



**UNIVERSITY OF RWANDA**

**COLLEGE OF SCIENCE AND TECHNOLOGY**

**AFRICAN CENTRE OF EXCELLENCE IN INTERNET OF THINGS (ACEIoT)**

**EFFICIENT CERTIFICATE-LESS PRIVACY-PRESERVING TECHNIQUES  
FOR SECURE SMART GRID NETWORK SYSTEM**

**PhD. Thesis submitted in the fulfilment of requirements for the award of PhD  
Degree in Internet of Things – Wireless Intelligent Sensor Networking**

**Thokozani Felix Vallent**

**AUGUST 2022**





**UNIVERSITY OF RWANDA**

**COLLEGE OF SCIENCE AND TECHNOLOGY**

**AFRICAN CENTRE OF EXCELLENCE IN INTERNET OF THINGS (ACEIoT)**

**EFFICIENT CERTIFICATE-LESS PRIVACY-PRESERVING TECHNIQUES  
FOR SECURE SMART GRID NETWORK SYSTEM**

**PhD. Thesis submitted in the fulfilment of requirements for the award of PhD  
Degree in Internet of Things – Wireless Intelligent Sensor Networking**

**Thokozani Felix Vallent  
Reg. No.: 218014375**

**Main Supervisor: Assoc. Prof. . Mikeka Chomora, PhD  
Co-Supervisor(s): Assoc. Prof. Hanyurwimfura Damien, PhD**

**AUGUST 2022**



## DECLARATION

I do declare that I am the sole author of this and hereby authorize University of Rwanda to lend this to use for scholarly research purposes. Parts of this work have been published in the following publications.

- Efficient Certificate-Less Aggregate Signature Scheme with Conditional Privacy-Preservation for Vehicular Ad Hoc Networks, Enhanced Smart Grid System, published in *Sensors Journal of MDPI*
- Lightweight Privacy-Preserving Data Aggregation Scheme Based on Elliptic Curve Cryptography for Smart Grid Communications, published in *SGIoT EAI-2021 Conference Proceedings*
- Certificate-Less Authenticated Key Agreement Scheme with Anonymity for Smart Grid Communications, published in *Journal of Intelligent & Fuzzy Systems in IOS Press*



---


Copyright@ 2022 by Thokozani Felix Vallent  
All Rights Reserved



## APPROVAL

Thokozani Felix Vallent, a Ph.D. student of UR-ACEIoT, student ID: 218014375, successfully defended the thesis entitled “Efficient Certificate-less Privacy-Preserving Techniques for Secure Smart Grid Network System”, which he prepared after fulfilling the requirements specified in the associated legislations, before the jury whose signatures are below.

**Main Supervisor :** **Assoc. Prof. Chomora Mikeka, PhD**  
University of Malawi

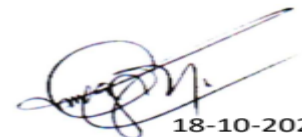


18/10/2022

**Co-Supervisor (s) :** **Assoc. Prof. Damien Hanyurwimfura, PhD**  
University of Rwanda

**Viva Voce Chair :** **Prof. Wali Garba Umalu, PhD**  
University of Rwanda

**External Examiner:** **Assoc. Prof. Udoinyang Godwin Inyang, PhD**  
University of Uyo, Nigeria



18-10-2022

**External Examiner:** **Assoc. Prof. Maiseli Baraka PhD**  
University of Dar Es Salaam, Tanzania



18-10-22

**Date of Defense :** **29/08/22**





## **DEDICATION**

To my beloved ones: mom, sons, relatives I salute you all and dedicate this incredible piece of work made possible because of positive energy and encouragement rendered to me. I cannot help to give respect to the Almighty God, whom I believe raised me up when I was down with studies as well as disturbing life circumstances. To my sons Fortune Vallent and Felix Vallent, I dedicate this work to you and may it incite your inner impetus to achieve even more when your times to advance with school come and I always wish you the best. Likewise, I do dedicate the work to myself for the ability to endure the huddles and all the tough moments passed. May all the hard life experiences serve as lessons to build on to do better in all fore coming endeavors.

*To my spouse and children,*



## ACKNOWLEDGEMENTS

There are many people whom I am indebted to express gratitude to, for all good thing of good intent that they rendered to me during the days of my labor in my studies. In the first place I would like to thank my family and relations for their patience, emotional support and pieces of advice, without which this project would not come to fruition.

In particular, my gratitude goes to my ever-caring mom, Janet Waekha Kulemeka and my lovely wife, Louiser, who stayed with me all along the way of my studies culminating to more than four years of rigorous research, regardless of the impeding huddles that I encountered. I salute the positive energy and encouragement they rendered unto me.

I am equally grateful to my supervisors, Prof. Chomora Mikeka and Dr Damien Hanyurwimfura for their valuable insights and guidance on how to proceed with my studies. On special note, I am very thankful to Dr Damien Hanyurwimfura's for his recommendation in relation to journal publications and good authorship practices he has been guiding me. All sorts of surmountable help rendered to me during my studies from different people in different scenarios eased my stress and anguish of seeking for solutions, of which revamped my energy in unexpected ways. I will always be grateful and remember the assistance I received in various forms from the officials of ACEIoT, CST of University of Rwanda from different areas like administration, PhD program coordination etc.

I sincerely thank my colleagues, friends and other well-wishers who sharpened my work through fruitful discussions in the area of my studies.

I am also indebted to express my gratitude to Prof. Hyunsung Kim, for constant support, inspiration and guidance whenever I needed technical support during my studies, I am very thankful for all your inputs professor.



## FOREWORD

The ever increasing digitization of all the operations of the grid has led to the birth of the smart grid (SG), which is an electricity grid equipped with bi-direction flow of both electrical energy and information. The system is empowered with smart devices throughout its segments that utilizes intelligent communication capabilities for different services and applications. However, the high frequency of communication renders the system prone to cyber-attacks as the medium of communication is over a public channel. Therefore, provision of security by design is the ultimate solution to safeguard the SG as it is a critical infrastructure. Nevertheless, the solutions is employed by using cryptographic measures which involve mathematical techniques to realize desirable standards for security, such as data confidentiality, authentication and integrity to prevent cyber-attacks. Various researches have endeavored to address the security and privacy concerns existent in different application scenarios of SG. However, the challenge of balancing between system efficiency and robust security provision rises. For instance, many schemes in SG communication are prone to common attacks or are based on computational intensive mathematical operations. Thus, this work aims at addressing these cyber-concerns with cryptosystems based on elliptic curve cryptography. Elliptic curves are choicest mathematical structures for security designs because their keys have small sizes, and subsequently have reduced storage and transmission requirements. The realization of these security features is based on either public key or private key cryptography or a combination of both, which is called asymmetric cryptography. By using asymmetric cryptography we designed certificate-less cryptosystem to achieve privacy preserving data aggregation and anonymous key agreement in an internet of things (IoT) enhanced SG that removes key escrow problems for the trusted anchor. The proposed schemes have significant comparative advantages over relevant related works in the sense of achieving robust security with optimal computation and communication overhead. The merits of the work are validated by the determination of formal security proofs and performance evaluation respectively.

AUGUST / 2022

Thokozani Felix Vallent



# Contents

<b>Declaration</b>	<b>iii</b>
<b>Approval Page</b>	<b>iv</b>
<b>Dedication</b>	<b>v</b>
<b>Acknowledgements</b>	<b>vii</b>
<b>Foreword</b>	<b>ix</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Generic System Architecture for Smart Grid . . . . .	3
1.2 Problem Statement . . . . .	6
1.3 Research Aim and Objectives . . . . .	7
1.4 Mathematical Primitives . . . . .	7
1.5 Outline of the Thesis . . . . .	8
<b>2 Efficient Certificate-less Aggregate Signature Scheme with Conditional Privacy-Preservation for Vehicular Ad Hoc Networks Enhanced Smart Grid System</b>	<b>9</b>
2.1 Introduction . . . . .	9
2.2 Related Works and Limitations . . . . .	12
2.2.1 System Model . . . . .	13
2.2.2 Security Model for CLAS Scheme . . . . .	14
2.3 The Proposed Certificate-less Aggregate Signature Scheme . . . . .	15
2.4 Analyses . . . . .	20
2.4.1 Security Proof . . . . .	20
2.4.2 Security and Privacy-Preservation Analyses . . . . .	24
2.4.3 Performance Evaluation . . . . .	26
2.5 Summary . . . . .	33
<b>3 Certificate-less Authenticated Key Agreement Scheme with Anonymity for Smart Grid Communications</b>	<b>35</b>
3.1 Introduction . . . . .	35

3.2	Related Works and Limitations . . . . .	37
3.3	Preliminaries . . . . .	38
3.4	The Proposed CL-AKA scheme for Smart Grid . . . . .	39
3.4.1	System Initialization Phase . . . . .	39
3.4.2	Entity Registration Phase . . . . .	40
3.4.3	Entity Self Key Generation Phase . . . . .	41
3.4.4	Authenticated Key Agreement Phase . . . . .	41
3.5	Security Analysis and Performance Evaluation . . . . .	43
3.5.1	Informal Security Analysis . . . . .	47
3.5.2	Comparison Analysis . . . . .	48
3.5.3	Security and Functionality Features Comparison . . . . .	49
3.5.4	Computation Cost Analysis . . . . .	50
3.5.5	Communication Cost Analysis . . . . .	53
3.6	Summary . . . . .	54
<b>4</b>	<b>Lightweight Privacy-Preserving Data Aggregation Scheme Based on Elliptic Curve Cryptography for Smart Grid Communications</b>	<b>55</b>
4.1	Introduction . . . . .	55
4.2	Related Works and Limitations . . . . .	57
4.2.1	Generic System Model . . . . .	59
4.2.2	Adversary Model . . . . .	61
4.2.3	Security Requirements . . . . .	61
4.3	Proposed Scheme . . . . .	62
4.4	Security Analysis and performance Evaluation . . . . .	69
4.4.1	Security Requirements Analysis . . . . .	69
4.4.2	Performance Evaluation . . . . .	71
4.4.3	Computation Cost . . . . .	72
4.4.4	Communication Cost . . . . .	77
4.5	Summary . . . . .	80
<b>5</b>	<b>Contribution to Knowledge, Conclusion and Future Works</b>	<b>83</b>
5.1	Contribution to the Current State of Knowledge . . . . .	83
5.2	Conclusion . . . . .	84
5.3	Future Works . . . . .	84
<b>A</b>	<b>List of Publications</b>	<b>103</b>



# List of Figures

1.1	Generic System Architecture for Smart Grid . . . . .	4
2.1	Two Layered VANETs Architecture. . . . .	13
2.2	TA set up system parameters . . . . .	16
2.3	TRA and KGC collaborates to generate partial private key . . . . .	17
2.4	Signature generation and aggregation . . . . .	18
2.5	Computation Cost Comparison Per Unit. . . . .	31
2.6	Verification Time Delays and Number of Signatures Relationship. . . . .	32
3.1	CL-AKA hierarchical communication model . . . . .	41
3.2	CL-AKA three phases summary diagram. . . . .	42
3.3	The session key establishment between SM and SP . . . . .	43
4.1	Generic System Model. . . . .	60
4.2	System initialization phase . . . . .	64
4.3	Private and public key generation phase . . . . .	65
4.4	Smart meter electricity reporting process . . . . .	66
4.5	Computation Cost for the Schemes. . . . .	78
4.6	Communication Cost for the Schemes. . . . .	80



# List of Tables

2.1	Notations Used in the Proposed Scheme . . . . .	14
2.2	Comparison Analysis of Security Features Satisfied . . . . .	27
2.3	Execution Times of Cryptographic Operations . . . . .	27
2.4	Comparison of Computation Cost for Related CLAS Schemes . . . . .	29
2.5	Communication Overhead Summary . . . . .	33
3.1	Notations Used in the Proposed Scheme . . . . .	40
3.2	Comparison Analysis of Security Features Satisfied . . . . .	49
3.3	Execution Times for Cryptographic Operations . . . . .	50
3.4	Comparison of Computation Cost in <i>ms</i> for Authentication & Key Agreement . . . . .	52
3.5	Communication cost comparison table for authentication and key agreement . . . . .	53
4.1	Notations Used in our Scheme . . . . .	63
4.2	Security Comparison . . . . .	72
4.3	Estimated Running Times for Different Operations in milliseconds ( <i>ms</i> ) Averaged after 1000 runs . . . . .	73
4.4	Communication Cost of SM-DAP and DAP-OC Transmissions . . . . .	79



# List of Abbreviations

3DES	Triple Data Encryption Algorithm
AES	Advanced Encryption Standard
AMI	Advanced Metering Infrastructure
BPL	Broadband over Power Line
CC	Control Center
CLAS	Certificate-Less Aggregate Signature
CRL	Certificate Revocation List
DAP	Data Aggregation Point
DCUs	Data Collection Units
DDoS	Distributed Denial of Service
DoS	Denial of Service
DR	Demand Response
DSL	Digital Subscriber Line
DSM	Demand Side Management
DSRC	Dedicated Short Range Communication
ECC	Elliptic Curve Cryptography
ECCDH	Elliptic Curve Computational Diffie-Hellman
ECDDH	Elliptic Curve Decisional Diffie-Hellman
ECDL	Elliptic Discrete Logarithm
eCK	extended Canetti–Krawczyk

EVs	Electric Vehicles
FDI	False Data Injection
G2V	Grid-to-Vehicle
GPS	Global Positioning System
HAN	Home Area Network
HE	Homomorphic Encryption
IEDs	Intelligent Electronic Devices
IP	Internet Protocol
ITS	Intelligent Transportation Systems
KGC	Key Generation Center
LPWAN	Low Power Wide Area Network
M2M	Machine-to-Machine
MANETs	Mobile Ad Hoc Networks
NANs	neighborhood area networks
NIST	National Institute of Standards and Technology
OBUs	On-Board Units
OC	Operation Center
PDCs	Phasor Data Concentrators
PHEVs	Plug-In-Hybrid-Electric Vehicles
PKI	Public Key Infrastructure
PLCs	Programmable Logic Controllers
PMUs	Phasor Measurement Units
RSA	Rivest-Shamir-Adleman
RSUs	Road Sign Units
SM	Smart Meter
TA	Trusted Authority

*List of Abbreviations*

TPD	Tamper-Proof Devices
TRA	Tracing Authority
TTP	Trusted Third Party
V2G	vehicle-to-grid
V2V	Vehicle-to-Vehicle
VANETs	vehicular Ad Hoc Networks
WAMS	Wide Area Monitoring Systems
WASA	Wide-Area Situational Awareness
WSN	Wireless Sensor Network





# Chapter 1

## Introduction

Smart grid (SG) is a digital communication based technology that detect and react to real time changes in the energy supply system enabled by distributed intelligent devices collaborating in an Internet of Things (IoT) manner for various automated services. The interplay of smart devices forms an intelligent system that is open to versatile applications, besides mere generation of energy. In this way various inter-operable intelligent devices are planted all the way from the generation, through to transmission up to distribution of power to the end consumer. So smart grid uses digital communication technology to detect and react to changes in near real-time throughout the energy supply chain segments. The coordination of these integrated intelligent devices empowers the system to be most reliable, responsive and resilient to faults occurrences, self-healing, efficient, sustainable and ensures provision of clean energy [1–4]. Thus, the development of smart grid has attracted multifaceted technologies that ensure power system planning, optimal system operations. An example of peripheral technologies to smart grid relates to distributed energy resources, electric vehicles, consumer managements among others. The smart grid has transformative advantages to the traditional grid in numerous ways. The on going transformation is enhanced with IoT integration by utilizing the information obtained from the devices to achieve various real-time based system monitoring [5]. Smart grid ensures power quality, reliability, increases consumer choice, resilience, integration of distributed energy resources and improves efficiency of existing network systems [1, 6, 7]. So this great feature of the grid of connecting the components of the electricity grid via communication networks, such as Internet or wireless sensor networks, IoT, to gather data about the grid's status and ensuring satisfaction of consumer needs has engendered the birth of network based digital technologies in smart grid operations.

The advent of these versatile technologies are now very useful in incorporation of environmental friendly alternative energy sources of which have variable power output like solar energy, wind energy and other variable sources like plug-in-hybrid-electric vehicles (PHEVs) . One such roadway energy source is on the utilization of energy harvesting systems by electric vehicles (EVs) from the solar radiation or mechanical vibrations induced by passing vehicles [8]. By utilizing various energy sources, smart

grid system overcomes the restriction of a single source-based energy system thereby circumventing either intermittent or low power generation [9, 10]. In this way the grid is able to warrant a balanced electricity levels by means of incorporating various distributed energy sources [11].

The real-time system monitoring is empowered by two-way flow of information and electricity and this in turn ensures, equilibrium energy balance and energy conservation, thereby assuring sustainable energy supply. So smart Grid is an improved grid enhanced with intelligent decision making in its operations and applications. Due to this two way communication, the utility provider and the consumer stay in touch and cooperatively co-work in all matters concerning system monitoring and control. This intelligent system awareness is an enabling factor for incorporation and emergency or other versatile smart technologies like renewable energy injection into the system, electricity energy storage and microgrids, and vehicular ad hoc networks (VANETs) technology into SG [12, 13]. Beyond electricity management according to supply demand by utilizing sensors, SG has many more advantage which are no longer a fantasy but a reality for modern grid system. Thus, SG is advantageous in so many ways as it can integrate isolated technologies that enables energy management, carbon emission reduction by incorporation of distributed energy resources, broaden electricity generation to meet the ever increasing demand of power and seamless fault detection. These applications of the grid enhances electricity generation and distribution in optimal ways. For instance, there is huge saving of electricity wastage by demand response services. Demand response (DR) is the effective way of balancing of electricity generation against demand, is achieved by liaising with customer side to reduce consumption during peak demand or system emergency to ensure stable power supply [14]. In demand response, customers are encouraged to use high intense consumption electrical appliances during off peak periods with attractively low tariffs on such time intervals. In smart grid technology, EVs can also be used as generation source as well as temporary storage infrastructure [15]. So electricity can ply between vehicles to the grid and vice-versa in accordance to the interplay of demand and supply. In this sense, the exchange of electricity among vehicles in recharging/discharging is applied to VANETs for location based services related electricity supply. Consequently, there is communication for electricity related services for purposes of regulating energy reserves, storage, selling out in vehicle-to-grid (V2G) or Vehicle-to-Vehicle (V2V) , energy transmission from the grid-to-vehicle (G2V) , but we will refer to both as V2G communications for simplicity. However, the V2G communications encounter cyber-threats in relation to malicious disclosure of the identity or location of the EV's owner identity as well as being prone to denial of service (DoS) attacks.

However, the biggest concern in realization of the full potential of SG pertains to information security and privacy-preservation, due to the usage of smart automated devices which communicate between power providers, services providers and the consumer. Obviously, the system would fall prey to malicious parties wishing to hack and take control of system activities for monetary gain [4, 16]. Since smart grid faces various challenges during this initial stages such as installation and implementation not limited

## 1.1. *Generic System Architecture for Smart Grid*

to, network latency, interoperability and scalability issues, and reliable cyber-security fortification [17]. This calls for cyber-security solutions that safeguards the grid operations in different ways according to user or operations specifications. For example, there is need to provide robust authenticated key agreement mechanisms that ensures secure communications of concerned entities in the grid [18]. Furthermore, secure lightweight data aggregation schemes that ensure efficient communication with significant bandwidth optimization are also needed. Improving the techniques to include aspects of privacy-preservation, efficient and certificate-less is most desirable according to many smart grid application areas. Thus, it is against this background that our work indulges to provide an adequate solution for secure management and adoption of the smart grid, reflecting the advanced applications of the unified NIST smart grid system model [19].

## 1.1 Generic System Architecture for Smart Grid

The smart grid system is fast growing and incorporates many multifaceted technologies by intertwining electrical and digital communication. Since smart grid is capable of providing electrical power from multiple and wide variety of distributed sources such as wind energy, solar power systems, and perhaps even PHEVs, it has captured research interest from academia and the industrial sector to ensure its full adoption. All these functionalities of smart grid are facilitated by bi-direction flow of information or are there to support the bi-direction flow of electrical energy for system decision making or monitoring purposes. The smartness in smart grid is enabled by key technologies throughout the supply chain of electricity such as: smart appliances at home area network (HAN) , smart meter (SM), smart substations, super conducting cables, phaser measurement units (PMUs) , integrated communication media. Of greater interest in this research are matters pertaining to information communication of different entities in the grid. Integrated communication technology is central to the real-time needs of the system and normal operations. Depending on the application scenario, bandwidth requirements and the segment of the grid different communication technologies are employed like wireless or wired communication technologies. In terms of wireless technologies WiFi, Zigbee, blue-tooth, Wi-max and other Low Power Wide Area Network (LPWAN) protocols are used whereas technologies such as fixed lines, Fiber optic, Programmable Logic Controllers (PLCs) , Broadband over Power Line (BPL) , Digital Subscriber Line (DSL) . To ensure smooth implementation of integrated communication technologies special consideration should be given to related issues that arise which are the ease of deployment, the latency factor, data carrying capacity, security, privacy-preservation, network coverage capability, standards and interoperability. The bearing of this work falls around the security, privacy-preservation and communication latency reduction aspects.

The system architecture of the grid comprises of power grid system and the information communication systems as depicted in Figure. 1.1 that is based on the NIST reference model of the standard architecture [20]. Overall the architecture has seven

main inter-operable domains altogether which are: the bulk generation, transmission, distribution, customer, service provider, market and operations domains. So these domains functions are based on communication and smart sensor technologies. However, communication systems comes with the drawback of cyber-security threats associated with the Internet and all wireless communications. Cyber-security is a complex field of its own that involves the organization and collection of resources, processes, and structures used to protect network systems and critical infrastructure from digital attacks [21]. Subsequently, smart grid falls prey to malicious adversaries existing on all public channels capable of eavesdropping, doing data modification jamming system control messages or causing high scale system failure.

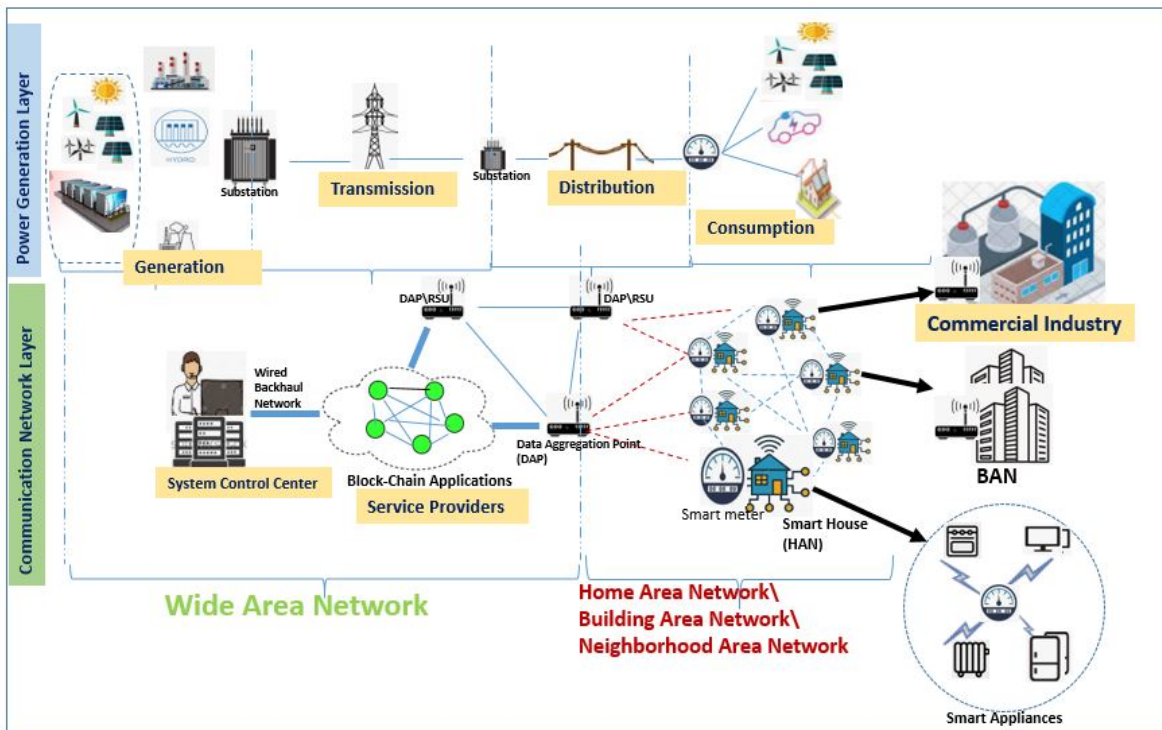


Figure 1.1: Generic System Architecture for Smart Grid

The importance of information security and privacy-preservation in smart grid applications cannot be overemphasized as it is a critical infrastructure operating in an insecure communication channel. This is the major reason why there is need to achieve security by design for concerned network environment. To this tune, several research works have been done in a quest to provide privacy-preservation as well as security for smart grid communications. So its a general challenge to first resolve the cyber-security vulnerabilities that put smart grid at high risk with the specific of Distributed Denial of Service (DDoS) attack to impede execution of some services to users, false data injection(FDI) to dupe the grid of the actual status information. Thus, the grid's threat model that arises can be categorized into the following major areas of concern.

## 1.1. Generic System Architecture for Smart Grid

- *User privacy concerns:* Its a concern to protect the customer's identity as well as the confidentiality of the transmitted data in SG. For instance, by using data analysis tools an adversary would extract personal information of users like what appliances are mostly used and at what times. This breaches in customer's information privacy can be used maliciously by an adversary like to plan house breaking when users are not there. For industrial customers, an adversary can learn about production line pattern, which is vital information to be sold maliciously to company's competitors. This entails customer privacy and data confidentiality are aspects that must be satisfied in the grid.
- *Data integrity concern:* As the adversary has full control of the channel of communication, she is capable of manipulating or modifying data in transmission between intended parties in the grid. This can either be done by a dishonesty customer attempting electricity consumption data forgery to fraudulently pay lower bills. The adversary can as well carry out FDI attacks on distributed measurement units to spread misleading false information about the status of the grid to lead stray the control center into irregular decision making. This ultimately and largely disturbs overall system operations, there by affecting normal service delivery.
- *System resource availability concerns:* An adversary here indulges to make the services unavailable to legal users in DoD or DDoS attacks. The adversary undermines system to affect its performance capacity by means of blocking, delaying or spoiling AIM information in an attempt to make services unavailable to users in the grid. This attack is typically present in wireless networks where the access point can be flooded with interrupting signal [22, 23].

It is generally understood in the research world and industry that the integration of communication technologies to the grid operations give rise to cyber-security challenges already existing in related communication technologies. So the grid risks from data integrity, identity and data confidentiality, network resource availability as well as information availability. Thus, the scope of this work is concentrated on developing the cyber-security solutions modeled to address specific security requirements for specific communications and applications in SG, posing threat to the entire smart grid unified conceptual reference model [24]. Therefore, this research work focuses on addressing the cyber-security challenges present in the SG networks applications in three distinct scenarios, by designing efficient and robust practical cryptographic techniques. The proposed works leverage the grid of excess computation overhead thereby ensures provision of security while improving the SG network performance due to elimination of system latency, of which can negatively affect grid operations. Details of the specific solutions and different application areas of the grid are discussed in appropriate chapters ahead.

## 1.2 Problem Statement

Although the advancement of wireless sensor network communication technologies in smart grid enables two-way flow of both electricity and information, it tends to open up the system to cyber-security vulnerabilities which obstructs normal operation of the system. As SG technology employs Internet Protocol (IP) empowered by bi-directional communication, it is therefore inherently susceptible to all sorts of cyber-security threats in terms of privacy and security breach. This research work seeks to design suitable schemes in safeguarding smart grid infrastructure in application technologies like VANETs communications, service provider and customer advanced metering infrastructure (AMI) communications. This work utilizes the merits of elliptic curve algebraic structure over finite fields as the fundamental building blocks for efficient security provision. The elliptic curve approach is choicest security primitive, forbearing its security advantages over mere finite field cryptographic approaches. So the goal is to achieve overall system fluidity in communication by avoiding unnecessary latency effects as a result of heavier computation operations used when designing security mechanisms in SG applications [25]. So this work seeks to provide robust security and privacy-preservation mechanisms in smart grid communications. Such mechanisms should be applied in practical operations and applications such as electricity reading aggregation, regulation of AMI commands between the smart meter (SM) and the control center (CC) side. There are different techniques of ensuring security in SG such as, security provision by hardware fortification like firstly usage of tamper resistant devices to manually conceal the secret credentials and data. This approach is however, disadvantageous to deploy for each and everyone of the milliard devices in the system. A second mechanism is by applying signal distortion functions on the transmitted data, which will be recovered back by the receiver. However, the draw back in this technique is the involvement of complex data mining reversal operations. Indirectly, this research work assists in availability of quality electricity since a secure grid ensures multiple sources of renewable energy integration into the grid such as solar, wind, and other sources of clean energy. In a nutshell, all desirable services of smart grid will be realized once the security and privacy protection in smart grid is guaranteed. On the other hand, cryptographic techniques are employed to ascertain data and identity security and privacy. Thus, various public key security model have already been proposed in different studies to provide the security requirements for safe communication. Commonly, these models employ bilinear pairings, homomorphism, paillier cryptosystems to achieve the sought after security and privacy-preservation [26]. However, some of the technique bear the high computation and communication complexity drawback, which is not ideal for resource constrained devices glutted, ubiquitous computing network like SG. Therefore, it is imperative to save the network latency effect by employing computational and communication overhead friendly security approaches to leverage the smart grid of excess network costs [26, 27].

## 1.3 Research Aim and Objectives

The main aim of this study is to address cyber-security challenges by devising optimally efficient secure and privacy-preserving cryptographic schemes in AMI and other user side wireless sensor network or IoT integrated applications in smart grid network.

1. To Design a practically efficient and secure certificate-less privacy-preserving communication model for real-time smart grid applications in vehicular ad hoc networks (VANETs) and demand-side management (DSM) applications, that supports overall system regulation against dishonest actors.
2. To devise an efficient asymmetric anonymous key exchange model for secure AMI data communication in smart grid that precludes escrow powers of a trusted anchor of the system. This intends to rigidly upholds the communications, free of breaches with respect to data integrity, user identity security as well as confidentiality by any other malicious party emerging as privileged inside attacker or ordinary ones.
3. To develop an efficient privacy-preserving key agreement or data aggregation model for energy usage reporting in SG with ideal bandwidth consumption to resolve overall system latency effects due to high generation of network data.

In line with the aforementioned objectives, this research develops secure communication models for user side applications and AMIs in SG. The scheme's construction will be clearly presented and validated based on formal and informal security analysis. Furthermore, a performance evaluation comparison with most related relevant works will be conducted to underpin the achievement of significant efficiency, reliability and robustness as highlighted.

## 1.4 Mathematical Primitives

The whole work discussed in this research is based on elliptic curve cryptography (ECC), which is a public key cryptosystem based on elliptic curve theory which has well known advantage of being a structure for faster and more efficient cryptosystems with robust security. Koblitz and Miller designed ECC to be applied in resource constrained environments [28, 29], and it is the choicest cryptographic primitive in pre-quantum cryptography era. ECC cryptosystems have low computational requirement and uses short keys whilst achieving equivalent security as RSA algorithm with very small key size. As such ECC saves on key storage capacity and has reduced processing overhead by default [30]. Its properties are therefore viable for securing resource constrained network systems that require seamless and real-time operations like IoT and SG system[31].

*Elliptic curve:* Given a prime number  $q$ , the equation  $y^3 = x^2 + ax + b \text{ mod } p$  defines an elliptic curve over a prime field  $E(F_p)$ , where  $p > 3, a, b \in F_q$  and satisfies

$\Delta = 4a^3 + 27b^2 \neq 0 \pmod{p}$ . The points on  $F_p$  together with the point at infinity  $\mathcal{O}$  form an additive cyclic group  $G$ . Let  $P$  be the generator point of order  $n$ , the scalar multiple operation is defined as,  $nP = P + P + \dots + P$ ,  $n$  times addition, where  $n \in Z_q^*$ , is a positive integer. So, there are a number of intractable problems in an elliptic curve group  $G$  of order  $n$ , suitable for cryptographic purposes as there is no polynomial algorithm to solve them efficiently by brute-force within probabilistic polynomial time.

*Elliptic Discrete Logarithm (ECDL) Problem:* Given an element  $Q \in G$ , the ECDL problem is to extract an element  $x \in Z_q^*$ , such that  $Q = xP$ .

*Elliptic Curve Computational Diffie-Hellman (ECCDH) Problem:* Given two elements  $xP, yP \in G$ , with unknown elements  $x, y \in Z_q^*$ , the ECCDH problem is to compute  $Q = xyP$ .

*Elliptic Curve Decisional Diffie-Hellman (ECDDH) Problem:* No any probabilistic polynomial time algorithm can distinguish between the tuples  $(P_1, xP_1, yP_1, T)$  and  $(P_1, xP_1, yP_1, xyP_1)$  where  $P_1, T \in G$ , with unknown elements  $x, y \in Z_q^*$ .

Thus, the trusted authority (TA) initiates the system by deciding of the secure parameters that would be used for formulation of security algorithms. The TA will decide on the type of elliptic curve,  $E : y^3 = x^2 + ax + b \pmod{p}$ , the prime field  $F_p$  determined by the prime number  $p$ . So,  $E_p$  define the elliptic curve points over the field,  $F_p$ . TA runs a set secure algorithm say,  $\mathcal{G}(1)^n$  to obtain  $\{G, q, P\}$ . The TA as a root administrator chooses a master private key, say  $\omega \in Z_q^*$ , where  $q$  is a prime number, with a respective master public key  $\Omega = \omega P$ . Then the public parameter are defined as  $\{q, p, P, G, E_p, F_q, \Omega, H\}$ , where  $H$  is a chosen secure hash function. Variants of such parameters are used in the preceding works in this study according to system design in achieving privacy preservation in smart grid network environment.

## 1.5 Outline of the Thesis

This thesis is organized as follows, Chapter 2, expounds on the main security and privacy-preserving problems pertaining to real-time SG applications in a VANETs system, AIMS communications and privacy-preserving data aggregation in SG setting and literature. Chapter 3, presents the proposed solution for security and privacy challenge in SG application in VANETs, focusing at safeguarding identity privacy and data integrity of vehicle owners during charging\discharging. The scheme has merits in terms of validated security analysis and performance evaluation. Chapter 4, portrays a proposed solution for secure and anonymous authenticated key exchange for AIMS communications in smart grid. Whilst, Chapter 5 presents a lightweight privacy-preserving mechanism for secure data aggregation in smart grid. Lastly, Chapter 6 concludes the thesis and sums up main contributions and projects the future research directions.



## Chapter 2

# Efficient Certificate-less Aggregate Signature Scheme with Conditional Privacy-Preservation for Vehicular Ad Hoc Networks Enhanced Smart Grid System

### 2.1 Introduction

Major advancement in wireless sensor network (WSN), Internet of Things (IoT) and the advent of big data paradigm has seen the birth of various network based advancement in cross-cutting technologies such as Vehicular Ad Hoc Network (VANETs) which support wireless communication of vehicles among themselves and road sign units (RSUs) for numerous applications like: traffic safety, location based-services, electric vehicles (EVs) and electricity exchange services among others [32–37]. Smart grid is one such technology motivated by the development of WSN and IoT in its functionality. The EVs technology will result in elevation of power consumption unsustainable by means of traditional electricity grid [38]. An obvious solution to sorting out EVs electricity demands is by formulating VANETs-enhanced smart grid, with coordinated charging system that is responsive to efficient cost and electricity utilization by using communication technologies [39, 40]. Thus, it is recommended that algorithms for security, authentication, information processing and data aggregation be of high-precision and efficiency to allow low communication latency for real-time pricing and optimal electricity dispatch decisions in a VANETs enhanced smart grid system [41, 42]. The concepts of VANET is an advancement of mobile ad hoc networks (MANETs) where there is real-time communication between EVs and RSUs for electricity charging/discharging [38, 43, 44]. Typically topology of VANETs includes trusted authorities (TAs), RSUs and on-board units (OBUs) mounted on vehicles [45–47]. The OBUs constantly casts

the traffic related messages about vehicles facilitating various smart applications and technologies such as current vehicle location, time, speed, direction and traffic condition in every 100-300 ms [44, 48, 49]. As is the case with many communication network based technologies, VANETs is not an exception to face various cyber-security challenges in terms of data security and user privacy [50–53]. With secure and privacy protection addressed, the applications of VANETs in traffic management and control, traffic accident avoidance features, traffic vigilance, gas emission, EVs charging and fuel consumption will be fully implemented [54]. So if the VANETs network system is not protected adversaries may launch all sorts of attacks like data modification, impersonation, replay, denial of service attacks amongst others. For instance, there are attacks launched by rogue vehicles broadcasting fake instructions to cause traffic accidents and general confusion. Thus, in terms of message senders legitimacy there should be security features when sending messages to check authentication and integrity [54, 55]. To this effect many authentication schemes have been proposed using traditional public key cryptography (PKC) to secure a VANETs system [56, 57]. In terms of privacy concerns, anonymity must be provided in the design mechanism to lid against eavesdropping adversaries. In this way the real identity of communicating party will not be known nor communication transactions be analyzed and linked to a particular VANETs participant. However, due to abuse of the anonymity feature, the pseudonym given to participating entities should be traceable and revocable, so that the TA can reveal the real identity of malicious vehicle under certain conditions [58]. Since OBUs have limited computation and storage capabilities, the use of less computation intensive cryptographic techniques is promoted, to handle large message flow in the system and improve smooth communication. Certificate-less aggregate signature (CLAS) is one efficient technique that improves message authentication and saves bandwidth. In CLAS  $n$  signatures on  $n$  distinct messages from  $n$  distinct users, are aggregated into a single short signature that can be verified at once as combined [59] in a process known as batch verification. This approach is very helpful in VANETs where RSUs collect and aggregate a large number of signatures from individual participants signatures into one signature that is broadcasted to vehicles in the system to achieve a particular VANETs enhanced smart grid application, and this greatly enhances efficiency in verification and communication overhead [44, 60]. Achieving efficiency by design is much encourage to cope up with the computation capabilities of RSUs and OBUs by constructing the algorithms with lighter computation operations. To this effect employing elliptic curve cryptography (ECC) based cryptosystems improves computation efficiency by a great margin and thereby a recommendable approach. Thus, we propose an efficient certificate-less aggregate scheme with conditional privacy-preservation by using ECC approach. The proposed scheme satisfies security and privacy requirements for VANETs with optimal efficiency and rigorous security proof is provided. There are different modes of communications in VANETs such as vehicle-to-vehicle (V2V), vehicle-to-grid (V2G) and vehicle-to-infrastructure (V2I), vehicle-to-everything (V2E) that use the short medium range communication protocol called dedicated short range communication (DSRC) to facilitate various vehicular network applications [61]. These computer sophisticated ve-

## 2.1. Introduction

hicles are being adopted for various smart services in intelligent transportation systems (ITS) . The following security requirements are important for any WSN based system such as VANETs:

- **Non-repudiation:** Any electric vehicle transaction has economic value and this can motivate fraudulent act by the entities selling or buying electricity. Therefore, this measure of non-repudiation ensures that any electricity transaction can be accounted for to the involved parties and any modification cannot be denied by the party.
- **Message integrity and authentication:** In a similar manner, any network transaction once completed cannot be modified by any malicious entity and once there is an attempt to tamper with the transaction, then it should be detectable by any legal entity of the system.
- **Privacy:** The actual identity of a consumer nor the information of a transaction in the network should not be known by any malicious party eavesdropping on the communications involving a particular targeted entity.
- **Unlinkability:** By observing transaction in the VANETs network the entity's activities should still not be analysed and be associated with a particular RSU or vehicle. Thus to say messages plying on the network for any participant should still look random to an attacker and nothing associated with the participant should be determined.
- **Traceability:** However, for undesirable conduct of an entity in the network such acts should be traced and be accounted for the individual. On the other hand the vehicle should be hidden or inaccessible from other unauthorized entities.
- **Resistance to Attacks:** Due to communication over a public channel, V2G security scheme must withstand various general attacks such as: impersonation attack, replay attack, modification attack, man-in-the-middle-attack and stolen verifier table attack in VANETs.

Therefore, we propose a novel anonymous certificate-less aggregate signature scheme for VANETs with conditional privacy-preservation in a smart grid system, that addresses common weaknesses of most existing certificate-less aggregate signature schemes. The main contribution of the paper can be summarized as follows:

- The proposed scheme achieves user anonymity with conditional privacy, such that each domain stores a Certificate Revocation List (CRL) in all road sign units located in that particular domain.
- The proposed scheme achieves optimal efficiency for certificate-less aggregate signature while precluding complex cryptographic operations like bilinear pairings and map-to-point hash operations.

- The proposed scheme withstand escrow property powers of the KGC but use of partial private key and user generated full private key for signature signing.

The rest of the paper is organized according to the outline given as follows. Section II reviews most relevant related works of CLAS schemes for VANETs. Section III provides that mathematical building blocks for the proposed scheme. Section IV give the detailed steps of the proposed work. Section V, presents an in-depth analysis of the scheme in terms of security, privacy and performance assessment. Finally, in VI we give concluding remarks about the proposed scheme.

## 2.2 Related Works and Limitations

In VANETs, source authentication and message integrity of traffic-related information form a very important security requirements in the system. Satisfaction of these security requirements ensure trust and proper functionality of all versatile technologies that comes with VANETs system by simply securing moving vehicles, RSUs, Application Servers, and roadside sensors. To this effect many research works have been done to provide the needed security to such an advent technology of smart city [55].

The key management problem posed by the certificate based PKI cryptosystem paved way to the pioneering work of certificate-less public key signature (CL-PKS) scheme by Al-Riyami and Paterson [62]. This idea caught much research interest in the aspect of improving the security and performance. In [63], Yum and Lee presented a general procedure to construct a CL-PKS scheme from any ID-based signature scheme. The first CL-PKS scheme was bilinear pairing based proposed by Li et al. in [64]. Whereas in [65], Au et al. presented a new security model for CL-PKS schemes which considers inside attack scenario. The first bilinear pairing free CL-PKS scheme was first proposed by He et al. in [66], which was found to be vulnerable to other attacks in [67]. In [68] a scheme ideal for IoT deployment was proposed, however it was found to bear some flaws concerning inside attack performance by KGC in [69]. In order to provide the needed security property of anonymous authentication in [70, 71] the idea of pseudonym-based authentication was employed. Despite providing privacy preservation, the limitation of overburdened TA in storing these pseudonyms for each vehicle was encountered as has shown out as the shortfall for their approach. In [72], having foreseen the problem of overburdened TA and sought to provide a solution they designed by using anonymous certificates but this was done at the expense of interactions between the infrastructures. In [73] et al., privacy protection for VANETs communications was achieved based on the technique of ID-based ring signature, but they failed to provide conditional privacy, since there was no any tracking mechanism in their algorithm [74]. Many more researchers demonstrated the need to formulate robust schemes in terms of security and privacy protection. To this cause, Bayal et al. [75] proposed an anonymous authentication scheme, however it is deemed computationally intensive in [76]. In [77], Cui et al. proposed a scheme that utilizes the methods of cuckoo filter and binary search to facilitate batch verification for vehicular communication of V2V

## 2.2. Related Works and Limitations

and V2I. He et al. [48] designed an ECC based certificateless based signature scheme for VANETs system with batch verification feature. However, Mahmood et al. [62] states that their scheme still vulnerable to side-channel attack since some of sensitive information like TA's master private key is stored in a tamperproof devices (TPD). A scheme in [78] uses pseudonyms instead of real identities in trying to secure VANETs communications. The scheme in [78] achieves efficiency and provides batch verification but falls short in terms of providing all security requirements like unlinkability.

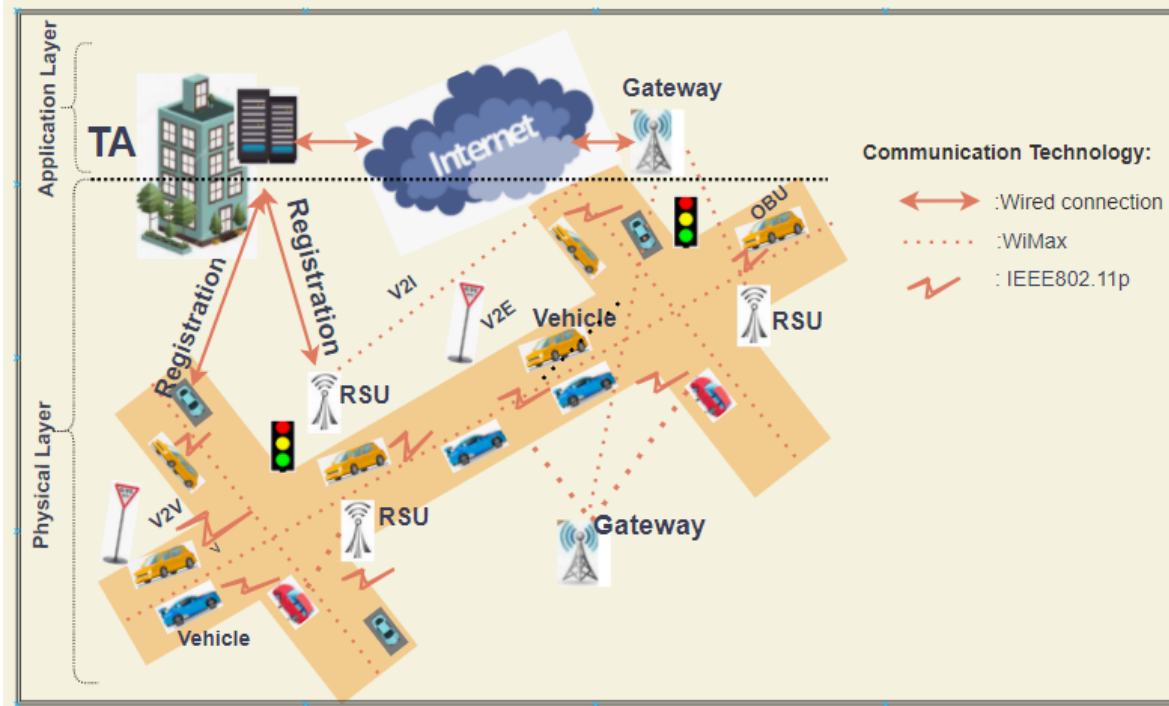


Figure 2.1: Two Layered VANETs Architecture.

### 2.2.1 System Model

In terms of communication process the VANETs' architecture is categorized into two layers namely the physical layer and the application layer. In which case the physical layer comprises of the vehicles, the RSUs situated on designated points of the road. Vehicles on the roads are embodied with OBUs as a communication enabling device to connect with other vehicles, RSUs or other advanced smart city facilities. [79, 80]. The OBU is equipped with a TPD device to secure stored sensitive information like secret key and the global positioning system (GPS). As such the vehicle is securely able to carry out advanced VANETs communications in smart cities includes V2X, V2V and V2I that are enabled by dedicated short range communication (DSRC) protocol specifically identified as IEEE 802.11p. On the other hand, the application layers comprises of the key generation center (KGC), the tracing authority (TRA) application server

which are the major components doing the TA roles in a conditional privacy preserving VANETs based system. The TRA is responsible authority for RSUs and issuing pseudo-identities to vehicle and can do real identity revocation whenever necessary. In like manner the KGC is responsible for public and partial private keys generation for both RSUs and vehicles. So in VANETs schemes, it is usually assumed that the KGC and TRA are trusted parties and hence assumed honest but curious [81]. Both KGC and TRA have sufficient computation power but the OBUs and RSUs are the one with limited computation and storage capabilities hierarchically with RSUs as most powerful one [54, 60, 82]. However, OBUs and RSUs are not trusted entities and therefore any communication initiative originating from them must be authenticated. Thus, this inspires devising of security protocols for VANETs with suitable computation requirements for OBUs and RSUs.

Table 2.1: Notations Used in the Proposed Scheme

Symbols	Meanings of Symbols in the Scheme
$V_i$	$i^{th}$ vehicle
$ID_i$	A pseudo-identity of $V_i$ such that $ID = (PID_1, PID_2, T_i)$
$psk_i$	Partial private key for a vehicle, $V_i$
$(x_i, x_iP)$	Secret key and public key for $V_i$
$sk_i$	Full private key for $V_i$
$T_i$	Validity period for the pseudo-identity $ID_i$ for $V_i$
$RID_i$	A real identity for the vehicle $V_i$
$(P_{pub}, \alpha)$	KGC's public key and master key respectively
$(T_{pub}, \beta)$	TRA's public key and master key respectively
$M_i$	Traffic-related message generated by $V_i$
$t_i$	Current timestamp

### 2.2.2 Security Model for CLAS Scheme

As proposed first in [62], in CLAS we assume two types of adversaries termed *Type 1 Adversary*,  $A_1$ , and *Type 2 Adversary*,  $A_2$ .  $A_1$  acts as a dishonest user and  $A_2$  acts as a

### 2.3. The Proposed Certificate-less Aggregate Signature Scheme

malicious KGC on the other hand. **Type 1 Adversary:**  $A_1$  adversary does not control the master key but is allowed to replace public keys at will with any desirable value of its choice. **Type 2 Adversary:**  $A_2$  adversary has access and controls the master key but cannot replace public keys of users.

The classical security model proposed in Zhang *et al.* [83] presents a security adversarial model for certificate-less key agreement schemes. The model is defined as a game between a challenger,  $C$ , and an adversary defined by a probabilistic polynomial-time turing machine,  $A \in \{A_1, A_2\}$ . Thus  $A$ , has full control of the communication channel of all parties and parties only respond to queries from  $A$  and cannot communicate directly with each other. As a controller of the communication channel  $A$  has powers to actively carry out the following actions, such as relaying, modifying, delaying, interleaving, deleting all the message flowing in the system.

## 2.3 The Proposed Certificate-less Aggregate Signature Scheme

In this section, we will explain the scheme design for VANETs integrated smart grid system titled Efficient certificate-less Aggregate Signature Scheme with Conditional Privacy-Preservation for Vehicular Ad Hoc Networks Enhanced Smart Grid System termed ECLAS for convenient referencing. The proposed scheme consists of eight algorithms which are: Set-up, Pseudo-Identity-Generation, Partial-Private-Key-Extraction, Vehicle-Key-Generation, Sign, Individual Verify, Aggregate and Aggregate verify, which are explained as follows.

1. *Set up:* In this section, the TA comprising of two mutually exclusive principle parts, which are the, TRA and the KGC will initialize the system, by generating the system parameters. The TA takes as input the security parameter  $1^k$  the algorithm outputs two large prime numbers,  $p$ ,  $q$  and a non-singular elliptic curve defined by  $y^2 = x^3 + ax + b \pmod{p}$ , where  $a, b \in F_p$ . This scheme algorithm phase is well illustrated in Figure 2.2.
  - The KGC sets a point  $P$  from  $E$  and with this point generates a group  $G$  of order  $q$ . Then KGC randomly selects a number  $\alpha \in Z_q^*$  and sets it as its master secret with its corresponding public key computed as  $P_{pub} = \alpha P$ .
  - Similarly, the TRA selects a points  $P$  on  $E$  and with it generates a group  $G$  of order  $q$ . Further, TRA chooses a random number  $\beta \in Z_q^*$  and computes its public key  $T_{pub} = \beta P$  while setting  $\beta$  as its master secret key used for traceability which is known to TRA only.
  - All these principle entities (TA, KGC and TRA) choose three hash functions,  $H_1 : G \rightarrow Z_q^*$ ,  $H_2 : \{0, 1\}^* \rightarrow Z_q^*$  and  $H_3 : \{0, 1\}^* \rightarrow Z_q^*$
  - Then the system public parameters  $params = \{P, p, q, E, G, H_1, H_2, H_3, P_{pub}, T_{pub}\}$  are published. These  $params$

are then pre-loaded in the tamper-proof communicating devices and RSU of the system.

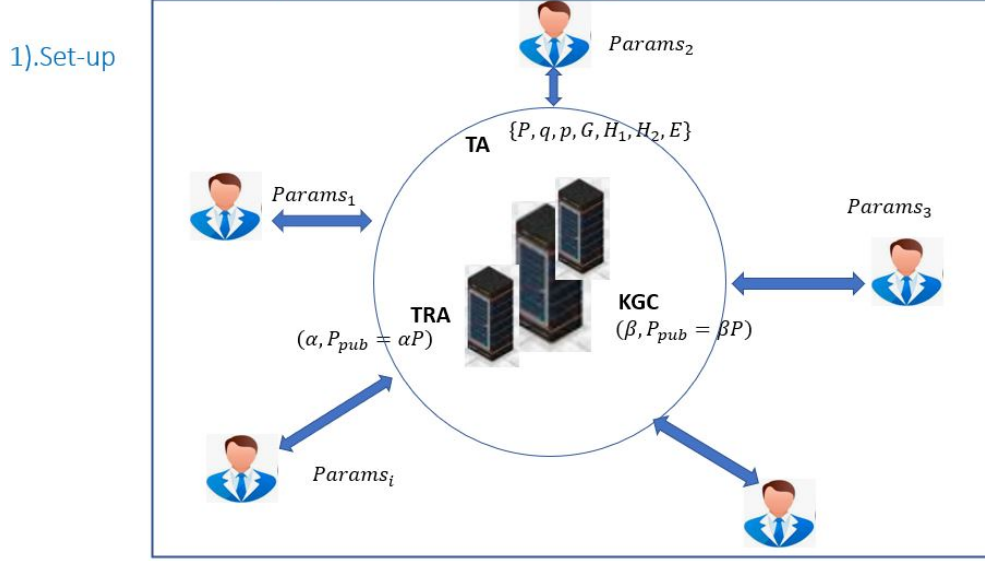


Figure 2.2: TA set up system parameters

2. *Pseudo-Identity-Generation | Partial-Private-Key-Extraction*: In this phase the TRA's responsibility is to generate pseudo-identities for the vehicles while the KGC's responsibility is to create corresponding partial private keys to the pseudo-identities. Thus, finally all vehicles under a TA are registered and pre-loaded with their pseudo-identities and partial private keys. By use of pseudo-identities that are closed linked to the real identities, the proposed scheme can achieve conditional privacy-preservation when it is necessary to revoke the real identity of an entity the TRA can ably do so. The process of pseudo-identity generation and linkage with partial-private-key is executed by TRA and KGC in a sequential manner as follows:

- A vehicle,  $V_i$ , with its unique real identity denoted as  $RID_i$  selects a random number  $k_i \in Z_q^*$  and calculates  $PID_1 = k_i P$ . Then the vehicle,  $V_i$ , sends  $(RID_i, PID_1)$  to the TRA through a secure channel.
- The TRA first checks the  $RID_i$ , if its acceptable then it calculates,  $PID_2 = RID_i \oplus H_1(\beta.PID_1 || T_i || T_{pub})$ , where  $T_i$  indicates the validity period the pseudo-identity. The pseudo-identity that is used to identify a vehicle,  $V_i$ , is  $ID_i = (PID_1 || PID_2 || T_i)$  and it is sent to the vehicle and KGC through a secure channel. During revocation TRA obtains the real identity by computing  $RID_i = PID_2 \oplus H_1(\beta || T_i || T_{pub})$ .
- Upon receipt of the pseudo-identity,  $ID_i$ , KGC chooses a random number,



### 2.3. The Proposed Certificate-less Aggregate Signature Scheme

$d_i \in Z_q^*$  and computes  $Q_{ID_i} = d_i P$  and then computes the partial private key,  $psk_i$ , for the vehicle,  $V_i$ , as  $psk_i = d_i + H_2(ID_i || Q_{ID_i}) \times \alpha \text{ mod } p$ .

- The KGC then sends the pseudo-identity and partial private key ( $Q_{ID_i}, psk_i$ ) to the vehicle,  $V_i$ , through a secure channel.

The vehicle is able to check the authenticity of the pseudo-identity and the partial private key received from the KGC by verifying whether  $psk_i \cdot P = Q_{ID_i} + H_2(ID_i || Q_{ID_i}) \cdot P_{pub}$ . The conditional privacy-preservation is enhanced in the design by combining the secret contribution from the vehicle,  $V_i$ , itself and the TRA on the other hand. It is designed in such a way that the TRA is able to revoke the real identity of the vehicle when needed to do so. At the end of it all, the pseudo-identity and the partial private key are stored in the tamper-proof devices in the vehicle. The interplay of the process is demonstrated in Figure 2.3.

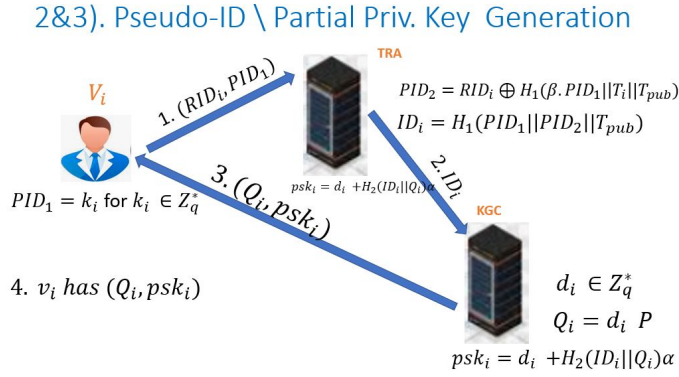


Figure 2.3: TRA and KGC collaborates to generate partial private key

3. *Vehicle-Key-Generation:* The vehicle,  $V_i$  proceeds by, randomly selecting a secret value  $x_i \in Z_q^*$  as its secret key noted as  $vs_k_i$  and then calculates its corresponding public key  $vpk_i = x_i \cdot P$ . Then  $V_i$  set the full private key as  $sk_i = x_i + psk_i$ .
4. *Sign:* Message signature is necessary for the sake of upholding authentication and integrity of the message to the receiver of the message who rightly does verification. The vehicle,  $V_i$ , selects one of its stored pseudo-identity,  $ID_i$ , and picks the latest timestamp,  $t_i$ . With the signing Keys ( $psk_i, sk_i$ ) and the traffic related message  $M_i$ , the vehicle  $V_i$  carries out the following steps to produce a signature.

- Selects a random number  $r_i \in Z_q^*$  and computes  $R_i = r_i P$ .
- Computes,

$$h_i = H_3(M_i || ID_i || Q_{ID_i} || vpk_i || R_i || t_i) \quad (2.1)$$

and

$$S_i = h_i \cdot r_i + sk_i \text{ mod } p \quad (2.2)$$

. Then

$$\sigma_i = (R_i, S_i) \quad (2.3)$$

is the computed certificate-less signature on the traffic related data  $M_i$  for latest timestamp  $t_i$  and identification  $ID_i$ .

- Then the final message that,  $V_i$  sends the to nearby RSU and vehicles for verification is  $(ID_i, Q_{ID_i}, vpk_i, M_i, t_i, \sigma_i)$ .

These steps are routinely carried out every time,  $V_i$  sends a message to RSU. The individual signature signing and signature aggregation by RSU is illustrated in Figure 2.4.

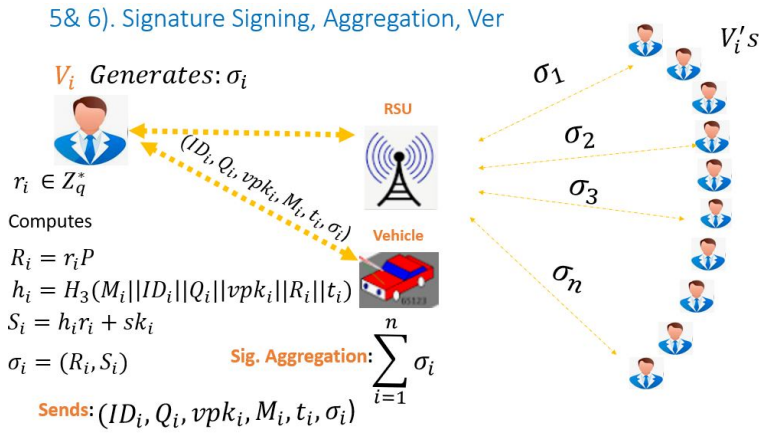


Figure 2.4: Signature generation and aggregation

5. *Individual Verify*: On receipt of the certificate-less signature  $\sigma_i = (R_i, S_i)$  on the traffic related data  $M_i$  and timestamped at  $t_i$  signed by the vehicle along with its public key  $vpk_i$ , if the received  $T_i$  in  $ID_i$  and  $t_i$  are both valid, then the RSU performs the following procedures.

- Computes

$$h_{i,0} = H_2(ID_i || Q_{ID_i}) \quad (2.4)$$

and

$$h_i = H_3(M_i || ID_i || Q_{ID_i} || vpk_i || R_i || t_i) \quad (2.5)$$

- Verifies whether

$$S_i \cdot P = h_i \cdot R_i + vpk_i + Q_{ID_i} + h_{i,0} \cdot P_{pub} \quad (2.6)$$

holds or not.

The RSU accepts the certificate-less signature if the verification holds. Correctness checking works, since  $P_{pub} = \alpha \cdot P$ ,  $Q_{ID_i} = d_i \cdot P$ ,  $psk_i = d_i + H_2(ID_i || Q_{ID_i}) \times$

### 2.3. The Proposed Certificate-less Aggregate Signature Scheme

$\alpha \bmod p$ ,  $R_i = r_i.P$ ,  $sk_i = x_i + psk_i$ ,  $h_{i,0} = H_2(ID_i || Q_{ID_i})$  and  $S_i = h_i.r_i + sk_i \bmod p$ . Thus the computation proceeds as follows:

$$\begin{aligned}
S_i.P &= (h_i.r_i + sk_i).P \\
&= h_i.r_i.P + (x_i + psk_i)P \\
&= h_i.R_i + x_i.P + psk_i.P \\
&= h_i.R_i + vpk_i + [d_i + H_2(ID_i || Q_{ID_i})\alpha] \\
&= h_i.R_i + vpk_i + Q_{ID_i} + (h_{i,0}.\alpha)P \\
&= h_i.R_i + vpk_i + Q_{ID_i} + h_{i,0}.P_{pub}
\end{aligned}$$

However for purposes of saving computation cost, it is recommended to do data aggregation and batch verification on the signatures from the network environment of a particular RSU.

6. *Aggregate*: Each RSU is an out-posted aggregate signature generator that collects individual certificate-less signatures into a single verifiable one. The components come for an aggregating set  $V$  on  $n$  vehicles,  $\{V_1, V_2, \dots, V_n\}$  whose corresponding pseudo-identities are,  $\{ID_1, ID_2, \dots, ID_n\}$  with public keys  $\{vpk, vpk_2, \dots, vpk_n\}$  and message signature pairs  $(M_1, t_1, \sigma_1), (M_2, t_2, \sigma_2), \dots, (M_n, t_n, \sigma_n)$  where  $\sigma_i = (R_i, S_i)$  for  $i = 1, 2, \dots, n$ . The RSU or an application server for the traffic control center for instance computes the sum  $S = \sum_{i=1}^n S_i$  and output an aggregate certificate-less signature as,

$$\sigma = (R_1, S_1), (R_2, S_2), \dots, (R_n, S_n) \quad (2.7)$$

, for  $i = 1, 2, \dots, n$ .

7. *Aggregate Verify*: On receipt of the certificate-less aggregate signature  $\sigma$  from  $n$  vehicle  $\{V_1, V_2, \dots, V_n\}$  whose pseudo-identities are  $\{ID_1, ID_2, \dots, ID_n\}$  with corresponding public keys,  $\{vpk, vpk_2, \dots, vpk_n\}$  and the traffic related messages  $\{M_1 || t_1, M_2 || t_2, \dots, M_n || t_n\}$  then the RSU or the application server carries out the following procedure if both  $T_i$  in  $ID_i$  and  $t_i$  are checked to be valid.

- RSU computes

$$h_{i,0} = H_2(ID_i || Q_{ID_i}) \quad (2.8)$$

and

$$h_i = H_3(M_i || ID_i || vpk_i || R_i || t_i) \quad (2.9)$$

for  $i = 1, 2, \dots, n$

- RSU verifies if the computation holds,

$$S.P = \sum_{i=1}^n h_i.R_i + \sum_{i=1}^n vpk_i + \sum_{i=1}^n Q_{ID_i} + \sum_{i=1}^n h_{i,0}.P_{pub} \quad (2.10)$$

If the verification holds, then RSU accepts the aggregate certificate-less signature. The computation is valid by the correctness check, since  $P_{pub} = \alpha.P$ ,  $Q_{ID_i} = d_i.P$ ,  $psk_i = d_i + H_2(ID_i||Q_{ID_i}) \times \text{mod } p$ ,  $R_i + r_i.P$ ,  $S_i = h_i.r_i + psk_i \text{ mod } p$ , and  $S = \sum_{i=1}^n S_i$ , thus we obtain.

$$\begin{aligned} S_i.P &= \sum_{i=1}^n (h_i.r_i + sk_i).P \\ &= \sum_{i=1}^n h_i.r_i.P + \sum_{i=1}^n (x_i + psk_i)P \\ &= \sum_{i=1}^n h_i.R_i + \sum_{i=1}^n x_i.P + \sum_{i=1}^n psk_i.P \\ &= \sum_{i=1}^n h_i.R_i + \sum_{i=1}^n vpk_i + \sum_{i=1}^n [d_i + H_2(ID_i||Q_{ID_i})\alpha]P \\ &= \sum_{i=1}^n h_i.R_i + \sum_{i=1}^n vpk_i + \sum_{i=1}^n Q_{ID_i} + \sum_{i=1}^n (h_{i,0}.\alpha)P \\ &= \sum_{i=1}^n h_i.R_i + \sum_{i=1}^n vpk_i + \sum_{i=1}^n Q_{ID_i} + \sum_{i=1}^n h_{i,0}.P_{pub} \end{aligned}$$

## 2.4 Analyses

From here forth we will devote to give a formal security proof, security privacy preservation analyses and then we will present the performance evaluation of the proposed ECLAS scheme with conditional privacy-preservation for a VANETs enhanced smart grid.

### 2.4.1 Security Proof

In this section now, we will provide security proof for the proposed ECLAS scheme for VANETs. We assume the security model for CLAS schemes where there are two types of adversaries, which are *Type 1 Adversary* and *Type 2 Adversary* as demonstrated in the security model for CLAS scheme.

## 2.4. Analyses

**Theorem 1.** *Under the assumption that ECDL in  $G$  is intractable, then the proposed scheme  $(\epsilon, t, q_c, q_s, q_h)$ , is secure against adversary 1 in random oracle model, where  $q_c, q_s, q_h$  are the **Create**, **Sign** and **Hash** queries respectively which the adversary is allowed to make.*

**Proof:** Suppose there is a probabilistic polynomial time adversary  $\mathcal{A}_1$ , we construct an algorithm  $\mathcal{F}$  that solves the ECDL problem by utilizing  $\mathcal{A}_1$ . Assume that  $\mathcal{F}$  is given a ECDL problem instance,  $(P, Q)$  to compute  $x \in Z_q^*$  so that  $Q = xP$ . Thus,  $\mathcal{F}$  chooses an challenging identity  $ID^*$  for the identity  $ID$  to answer any random queries from  $\mathcal{A}_1$  as follows:

- **Set-up ( $ID$ ) Query:** The challenger  $\mathcal{F}$  selects its random numbers  $\alpha^*$  and  $\beta^*$  as its master keys and has a corresponding public key as  $P_{pub}^* = \alpha^*P$  and  $T_{pub}^* = \beta^*P$  then sends the system parameters  $\{P, p, q, E, G, H_2, H_3, P_{pub}^*, T_{pub}^*\}$  to  $\mathcal{A}_1$ .
- **Create ( $ID$ ) Query:**  $\mathcal{F}$  stores the hash list  $L_C$  of the tuple  $(ID, Q_{ID_i}, vpk_i, psk_i, sk_i, h_2)$ . Whenever an adversary  $\mathcal{A}_1$  makes a query for  $ID$ , and if the  $ID$  is contained in  $L_C$ , then  $\mathcal{F}$  returns  $(ID, Q_{ID_i}, vpk_i, psk_i, sk_i, h_2)$  to  $\mathcal{A}_1$ . Then  $\mathcal{F}$ , execute the oracle as follows. if  $ID = ID^*$ ,  $\mathcal{F}$  randomly chooses the values  $a, b, c \in Z_q^*$  and sets  $Q_{ID} = a.P_{pub}^* + b.P$ ,  $vpk_i = c.P$ ,  $psk_i = b$ ,  $sk_i = c$ ,  $h_2 = H_2(ID || Q_{ID}) \leftarrow amodq$ , then  $\mathcal{F}$  adds  $(ID, Q_{ID}, h_2)$  to the list  $L_{H_2}$  and returns  $(ID, Q_{ID_i}, vpk_i, psk_i, sk_i, h_2)$  to  $\mathcal{A}_1$ . as the equation  $psk_i.P = Q_{ID} + h_2.P_{pub}^*$ , thereby implying that the partial private key is valid.
- **$H_2$  Query:** Whenever an  $H_2$  query with  $(ID, Q_{ID})$  is made, and  $ID$  is already in the hash list  $L_{H_2}$ , then  $\mathcal{F}$  reply with a corresponding  $h_2$ . On the other hand,  $\mathcal{F}$  runs **Create( $ID$ )** to obtain  $h_2$  and then sends  $h_2$  to  $\mathcal{A}_1$ .
- **Partial-Private-Key-Extract ( $ID$ ) Query:** if  $ID^* = ID$ , then  $\mathcal{F}$  aborts the game. Otherwise,  $\mathcal{F}$  looks in the hash list  $L_C$ , if  $ID$  is found in the list, then  $\mathcal{F}$  returns  $psk_i$  to  $\mathcal{A}_1$ . If  $ID$  is not in the list  $L_C$ ,  $\mathcal{F}$  executes **Create( $ID$ )** query to obtain  $psk_i$  and sends it to  $\mathcal{A}_1$ .
- **Public-Key ( $ID$ ) Query:** Upon receiving the query on  $ID$ , when  $ID$  is already in the list  $L_C$ ,  $\mathcal{F}$  replies with  $pk = (Q_{ID}, vpk_i)$ . On the other hand,  $\mathcal{F}$  executes **Create( $ID$ )** query to obtain  $(Q_{ID}, vpk_i)$  and sends it to  $\mathcal{A}_1$ .
- **Public-Key-replacement ( $ID, pk'$ ) Query:**  $\mathcal{F}$  stores the hash list  $L_R$  of tuple  $(ID, d_i, Q_{ID}, sk_i, vpk_i)$ . When  $\mathcal{A}_1$  executes the query with  $(ID, pk')$ , where  $Q'_{ID} = d'.P$ ,  $vpk'_i = x'_i.P$  and  $pk' = (Q'_{ID}, vpk'_i)$ , then  $\mathcal{F}$  sets  $Q_{ID} = Q'_{ID}$ ,  $vpk_i = vpk'_i$ ,  $psk_i = \perp$  and  $x_i = x'_i$ . Then the challenger  $\mathcal{F}$ , updates the list  $L_R$  to be  $(ID, d'_i, Q'_{ID}, vpk'_i, x'_i)$ .
- **$H_3$ ( $ID$ ) Query:**  $\mathcal{F}$  keeps the hash list  $L_{H_3}$  of the tuple  $(m, ID, R, vpk_i, t, h_3)$  and if the  $ID$  queries are not in the list,  $\mathcal{F}$  replies with  $h_3$ . Otherwise, it selects a

random number  $h_3$  such that  $h_3 = H_3(m||ID||vpk_i||R||t)$  then add it to the list  $L_{H_3}$  and returns  $h_3$  to  $\mathcal{A}_1$

- **Sign**  $(ID, m)$  **Query**:  $\mathcal{A}_1$  makes a sign query on  $(ID, m)$ , once  $ID$  is on the list  $L_R$ ,  $\mathcal{F}$  chooses random numbers  $a, b, c \in Z_q^*$ , and sets  $s = a$ ,  $R = P$ ,  $h_3 = H_3(m||ID||vpk_i||R||t) \leftarrow (a - b - c) \bmod q$  and then inserts  $(m, ID, R, vpk_i, t, h_3)$  to the list  $L_{H_3}$ . The resultant signature is  $(R, s)$ , and if  $ID$  is not in the list  $L_R$ , then  $\mathcal{F}$  acts according to scheme's procedure.

As a result  $\mathcal{A}_1$  produces a forged signature  $\sigma = (R, s_{\{1\}})$  on the message  $(ID, m)$  which passes verification process. If  $ID \neq ID^*$ ,  $\mathcal{F}$  aborts the process.  $\mathcal{F}$  keeps on challenging  $\mathcal{A}_1$  up until it responds to the  $H_3$  query.  $\mathcal{A}_1$  will be prompted to generate another valid signature  $\sigma = (R, s_{\{2\}})$  by using the same  $R$ . Thus we have:

$$s_{\{i\}} \cdot P = h_{3\{i\}} \cdot R + vpk_i + Q_{ID} + h_2 \cdot P_{pub} \quad (2.11)$$

, where  $i = 1, 2$

By solving the two linear equations  $\mathcal{A}_1$  obtain from equation (2.2), the value of  $r$  by

$$r = \frac{s_2 - s_1}{h_{\{2\}} - h_{\{1\}}} \quad (2.12)$$

, similarly with continuous querying  $H_2$  will allow computation of  $x$ .

**Probabilistic Analysis**: The simulation of  $\text{Create}(ID)$  queries fails when the random oracle assignment  $H_2(ID||Q_{ID})$  causes inconsistency with the probability of at most  $\frac{q_h}{q}$ . The probability of successful simulation of  $q_c$  times is at least  $(1 - \frac{q_h}{q})^{q_c} \geq 1 - (\frac{q_h q_c}{q})$ . Similarly, the simulation is  $q_h$  successful with the probability of at least  $(1 - \frac{q_h}{q})^{q_h} \geq (1 - \frac{q_h^2}{q})$  and  $ID = ID^*$  with the probability of  $\frac{1}{q_c}$ . Thus, in overall the probability of successful simulation is

$$\left(1 - \frac{q_h q_c}{q}\right) \left(1 - \frac{q_h^2}{q}\right) \left(\frac{1}{q_c}\right) \epsilon \quad (2.13)$$

**Theorem 2.** *Under the assumption that ECDL in  $G$  is intractable, then the proposed scheme  $(\epsilon, t, q_c, q_s, q_h)$ , is secure against adversary 2 in random oracle model, where  $q_c, q_s, q_h$  are the **Create**, **Sign** and **Hash** queries respectively which the adversary is allowed to make.*

**Proof**: Suppose there is a probabilistic polynomial time adversary  $\mathcal{A}_2$ , we construct an algorithm  $\mathcal{F}$  that solves the ECDL problem by utilizing  $\mathcal{A}_2$ . Assume that  $\mathcal{F}$  is given a ECDL problem instance,  $(P, Q)$  to compute  $x \in Z_q^*$  so that  $Q = xP$ . Thus,  $\mathcal{F}$  chooses an challenging identity  $ID^*$  for the identity  $ID$  to answer any random queries from  $\mathcal{A}_2$  as follows:

## 2.4. Analyses

- **Set-up ( $ID$ ) Query:** The challenger  $\mathcal{F}$  selects its random numbers  $\alpha^*$  and  $\beta^*$  as its master keys and has a corresponding public key as  $P_{pub}^* = \alpha^*P$  and  $T_{pub}^* = \beta^*P$  then sends the system parameters  $\{P, p, q, E, G, H_2, H_3, P_{pub}^*, T_{pub}^*\}$  to  $\mathcal{A}_2$ .
- **Create ( $ID$ ) Query:**  $\mathcal{F}$  stores the hash list  $L_C$  of the tuple  $(ID, Q_{ID_i}, vpk_i, psk_i, sk_i, h_2)$ . Whenever an adversary  $\mathcal{A}_2$  makes a query for  $ID$ , and if the  $ID$  is contained in  $L_C$ , then  $\mathcal{F}$  returns  $(ID, Q_{ID_i}, vpk_i, psk_i, sk_i, h_2)$  to  $\mathcal{A}_2$ . If  $ID = ID^*$ ,  $\mathcal{F}$  randomly selects  $a, b \in Z_q^*$  and computes  $Q_{ID} = aP$ ,  $vpk_i = Q$ ,  $h_2 = H_2(ID||Q_{ID}) \leftarrow b$ ,  $psk_i = a + x.h_2$ ,  $sk_i = \perp$ . If  $ID \neq ID^*$ ,  $\mathcal{F}$ , randomly selects  $a, b, c \in Z_q^*$  and computes  $Q_{ID} = a.P$ ,  $vpk_i = b.P$ ,  $h_2 = H_2(ID||Q_{ID}) \leftarrow c$ ,  $psk_i = a + x.h_2$ ,  $sk_i = b$ . Then  $\mathcal{F}$ , responds to the query with  $(ID, Q_{ID_i}, vpk_i, psk_i, sk_i, h_2)$  and then appends  $(ID, Q_{ID}, h_2)$  to the hash list  $L_{H_2}$ .
- **$H_2$  Query:** Whenever an adversary  $\mathcal{A}_2$  makes an  $H_2$  query with  $(ID, Q_{ID})$ , and  $ID$  is already in the hash list  $L_{H_2}$ , then  $\mathcal{F}$  reply with a corresponding  $h_2$ . On the other hand,  $\mathcal{F}$  runs Create( $ID$ ) to obtain  $h_2$  and then sends  $h_2$  to  $\mathcal{A}_2$ .
- **Partial-Private-Key-Extract ( $ID$ ) Query:** Upon receipt of the query on  $ID$ ,  $\mathcal{F}$  verifies from the hash list  $L_C$ , if  $ID$  is found to be in the hash list  $\mathcal{F}$  returns  $psk_i$  to  $\mathcal{A}_2$ . If  $ID$  is not in the hash list,  $L_C$ ,  $\mathcal{F}$  executes Create( $ID$ ) query to obtain  $psk_i$  and sends it to  $\mathcal{A}_2$ .
- **Public-Key ( $ID$ ) Query:** Upon receipt of query on  $ID$ , when  $ID$  is already in the list  $L_C$ ,  $\mathcal{F}$  replies with  $pk = (Q_{ID}, vpk_i)$ . On the other hand,  $\mathcal{F}$  executes Create( $ID$ ) query to obtain  $(Q_{ID}, vpk_i)$  and sends it to  $\mathcal{A}_2$ .
- **Secret-Key-Extract ( $ID$ ) Query:** On receipt of the queries from  $\mathcal{A}_2$ , if  $ID = ID^*$ ,  $\mathcal{F}$  stops the simulation. While, if  $ID$  is already in the list  $L_C$ , then  $\mathcal{F}$  reply with  $sk_i$ . Whereas if,  $ID$  is not in the list  $L_C$ ,  $\mathcal{F}$  executes Create( $ID$ ) query to obtain  $(ID, Q_{ID}, vpk_i, psk_i, sk_i, h_2)$  and sends  $sk_i$  to  $\mathcal{A}_2$ .
- **$H_3(ID)$  Query:**  $\mathcal{F}$  keeps the hash list  $L_{H_3}$  of the tuple  $(m, ID, R, vpk_i, t, h_3)$  and if the  $ID$  queries are in the list,  $\mathcal{F}$  replies with  $h_3$ . Otherwise, it selects a random number  $h_3$  such that  $h_3 = H_3(m||ID||vpk_i||R||t)$  then add it to the list  $L_{H_3}$  and returns  $h_3$  to  $\mathcal{A}_2$
- **Sign ( $ID, m$ ) Query:** As  $\mathcal{A}_2$  makes a sign query on  $(ID, m)$ , once  $ID \neq ID^*$ ,  $\mathcal{F}$  acts according to protocol flow. Otherwise,  $\mathcal{F}$  randomly chooses the values  $a, b, f \in Z_q^*$  and sets  $s = a$ ,  $h_3 = H_3(m||ID||vpk_i||R||t) \leftarrow f$ ,  $R = h_3^{-1}(bP_{pub}^* - Q)$ , and returns the signature  $(R, s)$ . If the verification,  $s.P = h_3.R + Q_{ID} + vpk_i + h_2.P_{pub}^*$ , holds then the signature is valid.

As a result  $\mathcal{A}_2$  produces a forged signature  $\sigma = (R, s_{\{1\}})$  on the message  $(ID, m)$  which passes verification process. If  $ID \neq ID^*$ ,  $\mathcal{F}$  aborts the process.  $\mathcal{F}$  keeps on challenging  $\mathcal{A}_2$  up until it responds to the  $H_3$  query.  $\mathcal{A}_2$  will be prompted to generate another valid signature  $\sigma = (R, s_{\{2\}})$  by using the same  $R$ . Thus we have:

$$s_{\{i\}}.P = h_{3\{i\}}.R + vpk_i + Q_{ID} + h_2.P_{pub}^* \quad (2.14)$$

$$s_{\{i\}} = h_{3\{i\}}.r + y + d_i + h_2.x \quad (2.15)$$

where  $i = 1, 2$

By solving the two linear equations involving  $r$  and  $y$  as variables, we can derive the value of  $y$  as an output of ECDL problem.

**Probabilistic Analysis:** The simulation of  $\text{Create}(ID)$  queries fails when the random oracle assignment  $H_2(ID||Q_{ID})$  causes inconsistency with the probability of at most  $\frac{q_h}{q}$ . The probability of successful simulation of  $q_c$  times is at least  $(1 - \frac{q_h}{q})^{q_c} \geq 1 - (\frac{q_h q_c}{q})$ . Similarly, the simulation is  $q_h$  successful with the probability of at least  $(1 - (\frac{q_h}{q}))^{q_h} \geq 1 - (\frac{q_h^2}{q})$  and  $ID = ID^*$  with the probability of  $\frac{1}{q_c}$ . Thus, in overall the probability of successful simulation is

$$\left(1 - \frac{q_h q_c}{q}\right) \left(1 - \frac{q_h^2}{q}\right) \left(\frac{1}{q_c}\right) \epsilon \quad (2.16)$$

## 2.4.2 Security and Privacy-Preservation Analyses

This part of the part discusses the security and privacy-preservation features satisfied by the proposed scheme specifically this is in respect to anonymity (identity privacy), message authentication, data integrity, traceability, unlinkability and resistance to attacks.

- **Anonymity:** In the proposed scheme the vehicle's identification  $ID_i$  is not the real identification  $RID_i$ , but rather a pseudo-identity as offered by the TRA for purposes of achieving conditional privacy of the vehicle in VANETs. The only way for an adversary or any malicious party to obtain the real identity it by computing  $RID_i = ID_i \oplus H_1(\beta.PID_1||T_i||T_{pub})$ . Without knowing the TRA's master private key  $\beta$  no other party can know the vehicle's real identity  $RID_i$ , since it requires  $\beta$  to calculate  $H_1(\beta.PID_1||T_i||T_{pub})$ . This manipulation is infeasible for an adversary to achieve since the extraction of  $\beta$  from  $T_{pub} = \beta.P$ , involves an intractable ECDL problem. Therefore, this claims ascertain the satisfaction of user identity privacy-preservation.
- **Message Integrity and Authentication:** By virtue of signing message before broadcasting the legitimate users authenticity is verified. Based on the ECDLP assumption the authenticity and integrity of the message  $(ID_i, Q_{ID_i}, vpk_i, M_i, t_i, \sigma_i)$  is upheld by verifying the computation  $S_i.P = h_i.R_i + vpk_i + Q_{ID_i} + h_{i,0}.P_{pub}$ . Since  $h_i = H_3(M_i||ID_i||Q_{ID_i}||vpk_i||R_i||t_i)$  and  $h_{i,0} = H_2(ID_i||Q_{ID_i})$  no malicious party



## 2.4. Analyses

can forge  $\sigma_i = (R_i, S_i)$  which achieves the message integrity and authentication of which needs knowledge of full private key  $sk_i = x_i + psk_i$  in its formulation.

- **Traceability:** Although the vehicle is identified by a pseudonym in necessary circumstances the real identity of a particular vehicle can be mapped back from the pseudonym. For instance, the pseudo-identity of a vehicle is  $ID_i = (PID_1 || PID_2 || T_i)$  and the TRA can revoke the real identity by calculating  $PID_2 = RID_i \oplus H_1(\beta.PID_1 || T_i || T_{pub})$ . As such, once a vehicle is flagged as questionable the TRA is able to trace its true identity and thereby carrying out whatever necessary procedures to curb any kind of malpractice. Once this is done the TRA records the real identity  $RID_i$  on the revocation list of the system and as a result the vehicle cannot use its corresponding pseudo-identity  $ID_i$ .
- **Unlinkability:** The message transmitted  $(ID_i, Q_{ID_i}, vpk_i, M_i, t_i, \sigma_i)$  from a vehicle  $V_i$  to others has the component  $PID_1 = k_i P$ , where  $k_i \in Z_q^*$  is random, that is randomly generated for any particular message transmitted. Since the  $PID_1$  is also a component for pseudo-identity generation, it means the randomness in  $PID_1$  results in the randomness of the publicized pseudo-identity  $ID_i$ , hence any two individual captures of the pseudo-identity  $ID_i$  for  $V_i$  still seem random and unrelated to the real identity  $RID_i$ , in the eyes of eavesdroppers. So by virtue of the identification being anonymous and distinct any captured signature cannot be linked to previously captured identity nor to a particular true signer. Thus, any communication is seen as random and new in the plying eyes of an adversary and has no any relationship to previous communications for an eavesdropper to learn any useful information from such communication.
- **Resistance to Attacks:** At this point we will present a demonstration of how the proposed ECLAS scheme can resist against the main common attacks such as: collusion attack, replay attack, modification attack, impersonation attack, and stolen verifier attack.
  - **Replay Attack Resilience:** In the message  $(ID_i, Q_{ID_i}, vpk_i, M_i, t_i, \sigma_i)$  the  $t_i$  in the message helps in checking replay attacks. The recipients, RSUs or vehicles will have to check the freshness of the message, and once the timestamp is invalid the message is discarded. As such the proposed scheme, ECLAS, could resist against replay attack.
  - **Modification Attack Resilience:** In the scheme a valid message  $(ID_i, Q_{ID_i}, vpk_i, M_i, t_i, \sigma_i)$  has a valid digital conditionally anonymous signature  $(ID_i, \sigma_i)$ . Any modification to the message  $(ID_i, Q_{ID_i}, vpk_i, M_i, t_i, \sigma_i)$  can be detected during verification  $S_i.P = h_i.R_i + vpk_i + Q_{ID_i} + h_{i,0}.P_{pub}$  which simultaneously authenticates the sender,  $V_i$ , and the TA side of TRA and KGC. Therefore, the proposed ECLAS scheme stands against modification attack.

- Impersonation Attack Resilience: It is not feasible for an attacker to launch a successful impersonation on the message  $(ID_i, Q_{ID_i}, vpk_i, M_i, t_i, \sigma_i)$  of which can pass verification as if it was generated by a legal user  $V_i$ . However, it is impossible for an attacker to obtain the KGC's master key  $\alpha$  and the users private key  $x_i$  from the publicly accessible parameters as it will involve solving the intractable problems of ECDLP and ECCDHP from  $vpk_i = x_iP$  and  $P_{pub} = \alpha P$ .
- Stolen Verifier Table Attack Resilience: The the proposed ECLAS scheme, both the TA side comprising of TRA and KGC and the user side comprising of RSUs and OBUs on the vehicle do not require a check list. This implies resistance against stolen verification table attack as it means the table can not be stolen.
- Key-Escrow Resilience: Although the TAs side has access to the master keys used for generating the user's partial private key, still more either TRA or KGC cannot generate a valid signature  $\sigma_i = (R_i, S_i)$  for a valid message  $(ID_i, Q_{ID_i}, vpk_i, M_i, t_i, \sigma_i)$ . This is due to the fact that, the vehicle adds a secret value  $x_i$  to the partial private key  $psk_i$  when computing its full private key  $sk_i = x_i + d_i + H_2(ID_i || Q_{ID_i})\alpha$  which is used for signing messages. To this effect although TRA knows the master key  $\beta$  and KGC knows the master key  $\alpha$  for the systems, they cannot forge messages to masquerade as  $V_i$  illegally. Thus, the proposed ECLAS scheme withstands the key escrow attacks.

Now we will present a comparison analysis of ECLAS with recent related works in terms of security features satisfied. In Table, 2.2 the results of the comparison is provided with the features coded as, SF-1, SF-2, SF-3, SF-4, SF-5, SF-6 to denote, integrity and authentication, anonymity, traceability and revocability, unlinkability, key escrow problem and resistance to common attacks respectively. In the Table, 2.2 the symbol  $\checkmark$  denotes the satisfaction whereas  $\times$ , denotes not satisfaction of the security feature. As shown by the comparison table the schemes in [78, 84, 85] fall short from fulfilling some of the features.

### 2.4.3 Performance Evaluation

In this section, we will present the performance analysis of the proposed ECLAS scheme in terms of comparable feature with related researches of the fields that gives merit to the proposed scheme. As such performance comparisons features are discussed in terms of computation cost analysis and communication cost analysis. We will assess the performance evaluation of the proposed work in terms computation cost comparison with other related works by adopting the method presented in [48]. In [48] bilinear pairing on a 80 bits security parameter length is created as  $: G_1 \times G_2 \rightarrow G_T$ , where  $G_1$  is an additive group whose generating point of order  $q$  is  $P$  on a super-singular elliptic curve  $E : y^2 = x^3 + x \text{ mod } p$  with an embedding degree of 2, where  $p$  is a 512 bits length number and  $q$  is a 160 bit length Solinas number prime number and the equation

## 2.4. Analyses

Security	Alazzawi	Bayat	Malhi	ECLAS
Feature	et al. [78]	et al. [84]	etal [85]	
SF-1	✓	✓	✗	✓
SF-2	✓	✓	✓	✓
SF-3	✓	✓	✓	✓
SF-4	✗	✗	✓	✓
SF-5	✗	✗	✗	✓
SF-6	✓	✗	✗	✓

Table 2.2: Comparison Analysis of Security Features Satisfied

OPs	$T_{bp}$	$T_{bp.m}$	$T_{bp.sm}$	$T_{bp.a}$	$T_H$	$T_{e.m}$	$T_{e.sm}$	$T_{e.a}$	$T_h$
ms	4.211	1.709	0.0535	0.0071	4.406	0.4420	0.0138	0.0018	0.0001

Table 2.3: Execution Times of Cryptographic Operations

$p + 1 = 12qr$  holds. For the ECC based scheme to achieve a security level of 80 bits  $G$  is an additive group that is generated by a point  $P$  on a non-singular elliptic curve  $E : y^2 = x^3 + ax + b \pmod{p}$  of order  $q$ , where  $p$  and  $q$  are two 160 bit prime numbers for  $p > 3$ ,  $a, b \in Z_q^*$ .

For convenience, we will define the notations for execution time for different cryptographic computations in the schemes under discussion as portrayed in Table 2.3, where OPs stands for the type of operations involved. We borrow the execution time directly from [48], which was evaluated using MIRACL cryptographic library, to assess the efficiency of schemes. Operations which are very light like addition operation in  $Z_q^*$  and multiplication operation in  $Z_q^*$  will not be considered.

The clear description of the operations is given as follows.

$T_{bp}$ : Execution time for bilinear pairing operation,  $e(P, Q)$ , where  $P, Q \in G_1$

$T_{bp.m}$ : Execution time for scale multiplication operation  $x.P$ , related to pairing operation  $e(P, Q)$ , where  $P, Q \in G_1$ , and  $x \in Z_q^*$

$T_{bp.sm}$ : Execution time for small scale multiplication operation,  $v_i.P$ , related to pairing operation  $e(P, Q)$ , where  $P, Q \in G_1$ ,  $v_i.P$ ,  $v_i \in [1, 2^t]$  is a small random integer, for a small integer  $t$ .

$T_{bp.a}$ : Execution time for point addition operation, related to pairing operation  $e(P, Q)$ , such that  $R = P + Q$ , where  $R, P, Q \in G_1$

$T_H$ : Execution time for map-to-point hash function operation related to pairing operation  $e(P, Q)$ , where  $P, Q \in G_1$ .

$T_{e.m}$ : Execution time for scale multiplication operation,  $x.P$ , over ECC group, where  $P \in G$  and  $x \in Z_q^*$ .

$T_{e.sm}$ : Execution time for small scale multiplication operation,  $v_i.P$ , for small exponent test, where  $P \in G$  and  $v_i \in [1, 2^t]$  is a small random integer, for a small integer  $t$ .

$T_{e.a}$ : Execution time for point addition operation,  $R = P + Q$ , where  $R, P, Q \in G$ , related to ECC.

$T_h$ : Execution time for one hash function operation.

Schemes	Message Signing	Individual verify	Aggregate verify
Horng et al [58]	$3T_{e.m} \approx 1.326$	$3T_{bp} + T_{e.m} + T_H$ $\approx 17.481$	$3T_{bp} + nT_{e.m} + nT_H$ $\approx 12.633 + 4.4198n$
Cui et al [44]	$T_{e.m} + T_{e.a} + T_h$ $\approx 0.4439$	$3T_{e.m} + 2T_{e.a} + 2T_h$ $\approx 1.3298$	$(n + 2)T_{e.m} + 4nT_{e.a}$ $+ nT_H + nT_h$ $\approx 6.2973n$
Xiong et al [86]	$3T_{bp.m} + 2T_{bp.a} + T_h$ $\approx 5.1413$	$3T_{bp} + 2T_{bp.m} + T_{bp.a}$ $+ T_H + T_h$ $\approx 19.2262$	$3T_{bp} + 2nT_{bp.m} + nT_{bp.a}$ $+ nT_H + nT_h$ $\approx 12.633 + 7.8312n$
Tzeng et al [33]	$3T_{bp.m} + T_H$ $\approx 9.533$	$2T_{bp} + T_{bp.m}$ $\approx 10.131$	$2nT_{bp} + nT_{bp.m}$ $\approx 10.131n$
Kamil et al [54]	$3T_{e.m} + 2T_{e.a} + 3T_h$ $\approx 1.3297$	$2T_{e.m} + T_{e.a} + T_h$ $\approx 0.8859$	$2nT_{e.m} + nT_{e.a} + nT_h$ $\approx 0.8859n$
ECLAS	$2T_{e.m} + T_h$ $\approx 0.8841$	$2T_{e.m} + T_h$ $\approx 0.8841$	$2nT_{e.m} + nT_h$ $\approx 0.8841n$

Table 2.4: Comparison of Computation Cost for Related CLAS Schemes

## Computation Cost Analysis

In this section, we give a formal security proof on the proposed certificate-less signature scheme. While using the computation execution times for various dominant time-consuming cryptographic operations summarized in Table 2.3, we carry out computation analysis of related CLAS schemes [33, 44, 54, 58, 86] in terms the three phases of message signing, individual verify and aggregate verify overhead in RSU. The observation is clear that our proposed scheme, ECLAS, has better computation performance to related works from Table 2.4. In [58], to generate a signature a vehicle carries out three scalar multiplication,  $3T_{e.m}$ , over elliptic curve. This means the computation cost for signing is  $3T_{e.m} \approx 1.326ms$ . Whilst for verifying a signature, three bilinear pairings, one scalar multiplication over elliptic curve and one map-to-point hash function operations are required. Thus, individual verification needs  $2T_{bp} + T_{e.m} + T_H \approx 17.481$ . In aggregate verification phase, three bilinear pairings,  $n$  scalar multiplication over elliptic curve and  $n$  map-to-point hash function operations are required,  $2T_{bp} + nT_{e.m} + nT_H \approx 12.633 + 4.4198n ms$ . In the proposed ECLAS scheme, for signature generation a vehicle requires two scalar multiplication with respect to elliptic curve and one hash function operation,  $2T_{e.m} + T_h$ , amounting to the computation load of  $2T_{e.m} + T_h \approx 0.8841 ms$ . For individual signature verification, ECLAS, similarly requires two scalar multiplication with respect to elliptic curve and one hash function operation,  $2T_{e.m} + T_h$ , amounting to the computation load of  $2T_{e.m} + T_h \approx 0.8841$ . Whereas for aggregate signature verification, ECLAS requires  $2n$  scalar multiplication with respect to elliptic curve and  $n$  hash function operation,  $2nT_{e.m} + nT_h$ , yielding computation cost of  $2nT_{e.m} + nT_h \approx 0.8841n ms$ . in a similar manner, the computation cost for other relevant comparable schemes [33, 44, 54, 86] can be calculated. The computation cost for message signing and individual signature verification is illustrated in Figure. 2.5, based on the summary results from Table 2.4 and Figure. 2.5, ECLAS has all over computation efficiency to the rest of the scheme except [44], and although it has slightly lower signing computation overhead it was found with security flaws in [54] whereas the proposed scheme satisfy the security requirements and withstand KGC escrow property. For simplicity sake, by regarding equal computation capabilities for signing and verifying then we can lump up the computation load that the same signing and verifying entity incurs for a single signature. As such the overall load for Horng et al. [58] comes up to  $1.326 + 17.481 = 18.807$  and for Cui et al. [44] the overall load is  $0.4439 + 1.3298 = 1.7737$ . Proceeding in this manner for the rest of the schemes, Xiong et al.[86], Tzeng et al. [33], Kamil et al. [54] the overall computation loads are; 24.3675, 19.664, 2.1887 respectively. Subsequently, ECLAS has an overall computation load of 1.7682, which is better than the rest as shown in Figure. 2.5.

The relationship of verification time delay for particular number of aggregate signatures that RSU takes to compute for the schemes [33, 44, 54, 58, 86], against the proposed scheme ECLAS, is portrayed in the Figure. 2.6.

As a requirement in VANETs, vehicles have to broadcast their messages every 100 – 300ms, thus it entails that an RSU or AS can receive about 180 messages every 300ms.

## 2.4. Analyses

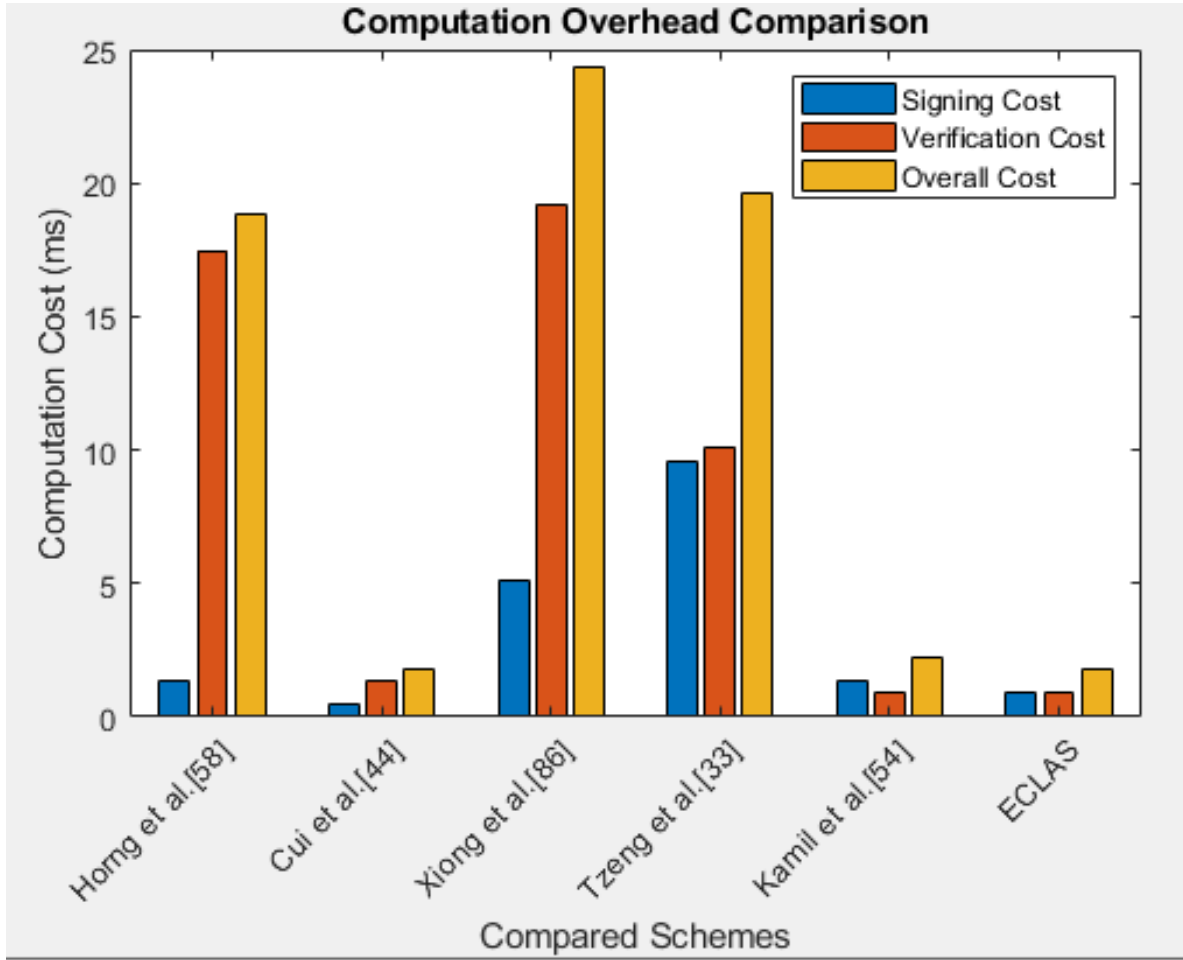


Figure 2.5: Computation Cost Comparison Per Unit.

Therefore, in one second an RSU is expected to verify about 600 – 2000 messages [54]. In Figure. 2.6, it endeavours to illustrate the time it takes to do batch verification for 2000 signatures. Thus, the comparative analysis shows that the proposed scheme has less verification time delay for  $n$  signature aggregation and the number of signatures has a direct proportion linear relationship to the verification delay.

### Communication Cost Analysis

In this portion of the chapter now, we will present the communication overhead of the proposed scheme against the related schemes [33, 44, 54, 58, 86] by borrowing experiment results from [48] to account for transmission cost for sending packets from vehicle to RSUs in V2I or V2V communication in VANETs, the sizes of elements in  $G_1$  and  $G$  are 128 bytes and 40 bytes respectively, in addition the elements in  $Z_q^*$ , the value of hash function and timestamps are 20 bytes, 20 bytes and 4 bytes respectively. We will consider the message traffic load for signatures only.

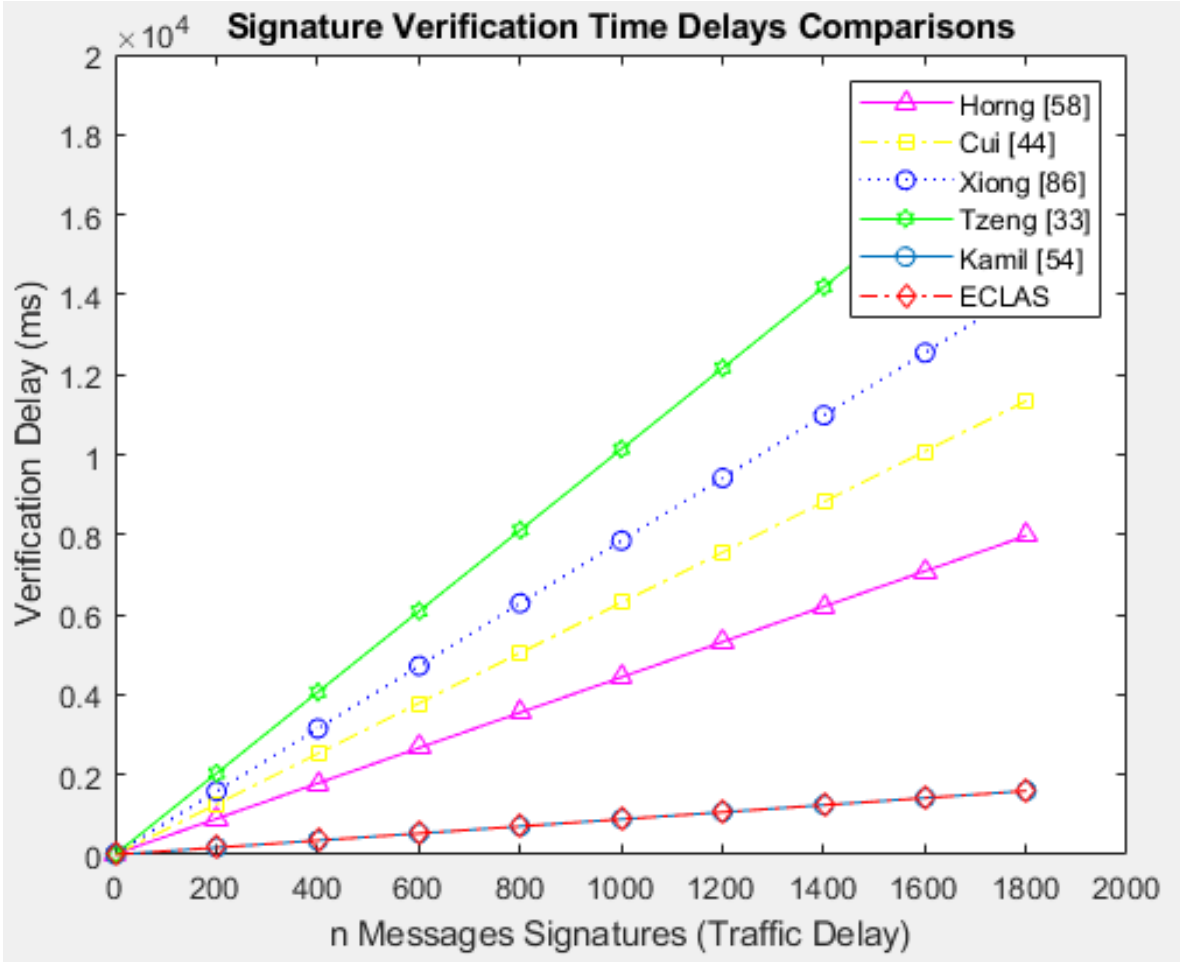


Figure 2.6: Verification Time Delays and Number of Signatures Relationship.

In [58], the vehicle broadcast the message  $(ID_i, vpk_i, M_i, t_i, \sigma_i = (R_i, S_i))$  to RSUs, where  $ID_i, vpk_i, R_i, S_i \in G$  and  $t_i$  is a timestamp. Therefore, the communication overhead is  $3 \times 40 + 4 = 124$  bytes. In [44] the vehicle sends the message  $(ID_i, vpk_i, Q_{ID_i}, \sigma_i = (R_i, S_i), t_i)$  to RSUs or AS, where  $ID_i, vpk_i, Q_{ID_i}, R_i \in G$ ,  $S_i \in Z_q^*$  and  $t_i$  is the timestamp. Thus, the communication load on the network is  $4 \times 40 + 20 + 4 = 184$  bytes. In [86] the vehicle sends  $(ID_i, m_i, upk_i, signature(U_i, V_i))$  to RSU, which requires the bandwidth size of  $4 \times 40 + 20 + 4 = 184$  bytes. Whereas, in [85] the message sent from a vehicle to RSU is  $(PS_j, PS1_j, P_i, PP_i, \sigma_i = (U_i, V_{ijk}))$  where  $PS_j, PS1_j, P_i, PP_i, U_i, V_{ijk} \in G$ . Therefore, the communication overhead is  $6 \times 128 = 768$  bytes. In the proposed, ECLAS, scheme a vehicle sends traffic related signed message  $(ID_i, Q_{ID_i}, vpk_i, M_i, t_i, \sigma_i)$  to the verifier where  $ID_i \in G$ . Therefore, the total communication overhead is  $4 \times 40 + 20 + 4 = 184$  bytes. The proposed scheme has less communication overhead load than [58, 85] and is at par with the schemes in [77, 82, 86] as outlined in Table 2.5. However these comparable work are found to be insecure in different aspects, like in [44], which so far has descent efficient output, was discovered



## 2.5. Summary

Schemes	Sending of one signature message	Sending of $n$ signature message
Horng et al. [58]	644 bytes	644n bytes
Cui et al. [44]	184 bytes	184n bytes
Xiong et al.[86]	184 btes	184n bytes
Malhi [85]	768 bytes	768n bytes
Kamil et al. [54]	184 bytes	184n bytes
ECLAS	184 bytes	184n bytes

Table 2.5: Communication Overhead Summary

that the scheme is insecure in [54, 58].

## 2.5 Summary

In this chapter, we presented an efficient certificate-less signature scheme with conditional privacy preservation for VANETs enhanced smart grid system that is based on elliptic curve cryptography and it provides user anonymity. The proposed work also removes the inherently key escrow problem associated with identity based cryptography by means of incorporating derivation of a full private key by the vehicle itself. Security proof under the random oracle model approach, shows that the proposed scheme is secure by virtue of satisfying all the security requirements for VANETs. In this scheme certificate-less property is achieved without key escrow problem since the signature is derived by using a vehicle's full private key which is not known by the KGC . Furthermore, the scheme does not require the computation intensive bilinear pairing and map-to-point hash function operations but rather is just based on less intensive operation over elliptic curve group in the design, hence achieving efficient computation cost. Even the communication overhead is within bounds with comparable schemes whilst achieving higher security merits. Thus, it is a comparatively efficient certificate-less aggregate signature scheme ideal for VANETs communications.



# Chapter 3

## Certificate-less Authenticated Key Agreement Scheme with Anonymity for Smart Grid Communications

### 3.1 Introduction

The modern grid has various functionalities by using remote sensor automation in power management, monitoring and controlling the system. Thus, it is imperative to ensure secure communications for various agents in smart grid, since the system is information communication based. Being information based the smart grid encounters security and privacy challenges impeding its adoption. One way of dealing with these cyber concerns is in devising robust cryptosystem for data encryption and authenticated key agreement in the communications of these remotely controlled smart devices. However, many proposed solutions are provided at the expense of computations cost. Thus, this paper designs a novel authenticated key agreement scheme with anonymity based on widely acceptable elliptic curve cryptography with efficiency. The scheme ensures optimal computation and communication overload whilst achieving mutual authentication and anonymity in the key agreement process. The scheme is proven in both formal and informal security analysis in portraying its satisfaction of the standard and extended Canetti–Krawczyk (eCK) security requirements. A comparative analysis with related schemes indicates that the proposed scheme have merits over others. The modern grid uses intelligent systems that seamlessly monitor all processes automatically in real-time [87–91]. In smart grid, the smart capability in facilitating near real-time service delivery relies on communication infrastructures like advanced metering infrastructure (AMI), wide-area situational awareness (WASA) and wide area monitoring systems (WAMS), which have promising applications. However, the concentration of the discussion will focus on the security of the AMI part of the grid. The AMI is a backbone network of smart devices that ensures two-way information flow between the consumer and the utility company [92]. It is an example of machine-to-machine (M2M) communication infrastructure with the SM on the customer side and control center (CC) on the util-

ity side. In between the SM and CC there are different kinds of intercommunicating intelligent electronic devices (IEDs) working in system stabilization functionalities like monitoring and system management such as, phasor measurement units (PMUs), phasor data concentrators (PDCs), circuit break monitors units, solar flare detectors. This section of the AMI employs smart data aggregation approaches and technologies, as a way of leveraging the computation load of the devices involved in an IoT context, to facilitate fast data exchange and reduce unnecessary delays. The considerable amount of data generated by these devices needs efficient handling and security assurance for smart grid applications [93]. It is apparent that smart grid cybersecurity and user privacy protection is a critical issue [91, 94, 95]. As such SG requires in-built security mechanism by design to maintain the systems operations securely and preserve users privacy. Therefore transactions in the modern grid bear a lot more economic value than in the ordinary grid. Some of the transactions with economic value in smart grids are dynamic pricing, demand response, distributive electricity trading. Thus, the system attracts fraud and cyber attacks. Therefore, there is need for good management to check without tampering of data or loss of information by using robust cryptographic measures. As a rule of thumb mutual authentication must be provided as a first recommendation to ensure trust in secure communications by ascertaining the true identity of the communicating party, before indulging in the exchange of sensitive information over the open channel. Even further, anonymity is a required technique that can help check user privacy and traceability concerns when carrying out regular transactions [96]. Thus, the importance of robust authenticated key agreement schemes comes into play to ensure smart meter's anonymity and untraceability on the network. Smart meter anonymity prevents an adversary from discovering the real identity of a smart meter, therefore the smart meter is not traceable and all its transmissions seem random to the adversary. Much research has been done and is still on-going in order to provide security and privacy protection. However, most of the recent work [97–104], have the drawback of involving time-consuming computation especially on the resource constrained smart meter side. Although, in the subsequent communications two entities are universally secured by symmetric key algorithms such as the AES, 3DES among others, however there is need of getting a shared key in advance. This calls for key establishment mechanisms to generate a symmetric key for a particular session, which is the focus of this work and most similar works in literature. The session key is generated by using public key cryptosystem, usually known as key agreement. The main contributions of the current paper are listed below as follows.

- An anonymous and untraceable key agreement scheme is presented, where the real identity for smart meter is never transmitted in plain text in the authentication process.
- Maintains the classical security requirements of confidentiality, integrity, and authentication while ensuring overall good performance.
- It achieves ideal performance in terms of computation and communication costs

### 3.2. Related Works and Limitations

as it excludes heavier computation operations.

- A careful security analysis shows that the scheme is provably secure in extended Canetti–Krawczyk (eCK) model amidst fulfilment of the security requirements in heuristic approach.

The rest of the paper is organized according to the outline given as follows. Section II reviews most relevant related works of AKA schemes for smart grids communication. Section III provides that mathematical building blocks for the proposed scheme. Section IV give the detailed steps of the proposed work. Section V, presents an in-depth analysis of the scheme in terms of security, privacy and performance assessment. Finally, in VI we give concluding remarks about the proposed scheme.

## 3.2 Related Works and Limitations

In SG, there has been continuous research in authentication and key exchange cryptosystems for securing AMI communications [97–99, 101–103, 105–110]. In this section, a critical scrutiny of the schemes will be presented thoroughly. In [102], a secure privacy preserving authentication scheme based on elliptic curve cryptography was proposed. Their scheme has merits in computation and communication efficiency and provides security requirements besides fulfilling anonymity and mutual authentication. Further, the analysis was presented in random oracle and validated in AVISPA security analysis tool. However, we feel there are some inconsistencies in the some elliptic curve point multiplication operations. Mahmood et al. [111], designed a hybrid Diffie-Hellman authentication scheme for smart with the goal of authenticating a smart meter and the gateway. Nevertheless, Li et al. [105], noted that their scheme is weak against identity leakage, impersonation attack and session key leakage. In [108], another ECC based scheme was proposed, however it is highlighted in [112] that their scheme fails to ensure password guessing attack, insider attack, privacy protection and impersonation attack. In [100], an efficient and secure authentication and key agreement protocol for 5G networks using block-chain was presented. The presented work employs digital signature and bilinear pairing technique to resolved distributed denial of service (DDoS) attack. Though deemed to have low computation overhead, it can still be improved by removing the computation intensive bilinear pairing operations. In [103] an anonymous key distribution scheme was presented by using identity-based signature that does not require a trusted anchor in the process. nevertheless, in [109], Odelu et al., exposes the scheme in [103], as being vulnerable to ephemeral key leakage attack. In [113], another anonymous furnished scheme was proposed, designed to withstand key escrow issue which was found in the work of [98, 103, 109]. The scheme was validated to be secure by using proverif tool and is purported to be comparatively more efficient. However, we notice computation in-consistence in key establishment process, especially the misuse of the bilinear pairing operations. Although, authentication cryptosystems have been widely worked on in recently years, still more research work needs to be

done to realise practical schemes suitable for resource constrained network environment [106, 109]. Generally, most of proposed schemes fall short in providing anonymity, resilience to common security attacks and untraceability security requirements. So to this effect, achieving robust security and privacy preservation with optimal computation cost in cryptosystems is still an open research issue. Although Mohammadali et al., [106], proposed a lightweight scheme based on ECC which was formally validated by using AVISPA tool, it is noted in [114] that their scheme does not consider privacy-preservation during authentication. In a quest to provide a solution to user privacy concern, Chen et al. [101], proposed an authentication scheme. However, the scheme was based on bilinear pairings and Diffie-Hellman problem. Although, explicit formal analysis was done using BAN logic and random oracle model, the bilinear pairings demerits the scheme in terms of required computation cost. The scheme in [98], by He et al., was devised with the aim of striking a balance between computation cost and provision for robust secure with privacy preservation by supporting smart meter anonymity. The authors in [99], however claim that, the scheme in [98] falls short of providing key escrow attack resilience, inferring that the trusted anchor (TA) can generate the session key, negotiates by entities under it. Additionally, the scheme in [98] suffers from private key leakage and known session-specific temporary information attacks. Wazid et al. [115] proposed, a three factor authentication protocol based on ECC by using lighter operations such as XOR and hash operations among others. In the same vain, Kumar et al. [97], designed an ECC based authenticated key exchange scheme, but was flawed by having time synchronization clock for the timestamp. So the scheme in [99], was proposed to provide novelty in efficiency and being ideal for anonymous authentication with formal proof and implementation experiment presented. However, the schemes in [97–99, 101] were quashed by [114] that they still bear relatively heavy computation load. Use of certificate-less cryptosystems to achieve robust and efficient security mechanism, formulated by combining the advantages of tradition public key cryptography and identity-based techniques in the construction, while solving the key escrow problem has inspired this work [86, 116, 117].

### 3.3 Preliminaries

This section, presents the mathematical primitives used, the system model, security requirements and the threat model for the against the proposed scheme.

#### Security Requirements

Any secure AKA scheme must ensure satisfaction of default security requirements which are key in any network based communication outlined as follows.

- **Mutual Authentication:** This is a means of ascertaining two-way authentication, whereby either of the two communicating entities authenticates the counterpart before indulging in the communication. This can be done presentation

### 3.4. The Proposed CL-AKA scheme for Smart Grid

of a valid verification token such as a digital certificate before the occurrence of subsequent communication. In our case, the smart meter and the service provider authenticates each other.

- **Anonymity and Untraceability:** The real identity of a smart meter is concealed and can not be linked to a particular session of communication. Any two completed session can not be related to a certain identity, but rather they all appear as random in the eyes of eavesdropping adversary.
- **Perfect Forward Secrecy:** In this feature, we are assured that the session key will not be compromised even in the case whereby the long-term private key of a user is compromised. Thus, an adversary in possession of a private key would not be able to derive any previously established session key and thereby access the previous communications.
- **Availability:** This aspect gives assurance that the system and data is accessible to any authenticated user whenever needed.
- **Integrity:** Integrity means the accuracy and completeness of transmitted data. Incorporating this feature in the design of a scheme entails that the data is secured from modification, or misuse by unauthorized party.

In cryptography, forward secrecy (FS), also known as perfect forward secrecy (PFS), is a feature of specific key agreement protocols that gives assurances that session keys will not be compromised even if long-term secrets used in the session key exchange are compromised. The notations used for the main scheme are outlined and described in Table 3.1.

## 3.4 The Proposed CL-AKA scheme for Smart Grid

This section presents the details of the proposed, Certificate-Less Authenticated Key Agreement Scheme for Smart Grid Communications, christened as (CL-AKA). CL-AKA follows a hierarchical communication model, with the SM at the lowest level and the control center as the highest while intermediate gateway point, link the two major communicating networks as illustrated in Figure 3.1.

The scheme has four main phases which are: (1) System Initialization Phase, (2) Entity Registration Phase, (3) Entity Self Key Generation and (4) Authenticated Key Agreement Phase, with the detailed description given as follows.

### 3.4.1 System Initialization Phase

The utility as the system trusted anchor (TA), initializes the system to produce the parameters used in the authentication process and it proceeds as follows.

Table 3.1: Notations Used in the Proposed Scheme

Symbols	Meanings of Symbols in the Scheme
$SM_i$	$i^{th}$ smart meter, where $i = 1, 2, \dots, n$
$AP_j$	$j^{th}$ access point, where $j = 1, 2, \dots, m$
$ID_i$	An identity for a smart meter, $SM_i$
$ID_j$	An identity for an access point, $AP_j$
$psk_k$	Partial private key for an entity identified by $k$
$(x_k, x_kP)$	Secret key & public key for an entity identified by $k$
$s_k$	Full private key for an entity $ID_k$ (i.e. $SM_i$ or $SP_j$ )
$T_i$	Validity period for the pseudo-identity $ID_i$ for $V_i$
$RID_i$	A real identity for the vehicle $V_i$
$(P_{pub}, \alpha)$	TA's public key & master key respectively
$M_i$	Session key established between two parties $i$ , for $i = 1, 2$
$t_i$	Current timestamp, for $i = 1, 2$

- The TA takes a  $k$ -bit prime  $q$  as its system security parameter and produces the set of  $\{F_q, q, p, P, G, E \setminus F_q\}$ .
- TA selects  $\alpha \in Z_{*q}$ , as its master secret key, with the corresponding public key computed as  $P_{pub} = \alpha P \in E \setminus F_q$ .
- Then TA selects hash functions defines as,  $H : \{0, 1\}^* \rightarrow Z_q^*$ .
- TA publishes the final system parameter,  $\{F_q, q, p, P, P_{pub}, G, E \setminus F_q, H\}$ .

### 3.4.2 Entity Registration Phase

This phase explains how the communicating entities which are, the smart meter and the service provider, under the the same overall TA are registered and issued with key parameters that enables secure session key between them. An entity identified



### 3.4. The Proposed CL-AKA scheme for Smart Grid

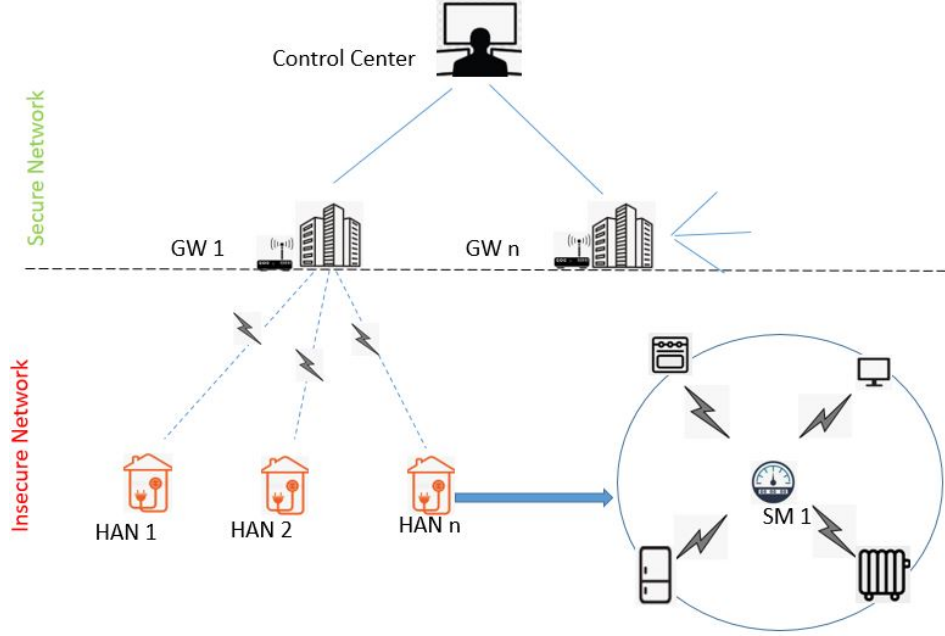


Figure 3.1: CL-AKA hierarchical communication model

by  $ID_k \in \{0,1\}^*$ , undergoes the following steps for registration. The  $ID_k$  is used for simplicity sake as the process stands for either smart meter or service provider.

- A user submits its identification,  $ID_k$ , to the TA.
- The TA chooses a random number  $d_k \in Z^*_q$  and then computes  $Q_k = d_kP$  and  $psk_k = d_k + H(ID_k||Q_k)\alpha$ .
- TA sends the partial private key to an entity  $ID_k$  as  $(psk_k, Q_k)$  through a secure channel.

#### 3.4.3 Entity Self Key Generation Phase

In this phase the concerned entity,  $ID_k$ , chooses a random number  $x_k \in Z^*_q$  and sets it as its private key with corresponding public key,  $pk_k = x_kP$ . Finally,  $ID_k$ , formulate its full private key by combining the self derived key materials with the partial private key material,  $psk_k$ , received from the TA during registration. So the full private key used for verifiable authentication is  $s_k = x_k + psk_k$ . The preceding three phases are summarized in Figure 3.2.

#### 3.4.4 Authenticated Key Agreement Phase

This phase allows mutual authentication between two entities  $ID_i$  and  $ID_j$  under the same TA. Here,  $ID_i$  stands for a smart meter whereas  $ID_j$  for the service provider,

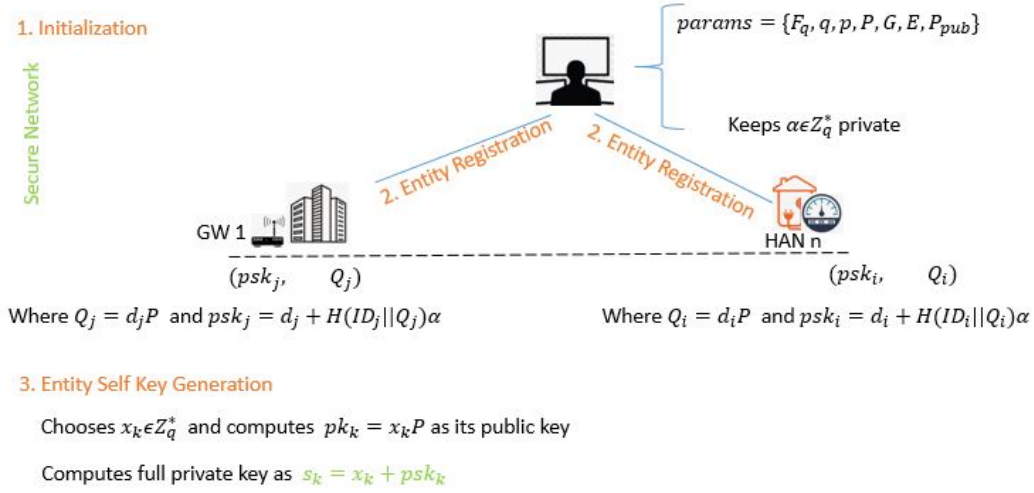


Figure 3.2: CL-AKA three phases summary diagram.

such that  $ID_i \in \{ID_k\}$  as well as  $ID_j \in \{ID_k\}$ . This notation applies to all the other parameters indexed by  $k$  respectively. Now in an event where the smart meter,  $SM_i$ , and any service provider,  $SP_j$ , want to agree on a session key for secure subsequent communications, then the following steps are sequentially executed. The whole process of the authenticated key agreement procedure is outlined in Figure 3.3.

1.  $SM_i$  selects a random number  $r_i \in Z_q^*$ , then computes,  $C_1 = r_i P$ ,  $C_2 = r_i(pk_j) \oplus ID_i$ ,  $V_i = H(C_1 || C_2 || t_1) + s_i$ . Then  $SM_i$  sends message  $M_1 = \{C_1, C_2, V_i, t_1\}$  to  $SP_j$ .
2. On receipt of message  $M_1$  at time  $t_1^*$ , first  $SP_j$ , checks the freshness of the received message by testing whether,  $t_1^* - t_1 < \Delta$ , otherwise it quits the session.
3. Then  $SP_j$ , extracts the identity  $ID_i$  but calculating,  $ID_i = C_2 \oplus x_j C_1$ , hence  $SP_j$  authenticates the message sender by checking whether,  $V_i.P = H(C_1 || C_2 || t_1) + pk_i + Q_i + H(ID_i || Q_i)P_{pub}$ , holds, otherwise the session can be aborted.
4.  $SP_j$  selects a random number  $r_j \in Z_q^*$  and further computes,  $C_3 = r_j P$ ,  $C_4 = r_j(pk_i) \oplus ID_j$ ,  $V_j = H(C_3 || C_4 || t_2) + s_j$ .
5. Lastly,  $SP_j$  sends the message  $M_2 = \{C_3, C_4, t_2\}$  to  $SM_i$ . For  $SP_j$ , the session key is calculated as,  $SK_{ji} = H(ID_i || ID_j || V_i || V_j || r_j C_1 || t_1 || t_2)$ .
6. On receipt of message,  $M_2 = \{C_3, C_4, V_j, t_2\}$ , first  $SM_i$  checks whether  $t_2^* - t_2 < \Delta$ , where  $t_2^*$  stands for current time, is within acceptable range, if its not within range the session is aborted right away.

### 3.5. Security Analysis and Performance Evaluation

7. Otherwise,  $SM_i$ , checks whether  $V_j.P = H(C_3||C_4||t_2) + pk_j + Q_j + H(ID_j||Q_j)P_{pub}$ . If the calculation holds,  $SM_i$  extracts the identity as  $ID_j = C_4 \oplus x_i(C_3)$ . The agreed session key with  $SP_j$  is computed as,  $SK_{ij} = H(ID_i||ID_j||V_i||V_j||r_iC_3||t_1||t_2)$ .

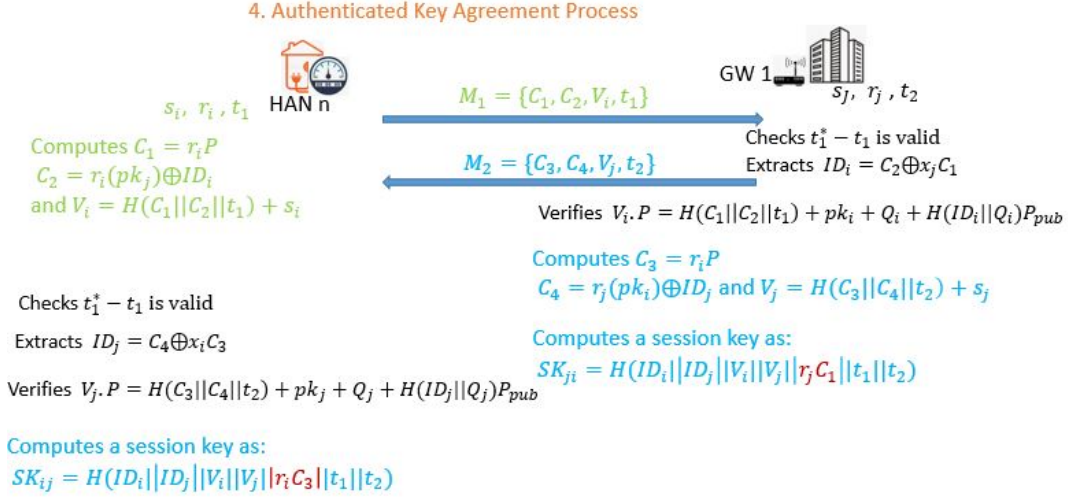


Figure 3.3: The session key establishment between SM and SP

## 3.5 Security Analysis and Performance Evaluation

This part of the section discusses the formal security proofs and the performance evaluation of the proposed scheme in terms of computation and communication costs efficiency. The security analysis is done in both eCK and standard model. In these models the adversary gets a hash function value from using the hash function instead of querying the challenger for a hash value. In these oracle security proofs, three lists  $L_i$ , where  $i = 1, 2, 3$  are set as input lists and the corresponding tuple of lists  $H_i$  where  $i = 1, 2, 3$  are set as output lists respectively. So in the interplay of oracle queries, the outputs of the hash functions are not randomly selected by the challenger  $\mathcal{C}$ , but rather are derived from a real hash function.

**Theorem 3.** *Two matching session instances generate the same session key.*

**Proof:** In line with consistency analysis, two matching sessions generate the same session key, in agreements with the state of the input. Separately, let's consider other important situations surrounding the capabilities of an adversary,  $\mathcal{A}$ , in carrying out an attack. Assume that  $\mathcal{A} \in \{\mathcal{A}_1, \mathcal{A}_2\}$  actuates at most  $n_1$  honest participants, of which each of them is engaged in at most  $n_2$  sessions. Suppose that the test session for  $\mathcal{A}$  is denoted as  $\Pi_{I,J}^S$ . Then there are three methods for  $\mathcal{A}$  to determine the session key from a randomly selected string.

1. Guessing method:  $\mathcal{A}$  gets the correct session key by guessing.
2. Key replication method:  $\mathcal{A}$ , sets a no-matching session key to a targeted session of choice  $\Pi_{IJ}^S$ . So  $\mathcal{A}$  will be tasked to obtain a real session key by querying a non-matching session.
3. Forging method: For an instance,  $\mathcal{A}$  computes the value  $H_3(ID_I || ID_J || V_I^S || V_J^S || (r_J C_1)^S || t_I || t_J)$ , thus to say  $\mathcal{A}$  gets the authentication validating elements for session key construction.

**Theorem 4.** *The advantage of  $\mathcal{A}_1$  against the new scheme is negligible in the standard model if the ECCDH problem is intractable.*

**Proof:** Let  $\mu$  be the secure parameter in the adversarial model game. Assume a Type I adversary  $\mathcal{A}_1$ , that can win the game with non-negligible advantage  $Adv_{\mathcal{A}_1}(\mu)$  exists. Then this entails existence of a challenger,  $\mathcal{C}$ , that can solve the ECCDH problem with non-negligible probability.

In the guessing method, the probability of correctly guessing the value for the session key  $SK \in Z_q^*$  at random is  $\frac{1}{q-1}$ .

In key replication method, the hash function,  $H_3$ , must output the same value for two unique input values. Since the assumption of a secure hash function with collusion resistance holds on  $H_3$ , then  $\mathcal{A}$ 's probability of success in this method of attack is negligible.

On the other hand, forging method of attack takes place in the eCK model, where a challenger,  $\mathcal{C}$ , interacts with an adversary,  $\mathcal{A}_1$ .

Let the tuple  $(P, aP, bP)$  stand for an instance of a ECCDH problem. If  $\mathcal{A}_1$  can successfully forge a correct secret value with non-negligible advantage  $Adv_{\mathcal{A}_1}(\mu)$ , then by implication the challenger,  $\mathcal{C}$ , can employ  $\mathcal{A}_1$  to solve the ECCDH problem,  $abP$ , with non-negligible probability. In the inception of the game,  $\mathcal{C}$  chooses two integers randomly say  $I, J \in \{1, n_1\}$  where  $I \neq J$ , and also chooses an integer  $S \in \{1, n_2\}$ , then sets the test session as  $\Pi_{IJ}^S$ . Thus the probability that  $\mathcal{C}$ , guesses the test session correctly is less than  $\frac{1}{n_1^2 n_2}$ . If  $\Pi_{IJ}^E$  and  $\Pi_{IJ}^S$  are matching sessions, then six attack scenario must be considered.

- $CA_1$ -1.  $\Pi_{IJ}^E$  exists, but  $\mathcal{A}_1$  can not obtain the ephemeral secret key of  $ID_I$  and  $ID_J$ .
- $CA_1$ -2.  $\Pi_{IJ}^E$  exists, but  $\mathcal{A}_1$  can not obtain the ephemeral secret key of  $ID_I$  nor obtain the partial private key of  $ID_J$ .
- $CA_1$ -3.  $\Pi_{IJ}^E$  exists, but  $\mathcal{A}_1$  can not obtain the partial private key of  $ID_I$  nor obtain the ephemeral key for  $ID_J$ .
- $CA_1$ -4.  $\Pi_{IJ}^E$  exists, but  $\mathcal{A}_1$  can not obtain the partial private key of  $ID_I$  and  $ID_J$ .

### 3.5. Security Analysis and Performance Evaluation

- $CA_1$ -5.  $\Pi_{IJ}^E$  does not exist, but  $\mathcal{A}_1$  can not obtain the ephemeral secret key of  $ID_I$  nor the partial private key  $ID_J$ .
- $CA_1$ -6.  $\Pi_{IJ}^E$  does not exist, but  $\mathcal{A}_1$  can not obtain the partial private key of  $ID_I$  and  $ID_J$ .

The concise details of the six attack scenarios is given individually in the following analysis.

#### $CA_1$ -1 analysis

**Set-up:** The attacker follows the same procedure as in the real scheme, LAC-AKA, as such  $\mathcal{C}$  sends the public  $params = \{F_q, q, p, P, P_{pub} = \alpha P, G, E, F_q, H_1, H_2, H_3\}$  to  $\mathcal{A}_1$  and keeps  $\alpha$  secret.

**Query:**  $\mathcal{C}$  would like to construct a matching session by utilizing the responses to queries from  $\mathcal{A}_1$  and it chooses  $ID_k^*$  for  $ID_k$  and answers successive queries from  $\mathcal{A}_1$ . The queries and corresponding answers are recorded into a list which is initially empty and it is used as a repository of responses. The steps proceed as follows.

- Query ( $PK_k$ ):  $\mathcal{C}$  has the list  $L_U$  of the tuple  $(ID_k, x_k, pk_k, s_k, Q_k, C_1, C_3)$ .  $\mathcal{A}_1$  submits an identity of choice  $ID_k^*$ , then  $\mathcal{C}$  randomly chooses  $x_k^*, r_k^*$  computes  $pk_k^* = x_k^*P$  and  $Q_k^* = d_k^*P$  and adds them to the list  $L_U$ . So the updated list becomes  $(ID_k, x_k^*, pk_k^*, s_k, Q_k^*, C_1, C_3)$ .
- Replace ( $PK_k$ ):  $\mathcal{A}_1$  substitutes  $ID_k$  public key for  $pk_k^* = x_k^*P$ . Thus  $\mathcal{C}$  replaces  $pk_k$  with  $pk_k^*$  and updates the tuple  $(ID_k, x_k, pk_k, s_k, Q_k, C_1, C_3)$  to  $(ID_k, *, pk_k^*, s_k, Q_k, C_1, C_3)$ , where  $*$  stands for a the secret value  $x_k^*$  or the symbol  $\perp$ . Meaning to say,  $\mathcal{A}_1$  may manage to replace the secret value randomly or not.
- Query ( $SV_k$ ):  $\mathcal{A}_1$  gives an identity  $ID_k$  and  $\mathcal{C}$  brings out  $(ID_k, x_k, pk_k, s_k, Q_k, C_1, C_3)$  from the list  $L_U$  and returns  $x_k$ . If  $\mathcal{A}_1$  replaced the public key  $pk_k$  but did not submit a new secret value, then  $\mathcal{C}$  replies with  $\perp$  to reject.
- Query ( $PPK_k$ ):  $\mathcal{A}_1$  submits an identity  $ID_k$ , and  $\mathcal{C}$  checks  $(ID_k, x_k, pk_k, s_k, Q_k, C_1, C_3)$  in the list  $L_U$  and computes,  $Q_k^* = d_k^*P$ ,  $psk_k^* = d_k^* + H_1(ID_k || Q_k^*)\alpha$  and then returns  $psk_k^*$ .
- Query ( $ESK_k$ ):  $\mathcal{C}$  has a list of the tuple  $(ID_i, ID_j, s, a_i, b_j)$ ,  $\mathcal{A}_1$  submits an instance of a session,  $\Pi_{ij}^s$ , and then  $\mathcal{C}$  follows the steps.
  1. If  $\Pi_{ij}^s = \Pi_{IJ}^S$  or  $\Pi_{ij}^s = \Pi_{IJ}^E$ , then  $\mathcal{C}$  fails and stops.
  2. Otherwise  $\mathcal{C}$ , chooses at random  $a_i^*, b_j^* \in Z_q^*$  and return  $(a_i^*, b_j^*)$  and adds  $(ID_i, ID_j, s, a_i^*, b_j^*)$  and updates  $L_W$ .
- Query ( $SK_k$ ):  $\mathcal{A}_1$  submits  $\Pi_{ij}^s$ , and  $\mathcal{C}$  does the following. If  $\mathcal{A}_1$  replaced the public key,  $pk_k$ , while it did not submit the new secret value  $x_k^*$ , then in this case  $\mathcal{C}$ , refuses to reply.

1. If  $\Pi_{ij}^s = \Pi_{IJ}^S$  or  $\Pi_{ij}^s = \Pi_{IJ}^E$ , then  $\mathcal{C}$  fails and stops.
  2. If  $\mathcal{A}_1$  makes Query( $ESK_k$ ) for  $\Pi_{ij}^s$ ,  $\mathcal{C}$  finds  $(ID_i, ID_j, s, a_i, b_j)$  in the list  $L_W$ , and finds  $(ID_k, x_k, pk_k, sk_k, Q_k, C_1, C_3)$  or  $(ID_k, x_k, pk_k, sk_k, Q_k, C_4, C_5)$  in the list  $L_U$ , and computes  $Q_k^* = d_k^*P$  and  $psk_k^* = r_k^* + H_1(ID_k || Q_k^*)\alpha$ , then it follows the schemes procedure to compute the session key by performing the key agreement algorithm.
  3. Otherwise  $\mathcal{C}$ , chooses at random  $a_i^*, b_j^* \in Z_q^*$  and return  $(Q_k^*, a_i^*P)$  and adds  $(ID_i, ID_j, s, a_i^*, b_j^*)$  and updates  $L_W$ .
- Send  $(\Pi_{ij}^s, m)$ : To this  $\mathcal{C}$  responds to the queries as follows.
    1. If  $(\Pi_{ij}^s, m) = (\Pi_{IJ}^S \perp)$ ,  $\mathcal{C}$  finds  $(ID_I, x_I, pk_I, s_I, Q_I, C_1, C_3)$  in the list  $L_U$  and then returns  $(Q_I, aP)$ .
    2. If  $(\Pi_{ij}^s, m) = (\Pi_{IJ}^E \perp)$ ,  $\mathcal{C}$  finds  $(ID_J, x_J, pk_J, s_J, Q_J, C_4, C_5)$  in the list  $L_U$  and then returns  $(Q_J, bP)$ .
    3. If  $(\Pi_{ij}^s, m) = (\Pi_{ij}^s \perp)$ , where  $(\Pi_{ij}^s, m) \neq (\Pi_{ij}^s \perp)$  and  $(\Pi_{ij}^s, m) \neq (\Pi_{IJ}^E \perp)$ ,  $\mathcal{C}$  finds  $(ID_I, x_I, pk_I, s_I, Q_I, C_1, C_3)$  and does as follows.
      - (a) If  $\mathcal{A}_1$  makes Query( $ESK_k$ ) for an instance  $\Pi_{ij}^s$ , then  $\mathcal{C}$  finds  $(ID_i, ID_j, s, a_i, b_j)$  in the list  $L_W$ , and returns  $(Q_k^*, aP)$ .
      - (b) Otherwise  $\mathcal{C}$ , chooses at random  $a_i^*, b_j^* \in Z_q^*$  and returns  $(Q_k^*, aP)$  and adds  $(ID_i, ID_j, s, a_i^*, b_j^*)$  to the list  $L_W$ .
    4. If  $m_2$  is the second message in the session, such that  $m_2 = (Q_k^*, *)$ ,  $\mathcal{C}$  accepts the session.
  - Test  $(\Pi_{ij}^s)$ :  $\mathcal{A}_1$  needs to submit a new secret value  $x_i^*$  ( $x_j^*$ ) when the public key  $(pk_i)$  (or  $pk_j$ ) has been replaced to  $(pk_i^*)$  (or  $pk_j^*$ ). This is a logical request, because  $\mathcal{C}$  cannot derive the session key, without knowledge of the secret values for  $ID_i$  and  $ID_j$ . So  $\mathcal{C}$  responds to the query as follows.
    1. If  $\Pi_{ij}^s \neq \Pi_{IJ}^S$ , then  $\mathcal{C}$  fails and stops.
    2. If  $\Pi_{ij}^s = \Pi_{IJ}^S$ ,  $\mathcal{C}$  selects at random  $s_k \in Z_q^*$  and returns it to  $\mathcal{A}_1$ .

**Solving ECCDH Problem:** If  $\mathcal{A}_1$  wins by forging method then  $\mathcal{A}_1$  must be able to compute,  
 $H_3(ID_I || ID_J || V_I^S || V_J^S || (r_J C_I)^S || t_I || t_J)$  or  
 $H_3(ID_I || ID_J || V_I^S || V_J^S || (r_I C_J)^S || t_I || t_J)$ , where  $V_I^S = H_2(C_1 || C_2 || t_1) + x_J + b_J + H_J(ID_J || Q_J)\alpha$ ,  
 $V_J^S = H_2(C_3 || C_4 || t_2) + x_I + a_I + H_1(ID_I || Q_I)\alpha$ ,  $r_J C_I^S = r_J \cdot r_I P$  or  $(r_I C_J^S = r_I \cdot r_J P)$ .  
Then,  $\mathcal{C}$  finds  
 $(ID_I, ID_J, V_I^S, V_J^S, C_1, C_2, C_3, C_4)$  in  $L_W$ ,  $(x_I, a_I)$  and  $(x_J, b_J)$  in the list  $L_U$ . finally,  $\mathcal{C}$  solve the problem  $abP$

### 3.5. Security Analysis and Performance Evaluation

**Probability:** If  $\mathcal{C}$  guesses the session test instance  $\Pi_{I,J}^S$ , then he will succeed during the query phase. Therefore  $\mathcal{C}$  can compute the value  $abP$  with the probability  $\frac{1}{n_1^2 n_2} Adv_{\mathcal{A}-1}(\mu)$ , if  $\mathcal{A}_1$  succeeds in winning the game with advantage  $Adv_{\mathcal{A}}(\mu)$ .

#### 3.5.1 Informal Security Analysis

The security attribute of the proposed scheme are further confirmed in the following heuristic security analysis.

- **Mutual Authentication:** The  $SM_i$  verifies that  $V_j.P = H_2(C_3||C_4||t_2) + pk_j + Q_j + H_2(ID_j||Q_j)P_{pub}$  and on the other hand  $SP_j$  verifies that  $V_i.P = H_2(C_1||C_2||t_1) + pk_i + Q_i + H_2(ID_i||Q_i)P_{pub}$  holds there by authenticating the legitimacy of the counterpart. Moreover, they generate the session key by exchanging the random ephemeral key components by using the ECDCH problem, in  $r_i C_3 = r_i r_j P$  and  $r_j C_1 = r_j r_i P$ . These values are an accessible and unchangeable to an attacker but only to a legitimate user hence the communicating entities authenticate each other hence, the proposed work achieves mutual authentication.
- **Anonymity:** In the scheme the real identity of an entity  $ID_i$  or  $ID_j$  if not transmitted in plain but rather in concealed and intractable state as in  $C_2 = r_i(pk_j) \oplus ID$  or  $C_4 = r_j(pk_i) \oplus ID_j$ . Moreover the identity is not even traceable as the ephemeral key is random for any session of communication. Therefore, privacy preservation is assured in the proposed work.
- **Perfect Forward Secrecy:** Calculation of session key  $SK_{ij}$  or  $(SK_{ji})$  is unique per each session due to dynamic random numbers  $r_i$  and  $r_j$  used in the message elements  $C_1$  and  $C_3$ . With this feature the generated session keys for an  $n^{th}$  session has no linkage to another one of an  $(n + 1)^{th}$  session. So compromise of a particular session is no use for an  $\mathcal{A}$  to deduce anything for any session key for another session.
- **Key Escrow:** The key escrow problem is solved in our proposed work by virtue of upgrading the partial private key element,  $psk_k = d_k + H_1(ID_k||Q_k)$ , issued by TA into an secretly known key termed full private key  $s_k = x_k + psk_k$  for  $x_k \in Z_q^*$ . The full private key, comprised of static secret values from the TA and the entity itself and no party of the two can generate it on its own. Thus any message encrypted by this key can not be decrypted by the TA since it does not know the the self generated secret  $x_k$  for an entity  $ID_k$ . In addition derivation of session key involves the ephemeral keys  $r_i, r_j$  which are inaccessible to any other party apart from the own as they are intractable in *ECDLP* problem. So by design the TA cannot generate the same session key of targeted entities of the system.
- **Known Key Security:** The generation of the session key,  $SK_{ij} = H_3(ID_i||ID_j||V_i||V_j||r_i C_1||t_1||t_2)$  or  $SK_{ji} = H_3(ID_i||ID_j||V_i||V_j||r_i C_3||t_1||t_2)$

involves dynamic random elements  $r_i, r_j$  by way of using hash function. Since these random elements are unique and dynamic in each session run no attack can re-use the message elements,  $C_1, C_2, C_3$  and  $C_4$  derived from these ephemeral keys  $r_i$  and  $r_j$  in other future session authentication. Moreover, the ephemeral keys cannot be extracted in  $C_1 = r_i P$  and  $C_3 = r_j P$ , since that involves a ECDLP problem. Therefore, the proposed scheme provides known-key security.

- **Man-in-the-Middle Attack Resilience:** The mutual authentication between two parties registered under the same TA is employed to check such malicious adversary as man-in-the-middle attacker. The computation of  $C_2$  and  $C_4$  respectively uses a fresh ephemeral key  $r$ , of which is validated to be true and intact in the verification of  $V_i$  and  $V_j$  in the computations,  $V_i.P = H_2(C_1||C_2||t_1) + pk_i + Q_i + H_2(ID_i||Q_i)P_{pub}$  and  $V_j.P = H_2(C_3||C_4||t_2) + pk_j + Q_j + H_2(ID_j||Q_j)P_{pub}$  respectively.  $\mathcal{A}$  can not manage to fabricate anything to pass the verification of the message element  $V_i$  or ( $V_j$ ), as there is integrity check as well as proper registration check. Therefore, launching a man-in-the-middle attack in this case is impossible.
- **Replay Attack Resilience:** Although an adversary  $\mathcal{A}$  intercepts plying messages between  $SM_i$  and  $SP_j$ , still she can not be successful to replay to either party at later time. This is so because all messages are timestamped and the lapse time interval,  $t_i^* - t_i < \Delta$  for  $i = 1, 2$  is checked. The integrity of  $t_i$  is upheld in the computation of  $V_1 = H_2(C_1||C_2||t_1)$  or  $V_2 = H_2(C_3||C_4||t_2)$ , implying that  $t_i$  cannot be manipulated to satisfy  $\Delta$  and either  $SM_i$  or  $SP_j$  will detect the modification during verification of  $V_1$  or  $V_2$  respectively.
- **Impersonation Attack Resilience:** An adversary  $\mathcal{A}$  cannot succeed to impersonate  $SM_i$  (or  $SP_j$ ) without knowledge of the static full private key  $s_i = x_i + psk_i$  and the same applies to  $SP_j$  impersonation. Surely, to maliciously obtain the static full private key of an entity  $s_i$  or  $s_j$  by  $\mathcal{A}$  is infeasible. So launching impersonation attack on the scheme is not possible.

### 3.5.2 Comparison Analysis

In this section, a detailed presentation of the proposed scheme on security and functionality features, computation and communication costs against related key agreement research works in smart grid and other resources constraint environment, is given to assess its performance. To carry out the evaluation we analyze the scheme with the notable ones in: Deng et al. [117], Abbasinezhadi-Mood and Nikooghadam [99], Mahmood et al. [108], Tsai and Lo [103].



### 3.5. Security Analysis and Performance Evaluation

#### 3.5.3 Security and Functionality Features Comparison

In Table 3.2, the security and functionality features is given against the highlighted schemes, with respected to the outlined features, in the Table 3.2 with the symbol  $\checkmark$  indicating provision of the said feature and the symbol  $\times$ , indicating failure to provide for the feature.

Table 3.2: Comparison Analysis of Security Features Satisfied

Security Feature	Deng et al. [117]	Abbasinezhadi & Nikooghadam [99]	Mahmood et al. [108]	Tsai & Lo [103]	Proposed
SF-1	$\checkmark$	$\checkmark$	$\times$	$\checkmark$	$\checkmark$
SF-2	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$
SF-3	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$
SF-4	$\times$	$\times$	$\checkmark$	$\checkmark$	$\checkmark$
SF-5	$\times$	$\times$	$\times$	$\checkmark$	$\checkmark$
SF-6	$\checkmark$	$\times$	$\times$	$\checkmark$	$\checkmark$
SF-1	$\checkmark$	$\checkmark$	$\times$	$\checkmark$	$\checkmark$
SF-2	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$
SF-3	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$
SF-4	$\times$	$\times$	$\checkmark$	$\checkmark$	$\checkmark$
SF-5	$\times$	$\times$	$\times$	$\checkmark$	$\checkmark$
SF-6	$\checkmark$	$\times$	$\times$	$\checkmark$	$\checkmark$

**Note:** SF-1: "Privileged-insider attack resilience"; SF-2: "Anonymity"; SF-3: "Untraceability"; SF-4: "Man-in-the-middle attack resilience"; SF-5: "Strong replay attack resilience"; SF-7: "Tamper resistance"; SF-8: "Perfect forward secrecy"; SF-9: "Impersonation attack resilience"; SF-10: "Key escrow-less"; SF-11: "Known key security"; SF-12: "Mutual authentication";

For instance, the scheme in [99] does not provide strong replay attack resilience and strong privacy preservation. Whereas in [108], it is found that the scheme is weak against, privacy preservation, strong replay attack, strong mutual authentication among other. In a similar manner the rest of the referred schemes are analysed comparatively.

### 3.5.4 Computation Cost Analysis

In this section, a computation comparison with related schemes designed for smart grid and other resource constrained network environments, [99, 103, 108, 117, 118] is presented. The execution times for different cryptographic operations, based on the experimental result found done in [98] is portrayed in Table 4.2. Negligible operations like bit-wise XOR, normal hash function are not included in the analysis.

Table 3.3: Execution Times for Cryptographic Operations

Symbol for Operation	Description of the Operation	Execution Time <i>ms</i>
$T_{bp}$	Bilinear pairings	0.032713
$T_s$	Symmetric encryption	0.000012
$T_{inv}$	Modular Inversion	0.000034
$T_{G_1-pm}$	Point multiplication in $G_1$	0.013405
$T_{G_1-pa}$	Point addition in $G_1$	0.000056
$T_{G_1-mtp}$	Map-to-a-point hashing in $G_1$	0.033582
$T_{G_2-mul}$	Multiplication in $G_2$	0.000008
$T_{G_2-exp}$	Exponentiation in $G_2$	0.002249
$T_{ecc-pm}$	An ECC point multiplication	0.003350
$T_{ecc-pa}$	An ECC point addition	0.000014

The computation cost incurred for authentication and key agreement, in the proposed work in comparison to relevant related works in tabulated in Table 4.3. We suppose that the smart meter side  $SM_i$ , stands for any resource constrained devices in need of establishing a session key with a more equipped computationally gateway side, here specified as the service provider side,  $SP_j$ . In the proposed scheme the  $SM_i$  side requires,  $4T_{ecc-pm} + 4T_{ecc-pa} \approx 0.013456ms$  and similarly the  $SP_j$  requires  $5T_{ecc-pm} + 4T_{ecc-pa} \approx 0.013456ms$  for the key negotiation process. On the other hand, in Jo et al. [118],  $5T_{ecc-pm} + T_{ecc-pa} \approx 0.016764ms$  is required for the  $SM_i$  side computation whilst the  $SP_j$  side requires  $4T_{ecc-pm} + T_{ecc-pa} \approx 0.013414ms$  respectively.

It is prominent that the proposed scheme is outstanding in computation cost efficiency as compared to relevant related worked as outline in Table 4.3. Even though, Jo

### *3.5. Security Analysis and Performance Evaluation*

et al. [118] has a slightly lower computation load with respect to the service provider's demand to our proposed work, our scheme only requires one smart meter message pass to service provider while in [118] two smart meter message passes are required, to achieve message authentication code (MAC), in the key agreement process.

Table 3.4: Comparison of Computation Cost in  $ms$  for Authentication & Key Agreement

Schemes	Smart meter side computational load	Service provider / data collection side computational load
Deng et al. [117]	$5T_{ecc-pm} + 3T_{ecc-pa}$ $\approx 0.016792$	$5T_{ecc-pm} + 3T_{ecc-pa}$ $\approx 0.016792$
mahmood et al. [108]	$9T_{ecc-pm} + 3T_{ecc-pa}$ $\approx 0.030192$	$9T_{ecc-pm} + 3T_{ecc-pa}$ $\approx 0.030192$
Tsai & Lo [103]	$6T_{G_1-pm} + 2T_{G_1-pa} + T_{bp} + T_{G_2-exp}$ $\approx 0.115504$	$3T_{bp} + T_{ecc+pm}$ $\approx 0.101489$
Abbasinezhadi & Nikooghada [99]	$8T_{ecc-pm} + 2T_{ecc-pa}$ $\approx 0.026828$	$8T_{ecc-pm} + 2T_{ecc-pa}$ $\approx 0.026828$
Jo et al. [118]	$5T_{ecc-pm} + T_{ecc-pa}$ $\approx 0.016764$	$4T_{ecc-pm} + T_{ecc-pa}$ $\approx 0.013414$
He et al. [98]	$10T_{ecc-pm} + 2T_{ecc-pa}$ $\approx 0.033528$	$10T_{ecc-pm} + 2T_{ecc-pa}$ $\approx 0.033528$
Odelu et al. [109]	$5T_{G_1-pm} + 2T_{G_1-pa} + 3T_{G_2-exp}$ $\approx 0.073884$	$4T_{G_1-pm} + 4T_{G_1-pa} + 2T_{bp} + 2T_{G_2-exp}$ $\approx 1.195182$
Proposed	$4T_{ecc-pm} + 4T_{ecc-pa} \approx 0.013456$	$4T_{ecc-pm} + 4T_{ecc-pa} \approx 0.013456$

### 3.5. Security Analysis and Performance Evaluation

An illustration of the incurred computation load for smart meters in the comparison analysis of the schemes [99, 103, 108, 109, 117–119], against the proposed CL-AKA scheme is given in Figure ??.

#### 3.5.5 Communication Cost Analysis

In this section we will consider different parameters and their bit length sizes to estimate the bandwidth consumption of different schemes. The outline is such that: "identity", "random nonce", "timestamp", "signature by using ECDSA", "bilinear pairings of groups  $G_1$  and  $G_2$ ", "hash function output", "message authentication code", require the sizes: 160, 128, 32, 320, 320, 512, 160, and 160 bits respectively and an elliptic curve point  $P = (P_x, P_y)$  requires  $(160 + 160 = 320)$ -bits. Table 4.4.3, gives a comparison table of the performance.

Table 3.5: Communication cost comparison table for authentication and key agreement

Scheme	No. of messages	Communication cost (in bits)
Deng et al. [117]	2	640
mahmood et al. [108]	2	2304
Tsai & Lo [103]	3	1408
Abbasinezhadi & Nikooghada [99]	3	1440
Jo et al. [118]	3	1536
He et al. [98]	3	1632
Odelu et al. [109]	3	1920
Proposed	2	960

As is well known that "the security of 160-bit ECC has the same security level to that 1024-bit RSA cryptosystem" . In the proposed scheme, two messages are needed for session key agreement,  $M_1 = \{C_1, C_2, V_i, t_1\}$  and  $M_2 = \{C_3, C_4, V_j, t_2\}$  which demands  $(160 + 160 + 128 + 32) = 480$ -bits and  $(160 + 160 + 128 + 32) = 480$ -bits respectively. so the cumulative communication cost is  $480 + 480 = 960$ -bits In [118], three messages are needed in the key establishment process,  $MSG_1$ ,  $MSG_2$  and  $MSG_3$  with their respective demands as follows;  $(320 + 32) = 352$ -bits,  $(320 + 160 + 320 + 32) = 832$ -bits and  $(160 + 160 + 32 = 352)$ -bits, so the cumulative communication load is

$352 + 832 + 352 = 1536$ -bits. On the other hand, the scheme in [117] has a decent output on communication cost with two message exchanges  $\{R_i, M_i\}$  and  $\{R_j, M_j\}$  demanding  $(160 + 160) = 320$ -bits and  $(160 + 160) = 320$ -bits and has a cumulative load of  $(320 + 320) = 640$ -bits.

## 3.6 Summary

In this chapter, we presented an anonymous efficient certificate-less authenticated key agreement scheme for smart grid communication. The main contribution is the designing of adaptable security scheme for resource constrained smart grid environment, based on elliptic curve cryptography. Key merits for the scheme are: ensuring mutual authentication, efficient computation and communication overhead. Semantic security proof is given in eCK model to show in-feasibility of breaking the scheme by the adversary, and heuristic proof is given to substantiate satisfaction of security features acclaimed. By virtue of precluding heavy computations the scheme has better comparative advantage to other key agreement scheme. Future work, will focus on doing network emulation using hardware implementation like Raspberry Pi, to emphasize the applicability of the proposed scheme.

# Chapter 4

## Lightweight Privacy-Preserving Data Aggregation Scheme Based on Elliptic Curve Cryptography for Smart Grid Communications

### 4.1 Introduction

As the future power grid, smart grid surpasses the legacy grid with a greater advantage due to incorporation of advanced communication technology in the electricity system [120–125]. In accordance to the model of National Institute of Standards and technology (NIST), smart meter based at the residential area collects and sends real-time electricity usage data to the operation center (OC) , and in a similar manner a SM receives command messages related to control and management of electricity from OC [20]. In SG the electricity data bears economic value as it can be used for electricity marketing, management and regulation in applications such as demand response [126–128]. An existing challenge with the electricity consumer’s consumption data is that it contains privacy information such that it can reveal the user’s identification, lifestyle pattern and habits of electricity usage of the consumers, which is not a desirable thing[129–133].

In smart grid, recording of power consumption data is done not on month-to-month basis as is the case with the legacy grid, but rather is based on times of the day and gives details of the power consumption of individual appliances on the customers side in near real-time intervals [81, 134]. On the negative note this detailed information has a potential of being used maliciously by an attacker to invade privacy and security. For instance, by knowing the times house owners’ sleep or are absent from home based on analysis of SM information flow, thieves can plan to break into the homes when nobody is at home. Hence there is great need to protect the consumer’s side against privacy and security breaches associated with smart meter information, with respect to the basic security requirements. That is to ensure SM communications should be supported with

user authentication and identification measures when transacting on the open network between the SM and the monitoring device. Encryption with efficient algorithm for the customer consumption information transmitted by the SM to the utility or third party service providers will also be needed. The communication scheme should also protect individual energy consumer information from third parties for commercial purposes not related to services provided by the utility that is the scheme should be resilient to all sort of insider attacks [116].

However, the current challenge is ensuring security and privacy of smart grid AMI communications and balancing between lightweight cryptographic measures and ideal computational complexity for resource constrained devices. Once lightweight privacy-preserving and security mechanism are ascertained, consumers and utility are likely to have a widely varying preferences on how they wish to control and monitor third party to access their information. Thus, the challenge to protect user's privacy information effectively and efficiently has attracted researchers attention to find a lasting solution [116, 135–138]. Such solutions would ensure the adoption of internet of things(IoT) applications over smart grid, since they consist of resource-constrained devices. Privacy-preserving data aggregation approach is one of viable mechanisms feasible for achieving data privacy[139–141]. Privacy-protection safeguards the fine-grained user data from disclosure to unwanted parties like the gateway or the system service provider during transmission and in some cases even protected from insider attack within the control center itself. Data aggregation is an ideal solution for securing data from eavesdroppers and has the advantage of improving network performance by virtue of reducing communication traffic. This approach goes with the following requirements: 1) the data aggregation operator can obtain sum of usage data in a region; 2) the data aggregation operator should know nothing about individual usage data in the data collection region [142–144].

In this regard, homomorphic encryption (HE) is a prospective mechanism for ensuring data aggregation privacy because it allows cipher-text manipulation without divulging plain-text [145]. The HE technique allows performing of addition operation or multiplication operation on encrypted cipher without requiring decryption, which is the desirable property for the aggregation operator to do, since it is a semi-trusted entity. There are several other data aggregation techniques such as using random numbers secrete sharing, Boneh-Goh-Nissim homomorphic encryption, Paillier homomorphic encryption, data slicing, differential privacy among other techniques [146]. In random number secret sharing design a series of random numbers with underlying properties are initially distributed to all the entities in the network that is to, all users and the data aggregation operators in advance, which are later used to obfuscate the usage data transmitted in the network [147]. The drawback of such a mechanism is reliance on Trusted Third Party (TTP) responsible for generating and distributing such random numbers. Differential privacy is also a technique for achieving privacy which adds random noise of Laplacian distribution or other distributions to mask the original value



## 4.2. Related Works and Limitations

[148]. However, in many studies, this technique of differential privacy is deemed less accurate, as it is easily affected by noise [149]. Secret sharing which was proposed by Shamir in [150], is also another mechanism used to achieve privacy data aggregation. In this method group secret is split into shares and distributed amongst the participants and each one is kept highly confidential. The secret can only be reconstructed with a sufficient number of participants colluding and combining their secret values together, as such it is good for storing highly sensitive information [151]. However, most of these approaches are coupled with unbearable computation burden, which is an issue of major concern.

In this chapter, a Lightweight Privacy Preserving Data Aggregation Scheme Based on Elliptic Curve for Smart Grid Communications is proposed, with the following main contribution are:

- The proposed scheme design precludes certificate and TTA or TA dependency, hence ensures system overall management requirements significantly.
- The scheme uses lightweight mathematical building blocks that are bilinear pairing-free, thus resulting in reduction of transmission delay from node to node communications.
- The proposed scheme has optimal computation and communication efficiency based on the security analysis and performance evaluation, and so the scheme has comparative advantage over other variant works, by its merits.
- Most importantly the proposed scheme ascertain user anonymity when communicating over a public channel beside providing content privacy.

In this vain, our work endeavors to design and incorporate these main contributions, and performance comparison with some state-of-the-art privacy-preserving data aggregation techniques provided. Thus, the proposed work achieves better overall communication and computation efficiency to the best comparable scheme besides better satisfaction of main security requirements.

The rest of the paper is organized as follows: Section 2, reviews related works in data aggregation over smart grid environment and pin-points the research gap and limitations in other researches. Then we present the generic system design model, basic mathematical and cryptographic preliminaries required for understanding the proposed scheme in Section 3. The proposed lightweight privacy-preserving data aggregation scheme is presented in Section 4. Further Section 5 gives the analysis and evaluation of results respectively. Finally, the conclusion and suggestions for further research are presented in Section 6.

## 4.2 Related Works and Limitations

A variety of techniques and approaches for privacy-preserving data aggregation (PPDA) have been proposed in literature in a quest to address the challenge of secure data

aggregation to be practical in SG network environment. In [152] Liu .Y, et al, proposed a 3PDA data aggregation scheme for SG, however the scheme uses computationally expensive bilinear pairings in the data collection units (DCUs) and the OC which is not ideal for a system of systems comprising of myriads of communicating devices. While in [147] He .D, et al, designed an efficient PPAD scheme but is based on TTP which is not also a desirable feature in a highly populated network since it bears a bottleneck for the TTP to manage the messages with efficiency. Similarly in [153] Jo H.J, et al asserts that their construction is efficient at the expense of using bilinear computations which contradicts the claim for a practical scheme. Additionally, in [27] it is disclosed that their scheme does not provide user privacy as the identity is transmitted in plain-text hence prone to human-factor-aware data aggregation (HDA) attacks and all sorts of privacy breaches. Other researches based their construction on computationally expensive Paillier's homomorphic cryptosystem [120, 154, 155], which still need some improvement to be deemed practical for smart grid because the Paillier's primitives is comparative heavier although is it widely used technique [156]. Achieving acceptable level of computational as well as communication efficiency is a default requirement for any real-time based communication technology like IoT-enhanced smart grid. In the schemes [120, 154, 155], their security is anchored in the gateway as it plays a trusted role and it provides the aggregated data to the OC. The proposed scheme in [153], does not rely on trusted gateway but rather uses a group approach to sent encrypted messages. The private key is secretly held by a group of smart meters and they collude to send an encrypted message to the AMI. In order for the AMI or OC to decrypt data, it requires the selected smart meters to help in the decryption which adds on overhead and clearly this is impractical design. Although the scheme removes trust-ship, it incurs unnecessary communication overhead in the collusion process. Also the design is prone to differential attack hence can suffer from privacy breach. To achieve this the AMI collude with participating smart meter to decrypt two different messages representing the sets which differ only by a single user. At the end the AMI can deduce the user's data from the difference of the two decrypted messages. Although the scheme [134] claims to be robust in security and efficiency, we analyzed it and found it lacking to provide user anonymity as the identity is transmitted in plain-text, hence is prone to eavesdropping, and also in [133] it was found to have its properties unattributed. In 2011, Wu and Zhou [157] proposed a key exchange scheme for smart grid based on elliptic curve cryptography (ECC) which required a trusted authority (TA) and a public key infrastructure (PKI) for key management. The authors of [157] claim their scheme is resistant to replay attacks and man-in-the-middle attacks. However in [158] Xia and Wang discovered that the scheme in [157] cannot provide replay attack and man-in-the-middle attack resilience and has even vulnerable session key. In 2018, Mahmood et al. [108] proposed an authentication scheme between two communicating entities in smart grid, however in [159] it is pointed out that the scheme in [108] has weakness of lack of perfect forward secrecy. Although in [160], it was assessed that the proposed data obfuscation approach provides good data throughput, good packet delay and delivery ratio under a variety of conditions, in [132] they found it bears high communication

## 4.2. Related Works and Limitations

latency due to large bandwidth requirement and also in [133] they point out that the scheme in [160] fails to explicitly state its focusing field, whether is it for customer billing applications or grid operations. Another ECC based multi-dimensional data aggregation scheme was proposed by Boudia et al. in [129], which does not require bilinear pairings hence having efficient computation overhead. However, the scheme is flawed by being TA dependent. In [131], Badra and Zeadally, proposed an ECC based privacy-preserving data aggregation scheme by utilizing homomorphic encryption and Diffie-Hellman techniques, however it bears heavy communication overhead.

Different schemes in literature have been proposed based on different approached and methodologies. Their short-falls varies widely ranging from; having high computation overhead [120, 152, 154, 160–163], prone to common attacks [31, 108, 157, 164] and high demand of system computation resources due to need of additional requirements for TTP, PKI and TA management in their designs [119, 126, 147, 165].

### 4.2.1 Generic System Model

In this section, we briefly describe the proposed data aggregation scheme’s network architecture, the preliminaries building blocks for the scheme and subsequently we define the security requirements for the model. The system design of our model is depicted in Figure 4.1, which consists of three main entities: SMs, data aggregation point (DAP) and the utility OC in a hierarchical structure, which follows the standard smart grid architecture[166, 167]. An OC has a number of neighborhood area networks (NANs) , in turns each NAN has numerous home area networks (HANs) [19, 126, 168–171]. The DAP is the gateway for a particular NAN which does data aggregation and relaying of information between OC and SM . Whereas for each HAN there is a SM enabling bi-directional communication with the DAP. In this model SMs collect real-time consumption data from the HAN and sends it to OC via DAP at 15 minutes regular intervals [108, 133, 172]. The communication between SM and DAP is through wireless technology such as Wi-Fi, RF mesh, 6LowPAN, ZigBee, Z-wave among other wireless communication protocols [134, 155, 163]. Smart meter transmitted data includes the bill, real-time electricity report, consumer identification and regular instruction dispatches. So, the DAP acts as a gateway for the neighborhood area network and bridges the SMs and the OC by utilizing long range and high bandwidth communication technology with low latency like WiMAX or, 3G, 4G communication technologies and wired links among others[134, 173–178]. As a gateway the DAP aggregates the collected individual SM data to leverage the computational overhead of OC in decrypting each SM’s information. Similarly, communication efficiency is still a challenging issue that requires permanent solution, since there will be hundreds or thousands of smart meters in regions reporting their electricity related information almost at the same time to the OC through the DAP.

The OC being in the utility side, is deemed honest-but-curious entity and can know customer’s electricity usage during a billing period of pricing and power management. This means the OC executes operations according to the scheme without launching

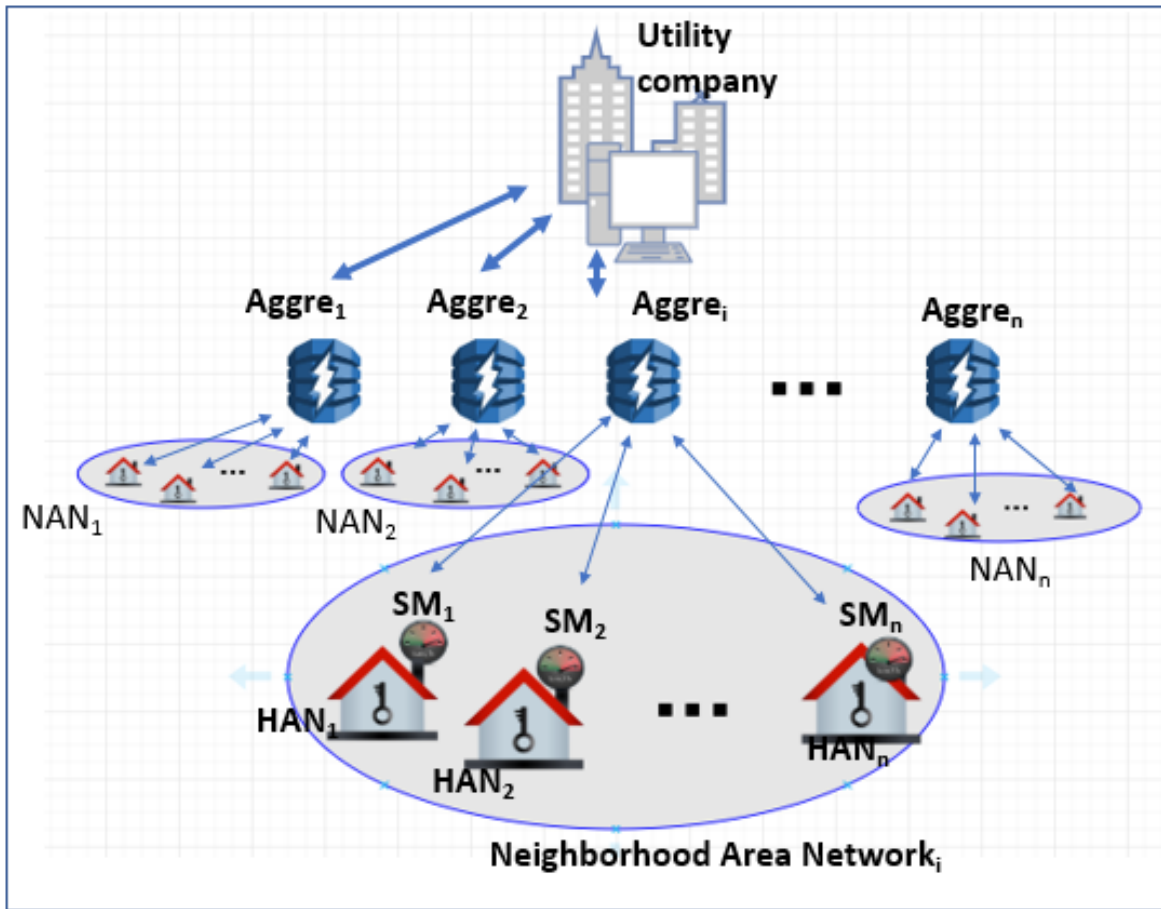


Figure 4.1: Generic System Model.

any active attack. On the other hand, the DAP is assumed not fully trusted since it can be easily controlled by an adversary. The user or SM is usually assumed as dishonest with some extent of trust or common interest to win incentives from the OC orders. A good property needed in this architecture is to conceal individual's electricity usage to neighboring SMs and the DAPs even in an attempt of smart meters launching a collusion attack. Thus, is necessary to secure the system from all sorts of attacks such as: data privacy attacks, relationship attacks, false data injection attacks and distortion attacks. Data privacy attack occurs when some malicious smart meter node collude with the gateway or another smart meter to obtain the real-time or total power consumption data of another uncompromised smart meter during a billing session. In relationship attack the gateway attempts to deduce user behavior and habits from the relationship between electricity consumption of different reporting intervals for one specific user. While false data injection refers to attack on the integrity of the data where an adversary introduces a code that compromises the correctness of the data. In distortion attack the gateway tries to forge a user's real-time power usage in order to disturb the billing system in smart grid.

## 4.2. Related Works and Limitations

### 4.2.2 Adversary Model

The public channel is open for an adversary,  $\mathcal{A}$ , which can forge, replay, modify and intercept plying message between communicating parties. However,  $\mathcal{A}$ , has no full access to private information from observing the public channel. Thus, the SM, DAP and OC are regarded as secure by themselves. The focus in this chapter, is to deal with a strong enough adversary which has access to the communication media able to perform the following malicious actions:

- Eavesdropping the communication channel between SM and DAP communications to get an idea of the smart devices usage data and other associated details.
- Impersonation attack on a particular user's smart meter and probably send falsified data on behalf of the targeted user
- Replay attack of legitimate transmitted messages to resend them after being intercepted. This attack can overload the authentication process and can result into transmission delay, denial of service (DoS) attack and communication bandwidth.
- Man-in-the-middle attack where by an adversary can actively eavesdrop on legitimate user's communications and relay modified messages between legitimate users making them believe they are communicating with intended counterpart.

### 4.2.3 Security Requirements

There is need to satisfy basic security requirements for the proposed scheme to ascertain the claimed security of the transmitted electricity reports from the consumer to the data aggregation points over the public channel as well as regulation and control commands originating from operation center to the consumer. Obviously, the data aggregation scheme faces all kinds of attacks from an adversary in between SM and DAP. The proposed scheme, achieves these attributes without relying on TTP or certificate issuance to facilitate the authentication process. Thus, our scheme design ensures conformity of the following prescribed requirements.

- *Authentication*: The DAP has to validate the true identity of the smart meter to make sure the data it receives really comes from the smart meter. Thus, the communicating entities should ascertain that they are communicating with the intended counterpart. This measure checks possible malicious acts such as message forgery, impersonation and masquerading attacks.
- *Data Confidentiality*: The mechanism must avoid any leakage of an individual's electricity usage data that could pose privacy breach. So, it is necessary to ascertain that no-one either internal or external attacker, extracts any individual's electricity usage data. So, confidentiality of user's electricity consumption data is very necessary since its leakage can reveal user's habit or identity which eventually exposes the user to attacks.

- *Data Integrity*: This mechanism ensures consistency and trustworthiness of the transmitted data, so that data is not altered nor modified by unauthorized party while in transit or elsewhere. This feature is of significantly importance in smart grid so that the data aggregation process should uphold integrity and message modification or forgery, and should there be any attempt for such attacks, should be detected.
- *Consumer Privacy and Anonymity*: The actual identity of a consumer in a community should not be known by any malicious party eavesdropping on the communications between consumer and OC. Thus, even if two instances of consumption data reports are eavesdropped the adversary should not distinguish if the two consumption reporting data are from the same user or not. Thus, a scheme should uphold user anonymity during the message flow of the concerned parties.
- *Attack Resilience*: Due to communication over a public channel, the data aggregation scheme must ensure security to withstand common attacks such as: impersonation attack, replay attack, modification attack and man-in-the-middle-attack [179, 180].

In regard to the discussed system model and security requirements, our main goal is to design a secure and efficient scheme for privacy-preserving data aggregation for smart grid AMI communications.

### 4.3 Proposed Scheme

We will present the framework of the proposed Lightweight Privacy-Preserving Data Aggregation (LPPDA) Scheme Based on Elliptic Curve Cryptography for Smart Grid Communications. The notation description of the symbols used in the proposed scheme is outlined in Table 4.1. Our construction suggests the variant construction of an El Gamal cryptosystem and an additive homomorphic encryption algorithm applied over elliptic curve field whose properties are:

- In order to encrypt a message  $m$  into a ciphertext  $C$  using an El Gamal approach, the sender, uses the public key of a receiver  $pk = xP$ , generates a random number  $r \in Z_q^*$ , with it computes  $C_a = rP$  and  $C_b = (pk)r + mP$ . Thus an encryption process proceeds as:

$$E_{pk}(m) = (C_a, C_b) = (rP, r(pk) + mP) = C \quad (4.1)$$

- So to decrypt a ciphertext  $C$ , the receiver uses its private key  $sk = x$ , and carry

### 4.3. Proposed Scheme

Table 4.1: Notations Used in our Scheme

symbols	Meanings of Symbols in the Scheme
$ID_s$	Identity of smart meter user, $SM_i$
$t_s, t_d$	Timestamps for SM and DAP
$e_i$	Electricity consumption generated by a smart meter at $t_s$
$\delta$	The time lapse for an interval of time from $t_s$ to $t_d$ .
$pk, sk$	Public key and private key respectively
$E_{pk}(\cdot)$	Encryption algorithm by using a public key $pk$ .
$D_{sk}(\cdot)$	Decryption algorithm by using a private key $sk$ .
$X_s, x_s$	Public key and private key of smart meter user respectively
$X_d, x_d$	Public key and private key of gateway respectively
$X_\alpha, x_\alpha$	Public key and private key of utility company

out the following operation.

$$\begin{aligned}
 D_{sk}(C) &= D_{sk}(E_{pk}(m)) & (4.2) \\
 &= (r(pk) + mP) - (sk)(rP) \\
 &= (r(xP) + mP) - x(rP) \\
 &= mP
 \end{aligned}$$

After which the message  $m$  can be retrieved by using the Pollards lambda method.

- (c) For additive homomorphic property, we suppose there are two messages encryption instances  $m_1$  and  $m_2$  transformed into two respective ciphertext instances  $C_1$  and  $C_2$  as follows.

$$\begin{aligned}
 E_{pk}(m_1) + E_{pk}(m_2) &= (r_1P, r_1(pk) + m_1P) + (r_2P, r_2(pk) + m_2P) & (4.3) \\
 &= ((r_1P + r_2P), ((r_1pk + m_1P) + (r_2pk + m_2P))) \\
 &= ((r_1 + r_2)P, (r_1pk + r_2pk) + (m_1P + m_2P)) \\
 &= ((r_1 + r_2)P, (r_1 + r_2)pk + (m_1 + m_2)P) \\
 &= E_{pk}(m_1 + m_2) \\
 &= (C_1 + C_2)
 \end{aligned}$$

(d) Scalar multiplication property.

$$\begin{aligned}
 E_{pk}(cx) &= \underbrace{E_{pk}(x) + E_{pk}(x) + \cdots + E_{pk}(x)}_{c\text{-times}} \\
 &= \sum_{i=1}^c E_{pk}(x)
 \end{aligned} \tag{4.4}$$

Where  $+$  is the additive homomorphic encryption operation and  $c$  is a constant for scalar multiplication.

The construction of the scheme consists of the following five algorithms, namely System Initialization, Key Generation, Smart Meter Data Reporting, Data Aggregation and Data Recovery as explained below.

- (a) **System Initialization:** OC runs a system initialization algorithm with  $1^k$  as a security parameter and outputs a cyclic group  $G$  of prime order  $q$ , with  $P \in G$  as its generator, an elliptic curve  $E : y^2 = x^3 + ax + b \text{ mod } p$ , where  $a, b \in F_p$ , for  $F_p$  a prime field of order  $p$ . The OC then chooses  $P$  from the elliptic curve  $E$ , by using  $P$  generates a group  $G$  of order  $q$ . Later OC chooses  $x_\alpha \in Z_q^*$  as its master secret key (private key) and  $X_\alpha = x_\alpha P$  as its public key. OC selects secure hash functions:  $H_1 : \{0, 1\}^* \rightarrow Z_q^*$ ,  $H_2 : \{0, 1\}^* \rightarrow Z_q^*$ . After initialization the following public parameters for system management are published,  $params = \{P, p, q, E, F_p, G, X_\alpha, H_1, H_2\}$  as depicted in Figure 4.2.

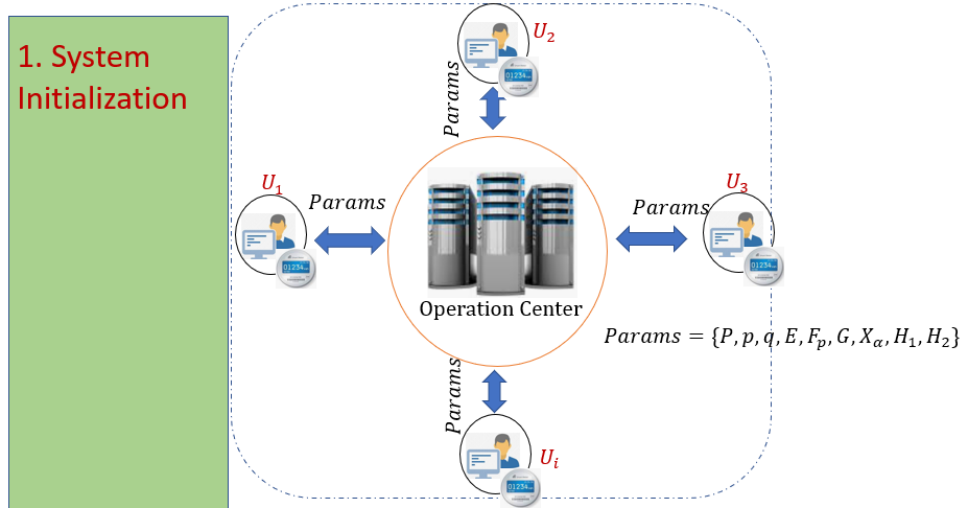


Figure 4.2: System initialization phase

- (b) **Key Generation:** After system parameter initialization each smart meter is issued with a private key  $x_s$  whose corresponding public key is,  $X_s = x_s P$ . Similarly the neighborhood or residential area gateway, DAP is securely issued with



### 4.3. Proposed Scheme

a pair of public and private key as,  $X_d$  and  $x_d$  respectively, where  $X_d = x_dP$  and  $x_d \in Z_q^*$ . The process of smart meter private and public key generation is illustrated in Figure 4.3.

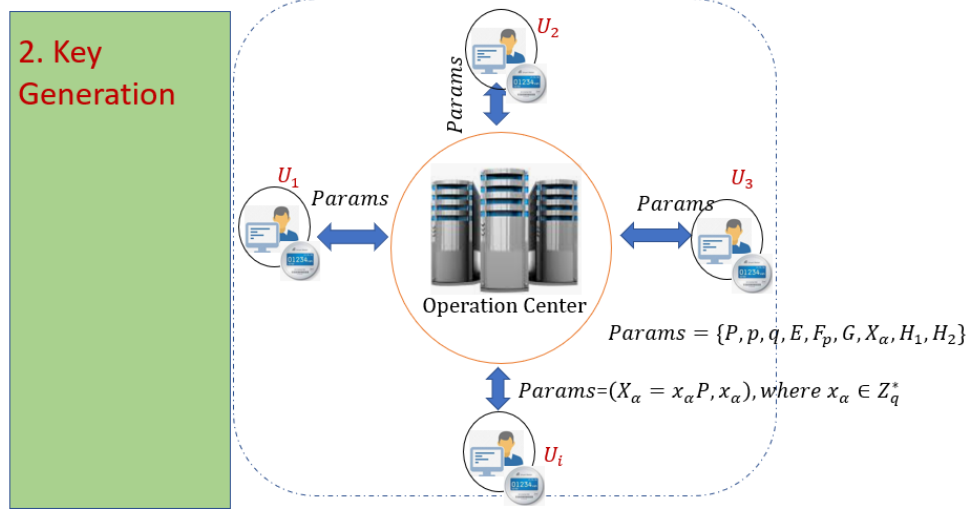


Figure 4.3: Private and public key generation phase

(c) **Smart Meter Data Reporting:** The smart meter uses the public keys of the DAP and OC to send a cipher-text for smart metering data report for a particular period of time. For management purposes, the electricity reports from SMs to OC are transmitted in 10 - 15 minutes intervals. Let  $e_i$  represents an individual user's electricity consumption report in the specified time interval for  $i = 1, 2, \dots, n$ . The SM deployed at household is in charge of all home appliances, and it collects the usage data, and then encrypts it before transmission to the DAP. Before SM sends the data,  $e_i$  to the receiver, it is necessary to map the message  $e_i$  to a point on the elliptic curve using a homomorphic mapping as  $m_i = e_i G$ . Then later, the SM carries out data encryption procedure by using the public keys of DAP and OC which are,  $x_d, X_\alpha$  respectively as follows and this is depicted in Figure 4.4:

- Step 1: Each smart meter generates random numbers,  $r_d, r_\alpha \in Z_q^*$ , and then computes  $C_1 = r_d P$ ,  $C_2 = r_\alpha P$ ,  $C_3 = r_\alpha X_\alpha \oplus ID_s$  then encrypts the data as,  $C_i = m_i + ID_s + r_\alpha X_\alpha + r_d X_d$ . Furthermore, the SM computes the authentication and integrity check component  $\sigma_1 = H_1(C_i || C_1 || X_s || t_s) x_s$ , by using its own private key as a signature and public with its timestamp  $t_s$
- Step 2: Then the smart meter sends  $M_1 = \{C_1, C_2, C_3, C_i, X_s, t_s, \sigma_1\}$  to the DAP of its residential area network. Thus  $C_i$  is the actual cipher-text of the reporting data.

Furthermore, its worth to take note that,  $C_1, C_2$  and  $C_3$  can be pre-computed to expedite the smart meter data reporting process.

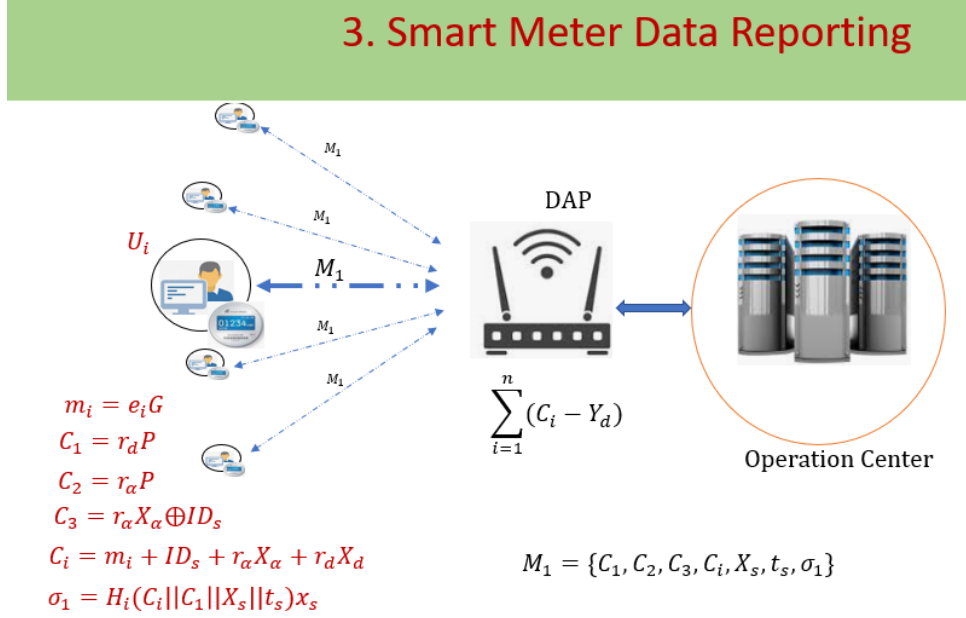


Figure 4.4: Smart meter electricity reporting process

(d) **DAP Data Aggregation:** Upon receipt of the message  $M_1$  from SM, the gateway (DAP) has to perform aggregation on the encrypted data and partially decrypt the message to leverage the OC of some computational overhead by using its private key. DAP proceeds as follows:

- step 1: Selects the timestamps  $t_d$ , and checks the validity by computing  $|t_d - t_s| < \delta$  otherwise it aborts the session, where  $\delta$  is the acceptable threshold of time lapse.
- step 2: Checks both the source and message authenticity and validity of the received message by verifying that  $\sigma_1.P = H_1(C_i || C_1 || X_s || t_s) X_s$  and it proceeds only if the computation holds
- Step 3: First computes,  $Y_d = x_d C_1$  and then DAP carries out data aggregation by partial decryption of the message from SM to OC as follows:

$$\begin{aligned}
 C_T^{agg} &= \sum_{i=1}^n (C_i - Y_d) \\
 &= \sum_{i=1}^n (m_i + ID_s + r_\alpha X_\alpha)
 \end{aligned} \tag{4.5}$$

which is the result of additive homomorphic operation on an encrypted data

- step 4: Then DAP computes a signature of the partially decrypted ciphertext, including both its private key and public key in the computation ,  $\sigma_2 = H_2(C_T^{agg} || C_2 || C_3 || X_d || t_d) x_d$ .

### 4.3. Proposed Scheme

- step 5: Now DAP forwards the partially decrypted message  $M_2 = \{C_2, C_3, C_T^{agg}, X_d, t_d, \sigma_2\}$  to the OC.

(e) **Data Recovery:** Upon receipt of the partially decrypted message  $M_2$  from DAP, the OC carries the following steps in the process of decrypting.

- step 1: Selects the timestamp  $t_\alpha$ , and checks if  $|t_\alpha - t_d| < \delta$  holds and then proceeds, otherwise it quits the process.
- step 2: Furthermore the OC checks the integrity of the partially decrypted ciphertext from the DAP by verifying,  $\sigma_2.P = H_2(C_T^{agg}||C_2||C_3||X_d||t_d)X_d$ .
- step 3: Afterwards, OC carries out user identification extraction by computing:

$$ID_s = C_3 \oplus C_2.x_\alpha$$

- step 4: Finally, the OC is able to securely extract the total electricity consumption reporting data for each user by carrying out the computation:

$$\begin{aligned} Cons_{Total} &= C_T^{agg} - \sum_{i=1}^n (ID_s + x_\alpha C_2) \quad (4.6) \\ &= \sum_{i=1}^n m_i + \sum_{i=1}^n ID_s + r_\alpha X_\alpha - \sum_{i=1}^n (ID_s + x_\alpha C_2) \\ &= \sum_{i=1}^n (m_i + ID_s + r_\alpha X_\alpha) - \sum_{i=1}^n (ID_s + x_\alpha r_\alpha P) \\ &= \sum_{i=1}^n m_i \end{aligned}$$

It should be noticed that, if any checking in the scheme's steps fails to hold then the scheme is immediately aborted.

Now we can look at the correctness of the main computations of DAP and OC to verify the consistence of the messages.

**DAP Computation correctness:**

$$\begin{aligned} Y_d &= x_d C_1 \quad (4.7) \\ &= x_d r_d P \\ &= r_d x_d P \\ &= r_d X_d \end{aligned}$$

The DAP computes partial decryption:

$$\begin{aligned}
 C_T^{agg} &= \sum_{i=1}^n (C_i - Y_d) & (4.8) \\
 &= \sum_{i=1}^n (m_i + ID_s + r_\alpha X_\alpha + r_d X_d + k_i - x_d C_1) \\
 &= \sum_{i=1}^n (m_i + ID_s + r_\alpha X_\alpha + r_d X_d + k_i - x_d r_d P) \\
 &= \sum_{i=1}^n (m_i + ID_s + r_\alpha X_\alpha + r_d X_d + k_i - r_d x_d P) \\
 &= \sum_{i=1}^n (m_i + ID_s + r_\alpha X_\alpha + k_i) \\
 &= \sum_{i=1}^n (m_i + ID_s + r_\alpha X_\alpha) + \sum_{i=1}^n k_i \\
 &= \sum_{i=1}^n (m_i + ID_s + r_\alpha X_\alpha)
 \end{aligned}$$

**OC Computation correctness:**

Extraction of  $ID_s$ :

$$\begin{aligned}
 ID_s &= C_3 \oplus C_2 x_\alpha & (4.9) \\
 &= (r_\alpha X_\alpha \oplus ID_s) \oplus (r_\alpha P) x_\alpha \\
 &= (r_\alpha X_\alpha \oplus ID_s) \oplus (r_\alpha X_\alpha) \\
 &= r_\alpha X_\alpha \oplus ID_s \oplus r_\alpha X_\alpha \\
 &= ID_s \oplus r_\alpha X_\alpha \oplus r_\alpha X_\alpha
 \end{aligned}$$

#### 4.4. Security Analysis and performance Evaluation

Electricity data extraction:

$$\begin{aligned}
Cons_{Total} &= C_T^{agg} - \sum_{i=1}^n (ID_s + x_\alpha C_2) \tag{4.10} \\
&= \sum_{i=1}^n (m_i + ID_s + r_\alpha X_\alpha) - \sum_{i=1}^n (ID_s + x_\alpha C_2) \\
&= \sum_{i=1}^n (m_i + ID_s + r_\alpha X_\alpha) - \sum_{i=1}^n (ID_s + x_\alpha r_\alpha P) \\
&= \sum_{i=1}^n m_i + \sum_{i=1}^n (ID_s + r_\alpha X_\alpha) - \sum_{i=1}^n (ID_s + X_\alpha r_\alpha) \\
&= \sum_{i=1}^n m_i + \sum_{i=1}^n (ID_s + r_\alpha X_\alpha) - \sum_{i=1}^n (ID_s + X_\alpha r_\alpha) \\
&= \sum_{i=1}^n m_i + n(ID_s + r_\alpha X_\alpha) - n(ID_s + X_\alpha r_\alpha) \\
&= \sum_{i=1}^n m_i
\end{aligned}$$

The actual total consumption data  $\sum_{i=1}^n e_i$  is extracted from  $\sum_{i=1}^n m_i G$  by applying the Pollard lambda operation since  $e_i = m_i G$ .

Thus, this shows that the computations are consistently correct as the entities in the scheme carry out them.

## 4.4 Security Analysis and performance Evaluation

We will first give formal security and privacy proofs by random oracle model of the proposed electricity power consumption aggregation scheme and then conduct a performance evaluation in terms of computational overhead and communication overhead to demonstrate the feasibility of the proposed scheme's merits.

### 4.4.1 Security Requirements Analysis

Here we will analyze the satisfaction of security requirements of the proposed scheme and also compare it with other related works.

1. **Authentication:** The messages plying between SM and DAP as well as the ones between DAP and OC are intrinsically authenticated by either party to assure the communication is with the rightful or intended entity. The message,  $\{C_1, C_2, C_3, C_i, X_s, t_s, \sigma_1\}$ , is authenticated by DAP by checking that  $\sigma_1.P = H_1(C_i || C_1 || X_s || t_s)X_s$  in the message  $M_1$  against the timestamp  $t_s$ . This checking

additionally affirms the sender as legitimate since it works as a digital signature as  $\sigma_1$  is generated by SM's private key and verified with its public key. Similarly, the receiver is authenticated before carrying out partial decryption by ensuring that it is able to calculate  $Y_d = x_d C_1$ , which is used in the partial decryption. The message is designed such that only the intended DAP, is the one able to compute  $Y_d = x_d C_1$ , since the computation requires a private key of DAP. Hence this entails the partially decrypted data  $C_T^{agg}$  sent to OC is an authenticated one. In turn upon extraction of user  $ID_s$ ,  $C_T^{agg}$  is further used to calculate the total consumption report, which ensures authentication of the smart meter user,  $ID_s$ , to OC. Consequently the message itself and the source authentication is satisfied.

2. **Data Confidentiality:** In order to obtain the electricity consumption reporting data the OC must compute  $Cons_{Total} = C_T^{agg} - \sum_{i=1}^n ID_s(x_\alpha C_2)$  of which is infeasible to be calculated by any malicious party without the specific knowledge of the private key  $x_\alpha$  and the hidden identity  $ID_s$ . An attacker will have to solve an intractable problem of ECCDH to obtain  $x_\alpha$  from the public key  $X_\alpha = x_\alpha P$  as well as extracting  $ID_s$  from  $C_3 = r_\alpha X_\alpha \oplus ID_s$ , which is impossible. Therefore, the proposed scheme does meet the data confidentiality requirement.
3. **Data Integrity:** In the proposed scheme the ciphertext integrity is ensured by inclusion of verifiable signatures and freshness checking values. In the ciphertext  $M_1$ ,  $\sigma_1$  is used to check the integrity of the sent message to DAP by verifying whether  $\sigma_1.P = H_1(C_i || C_1 || X_s || t_s) X_s$  holds. This subsequently checks the integrity of the sent message as well as the source. Likewise  $\sigma_2$  upholds the integrity of the ciphertext  $M_2$  from DAP to OC and if the verification of  $\sigma_2.P = H_2(C_T^{agg} || C_2 || C_3 || X_d || t_d) X_d$  fails the session will be aborted. Since no attacker can generate a valid  $\sigma_1$  associated with the ciphertext  $C_i$  as it is infeasible to calculate the components  $r_d, r_\alpha, ID_s$  and  $m_i$  from the publicly accessible message  $M_1$ . Similarly,  $\sigma_2$  cannot be forged to fake the authenticity of the message  $M_2$ , as it is impossible for an attacker to fabricate  $C_T^{agg}$  without knowledge of DAP's private key  $x_d$ . Thus, the proposed scheme provides message integrity.
4. **Consumer Privacy and Anonymity:** In the proposed scheme an attacker has no access to any consumer related information from the plying messages from SM to OC. The user related information in  $C_3 = r_\alpha X_\alpha \oplus ID_s$  and  $C_i = m_i + ID_s + r_\alpha X_\alpha + r_d X_d$  from SM to DAP is transmitted in concealed form and cannot be obtained by an attacker before solving an intractable ECCDH problem to obtain the  $ID_s$  from  $C_3 = r_\alpha X_\alpha \oplus ID_s$ . This is well known hard problem for an attacker to resolve, hence the proposed scheme LPPDA provides consumer privacy and anonymity befitting the wireless communication between SM and DAP, where eavesdropping can easily be done in the public channel.
5. **Attack Resilience:** The proposed LPPDA scheme has the merits to resist against well known attacks such as: replay attack, impersonation attack and man-in-the-middle attack.

#### 4.4. Security Analysis and performance Evaluation

- *Replay attack*: User electricity data report from SM to OC for a particular time slot  $i = 1, 2, \dots, n$  is hashed in  $\sigma_1 = H_1(C_i || C_1 || X_s || t_s)x_s$  which comprises of fresh random numbers  $r_d$  and  $r_\alpha$  for each session run. Similarly, OC verifies the freshness of  $M_2$  by checking that  $\sigma_2 = H_2(C_T^{agg} || C_2 || C_3 || X_s || t_d)x_d$  holds. Thus, the timestamp  $t_s$  and  $t_d$  checks against any replay attempts by an attacker on the messages  $M_1$  and  $M_2$  respectively. Therefore by this procedure, LPPDA could resist replay attack.
- *Impersonation attack*: No attacker can produce the ciphertext  $C_i = m_i + ID_s + r_\alpha X_\alpha + r_d X_d$  associated with the identity  $ID_s$  without knowledge of either random number  $r_d$  or the private key,  $x_d$ . Thus, an attacker has no idea of the user who is to be impersonated on. By this, LPPDA is able to resist any impersonation attack.
- *Man-in-the-middle attack*: From the ciphertext  $M_2$  obtained by OC originating from SM, only the OC could extract the identity  $ID_s$  that authenticates SM to OC in the process  $ID_s = C_3 \oplus C_2 \cdot x_\alpha$ . Furthermore, the integrity check components,  $\sigma_1 = H_1(C_i || C_1 || X_s || t_s)x_s$  and  $\sigma_2 = H_2(C_T^{agg} || C_2 || C_3 || X_s || t_d)x_d$  are generated with sender's private key to be verified by its corresponding public key, meaning that no attacker can formulate a verifiable ciphertext impersonating  $ID_s$  to DAP and OC, because of lack of private keys of the victims. Therefore an attacker in between SM and DAP cannot generate valid  $C_i$  and  $\sigma_1$  that can be verified. Similarly the messages from DAP to OC are secure from an attacker in between as  $C_T^{agg}$  cannot be forged for a targeted identity  $ID_s$  as it is verified by  $\sigma_2$ .

Furthermore, the merits of the proposed LPPDA scheme are compared against other related schemes [181], [154], [81], [134], [162] with respect to security features satisfied, as shown in the Table 4.2. In the table the  $\checkmark$  symbol shows that a particular security feature is satisfied while the  $\times$  symbol shows that the security feature is not satisfied. For easy representation in the table the following features: confidentiality, authentication, integrity, anonymity, replay attack, impersonation attack, internal attack and man-in-the-middle attack are denoted as, F1, F2, F3, F4, F5, F6, F7, F8 respectively. So clearly, it is evident from the Table 4.2, that LPPDA scheme has merits on satisfaction of security requirements over related works.

#### 4.4.2 Performance Evaluation

In this section, performance analysis is carried out in comparison with relevant related schemes Lu et al.[181], Lu et al.[154], [81], Vahedi et al. [134] and Tahir et al.[162] based on computational cost required for SM, DAP and OC as well as the communication cost analysis of the channels SM to DAP and DAP to OC respectively are presented.

Security Features Comparison								
Scheme	F1	F2	F3	F4	F5	F6	F7	F8
[181]	✓	✗	✗	✗	✓	✓	✗	✗
[154]	✓	✓	✓	✗	✓	✓	✗	✓
[81]	✓	✓	✓	✗	✓	✓	✓	✓
[134]	✓	✓	✓	✗	✓	✓	✓	✓
[162]	✓	✓	✓	✗	✓	✓	✗	✗
LPPDA	✓	✓	✓	✓	✓	✓	✓	✓

Table 4.2: Security Comparison

### 4.4.3 Computation Cost

The computational times variables used in LPPDA, for carrying out specific cryptographic operations are adapted from [81] which were simulated on MIRACL Crypto SDK, which is a multi-precision integer, rational arithmetic C/C++ library, [182] run on a 2.53GHz i5 CPU, 4 GB RAM on a 64 bit windows 10 operating system. The experimentation used a 160 bit key length for security parameters chosen from  $G$  over  $F_p$ . The data of the average quantified running times is depicted in given Table 4.3, which was obtained after taking the averages of 1000 runs in the simulation.

In this regard the computation cost comparison will be done based on the quantification weights in Table 4.3, averaged after 1000 experiment runs in order to estimate time complexities for different operations. In this evaluation, lightweight operations like hash functions, hash chain, concatenation, point addition and XORing are disregarded, since they have negligible computation overload. So, our focus will be on heavier computation operations only such as: map-to-point hash function, bilinear parings, paillier public key encryption and paillier public key decryption operations among others as portrayed in the Table 4.4.3.



#### 4.4. Security Analysis and performance Evaluation

Notations	Description of operation	Execution time
$T_{sm-ecc}$	Scalar multiplication in ECC	0.38
$T_{DL}$	Solving DL operation in mod $p$	0.64
$T_{mtp}$	Map to a point hash function	3.58
$T_{n^2}$	Exponentiation in $Z_{n^2}$	2.02
$T_p$	Bilinear pairing	10.31
$T_{p-D}$	Paillier public key decryption	11.82
$T_{p-E}$	Paillier public key encryption	9.89
$T_{exp-p}$	Exponentiation in $p$	0.13
$T_m$	Scalar multiplication in bilinear pairing	1.42
$T_n$	Exponentiation in $Z_n$	0.58

Table 4.3: Estimated Running Times for Different Operations in milliseconds ( $ms$ ) Averaged after 1000 runs

*Chapter 4. Lightweight Privacy-Preserving Data Aggregation Scheme Based on  
Elliptic Curve Cryptography for Smart Grid Communications*

Scheme	SM	DAP	OC	Total time
[181]	$1T_m + (n+1)T_{n^2} + 1T_{mtp}$ $= 2.02n + 7.02ms$	$(w+1)T_p + 1T_m + (w+1)T_{mtp}$ $= 13.89w + 15.70ms$	$2T_p + 1T_{mtp}$ $= 36.04ms$	$13.89w + 2.02n + 56.74ms$
[154]	$3T_{exp-p} + 3T_m$ $= 4.65ms$	$(3w+1)T_{exp-p} + 3T_m$ $= 0.39w + 4.39ms$	$4T_{exp-p} + 3T_m$ $= 4.78ms$	$0.39w + 13.82ms$
[81]	$6T_{sm-ecc}$ $= 2.28ms$	$(2w+2)T_{sm-ecc}$ $= 0.76w + 0.76ms$	$4T_{sm-ecc} + 1T_{DL}$ $= 2.16ms$	$0.76w + 5.2ms$
[134]	$5T_{sm-ecc}$ $= 1.9ms$	$2T_p + (w+1)T_{sm-ecc}$ $= 0.38w + 21ms$	$1T_p + (2z+1)T_{sm-ecc} + 1T_{mtp}$ $= 4.78z + 14.26ms$	$= 0.38w + 4.78z + 37.16ms$
[162]	$3T_{exp-p} + 3T_m$ $= 4.65ms$	$(3w+1)T_{exp-p} + 3T_m$ $= 0.39w + 4.39ms$	$4T_{exp-p} + 3T_m$ $= 4.78ms$	$0.39w + 13.82ms$
LPPDA	$6T_{sm-ecc}$ $= 2.28ms$	$wT_{sm-ecc}$ $= (1.14w)ms$	$(z+3)T_{sm-ecc}$ $= (0.76z)ms$	$= 0.76w + 0.38z + 3.68ms$

#### 4.4. Security Analysis and performance Evaluation

The computational cost is categorized in three levels according to the entity carrying out the operation which are the smart meters, data aggregation points and the operations center for the sake of clarity and fairness in the evaluation. Thus, we will evaluate the computational cost of the SM, DAP and OC individually before calculating the total computation incurred in the schemes [181], [154], [81], [134], [162] and the summary of the comparison is done in Table 4.4.3.

Firstly, we calculate computational cost required for a SM in different schemes. The computational cost required for SM in [181] is  $(n + 1)$  exponentiation operations in  $Z_{n^2}$ , one map-to-point hash operation and one scalar multiplication in bilinear pairing. So the amount of the computation cost for a SM is  $(n + 1)T_{n^2} + 1T_m + 1T_{mtp} = 2.02 + 7n.02ms$ . In schemes [154] and [162], there are three exponentiation operations in  $G_1$  and three scalar multiplication in bilinear pairing. So the amount of computation needed for SM is  $3T_{exp-p} + 3T_m = 4.65ms$ . While in [81], SM needs six scalar multiplication which amounts to  $6T_{sm-ec} = 2.28ms$  and in [134] five scalar multiplication operations are needed with an overhead of  $5T_{sm-ec} = 1.9ms$ . On the other hand in LPPDA, SM requires six scalar multiplication with the computational cost of  $6T_{sm-ec} = 2.28ms$ . However, although [134] has the same SM computational cost as in the proposed scheme, in LPPDA scheme the computation of which,  $C_1$ ,  $C_2$  and  $C_3$  can be pre-computed prior to the data reporting time and this further reduces the computational requirement. Thus, our design would require  $3T_{sm-ec} = 1.14ms$  for real-time computations, therefore it does not overload the SM computation overhead during the run time, besides it ensures provision of user anonymity, unlike in the other schemes.

Secondly, the computation cost for DAP in these schemes is such that in [181] there are  $w + 1$  bilinear pairing operations where  $w$  is the numbers of smart meters in a particular neighborhood, one scalar multiplication in bilinear pairing and  $w + 1$  map-to-point hash operations. Consequently, the DAP requires  $(w + 1)T_p + 1T_m + (w + 1)T_{mtp} = 13.89w + 15.7ms$  computation cost. Whereas in [154] and [162], the schemes need  $3w + 1$  exponentiation operations in  $G_1$  and three scalar multiplication operations in bilinear pairing and DAP's computation cost is  $(3w + 1)T_{exp-p} + 3T_m = 0.39w + 4.39ms$ . In scheme [81], the DAP requires  $(2w + 2)$  scalar multiplication operations with a computation cost overhead of  $(2w + 2)T_{sm-ec} = 0.76w + 0.76ms$ . Whereas in [134], two bilinear pairing operations and  $(w + 1)$  scalar multiplication are needed so the computation cost overhead for DAP is  $2T_p + (w + 1)T_{sm-ec} = 0.38w + 21ms$ . On the other hand the DAP in the proposed LPPDA, requires  $3w$  scalar multiplication operations and one exponentiation operation, thus the computation cost for DAP is  $3wT_{sm-ec} = (1.14w)ms$ .

Thirdly, we analyze the computation cost required for OC in each scheme and we assume that there are  $z$ , DAPs in the wide area network where OC is in-charge. In Lu et' al [181] scheme, OC requires to two bilinear pairing operations, one paillier public key decryption operation and one map-to-point hash operation. The computation cost required in this case is  $2T_p + 1T_{p-D} + 1T_{mtp} = 36.04$ . Whereas in [154] and [162], the OC

#### 4.4. Security Analysis and performance Evaluation

requires four exponentiation operations in  $G_1$ , three scalar multiplication operations in bilinear pairings, so the computation cost overhead is  $4T_{exp-p} + 3T_m = 4.78ms$ . In Ming et al [81], on the other hand, OC requires four scalar multiplication operations and DL operation *mod*  $p$ , with the computational cost of  $4T_{sm-ecc} + 1T_{DL} = 2.16ms$ . In [134], the OC needs one bilinear pairing operation,  $(2z + 1)$  scalar multiplication operation and one map-to-point hash operation, resulting into the computation cost of  $1T_p + (2z + 1)T_{sm-ecc} + 1T_{mtp} = 4.78z + 14.26ms$ . While in the proposed LPPDA, the OC requires  $2zT_{sm-ecc}$  scalar multiplication operations yielding to computation cost of  $2zT_{sm-ecc} = 0.76zms$ .

Thus, with reference to the computation loads of each entity reflected in Table 4.4.3, where  $w$  stands for the number of smart meters reporting to DAP and  $z$  stands for number of DAPs reporting to OC. The proposed LPPDA scheme has overall lower computation cost as depicted in **Figure 4.5**, with both  $w$  and  $z$  equated to one for simplicity, even though [81] and [134] have a slightest edge for lower SM overhead. The computation results considers the incurred overhead per individual entity, that is SM, DAP and OC separately. The actual run time computation cost for SM is much lower to the tune of  $1.14ms$  upon excluding pre-computed operations unlike the  $2.28ms$  shown in the **Figure 4.5**, of which is still lower than comparable schemes hence affirming the efficiency of the proposed LPPDA scheme.

#### 4.4.4 Communication Cost

Now we will evaluate the communication cost of the proposed LPPDA scheme in relation to the schemes [181], [154], [81], [134], [162], however ECC based schemes are generally more efficient and saves more bandwidth since with reduced short length security parameter with high security achievement. Different mathematical structures have different lengths for the security parameters. The elements in  $G_1$ ,  $G_T$ ,  $G$ ,  $Z_q^*$ ,  $Z_n$  and  $Z_{n^2}$  respectively, have the lengths, 512 bits, 1024 bits, 160 bits, 160 bits, 1024 bits and 2048 bits. The length of a hash function is 160 bits whilst that for an identity and timestamp is 32 bits. The communication cost analysis between SM and DAP is given as follows. SM sends the message  $\{C_i, \sigma_i, RA, U_i, TS\}$  to the DAP in [154], such that  $C_i \in Z_{n^2}$ ,  $\sigma_i \in G_1$  whereby  $RA$ ,  $U_i$  and  $TS$  are all 32 bit long each. SM to DAP communication cost is therefore,  $|C_i + \sigma_i + RA + U_i + TS| = 2048 + 512 + 32 + 32 + 32 = 2659$  bits. Whereas in scheme [181], the SM sends the message  $C_i$  of length  $|C_i| = 1024$  bits. While in [81] et 'al, the message  $\{C_{1,i}, C_{2,i}, ID_i, L_i, v_i, T\}$  is sent from SM to DAP with the overall communication load of  $|C_{1,i} + C_{2,i} + ID_i + L_i + v_i + T| = 160 + 160 + 32 + 160 + 160 + 32 = 704$ , where  $C_{1,i}, C_{2,i}, L_i \in G$ ,  $v_i \in Z_q^*$  and further,  $ID_i$  and  $T$  are both 32 bit identity and timestamp respectively. On the other hand, in the scheme [134], SM sends the message  $R_{it} || S_{it} || t || ID_{U_i} || \sigma_{it}$  to corresponding DAP. By considering the same conditions for [134] elements in the group  $G$  has length of 160 bits. Thus, the communication bandwidth required for [134] is,  $|R_{it} + S_{it} + t + ID_{U_i} + \sigma_{it}| = 160 + 160 + 32 + 32 + 160 = 544$  bits. In the scheme [162], SM sends the message  $\{C_i, H_i\}$  to DAP with  $C_i \in G_T$  and  $H_i$  a one way hash function. The computation cost requirement is therefore,

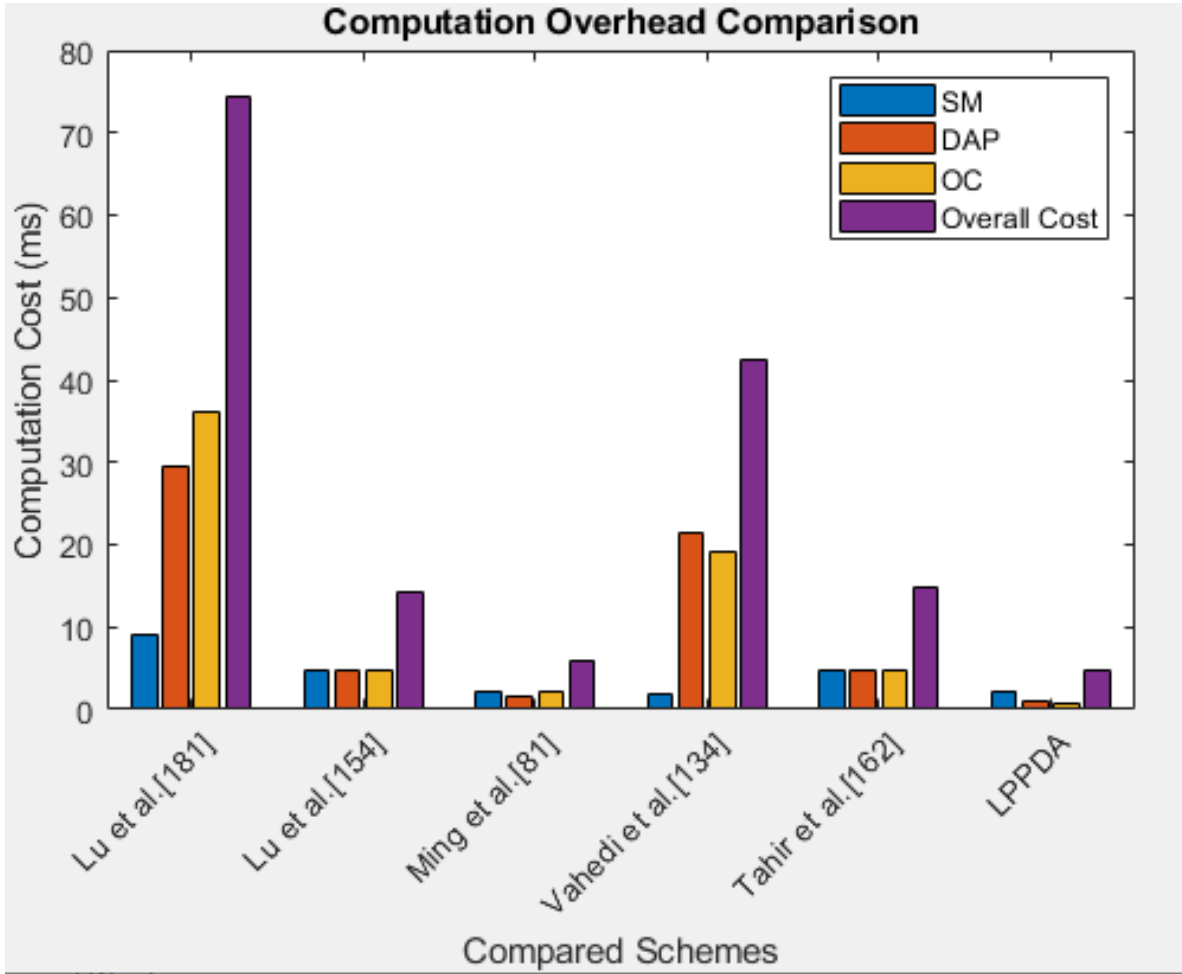


Figure 4.5: Computation Cost for the Schemes.

$|C_i + H_i| = 1024 + 160 = 1184$  bits. On the other hand, in the proposed LPPDA, SM sends the message  $M_1 = \{C_1, C_2, C_3, C_i, X_s, t_s, \sigma_1\}$  to DAP all from the group  $G$ . So the required communication bandwidth is  $|C_1 + C_2 + C_3 + C_i + X_s + t_s + \sigma_1| = 160 + 160 + 160 + 160 + 160 + 32 + 160 = 992$ .

Lastly, the communication cost between DAP and OC in the concerned schemes is analyzed as follows. DAP sends the message  $\{C, \sigma_g, RA, GW, TS\}$  to OC in [181], where  $C \in Z_{n^2}$ .  $\sigma_g \in G_1$ , and further,  $RA$  and  $TS$  are both 32 bits elements. Thus, the communication cost is  $|C + \sigma_g + RA + GW + TS| = 2048 + 512 + 32 + 32 + 32 = 2659$  bits. The DAP in [154] sends  $C$  as the message to OC where  $C \in G_T$ , so the communication cost is  $|C| = 1024$  bits. On the other hand, DAP sends the message  $\{C_1, C_2, ID_{GW}, L_{GW}, v_{GW}, T\}$  to OC in [81], with  $C_1, C_2, L_{GW} \in G$ ,  $v_{GW} \in Z_q^*$  and further,  $ID_{GW}$  and  $T$  are both 32 bits long elements. Hence the communication cost amounts to  $|C_1 + C_2 + ID_{GW} + L_{GW} + v_{GW} + T| = 160 + 160 + 32 + 160 + 160 + 32 =$

#### 4.4. Security Analysis and performance Evaluation

704 bits. In [134], the DAP sends the message  $R_t||S_t||t||ID_{AG_j}||\sigma_{AG_j,t}$  to OC, so the communication cost is  $|R_t + S_t + t + ID_{AG_j} + \sigma_{AG_j,t}| = 160 + 160 + 32 + 32 + 1024 = 1408$  bits. While in Tahir et al [162], DAP sends the message,  $\{C, H\}$  to OC with  $C \in G_T$  and  $H$  as a 160 bits one-way hash function, therefore yielding the communication cost of  $|1024 + 160| = 1184$  bits. On the other hand, in the proposed LPPDA the DAP sends the message  $M_2 = \{C_2, C_3, C_T^{agg}, X_d, \sigma_2, t_d\}$  to the OC which has the communication cost of  $|C_2 + C_3 + C_T^{agg} + \sigma_2 + X_d + t_d| = 160 + 160 + 160 + 160 + 160 + 32 = 832$  bits.

Scheme	SM-DAP	DAP-SM
[181]	1024	2659
[154]	2659	1024
[81]	704	704
[134]	544	1408
[162]	1184	1184
LPPDA	992	832

Table 4.4: Communication Cost of SM-DAP and DAP-OC Transmissions

Based on the comparison values of the concerned schemes summarized in Table 4.4, we obtain the graphical representation in Figure 4.6 to show the performance of the proposed scheme.

Thus, from the analysis, the proposed LPPDA has an overall efficient communication cost to the related works as seen in Figure 4.6 relative to the scheme in [81] in terms of SM-DAP communication segment cost while our scheme, LPPDA, has better merits overall the comparable schemes. In regards to the DAP-OC communication segment, our scheme has an efficient bandwidth load of 832 bits which providing desirable security requirements. Therefore, from the performance evaluation, in general our scheme is lightweight in both computation cost and communication cost, making it an ideal security scheme in a complex communication based network environment as that of smart grid.

*Remark:* By considering pre-computed operations, the overall communication and computation performance efficiency of LPPDA scheme surpasses that of relevant related works with a significant margin. The performance of the proposed work is achieved with a great advantage comparatively, as much as twice to the better performing scheme, while achieving user anonymity without sacrificing computation efficiency.

This work is on going and we will progressively devote on including other versatile

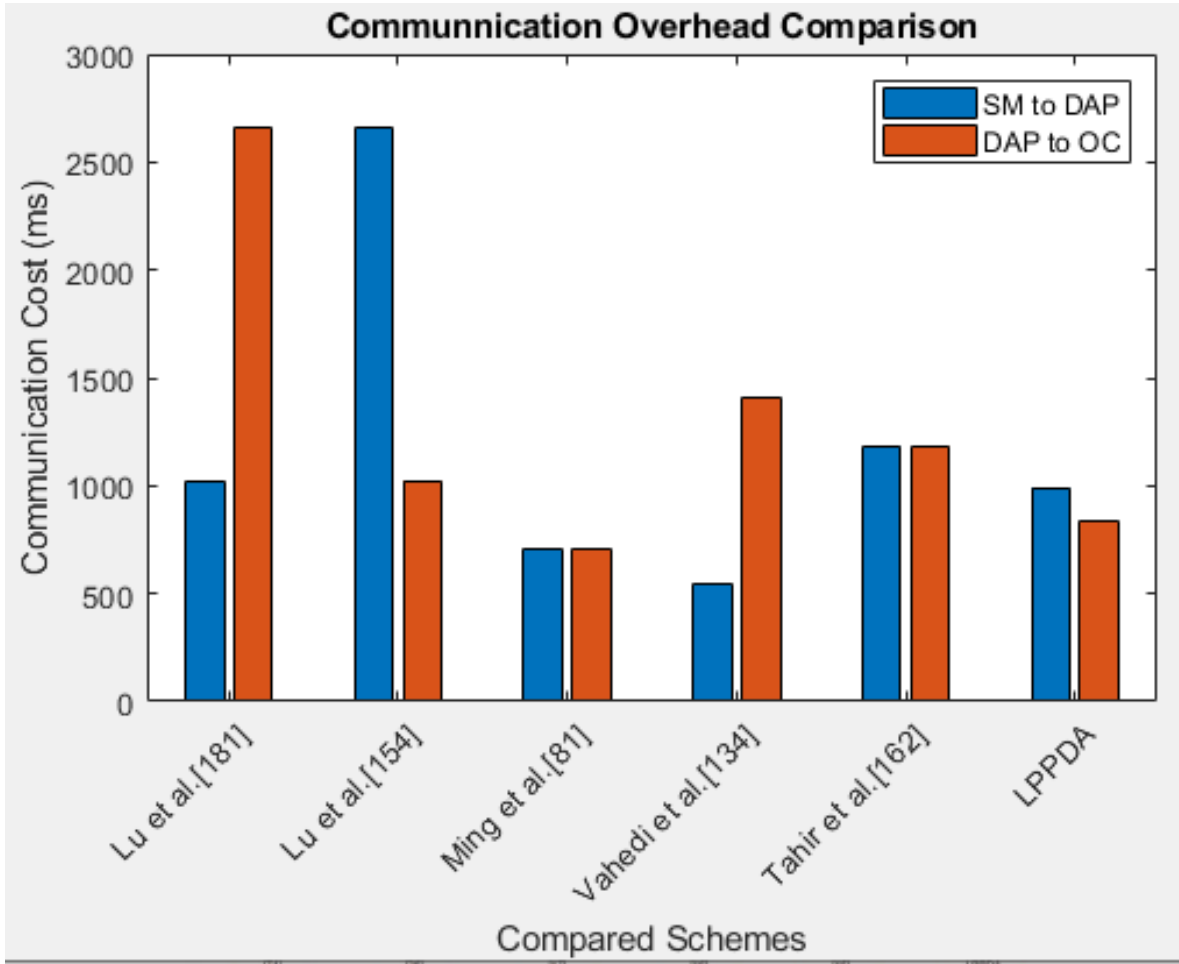


Figure 4.6: Communication Cost for the Schemes.

security techniques that ensure a robust modern grid with its applications and functionalities. In our further works, multi-dimension data aggregation techniques will be considered, to ensure security, classification and uploading of different types of electrical appliance measurements data to the utility company. We consider incorporating a privacy-preserving data aggregation focusing on a block-chain smart grid network environment and its functionality requirements. We also would endeavor to employ smart grid security schemes adaptive to dynamic machine learning based techniques in optimal scheduling and billing.

## 4.5 Summary

In this chapter, we proposed a lightweight privacy-preserving data aggregation scheme based on elliptic cryptography, for smart grid communications. The framework is a two leveled architecture with the residential area data aggregator acting as an intermediate



#### 4.5. *Summary*

party between the smart meter and the utility service company. Unlike many other researches the proposed scheme protects user's real-time power consumption and identity from privacy and security breaches in an efficient manner by using a ECCDH problem in the encryption algorithm and additive homomorphic encryption. The comparison analysis shows that the scheme is efficient on overall system performance as well as robust in security, hence ideal for an IoT enhanced smart grid system. Our future work, related to this discipline will focus on secure and efficient multidimensional data preservation in smart grid network environment. Aspects of versatile technologies such as; block-chain, lattice cryptography and machine learning techniques will be considered, in order to realize a modern smart grid.

*Chapter 4. Lightweight Privacy-Preserving Data Aggregation Scheme Based on  
Elliptic Curve Cryptography for Smart Grid Communications*

# Chapter 5

## Contribution to Knowledge, Conclusion and Future Works

### 5.1 Contribution to the Current State of Knowledge

The portrayed work has various novelties in various ways and forms to the research world. Spanning through all this work, note worthy is the aspect of reducing the powers of the system's operations center in deducing the private key of users within its domain and thereby capabilities of masquerading the legal user or eavesdropping the secret messages encrypted by the user's private key. This research argues why it is important to remove escrow power of the operations center and then provides the solution in distributed smart grid environment. Evidently, the property of anonymous authenticate is upheld in all the security design to achieve privacy-preservation in VANETs, AMI data aggregation and key agreement. Throughout the whole work the user's real identity is concealed from eavesdroppers over the public channel. Specific to VANETs the proposed scheme provides conditional privacy preservation where the system authority can trace entities acting contrary to terms and conditions of safe communications. Additionally, the security designs in this work are based elliptic curve cryptography which is one of the most efficient mathematical structures used in security. These measures were applied over a hierarchical architecture which is deemed fast and therefore it factor in another degree of communication efficiency to the system. The proposed work greatly saves on bandwidth, since minimum possible handshakes was employed in all the scheme designs. For instance for key agreement design, the work uses a single message transmission for either party involved. On the contrary, many works in literature require at least two message transmissions by an entity to be able to achieve authenticated key agreement . Whereas for signature schemes the work similarly uses single message transmission but it is able to achieve batch verification at the cluster or domain data collection point.

## 5.2 Conclusion

This work emerged to resolve the long standing security challenge on trading-off the balance between provision of robust security and acceptable computational demand for ubiquitous computing grid system. The baffling phenomenon seen in most works is that efforts to attain profound security faltered by the drawback of involving impractically heavy computation overload. Whereas on the other hand, most works with lightweight computation requirement are found to be feeble against serious attacks as they are secure to selected common attacks. Thus, this PhD research work focuses on analyzing security concerns for the three principal smart grid's communication architectures: the V2G connection in a VANETs network system, customer and utility key exchange mechanism and then AMI communication for electricity reporting data aggregation. Worth to mention is that all these scheme are built of ECC and constructed to provide anonymity, certificate-less construction which ensures maximum security, optimum efficiency surpassing most researches as evidenced by comparison analysis. The designs were constructed in an ideal way for smart grid applications and advanced technologies by virtue of meeting the security needs of the SG architecture, in that:

- The schemes are all lightweight guaranteeing incorporation of resource constrained technologies laden with limited capability devices. This feat is achieved by the consistent effort to achieve optimum computation and communication overhead.
- Wholesomely, the schemes are designed to preclude escrow weakness loophole and excess key management overhead, as they are all certificate-less based.
- The schemes also guarantee privacy-preservation by ensuring anonymous communication and conceal the actual identity over the public channel.

Since smart grid is based on real-time operation the proposed schemes address this challenge by reducing the latency factor as result of heavy computation and communication overload to the network. Consequently, the grid improves its reliability which is significant for whole adoption of the technology. In all the cases security analysis was given in both formal and informal approaches. The formal analysis were done using the mathematical models such as random oracle model (ROM) and the extended Canetti-Krawczyk (eCK).

## 5.3 Future Works

The study that led to the production of this work, has inspired possible research avenues to substantiate some discussion point presented. Thus the work has incited the idea of incorporating block-chain system to enhance robust security and privacy-preservation by taking advantage of the immutability property of block-chain technology. So we envision the proposed designs to be tailored towards satisfying security needs of a block-chain network and applications. In the same vein, one possible area of exploitation

### 5.3. Future Works

for future work is to devise post-quantum computing cryptographic security algorithm which has gained research interest since 2006, in anticipation to fresh attacks of the future. Since research shows that the current security algorithms based on mathematical hard problems such as: discrete logarithm problem, integer factorization problem, or elliptic-curve discrete logarithm problem can easily be broken by a powerful quantum computer running a Shor's algorithm [183, 184]. Although, at the moment most powerful algorithms are able to stand quantum computing experiments to break the algorithm, it is imperative research direction to get prepared for. Further to the present work, we devote to emulate the physical emulation and implementation of the cryptosystem in a smart grid network environment to assess the practical ability and draw its performance parameters.

*Chapter 5. Contribution to Knowledge, Conclusion and Future Works*

# Bibliography

- [1] S. R. Salkuti, “Challenges, issues and opportunities for the development of smart grid,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 2, pp. 1179–1186, 2020.
- [2] D. Sarathkumar, M. Srinivasan, A. A. Stonier, R. Samikannu, N. R. Dasari, and R. A. Raj, “A technical review on self-healing control strategy for smart grid power systems,” in *IOP Conference Series: Materials Science and Engineering*, vol. 1055, p. 012153, IOP Publishing, 2021.
- [3] S. S. Refaat, A. Mohamed, and P. Kakosimos, “Self-healing control strategy; challenges and opportunities for distribution systems in smart grid,” in *2018 IEEE 12th International Conference on Compatibility, Power Electronics and Power Engineering (CPE-POWERENG 2018)*, pp. 1–6, IEEE, 2018.
- [4] M. Z. Gunduz and R. Das, “Cyber-security on smart grid: Threats and potential solutions,” *Computer networks*, vol. 169, p. 107094, 2020.
- [5] S. Kulkarni, Q. Gu, E. Myers, L. Polepeddi, S. Lipták, R. Beyah, and D. Divan, “Enabling a decentralized smart grid using autonomous edge control devices,” *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7406–7419, 2019.
- [6] Y. T. Aklilu and J. Ding, “Survey on blockchain for smart grid management, control, and operation,” *Energies*, vol. 15, no. 1, p. 193, 2022.
- [7] B. Chai, H. Zou, R. Liu, W. Chen, and J. Li, “Energy efficient protocol design for the wsn integrated supporting system of the smart grid,” in *2021 IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe)*, pp. 1–6, IEEE, 2021.
- [8] A. N. A. Randriantsoa, D. A. H. Fakra, L. Rakotondrajaona, and W. J. Van Der Merwe Steyn, “Recent advances in hybrid energy harvesting technologies using roadway pavements: A review of the technical possibility of using piezothermoelectrical combinations,” *International Journal of Pavement Research and Technology*, pp. 1–26, 2022.
- [9] R. Romo and O. Micheloud, “Power quality of actual grids with plug-in electric vehicles in presence of renewables and micro-grids,” *Renewable and Sustainable Energy Reviews*, vol. 46, pp. 189–200, 2015.

- [10] M. El Chehaly, O. Saadeh, C. Martinez, and G. Joos, “Advantages and applications of vehicle to grid mode of operation in plug-in hybrid electric vehicles,” in *2009 IEEE Electrical Power & Energy Conference (EPEC)*, pp. 1–6, IEEE, 2009.
- [11] Y. Kabalci, “A survey on smart metering and smart grid communication,” *Renewable and Sustainable Energy Reviews*, vol. 57, pp. 302–318, 2016.
- [12] M. L. Tuballa and M. L. Abundo, “A review of the development of smart grid technologies,” *Renewable and Sustainable Energy Reviews*, vol. 59, pp. 710–725, 2016.
- [13] F. Ayadi, I. Colak, I. Garip, and H. I. Bulbul, “Impacts of renewable energy resources in smart grid,” in *2020 8th International Conference on Smart Grid (icSmartGrid)*, pp. 183–188, IEEE, 2020.
- [14] D. Wenxiu, Z. Yan, and R. H. Deng, “Privacy-preserving data processing with flexible access control,” *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 2, pp. 363–376, 2017.
- [15] F. Calise, F. L. Cappiello, M. D. d’Accadia, and M. Vicidomini, “Smart grid energy district based on the integration of electric vehicles and combined heat and power generation,” *Energy Conversion and Management*, vol. 234, p. 113932, 2021.
- [16] J. Sakhnini, H. Karimipour, A. Dehghantanha, R. M. Parizi, and G. Srivastava, “Security aspects of internet of things aided smart grids: A bibliometric survey,” *Internet of things*, vol. 14, p. 100111, 2021.
- [17] G. Suci, M.-A. Sachian, A. Vulpe, M. Vochin, A. Farao, N. Koutroumpouchos, and C. Xenakis, “Sealedgrid: Secure and interoperable platform for smart grid applications,” *Sensors*, vol. 21, no. 16, p. 5448, 2021.
- [18] X. Xiang and J. Cao, “An efficient authenticated key agreement scheme supporting privacy-preservation for smart grid communication,” *Electric Power Systems Research*, vol. 203, p. 107630, 2022.
- [19] S. Goel and Y. Hong, “Security challenges in smart grid implementation,” in *Smart Grid Security*, pp. 1–39, Springer, 2015.
- [20] G. J. FitzPatrick and D. A. Wollman, “Nist interoperability framework and action plans,” in *IEEE PES General Meeting*, pp. 1–4, IEEE, 2010.
- [21] M. Taddeo, T. McCutcheon, and L. Floridi, “Trusting artificial intelligence in cybersecurity is a double-edged sword,” *Nature Machine Intelligence*, vol. 1, no. 12, pp. 557–560, 2019.



## Bibliography

- [22] P. Wang and M. Govindarasu, “Multi-agent based attack-resilient system integrity protection for smart grid,” *IEEE Transactions on Smart Grid*, vol. 11, no. 4, pp. 3447–3456, 2020.
- [23] A. Huseinović, S. Mrdović, K. Bicakci, and S. Uludag, “A survey of denial-of-service attacks and solutions in the smart grid,” *IEEE Access*, vol. 8, pp. 177447–177470, 2020.
- [24] A. Gopstein, C. Nguyen, C. O’Fallon, N. Hastings, D. Wollman, *et al.*, *NIST framework and roadmap for smart grid interoperability standards, release 4.0*. Department of Commerce. National Institute of Standards and Technology, 2021.
- [25] H. Li, *Enabling Secure and Privacy Preserving Communications in Smart Grids*. Springer, 2014.
- [26] J. Wang, L. Wu, S. Zeadally, M. K. Khan, and D. He, “Privacy-preserving data aggregation against malicious data mining attack for iot-enabled smart grid,” *ACM Transactions on Sensor Networks (TOSN)*, vol. 17, no. 3, pp. 1–25, 2021.
- [27] P. Gope and B. Sikdar, “Lightweight and privacy-friendly spatial data aggregation for secure power supply and demand management in smart grids,” *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 6, pp. 1554–1566, 2018.
- [28] N. Koblitz, “Elliptic curve cryptosystems,” *Mathematics of computation*, vol. 48, no. 177, pp. 203–209, 1987.
- [29] V. S. Miller, “Use of elliptic curves in cryptography,” in *Conference on the theory and application of cryptographic techniques*, pp. 417–426, Springer, 1985.
- [30] X. Ye, G. Xu, X. Cheng, Y. Li, and Z. Qin, “Certificateless-based anonymous authentication and aggregate signature scheme for vehicular ad hoc networks,” *Wireless Communications and Mobile Computing*, vol. 2021, 2021.
- [31] N. Saxena, B. J. Choi, and R. Lu, “Authentication and authorization scheme for various user roles and devices in smart grid,” *IEEE transactions on Information forensics and security*, vol. 11, no. 5, pp. 907–921, 2015.
- [32] J. Li, K.-K. R. Choo, W. Zhang, S. Kumari, J. J. Rodrigues, M. K. Khan, and D. Hogrefe, “Epa-cppa: An efficient, provably-secure and anonymous conditional privacy-preserving authentication scheme for vehicular ad hoc networks,” *Vehicular Communications*, vol. 13, pp. 104–113, 2018.
- [33] S.-F. Tzeng, S.-J. Horng, T. Li, X. Wang, P.-H. Huang, and M. K. Khan, “Enhancing security and privacy for identity-based batch verification scheme in vanets,” *IEEE Transactions on Vehicular Technology*, vol. 66, no. 4, pp. 3235–3248, 2015.

- [34] M. Fotros, J. Rezazadeh, and O. A. Sianaki, "A survey on vanets routing protocols for iot intelligent transportation systems," in *Workshops of the International Conference on Advanced Information Networking and Applications*, pp. 1097–1115, Springer, 2020.
- [35] E.-K. Lee, M. Gerla, G. Pau, U. Lee, and J.-H. Lim, "Internet of vehicles: From intelligent grid to autonomous cars and vehicular fogs," *International Journal of Distributed Sensor Networks*, vol. 12, no. 9, p. 1550147716665500, 2016.
- [36] M. Hayes and T. Omar, "End to end vanet/iot communications a 5g smart cities case study approach," in *2019 IEEE International Symposium on Technologies for Homeland Security (HST)*, pp. 1–5, IEEE, 2019.
- [37] E. S. Rigas, S. D. Ramchurn, and N. Bassiliades, "Managing electric vehicles in the smart grid using artificial intelligence: A survey," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 4, pp. 1619–1635, 2014.
- [38] S. Alshahrani, M. Khalid, and M. Almuahini, "Electric vehicles beyond energy storage and modern power networks: Challenges and applications," *IEEE Access*, vol. 7, pp. 99031–99064, 2019.
- [39] Z. Zhao, B. Zhao, and Y. Xia, "Research on power grid load after electric vehicles connected to power grid," in *2015 8th International Conference on Grid and Distributed Computing (GDC)*, pp. 36–39, IEEE, 2015.
- [40] J. Wang, C. Liu, D. Ton, Y. Zhou, J. Kim, and A. Vyas, "Impact of plug-in hybrid electric vehicles on power systems with demand response and wind power," *Energy Policy*, vol. 39, no. 7, pp. 4016–4021, 2011.
- [41] Q. Wang, X. Liu, J. Du, and F. Kong, "Smart charging for electric vehicles: A survey from the algorithmic perspective," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1500–1517, 2016.
- [42] J. Du, S. Ma, Y.-C. Wu, and H. V. Poor, "Distributed hybrid power state estimation under pmu sampling phase errors," *IEEE Transactions on Signal Processing*, vol. 62, no. 16, pp. 4052–4063, 2014.
- [43] J. Song, F. Yang, K.-K. R. Choo, Z. Zhuang, and L. Wang, "Sipf: A secure installment payment framework for drive-thru internet," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 16, no. 2, pp. 1–18, 2017.
- [44] J. Cui, J. Zhang, H. Zhong, R. Shi, and Y. Xu, "An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks," *Information Sciences*, vol. 451, pp. 1–15, 2018.
- [45] S. Sharma and A. Kaul, "Vanets cloud: Architecture, applications, challenges, and issues," *Archives of Computational Methods in Engineering*, pp. 1–22.

## Bibliography

- [46] R. Shrestha, R. Bajracharya, and S. Y. Nam, “Challenges of future vanet and cloud-based approaches,” *Wireless Communications and Mobile Computing*, vol. 2018, 2018.
- [47] M. Whaiduzzaman, M. Sookhak, A. Gani, and R. Buyya, “A survey on vehicular cloud computing,” *Journal of Network and Computer applications*, vol. 40, pp. 325–344, 2014.
- [48] D. He, S. Zeadally, B. Xu, and X. Huang, “An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks,” *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, 2015.
- [49] M. A. Al-shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, “An efficient identity-based conditional privacy-preserving authentication scheme for secure communication in a vehicular ad hoc network,” *Symmetry*, vol. 12, no. 10, p. 1687, 2020.
- [50] A. Sari, O. Onursal, M. Akkaya, *et al.*, “Review of the security issues in vehicular ad hoc networks (vanet),” *International Journal of Communications, Network and System Sciences*, vol. 8, no. 13, p. 552, 2015.
- [51] L. Cheng, Q. Wen, Z. Jin, H. Zhang, and L. Zhou, “Cryptanalysis and improvement of a certificateless aggregate signature scheme,” *information sciences*, vol. 295, pp. 337–346, 2015.
- [52] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, “A security and privacy review of vanets,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 2985–2996, 2015.
- [53] M. B. Mansour, C. Salama, H. K. Mohamed, and S. A. Hammad, “Vanet security and privacy-an overview,” *International Journal of Network Security & Its Applications (IJNSA) Vol*, vol. 10, 2018.
- [54] I. A. Kamil and S. O. Ogundoyin, “An improved certificateless aggregate signature scheme without bilinear pairings for vehicular ad hoc networks,” *Journal of information security and applications*, vol. 44, pp. 184–200, 2019.
- [55] I. Ali and F. Li, “An efficient conditional privacy-preserving authentication scheme for vehicle-to-infrastructure communication in vanets,” *Vehicular Communications*, vol. 22, p. 100228, 2020.
- [56] C. Zhang, X. Lin, R. Lu, P.-H. Ho, and X. Shen, “An efficient message authentication scheme for vehicular communications,” *IEEE transactions on vehicular technology*, vol. 57, no. 6, pp. 3357–3368, 2008.

- [57] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, “Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications,” in *IEEE INFOCOM 2008-The 27th Conference on Computer Communications*, pp. 1229–1237, IEEE, 2008.
- [58] S.-J. Horng, S.-F. Tzeng, P.-H. Huang, X. Wang, T. Li, and M. K. Khan, “An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks,” *Information Sciences*, vol. 317, pp. 48–66, 2015.
- [59] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, “Aggregate and verifiably encrypted signatures from bilinear maps,” in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 416–432, Springer, 2003.
- [60] K. Li, M. H. Au, W. H. Ho, and Y. L. Wang, “An efficient conditional privacy-preserving authentication scheme for vehicular ad hoc networks using online/offline certificateless aggregate signature,” in *International Conference on Provable Security*, pp. 59–76, Springer, 2019.
- [61] M. M. Taha and Y. M. Hasan, “Vanet-dsrc protocol for reliable broadcasting of life safety messages,” in *2007 IEEE International Symposium on Signal Processing and Information Technology*, pp. 104–109, IEEE, 2007.
- [62] S. S. Al-Riyami and K. G. Paterson, “Certificateless public key cryptography,” in *International conference on the theory and application of cryptology and information security*, pp. 452–473, Springer, 2003.
- [63] D. H. Yum and P. J. Lee, “Generic construction of certificateless signature,” in *Australasian Conference on Information Security and Privacy*, pp. 200–211, Springer, 2004.
- [64] X.-x. Li, K.-f. Chen, and L. Sun, “Certificateless signature and proxy signature schemes from bilinear pairings,” *Lithuanian Mathematical Journal*, vol. 45, no. 1, pp. 76–83, 2005.
- [65] M. H. Au, Y. Mu, J. Chen, D. S. Wong, J. K. Liu, and G. Yang, “Malicious kgc attacks in certificateless cryptography,” in *Proceedings of the 2nd ACM symposium on Information, computer and communications security*, pp. 302–311, 2007.
- [66] D. He, J. Chen, and R. Zhang, “An efficient and provably-secure certificateless signature scheme without bilinear pairings,” *International Journal of Communication Systems*, vol. 25, no. 11, pp. 1432–1442, 2012.
- [67] J.-L. Tsai, N.-W. Lo, and T.-C. Wu, “Weaknesses and improvements of an efficient certificateless signature scheme without using bilinear pairings,” *International Journal of Communication Systems*, vol. 27, no. 7, pp. 1083–1090, 2014.

## Bibliography

- [68] K.-H. Yeh, C. Su, K.-K. R. Choo, and W. Chiu, “A novel certificateless signature scheme for smart objects in the internet-of-things,” *Sensors*, vol. 17, no. 5, p. 1001, 2017.
- [69] X. Jia, D. He, Q. Liu, and K.-K. R. Choo, “An efficient provably-secure certificateless signature scheme for internet-of-things deployment,” *Ad Hoc Networks*, vol. 71, pp. 78–87, 2018.
- [70] X. Yang, X. Huang, and J. K. Liu, “Efficient handover authentication with user anonymity and untraceability for mobile cloud computing,” *Future Generation Computer Systems*, vol. 62, pp. 190–195, 2016.
- [71] J. Sánchez-García, J. M. García-Campos, D. Reina, S. Toral, and F. Barrero, “On-sitedriverid: A secure authentication scheme based on spanish eid cards for vehicular ad hoc networks,” *future generation computer systems*, vol. 64, pp. 50–60, 2016.
- [72] F. Ye, S. Roy, and H. Wang, “Efficient data dissemination in vehicular ad hoc networks,” *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 4, pp. 769–779, 2012.
- [73] C. Gamage, B. Gras, B. Crispo, and A. S. Tanenbaum, “An identity-based ring signature scheme with enhanced privacy,” in *2006 Securecomm and Workshops*, pp. 1–5, IEEE, 2006.
- [74] T. Wang and X. Tang, “A more efficient conditional private preservation scheme in vehicular ad hoc networks,” *Applied Sciences*, vol. 8, no. 12, p. 2546, 2018.
- [75] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, “A secure authentication scheme for vanets with batch verification,” *Wireless networks*, vol. 21, no. 5, pp. 1733–1743, 2015.
- [76] Y. Ming and X. Shen, “Pcpa: A practical certificateless conditional privacy preserving authentication scheme for vehicular ad hoc networks,” *Sensors*, vol. 18, no. 5, p. 1573, 2018.
- [77] J. Cui, J. Zhang, H. Zhong, and Y. Xu, “Spacf: A secure privacy-preserving authentication scheme for vanet with cuckoo filter,” *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 10283–10295, 2017.
- [78] M. A. Alazzawi, H. Lu, A. A. Yassin, and K. Chen, “Efficient conditional anonymity with message integrity and authentication in a vehicular ad-hoc network,” *IEEE Access*, vol. 7, pp. 71424–71435, 2019.
- [79] T. Evariste, W. Kasakula, J. Rwigema, and R. Datta, “Optimal exploitation of on-street parked vehicles as roadside gateways for social iov—a case of kigali city,”

- Journal of Open Innovation: Technology, Market, and Complexity*, vol. 6, no. 3, p. 73, 2020.
- [80] S. A. Jan, N. U. Amin, M. Othman, M. Ali, A. I. Umar, and A. Basir, "A survey on privacy-preserving authentication schemes in vanets: Attacks, challenges and open issues," *IEEE Access*, vol. 9, pp. 153701–153726, 2021.
- [81] Y. Ming and H. Cheng, "Efficient certificateless conditional privacy-preserving authentication scheme in vanets," *Mobile Information Systems*, vol. 2019, 2019.
- [82] I. A. Kamil and S. O. Ogundoyin, "A big data anonymous batch verification scheme with conditional privacy preservation for power injection over vehicular network and 5g smart grid slice," *Sustainable Energy, Grids and Networks*, vol. 20, p. 100260, 2019.
- [83] L. Zhang, F. Zhang, Q. Wu, and J. Domingo-Ferrer, "Simulatable certificateless two-party authenticated key agreement protocol," *Information Sciences*, vol. 180, no. 6, pp. 1020–1030, 2010.
- [84] M. Bayat, M. Pournaghi, M. Rahimi, and M. Barmshoory, "Nera: A new and efficient rsu based authentication scheme for vanets," *Wireless networks*, pp. 1–16, 2019.
- [85] A. K. Malhi and S. Batra, "An efficient certificateless aggregate signature scheme for vehicular ad-hoc networks," *Discrete Mathematics and theoretical computer science*, vol. 17, no. 1, pp. 317–338, 2015.
- [86] H. Xiong, Z. Guan, Z. Chen, and F. Li, "An efficient certificateless aggregate signature with constant pairing computations," *Information Sciences*, vol. 219, pp. 225–235, 2013.
- [87] A. Kumari, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and J. J. Rodrigues, "Fog computing for smart grid systems in the 5g environment: Challenges and solutions," *IEEE Wireless Communications*, vol. 26, no. 3, pp. 47–53, 2019.
- [88] R. Bayindir, I. Colak, G. Fulli, and K. Demirtas, "Smart grid technologies and applications," *Renewable and Sustainable Energy Reviews*, vol. 66, pp. 499–516, 2016.
- [89] R. Chaudhary, G. S. Aujla, S. Garg, N. Kumar, and J. J. Rodrigues, "Sdn-enabled multi-attribute-based secure communication for smart grid in iiot environment," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2629–2640, 2018.
- [90] T. Alladi, V. Chamola, J. J. Rodrigues, and S. A. Kozlov, "Blockchain in smart grids: A review on different use cases," *Sensors*, vol. 19, no. 22, p. 4862, 2019.

## Bibliography

- [91] V. Thakur, G. Indra, N. Gupta, P. Chatterjee, O. Said, and A. Tolba, “Cryptographically secure privacy-preserving authenticated key agreement protocol for an iot network: A step towards critical infrastructure protection,” *Peer-to-Peer Networking and Applications*, vol. 15, no. 1, pp. 206–220, 2022.
- [92] F. Ye, Y. Qian, and R. Q. Hu, “Smart grid communication infrastructures: big data, cloud computing, and security,” 2018.
- [93] X. Yuan and M. Elhoseny, “Intelligent data aggregation inspired paradigm and approaches in iot applications,” *Journal of Intelligent & Fuzzy Systems*, vol. 37, no. 1, pp. 3–7, 2019.
- [94] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, “A survey on cyber security for smart grid communications,” *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 998–1010, 2012.
- [95] N. Komninos, E. Philippou, and A. Pitsillides, “Survey in smart grid and smart home security: Issues, challenges and countermeasures,” *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1933–1954, 2014.
- [96] 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.
- [97] P. Kumar, A. Gurtov, M. Sain, A. Martin, and P. H. Ha, “Lightweight authentication and key agreement for smart metering in smart energy networks,” *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 4349–4359, 2018.
- [98] D. He, H. Wang, M. K. Khan, and L. Wang, “Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography,” *IET Communications*, vol. 10, no. 14, pp. 1795–1802, 2016.
- [99] D. Abbasinezhad-Mood and M. Nikooghadam, “An anonymous ecc-based self-certified key distribution scheme for the smart grid,” *IEEE Transactions on Industrial Electronics*, vol. 65, no. 10, pp. 7996–8004, 2018.
- [100] Z. Haddad, M. M. Fouda, M. Mahmoud, and M. Abdallah, “Blockchain-based authentication for 5g networks,” in *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, pp. 189–194, IEEE, 2020.
- [101] Y. Chen, J.-F. Martínez, P. Castillejo, and L. López, “An anonymous authentication and key establish scheme for smart grid: Fauth,” *Energies*, vol. 10, no. 9, p. 1354, 2017.
- [102] D. Sadhukhan, S. Ray, M. S. Obaidat, and M. Dasgupta, “A secure and privacy preserving lightweight authentication scheme for smart-grid communication using

- elliptic curve cryptography,” *Journal of Systems Architecture*, vol. 114, p. 101938, 2021.
- [103] J.-L. Tsai and N.-W. Lo, “Secure anonymous key distribution scheme for smart grid,” *IEEE transactions on smart grid*, vol. 7, no. 2, pp. 906–914, 2015.
- [104] M. Joye and G. Neven, *Identity-based cryptography*, vol. 2. IOS press, 2009.
- [105] X. Li, F. Wu, S. Kumari, L. Xu, A. K. Sangaiah, and K.-K. R. Choo, “A provably secure and anonymous message authentication scheme for smart grids,” *Journal of Parallel and Distributed Computing*, vol. 132, pp. 242–249, 2019.
- [106] A. Mohammadali, M. S. Haghghi, M. H. Tadayon, and A. Mohammadi-Nodooshan, “A novel identity-based key establishment method for advanced metering infrastructure in smart grid,” *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2834–2842, 2016.
- [107] Z. Wan, G. Wang, Y. Yang, and S. Shi, “Skm: Scalable key management for advanced metering infrastructure in smart grids,” *IEEE Transactions on Industrial Electronics*, vol. 61, no. 12, pp. 7055–7066, 2014.
- [108] K. Mahmood, S. A. Chaudhry, H. Naqvi, S. Kumari, X. Li, and A. K. Sangaiah, “An elliptic curve cryptography based lightweight authentication scheme for smart grid communication,” *Future Generation Computer Systems*, vol. 81, pp. 557–565, 2018.
- [109] V. Odelu, A. K. Das, M. Wazid, and M. Conti, “Provably secure authenticated key agreement scheme for smart grid,” *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 1900–1910, 2016.
- [110] L. Zhang, S. Tang, and H. Luo, “Elliptic curve cryptography-based authentication with identity protection for smart grids,” *PloS one*, vol. 11, no. 3, p. e0151253, 2016.
- [111] K. Mahmood, S. A. Chaudhry, H. Naqvi, T. Shon, and H. F. Ahmad, “A lightweight message authentication scheme for smart grid communications in power sector,” *Computers & Electrical Engineering*, vol. 52, pp. 114–124, 2016.
- [112] J. Srinivas, A. K. Das, X. Li, M. K. Khan, and M. Jo, “Designing anonymous signature-based authenticated key exchange scheme for internet of things-enabled smart grid systems,” *IEEE Transactions on Industrial Informatics*, vol. 17, no. 7, pp. 4425–4436, 2020.
- [113] D. Abbasinezhad-Mood, A. Ostad-Sharif, M. Nikooghadam, and S. M. Mazinani, “A secure and efficient key establishment scheme for communications of smart meters and service providers in smart grid,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1495–1502, 2019.



## Bibliography

- [114] L. Zhang, L. Zhao, S. Yin, C.-H. Chi, R. Liu, and Y. Zhang, “A lightweight authentication scheme with privacy protection for smart grid communications,” *Future Generation Computer Systems*, vol. 100, pp. 770–778, 2019.
- [115] M. Wazid, A. K. Das, N. Kumar, and J. J. Rodrigues, “Secure three-factor user authentication scheme for renewable-energy-based smart grid environment,” *IEEE Transactions on Industrial Informatics*, vol. 13, no. 6, pp. 3144–3153, 2017.
- [116] T. F. Vallent, D. Hanyurwimfura, and C. Mikeka, “Efficient certificate-less aggregate signature scheme with conditional privacy-preservation for vehicular ad hoc networks enhanced smart grid system,” *Sensors*, vol. 21, no. 9, p. 2900, 2021.
- [117] L. Deng and R. Gao, “Certificateless two-party authenticated key agreement scheme for smart grid,” *Information Sciences*, vol. 543, pp. 143–156, 2021.
- [118] M. Jo, S. Jangirala, A. K. Das, X. Li, and M. K. Khan, “Designing anonymous signature-based authenticated key exchange scheme for iot-enabled smart grid systems,” *IEEE Transactions on Industrial Informatics*, 2020.
- [119] D. He, S. Zeadally, H. Wang, and Q. Liu, “Lightweight data aggregation scheme against internal attackers in smart grid using elliptic curve cryptography,” *Wireless Communications and Mobile Computing*, vol. 2017, 2017.
- [120] 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.
- [121] R. Morello, S. C. Mukhopadhyay, Z. Liu, D. Slomovitz, and S. R. Samantaray, “Advances on sensing technologies for smart cities and power grids: A review,” *IEEE Sensors Journal*, vol. 17, no. 23, pp. 7596–7610, 2017.
- [122] R. Deng, G. Xiao, R. Lu, and J. Chen, “Fast distributed demand response with spatially and temporally coupled constraints in smart grid,” *IEEE Transactions on Industrial Informatics*, vol. 11, no. 6, pp. 1597–1606, 2015.
- [123] Y. Liu, C. Cheng, T. Gu, T. Jiang, and X. Li, “A lightweight authenticated communication scheme for smart grid,” *IEEE Sensors Journal*, vol. 16, no. 3, pp. 836–842, 2015.
- [124] D. Das and D. K. Rout, “Adaptive algorithm for optimal real-time pricing in cognitive radio enabled smart grid network,” *ETRI Journal*.
- [125] M. S. Alvarez-Alvarado and D. Jayaweera, “Reliability-based smart-maintenance model for power system generators,” *IET Generation, Transmission & Distribution*, vol. 14, no. 9, pp. 1770–1780, 2020.

- [126] Y. Gong, Y. Cai, Y. Guo, and Y. Fang, “A privacy-preserving scheme for incentive-based demand response in the smart grid,” *IEEE Transactions on Smart Grid*, vol. 7, no. 3, pp. 1304–1313, 2015.
- [127] M. A. Ferrag and A. Ahmim, *Security solutions and applied cryptography in Smart Grid Communications*. IGI Global, 2016.
- [128] J. B. Ekanayake, N. Jenkins, K. Liyanage, J. Wu, and A. Yokoyama, *Smart grid: technology and applications*. John Wiley & Sons, 2012.
- [129] O. R. M. Boudia, S. M. Senouci, and M. Feham, “Elliptic curve-based secure multi-dimensional aggregation for smart grid communications,” *IEEE Sensors Journal*, vol. 17, no. 23, pp. 7750–7757, 2017.
- [130] H. Qu, P. Shang, X. J. Lin, and L. Sun, “Cryptanalysis of a privacy-preserving smart metering scheme using linkable anonymous credential.,” *IACR Cryptol. ePrint Arch.*, vol. 2015, p. 1066, 2015.
- [131] M. Badra and S. Zeadally, “Lightweight and efficient privacy-preserving data aggregation approach for the smart grid,” *Ad Hoc Networks*, vol. 64, pp. 32–40, 2017.
- [132] S. Desai, R. Alhadad, N. Chilamkurti, and A. Mahmood, “A survey of privacy preserving schemes in ioe enabled smart grid advanced metering infrastructure,” *Cluster Computing*, vol. 22, no. 1, pp. 43–69, 2019.
- [133] S. Sultan, “Privacy-preserving metering in smart grid for billing, operational metering, and incentive-based schemes: A survey,” *Computers & Security*, vol. 84, pp. 148–165, 2019.
- [134] E. Vahedi, M. Bayat, M. R. Pakravan, and M. R. Aref, “A secure ecc-based privacy preserving data aggregation scheme for smart grids,” *Computer Networks*, vol. 129, pp. 28–36, 2017.
- [135] C. Hu, Y. Huo, L. Ma, H. Liu, S. Deng, and L. Feng, “An attribute-based secure and scalable scheme for data communications in smart grids,” in *International Conference on Wireless Algorithms, Systems, and Applications*, pp. 469–482, Springer, 2017.
- [136] H. Bao and R. Lu, “Comment on “privacy-enhanced data aggregation scheme against internal attackers in smart grid”,” *IEEE Transactions on Industrial Informatics*, vol. 12, no. 1, pp. 2–5, 2015.
- [137] D. Li, Z. Aung, J. Williams, and A. Sanchez, “P3: Privacy preservation protocol for automatic appliance control application in smart grid,” *IEEE Internet of things Journal*, vol. 1, no. 5, pp. 414–429, 2014.

## Bibliography

- [138] M. Yun and B. Yuxin, “Research on the architecture and key technology of internet of things (iot) applied on smart grid,” in *2010 International Conference on Advances in Energy Engineering*, pp. 69–72, IEEE, 2010.
- [139] C. Bekara, “Security issues and challenges for the iot-based smart grid,” in *FNC/MobiSPC*, pp. 532–537, 2014.
- [140] C. Savaglio, M. Ganzha, M. Paprzycki, C. Bădică, M. Ivanović, and G. Fortino, “Agent-based internet of things: State-of-the-art and research challenges,” *Future Generation Computer Systems*, vol. 102, pp. 1038–1053, 2020.
- [141] X. Zuo, L. Li, H. Peng, S. Luo, and Y. Yang, “Privacy-preserving multidimensional data aggregation scheme without trusted authority in smart grid,” *IEEE Systems Journal*, vol. 15, no. 1, pp. 395–406, 2020.
- [142] R. Lu, K. Heung, A. H. Lashkari, and A. A. Ghorbani, “A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced iot,” *IEEE Access*, vol. 5, pp. 3302–3312, 2017.
- [143] J. Hur, D. Koo, and Y. Shin, “Privacy-preserving smart metering with authentication in a smart grid,” *Applied Sciences*, vol. 5, no. 4, pp. 1503–1527, 2015.
- [144] S. Li, K. Xue, Q. Yang, and P. Hong, “Ppma: Privacy-preserving multisubset data aggregation in smart grid,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 2, pp. 462–471, 2017.
- [145] P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes,” in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 223–238, Springer, 1999.
- [146] I. Ali, E. Khan, and S. Sabir, “Privacy-preserving data aggregation in resource-constrained sensor nodes in internet of things: A review,” *Future Computing and Informatics Journal*, vol. 3, no. 1, pp. 41–50, 2018.
- [147] D. He, N. Kumar, S. Zeadally, A. Vinel, and L. T. Yang, “Efficient and privacy-preserving data aggregation scheme for smart grid against internal adversaries,” *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2411–2419, 2017.
- [148] C. Dwork, K. Kenthapadi, F. McSherry, I. Mironov, and M. Naor, “Our data, ourselves: Privacy via distributed noise generation,” in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 486–503, Springer, 2006.
- [149] A. Dyda, M. Purcell, S. Curtis, E. Field, P. Pillai, K. Ricardo, H. Weng, J. C. Moore, M. Hewett, G. Williams, *et al.*, “Differential privacy for public health data: An innovative tool to optimize information sharing while protecting data confidentiality,” *Patterns*, vol. 2, no. 12, p. 100366, 2021.

- [150] R. L. Rivest, "Cryptography," in *Algorithms and Complexity*, pp. 717–755, Elsevier, 1990.
- [151] K. K. Phiri and H. Kim, "Linear secret sharing scheme with reduced number of polynomials," *Security and Communication Networks*, vol. 2019, 2019.
- [152] Y. Liu, W. Guo, C.-I. Fan, L. Chang, and C. Cheng, "A practical privacy-preserving data aggregation (3pda) scheme for smart grid," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 3, pp. 1767–1774, 2018.
- [153] H. J. Jo, I. S. Kim, and D. H. Lee, "Efficient and privacy-preserving metering protocols for smart grid systems," *IEEE Transactions on Smart Grid*, vol. 7, no. 3, pp. 1732–1742, 2015.
- [154] 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.
- [155] T. W. Chim, S.-M. Yiu, V. O. Li, L. C. Hui, and J. Zhong, "Prga: Privacy-preserving recording & gateway-assisted authentication of power usage information for smart grid," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 1, pp. 85–97, 2014.
- [156] X. Dong, J. Zhou, K. Alharbi, X. Lin, and Z. Cao, "An elgamal-based efficient and privacy-preserving data aggregation scheme for smart grid," in *2014 IEEE Global Communications Conference*, pp. 4720–4725, IEEE, 2014.
- [157] D. Wu and C. Zhou, "Fault-tolerant and scalable key management for smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 375–381, 2011.
- [158] J. Xia and Y. Wang, "Secure key distribution for the smart grid," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1437–1443, 2012.
- [159] D. Abbasinezhad-Mood and M. Nikooghadam, "Design and hardware implementation of a security-enhanced elliptic curve cryptography based lightweight authentication scheme for smart grid communications," *Future Generation Computer Systems*, vol. 84, pp. 47–57, 2018.
- [160] S. Tonyali, K. Akkaya, N. Saputro, A. S. Uluagac, and M. Nojournian, "Privacy-preserving protocols for secure and reliable data aggregation in iot-enabled smart metering systems," *Future Generation Computer Systems*, vol. 78, pp. 547–557, 2018.
- [161] M. Bae, K. Kim, and H. Kim, "Preserving privacy and efficiency in data communication and aggregation for ami network," *Journal of Network and Computer Applications*, vol. 59, pp. 333–344, 2016.

## Bibliography

- [162] M. Tahir, A. Khan, A. Hameed, M. Alam, M. K. Khan, and F. Jabeen, “Towards a set aggregation-based data integrity scheme for smart grids,” *Annals of Telecommunications*, vol. 72, no. 9-10, pp. 551–561, 2017.
- [163] A. Abdallah and X. S. Shen, “A lightweight lattice-based homomorphic privacy-preserving data aggregation scheme for smart grid,” *IEEE Transactions on Smart Grid*, vol. 9, no. 1, pp. 396–405, 2016.
- [164] T. W. Chim, S.-M. Yiu, L. C. Hui, and V. O. Li, “Pass: Privacy-preserving authentication scheme for smart grid network,” in *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 196–201, IEEE, 2011.
- [165] F. D. Garcia and B. Jacobs, “Privacy-friendly energy-metering via homomorphic encryption,” in *International Workshop on Security and Trust Management*, pp. 226–238, Springer, 2010.
- [166] M. A. Ferrag, “Epec: an efficient privacy-preserving energy consumption scheme for smart grid communications,” *Telecommunication Systems*, vol. 66, no. 4, pp. 671–688, 2017.
- [167] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, “A systematic review of data protection and privacy preservation schemes for smart grid communications,” *Sustainable cities and society*, vol. 38, pp. 806–835, 2018.
- [168] J. Koo, X. Lin, and S. Bagchi, “Rl-blh: Learning-based battery control for cost savings and privacy preservation for smart meters,” in *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pp. 519–530, IEEE, 2017.
- [169] A. Humayed, J. Lin, F. Li, and B. Luo, “Cyber-physical systems security—a survey,” *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802–1831, 2017.
- [170] V. Ford, A. Siraj, and M. A. Rahman, “Secure and efficient protection of consumer privacy in advanced metering infrastructure supporting fine-grained data analysis,” *Journal of Computer and System Sciences*, vol. 83, no. 1, pp. 84–100, 2017.
- [171] 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.
- [172] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin, “Private memoirs of a smart meter,” in *Proceedings of the 2nd ACM workshop on embedded sensing systems for energy-efficiency in building*, pp. 61–66, 2010.

- [173] S. Tan, D. De, W.-Z. Song, J. Yang, and S. K. Das, “Survey of security advances in smart grid: A data driven approach,” *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 397–422, 2017.
- [174] B. A. Akyol, H. Kirkham, S. L. Clements, and M. D. Hadley, “A survey of wireless communications for the electric power system,” tech. rep., Pacific Northwest National Lab.(PNNL), Richland, WA (United States), 2010.
- [175] M. Eissa, “New protection principle for smart grid with renewable energy sources integration using wimax centralized scheduling technology,” *International journal of electrical power & energy systems*, vol. 97, pp. 372–384, 2018.
- [176] T. S. Ustun, R. H. Khan, A. Hadbah, and A. Kalam, “An adaptive microgrid protection scheme based on a wide-area smart grid communications network,” in *2013 IEEE Latin-America Conference on Communications*, pp. 1–5, IEEE, 2013.
- [177] A. Pawar and S. Rahane, “Opportunities and challenges of wireless communication technologies for smart grid applications,” *International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC)*, vol. 3, no. 1, pp. 289–296, 2013.
- [178] M. Eissa and N. Ali, “Performance evaluation of ieee 802.16 real time polling and unsolicited grant service scheduling for protecting transmission and sub-transmission systems with multi-terminals,” *Electric Power Systems Research*, vol. 167, pp. 48–57, 2019.
- [179] M. S. Farash and M. A. Attari, “A secure and efficient identity-based authenticated key exchange protocol for mobile client–server networks,” *The Journal of Supercomputing*, vol. 69, no. 1, pp. 395–411, 2014.
- [180] J. K. Liu, T. H. Yuen, M. H. Au, and W. Susilo, “Improvements on an authentication scheme for vehicular sensor networks,” *Expert Systems with Applications*, vol. 41, no. 5, pp. 2559–2564, 2014.
- [181] 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)*, pp. 1–6, IEEE, 2015.
- [182] M. Scott, “Multiprecision integer and rational arithmetic cryptographic library,” 2003.
- [183] D. J. Bernstein, “Introduction to post-quantum cryptography,” in *Post-quantum cryptography*, pp. 1–14, Springer, 2009.
- [184] L. Chen, L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, *Report on post-quantum cryptography*, vol. 12. US Department of Commerce, National Institute of Standards and Technology . . . , 2016.

# Appendix A

## List of Publications

The main work comprising this thesis led up to three publications in the following journals.

1. Vallent, Thokozani Felix, Damien Hanyurwimfura, and Chomora Mikeka. "Efficient certificate-less aggregate signature scheme with conditional privacy-preservation for vehicular ad hoc networks enhanced smart grid system." *Sensors* 21, no. 9 (2021): 2900.
2. Vallent, Thokozani Felix, Damien Hanyurwimfura, Hyunsung Kim, and Chomora Mikeka. "Certificate-less authenticated key agreement scheme with anonymity for smart grid communications." *Journal of Intelligent & Fuzzy Systems Preprint*: 1-11, 2022.
3. Vallent Thokozani Felix, Hanyurwimfura Damien, Jayavel Kayalvizhi, Kim Hyunsung Kim and Mikeka Chomora, "Lightweight Privacy-Preserving Data Aggregation Scheme Based on Elliptic Curve Cryptography for Smart Grid Communications", in *SGIoT EAI-2021 Conferences Proceedings*