JOURNAL OF MECHANICS OF CONTINUA AND
MATHEMATICAL SCIENCES
www.journalimcms.org

ISSN (Online) : 2454 -7190 Vol.-15, No.-3, March (2020) pp 19-35 ISSN (Print) 0973-8975

# EXPERT SMART METERING SYSTEM USING HOMOMORPHIC ENCRYPTION WITH DOUBLE CONJUGACY PROBLEM

**V. Jalaja[1], G.S.G.N. Anjaneyulu[2]**

[1]Research Scholar, Department of Mathematics, Vellore Institute of Technology, Vellore, India.

[2]Professor, Department of Mathematics, Vellore Institute of Technology, Vellore, India.

[1]valisireddyjalaja0@gmail.com, [2]anjaneyulu.gsgn@vit.ac.in

Corresponding Author: V. Jalaja

https://doi.org/10.26782/jmcms.2020.03.00002

## Abstract

*In this article, initially we propose a new cryptosystem based on conjugacy using automorphism over non-commutative groups. We applied the proposed cryptosystem to design expert smart meters based on homomorphic encryption with double conjugacy. Smart meters will communicate mostly errorless client electricity consumption readings to suppliers. Although this provides benefits for both entities, it results in a severe loss of privacy for customers. We integrate a monitoring purpose system that preserves customer's privacy by homomorphically accumulating the consumptions of all n members of a domain. This expert smart system has an proficient linear O(n) communication cost and is proven to protect customer's privacy even in the presence of a corrupted substation and some malicious smart meters. It need not have any secure communication channels or a trusted third party(except for allotting public key certificates). The security of cryptosystem and smart metering depends on conjugacy and homomorphism. We also demonstrated that the comparison of smart meters with electronic meters by real time data.*

**Keywords:** Cryptosystem, Homomorphic Encryption, Conjugacy Problem and Smart Metering**.**

## I. Introduction

### Homomorphic Encryption

An encryption is homomorphic if it is possible to find Enc(f(a ,b)) from Enc(a) and Enc(b), where f can be +,× even without knowing the private key. In 1978 Ronald Rivest, Leonard Adleman and Michael Dertouzos proposed the idea of homomorphic encryption[XVIII]. From that point forward, little advancement has been made for a long time. The encryption system of Shafi Goldwasser and Silvio

Micali was proposed in 1982 was a provable security encryption scheme, which reached a remarkable level of security. It is based on additive Homomorphic encryption, however it can encrypt only a single bit. In the same concept in 1999 Pascal Paillier was also proposed a provable security encryption system that was also an additive homomorphic encryption. Few years later, in 2005, Dan Boneh, Eu-Jin Goh and KobiNissim [VI] created an arrangement of provable security encryption. During this scheme an infinite number of additions were possible however just one multiplication.

**Introduction of Smart Meters**

Generally, electricity suppliers have started replacement of electricity meters with smart meters. In short intervals of time smart meters will sends the electricity consumption reading to supplier. Smart meters measure energy utilization in much more detail than a regular meter, so it is an advanced meter.

In future, smart meters can communicate data back to the nearby utility for checking and charging purposes. Now a days electrical network is changing quickly to address the requests of distributed power generation. The significant component of the new smart grid is an advanced metering infrastructure. A smart grid is a model and modern system of monitors which cultivates communication between the power utility and the end user. This communication life cycle includes, sending generated electricity to the distribution center where it can be dispersed depending on need.

## II. Related Work

Research on Smart metering has introduced in 2010 with publications highlighting the privacy problems introduced by smart metering [III]. They proposed the security assurance of smart metering by implementing the principle that the company should know the general utilization of power by its customers as well as the sum of a customer's electricity utilization during the period of billing. They also introduced a smart metering security model for estimating the level of protection that a smart metering application can give.

In 2016, N.Busom et al. [IV] presented an efficient privacy preserving system for reporting the consumption of a neighborhood of n smart meters. By adding these consumptions homomorphically the link between customers and their individual consumption values is broken. So, they are sending detailed information without leaking any data and has a liner O(n) communication complexity.

In 2015, C. Thoma et al. projected "secure multiparty computation based privacy preserving protocol for smart metering system". This scheme satisfies the four conditions, first one is that the scheme will provide detailed users data , and second one, it has a verification process, third one, third party is not required and finally fourth one, it does not sacrifice the information goals for proposed smart grid control and board functionalities. N.Yukun et al. C.R.xie et al. B.Alohali et al. investigated in [I,XXIII,XXIV,] that secure against a coalition composed of a misbehaving substation and some corrupted meters. It does not require complicated tools such as an anonymous channel, group signatures.

In 2014, S.Finster et al. suggested in privacy aware smart metering [IX] is that various approaches to protect the privacy of customers, while still using smart metering. Mainly they identified two problems that have to be solved to realize privacy aware smart metering. They identified the approaches to these problems in research concerning privacy in smart metering. Using different generic approaches, they identified specific solutions and comparisons of the generic approaches.

In 2013, G. Danezis et al. [VII] presented in smart meter aggregation via secret sharing is that before transmitting reading to the supplier it divides into communities in that aggregate their readings for making use of homomorphic property of some cryptosystems. The homomorphic solutions require the use of secure computation techniques, when some of the participants in the system may not be honest.M.Joye et al. [XII] and in 2015, T. Jung et al. [XIII] emphasized a protocol for privately computing a sum can replace trusted dealer. As a result, we take an efficient system in which an aggregator obtains the sum of the private inputs of a set of parties after the transmission of only one message from each party to the aggregator.

In 2012, B. Vetter et al. [XXII] suggested an approach that enables flexible server side aggregation of smart meter readings. It combines homomorphic encryption with homomorphic message authentication codes for preserving customers privacy.

In 2011, F. Garcia and B. Jacobs [X] were among the first to propose a privacy friendly smart metering architecture based on additive homomorphic encryption. In this investigation, they choose n smart meters. Each smart meter, $M_i$, $i\epsilon\{1,2,3,\ldots\ldots,n\}$ divides it’s energy reading $m_i$ into n parts $m_{ij}$, $j\epsilon\{1,2,3,\ldots,n\}$ then encrypts each share $m_{ij}$forj $\neq$ i, under $M_i$’s public key and sends the resulting cipher texts to its substation SSt. After receiving cipher text SSthomomorphically aggregates all (n-1) shares encrypted under the public key of $M_i$. Then SSt sends the results to it. Each $M_i$decrypts the received cipher text and adds $m_{ii}$ to it. Finally, it sends the result to SSt. The SSt computes the aggregatedenergy consumption by adding all the received results.The general proposal of E.shi et al. [XIX] on privacy preserving aggregation of time series data can be indeed applied to smart metering systems. It combines perturbation based techniques with data aggregation. Every meter adding noise to its reading before encrypting it. Afterwards, the encrypted values are transmitted to an aggregator which homomorphically aggregates them.

In 2010, F.Li et al [XIV] and R. Lu et al[XV] designed on an efficient and privacy preserving aggregation scheme for secure smart grid is that they inspired by the fact that electricity usage data in small size. In [XIV] a neighborhood of n meters is represented by a graph G whose vertices denote the meters and each edge represents an available wireless link. Then, they take a spanning tree of G rooting at the collector node is taken and the power consumption is recursively computed from children to parent nodes and they used additive homomorphic property. In [XV] a centralized aggregating entity uses the paillier cryptosystem to efficiently aggregate the collected data.R. Petrlic [XVI] proposed the introduction of collector systems with in switchyards. In this, each meter sends their readings to the collector, the collector checks their authenticity and removes identifying information. Later the readings will be forwarded to electricity supplier.C. Efthymiou and G. kalogridis[VIII] reported that each smart meter has a high frequency identity and low frequency identity. High frequency identity is utilized for transmitting power utilization readings all the time and low frequency identity is utilized for computing bills which is based on smart meter readings. The connection between these two personalities is not known by the energy supplier, however just by an escrow mechanism (i.e., if it is already there in between supplier and distributor). Later M. Jawurek et al.[XI] discussed that each reading is transmitted after adding some random noise to it. Since this random noise will not be removed, these arrangements must be tuned to provide an appropriate tradeoff between privacy and accuracy in privacy preserving statistics.

In 2005, C. Castellucia et al. [V] proposed an efficient aggregation of encrypted data in wireless sensor networks. In that they designed an architecture that allows the transmission of up to date electricity measurements to energy suppliers on a group basis. In this, the solution is calculated by using additive homomorphic encryption. In this, trusted third party is not required. Each smart meter encrypts it's power consumption value with a homomorphic key.

In 1991, T.Pedersen identified in a threshold cryptosystem without a trusted party[XVII] in two points. One is a trusted party for selecting and distributing the secret is no longer needed. And another one is that each member of the group can verify that his share of the secret key corresponding to the public key.

In this paper, we would like to propose a cryptosystem using single conjugacy and homomorphism. Later we designed a smart metering system based on double conjugacy and homomorphism. We also presented comparative analysis of smart meters with electronic meters by taking real time electricity consumption readings in one specific neighborhood.

The rest of the paper is organized as follows. In section2, we introduced the required mathematical background for public key cryptography. In section3, we propose a non-commutative Elgamal cryptosystem on conjugacy. In section4, we implemented proposed cryptosystem for smart meters in power distribution. In section 5, we demonstrated security analysis and performance evaluation based on the mathematical logic. In section 6, we compare the experimental results of electronic meters with smart meters and benefits. In section7, we emphasis the main conclusions of the paper.

## III. Mathematical Primitives

In this section, we summarize the public key cryptography and significant mathematical background which is necessary to implement the proposed system.

### The Conjugacy Problem

Let $G$ be a non-commutative group, Theconjugacy problem in $G$ is defined as follows:

Let $x$ and $y$ be two elements in $G$ that are said to be conjugate to each other if $y = a^{-1} x a$ for some $a \in G$. It can be written as $x$ □ $y$, here $a$ (or) $a^{-1}$ is called conjugator and the pair $(x, y)$ is said to be conjugate. In a non-commutative group $G$, the Conjugacy problem is believed to be a hard problem.

### Double Conjugacy

Applying two times conjugacy with valid parameters in a given plat form is called double conjugacy and it provides more complexity to the hard mathematical problem.

## IV. Proposed Elgamal Cryptosystem with Conjugacy by Automorphism

In 2008, Ayan Mahalanobis proposed MOR cryptosystem based on discrete logarithm using automorphism over groups. The MOR cryptosystem is in fact natural generalization of Elgamal Cryptosystem over groups. In our invention we propose a new cryptosystem based on conjugacy using automorphism over non-commutative groups. The security of the proposed Elgamal public key cryptosystem is based on the assumed intractability of the conjugacy problem.

**Initial setup**

Let G be a finite non-commutative group. Let an inner automorphism of G is $\phi^*$ and is defined by $\phi^*(x) = g^{-1}x\ g$ for all $x \in G$. Here g is the private key. In place of $\phi_g$ , a standard notation of inner automorphism we replace with $\phi^*$ for security reason to keep secret key as secured.

**Encryption**

To send a message $m \in G$ Bob computes $\phi^*(m) = g^{-1}m\ g$ .After wards he publishes $\phi^*(m)$.

**Decryption**

By receiving $\phi^*(m)$ Alice computes m in such a way that $m=g\phi^*(m)g^{-1}$.

**Homomorphic Property of Elgamal Cryptosystem over Conjugacy**

Let $\phi^*(m_1) = g^{-1}m_1g$ and $\phi^*(m_2) = g^{-1}m_2g$ be two cipher texts encrypting $m_1$& $m_2$ respectively.

$$\begin{aligned}\phi^*(m_1).\phi^*(m_2) &= (g^{-1}m_1g).(g^{-1}m_2g)\\ &=(g^{-1}m_1.m_2g)\\ &=\phi^*(m_1.m_2)\end{aligned}$$

Hence Elgamal is a multiplicative homomorphic cryptosystem.

## V.Application: Smart Meters Based on Proposed Elgamal Cryptosystem in Power Distribution

**Mathematical Background for Smart Meter**

Let $\Psi^*$ be another inner automorphism defined on G and is defined as follows

$\Psi^*\left(\begin{bmatrix} m_i \\ q \end{bmatrix}, y_i z_i\right) = \left(gy_i g^{-1}, q^{m_i} z_i\right) = \left(c_i, d_i\right)$ where $m_i$,$y_i$, $z_i$, q, gare suitable elements defined in G. And also note that $\begin{bmatrix} m_i \\ q \end{bmatrix}$ it is single structure and it cannot be viewed as ordered pair.

Then,

$$\begin{aligned}\Psi^{*}\left(\begin{bmatrix} m_1 \\ q \end{bmatrix}, y_1 z_1\right) . \Psi^{*}\left(\begin{bmatrix} m_2 \\ q \end{bmatrix}, y_2 z_2\right) &= \left(g y_1 g^{-1}, q^{m_1} z_1\right) . \left(g y_2 g^{-1}, q^{m_2} z_2\right) \\ &= \left(g y_1 g^{-1} g y_2 g^{-1}, q^{m_1} z_1 q^{m_2} z_2\right) \\ &= \left(g y_1 y_2 g^{-1}, q^{m_1} z_1 q^{m_2} z_2\right) \\ &= \left(g y_1 y_2 g^{-1}, q^{m_1+m_2} z_1 z_2\right) \\ &= \Psi^{*}\left(\left(\begin{bmatrix} m_1 \\ q \end{bmatrix}, y_1 z_1\right) . \left(\begin{bmatrix} m_2 \\ q \end{bmatrix}, y_2 z_2\right)\right)\end{aligned}$$

where $z_1, z_2, \ldots\ldots, z_n, \ldots$have to be either constructed or extended as a cyclic group generated by q. Then $q^{m_1} z_1 q^{m_2} z_2 = q^{m_1+m_2}$ $z_1.z_2$

### Smart Metering Proposal Using Homomorphism with Double Conjugacy

In 2016, N. Busomet.al. proposed smart meter and it's functioning using discrete logarithm problem. In this paper we designed the execution of smart meters using Conjugacy problem twice by inclusion of homomorphism.

We consider neighborhood of n smart meters $M_i$ ,$i \in \{1,2,3\ldots..n\}$ and an electricity supplier substation SSt. Periodically smart meters send electricity measurements to SSt. After each electricity consumption transmission operation, the SSt obtains the aggregated value m= $\sum_{i=1}^{n} m_i$ with $m_i$ denoting the reading of $M_i$. In this article, we assume that each smart meter is performing encryption operations. Each smart meter $M_i$stores a secrete key as well as corresponding public key.

### System Set-up

In a home, a smart meter is installed, it establishes a connection with the SSt. Before transmitting electricity measurements the SSt indicates to all the smart meters the beginning of a key establishment operation, which isdefined as follows.

1. SSt sends a message to each smart meter with a key establishment.
2. Each $M_i$ sends $z_i$ and $\text{Cert}_i$ to SSt.
3. Then SSt verifies the correctness of $\text{Cert}_i$. If it is correct, $z_i$ and $\text{Cert}_i$ are sent to remaining smart meters that will perform the same check.
4. Finally, each smart meter calculates the group public key as $z = \prod_{i=1}^{n} z_i$ (under its region).

After step3, the SSt sends rest of n-1 public keys and certificates to each of other smart meters. Therefore, each smart meter receives O(n) amount of data. Here n smart meters, so the total amount of data which is transmitted by SSt is $O(n^2)$.

**Electricity Consumption Transmission**

In small intervals the smart meters sends their electricity consumption to SSt. Let $r_i$be the reading in the meter $M_i$and$e_i$be the power consumed by the local network under the control region of $M_i$. Hence reading $m_i = r_i + e_i$.

1. First SSt sends a message to each smart meter requesting it's electricity measurement.
2. Each smart meter $M_i$sentsSSt to cipher text as $\Psi^*(m_i) = (c_i, d_i)$.
3. SSt aggregates all the messages as $c = \left(\prod_{i=1}^{n} c_i, \prod_{i=1}^{n} d_i\right) = (c, d)$ and sends c to each $M_i$
4. Each $M_i$ computes $T_i=g_i^{-1}cg_i$ and $S_i=k_i^{-1}T_ik_i$
5. Then each smart meter sends the result to the SSt.

After receiving $S_i$, SSt computes $D = \prod_{i=1}^{n} s_i$ and $E=D^{-1} .d^n=q^{mn}$. Therefore m $= \frac{1}{n} \log_q E$

$\log_q E$ will be adjusted to thenext natural number, if it is real.

**Confirmation Theorem**

If all the parties act honestly, at step 6 of the transmission protocol of the SSt obtains the addition of electricity consumptions in the neighborhood, that is $\sum_{i=1}^{n} m_i$

**Proof:**

In electricity consumption transmission, the smart meter and the SSt compute the following values.

Each smart meter $M_i$ calculates the cipher text as

$$\Psi^*(m_i) = (c_i, d_i) \text{ where } c_i=g_iy_ig_i^{-1}$$
$$\& d_i=q^{m_i} z_i$$

Then SSt aggregates the received cipher texts as follows

$$C = \left( \prod_{i=1}^{n} c_i, \prod_{i=1}^{n} d_i \right)$$

$$= \left( \prod_{i=1}^{n} x_0^{-1} x_i x_i^{-1} a x_i x_i^{-1} x_0, q^{\sum_{i=1}^{n} m_i} z_i \right)$$

$$= \left( x_0^{-1} a^n x_0, q^m z \right) = (c, d) \text{Where m=} \sum_{i=1}^{n} m_i$$

After each smart meter receives $c$ and computes $T_i$ as

$$T_i=g_i^{-1}cg_i$$
$$= (x_0^{-1}x_i)^{-1}x_0^{-1}a^nx_0(x_0^{-1}x_i)$$
$$=x_i^{-1}a^nx_i$$

And $S_i=k_i^{-1}T_ik_i$

$$= (x_i^{-1}x_0)^{-1} (x_i^{-1}ax_i)(x_i^{-1}x_0)$$

Finally, SSt computes,

$$D = \prod_{i=1}^{n} s_i$$

E=D$^{-1}$.d$^{n}$

$= \left( x_0^{-1} a^n x_0 \right)^{-n} . \left( q^m z \right)^n = \mathrm{q}^{\mathrm{mn}}$

Finally m.n= $\log_q E$

$\Rightarrow$ m = $\frac{1}{n} \log_q E$ will be adjusted to the next natural number, if it is real.

**Strength of the Algorithm**

In smart meter consumption transmission protocol each smart meter receives a length of constant message and sends a length of constant message to SSt. Therefore, the communication cost for each smart meter is O(1). The SSt sends a constant length message to each of the n smart meters. So the overall communication cost at the SSt is O(n).

Here, M denotes the total number of units discharged by the power station and m$_1$,m$_2$,…..m$_n$ be the total units consumed by the n smart meters.

$\therefore$ m=m$_1$+m$_2$+…..+m$_n$ = m= $\sum_{i=1}^{n} m_i$

The power consumed by the local network under the control region of each smart meter is e.

$\therefore$ e=e$_1$+e$_2$+……..+e$_n$ and therefore M=m +e$\Rightarrow$e=M-m

For $1 \le \mathrm{i} \le \mathrm{n}$ ;  e$_i$ =Total units received- Total units metered

This will be predicted approximately depending on the domain, where we are applying this algorithm and by using advanced statistical techniques.

**Soundness of the Algorithm**

In this, the capability of a corrupted meter is equal to the revealing it's individual reading. That means the attacker can obtain the addition of the remaining meter readings. Getting individual reading would require the corruption of all the remaining n-1 meters. This is achieved by making use of a modified proposed Smart meter over conjugacy in which electricity reading is encrypted after masking them with a random value. The additional masking value is truncated later when the partial decryption is computed.

1. Reducing human intervention.
2. Accuracy of reading can be communicated to Sstin frequent intervals.
3. Reducing errors.
4. Development of economy.

## VI. Security Analysis

The main aim of the proposed protocol is to protect the individual consumptions in order to prevent monitoring of customer's behavior. The designed system is providing privacy in the sense that the only data a coalition composed of a corrupted SSt and some corrupted smart meters can obtain is the aggregation of electricity measurements of the honest smart meters.

Regarding data integrity, integrity against external attackers can be easily achieved by a digital signature to the transmitted data. Integrity against internal attackers cannot be provided because SSt or any corrupted smart meter can generate a corrupted message and attach an appropriate redundancy to it. Our system is providing privacy without requiring integrity.

**Attacker Model**

Our security analysis holds on the following very likely assumptions:

- Every smart meter store a private/public key pair. The public key comes with a digital certificate whose validity can be verified by the smart meters. Smart meters can become corrupted and reveal their private information.
- The substation SSt is not trusted. If corrupted, its objective is to obtain the individual reading $m_i$ of some meter $M_i$ possibly after colluding with some corrupted smart meters. A corrupted SSt will not necessarily follow the protocol steps as they are indicated.
- The communication channel between the SSt and a smart meter is not trusted. Data sent through it may be eavesdropped on or even modified.

**Privacy Analysis**

After proper protocol execution, the substation obtains the addition of all the readings $\sum_{i=1}^{n} m_i$ . Hence, if some meters are corrupted, they reveal their individual readings which can be subtracted from the previous addition. So, the addition of the honest meters readings is obtained. In this section, we will prove that such a coalition cannot obtain more than that, so that privacy is guaranteed.

**Lemma 1:**The neighborhood public key generated during the set up protocol is of the form $z_i = k_i^{-1} y_i k_i$ with each $y_i$being values only know by smart meter $M_i$.

**Proof:** We assume each smart meter is provided with some hardware storing a secret key$k_i$, the corresponding public key $z_i$ and its digital certificate $Cert_i$. In set up protocol each smart meter computes the neighborhood key $z = \prod_{i=1}^{n} z_i$ on its own after checking the certificate $Cert_i$of each received public key $z_i$. The validity of $Cert_i$ ensures that $z_i$ is of the form $k_i^{-1} y_i k_i$ with $y_i$being only known by smart meter $M_i$.

## V. Comparison of Smart Meters with Electronic Meters - Experimental Results and Benefits

This chapter intensely recommends the usage of smart meters based on several reasons as given in the following, but also significantly supports the innovation. The Smart meters considerably reduces the error between the total number of units discharged by the power station and total number of units metered by the substation. This must help to get more revenue at each substation region for government and so that the country will be benefitted economically in a large scale per year. Therefore the usage of smart meters definitely useful in all developing countries and particularly in the regions, in which where there are huge number of consumers. The power utilities across the world transforming from electronic meters to smart meters by the following reasons.

- Smart meters enable utility to provide customers with detailed information about their energy usage in small intervals of time.
  - It eliminates the collecting of manual meter readings.
  - By using smart meters we can avoid the capital expenses for building new power plants.
  - It helps to optimize income with existing resources.
  - It helps to decrease the amount of electronic bills.
  - By using smart meters we can monitor the electric system more quickly.
  - Now a days by using smart meters customers can access their prior day's electricity usage through their utility website.
  - In the near future, it may be possible for a customer to receive automatic alerts to notify them of when the electricity consumption exceeds a pre-determined threshold.

Here we considered the customers of 11KV KMM College TTD waterworks under 33/11KV Sreenivasa Mangapuram Substation in Tirupati Division. In this there are 51 services. These 51 services are divided into 6 categories.

**Table 1:Categories and Services**

| **Categories** | I | II | III | IV | V | VI |
|---|---|---|---|---|---|---|
| **Services** | 26 | 14 | 3 | 4 | 3 | 1 |

Where Category I denotes Domestics,
Category II denotes Non-Domestics,
Category III denotes Industries,
Category IV denotes Heavy Industries,
Category V denotes Street lights and water works &
Category VI denotes General [i.e., temples, schools etc].

**Table 2:Readings of Electronic Meters**

| Iteration No. | Month | Input Units | Total Sales(services) | (Input - sales) | % Losses | % Metered Sales | Cat-I Sales (services) | Cat-II Sales (services) | Cat-III Sales (services) | Cat-IV Sales (services) | Cat-V Sales (services) | Cat-VI Sales (services) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | May-17 | 990,800 | 951,440 | 39,360 | 3.97 | 96.03 | 4759 | 42486 | 2602 | 901124 | 0 | 469 |
| 2 | Jun-17 | 1,090,000 | 1,031,596 | 58,404 | 5.36 | 94.64 | 3293 | 29807 | 794 | 997368 | 0 | 334 |
| 3 | Jul-17 | 959,200 | 898,320 | 60,880 | 6.35 | 93.65 | 3394 | 32135 | 720 | 861736 | 0 | 335 |
| 4 | Aug-17 | 589,800 | 569,771 | 20,029 | 3.4 | 96.6 | 1821 | 15066 | 849 | 551762 | 0 | 273 |
| 5 | Sep-17 | 678,200 | 620,912 | 57,288 | 8.45 | 91.55 | 1737 | 18756 | 1424 | 598916 | 0 | 79 |
| 6 | Oct-17 | 616,600 | 574,935 | 41,665 | 6.76 | 93.24 | 1629 | 22177 | 1337 | 549792 | 0 | 0 |

## Computation of Error in Electronic Meters

Stephen Habenet.al., Presented A New Error Measure for Forecasts of Household-Level, High Resolution Electrical Energy Consumption[VII].In that they introduced a new forecast verification error measure, it reduces the double penalty effect, incurred by forecasts whose features are displaced in time. In this they proposed a measure which is based on finding a restricted permutation of the original forecast, which will minimizes the point-wise according to a given metric.

For finding the predicted input units and total sales we considered a straight line equation is y = a + bx. The normal equations which are used to find a constants presented in the straight line are

$$\sum y = na + b\sum x$$

$$\sum xy = a\sum x + b\sum x^2$$

By solving above equations we get the values of a &b. According to the experimental electronic meter readings, the values of a & b are a=1168347 and b= −99309.

Therefore the curve which is used to predict the input and sales units for the month of the November and December is

$$Y=1168347 - 99309\ X \quad \rightarrow (1)$$

To predict the meter reading and the corresponding error for the 7th iteration by using previous 6 iterations. Take X=7 in equation (1).

The predicted input units for the month November are 473184, and for the month December is 373875.

By applying the same procedure we also predict the total sales for November and December months. The predicted total sales for November = 430138 and December =

331808. The error predicted for the month of November is 43001 and it's percentage is 9.08% and also for the month December is 42067 and it's percentage is 11.25%.

**Comparison of Experimental Electrical Meter Readings with Smart Meter Readings by Prediction**

As the practical Design, Implementation and Testing of the results by the above said Smart meters are highly expensive and beyond our limits, we predict the worst case error in Electronic meters is approximately 5%. The lawful and justified cause for this prediction is already some countries are using smart meters. They enjoying the services and benefits by the smart meters. We considered 11KV KMM College TTD waterworks from 33/11KV Sreenivasa Mangapuram Substation in Tirupati Division. We computed the following input units, total sales and loss% by above said prediction. We will prove the major benefit of revenue even under small substation region. So that the revenue can be estimated and generalized over the country.

**Table 3:Readings of Smart Meter**

| Iteration No | Month | Input Units | Total Sales(services) | (Input-sales) | % Losses | % Metered Sales | Cat-I Sales (services) | Cat-II Sales (services) | Cat-III Sales (services) | Cat-IV Sales (services) | Cat-V Sales (services) | Cat-VI Sales (services) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | May-17 | 990,800 | 967342 | 23458 | 2.36 | 97.64 | 5112 | 53485 | 3432 | 904740 | 0 | 573 |
| 2 | Jun-17 | 1,090,000 | 1038493 | 51507 | 4.95 | 95.05 | 3535 | 32708 | 896 | 1000960 | 0 | 394 |
| 3 | Jul-17 | 959,200 | 906320 | 52880 | 5.51 | 94.49 | 3778 | 37238 | 840 | 864068 | 0 | 396 |
| 4 | Aug-17 | 589,800 | 575771 | 14029 | 2.37 | 97.63 | 1998 | 18042 | 949 | 554493 | 0 | 289 |
| 5 | Sep-17 | 678,200 | 624705 | 53495 | 7.88 | 92.12 | 1846 | 21343 | 1624 | 599808 | 0 | 84 |
| 6 | Oct-17 | 616,600 | 583317 | 33283 | 5.39 | 94.61 | 1743 | 24236 | 1473 | 555865 | 0 | 0 |

For finding the predicted input units and total sales, here also we considered same straight line equation

y = a + b x. The predicted input unit for the month November is 473184 and for the month December is 373875. According to the predicted input units and total sales instead of electrical meters by smart meters, the values of a & b are a = 1131861.8 and b=-99772.5.

Therefore the fitted curve which is used for finding the values are Y = 1131861.8 - 99772.5. The predicted total sale for the month of November by using smart meter is 433454 and December is 333682. The error predicted for the month November is 39370 and it's percentage is 8.39% and December month is 40193.2 and it's percentage is 10.75%.

The error average for 6 months of electrical meter readings = 5.75% and the error average for 6 months of smart meter readings are 4.74%. That is if we use smart meters instead of electronic meters, approximately we can reduce at least 5% of loss.

## The Correlation Between the Losses for Electrical Meters and Smart Meters

By using correlation we can calculate the relation between the losses for electric meters and smart meters, we observed the value 0.971329. That means it's says two meters are positively correlated. That is when compare to electric meters smart meters reduce the loss percentage for the government. The below column graph shows the losses of electrical meters and reduced losses of smart meters for 8 months data.

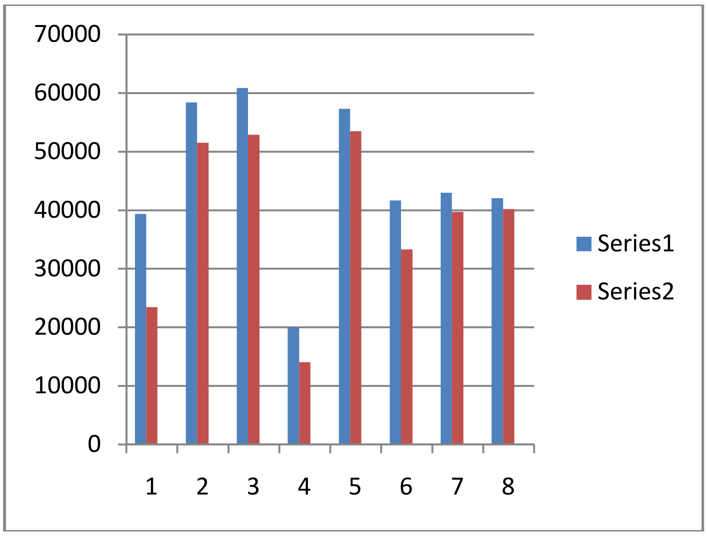
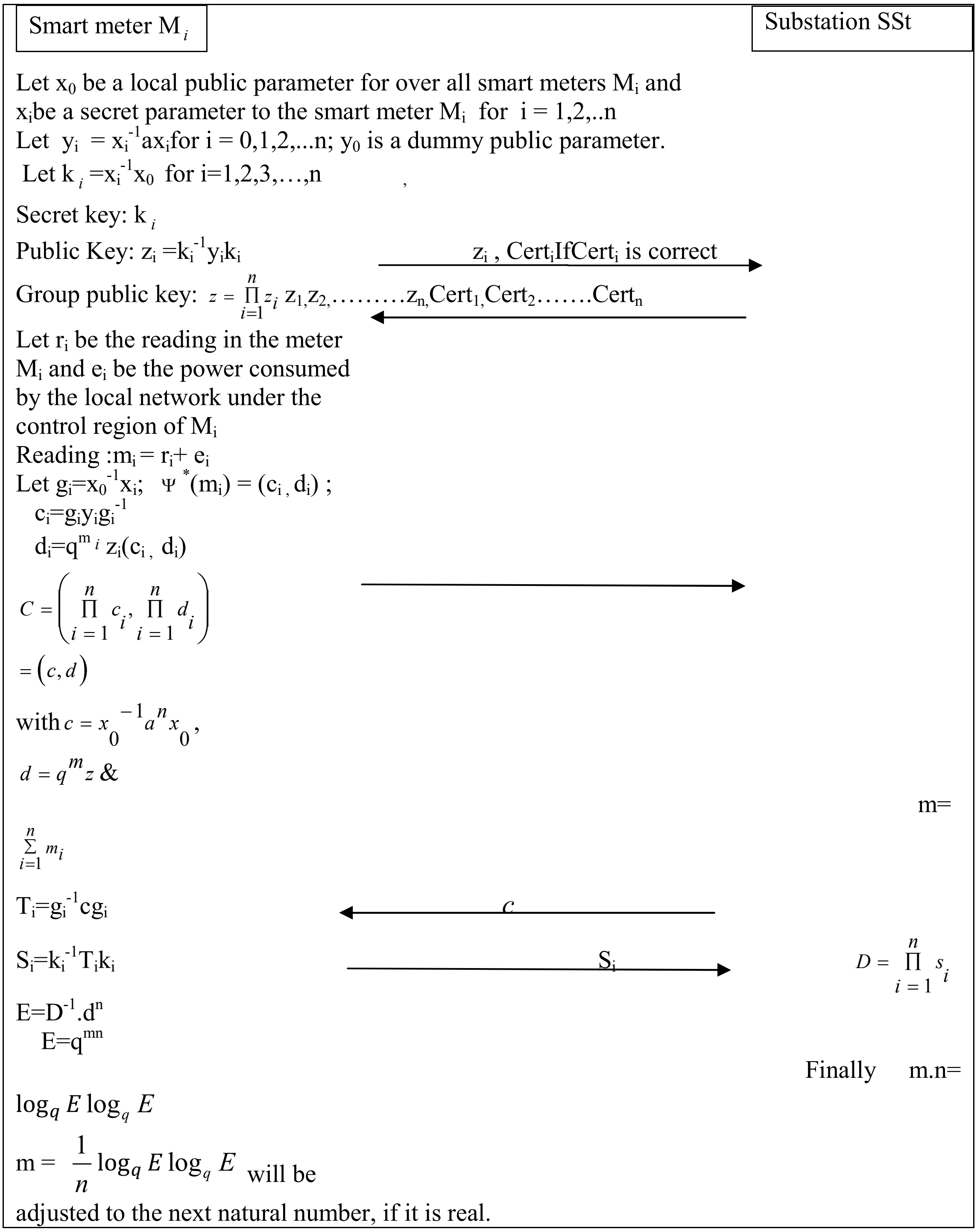


**Fig. 2:** Graph of Smart and Electronic Meter Readings

Here service1 denotes the losses by using electrical meter and service 2 denotes reduced losses by using smart meters.

Entire structure is shown in Fig 1.



Smart meter $M_i$

Substation SSt

Let $x_0$ be a local public parameter for over all smart meters $M_i$ and $x_i$be a secret parameter to the smart meter $M_i$ for $i = 1,2,..n$

Let $y_i = x_i^{-1} a x_i$for $i = 0,1,2,...n$; $y_0$ is a dummy public parameter.

Let $k_i = x_i^{-1} x_0$ for $i=1,2,3,\dots,n$ ,

Secret key: $k_i$

Public Key: $z_i = k_i^{-1} y_i k_i$

$z_i$ , $Cert_i$IfCert$_i$ is correct

Group public key: $z = \prod_{i=1}^{n} z_i$ $z_1, z_2, \dots\dots\dots z_n, Cert_1, Cert_2 \dots\dots Cert_n$

Let $r_i$ be the reading in the meter $M_i$ and $e_i$ be the power consumed by the local network under the control region of $M_i$

Reading :$m_i = r_i + e_i$

Let $g_i = x_0^{-1} x_i$;  $\Psi^*(m_i) = (c_i, d_i)$ ;

$c_i = g_i y_i g_i^{-1}$

$d_i = q^{m_i} z_i(c_i, d_i)$

$C = \left( \prod_{i=1}^{n} c_i, \prod_{i=1}^{n} d_i \right)$

$= (c, d)$

with $c = x_0^{-1} a^n x_0$,

$d = q^m z$ &

m=

$\sum_{i=1}^{n} m_i$

$T_i = g_i^{-1} c g_i$

$c$

$S_i = k_i^{-1} T_i k_i$

$S_i$

$D = \prod_{i=1}^{n} s_i$

$E = D^{-1}.d^n$

$E = q^{mn}$

Finally m.n=

$\log_q E \log_q E$

m = $\frac{1}{n} \log_q E \log_q E$ will be adjusted to the next natural number, if it is real.

**Fig. 1:**Sketch of the Protocol

## VII. Conclusions

In this paper, we have presented smart metering based on homomorphic encryption over conjugacy. In this we developed a system for reporting the consumption of a neighborhood of n smart meters. By homomorphically adding all n consumptions, the existing link between customers and their individual consumption values is broken. In this way detailed information can be sent without leaking individual personal data. Our solution does not require communication among smart meters, but only with the electricity supplier(represented by the substation). The individual reading of a smart meter has been kept secret. Our approach does not require a trusted third party and has linear O(n) communication complexity. And also we compared experimental values of electrical with predicted smart meter readings. Finally, we can conclude that average error for eight months by using electrical meter is 5.715% , if we replace smart meters instead of electrical meters we will get average loss percentage 4.75% that is it will reduces error and it also benefit for the government.

## VIII. Acknowledgements

The authors would like to thank 33/11KV Sreenivasa Mangapuram Substation in Tirupati Division for providing the valuable consumers data of 11KV KMM College TTD waterworks subdivision. This is really helpful to us to project how smart meters will be helpful to measure the accurate rate reading. Since India is having huge number of electric customers, the usage of smart meters in a country like ours, the error for maintenance of the network will be reduced drastically. So that the economy of the country will be enriched.

## References

I. Alohali B, Kifayat K, Shi Q, Hurst W, "A survey on cryptography key management schemes for smart grid", in Journal of Computer sciences and Applications, pp.27-39, 2015.

II. AyanMahalanobis, "A Simple Generalization of Elgamal Cryptosystem to Non-abelian Groups", in communications in algebra , pp.3878-3889, 2008.

III. Bohli JM, Sorge C, Ugus O, "A Privacy model for smart metering", in Proceedings of the First IEEEInternational Workshop on Smart Grid Communications(in conjunction with IEEE ICC 2010), 2010.

IV. Busom N , Petrlic R , Sebe F, Sorge C, Valls M., "Efficient smart metering based on homomorphic encryption", in Computer Communications, pp. 95-101, 2016.

V. Castelluccia C, Mykletun E, Tsudik G, "Efficient aggregation of encrypted data in wireless sensor networks, in Proceedings of the second Annual International conference on Mobile and Ubiquitous systems: Networking and services , pp.109-117, 2015.

VI. Dan Boneh, Eu-Jin Goh, KobbiNissim, “Evaluating 2-DNF formulas on cipher texts”, in Theory of Cryptography Conference, pp. 325-341, 2005.

VII. Danezis G, FournetC, Kohlweiss M, Zanella-BeguelinS, “Smart meter aggregation via secret sharing”, in Proceedings of Smart Energy Grid Security Workshop , pp.75-80, 2013.

VIII. Efthymiou C, Kalogridis G, “Smart grid privacy via anonymization of smart metering data”, in Proceedings of the First IEEE International Conference on smart Grid Communications, pp.238-243, 2010.

IX. Finster S, Baumgart I, “Privacy aware smart metering: a survey”, in IEEECommun.Surv.Tutor, 2014.

X. Garcia F, Jacobs B, “ Privacy friendly energy metering via homomorphic encryption”*, in* Proceedings of 6thInternational Conference on security and Trust Management, LNCS, pp.226-238, 2011.

XI. Jawurek M, Kerschbaum F, Danezis G, “ Privacy Technologies for smart Grids- a survey of options”, in Technical report, Micro Technical Report 2010.

XII. Joye M, Libert B, “ A scalable scheme for privacy preserving aggregation of time series data”, in Financial Cryptography and Data security, Springer-verlag, Berlin Heidelberg , pp.111-125, 2013.

XIII. Jung T, Li X, “Collusion tolerable privacy preserving sum and product calculation without secure channel, in IEEE Trans. Dependable and Secur. Comput , pp.45-57, 2015.

XIV. Li F, Luo B, liuP, “Secure information aggregation for smart grids using homomorphic encryption”, in Proceedings of the First IEEE International Conference on smart Grid Communications , pp.327-332, 2011.

XV. Lu R, Liang X, Li X, Shen X, Eppa, “ An efficient and privacy preserving aggregation scheme for secure smart grid Communications”, in IEEE Trans.Paralleldistrib. Syst: 2012.

XVI. Petrlic R., “A privacy preserving concept for smart grids”, in Sicherh.Vemetztensyst, 2010.

XVII. Pedersen T, “A threshold cryptosystem without a trusted party”, Proceedings of Advances in Cryptology Eurocrypt 91 LNCS 1991, pp.522-526.

XVIII. Ronald L, RivestLeonardAdleman, Michael L. Dertouzos, “On Data Banks and Privacy Homomorphisms, chapter On Data Banks and Privacy Homomorphisms”, Academic Press 1978, pp. 169-180.

XIX. Shi E, Chow R, Chan T H, Song D, Rieffel E, “Privacy preserving aggregation of time series data”, in Proceedings of Network and Distributed System Security symposium, NDSS, The Internet Society, 2011.

XX. Stephen Haben, Jonathan Ward, DanicaVukadinovicGreetham, Colin singleton, peter Grindrod, “A new error measure for forecasts of household level, high resolution electrical energy consumption”, in International Journal of Forecasting , pp.246-256, 2014.

XXI. Thoma C, Franz Franchetti T C, “Secure multiparty computation based privacy preserving smart metering system”, 2012.

XXII. Vetter B, Ugus O, Westhoff D, SorgeC, “Homomorphic primitives for a privacy friendly smart metering Architecture*”,* inProceedings of the International Conference on Security and Cryptography, SECRYPT, pp.102-112, 2012.

XXIII. Xie C R, Zhang R Y, “Privacy preserving power consumption data measuring protocol for smart grid*”,* in Proceedings of International Conference on Computer Information Systems and Industrial applications, CISIA, 2015.

XXIV. Yukun N, Xiaobin T, Shi C, Haifeng W, Kai Y , Zhiyong BU, “A security privacy protection scheme for data collection of smart meters based on homomorphic encryption”, in Eurocon, 2013.