

# Innovative Privacy-preserving Aggregation Techniques for Smart Meters



By

**Nazish Kanwal**

**Fall 2017-MS(IS) - 00000203466**

Supervisor

**Dr. Syed Taha Ali**

**Department of Electrical**

A thesis submitted in partial fulfillment of the requirements for the degree  
of Masters of Science in Information Security (MS IS)

In

School of Electrical Engineering and Computer Science,  
National University of Sciences and Technology (NUST),

Islamabad, Pakistan.  
(November 2020)

## Approval

It is certified that the contents and form of the thesis entitled "Innovative Privacy-preserving Aggregation Techniques for Smart meters" submitted by NAZISH KANWAL have been found satisfactory for the requirement of the degree

Advisor : Dr. Syed Taha Ali

Signature:  \_\_\_\_\_


Date: 23-Oct-2020

Committee Member 1: Dr. Arsalan Ahmad

Signature:  \_\_\_\_\_

Date: 23-Oct-2020

Committee Member 2: Dr. Wajahat Hussain

Signature:  \_\_\_\_\_

Date: 22-Oct-2020

Committee Member 3: Mr. Muhammad Imran  
Abeel

Signature:  \_\_\_\_\_

Date: 22-Oct-2020

## THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS/MPhil thesis entitled "Innovative Privacy-preserving Aggregation Techniques for Smart meters" written by NAZISH KANWAL, (Registration No 00000203466), of SEECS has been vetted by the undersigned, found complete in all respects as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial fulfillment for award of MS/M Phil degree. It is further certified that necessary amendments as pointed out by GEC members of the scholar have also been incorporated in the said thesis.

Signature: \_\_\_\_\_  \_\_\_\_\_

Name of Advisor: Dr. Syed Taha Ali

Date: 23-Oct-2020

Signature (HOD): \_\_\_\_\_

Date: \_\_\_\_\_

Signature (Dean/Principal): \_\_\_\_\_

Date: \_\_\_\_\_


# Dedication

I dedicate this thesis to my **Parents** for their endless prayers, love and encouragement.

## **Certificate of Originality**

I hereby declare that this submission titled "Innovative Privacy-preserving Aggregation Techniques for Smart meters" is my own work. To the best of my knowledge it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at NUST SEECS or at any other educational institute, except where due acknowledgement has been made in the thesis. Any contribution made to the research by others, with whom I have worked at NUST SEECS or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except for the assistance from others in the project's design and conception or in style, presentation and linguistics, which has been acknowledged. I also verified the originality of contents through plagiarism software.

Student Name: NAZISH KANWAL

Student Signature:  \_\_\_\_\_

# Acknowledgment

First and foremost, I am grateful to Allah Almighty for his countless blessings and for giving me the knowledge to accomplish my research work. I would like to express my deep gratitude to my supervisor, Dr. Taha Ali. Thank you for your continuous guidance, support, and encouragement throughout the thesis. Without his guidance, advice, and valuable input on my research ideas and writings, this work would have not been possible. I gratefully acknowledge my thesis committee members, for their valuable comments and insightful suggestions that helped increase the quality of the thesis. My deepest appreciation and grateful thanks go to my parents and family for their prayers, support, and care. Your love and encouragement have been and will always be a great source of inspiration in my life.

# Table of Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Motivation . . . . .	1
1.1.1	Smart Electricity is the Future . . . . .	1
1.1.2	Smart Meter Market . . . . .	2
1.1.3	Privacy Concerns . . . . .	2
1.1.4	Privacy Concerns and Politics . . . . .	3
1.1.5	GDPR and Smart Metering . . . . .	3
1.1.6	Proposed Solutions . . . . .	5
1.1.7	My Thesis Contribution . . . . .	5
1.2	Problem Statement . . . . .	6
1.3	Thesis Organization . . . . .	7
<b>2</b>	<b>Background Study</b>	<b>8</b>
2.1	Smart Meter and its Importance . . . . .	8
2.1.1	An Introduction of Smart Meter . . . . .	8
2.1.2	Benefits of Smart Meter . . . . .	9
2.1.3	Security Risks of Smart Meter . . . . .	10
2.1.4	Why Forecasting is Necessary in Case of Smart Meters? . . . . .	10

2.1.5	Privacy Issues Due to Load Monitoring . . . . .	11
2.1.6	Prevention of Privacy Intrusion in Various Countries . . . . .	12
2.2	The Smart Grid Ecosystem . . . . .	13
2.2.1	Smart Meter Architecture . . . . .	14
2.2.2	The Smart Meter Ecosystem . . . . .	17
2.2.3	General Properties . . . . .	19
2.2.4	Trust Model . . . . .	21
<b>3</b>	<b>Literature Review</b>	<b>25</b>
3.0.1	Anonymization . . . . .	26
3.0.2	Aggregation . . . . .	27
3.0.3	Differential Privacy . . . . .	28
3.0.4	Verifiable Computing . . . . .	28
3.0.5	Electricity Billing . . . . .	29
<b>4</b>	<b>Research Methodology</b>	<b>31</b>
4.1	Defining Research . . . . .	31
4.2	Research Methodology . . . . .	31
4.2.1	Define Research Question . . . . .	32
4.2.2	Determine Research Objective . . . . .	32
4.2.3	Literature Review . . . . .	33
4.2.4	Data Collection and Analysis . . . . .	33
4.2.5	Research Design . . . . .	34
<b>5</b>	<b>Proposed Solution</b>	<b>35</b>
5.1	The Main Entities . . . . .	35



5.2	Overview of Proposed Scheme . . . . .	36
5.3	The Workflow . . . . .	37
5.4	The Cryptogram . . . . .	40
5.4.1	Cryptograms with Dynamic Tariffs . . . . .	42
5.5	Overview of Dataset . . . . .	43
<b>6</b>	<b>Implementation and Results</b>	<b>45</b>
6.1	Research and Implementation Overview . . . . .	45
6.2	Evaluation . . . . .	46
6.2.1	Security Analysis . . . . .	46
6.2.2	Performance Testing . . . . .	47
<b>7</b>	<b>System Analysis</b>	<b>60</b>
7.1	Security Properties . . . . .	60
7.1.1	Attack Scenarios . . . . .	61
7.2	Securing the Regulator . . . . .	62
7.3	Securing within the Aggregate . . . . .	62
7.4	An Alternative Mode . . . . .	63
<b>8</b>	<b>Conclusion &amp; Future Work</b>	<b>64</b>
8.1	Conclusion . . . . .	64
8.2	Future Work . . . . .	65

# List of Tables

3.1	Comparison of Similar Schemes . . . . .	30
5.1	Overview of Datasets . . . . .	44

# List of Figures

2.1	Electricity Grid . . . . .	17
5.1	Overview of Proposed Scheme . . . . .	36
5.2	Work Flow of Smart Metering . . . . .	38
6.1	Time Analysis on Core i7 . . . . .	49
6.2	Time Analysis on Raspberry Pi . . . . .	50
6.3	Time Analysis of Cryptogram Generation . . . . .	51
6.4	Time Analysis of Cryptogram Generation with Tariffs . . . . .	51
6.5	Cryptogram Aggregation Time . . . . .	52
6.6	Cryptogram Aggregation Time with Tariffs . . . . .	53
6.7	Neighborhood Aggregation Time . . . . .	53
6.8	Simple Lookup Time . . . . .	54
6.9	Tariffs Lookup Time . . . . .	55
6.10	Neighborhood Lookup Time . . . . .	55
6.11	Cryptogram Generation and Aggregation Comparison . . . . .	56
6.12	Lookup Time Comparison . . . . .	56
6.13	Cryptogram Generation Time Comparison . . . . .	57
6.14	Cryptogram Aggregation Time Comparison . . . . .	58

6.15 Simple Lookup and Simple Lookup with Threading . . . . .	58
6.16 Neighbourhood Lookup and Neighbourhood Lookup with Thread- ing . . . . .	59
6.17 Tariff Lookup and Tariff Lookup with Threading . . . . .	59

# Abstract

The way energy is provided by electricity providers is changed because of various upgrades in power grid. Advanced Metering Infrastructure (AMI) is one of the main reasons to modernise the the electricity grid. There are some privacy concerns associated with this electricity grid. This process can reveal the private information of consumer's as it collects fine-grained power consumption data. This has led to limited consumer acceptance of the smart grid. Hence, it is important to design some mechanism to prevent disclosure of consumer electricity usage information. Security researchers have provided a lot of efforts in various private data aggregation techniques. In this thesis, elliptic curve and Diffie–Hellman based privacy preserving aggregation scheme is proposed with very less computation overhead. It's performance is evaluated and validated by statistical analysis and by testing it on a dataset. This scheme provides promising solution for fine-grained load monitoring, secure billing, dynamic tariffs, accountability, fault tolerance, selective unmasking of energy readings altogether in a very efficient way comparative to other schemes. This scheme is applicable on limited-capability smart meters. So, this work is an important progress toward more reliable, secure and authentic smart meter communication.

# Chapter 1

## Introduction

### 1.1 Motivation

#### 1.1.1 Smart Electricity is the Future

Energy distribution systems are transitioning towards the smart grid paradigm and pilot projects are actively being researched and deployed. Smart grid technologies are anticipated to introduce several benefits [1]: to make energy systems more efficient and easier to manage. They would reduce greenhouse gas emissions and incorporate variable and distributed energy sources into the grid, including wind and solar power. Operators could troubleshoot faults and failures in the grid more effectively and curtail theft. Utilities could introduce dynamic tariffs and assist consumers in proactively managing their electricity consumption.

### **1.1.2 Smart Meter Market**

A key component of smart grid infrastructure is the smart meter, which is deployed in customer premises, and enable utilities to monitor user energy consumption in real-time, and thereby forecast demand and undertake demand-side management. Various countries have legislated to encourage uptake of smart meters, including US, Japan, and South Korea. The EU Electricity Directive 2009/72/EC states that “Where roll-out of smart meters is assessed positively, at least 80% of consumers shall be equipped with intelligent metering systems by 2020” [2]. The UK government has set a target to install smart meters in 85% of customer homes by the end of 2024 [3]. A recent report estimates that the global smart meter market is predicted to reach nearly \$10.4 billion by 2022 with over 588 million units deployed [4].

### **1.1.3 Privacy Concerns**

However, the fine-grained readings collected by these meters give rise to significant privacy concerns [5] [6], and are a key factor in customers’ resistance to deployment of smart meters [2] [7] [8] [9]. Opponents argue that energy readings can reveal personal user information, including a home’s occupancy status, and clues to users’ activities and lifestyle. Moreover, researchers have been able to identify specific appliances and user activity within homes from energy signatures [10] [11] [12] [13], even to the extent of identifying which movie is playing on the television [14]. Smart meter data can also be monetised by building highly personalized user profiles and selling this information to third parties, such as advertisers, vendors, etc. [9]

### **1.1.4 Privacy Concerns and Politics**

These concerns are widely acknowledged. In the United States, NIST has documented various scenarios of how smart meter data could reveal “business activities, manufacturing procedures, and personal activities in a given location” [15]. The EU data protection watchdog body has issued similar warnings. Consumer privacy groups have argued for utility customers to control ownership of this data to protect their privacy [16] and that law enforcement should require a warrant to access smart meter data [17]. In the Netherlands, in 2009-2011, citizen groups successfully campaigned against legislation mandating smart meters by highlighting the privacy issues [18]. There have also been attempts at self-regulation within the energy industry [19].

### **1.1.5 GDPR and Smart Metering**

General Data Protection Regulation (GDPR) is an EU regulation related to ownership and protection of personal data of European union’s citizen. It requires EU companies and non EU companies that process data of EU citizens, to provide privacy and protection to personal data of individuals.

Smart meters collect electricity usage data from users and then process it into meaningful optimization strategies. Adoption of General Data Protection Regulation (GDPR) raises some questions related to maintaining customers privacy and protection in case of smart meters.

These definitions of GDPR will be affecting utility companies:

1. The definition of personal information applies to any information re-



lated to an individual, that can be used to identify an individual. This means that utility companies using customer's location data to enhance their experience must inform them about the purpose of collection and usage of that data

2. Data processing includes collection, recording, structuring, storage, transmission, dissemination, and destruction, retrieval of personal data among others by manual or automated means. The utility companies needs customers permission in collection, storage and transmission of his data to some third party. The companies must inform their customers about the purpose of processing their personal data.

Smart metering results in substantial reduction of energy cost and enables utilities to find out customers electricity usage pattern and finding out electricity leakage and wastage.

GDPR will provide greater security and privacy to smart devices like smart meter. Utility companies requires upgradation in infrastructure, systems and process. Regular audits should be carried out in companies. Data should not be available to everyone in the company, authorization and different access levels should be defined for the management of data.

A Data Protection Officer (DPO) must be hired by companies to ensure GDPR compliance. This whole process will become more efficient and transparent because of GDPR. GDPR non-compliance will result in fine of 4% of company's turnover or €20 million.

### **1.1.6 Proposed Solutions**

Researchers have proposed various solutions to resolve these privacy issues while ensuring fine-grained monitoring and accurate billing. One approach considers anonymization techniques, enabling utilities to collect smart meter readings without being able to link the readings to particular users [20] [21] [22]. Differential privacy methods have also been proposed which inject noise into meter readings to preserve privacy of individual users [23] [24].

A popular strategy in the research literature is to protect the privacy of individual users by reporting aggregated energy readings to utilities [25]. This approach relies on two primary techniques: homomorphic encryption [26] [27] [28] [29] and secure multi-party computation [30] [31]. Typical challenges with this strategy involve use of trusted parties and proxies and complicated protocols.

Drawbacks involved in other proposed schemes are complicated protocols, proxies, trusted parties, size of aggregation set. Recent work of [32] has also studied the trade-off between the size of the aggregation set and individual privacy.

### **1.1.7 My Thesis Contribution**

1. Presenting a practical homomorphic aggregation scheme for privacy-preserving billing and analytics using smart meters
2. Design and implementation of an algorithm which provides fine-grained load monitoring, secure billing, dynamic tariffs, accountability, fault tolerance, selective unmasking of energy readings. This is the first

solution which is providing all these things together.

3. Prototype this scheme and bench-mark its performance using datasets of real-world household energy readings

This scheme relies on a cryptographic primitive which enables homomorphic computations in two dimensions i.e. the same reading can be used for analytics across a subset of houses in a neighborhood over small-sized epochs e.g. every 15 minutes, as well as for billing individual users for energy consumption over a longer time frame e.g. one month. Moreover, these individual readings cannot be deciphered in themselves, they cannot be distinguished from random data but only be viewed as part of the aggregate set.

Dynamic tariffs can be implemented within this scheme. However, if required, these readings can be unmasked by authorities using warrants if needed. In this scheme no proxies or complicated interactive protocols are involved, Smart meters have to perform a simple multiplication operation at their end.

This scheme successfully resolves outstanding privacy concerns while enabling multiple desirable features.

## **1.2 Problem Statement**

Design and implementation of an algorithm which provides fine-grained load monitoring, secure billing, dynamic tariffs, accountability, fault tolerance, selective unmasking of energy readings. This is the first solution which is

providing all these things together.

## 1.3 Thesis Organization

This thesis has been organized within seven chapters, where each chapter is compiled to shed light on all research aspects of the thesis.

- Chapter 1 “Introduction” describes the motivation behind choosing the topic for research, the problem statement, objectives and organization of the thesis.

- Chapter 2 “Background Study” goes through the background of smart meter infrastructure.

- Chapter 3 “Literature Review” goes through the previous work done by authors and their schemes.

- Chapter 4 “Research Methodology” explains the research pathway that has been adopted to achieve the goals.

- Chapter 5 “Proposed Solution” describes the solution suggested for the research topic. It includes the workflow, an introduction to the cryptograms and overview of the datasets used.

- Chapter 6 “Implementation and Results” shows the architecture of system. It also shows the results of the proposed scheme.

- Chapter 7 “System Analysis” contains the properties of the proposed system and discusses various attack scenarios.

- Chapter 8 “Conclusion and Future Work” concludes the thesis highlighting the areas which are open for future work.

# Chapter 2

## Background Study

### 2.1 Smart Meter and its Importance

#### 2.1.1 An Introduction of Smart Meter

Some smart meters look similar to the old meters, but the key difference is that the utility company does not have to send a meter reader out to get the readings. Instead, they can see your energy activity remotely. Smart meter is an energy meter that measures various additional information along with electricity consumption, as compared to analog meters. Smart meters are being used in various countries for the significant technological enhancement of electric power supply infrastructure. By the year 2020, every home in United kingdom is expected to have installed smart meters [3].

According to [33] smart meter market will remarkably grow in the next ten years. As per Navigant Research forecasts the overall economic opportunity is nearly \$57 billion that is coming from smart metering worldwide. It is

expected that china will lead country-level installation base of electric smart meters, by installing more than 435 million electric devices by December 31, 2020. United States will also install 132 million smart meters by the date.

In 2022, the global smart meter market is estimated to nearly reach \$10.4 billion and over 588 million units by 2022. [4]. Some Countries like US, South Korea, and Japan have issued legislation to install smart meters.

### **2.1.2 Benefits of Smart Meter**

The reason for this enormous growth in smart meter market is that it is economically beneficial. It is useful for customers as it helps in reducing electricity cost and is useful for utility providers as it helps in troubleshooting failures and improving reliability. If smart meters are not used in electricity grid then it will effect power quality and energy wastage, The alternative to a digital grid is wasted energy, fluctuating power quality and a return to the physical presence of meter readers on private property. Electricity supplies can be routed intelligently to the area where they are needed, By providing the exact meter reading after regular interval to service providers from smart meters. This will provide benefits to the customer by providing them their electricity usage pattern, helping them to save their money by changing their electricity consumption habits. This could result in flexible and novel payment scheme, also reduce the risk of power blackout. However, more information like consumers activities can be inferred from the meter readings other than just power consumption.

### **2.1.3 Security Risks of Smart Meter**

These fine-grained readings can distinguish specific appliances like alarms and electronic devices. Every device consumes energy at different levels and times, with smart metering it is possible to construct a breakdown of which devices were being used, and when. For marketing perspective, it is highly valuable to know which consumers use vacuum cleaners more than others, or electrical tools, or play video games. This will expose customer at the risk of theft or sale of their data. Higher the frequency of smart meter readings, more will be the information obtained from them about consumers lifestyle. So, a balance should be maintained between infrastructure benefits and consumer's privacy. Due to these privacy issues Netherlands rejected smart metering [34].

### **2.1.4 Why Forecasting is Necessary in Case of Smart Meters?**

Smart meters provide two type of data to service provide, billing data after a month and load reporting data after every five minutes interval. Fine-grained readings to electric providers is needed for real-time monitoring and energy management. The production of energy from small scale sources requires load forecasting to some extant for adjustment of energy generation. It also helps in implementing variety of value-added services. Therefore, Energy providers needs to know the information about the amount of energy required in a network. So that they can ensure that their is always enough energy according to the requirement of customers and match generation and demand

by using higher rates during peak consumption hours of a day i.e. dynamic tariffs. Another aim is to adjust appliances like fridge and air-conditioner during energy shortage time.

### **2.1.5 Privacy Issues Due to Load Monitoring**

Load monitoring helps in identification of specific electrical appliances. This detailed consumption data will result in creation of profiles of consumer's lifestyle and can leak sensitive information related to consumers activities.

According to the Electronic Privacy Information Center (EPIC), "an attacker with \$500 of equipment and materials could take command of a smart meter, making it possible that "just as identities, credit card numbers and financial information are harvested and sold, so too can smart grid information." [35]

Everyone is not happy and convinced with smart meters. Some private citizens are opposing smart meters because of they are concerned about the use of their data. Therefore, some states like Texas are giving consumers to opt-out of smart meter by paying some fee.

Basically, it's a trade off between privacy and efficiency [33], the State of Pennsylvania - Katzman says - "the legislature actually passed a law in 2009, requiring all electric distribution companies that had over 100,000 customers to deploy smart meters by 2025". So, companies are forced to replace the old devices with the smart meters.

On January 16, 2018, the Electronic Privacy Information Center (EPIC) speak about proposed smart meter-related legislation in the state of Mary-



land. According to them personal data about the utility services usage is collected by smart meters. Smart meter can also find out that when a person is in home, and what is he doing. This data collection would result in ongoing surveillance of utility consumers without any criminal suspicion. Their aim is to prevent government agencies from accessing utility data without search warrant for investigation or surveillance [36].

While discussing smart meters advantages and its privacy and data security issues, Naperville Smart Meter Awareness v. City of Naperville is an important case. Claim of privacy advocates was that the smart meter readings constitute an unreasonable search but the Seventh Circuit panel disagreed and concluded that the smart meter search was reasonable because of its advantages. Court also said that this gathering of information did not violate citizen's Fourth Amendment rights. Where Fourth amendment of US court States that "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches, shall not be violated ..." The court still accept the fact that smart meter is providing private information to government official that would not be possible without this search warrant [37].

### **2.1.6 Prevention of Privacy Intrusion in Various Countries**

Various solutions have been presented to protect user's privacy and are referenced in literature review. They can be grouped into these basic techniques:

## 2.2 The Smart Grid Ecosystem

The smart grid is a self-sufficient smart electricity network system capable of providing electricity from multiple distributed sources like solar power systems and wind turbines etc. The gathering and transmission of data is performed by sensors in smart grid. In case of any problem grid managers are informed immediately. This system can find out solution very quickly providing reliable and sustainable electricity to all consumers. The grid can communicate with meters and at the time when there is a lot of electricity can turn on user's appliances automatically on lower prices [38]

The growing population, climate changes, energy storage and generation problem faced by electricity industry requires certain upgradation in existing power grid. In today's smart grid, one of the main component is Advanced Metering Infrastructure(AMI). It gathers and analyze smart meters data through systems and networks. It also provides services using smart meter data and management of electricity related applications [39].

Modern communication technologies and automated control is used in Smart Grid that improves efficiency, reliability and security of electric grid. In AMI system two way communication between Consumers and Service Provider takes place. Smart Meter can not only draw power from electric grid but it also provide the facility to supply surplus power to the electricity grid. Smart meter helps in measurement of this bidirectional electricity flow. It improves load balancing.

Levels involved in today's smart grid are network of Power generators, transmitters, distribution systems, and its customers. First step is energy

generation from various energy sources such as wind, solar panels or hydroelectric power stations. Electricity generators are far away from population centers. Therefore, electricity is then transmitted to the distributors through transmission lines. Distributors then transmit this electricity to the customers. Electricity distributor system consists of medium voltage power lines, substations and transformers [39].

### **2.2.1 Smart Meter Architecture**

The times when electricity man was knocking on the door for checking the meter has been ended due to a technology called smart meters. Smart meter's identify electricity consumption in much more detail comparative to conventional meter. It periodically sends the electricity consumption back to the utility provider for load monitoring and billing. Typically, smart meter records electricity consumption hourly or more frequently and reports it daily to energy provider [39]. Data Collected by smart meters consists of the following parameters unique meter identifier, timestamp, and the electricity consumption values. Smart meter can monitor and execute control commands for all appliances and devices at customer's place. Smart Meter can communicate with other meters in it's neighbourhood using home area network(HAN) for collection of diagnostic information about devices. Smart meters only generate bills for the electricity consumed from utility provider and not for the electricity taken from the devices owned by customers. It can terminate and begin electricity supply to any customer remotely and can also limit maximum electricity consumption [40]. Smart meters can be integrated

in electricity grid for the detection and identification of electricity theft and unauthorized power consumption [41].

Smart meter readings not only provide information to service provider for demand and response but it also helps customer to control their power consumption and managing the peak load. Hence, utility companies can provide electricity to all the customers at very low and even rates [39]. .

Two major functionalities implemented in smart meters are measurement and communication.

Now a days, two way communication takes place between smart meter and provider comparative to automatic meter reading. In one-way communication meters report their readings on intervals however, bi-directional meters can be polled by the utility when needed. Smart meter not only sends its transmission data to user's personal energy monitor but also to the energy provider. These meters boost efficiency and lower costs and enables users to monitor their real time consumption. This communication may be wireless or fixed wired connections(power line). By this, energy provider can gain understanding of electricity load, high demand time and can mitigate the possibility of power blackout. Utilities can also create dynamic pricing models for their customers which will encourage them to conserve electricity for high demand hours.

Various control devices and sensors are used in smart meter architecture for identification and collection of parameters and then transmission to the control center.

Smart meters are located far from the utility therefore intermediate devices are needed to route the data of smart meters to the utility. Gateways

(or concentrators) collects data from smart meters and then send it to the utility over Wide Area Network (WAN) connection. Gateways also propagate control information to smart meters. The architecture of smart grid necessitates the smart meters, sensing devices, gateways and the control centers to exist in the path between the customers and the utility providers for the two-way communication

Smart meters are located far from the utility provider so the next point here is the communication of smart meter with utility in real world scenario. Smart meter don't communicate using internet. They work by using wireless networks namely HAN(home area network) and WAN(wide area network). HAN is a secure network within a home which allows communication between digital devices. This network allows communication between smart meters and with an in-home display. WAN is used for communication between smart meters and utility providers. It is a network to send and receive data. It must be regulated and secure enough so that the smart meter data is kept secure and private.

In this section, typical smart meter architecture is discussed. Each home is provided with smart meter. These smart meters are then connected to utility provider to send them meter readings for load monitoring, billing and tariffs etc. This gathering of detailed energy usage information by utility is user's privacy invasion. This information is needed by the utility provider. Various research has been conducted to provide electricity consumption data to utility provider while maintaining users privacy.

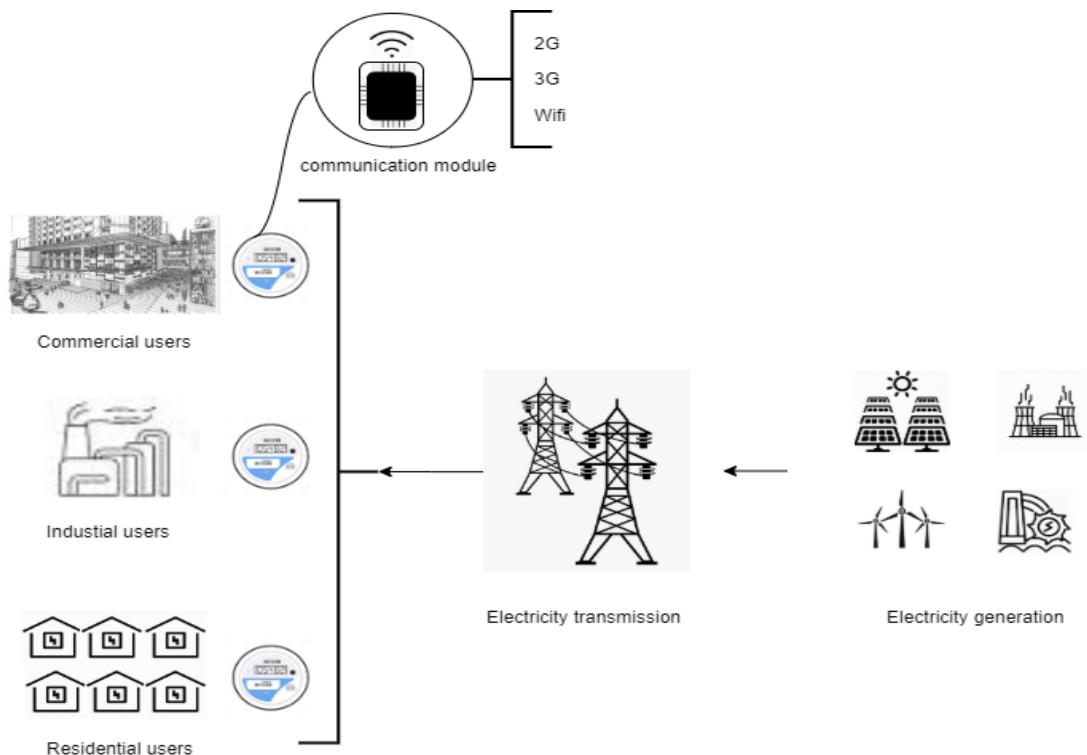


Figure 2.1: Electricity Grid

### 2.2.2 The Smart Meter Ecosystem

Electricity grid is basically a network for transmitting electricity from electricity generators to the consumers. In Fig.2.1 a general electricity grid scenario is depicted in which there are: **Electricity generating stations** that produce electricity. Electricity generation is a process of electricity generation from primary energy sources. Electricity is produced from other forms of energy. Electricity can be generated by electromechanical generators, kinetic energy of water and wind, solar energy and geothermal power.

**Electricity transmission lines** that carry electricity from power generating stations to different electricity users. Electricity transmission is the movement of bulk of electricity from electricity generating site to electrical

substations and then to electricity users. Users can be residential, industrial and commercial. The lines which facilitate this movement are known as electricity transmission network.

Electricity grid can be susceptible of various malicious and privacy intrusion attacks. Therefore, there is a need for security in electricity grid. Smart meters have to share their electricity consumption information to utility provider after a 15 minutes interval for load monitoring. Due to privacy reasons it is required to report this reading to service providers using some method which will protect users privacy while transmitting this information.

### **The Main Entities**

The energy distribution ecosystem typically comprises three entities: **power utilities** distribute energy and maintain grid infrastructure. **Subscribers** or consumers purchase energy from utilities and primarily consist of residential, commercial, and industrial users. **Regulators** oversee the energy market, define policies and standards, and adjudicate disputes.

A key innovation of the smart grid paradigm is to deploy smart meters with a communications link, thereby enabling utilities to monitor consumer energy usage in real-time. The setup is depicted in Fig.2.1. Smart meters typically record and report energy readings at short-time intervals (e.g. once every 15 minutes is a common specification). The communication may be over a wired or wireless link.

Monitoring energy consumption in real-time enables various benefits including efficient load monitoring and forecast, dynamic tariffs, accurate billing and settlement, use of demand-response technologies, fraud detection, and

value-added services. **Dynamic tariffs** which incentivize subscribers to undertake energy-intensive activities during periods in the day when energy generation is comparatively cheaper. This includes activities such as space heating, using washing machines, dishwashers and dryers, and charging electric vehicles. Studies also indicate that providing subscribers with feedback regarding live energy consumption may contribute to meaningful reductions in energy usage [42] [43].

However, it is also clear that this existing model makes the subscriber’s energy consumption completely transparent to the utility. Indeed features such as dynamic tariffs explicitly rely on access to fine-grained user readings. As mentioned earlier in chapter 1, considerable personal information about subscribers can be inferred from these readings, including their house occupancy status, their activities, their religious background (Sabbath), etc. Researchers have demonstrated that machine learning can infer even greater detail from these readings, including what appliances residents use, even what movies they watch on TV and whether the fridge has been opened recently.

### **2.2.3 General Properties**

At the minimum, this system aims to retain general features and properties of existing systems. This solution does not require changes to the existing ecosystem of power utilities, subscribers, and regulators and does not introduce new entities or complicated protocols. The only significant change is that our solution requires regulators to play a more active role in the system by directly bootstrapping privacy-preserving communications. Moreover, our



solution does not require active human intervention, it is automated and efficient. System complexity is also constant, in that the system can scale easily to cater to large numbers of users. It does not create new vulnerabilities or facilitate attackers beyond their existing capacities. We next focus on privacy properties.

### **Privacy Properties**

Our scheme relies on a privacy-preserving primitive termed the cryptogram to encode smart meter readings, which ensures that these readings can only be deciphered within an aggregate set of multiple readings. For purposes of monitoring, the utility will have to aggregate real-time readings for a pre-specified number of subscribers (usually over a neighborhood) to be able to access readings at the individual meter level. The structure of the cryptogram ensures that the utility is not able to link readings to the meters from which they originated.

Moreover, these same individual meter readings may also be aggregated over the duration of a billing period (usually over a month) for billing purposes. In this case, the utility can compute an accurate bill, but is unable to link individual readings to specific instances in time. If dynamic tariffs are operational, the cryptogram itself does not reveal to the utility if the client is availing those tariffs.

The utility therefore is able to monitor energy consumption of groups of subscribers in real-time and can also undertake accurate customer billing. However, since it cannot link individual readings to originating meters or to specific points in time, the utility cannot profile individual customers beyond

any information that may be deduced from the aggregate data itself. It is important to note this qualification: research has revealed that the energy readings of a typical household may be identified in the aggregate if the size of the aggregate set is too small [32].

### **Other Properties**

This is a key novelty of our scheme: prior work primarily treated privacy-preserving billing and real-time monitoring each in isolation, as distinct problems, and usually prescribing individual solutions for each. We believe we are the first to propose a unified solution which addresses both these vital concerns using the same underlying primitive.

### **2.2.4 Trust Model**

Here we list trust assumptions for all participating parties and spell out the threat model.

#### **Subscriber**

The subscriber installs a smart meter on her premises which records energy readings at periodic intervals, encodes them using our protocol, and transmits them to the utility. All meters have a unique public-private key pair, enabling authenticated and encrypted data communication with the utility. Subscribers may view their own cleartext readings directly from the visual display on the meter. Some meters even allow users to access readings over WiFi. Subscribers may even freely share their readings with third parties

(such as energy-efficiency consultants, other value-added services providers, etc.).

An attacker, or perhaps even the subscriber herself, may try to hack into the smart meter, either physically or via the network, to access and even alter energy readings. Smart meters typically employ a wide array of measures to protect against unauthorized access, including rugged metal casing, specialized sensors, and tamper-detection algorithms [44]. However, it is still possible that an attacker may view or change readings. In this paper, we do not consider attacks mounted directly on the smart meter. (discussed in chapter 3).

Our scheme does not secure smart meters against attacks and would be as vulnerable to them as existing systems. Our scheme does not defend against attacks that corrupt readings at the source. Instead, we provide a protocol for secure aggregation and computation on data in a privacy preserving manner. For our purposes, we assume the smart meter is a relatively trusted device that faithfully executes our protocol. Our specific contribution is a communication protocol for secure aggregation and computation on data in a privacy preserving manner.

However, an attacker with unauthorized access to the smart meter may tamper with the execution of our protocol by withholding readings. This is a genuine concern since individual meter readings of all subscribers in the aggregate set can only be decoded once readings from all meters are obtained. We describe a technique which would allow our protocol to recover in case some readings are withheld or lost (due to network faults, meter failure, etc.). Moreover, in these cases, the problematic meters can be easily identified and

remedial measures can be taken.

## **Utility**

The role of the utility is simply to collect and aggregate readings from individual smart meters. We treat the utility as a hostile entity which is interested in obtaining energy readings of individual households. For this reason, we have expanded the role of the regulator in our scheme to act as a counter-balance.

## **Regulator**

Regulators typically ensure fair practices, market competition, and protect consumer interests in energy markets. In our solution, the regulator directly participates in the protocol and bootstraps privacy by providing encoding information directly to individual smart meters. The meters encode the readings accordingly and transmit them to the utility. These encoded readings are not shared with the regulator. This separation is critical since individual privacy will be compromised if the regulator and the utility collude. We believe this separation can be legally enforced, given the growing awareness among stakeholders of the key importance of privacy of smart meter data and the need for novel architectures to secure it [45].

The regulator may be honest-but-curious (Hbc), i.e. he participates in the protocol but still tries to learn whatever information he can. This threat is mitigated since he does not access any encoded meter readings. There is a second possibility where the regulator may be malicious and colludes with the utility to decipher individual meter readings.

However, there may arise legitimate instances which necessitate access

to cleartext smart meter readings, especially from a law enforcement perspective [44]. Moreover, the subscriber herself may request that her readings specifically be unmasked, e.g. for value-added services. In this case, if there is a legal obligation (e.g. a warrant) or express permission to share cleartext readings, the regulator and utility can collaboratively unmask the encoded readings. no new trusted entities introduced!

# Chapter 3

## Literature Review

Despite the benefits provided by smart meters there are risks. Current smart meters are providing user's fine grained data to service provider. Various researches have been conducted to find out that which data is provided to service provider by smart meters and what information can be inferred from it. Researches have shown that this data is revealing the activities of people by measuring frequent electricity consumption. The insufficient security measures while transmitting smart meter data will expose it to misuse [46,47]. The utility servers can use data mining algorithm to analyse the fine grained household data and can find out appliances and electricity usage pattern of users.

In some papers, smart meters are considered as tamper resistant for the sake of convenience and in some paper they are not. In those scenarios in which Smart meter are not tamper resistant there need to be certain confirmation that the smart meters are sending correct information [48]. In this thesis we are assuming that smart meters will be tamper proof.

To protect users privacy in smart metering various schemes have been proposed. Various Cryptographic and non-cryptographic schemes have been proposed for collecting smart meter reading in AMI networks while providing users privacy. Non-cryptographic schemes include rechargeable battery which hides users electricity consumption patterns. By using rechargeable battery, privacy of user's data contained in his electricity load profile can be partially protected but the privacy of user is dependent on capacity of battery. It's negative point is that it depends on battery's performance and pricing [49]. [50] uses trellis algorithm for finding electricity leakage by computing the battery's input and output loads. It also discusses a realistic model of battery system. In table 3.1, comparison of relevant schemes is shown.

### **3.0.1 Anonymization**

In Anonymization techniques the meter data is sent to the utility provider without linking it to a single meter, however, it can be linked to a specific location i.e group of houses. This is also useful for schemes like load monitoring where linking of meter data to a smart meter is not needed.

In this paper, a third party escrow mechanism for authenticated anonymous meter reading is used. This scheme is just an additional layer of security for smart meter privacy protection. Messages should follow a new route every time it sends reading to prevent Smart meter traceability [20, 22]. Another anonymization scheme implements their scheme using CL signatures [21].

## 3.0.2 Aggregation

### Homomorphic Paillier Algorithm

Another approach for providing privacy is data aggregation. It is an inexpensive practical approach which provides privacy in smart metering. [26] uses homomorphic Paillier cryptosystem technique to encrypt multi-dimensional data.

[51] is an aggregation scheme, that uses Paillier cryptosystem and Horner's Rule to perform multi-dimensional aggregation.

In [52] Aggregated energy consumption is computed by using the combination of Paillier's homomorphic encryption and additive secret sharing to prevent electricity leakage.

Homomorphic signatures are used as an end-to-end signature scheme in [53] that provides data integrity. However, the batch verification scheme proposed in the paper does not verify individual node's input.

In [54], a privacy enhancing data aggregation scheme is proposed which provides protection against internal attackers like electricity suppliers and batch verification for efficient verification. Blinding factors are added with smart meter readings to make them meaningless for the attackers which are then cancelled upon aggregation.

[55] proposed three aggregation schemes providing data integrity with trade-off between various parameters i.e. security assumptions, computation cost and communication payload. These schemes include combination of homomorphic MAC and homomorphic hash.

[30] performs privacy friendly secure multi-party computations (SMC)



for complex non-linear problems on smart meter readings. However, their scheme causes communication bandwidth and latency overhead in case of large number of multiplications.

[31] provides privacy-preserving aggregation for network monitoring and billing over space and time. For the correctness of mask updates, all the smart meters in the ring topology must communicate sequentially resulting delay in collecting fine-grained data.

### **3.0.3 Differential Privacy**

Differential privacy method adds noise to meter readings so that the statistical queries on the readings does not reveal information about electricity usage. In [56] smart meter adds noise to the meter readings and then encrypts it with steam cipher. Privacy-preserving billing protocol is used along with differential privacy to add noise to the bill to conceal it from service provider.

### **3.0.4 Verifiable Computing**

In verifiable computing a computer due to its limited resources outsources the computation of it's function to parties which are not trusted because the cost of verification is comparatively less than the actual computation of the function itself.

## **Public Verifiability in Verifiable Computing**

In public verifiability result can be verified by any party. Our proposed scheme is also publicly verifiable. If we post the 2D cryptogram values anywhere then anyone can verify the load monitoring and billing value.

## **Trusted Party**

In this case, trusted third party receives meter readings and only disclose the results after performing certain computations on them. So that the original readings are not disclosed. In Secure Two-Party Computation, two parties provide certain input and after combining these inputs certain computations are performed on them and result is given. Here, both parties will keep their input private. In multi-party secure communication, Instead of two parties there are multiple parties providing their private input for certain computations, which will then give result. The utility provider is not resource constrained and computation power is not an issue for it. In our protocol, things will be simplified for user comparative to utility provider. It is saving utility provider resources on the cost of user's resources.

### **3.0.5 Electricity Billing**

Bill calculation can be performed inside the meter or signed meter reading can be sent to an application [57]. That application will then calculate bill and send it to service provider with some proof that bill calculation is correct. The later one is better comparative to the first one because in this case we do not have to update smart meter after every policy change in tariffs

	Properties														
	Installable Batteries	Affordable	resist against power load changes	Privacy	Dataset	Load Balancing	Electricity Leakage detection	untraceability	Trusted Third Party	Linkability	Confidentiality	Authenticity	Integrity	Anonymity	Verifiability
[49]	(=)	(=)	(=)	∅	(=)	(=)	(=)								
[50]	(=)			∅				(=)	(=)		(=)	(=)	(=)	(=)	(=)
[22]				(=)					(=)	(=)	(=)	(=)	(=)	(=)	(=)
[21]				(=)						(=)		(=)	(=)	(=)	(=)
[54]		(=)		(=)					(=)			(=)	(=)	(=)	(=)
[26]				(=)							(=)	(=)	(=)	(=)	(=)
[51]				(=)								(=)	(=)	(=)	(=)
[53]													(=)		(=)
[27]													(=)	(=)	
[52]							(=)						(=)	(=)	
[55]													(=)	(=)	
[30]				(=)									(=)		
[31]				(=)					(=)						(=)

(=) provides property

\$ partial provides property

Table 3.1: Comparison of Similar Schemes

and meter will have to perform less computations [48]. Our scheme is also following the later one. In [57] the cost of Zero Knowledge proof of a tariff that is polynomial increases with Polynomial degree.

In [48] privacy preserving billing protocol is proposed, which generate bills with variable tariff policies, without revealing the user's consumption measurements. This protocol is based on polynomial commitments. Digital signatures are computed on smart meters.

# Chapter 4

## Research Methodology

This chapter discusses the steps that have been followed to accomplish the research end goals. All the steps involved in the research methodology are clearly explained, and the end results achieved after each step are also presented.

### 4.1 Defining Research

A collection of methods and methodologies systematically applied by researchers to produce some sort of record of procedures and a report of result or conclusion. In the next section, the research methodology steps followed for the thesis are explained in detail.

### 4.2 Research Methodology

Research Methodology involves specific procedure or techniques followed in carrying out the research process. In following sections the steps performed

for the undergoing thesis are explained.

### **4.2.1 Define Research Question**

RQ.1) What are the main privacy concerns in smart meter environment?

RQ.2) What are the methods to transmit fine-grained electricity consumption readings to service providers?

RQ.3) What are the methods for secure billing in smart meter environment?

RQ.4) What are the other features that can be added in an algorithm along with load monitoring and secure billing?

The first step is to define a research question. A major problem in power grid is that the fine-grained readings collected by meters give rise to significant privacy concerns and are a key factor in consumers' resistance to deployment of smart meters. fine-grained energy readings can reveal personal user information. Moreover, researchers have been able to identify specific appliances and user activity within homes on the basis of energy signatures.

The main focus of this thesis is to design and implement a privacy preserving algorithm for billing and the transmission of fine-grained readings collected by smart meters.

The next step was to conduct a thorough study in both problem and solution domains.

### **4.2.2 Determine Research Objective**

After determining the research area the next step was to narrow down the research objectives. The objectives of this thesis are as follows:

To implement an algorithm that preserves users privacy while providing the features of load monitoring and secure billing. Along with other attributes like dynamic tariffs, accountability and fault tolerance etc.

To identify the issues in previously proposed schemes so that we can overcome these issues in our scheme.

The next objective was to identify the properties that should be present in our system.

The final objective is to find out that what results we want from our scheme with less computation overhead.

### **4.2.3 Literature Review**

Before developing our own scheme the related work was studied and summarized. For literature, papers(of conferences and journals) were used along with various similar researches to compare statistics, reports and news articles. The next task was to find out other schemes related to our schemes. Then, the analysis and detailed study of these schemes were carried out to find out the issues in previous schemes. So that, our scheme can overcome these issues.

### **4.2.4 Data Collection and Analysis**

In this stage, a detailed study and analysis of various similar projects were conducted. We compared the schemes used by these projects and their performance capabilities. The results are statistically summarized from the collected data of other researches. After collecting all this data the architecture

and workflow for this scheme was designed. A privacy preserving method to transmit fine-grained electricity consumption readings to service providers along with secure billing is identified and developed.

#### **4.2.5 Research Design**

For deciding the features and specifications of our domain, we went through numerous research work. Conclusions are then drawn from the analysis. We then started searching the c++ libraries that we can use for Elliptic curve cryptography. In various researches smart meters were simulated using Raspberry Pi to evaluate the performance and computations of proposed scheme.

For implementation and testing of our scheme we are using:

- Elliptic-Curve Cryptography (ECC)
- Cryptograms
- Visual Studio C++
- Raspberry Pi 2
- Library-CryptoPP
- Decisional Diffie-Hellman

# Chapter 5

## Proposed Solution

In this chapter, we explain in detail about our proposed system for providing load monitoring and smart metering in electricity grid. This section will walk the readers through the technical details of the system.

### 5.1 The Main Entities

The energy distribution ecosystem typically comprises three entities: **power utilities** distribute energy and maintain grid infrastructure. **Subscribers** or consumers purchase energy from utilities and primarily consist of residential, commercial, and industrial users. **Regulators** oversee the energy market, define policies and standards, and adjudicate disputes.

At the minimum, this system aims to retain general features and properties of existing systems. This solution does not require changes to the existing ecosystem of power utilities, subscribers, and regulators and does not introduce new entities or complicated protocols. The only significant



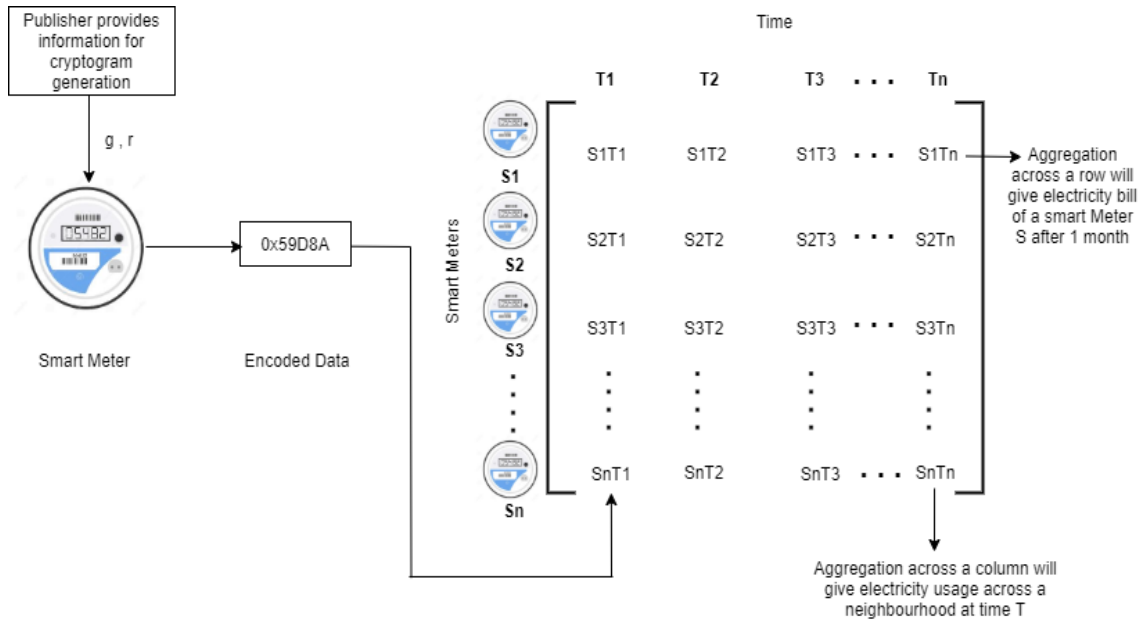


Figure 5.1: Overview of Proposed Scheme

change is that our solution requires regulators to play a more active role in the system by directly bootstrapping privacy-preserving communications. Moreover, our solution does not require active human intervention, it is automated and efficient. System complexity is also constant, in that the system can scale easily to cater to large numbers of users. It does not create new vulnerabilities or facilitate attackers beyond their existing capacities.

## 5.2 Overview of Proposed Scheme

The main aim of this scheme is to design a secure billing mechanism for smart meters which will also provide fine-grained readings for load monitoring to service providers without invading user's privacy. The entities involved are:

Smart meters (subscribers), Regulators, Electricity Service Provider (ESP). Regulators will help smart meter in cryptogram generation. Cryptogram will be generated by smart meter. Smart meter of certain neighborhood will send cryptograms to the ESP. ESP will aggregate cryptograms to get the fine grained readings for load monitoring of the neighborhood. At the end of a month, ESP will aggregate the cryptograms of a single smart meter to get its individual bill.

### 5.3 The Workflow

Here, a detailed description of the proposed scheme's workflow is discussed. The information flow between the three entities is presented in Fig. [5.2].

1. In the initialization step, each smart meter is assigned a unique ID. The regulator and the utility negotiate fundamental parameters of the scheme, including the members and size,  $n$ , of the aggregate set over which monitoring is to be done, the duration of the monitoring epochs,  $t_m$ , and the billing period,  $t_b$ , for subscribers. There may be cases in which some readings may be lost due to meter faults, communication breakdown, etc. and it is not possible to complete the protocol. In this case, the utility and regulator can agree on a threshold value of missing readings for which the regulator can compensate. These parameters can be listed in a document and signed by the utility and the regulator and shared with the subscriber if needed.
2. The regulator then generates encoding parameters, referred to as cryp-

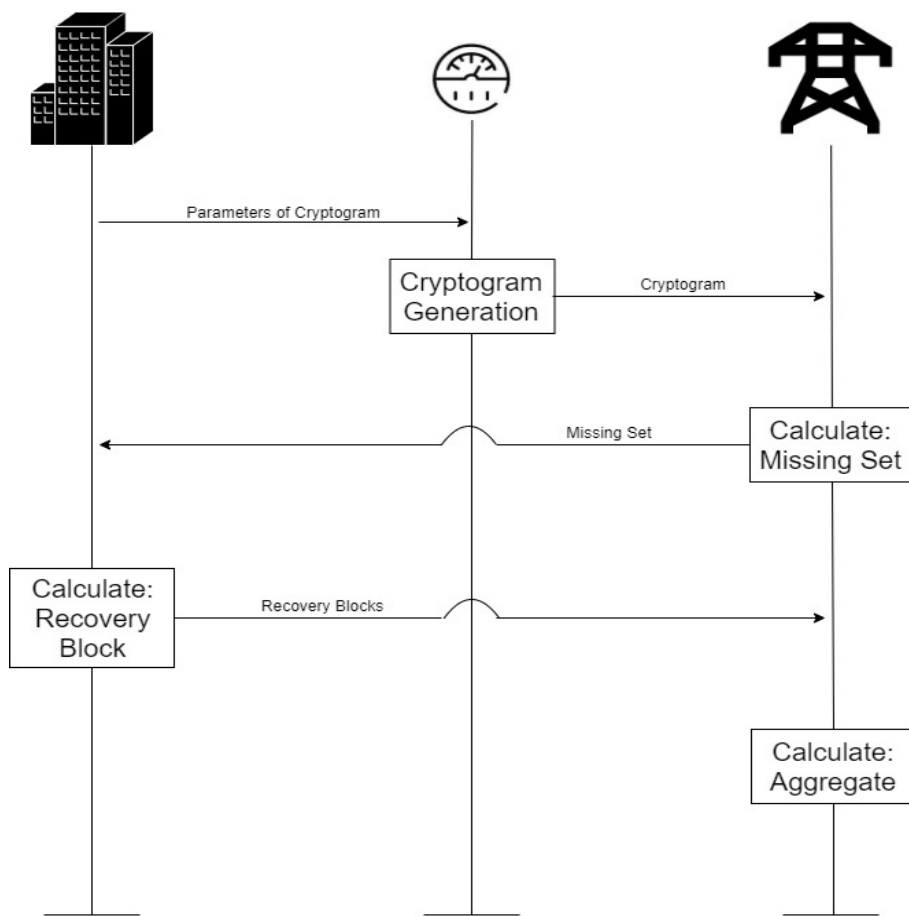


Figure 5.2: Work Flow of Smart Metering

tograms. Each meter in the aggregate set is assigned a unique set of cryptograms where each cryptogram corresponds to a specific epoch in the billing period. The regulator transmits these cryptograms to the individual meters over a secure connection. A detailed description of the cryptograms and how to generate them is described in the next section.

3. The smart meter records energy usage readings for every epoch and then encodes them using the cryptograms. These encoded readings are then digitally signed and transmitted to the utility. These readings are not shared with the regulator. However, for record keeping purposes, the meter transmits a confirmation to the regulator that it has dispatched the reading to the utility for the specific epoch.
4. The utility receives epochal readings from all meters. For every epoch, it aggregates all meter readings in the set to compute fine-grained energy readings across the set. This enables the utility to undertake energy prediction and demand-side management.

The utility also aggregates all epochal readings for individual smart meters for the duration of the billing period, thereby computing the energy bill for individual subscribers.

5. Some meter readings may be lost due to meter faults or communication problems and aggregation is not possible. In this case, the utility contacts the regulator with a list of meter IDs with missing readings. The regulator checks its own records to see if it received a confirmation from

the meter in question. If not, the regulator computes a Recovery Set, which enables the utility to complete the aggregation for the remaining meters in the set.

This process, however, effectively reduces the size of the aggregate set and could potentially compromise the privacy of the subscribers if too many readings are lost. Therefore, in Step 1. all stakeholders need to agree on a threshold value of number of missing readings that the regulator may compensate for. If missing readings exceed this value, the regulator may refuse to compute the Recovery Set to protect privacy of subscribers.

6. There may be a legitimate need to decode individual meter readings, such as for purposes of law enforcement or to provide the subscriber with value-added services. In these cases, the regulator can reveal the epochal encoding parameters for the meter in question. Any concerned party can then easily decode the individual energy readings issued by the meter.

## 5.4 The Cryptogram

The primitive in [16] has been adapted to meet the requirements of our model. There are  $i \in [1, 2, 3, \dots, n]$  number of smart meters and  $j \in [0, t]$  time intervals. The smart meter reading values  $v_i$  range from 0 to 999 (In the data set maximum reading is 15). Consider a cyclic group consisting of large primes  $p$  and  $q$  satisfying  $q \mid p - 1$ . We have two generators  $g_1$  and  $g_2$

of subgroup  $Z_q$  of order  $q$  of the group  $Z_p$ . The system on setup generates random values  $r_i$  then the following 2D matrices are calculated,

$$R_{ij} = g_2^{r_{ij}}$$

and the corresponding cryptogram matrix is calculated using,

$$Z_{ij} = g_1^{r_{ij}} g_1^{v_{ij}}$$

where  $v_i \in [0, 999]$  is the smart meter reading. For the last cryptogram in each row ( $j = m$ ), we set

$$r_{im} = - \sum_{j < m} r_{ij} \quad (5.1)$$

For the last cryptogram in each column ( $i = n$ ), we set

$$r_{nj} = - \sum_{i < n} r_{ij} \quad (5.2)$$

We can easily check that  $r_{nm}$  will be the same calculated either way i.e. is basically a dummy cryptogram which helps in cancellation of random factors. The last  $r_n$  is set such as

$$\sum_{i \in n} \sum_{j \in t} r_{ij} = 0. \quad (5.3)$$

and the corresponding  $R_i$  and  $Z_i$  are calculated. In the 2D matrix  $Z_{ij}$ , the sum across the  $x - axis$  gives us the fine grained load consumption of a neighbourhood, whereas the sum across  $y - axis$  gives us the monthly bill of

a single household.

Correspondingly in Elliptic curve cryptography,  $G_1$  and  $G_2$  are generators of safe elliptic curve *curve25519*. The equations are then converted as follows,

$$R_{ij} = r_{ij} * G_2$$

and the corresponding cryptogram is calculated using,

$$Z_{ij} = [r_{ij} + v_{ij}] * G_1$$

and the condition in equation (5.1) remains the same.

### 5.4.1 Cryptograms with Dynamic Tariffs

Tariffs are represented in the form of matrix of size  $[n * t]$ . Instead of calculating the last ballot in a row  $i$  as

$$r_{in} = - \sum_{j < t} r_{ij} \tag{5.4}$$

if we calculate it as,

$$r_{in} = -a_{it}^{-1} \sum_{j < t} a_{ij} r_{ij} \tag{5.5}$$

then for that row we will have,

$$\sum_{i < n} \sum_{j < t} a_{ij} r_{ij} = 0 \tag{5.6}$$

hence for that row, we have

$$\prod Z_{ij}^{a_{ij}} = g_1^{\sum a_{ij}r_{ij}} * g_1^{\sum a_{ij}v_{ij}} = g_1^{\sum a_{ij}v_{ij}} \quad (5.7)$$

All the last elements of rows and columns are reserved for dummy ballots.

Correspondingly in elliptic curve, eq (5.4),(5.5),(5.6) will be the same, however eq (5.7) will be converted as,

$$\sum a_{ij}Z_{ij} = g_1 \prod (a_{ij} + r_{ij}) + g_1 \prod (a_{ij} + v_{ij}) \quad (5.8)$$

Final result is this:

$$\sum a_{ij}Z_{ij} = g_1 \prod (a_{ij} + v_{ij}) \quad (5.9)$$

## 5.5 Overview of Dataset

The dataset which is used in this thesis is provided by Dataport. Dataport provides us access to the consumer energy consumption data with fine grained smart meter readings. The highest resolution of data collection is per minute. The data is collected from 900 homes located in various states of U.S. such as Texas, Colorado and California. This is the largest dataset of energy consumption publicly available and has been used by various researchers. To preserve privacy, it has been is stripped of the Personal Identifiable Information.

Another dataset of energy disaggregation is the Reference Energy Disaggregation Data Set (REDD). It is available online for free, containing elec-



tricity usage data of 6 households of US recorded over several weeks with a resolution of one second. It also contains high frequency voltage and current readings.

Electricity Consumption and Occupancy (ECO) contains data collected from 6 households of Switzerland over a period of 8 months as shown in Table 5.1. It is also publicly available. It provides aggregate consumption data at the frequency of 1 Hz.

Smart dataset for sustainability is open for public access. It contains electricity usage data from 400+ anonymous homes of US. It also provides environmental and operational data. The electricity usage data is collected at a resolution of one minute.

Datasets			
Name	Origin	Households	Resolution
Dataport	US	707	15min
REDD	US	5	1s
UMASS	US	376	1min
ECO	Switzerland	6	1min

Table 5.1: Overview of Datasets

# Chapter 6

## Implementation and Results

In this chapter, the performance details of the developed prototype for the proposed scheme have been discussed.

### 6.1 Research and Implementation Overview

This scheme is designed mainly to provide a secure billing mechanism for smart meters and also provides a method of sending fine-grained readings for load monitoring to service providers without invading user's privacy. The entities involved in this scheme are: Smart meters (subscribers), Regulators, Electricity Service Provider (ESP). Regulators will help in bootstrapping the system. It will send some information to smart meter for cryptogram generation. Cryptogram will be generated by smart meter using those values. Cryptograms generated in this scheme will be 2D. Smart meter of some defined number of neighborhood will send cryptograms to the ESP. ESP will aggregate these cryptograms in one direction to get the fine grained readings

for load monitoring of the neighborhood. At the end of a month, ESP will aggregate the cryptograms of a single smart meter in the other direction to get its individual bill.

## 6.2 Evaluation

Evaluation and testing is an important part during and after a system is developed.

### 6.2.1 Security Analysis

Our scheme relies on a privacy-preserving primitive termed the cryptogram to encode smart meter readings, which ensures that these readings can only be deciphered within an aggregate set of multiple readings. For purposes of monitoring, the utility will have to aggregate real-time readings for a pre-specified number of subscribers (usually over a neighborhood) to be able to access readings at the individual meter level. The structure of the cryptogram ensures that the utility is not able to link readings to the meters from which they originated.

Moreover, these same individual meter readings may also be aggregated over the duration of a billing period (usually over a month) for billing purposes. In this case, the utility can compute an accurate bill, but is unable to link individual readings to specific instances in time. If dynamic tariffs are operational, the cryptogram itself does not reveal to the utility if the client is availing those tariffs.

The utility therefore is able to monitor energy consumption of groups of

subscribers in real-time and can also undertake accurate customer billing. However, since it cannot link individual readings to originating meters or to specific points in time, the utility cannot profile individual customers beyond any information that may be deduced from the aggregate data itself. It is important to note this qualification: research has revealed that the energy readings of a typical household may be identified in the aggregate if the size of the aggregate set is too small [32].

## 6.2.2 Performance Testing

In this section, the detailed implementation and evaluation of the proposed scheme is discussed. It is implemented on meter readings of different numbers of houses and dedicated cores.

The system which is used for scheme implementation and performance analysis is Core i7 running at 2.60 GHz with 16.0 GB RAM running a 64 bit windows system. The scheme is implemented on a single core, all it's four cores and then on dedicated cores with multiple threads of execution concurrently. This scheme is also implemented on Raspberry Pi 2 simulating smart meters.

In this scheme, the smart meter does not have to store any keys like other schemes. The number of homes with smart meters in a local substation is in few hundred's [58], So, this scheme can be easily implemented.

The smart meter just have to perform some multiplication and addition operations in this scheme. This is within the capabilities of a smart meter. We can categorize it in generic and fast protocol by using parallel program-

ming.

Cryptogram generation time for one smart meter takes 8715 microseconds.

In this case, communication between smart meter and aggregator is not bidirectional. The broker will send certain values to the smart meter for cryptogram generation and then smart meter will use these values and will send cryptogram to the service provider after every 15 minutes.

These graphs are created by applying the proposed scheme on Dataport dataset. This dataset was providing high resolution readings at an interval of 1 minute but we needed the smart meter readings at an interval of 15 minutes as recommended by NIST. So, we applied the formula and changed it to 15 minutes interval. The electricity usage of each smartmeter was in microseconds and we changed it form milliseconds to microseconds. We also organised the electricity consumption of each meter.

Here is some explanation of the functions discussed in these graphs.

**Simple Generation** refers to the function in which simple cryptograms are generated without incorporating tariffs in it.

**Tariff Generation** is a function in which simple cryptograms with tariffs are generated.

**Simple Aggregation** is a function in which cryptograms generated in simple generation process are aggregated to get results.

**Tariff Aggregation** is a function in which cryptograms are generated on the basis of decided tariff policy and aggregated to get results.

**Neighbourhood Aggregation** is the function in which cryptograms of

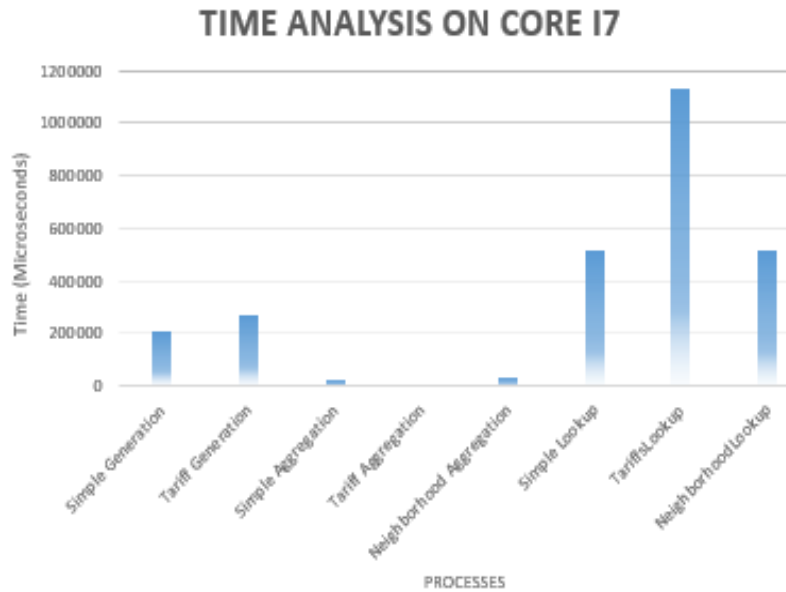


Figure 6.1: Time Analysis on Core i7

different smart meters across a neighbourhood is aggregated.

**Simple Lookup** In Simple Lookup the final value of simple aggregated cryptogram is compared with the pre-computed values stored in file to find out the the final aggregated number.

**Tariff Lookup** In Tariff Lookup the final value of aggregated cryptograms with tariffs is compared with the pre-computed values stored in file to find out the the final aggregated value.

**Neighbourhood Lookup** In Neighbourhood Lookup the final value of Neighbourhood Aggregation is compared with the values stored in file to find out the the final aggregated number.

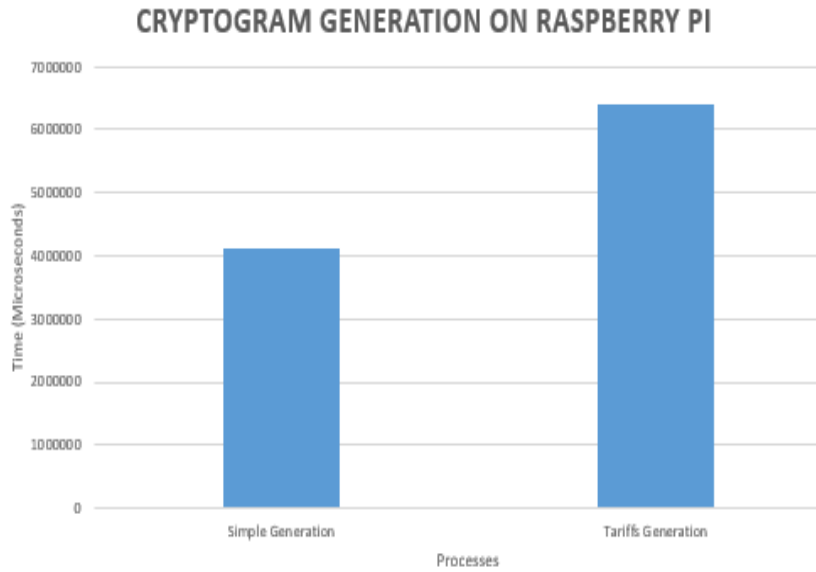


Figure 6.2: Time Analysis on Raspberry Pi

The graph in Fig. 6.1 shows the comparison of various processes of our scheme performed on Core i7 to find out that which process is more time consuming and which one is taking less time. The graph shows that the cryptogram aggregation is taking very less time. The lookup process is taking more time than other processes. Cryptogram generation with tariff is taking more time than other cryptogram generation. Tariff lookup time is taking more time than all other processes.

The graph in Fig.6.2 shows the time of cryptogram generation on Raspberry Pi. It compares the time of cryptogram generated with and without tariffs in microseconds.

The graph in Fig.6.3 shows the time of cryptogram generation for different number of houses. The time taken for the generation of cryptograms for 50 number of houses is 210 microseconds.

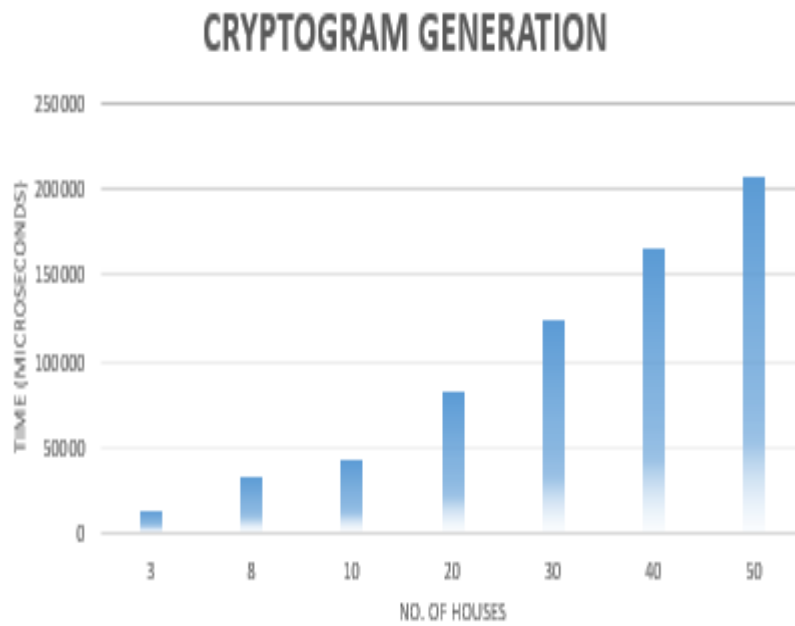


Figure 6.3: Time Analysis of Cryptogram Generation

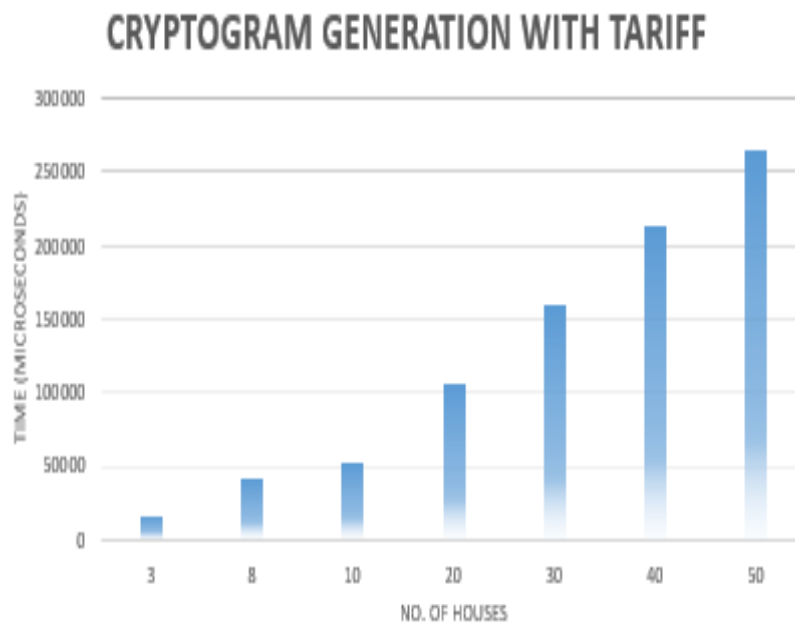


Figure 6.4: Time Analysis of Cryptogram Generation with Tariffs



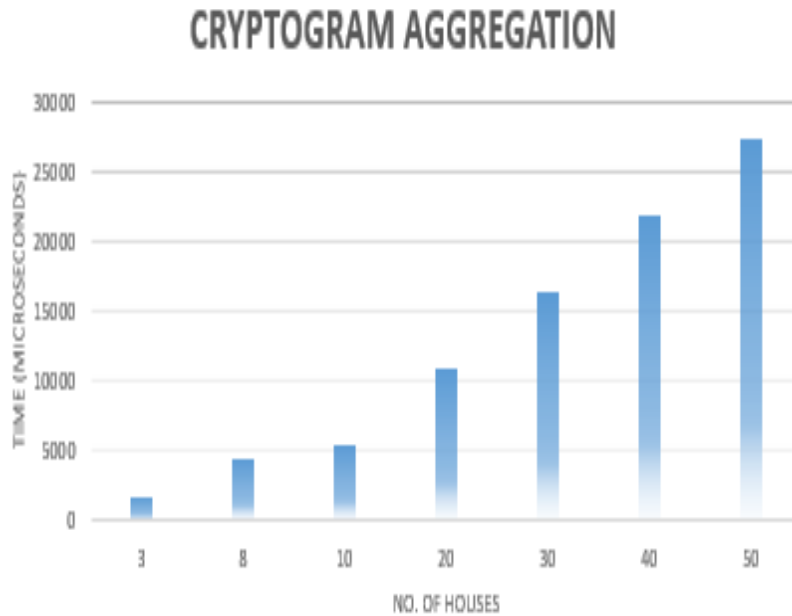


Figure 6.5: Cryptogram Aggregation Time

The graph in Fig.6.4 shows the time of cryptogram generation along with dynamic tariffs for different number of houses. The time complexity with tariffs is nearly same as that of in the case of simple cryptogram generation.

The graph in Fig.6.5 shows the time of cryptogram aggregation for different number of houses. Cryptogram aggregation time is a little bit more than cryptogram generation time.

The graph in Fig.6.6 shows the aggregation time of cryptograms with tariffs for different number of houses. Cryptogram aggregation time with tariffs is more than simple cryptogram aggregation.

The graph in Fig.6.7 shows the aggregation time of cryptogram across neighbourhood for different number of houses.

The graph in Fig.6.8 shows the time of finding the value of cryptogram

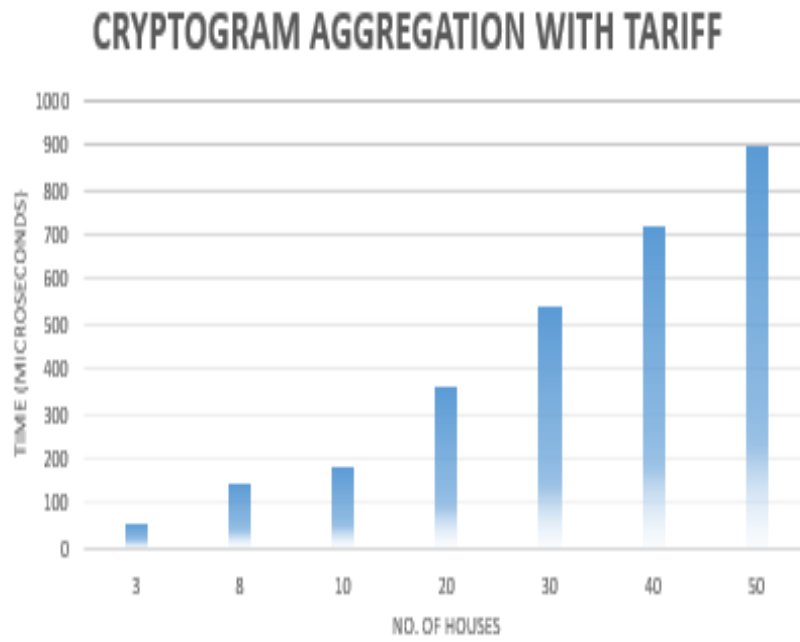


Figure 6.6: Cryptogram Aggregation Time with Tariffs

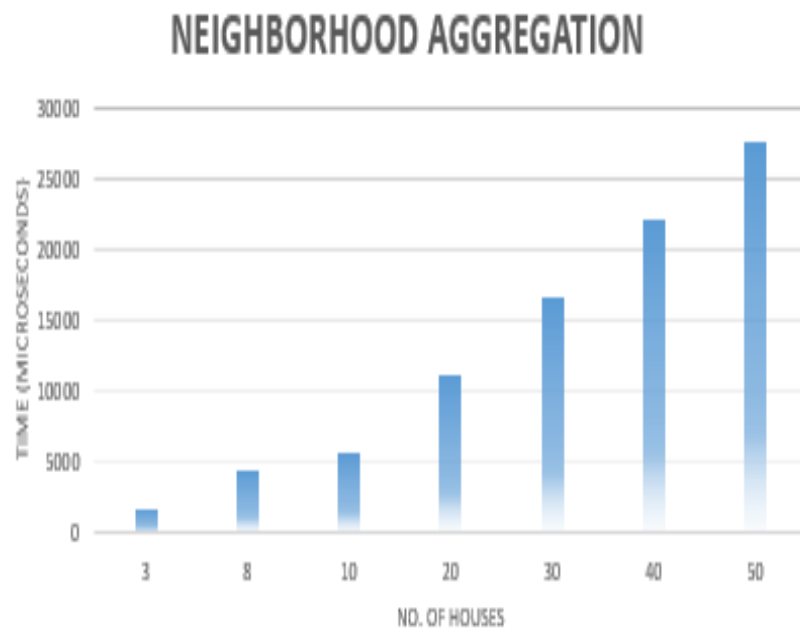


Figure 6.7: Neighborhood Aggregation Time

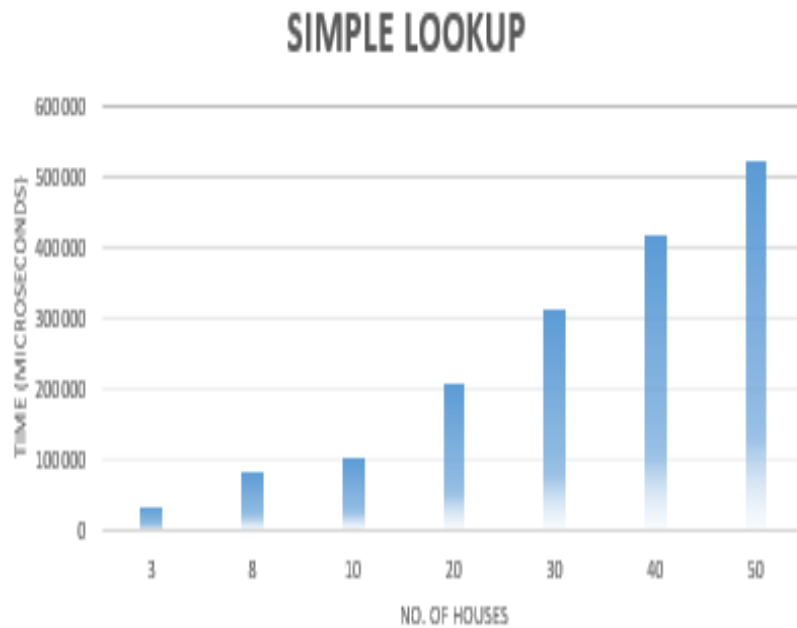


Figure 6.8: Simple Lookup Time

by comparing it with the values stored in file.

The graph in Fig.6.9 shows the time of finding the value of cryptograms with tariff by comparing it with the values stored in file. The tariff lookup time is less as compare to simple lookup time.

The graph in Fig.6.10 shows the time of finding the value of cryptograms aggregated across neighbourhood.

The graph in Fig.6.11 shows the comparison of cryptogram generation and aggregation time. The time complexity of the processes is in this order i.e. cryptogram generation with tariffs, cryptogram generation, cryptogram aggregation with tariffs, cryptogram aggregation and neighbourhood aggregation.

The graph in Fig.6.12 shows the comparison of different lookup times.

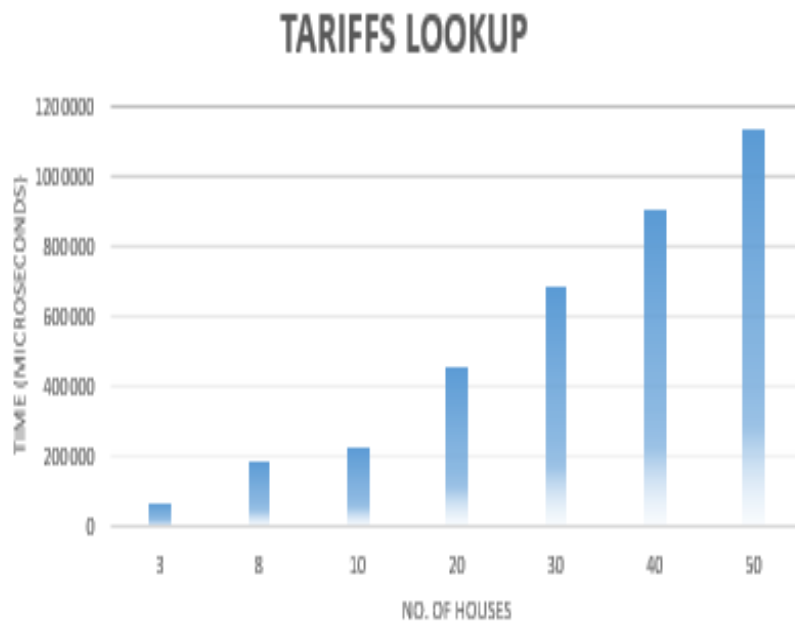


Figure 6.9: Tariffs Lookup Time

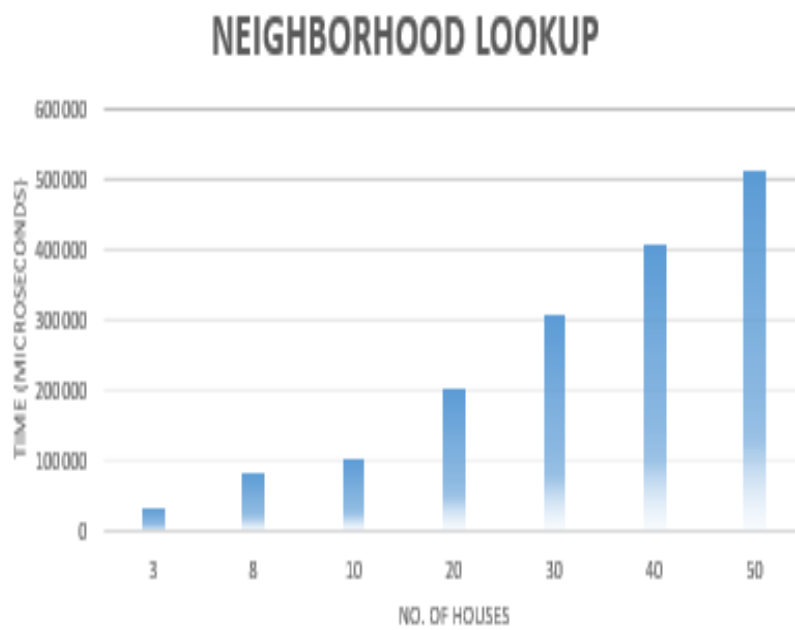


Figure 6.10: Neighborhood Lookup Time

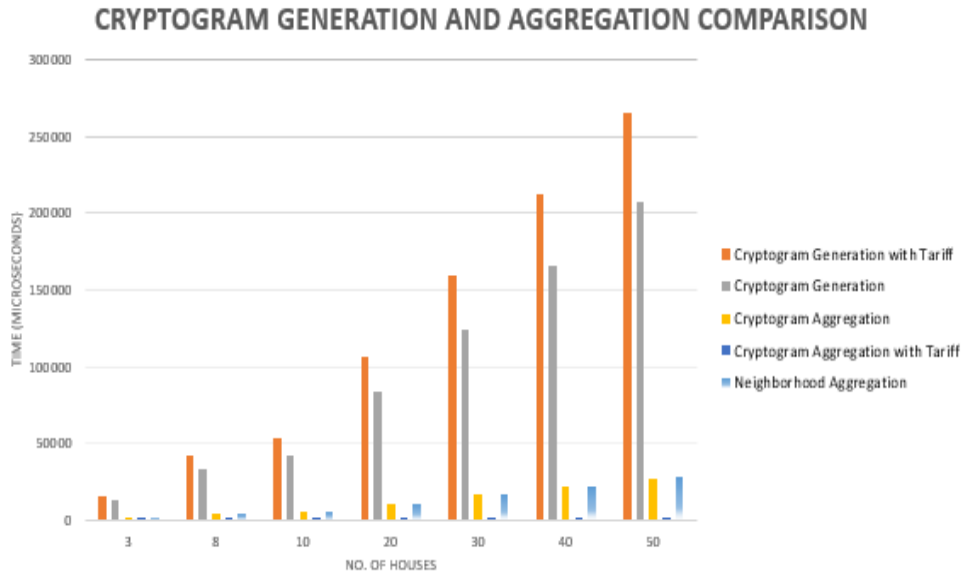


Figure 6.11: Cryptogram Generation and Aggregation Comparison

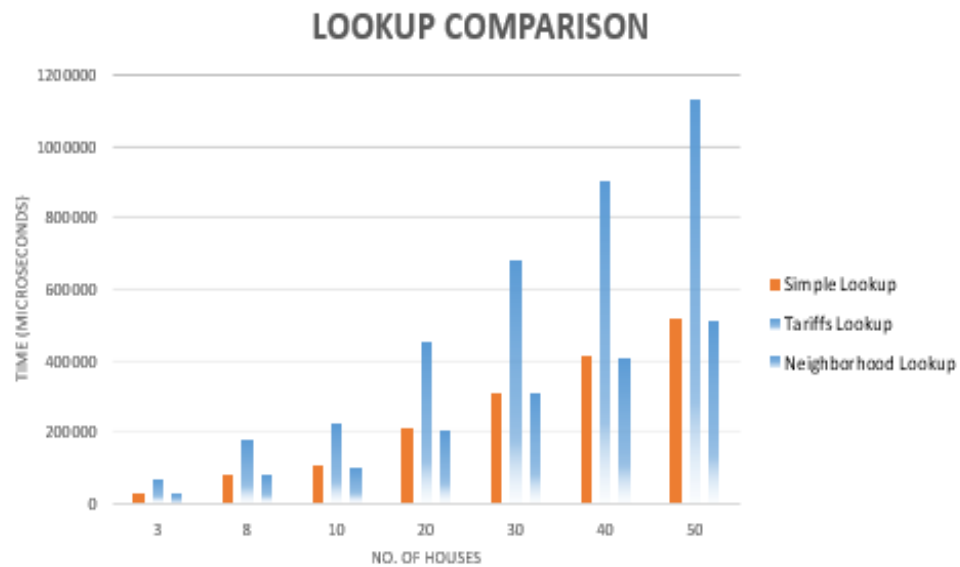


Figure 6.12: Lookup Time Comparison

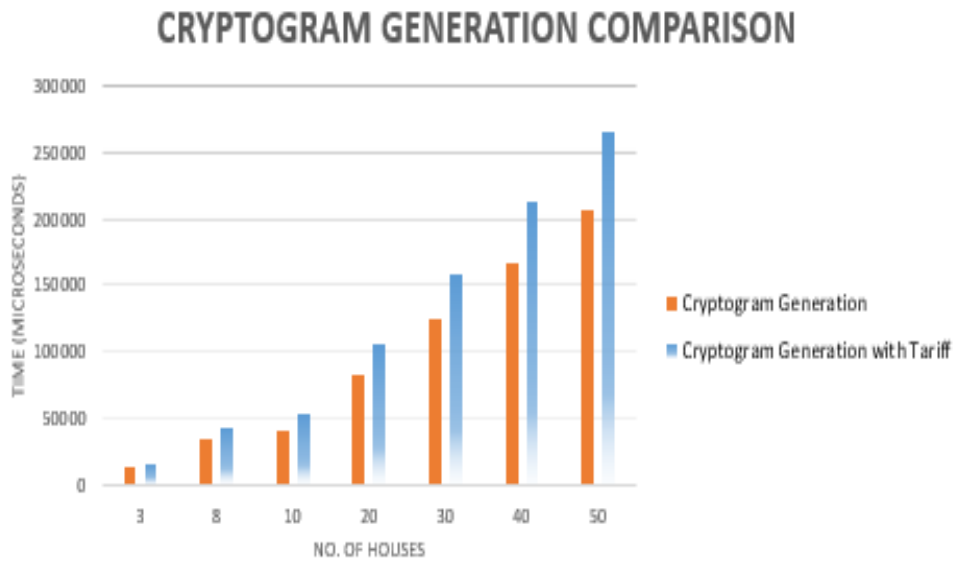


Figure 6.13: Cryptogram Generation Time Comparison

The time complexity of the lookup time is in this order neighbourhood lookup, tariff lookup and simple lookup.

The graph in Fig.6.13 shows the comparison of cryptogram generation times. The cryptogram generation with tariffs is taking more time as compare to simple cryptogram generation.

The graph in Fig.6.14 shows the comparison of cryptogram aggregation times. The time complexity of the aggregation processes is in this order i.e. cryptogram aggregation, neighbourhood aggregation and cryptogram aggregation with tariffs.

The graphs in Fig.6.15, 6.16 and 6.17 shows that lookup time can be comparatively reduced by using parallel programming scheme named threading. We have assigned different range of points in file to different threads for point comparison in lookup process.

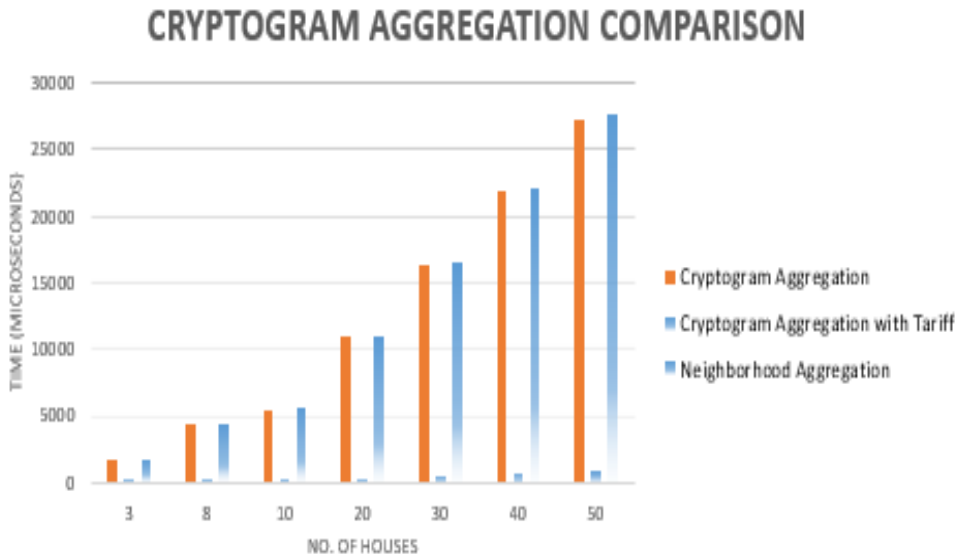


Figure 6.14: Cryptogram Aggregation Time Comparison

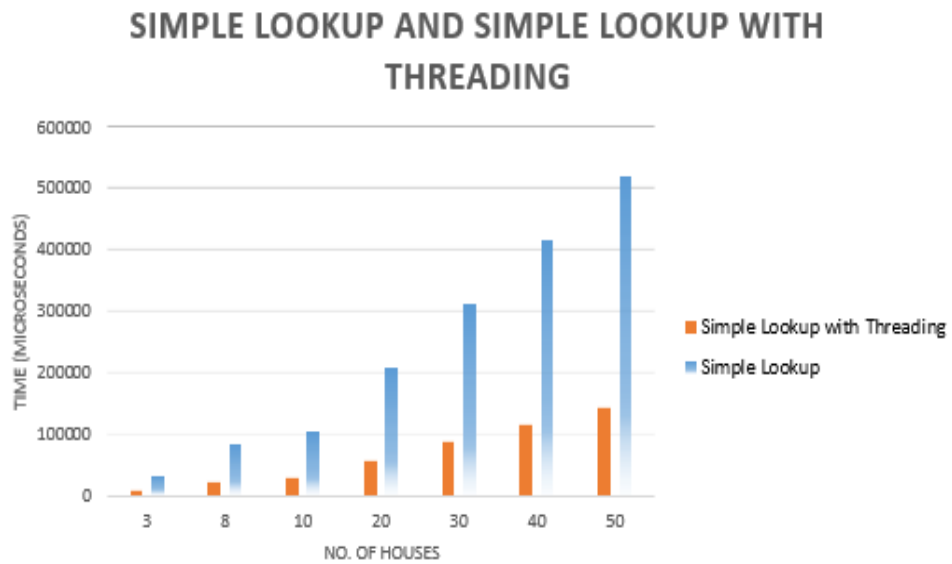


Figure 6.15: Simple Lookup and Simple Lookup with Threading

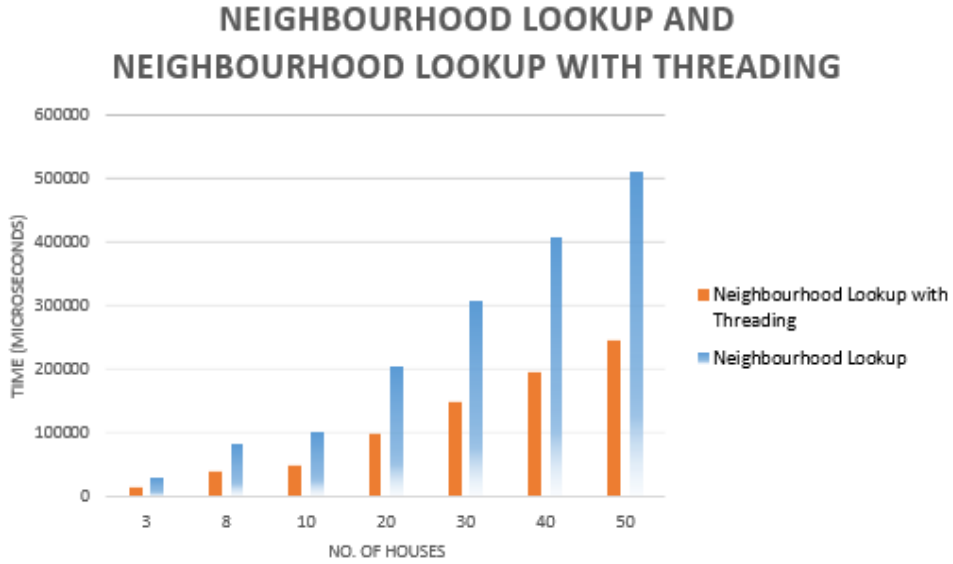


Figure 6.16: Neighbourhood Lookup and Neighbourhood Lookup with Threading

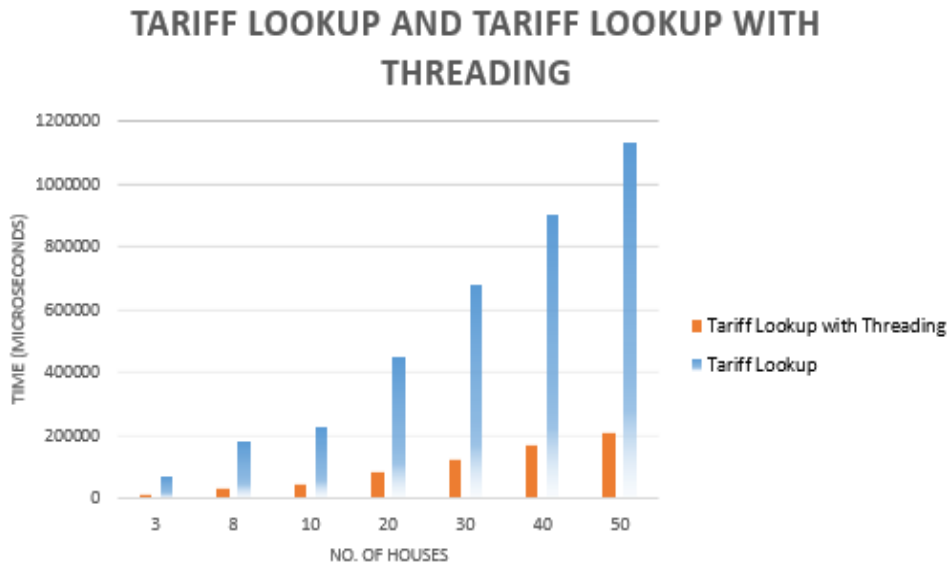


Figure 6.17: Tariff Lookup and Tariff Lookup with Threading



# Chapter 7

## System Analysis

### 7.1 Security Properties

In this section, the security properties of the proposed protocol is discussed, considering the broker and service provider will not collude. These are the main desirable properties that our system provide.

1. Users are Guaranteed privacy: Individual smart meter readings remains fully secret from broker since broker does not receive the smart meter responses. The Utility provider only see encrypted responses which individually does not give any information about individual electricity consumption. Individual responses will only convey meaning when aggregated with other encrypted readings.
2. Utility provider is guaranteed an accurate aggregate: This scheme provides correct aggregate of individual responses to service provider.
3. The users can be sure that the service provider gets no extra infor-

mation other than revealed by the aggregated results. No post facto queries can be executed over the data collected from user's smart meters and any of his life pattern will not be disclosed. Users therefore retain ownership of their data as recommended by GDPR.

4. Verifiability: Any one who receives the bill and cryptogram can verify the correctness of bill.

### **7.1.1 Attack Scenarios**

In this section, various attack scenarios are considered and we have also discussed how our solution can defend against them.

#### **Dishonest Broker**

The broker sends information to smart meter for generation of cryptogram. In our scheme we are just assuming that broker is honest and will not manipulate the results. The broker can try to manipulate this protocol by choosing initial random values that are dependent on one another and can try to embed tracking information into them. However, It is not possible for the Utility Provider to know the response cryptogram unless he colludes with broker. The privacy of customer is not compromised even when broker is deviated from protocol.

#### **Dishonest Utility Provider**

In this protocol the utility provider only has to aggregate the result sent by the smart meters. The utility provider can only run the queries that are

initially agreed upon.

Here, the utility provider is left with only one dishonest strategy that it will aggregate results at smaller set of cryptograms and not on the decided set of cryptograms. It will try to find out the result of smaller subsets, targeting a user or group of users to find out their electricity usage pattern.

## **7.2 Securing the Regulator**

In our protocol, the regulator is trusted not to collude with the utility provider our protocol privacy rely on this assumption. This guarantee can be hardened by distributing the trust among multiple regulators. To get an individual smart meter reading, regulator has to collude with all the regulators. Some Parties like Ofgem or watchdog bodies can be added which are trustworthy. Now smart meter has to contact multiple parties to receive information for the generation of cryptogram.

## **7.3 Securing within the Aggregate**

However, it is prudent to note that the size and the diversity of the aggregate set has to be carefully chosen to guarantee privacy of subscribers. Prior research shows that certain load profiles (e.g. a typical house-hold) may be isolated with very high probability in real-world datasets, and that individual appliances can be identified in small aggregation sets (e.g. 10 households)

## 7.4 An Alternative Mode

The proposed protocol is so lightweight in terms of computation. Broker only sends the necessary data (i.e.  $g_1$ ,  $g_2$  and  $r$ ) for the generation of cryptogram. Smart meter will compute cryptogram itself. There will be no overhead for transmitting all the possible cryptograms. It will save communication bandwidth.

# Chapter 8

## Conclusion & Future Work

### 8.1 Conclusion

In today's world, electricity is the most basic need in our everyday use. Due to the privacy concerns from the consumers, the deployment of future power grid is getting slow. Various techniques have been proposed to protect the user's privacy. In this thesis, we proposed an algorithm for fine-grained Load monitoring and secure electricity billing. It also provides other features like dynamic tariffs, accountability, fault tolerance and selective unmasking of energy readings.

1. Firstly, the security and privacy threats for smart grid's have been studied.
2. We conducted a detailed and thorough literature review of the current research going on in this field.
3. This proposed system based on ECC and Diffie-Hellman is then im-

plemented based on the literature review on Core i7 and Raspberry Pi and then it's performance analysis is carried out on a real electricity dataset. That data was collected from households. It is also evaluated in detail to make sure that security concerns are taken care of.

Our proposed approach is a lightweight scheme, so it is also appropriate for limited-capabilities smart meters in the network. Our proposed scheme guarantees the privacy of consumers. The electricity consumption pattern and personal habits of consumers are concealed from other parties.

## **8.2 Future Work**

There are several directions in which future work can be carried out on this thesis.

1. To apply machine learning algorithm on the proposed cryptogram scheme.
2. This thesis work can be extended on other datasets obtained from other energy sources like water and electricity.
3. To prevent attacks on smart meter itself, research can also be carried out on the physical security of smart meter.

# Bibliography

- [1] F. Li, W. Qiao, H. Sun, H. Wan, J. Wang, Y. Xia, Z. Xu, and P. Zhang, “Smart transmission grid: Vision and framework,” *IEEE transactions on Smart Grid*, vol. 1, no. 2, pp. 168–177, 2010.
- [2] C. Nunez, “Who’s watching? privacy concerns persist as smart meters roll out,” *NATIONAL GEOGRAPHIC NEWS*, pp. –, 2012.
- [3] K. Peachey, “Smart meters will get to star trek phase, says minister,” <https://www.bbc.com/news/business-50232763>, BBC, Oct 2019.
- [4] “Global smart meter market expected to see huge rollout,” <https://www.power-technology.com/comment/global-smart-meter-market-expected-see-huge-rollout/>, Power Technology, September 2018, [Online; accessed 12-October-2019].
- [5] E. McKenna, I. Richardson, and M. Thomson, “Smart meter data: Balancing consumer privacy concerns with legitimate applications,” *Energy Policy*, vol. 41, pp. 807–814, 2012.
- [6] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, “Smart-grid security issues,” *IEEE Security & Privacy*, vol. 8, no. 1, pp. 81–85, 2010.

- [7] M. Melissa and Chicago, “Naperville woman faces down smart power meters,” *Naperville Sun*, pp. –, 2013.
- [8] K. Bode, “Your smart electricity meter can easily spy on you, court ruling warns,” *Motherboard Tech by VICE*, pp. –, 2018.
- [9] P. Collinson, “Is your smart meter spying on you?” *On reflection Energy bills*, pp. –, 2017.
- [10] J. Liao, G. Elafoudi, L. Stankovic, and V. Stankovic, “Non-intrusive appliance load monitoring using low-resolution smart meter data,” in *2014 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2014, pp. 535–540.
- [11] C. Laughman, K. Lee, R. Cox, S. Shaw, S. Leeb, L. Norford, and P. Armstrong, “Power signature analysis,” *IEEE power and energy magazine*, vol. 1, no. 2, pp. 56–63, 2003.
- [12] M.-S. Tsai and Y.-H. Lin, “Modern development of an adaptive non-intrusive appliance load monitoring system in electricity energy conservation,” *Applied Energy*, vol. 96, pp. 55–73, 2012.
- [13] O. Parson, S. Ghosh, M. Weal, and A. Rogers, “An unsupervised training method for non-intrusive appliance load monitoring,” *Artificial Intelligence*, vol. 217, pp. 1–19, 2014.
- [14] U. Greveler, B. Justus, and D. Loehr, “Forensic content detection through power consumption,” in *2012 IEEE International Conference on Communications (ICC)*. IEEE, 2012, pp. 6759–6763.



- [15] T. S. G. I. P. G. C. Committee, “Nistir 7628 rev. 1: Guidelines for smart grid cyber security,” Tech. Rep., 2014.
- [16] “Epic recommends consumer privacy protections for california smart grid,” *epic.org* — *Electronic Privacy Information Center*, 2010.
- [17] “Epic comments on maryland ”smart meter” privacy bill,” *epic.org* — *Electronic Privacy Information Center*, 2018.
- [18] C. Cuijpers and B.-J. Koops, “Smart metering and privacy in europe: lessons from the dutch case,” in *European data protection: coming of age*. Springer, 2013, pp. 269–293.
- [19] F. Staff, “Smart grid consumer privacy seal launch press release,” 2010.
- [20] C. Efthymiou and G. Kalogridis, “Smart grid privacy via anonymization of smart metering data,” in *2010 First IEEE International Conference on Smart Grid Communications*. IEEE, 2010, pp. 238–243.
- [21] F. Diao, F. Zhang, and X. Cheng, “A privacy-preserving smart metering scheme using linkable anonymous credential,” *IEEE Transactions on Smart Grid*, vol. 6, no. 1, pp. 461–467, 2014.
- [22] M. Ambrosin, H. Hosseini, K. Mandal, M. Conti, and R. Poovendran, “Verifiable and privacy-preserving fine-grained data-collection for smart metering,” in *2015 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2015, pp. 655–658.

- [23] G. Ács and C. Castelluccia, “I have a dream!(differentially private smart metering),” in *International Workshop on Information Hiding*. Springer, 2011, pp. 118–132.
- [24] G. Barthe, G. Danezis, B. Grégoire, C. Kunz, and S. Zanella-Beguelin, “Verified computational differential privacy with applications to smart metering,” in *2013 IEEE 26th Computer Security Foundations Symposium*. IEEE, 2013, pp. 287–301.
- [25] Z. Erkin, J. R. Troncoso-Pastoriza, R. L. Lagendijk, and F. Pérez-González, “Privacy-preserving data aggregation in smart metering systems: An overview,” *IEEE Signal Processing Magazine*, vol. 30, no. 2, pp. 75–86, 2013.
- [26] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, “Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1621–1631, 2012.
- [27] Z. Erkin and G. Tsudik, “Private computation of spatial and temporal power consumption with smart meters,” in *International Conference on Applied Cryptography and Network Security*. Springer, 2012, pp. 561–577.
- [28] R. Lu, K. Alharbi, X. Lin, and C. Huang, “A novel privacy-preserving set aggregation scheme for smart grid communications,” in *2015 IEEE global communications conference (GLOBECOM)*. IEEE, 2015, pp. 1–6.

- [29] A. Alsharif, M. Nabil, S. Tonyali, H. Mohammed, M. Mahmoud, and K. Akkaya, “Epic: Efficient privacy-preserving scheme with etoe data integrity and authenticity for ami networks,” *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3309–3321, 2018.
- [30] G. Danezis, C. Fournet, M. Kohlweiss, and S. Zanella-Béguelin, “Smart meter aggregation via secret-sharing,” in *Proceedings of the first ACM workshop on Smart energy grid security*. ACM, 2013, pp. 75–80.
- [31] F. Knirsch, G. Eibl, and D. Engel, “Error-resilient masking approaches for privacy preserving data aggregation,” *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 3351–3361, 2016.
- [32] N. Buescher, S. Boukoros, S. Bauregger, and S. Katzenbeisser, “Two is not enough: Privacy assessment of aggregation schemes in smart metering,” *Proceedings on Privacy Enhancing Technologies*, vol. 2017, no. 4, pp. 198–214, 2017.
- [33] F. Guerrini, “Smart meters: Between economic benefits and privacy concerns,” <https://www.forbes.com/sites/federicoguerrini/2014/06/01/smart-meters-friends-or-foes-between-economic-benefits-and-privacy-concerns/35618a2263a6>, Forbes, June 2014, [Online; accessed 12-October-2019].
- [34] W. Ashford, “Think tank: What are the security implications of putting a smart meter in every uk home?” <https://www.computerweekly.com/opinion/Think-Tank-What-are->

- the-security-implications-of-putting-a-smart-meter-in-every-UK-home, Power Technology, January 2011, [Online; accessed 12-October-2019].
- [35] C. C. of Missouri, “Privacy policies are needed with utility smart meters,” [http://www.stlamerican.com/business/business\\_news/privacy\\_policies\\_are\\_needed\\_with\\_utility\\_smart\\_meters/article\\_646dfd22\\_9b83\\_11e8\\_aaf6\\_cb3855dd5ec4.html](http://www.stlamerican.com/business/business_news/privacy_policies_are_needed_with_utility_smart_meters/article_646dfd22_9b83_11e8_aaf6_cb3855dd5ec4.html), note =, *TheST, LouisAmerican*, August 2018.
- [36] K. Weaver, “Smart meters enable ongoing surveillance of residents,” <https://smartgridawareness.org/2018/01/17/smart-meters-enable-ongoing-surveillance-of-residents/>, Power Technology, January 2018.
- [37] R. Walton, “Smart meter readings are a valid ‘warrantless search,’ court rules,” <https://www.utilitydive.com/news/smart-meter-readings-are-a-valid-warrantless-search-court-rules/530507/>, The ST, Louis American, August 2018.
- [38] “Overview of smart grid technology and its operation and application (for existing power system).”
- [39] T. N. Le, W.-L. Chin, D. K. Truong, T. H. Nguyen, and M. Eissa, “Advanced metering infrastructure based on smart meters in smart grid,” *Smart Metering Technology and Services-Inspirations for Energy Utilities*, 2016.
- [40] D. G. Hart, “Using ami to realize the smart grid,” in *2008 IEEE Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century*. IEEE, 2008, pp. 1–2.

- [41] S. S. S. R. Depuru, L. Wang, and V. Devabhaktuni, “A conceptual design using harmonics to reduce pilfering of electricity,” in *IEEE PES General Meeting*. IEEE, 2010, pp. 1–7.
- [42] J. Schleich, C. Faure, and M. Klobasa, “Persistence of the effects of providing feedback alongside smart metering devices on household electricity demand,” *Energy Policy*, vol. 107, pp. 225–233, 2017.
- [43] S. Darby *et al.*, “The effectiveness of feedback on energy consumption,” *A Review for DEFRA of the Literature on Metering, Billing and direct Displays*, vol. 486, no. 2006, p. 26, 2006.
- [44] S. Evanczuk, “Employing tamper detection and protection in smart meters,” *Electronic Products*, 2015.
- [45] I. Brown, “Britain’s smart meter programme: A case study in privacy by design,” *International Review of Law, Computers & Technology*, vol. 28, no. 2, pp. 172–184, 2014.
- [46] S. S. K.T. Weaver, “How smart meters invade individual privacy,” <https://smartgridawareness.org/privacy-and-data-security/how-smart-meters-invade-individual-privacy/>, Smart Grid Awareness, August 2014, [Online; accessed 12-October-2019].
- [47] T. Zabkowski and K. Gajowniczek, “Smart metering and data privacy issues,” *Information Systems in Management*, vol. 2, no. 3, pp. 239–249, 2013.

- [48] A. Rial, G. Danezis, and M. Kohlweiss, “Privacy-preserving smart metering revisited,” *International Journal of Information Security*, vol. 17, no. 1, pp. 1–31, 2018.
- [49] G. Kalogridis, Z. Fan, and S. Basutkar, “Affordable privacy for home smart meters,” in *2011 IEEE Ninth International Symposium on Parallel and Distributed Processing with Applications Workshops*. IEEE, 2011, pp. 77–84.
- [50] D. Varodayan and A. Khisti, “Smart meter privacy using a rechargeable battery: Minimizing the rate of information leakage,” in *2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2011, pp. 1932–1935.
- [51] H. Shen, M. Zhang, and J. Shen, “Efficient privacy-preserving cube-data aggregation scheme for smart grids,” *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 6, pp. 1369–1381, 2017.
- [52] F. D. Garcia and B. Jacobs, “Privacy-friendly energy-metering via homomorphic encryption,” in *International Workshop on Security and Trust Management*. Springer, 2010, pp. 226–238.
- [53] F. Li and B. Luo, “Preserving data integrity for smart grid data aggregation,” in *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2012, pp. 366–371.
- [54] C.-I. Fan, S.-Y. Huang, and Y.-L. Lai, “Privacy-enhanced data aggregation scheme against internal attackers in smart grid,” *IEEE Transactions on Industrial Informatics*, vol. 10, no. 1, pp. 666–675, 2013.

- [55] Z. Li and G. Gong, “Data aggregation integrity based on homomorphic primitives in sensor networks,” in *International Conference on Ad-Hoc Networks and Wireless*. Springer, 2010, pp. 149–162.
- [56] G. Danezis, M. Kohlweiss, and A. Rial, “Differentially private billing with rebates,” in *International Workshop on Information Hiding*. Springer, 2011, pp. 148–162.
- [57] A. Rial and G. Danezis, “Privacy-preserving smart metering,” in *Proceedings of the 10th annual ACM workshop on Privacy in the electronic society*. ACM, 2011, pp. 49–60.
- [58] W. Jia, H. Zhu, Z. Cao, X. Dong, and C. Xiao, “Human-factor-aware privacy-preserving aggregation in smart grid,” *IEEE Systems Journal*, vol. 8, no. 2, pp. 598–607, 2013.