifier for CLGS

Since the pairings (w, h_θ) , $e(w, h_1)$, $e(g_1, h_1)$ and $e(g_2, h_1)$ can be pre computed and included in the group public key, signing requires no pairing computation [12], and only one pairing for verification. Let $E_1 = e(w, h_\theta)$, $E_2 = e(w, h_1)$, $E_3 = e(g_1, h_1)$ and $E_4 = e(g_2, h_1)$, be pre computed in group public key, so :

$$gpk = (e, g, h_1, h_\theta, H, g_1, g_2, u, w, d, E_1, E_2, E_3, E_4) \quad (6)$$

Since $e(D_2, h_1)$ can be computed by $e(A, h_1)e(w, h_1)^{\alpha}$ and consider $E_5 = e(A, h_1)$ as one time pairing computation. In GSig, computing R_2 changes to:

$$R_2 \leftarrow E_1^{-r_\alpha} E_2^{-\alpha r_\gamma} E_4^{r_y} E_5^{r_x} \quad (7)$$

In GVfy, A verifier can derive R_2 by merging $e(D_2, h_1)^{s_x}$ and $e(D_2, h_\theta)^{c}$ and evaluating one pairing:

$$R_2 \leftarrow e(D_2, h_1^{s_x} h_\theta^{c}) E_1^{-s_\alpha} E_2^{-s_\gamma} E_3^{c} E_4^{s_y} \quad (8)$$

Pairing based cryptography produce a number of ”short" signatures which provide high security. Unfortunately, verifying these signatures is computationally intensive due to the expensive pairing operation. In an attempt to achieve “short and fast" signatures, we adopts the batch verification technique to reduce verification cost. In GVfy, Computing R2 is the most expensive section. At first glance it is not clear that this can be batched, because each R2 is hashed. The signature and the verification algorithm can be modified at the expense of increasing the signature size by one element. To this end we add R2, Let $\sigma = (D_1, D_2, D_3, R_2, c, S_\alpha, S_x, S_\gamma, S_y)$ be the modified signature, together with:

MoGVfy: For the given group public key $gpk = (e, g, h_1, h_\theta, H, g_1, g_2, u, w, d)$, a message M and a group modified signature (M, σ) ,it computes: the values $R_1 \leftarrow u^{s_\alpha} D_1^{-c}$, $R_3 \leftarrow g^{s_y} d^{s_\alpha} D_3^{-c}$. Then check if

$$R_2 = e(D_2, h_1)^{s_x}\, e(w, h_\theta)^{-s_\alpha}\, e(w, h_1)^{-s_\gamma}\, e(g_2, h_1)^{s_y}\, (e(D_2, h_\theta)/e(g_1, h_1))^{c}$$

And check if $c = H(M, D_1, D_2, D_3, R_1, R_2, R_3)$ output 1, and otherwise 0. Now we define a batch verifier using ‘small exponents test’.

Batch GVfy: For the given group public key $gpk = (e, g, h_1, h_\theta, H, g_1, g_2, u, w, d, E_1, E_2, E_3, E_4)$, Let $\sigma_i = (D_{i,1}, D_{i,2}, D_{i,3}, R_{i,2}, c_i, S_{i,\alpha}, S_{i,x}, S_{i,\gamma}, S_{i,y})$ be the i'th signature on the message M_i, for each $i = 1, \ldots, l$. For each i, compute the values:

$$R_{i,1} \leftarrow u^{s_{i,\alpha}} D_{i,1}^{-c_i} \ , \ R_{i,3} \leftarrow g^{s_{i,y}} d^{s_{i,\alpha}} D_{i,3}^{-c_i}$$

Then check if $c_i = H(M_i, D_{i,1}, D_{i,2}, D_{i,3}, R_{i,1}, R_{i,2}, R_{i,3})$. Then check the following double pairing based equation:

$$\prod_{i=1}^{l} R_{i,2}^{\delta_i} \leftarrow^{?} e\left(\prod_{i=1}^{l} D_{i,2}^{s_{i,x}\delta_i}, h_1\right) . e\left(\prod_{i=1}^{l} D_{i,2}^{c_i\delta_i}, h_\theta\right) . \prod_{i=1}^{l} (E_1^{-s_{i,\alpha}} E_2^{-s_{i,\gamma}} E_3^{c_i} E_4^{s_{i,y}})^{\delta_i} \quad (9)$$

Where $(\delta_1, \ldots, \delta_l)$ is a random vector from $\mathbb{Z}_p$. The accuracy of the above statements is proved by ‘small

978-1-4799-2093-8/13/$31.00 ©2013 IEEE

exponents test', which cannot be discussed about according to the limited room.

VI. PROPOSED PRIVACY PRESERVING SCHEME OF HIGH FREQUENCY REPORTS IN THE SMART GRID - SGGS

One of the concerns of the smart grid development is the privacy policy in the time of collecting high frequency data on the level of distribution grid. This grid requires safe, secure and quick data collection. To reach this goal, we have proposed a schema which includes a combination of obfuscation techniques, cryptography and group signature. In this schema the required process for producing the secure reports and assuring about the verity of the data has been decreased. Also there are a lot of sidelong advantages in this schema. Some of those advantages are the possibility of complete control over the grid along with preserving the privacy, the possibility of data mining out of those which are collected from the grid, recognizing the hazardous users and theft in the grid and recognizing meters which are out of service or manipulated. We will discuss about the description of the proposed schema, the evaluation of the schema efficiency and its comparison to the current schemas.

A. Setup Phase

Setup phase includes several parts such as setup the local gateway (the local portal of one area), setup the group and setup the members (the smart meter). As you read in the section of the system schema, we need a trusted manager for every group. This manager does not belong to the distribution grid. One manager can be assigned for several groups. We assume that there is a trusted operation authority (OA) in the distribution grid; therefore controlling of all arrivals and departures is in their hand.

On the setup phase, first of all OA produces the group gpk's public key and secret keys mik, mok and mlk. To do that, he runs the setup algorithm that is derived from the developed schema of the group signature CLGS. The identity of every GW is confirmed by OA. Every GW makes a pair of private and general key to sign its produced messages by running the algorithm GWSetup:

GWSetup: For given random values $g_1 \in \mathbb{G}_1$, $h_1 \in \mathbb{G}_2$ in Group public key, it picks random number $x_j, y_j \overset{R}{\leftarrow} \mathbb{z}_p^*$ and computes $u_i \leftarrow h_1^{x_j} \in \mathbb{G}_2$, $v_j \leftarrow h_1^{y_j} \in \mathbb{G}_2$. Then it sends public key for OA and $GWsk_j = (x_j, y_j)$ as his private key are securely stored.

Plus every GWj makes a pair of key to receive the confidential data. To do so, we use Paillier schema of cryptography. Each manager of the groups uses KeyGen algorithm and Paillier cryptography schema to make a pair of keys which are($Ppk_j = (n_j, g_j)$, $Psk_j = (\lambda_j, \mu_j)$). Then GWpkj gives its public key (Ppkj) and its public key of its digital signature (GWpkj) to OA. Whenever a new member joins to the group j, OA gives him the public key of cryptography (GWj), so that he can send his confidential data to his local gateway. To join the group, each member uses the algorithm UserJoin which is installed on the meter to get his private key $usk_i = (x_i, y_i, z_i, A_i, C_{5,i} = e(A, h_1))$.

B. Measurement and reports of the data phase

The main objective of the provided schema is collection of the consumption amount of each meter in a specified period of time in a way that the privacy would be preserved. Also the consumers should be able to trust the smart grid and not be concerned about revealing of their daily action. To do so, each meter registers a pseudonym and a signature anonymously for itself. This meter sends its data through a pseudonym. The local gateway receives the pseudonym and the public key from smart meters and then registers them in the list of active meters. After that, the credit of each new package is considered using the registered keys in the list of active meters. They perform the following steps:

Step 1: The smart meter SM_i creates pseudonym, $PID_{i,t}$, and temporary short signature's keys using PID_SetUp algorithm as follow:

PID_SetUp: it picks random pseudonym $PID_{i,t} \overset{R}{\leftarrow} \mathbb{N}_{l_p}^*$. For given random values $g_1 \in \mathbb{G}_1$, $h_1 \in \mathbb{G}_2$ in Group public key, it picks random number $x_i \overset{R}{\leftarrow} \mathbb{z}_p^*$, and computes $u_i \leftarrow h_1^{x_i} \in \mathbb{G}_2$. The smart meter's temporary public key is $Tpk_i = (h_1, g_1, v_i, u_i)$ .The smart meter's temporary private key is $Tsk_i = x_i$ which is securely stored. The values h_1, g_1 in public key are duplicate and can be removed.

Step 2: The smart meter signs message $(PID_{i,t} || Tpk_i)$ using CLGS Group signature schema and sends $(PID\_Reg, PID_{i,t}, Tpk_{i,t}, TS, \sigma_i)$ to local gateway.

Step 3: The local gateway receives m request of PID_Reg , and batch verify them using 'Batch GVfy' algorithm. Since the signatures are anonymously under the group, the main id of smart meters is hidden from local gateway. So there are valid list of meters $LG\_REG_{j,t} = ((PID_{0,t}, Tpk_{0,t}, TS, \sigma_0), \dots, (PID_{m,t}, Tpk_{m,t}, TS, \sigma_m))$ on local gateway. Finally, the smart meter can sends power consumption, it performs following steps:

Step 1: The smart meter picks random values $RKey_{i,t} = (k_{i,1}, \dots, k_{i,n})$ which are $k_{i,j} \leftarrow \mathbb{z}_{l_e}^*$ and $nl_e < |n_j|$. It sends $RKey_{i,t}$ confidential by Paillier encryption using local gateway's $Ppk_j = (n_j, g_j)$. It picks random value $r_i \leftarrow \mathbb{z}_{n_j}^*$ and computes $c_i = g_j^m . r_i^{n_j} \bmod n_j^2$ for given message $m_i = k_{i,1} || \dots || k_{i,n}$.

Step 2: the smart meter sign $m_i = PID_{i,t} || c_i || TS$ using its temporary private key which is created in PID_Reg step. It sends $(Ran\_Keys, PID_{i,t}, c, TS, \sigma = g_1^{1/(x_i + m_i)})$ to the local gateway.

Step 3: The local gateway verify Incoming messages by BSVfy algorithm and decrypt $RKey_{i,t} = k_{i,1} || \dots || k_{i,n}$. It stores each $RKey_{i,t}$ in active smart meters list.

Therefore whenever the smart meter intends to send a piece of data to the local gateway, it uses one of the random keys to cryptograph its data. The random keys get renewed after n number of sending data. The smart meters send data at $+1, \dots, t + n$. It performs following steps:

978-1-4799-2093-8/13/$31.00 ©2013 IEEE

Step 1: The smart meter encrypt real data m_i at $t+z$, $z=1,\dots,n$ by computing $c_i = m_i + k_{i,z}$ and sends $(Rep, PID_{i,t}, c_i, TS, \sigma_i \leftarrow g_1^{1/(x_i+m_i)})$ to the local gateway.

Step 2: The local gateway verify Incoming messages by BSVfy algorithm and decrypt $m_i = c_i - k_{i,z}$. It computes $M_j = \sum_{i=1}^{m} m_i$ and send $(GW\_Rep, ID_j, M_j, TS, \sigma_j = g_1^{1/(x_j+M_j+y_j r_j)}, r_j \in \mathbb{z}_p)$ to the control center .

VII. Performance analysis

One of the usages of collecting data with high frequency in the smart grid is the possibility of data mining of the collected data. These data contain very useful information. By extracting this information, we can respond to the demands of power suppliers, governmental section, insurance companies and the providers of electrical devices. It would be very pleasant if we could access to this information with preserving the users' privacy. In our schema it is possible for the smart grid to data mining over the users' consumption amount of power in a short specified period of time without endangering their privacy. As we said before, the collected data are in somewhere unknown in the gateway. The sender of each piece of data is recognized by a pseudonym which is a random value. This pseudonym is temporary and not unique during the lifetime of a smart meter. Using the group signature, the smart meter sends its pseudonym for the local gateway, Therefore OA can use the ability of linkability (algorithm link from the schema CLGS) between the group signatures and recognizes pseudonym which belong to a smart meter. By this form of dividing, the data belonging to a smart meter would be recognized without revealing their identity.

A. Computational Complexity

In group signature, to make a signature, we do not need a bilinear mapping. As we discussed, each smart meter needs to calculate 3 exponents in $\mathbb{G}_1$, 2 multiplication-exponents in $\mathbb{G}_1$ and 1 multiplication- exponent in $\mathbb{G}_t$ with four fixed bases. The verification algorithm 'MoGVfy' needs to calculate 2 multiplication-exponents in $\mathbb{G}_1$, 1 multiplication-exponent in $\mathbb{G}_2$, 1 multiplication-exponent in $\mathbb{G}_t$ with four fixed bases. It also requires a bilinear mapping. The batch verification algorithm 'Batch GVfy' needs to calculate 4 multiplication-exponents in $\mathbb{G}_1$, 1 multiplication-exponent in $\mathbb{G}_t$ with four fixed bases and also two bilinear mappings. The short signature schema which was used in the smart meters needs 1 exponent in $\mathbb{G}_1$ to produce a signature according to BSSig algorithm. We need one multiplication-exponent in $\mathbb{G}_2$ and 1 bilinear mappings for validating short signatures according to BSVfy algorithm. The short signature schema which was used in the local gateway needs one exponent in $\mathbb{G}_1$ to produce a signature. And the validation of the produced signature which was done by the local gateway in the control center needs one exponent in $\mathbb{G}_2$ and one bilinear mapping. In Paillier cryptography schema which is used to send the random keys requires one multiplication-exponent by mod n^2. Also the local gateway needs one exponent in mod n^2 and one multiplication in mod n to decrypt the random keys it receives from the smart meter.

B. communication Overload

We assume that the actual length of the data (energy consumption amount) which in sent to the local portal is l_{ec} bits and also that in the Paillier cryptography schema, n is 1024 bits, a piece of data with the length of 1024 can be cryptographed. Number of the random keys in every dispatch can be $1024/l_{ec}$. If we assume that we maintain the energy consumption on 2 bytes number in a short period, each time the smart meter would be able to send 64 random keys to the local gateway. When we count the data dispatch overhead from the smart meter to the local gateway, we divide the content of the data by $1024/l_{ec}$. If we consider the number of 4 bytes for $|PID_{i,t}| + |TS|$, 2 bytes for l_{ec}, then the average length of the sent message from the smart meter would be 254 bits.

C. Efficiency Comparison

On this section we will talk about the efficiency comparison of the proposed schema (SGGS) to TRAD and EPPA schemes. EPPA schema has some advantages in the field of sending the multidimensional data compared to the TRAD schema. These advantages decrease the grid traffic. EPPA schema cryptographs the multidimensional data and then by using the property of homomorphic encryption collects them. In case the data are one-dimensional, the efficiency of both TRAD and EPPA would be equal. In EPPA and TRAD schemas it is not possible to access the actual data one by one due to preserving the privacy. On these two schemas only the collected data are accessible assuming the local gateway is trusted. This issue makes us miss several advantages that we were looking for over collecting the data. This problem has been solved in the proposed schema SGGS. In the proposed schema the preservation of the privacy does not subject to the collection of the data. In this schema we can use all the informative capacity that is needed in the smart grid. In addition to the stronger guarantee of the preservation of the privacy in comparison to EPPA and TRAD, On the SGGS schema the traffic of the smart grid and the computational expenses of the smart meter and the control center will be decreased. The increase of efficiency in dispatch of both one-dimensional and multidimensional data is evident. As you can see in the Fig.3, the length of data package which is sent from the smart meter to the local gateway in schema EPPA is 2308 bits regardless of data's being one-dimensional or multidimensional. In case the data are one-dimensional, the length of the data package which in sent from the smart meter to the local gateway in TRAD schema is 2308 bits. And if the data are L-dimensional, the length of each message is $2048 * L + 260$. In the proposed SGGS schema, if the data are one-dimensional, the length of each message will be 254 bits and if the data are L-dimensional, the length of each message will be $16 * l + 238$. It should be noted that the value L is limited in EPPA schema. Fig.2 indicates the three dimensional diagram of the smart grid traffic for the sent packages from the smart meter to the local portal based on dimensions of the data and number of smart meters on SGGS and EPPA. In the proposed schema the amount of the needed calculations in the smart meter has been decreased compared to EPPA and TRAD schemas because we do not need cryptography for each dispatch of the data.

978-1-4799-2093-8/13/$31.00 ©2013 IEEE

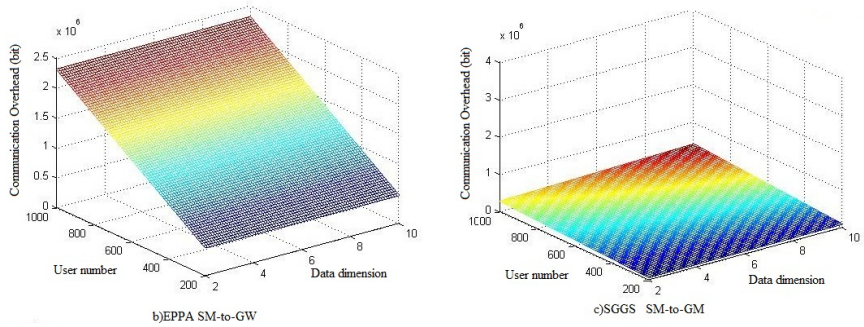

Figure 2. Communication overhead between the users (the smart meters) and the local gateway as the multidimensional data are sent

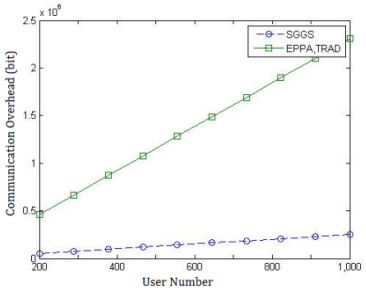

Figure 3. Communication overhead between the users (the smart meters) and the local gateway as the one-dimensional data are sent

Since the volume of the actual data in little, the produced traffic is so much less than the previous schema. According to the high number of smart meters in the grid and the connective limitation, the reduction of the amount of the produced traffic is very important.

VIII. CONCLUSION

In SGGS schema, for the first time we used the group signature in a different way. As we discussed on efficiency evaluation section, the amount of computational overhead of SGGS in the smart meters has been decreased compared to the previous schemas. We face a high volume of data in the smart grid which are sent from the smart meters. The reduction of communication overhead with the preservation of privacy parameters is very important. The produced traffic in SGGS is approximately one tenth of the same thing in EPPA; whereas both of them have the same security level. Plus, SGGS schema would be more reliable for the users, because in case of exchanging data without collecting them between the local gateway and the control center, the violation of the privacy policy would be impossible. The collected data in the smart grid contain very useful information. By extracting this information, we can respond to the demands of power suppliers, governmental section, insurance companies and the providers of electrical devices. On SGGS this kind of information is accessible with preservation of the users' privacy.

REFERENCES

[1] Hervais Simo Fhom and Kpatcha M. Bayarou ," Towards a Holistic Privacy Engineering Approach for Smart Grid Systems",2011 IEEE TrustCom,pp 234 – 24.

[2] Flavio D. Garcia ,Bart Jacobs ,"Privacy-friendly Energy-metering via Homomorphic Encryption ",2011 IEEE 6th international conference on security and trust management.

[3] Dongwon Seo , Heejo Lee Adrian Perrig," Secure and Efficient Capability-based Power Management in the Smart Grid ",2011 IEEE International Symposium on Parallel and Distributed Processing ,pp 119 – 126.

[4] F. Li, B. Luo, and P. Liu. "Secure information aggregation for smart grids using homomorphic encryption". 2010 IEEE , Smart Grid Communications (SmartGridComm) conf, pp 327 – 332.

[5] Félix Gómez Mármol Osman Ugus, " Do Not Snoop My Habits: Preserving Privacy in the Smart Grid" IEEE Communications Magazine, vol 50 pp 166 - 172 ,May 2012

[6] Rongxing Lu, Xiaohui Liang, Xu Li, "EPPA: An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Communications" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, Vol 23, pp 1621 – 1631,2012

[7] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," , in 2010 IEEE Smart Grid Communications, pp. 238 – 243.

[8] Cheung,J.C.L,Chim, T.W. , Yiu, S.M. , Hui, L.C.K. , Li, V.O.K. ,"Credential-based Privacy-preserving Power Request Scheme for Smart Grid Network" ,2011 IEEE Global Telecommunications Globecom conf, pp 1-5

[9] Georgios Kalogridis, Costas Efthymiou, Stojan Z. Denic," Privacy for Smart Meters: Towards Undetectable Appliance Load Signatures", in Proc. 2010 IEE Smart Grid Communications (SmartGridComm) conf, pp 232- 237.

[10] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, "A practical and provably secure coalition-resistant group signature scheme", Crypto 2000, vol. 1880, pp.255-270, Springer-Verlag, 2000.

[11] D. Boneh, X. Boyen and H. Shacham, "Short group signatures", Crypto 2004, vol. 3152, pp. 41-55, Springer-Verlag, 2004

[12] J.Hwang, S.Lee, B.Chung, H.Cho ,"Group signatures with controllable linkability for dynamic membership", Information Sciences ,Volume 222, 10 February 2013, pp. 761–778.

[13] C. Delerablee and D. Pointcheval, "Dynamic fully anonymous short group signatures", Vietcrypt 2006, vol. 4341, pp. 193-210, Springer, 2006.

[14] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in EUROCRYPT, 1999, pp. 223–238.

[15] Dan Boneh, Ben Lynn, and Hovav Shacham. "Short signatures from the Weil pairing". In ASIACRYPT '01, volume 2248 of LNCS, pages 514 -532, 2001.

978-1-4799-2093-8/13/$31.00 ©2013 IEEE