

Cryptographic-Based Secure Data Exchange Schemes for Uplink and Downlink Communication in AMI Networks

by

Samer KHASAWNEH

THESIS PRESENTED TO
ÉCOLE DE TECHNOLOGIE SUPÉRIEURE
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY
Ph.D.

MONTREAL, JULY 15, 2020

ÉCOLE DE TECHNOLOGIE SUPÉRIEURE
UNIVERSITÉ DU QUÉBEC



Samer Khasawneh, 2020



This Creative Commons license allows readers to download this work and share it with others as long as the author is credited. The content of this work can't be modified in any way or used commercially.

BOARD OF EXAMINERS

THIS THESIS HAS BEEN EVALUATED

BY THE FOLLOWING BOARD OF EXAMINERS

Mr. Michel Kadoch, Thesis Supervisor
Department of Electrical Engineering at École de technologie supérieure

Mr. Alain April, President of the Board of Examiners
Department of Software Engineering at École de technologie supérieure

Mr. Abdelouahed Gherbi, Member of the jury
Department of Software Engineering at École de technologie supérieure

Mr. Rommel Torres, External Independent Examiner
Electronics and Computer Science Department at Universidad Tecnica Particular de Loja

THIS THESIS WAS PRESENTED AND DEFENDED

IN THE PRESENCE OF A BOARD OF EXAMINERS

ON JULY 10, 2020

AT ÉCOLE DE TECHNOLOGIE SUPÉRIEURE

Systèmes D'échange De Données Sécurisées à Base De Cryptographie Pour La Communication En Liaison Montante et En Liaison Descendante Dans Des Réseaux AMI

Samer KHASAWNEH

RESUME

La demande croissante d'électricité et le besoin d'infrastructures électriques intelligentes et modernisées ont créé le concept de réseau « intelligent ». Ce dernier intègre les technologies de l'information et de la communication (TIC) dans ses réseaux sous-jacents afin de parvenir à un contrôle décentralisé de l'offre et de la demande d'électricité et de réduire les pertes d'électricité et les coûts énergétiques. L'information bidirectionnelle et le flux d'électricité entre la station de tête de services et les clients sont les principales caractéristiques du réseau intelligent. Ces fonctionnalités permettent d'appliquer de nombreuses fonctions qui permettraient d'améliorer le réseau électrique traditionnel.

L'infrastructure de mesure avancée (AMI) est une architecture centrale du réseau intelligent qui joue un rôle essentiel dans la réalisation de nombreuses applications modernisées telles que la réponse à la demande, la lecture automatisée des compteurs et le contrôle de la gestion à distance en permettant la communication bidirectionnelle entre le service public et son client. Cette architecture repose sur des appareils pertinents tels que des compteurs intelligents et des canaux de communication semi-ouverts pour échanger une quantité massive d'informations sensibles. Ceci, en plus de la faiblesse héritée du réseau électrique, ouvre la voie à un nombre incalculable de menaces de sécurité qui n'ont jamais existé dans le réseau électrique traditionnel. Faisant partie d'un système électrique, AMI possède des caractéristiques uniques qui mettent à rude épreuve la conception de protocoles de sécurité efficaces pour protéger l'échange de données dans ses réseaux.

Dans cette thèse, nous répondons à la nécessité d'un échange de données sécurisé dans les réseaux AMI en proposant des solutions basées sur les exigences cryptographiques pour protéger les communications à destinataire unique et à destinataires multiples. La communication à destinataire unique représente la transmission de données unicast des rapports de consommation d'énergie des compteurs intelligents vers le centre de contrôle du réseau pour assurer une facturation correcte des clients. La préservation de la confidentialité des clients est l'objectif de sécurité le plus important pour la communication de données en liaison montante. Nous avons donc conçu HE-SSRU, un schéma de cryptage hybride qui exploite la force de la cryptographie à clé publique avec l'efficacité de la cryptographie symétrique pour sécuriser la communication en liaison montante entre les compteurs intelligents et l'Ordinateur maître de ressources (UMC). Le schéma proposé intègre des fonctionnalités de sécurité supplémentaires pour garantir l'authenticité des informations de mesure et atténue de nombreuses attaques telles que la relecture, la modification des données et l'attaque d'usurpation. De plus, nous proposons S-CP-ABE, un nouveau schéma de chiffrement léger basé sur le chiffrement basé sur les attributs pour réaliser une communication

sécurisée à plusieurs destinataires en liaison descendante dans les réseaux AMI. Le schéma applique un mécanisme de contrôle d'accès robuste en permettant au centre de contrôle de déterminer les compteurs intelligents éligibles pour accéder aux données sécurisées en construisant le texte chiffré selon une politique d'accès définie sur un ensemble d'attributs. Les compteurs autorisés dont les attributs satisfont à la politique d'accès peuvent décrypter le texte chiffré en obtenant un jeton de décryptage auprès de l'autorité d'attribut. Le protocole est différent de la plupart des schémas ABE dans le sens où nous l'avons construit sans utiliser les opérations d'appariement bilinéaires complexes. Notre système préserve la confidentialité et l'authenticité des messages du centre de contrôle et résiste aux attaques de collusion, de relecture et de contrefaçon de signature.

L'évaluation des performances montre que nos approches proposées surpassent les schémas existants de la littérature en termes de complexité de calcul, de surcharge de communication et d'exigences de stockage.

Mots-clés: smart grid, réseaux AMI, communication bidirectionnelle, sécurité, cryptographique, cryptage hybride, cryptage basé sur les attributs, cryptage des signes

Cryptographic-based Secure Data Exchange Schemes for Uplink and Downlink Communication in AMI Networks

Samer KHASAWNEH

ABSTRACT

The growing electricity demand and the need for intelligent and modernized power infrastructures have emerged in the concept of "smart" grid. This later integrates Information and Communication Technologies (ICTs) in its underlying networks to achieve decentralized control of electrical supply and demand in order to reduce electricity waste and energy costs. Two-way information and electricity flow between the utility headend and customers are the main features that characterize the smart grid. These features empower many functions to be implemented and enhancements to be applied to the legacy power grid.

Advanced Metering Infrastructure (AMI) is a central smart grid element that plays a vital role in realizing numerous modernized applications such as demand response, automated metering reading and remote management control by empowering bi-directional communication between the utility and its' customers. This architecture relies on violable devices such as smart meters and semi-open communication channels to exchange massive amount of sensitive information. This, in addition to the inherited weakness of the power grid paves the way to countless number of security threats that never existed in the legacy power grid. Being a part of an electricity system, AMI possess unique characteristics that puts challenging constraints on designing efficient security protocols to protect data exchange in its' networks.

In this thesis, we address the need for secure data exchange in AMI networks by proposing requirements-driven cryptographic-based solutions to protect single and multiple recipient communications. Single-recipient communication represents the unicast data transmission of energy consumption reports from the smart meters towards the utility headend to ensure correct customer billing. Preserving customer privacy is the most important security goal for uplink data communication, therefore we designed *HE-SSRU*, a hybrid encryption scheme that exploits the strength of public-key cryptography with the efficiency of symmetric cryptography to secure uplink communication between the smart meters and Utility Master Computer (UMC). The proposed scheme integrates additional security features to ensure authenticity of metering information and mitigates numerous attacks such as replay, data modification and spoofing attack. In addition, we propose *S-CP-ABE*, a novel lightweight signcryption scheme based on Attribute-Based Encryption to achieve secure multiple-recipient downlink communication in AMI networks. The scheme enforces robust access control mechanism by permitting the control center to determine the smart meters eligible for accessing the secure data by constructing the ciphertext according to an access policy defined over a set of attributes. Authorized meters with attributes satisfying the access policy can decrypt the ciphertext by obtaining a decryption token from the attribute authority. The protocol is different from most of the ABE schemes in the sense that we built it without using the complex bilinear pairing

operations. Our scheme maintains confidentiality and authenticity of control center messages and is resilient against collusion, replay, and signature forgery attacks.

Performance evaluation shows that our proposed approaches outperform existing schemes from the literature in terms of computational complexity, communication overhead and storage requirements.

Keywords: smart grid, AMI networks, bidirectional communication, security, cryptographic-based, hybrid encryption, attribute based encryption, signcryption

TABLE OF CONTENTS

	Page
CHAPTER 1 INTRODUCTION	1
1.1 Smart Grid Architecture.....	3
1.2 Advanced Metering Infrastructure (AMI)	4
1.2.1 AMI Programs	5
1.2.2 AMI Architecture.....	7
1.3 The Security of AMI Networks	8
1.3.1 AMI Vulnerabilities and Attacks	9
1.3.1.1 Vulnerabilities of AMI Information Networks	9
1.3.1.2 Passive and Active Attacks in AMI Networks	10
1.3.2 Problem Overview	13
1.4 Research Objectives.....	15
1.5 Thesis Contribution.....	16
1.6 Thesis Outline	17
 CHAPTER 2 BACKGROUND INFORMATION AND LITERATURE REVIEW	 19
2.1 Background.....	19
2.1.1 Elliptic Curve Cryptography (ECC)	19
2.1.2 Pairing-Based Cryptography (PBC)	20
2.1.2.1 Bilinear Pairing	21
2.1.2.2 Identity-Based Encryption (IBE)	21
2.1.2.3 Attribute-Based Encryption (ABE).....	22
2.1.3 The Paillier Cryptosystem	24
2.2 Literature Review.....	25
2.2.1 Security Schemes for Uplink Data Communication	25
2.2.1.1 Schemes Based on Secret Key Encryption	25
2.2.1.2 Schemes Based on Elliptic Curve Encryption	26
2.2.1.3 Schemes Based on Identity-Based Encryption	27
2.2.1.4 Schemes Based on Homomorphic Encryption	28
2.2.2 Security Schemes for Downlink Data Communication.....	30
2.2.2.1 Schemes Based on Group Key Management.....	30
2.2.2.2 Schemes Based on Pairing Based Cryptography	31
 CHAPTER 3 HE-SSRU: A HYBRID ENCRYPTION SECURE SINGLE-RECIPIENT UPLINK COMMUNICATION SCHEME FOR AMI NETWORKS	 33
3.1 Overview.....	33
3.2 Mechanism Description and Design Goals.....	33
3.3 Preliminaries	35

3.3.1	Elliptic Curve Cryptography (ECC)	35
3.3.2	Elliptic Curve Discrete Logarithmic Problem (ECDLP) and Keys Generation	36
3.3.3	The Road to Elliptic Curve Integrated Encryption Scheme (ECIES).....	37
3.4	The Proposed Hybrid Encryption Secure Single-Recipient Uplink Communication Scheme (HC-SSRU)	43
3.4.1	The Network Model.....	44
3.4.2	The Threat Model	45
3.4.3	Optimizing the Computation Overhead of ECIES.....	45
3.4.4	Message Format	47
3.4.5	Details of HE-SSRU	48
3.5	Performance Analysis	52
3.5.1	Computation Overhead	52
3.5.1	Communication Overhead	53
3.5.2	Storage Overhead.....	54
3.6	Security Analysis	56
3.7	Chapter Summary	59

CHAPTER 4	ESUD: AN ENCRYPTION AND SIGNATURE SCHEME TO SECURE UPLINK AND DOWNLINK COMMUNICATIONS IN AMI NETWORKS.....	61
4.1	Mechanism Description and Design goals.....	61
4.2	Preliminaries : Elliptic Curve Digital Signature Algorithm (ECDSA).....	61
4.3	The proposed Scheme	62
4.3.1	Network and Communication Mode.....	62
4.3.2	Adversarial Model	64
4.3.3	The Proposed Scheme to Ensure Secure Uplink and Downlink Communication.....	64
4.4	Performance Evaluation and Security Analysis.....	68
4.4.1	Performance Evaluation.....	69
4.4.1.1	Computation Cost	69
4.4.1.2	Ciphertext Size.....	71
4.4.1.3	Storage Overhead.....	72
4.4.2	Security Analysis	73
4.4.2.1	Resiliency Against Passive Attacks	74
4.4.2.2	Resiliency Against Impersonation Attack	74
4.4.2.3	Resiliency Against Replay Attacks.....	75
4.4.2.4	Resiliency Against Message Modification Attack.....	75
4.4.3	Limitation of the proposed scheme.....	75
4.5	Chapter Summary	76

CHAPTER 5	S-CP-ABE: A SIGNCRYPTION SCHEME BASED ON CP-ABE TO SECURE DOWNLINK MULTICAST COMMUNICATION IN AMI NETWORKS	79
5.1	Overview.....	79
5.2	Mechanism Description and Design goals.....	80
5.3	Preliminaries	81
5.4	The Proposed CP-ABE Signcryption Scheme.....	83
5.4.1	The Network Model.....	84
5.4.2	The Adversarial Model	86
5.4.3	The Details of the Proposed S-CP-ABE	87
5.4.3.1	Global System Setup (Υ).....	88
5.4.3.2	Authority Setup (GP)	88
5.4.3.3	Supervisory Control Center Setup (GP)	89
5.4.3.4	Signcryption: Ciphertext and Signature Generation (GP, m, PK, A, ks).....	89
5.4.3.5	Key Generation (GP, SID, MK, i)	90
5.4.3.6	Designcryption: Signature Verification and Decryption ($GP, \hat{C}, \{SK\}i, SID, kv$)	91
5.4.4	The Correctness Proof of The Proposed Scheme	92
5.5	Performance Analysis	94
5.5.1	Message Size.....	94
5.5.2	Communication and Revocation Overhead	95
5.5.3	Computation Overhead	96
5.6	Security Analysis	99
5.6.1	Collusion Attack Resistance	100
5.6.2	Data Confidentiality.....	101
5.6.3	Data Integrity and Signature Forgery	101
5.7	Chapter Summary	102
	CONCLUSIONS AND FUTURE WORK	103
APPENDIX I	ELLIPTIC CURVE ARITHMATIC.....	107
APPENDIX II	CONVERTING MONOTONIC BOOLEAN FORMULA INTO LSSS MATRIX.....	109
APPENDIX III	LIST OF PUBLICATIONS	111
	LIST OF BIBLIOGRAPHICAL REFERENCES.....	113

LIST OF TABLES

		Page
Table 3.1	The size of cryptographic parameters for the same security level.....	36
Table 3.2	Computation time for single scalar-point multiplication	46
Table 3.3	Simulation environment parameters	52
Table 3.4	Storage overhead on smart meters	56
Table 4.1	Notation guide used in section 4.3	66
Table 4.2	List of notations used in section 4.4.....	69
Table 4.3	Computation overhead comparison between ESUD and IBS.....	70
Table 4.4	Comparison of keys storage overhead	73
Table 5.1	List of notations used in section 5.4.....	85
Table 5.2	List of new notations used in section 5.5	94
Table 5.3	Comparison of messages size for different CP-ABE schemes	95
Table 5.4	Comparison of computation overhead for different CP-ABE schemes.....	98

LIST OF FIGURES

	Page
Figure 1.1 The smart grid multi-layer architecture Taken from Komninos et al. (2014).....	3
Figure 1.2 The architecture of AMI network deployed in the smart grid	8
Figure 1.3 Classification of attacks	10
Figure 3.1 The structure of hybrid cryptosystem. (a) Encryption. (b) Decryption	34
Figure 3.2 Elliptic curve points calculator	40
Figure 3.3 AMI network model assumed in HE-SSRU	44
Figure 3.4 The simplified AMI network model	45
Figure 3.5 The message format of the proposed hybrid cryptosystem	47
Figure 3.6 The initialization phase of HE-SSRU	49
Figure 3.7 Message encryption procedure	50
Figure 3.8 Comparison of decryption time incurred by NAN gateway	54
Figure 3.9 The computation overhead for different number of smart meters	55
Figure 3.10 Storage overhead on NAN gateway for variable number of smart meters	57
Figure 4.1 The AMI communication model assumed in the proposed security Scheme. a) Unicast uplink ommunication. b) Multicast downlink communication.....	64
Figure 4.2 The details of registration phase	68

Figure 4.3	The computation overhead for transmitting or receiving multiple secure uplink messages71
Figure 4.4	A comparison between our scheme and IBS in terms of ciphertext size...72
Figure 4.5	Storage overhead comparison74
Figure 5.1	The typical architecture of CP-ABE scheme80
Figure 5.2	AMI network model for the proposed signcryption scheme86
Figure 5.3	The steps of the proposed signcryption scheme87
Figure 5.4	Ciphertext format in the proposed signcryption scheme. Shaded fields are encrypted95
Figure 5.5	Signcryption/Encryption overhead comparison for different access policy sizes.....99
Figure 5.6	Designcryption/Decryption overhead comparison for different access Policy Sizes100
Figure A1.1	The points of elliptic curve $E_{37}(-5,8)$108
Figure A2.1	Access tree corresponding to Boolean formula (A2.1).....110

LIST OF ALGORITHMS

	Page
Algorithm 3.1 Cryptographic keys generation using elliptic curves	37
Algorithm 3.2 ECIES decryption procedure	43
Algorithm 3.3 Decryption procedure in HE-SSRU	51
Algorithm 5.1 Global Setup($\mathcal{Y}$)	88
Algorithm 5.2 Authority_Setup(GP)	89
Algorithm 5.3 Signcryption (GP, m, PK, A, k_s)	90
Algorithm 5.4 Designcryption ($GP, \hat{C}, \{SK\}_{i, SID}, k_v$)	92

LIST OF ABBREVIATIONS

AA	Attribute Authority
ABE	Attribute Based Encryption
AES	Advance Encryption standard
AMI	Advanced Metering Infrastructure
AMR	Automatic Meter Reading
ANSI	American National Standards Institute
API	Authentication Path Information
BAN	Building Area Network
BGKM	Broadcast Group Key Management
CA	Certificate Authority
CO ₂	Carbon Dioxide
CP-ABE	Ciphertext-Policy Attribute Based Encryption
CPU	Central Processing Unit
CR	Cognitive Radio
DER	Distributed Energy Resource
DG	Distributed Generation
DH-DSA	Diffie Hellman Digital Signature Algorithm
DMC	Data Management Center

DoS	Denial of Service
DR	Demand Response
DSM	Demand Side Management
ECC	Elliptic Curve Cryptography
ECDLP	Elliptic Curve Discrete Logarithmic Problem
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Scheme
EISA	Energy Independence and Security Act
eMTC	Enhanced Machine Type Communication
ESP	Energy Service Provider
EV	Electric Vehicle
FAN	Field Area Network
FHMQV	Fully Hashed Menezes-Qu-Vanstone
HAN	Home Area Network
HC	Hybrid Cryptosystem
HEV	Hybrid Electric Vehicle
$HMAC_k$	Cryptographic keyed-hash message authentication function
IAN	Infrastructure Area Network
IBE	Identity-Based Encryption

IBS	Identity Based Signcryption
ICT	Information and Communication Technology
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
KDF	Key Derivation Function
KGS	Key Generation Server
KP-ABE	Key-Policy Attribute Based Encryption
LP	Load Profiling
LSSS	Liner Secret Sharing Scheme
MAC	Message Authentication Code
MDMS	Meter Data Management System
MSP	Monotone Span Program
MTBA	Merkle-Tree-Based Authentication
NAN	Neighborhood Area Network
PCB	Pairing-Based Cryptography
PG&E	Pacific Gas and Energy
PKG	Private Key Generator
PLC	Power Line Communication
PMU	Phasor Measurement Unit

PS	Peak Shaving
PUF	Physically Unclonable Function
RSA	Rivest–Shamir–Adleman
RTU	Remote Terminal Units
SCADA	Supervisory Control And Data Acquisition
SCC	Supervisory Control Center
S-CP-ABE	Signcryption Scheme Based on CP-ABE to Secure Downlink Multicast Communication in AMI Networks
SHA	Secure Hash Algorithm
SID	Smart meter IDentifier
SM	Smart Meter
TPA	Third Party Auditor
TTP	Trusted Third Party
U.S	United States
UMC	Utility Master Computer
WAN	Wide Area Networks
WiMAX	Worldwide Interoperability for Microwave Access
XOR	Exclusive OR

LIST OF SYMBOLS

A	LSSS access matrix of dimension $n \times l$
$AUTH$	Authentication code
AK_i	The public key of attribute i
B_i	Block i of ciphertext
$C_0, C_{1,x}$	Ciphertexts generated by control center
C_m	Ciphertext of point m
D_x	Decryption token of attribute x
E_q	Elliptic curve over prime field q
H_1, H_2, F	Hash functions
k_U	Secret key for unicast communication
k_s	Control center private signing key
k_v	Signature verification public key
k_B	Secret key for broadcast communication
k_M	Secret key for multicast communication
K_h	Authentication key
KP_{BD}	Public key for signature verification of downlink broadcast communication
KP_{MD}	Public key for signature verification of downlink multicast communication
KP_{UD}	Public key for signature verification of downlink unicast communication
KP_{UU}	Public key for signature verification of uplink unicast communication
KS_{BD}	Secret key for signature generation of uplink broadcast communication
KS_{MD}	Secret key for signature generation of uplink multicast communication

KS_{UD}	Secret key for signature generation of uplink unicast communication
KS_{UU}	Secret key for signature generation of uplink unicast communication
K_e	Encryption/decryption key
K_r	Arbitrary key
K'_r	Encrypted arbitrary key
K_{sh}	Shared secret key
$ L $	Broadcast domain size
m	Message (plaintext) generated by the control center
$ M $	Message M size
M'	Message Ciphertext
$\bar{M}_t$	Ciphertext of message M_t
N_t	Nonce value for message t
$SK_{i,SID}$	Secret key of attribute i given to smart meter SID
T_{mul}	Time to perform scalar-point multiplication
T_{pair}	Time to perform bilinear pairing operating
T_{symm}	Encryption/decryption time of secret key algorithm
$ point $	The size of an elliptic curve point in bits
$\mathbb{F}_q$	Finite Field of order q
σ_t	Signature of message t
τ_m	Timestamp assigned to message m
ω_A, Y_A	Attribute authority secret keys
$ $	Concatenation
$ \mathcal{M} $	Multicast domain size

$\hat{C}$	Digitally signed ciphertext
γ	Security parameter
O	Point of Infinity
G	Elliptic curve generator point
PK	Attribute authority public key
Q	Precomputation Value
SID	The identifier assigned to the smart meter
$SYNCH$	Timestamp
i	Attribute identifier
l	Substring length
N	Number of multicast domains
s	Secret value
v	Message (plaintext) size
$\mathcal{SS}$	Set of user attributes satisfying the access policy
$\mathcal{US}$	Set of all user attributes
$\mathcal{M}$	Multicast domain
$\mathcal{U}$	Attributes universe
$\mathbb{G}$	Group of order q
$\mathbb{Z}_q$	Finite Field of order q
δ	Elliptic curve-based signature algorithm (ex. ECDSA)
θ	Threshold value to determine message validity
$\rho()$	Function to map a row from matrix A to an attribute

CHAPTER 1

INTRODUCTION

Without a doubt, electricity is one of the most important blessings in mankind modern life. It powers many of the world's most important innovations, including our telecommunications, underground transportations and healthcare systems. Electricity is generated by what is called power grid that constitutes power generation network of extra-high voltage lines, long-distance transmission networks of high voltage lines and local distribution networks with usable low-voltage lines connected to the customers. In most countries, the power grid is a complex infrastructure with billions of components, hundreds of corporate entities and millions of customers.

Despite being a reliable source of electricity for decades, the traditional power grid is getting obsolete and suffer from many limitations. This power grid exploits fossil fuel-based generation plants that produce high CO₂ emission which contributes negatively to the climate change, thereby increasing the frequency and period of blackouts due to extreme weather (wildfires, floods, freezing rain). For example, in 2019, Pacific Gas and Energy (PG&E) has planned the largest blackout in history that left more than 2 million people without electricity in an effort to fight California wildfires (Newburger, 2019). With the new environmental regulations and restrictions to limit the climate change, using non-renewable power generation sources is no longer efficient or recommended.

In addition, traditional power grid employs one-way power flow from generation plants to customer providing limited mechanisms for monitoring and control. Therefore, human operators are needed to continuously monitor the network and actively gather real-time information describing the state of the power grid. As such, pinpointing faults and outages is extremely challenging due to the cost and geographical consideration. On the customer side, the one-way power flow doesn't promote the customer to effectively monitor and adjust his energy usage.

The cost of renewable energy has fallen significantly in the last decade (Blazquez, Fuentes-Bracamontes, Bollino & Nezamuddin, 2018), yet renewable energy sources such as wind, solar and waterfalls are poorly integrated in the traditional power grid due to many infrastructure constraints. This with the depletion of non-renewable energy sources justifies the continuous rising in retail electricity prices. The traditional grid is assembled in a way that reflects years of additions and build-outs so modifying its structure to accommodate renewable sources of energy is not a straightforward task to do.

In an attempt to overcome the significant limitations aforementioned and accommodate the huge increasing demand on electricity supply competently, pressure has been put forth to transfer the legacy power grid into what is so called “smart” grid. It is a goal and a technology to prepare the current energy infrastructure for the challenges of the forthcoming decades. The U.S. Department of Energy defined the smart grid as “An automated, widely distributed energy delivery network, the Smart Grid will be characterized by a two-way flow of electricity and information and will be capable of monitoring everything from power plants to customer preferences to individual appliances. It incorporates into the grid the benefits of distributed computing and communications to deliver real-time information and enable the near-instantaneous balance of supply and demand at the device level (Duan, & Deconinck, 2010). The smart grid relies on the integration of communication networks to reliably interconnect millions of electrical and communication devices. Thus, the emerging of the Internet of Things (IoT) concept greatly supported the realization of the smart grid. The use of IoT-enabled devices can lead to numerous benefits such as increasing the power system reliability, improving remote monitoring and control tasks and facilitate implementing Advanced Metering Infrastructure (AMI) networks. The smart grid represents an unprecedented opportunity to shift the energy production into a new era of reliability, availability, sustainability and efficiency that will contribute to our economic and environmental wellbeing. The main features that characterize the smart grid are:

- Implementing numerous technologies to achieve two-way power and information flows between the utility and its customers. This is by far the leading smart grid flagship feature that facilitate balancing energy demand and supply;

- Near-optimal integration of renewable energy sources by installing Distributed Energy Resources (DERs), small-scale decentralized structures that are capable of providing power to or storing power from distribution networks. These structures permit customer-based power generation to be integrated into the power grid using units such as solar panels or small wind turbines. Utilizing renewable energy sources can notably decrease the rapid climate change by reducing carbon emission;
- The integration of advanced electricity storage and peak-shaving technologies including advanced storage batteries, Demand Side Management (DSM), Hybrid Electric Vehicles (HEVs) and thermal storage air conditioning;
- Saving in energy by keeping customers informed of their consumption at any time so that they adjust the consumption to meet the real need;
- The deployment of smart technologies (for metering and communication) and the use of smart appliances.

1.1 Smart Grid Architecture

In spite of the similarity between their basic functions, the smart grid utilizes different technologies and achieves a different structure when compared to the legacy grid. The most interesting smart grid architecture is presented in (Komninos, Philippou & Pitsillides, 2014) and is shown in Figure 1.1.

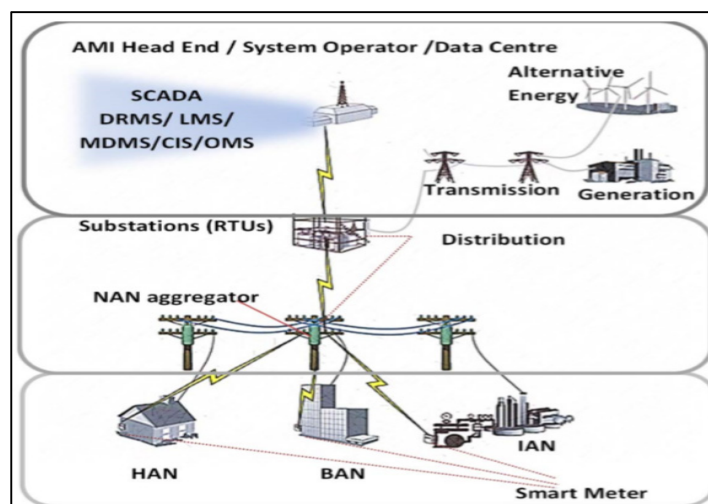


Figure 1.1 Smart grid multi-layer architecture Taken from Komninos et al. (2014)

In this model, the smart grid is logically divided into three stacked layers, with the bottom layer having three networks: Home Area Networks (HANs), Building Area Networks (BANs), and Infrastructure Area Networks (IANs) utilizing short-distance wired and wireless connections in customer premises. These networks span small geographic areas and connect the smart meters and appliances to the grid headend to allow exchanging real-time data and control messages such as consumption readings and energy management commands. This layer plays a vital role in realizing the two-way communication between the utility and the customer. The middle layer contains Neighborhood Area Networks (NANs) and Field Area Networks (FANs) in addition to other units such as Remote Terminal Units (RTUs) and Phasor Measurement Units (PMUs). Networks in this layer are responsible for collecting and aggregating the meters data before forwarding them to the top layer. RTUs transmit telemetry data to the top layer, where PMUs synchronize the grid devices (Ancillotti, Bruno & Conti, 2013). The top layer of this model contains Wide Area Networks (WANs) that delivers the aggregated data from multiple NANs to the utility. The layer also contains two software curial to the operation of the smart grid are found in this layer: Supervisory Control And Data Acquisition (SCADA) and Meter Data Management System (MDMS). SCADA is responsible for data receiving, processing, presentation, and management (Panda, Mishra & Ratha, 2016). Several control commands are issued using this software such as load shedding and demand response. MDMS provides a single repository for processing and storing long-term data delivered by the smart metering system. In addition, distributed generation, distribution and transmission networks are considered part of this layer too (Järventausta, Repo, Rautiainen & Partanen, 2010).

1.2 Advanced Metering Infrastructure (AMI)

In the past, electricity companies used a tedious and inefficient technique to bill their customers by physically reading every customer meter to determine how much energy he was using. If visiting the customer is not possible for some reason, he will be billed based on past or predicted consumption. Derived by the need to improve billing accuracy and reducing the time and cost of reading the meters, a new mechanism called Automatic Meter Reading (AMR) is developed later. AMR is an automated technology that exploits one-way communication

between the utility and customers to collect consumption readings and status data from meters and transferring the collected data to a central database for analyzing and billing (Mahmood, Aamir & Anis, 2008). Despite being an efficient technique to gain meter data remotely, corporates started to look for an alternative to AMR that can better utilize the available communication technologies to bring additional functionalities.

Advanced Metering Infrastructure (AMI) replaced AMR as a new technology that permits the utility to do more than gathering meter readings remotely. It is a hierarchical and functional infrastructure that forms the foundation of the smart grid as it empowers two-way communication between utilities and customers. Typically, AMI embeds AMR functionality through smart meters, yet it implements additional functions and services. Consequently, the metering infrastructure attracted a great attention from electricity providers around the world. (Hisock & Beauvais, 2013). show that by 49% and 87% of the meters used by the Canadian electricity systems were smart by 2013 and 2016 respectively. In 2013, AMI is either deployed or under deployment in Alberta, British Colombia, Ontario, Quebec, Saskatchewan and Nova Scotia electricity systems, where Ontario was one of the first in the world to fully deploy smart meters and AMI throughout its electricity system, with 4.8 million meters deployed and connected to a central management database in utility side.

1.2.1 AMI Programs

From the utility point of view, the best-case scenario in achieving the maximum cost saving is to operate the power plant continuously to supply the needed power but in a way that guarantee the power generated by the generation networks are always sold (Sorebo & Echols, 2011). Given that customers consumption patterns are subject to a high variance and knowing that shutting down the generation facilities during low energy demand to restart them when high demand is encountered leads to a higher cost than running them continuously, the previous best-case scenario was not possible in traditional power grid. However, the introduction of smart grid AMI networks brings additional programs and functionalities that facilitate intelligent and automated responding to customer demand so that both the utility and customers

can cut tremendous part of their cost. In this section, we will briefly explain some smart metering programs (Sorebo & Echols, 2011) that can achieve better overall grid performance.

- 1- *Real-time Remote Meter Reading*. The utility can dynamically collect and analyze consumption readings from smart meters to ensure that consumption is aligned with the base load output from the generation facilities. This will allow the utility to act promptly if consumption and generators load found inconsistent.
- 2- *Demand Response (DR)*. This technique ensures that the customer is dynamically and continuously informed of real energy price, so that he is encouraged to make consumption decisions economically. For example, customer may decide to turn off unnecessary appliances during high tariff (peak) periods.
- 3- *Peak Shaving (PS)*. This program aims to avoid building extra generation plants to handle instantaneous and sudden spike in energy demand. One way of doing this is by drawing energy back from unutilized AMI entities that has energy storage capabilities such as batteries and Electric vehicles (EV) during peak times. Cooperative customers could be offered to charge the storage units at a lower rate during low demand period.
- 4- *Customer Load Profiling (LP)*. This mechanism permits the utility to collect comprehensive information regarding its customers' consumption patterns, in which the profiled information is used to determine the optimal base load that generators should run at.
- 5- *Distributed Generation (DG)*. Smart grid is by no means a centralized energy generation system, rather it supports decentralized power generation through utilizing renewable energy sources deployed in different locations of the grid including customer side. This capability allows qualified customers generate their own electricity and even sell excess generation to reduce their own bills.

It is worth nothing that the aforementioned programs and many more such as detecting power outages and enabling/disabling energy services are enabled thru AMI that implements two-way communication between the utility and consumers.

1.2.2 AMI Architecture

AMI architecture begins at the customer premises and ends at the utility headend. It comprises several components and networks that span the three smart grid layers to implement two-way communication between consumers and utility companies. The main components that build up AMI architecture are the smart meters, data concentrators and MDMS (Rashed Mohassel, Fung, Mohammadi & Raahemifar, 2014) (Finster & Baumgart, 2015). Smart meters (SMs) are solid state devices deployed in customer premises such as homes, offices, or buildings to collect consumption readings from the smart appliances. Primarily, meters are dedicated to perform measurement and communication functions, thus are equipped with metering circuitry to perform energy consumption measurements and a few interfaces to handle communication with other external nodes. Meters are referred to as smart because they enable the utility headend to interact with them from centralized remote sites and perform intelligent automated decisions on behalf of IT or control systems (Albu, Sanduleac & Stanescu, 2017). Data concentrators collect and aggregate real-time data from smart meters before transmitting it to the ultimate destination in utility headend, more specifically to MDMS. Metering data is routed from customer premises towards the utility storage system in hierarchical many-to-one multi-hop style. In HAN, BAN, and IAN, consumer smart appliances propagate their readings to a single smart meter using Power Line Communications (PLCs) or wireless communications such as ZigBee. Similarly, NAN connects a predetermined number of smart meters to one concentrator using WiMAX or cellular technologies. Last mile delivery is done over WAN where a number of concentrators are linked to AMI headend in the utility side.

The AMI components aforementioned relies on additional communication networks such as In-home display and utility WAN. The In-home display is a network segment that enables consumers making prompt decisions regarding their energy consumption by providing them with Internet Protocol (IP) connectivity to their in-home appliances. Utility WAN comprises two interconnected networks namely core and backhaul (Saputro, Akkaya & Uludag, 2012). Core networks utilizes cellular and fiber optics technologies to provide connectivity to the control center using high data rates. Backhaul networks favors low cost flexible technologies such as Cognitive Radio (CR) to provide broadband connections with NAN modules. Apparently, the evolving smart grid depends on comprehensive communication protocols to

1.3.1 AMI Vulnerabilities and Attacks

In this section, we will shed light on the security threats exist in AMI networks by discussing vulnerabilities and attacks in these networks.

1.3.1.1 Vulnerabilities of AMI Information Networks

In information security, vulnerabilities and attacks are two terms used in the context of describing the threats targeting data or network security, thus it's vital to understand difference between these two terms. A vulnerability refers to an inherited weakness in the design, technology or configuration, whereas the attack is an intentional unauthorized action to exploit the vulnerability to breach system security. The severity of a successful attack in AMI networks ranges from invading consumers privacy to complete system shutdown. Vulnerabilities and the associated attacks exist in both AMI power and information networks, however in this thesis we are considering security of information networks solely. In addition, we are considering system threats caused by adversaries rather than the ones raised due to environmental reasons such as natural disasters. Below we summarize the most serious AMI vulnerabilities linked to information networks:

- 1- AMI comprises components that are deployed in an extremely large geographical area, where most of these components are out of utilities properties. Such unattended components are insecure and subject to many physical attacks;
- 2- Two-way communication requires using IP protocols and standards to maintain connectivity between AMI devices. Therefore, devices such as smart meters and data concentrators will be inherently vulnerable to numerous IP-based attacks;
- 3- AMI spans the three smart grid layers with millions of intelligent interconnected multi-vendor devices, where every device corresponds to a possible attack point that can jeopardize the security of the whole AMI network;
- 4- The main AMI functionality is to enable the utility to remotely collect meters readings for billing and profiling purposes. This involves transmitting massive amount of data that include sensitive customers information that if exposed can lead to serious privacy invasion;

- 5- With different privileges, smart grid stakeholders including consumers, utilities, governments, technologies vendors, policy makers, and employees have access to AMI in some way or another. This will open the door wide for terrorists and psychopaths to exploit the infrastructure weaknesses to launch insider attacks. In such situation, if an attack is detected, it will be difficult to determine who is liable;
- 6- There exists an implicit trust between AMI components (Clements & Kirkham, 2010) in a sense that a compromised device can be used maliciously to control the network to behave in an unwanted way.

1.3.1.2 Passive and Active Attacks in AMI Networks

By exploiting one or more of the aforementioned vulnerabilities, the attacker can launch wide set of attacks against AMI components, communication channels or the data exchanged in these networks. Here, we discuss the major security threats targeting metering networks by describing the attack surface and the possible consequences. Figure 1.3 shows the attacks categories classified based on attack methodology into passive and active attacks.

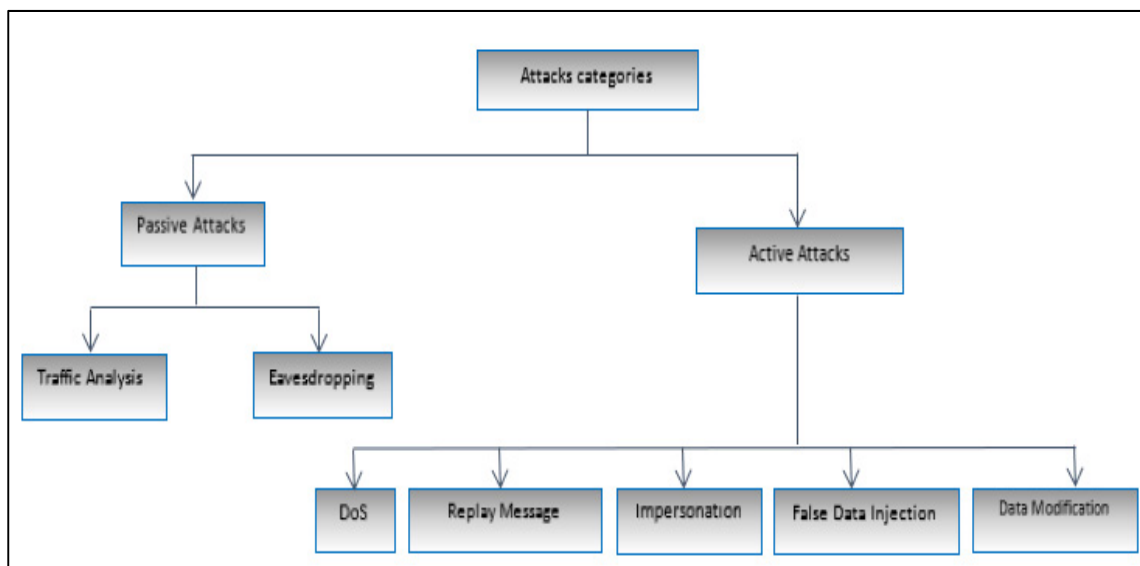


Figure 1.3 Classification of Attacks

Passive Attacks

Eavesdropping and traffic analysis are two passive attacks in which an unauthorized intruder silently listens to the communication channels in order to collect the data being transmitted without the intention to manipulate the data. The data may correspond to control commands issued by the utility headend to a group of meters or metering information reported by customers' smart meter. Eavesdropping is less harmful than traffic analysis in the sense that the attacker has no intention to deduce useful information from the collected data. Therefore, traffic analysis may lead to more serious consequences such as consumption profiling, identity theft, and robbery (Abdullah, Hanapi, Zukarnain & Mohamed 2015). Passive attacks are hard to detect because the legitimate data is not altered, therefore the security measures are put in place to avoid the occurrence of such attacks rather than detecting them.

Active Attacks

Active attacks are a broader range of attacks in which the adversary attempts to disrupt system operation or amend its resources by introducing fraudulent data into the system or corrupting its data. This category of attacks comprises: Denial of Service (DoS), false data injection, data manipulation, replay, and impersonation attacks. Compared to passive attacks, this kind of attacks has more impact on systems performance. Mitigating active attacks focus on detecting and handling mechanisms rather than avoidance. In this section, we discuss the main active attacks associated with metering networks and we demonstrate the impact of such attacks on AMI performance.

DOS Attacks

Denial of Service (DoS) is the attack that threatens data transmission in AMI networks by disabling the availability of communication resources either temporarily or permanently (Lu, Lu, Wang & Wang 2010). Jamming is by far the most known DoS attack in first mile metering networks, where the attacker tries to disrupt the smart meters wireless communication by utilizing different radio signals to interfere with the radio frequencies the smart meters are using. Other DoS attacks include packet flooding (the adversary massively retransmits legitimate network packets to overwhelm the receiver storage capabilities) and packet dropping

(the attacker maliciously drops network packets to deceive the communicating parties of disconnection).

Replay attack

Replay attack occurs when a malicious node captures and stores valid network messages for the purpose of retransmitting them at a later point in time to produce undesirable effect. For example, the attacker may replay utility peak shaving command to force customers reduce their energy consumption. Likewise, a malicious node can replay obsolete appliances consumption readings to the smart meter causing a significant increase in customer's bill. (Alohali, Kifayat, Shi, & Hurst 2016) shows that replay attack can be as serious as DoS in draining AMI network resources under certain circumstances.

Impersonation attack

This attack is carried out when a mischievous node snatches the identity of a legitimate node. In the context of AMI networks, the adversary may steal the identity of an appliance, smart meter, data concentrator or even control center at utility side. For example, an adversary masquerading a legal meter can send consumption reports for the purpose of producing incorrect bills (Kumar et al., 2019). Similarly, a forged data concentrator may collect, drop, or redirect messages exchanged in metering networks causing instable grid performance. The threat of this attack becomes more severe when the number of fake nodes increases leading, to what is so called sybil attack (Najafabadi, Naji, & Mahani, 2013).

False Data Injection attack

In such an attack, the adversary injects falsified data to the network for the purpose of misleading the control center and triggering erroneous responses that can significantly disrupt the grid performance. In particular, there are two ways in which the adversary can conduct false data injection attack. In systems with fragile authentication schemes, the attacker can use his own components to inject falsified codes and data to the networks. Alternatively, in systems with solid authentication protocols, the attacker tries to remotely or physically compromise

legit measuring components before utilizing these components to inject fraudulent measurements to the grid.

False measurements such as fake energy supply or demand messages or incorrect power states will fool control center resulting into serious grid instabilities or even blackouts (Xie, & Sinopoli, 2010). In fact, failing to provide the control center with an accurate estimation regarding the grid state was the main reason that caused the famous 2003 blackout that affected around 50 million customers in US and Canada (Quebec and Ontario) (White et al., 2003). The impact of this attack increases as the number of colluding attackers injecting falsified measurements increases. Therefore, this attack can lead to catastrophic consequences thus it is by far the most serious threat to power grid infrastructure.

Data Manipulation attack

It is the unauthorized action of intercepting, modifying and retransmitting network messages to create undesirable effect on network functionality. The difference between this attack and false data injection attack is the fact that the adversary maliciously modifies valid network messages rather than fabricating new fake messages. Authors in (Khan, McLaughlin, Lavery, David & Sezer, 2018). showed that stealthy data manipulation is injurious to smart grid synchrophasor-based control and monitoring applications.

1.3.2 Problem Overview

Thanks to its' critical architecture, AMI communication channels are subject to numerous attacks that can cripple the bidirectional data exchange between customers' meters and the utility control center. The severity of the attacks varies greatly from exposing customers privacy to disabling AMI functions. For instance, external passive adversaries intercepting on the first mile networks can collect massive amount of customer information that may be analyzed to conduct further malicious actions. Whereas, active adversaries can manipulate network information or inject fake messages to interrupt the functions of AMI programs which leads to significant revenue loss and disruption to human life. Accordingly, enforcing strong and efficient protocols to secure the two-way communications in AMI network is an indispensable requirement.

The fundamental security solutions developed for the enterprise internet are not suitable for the metering networks because AMI has unique communication and architectural characteristics making it distinguished from any other distributed systems. First, AMI networks interconnects millions of resource constrained devices that have limited processing and storage capabilities thus it is infeasible to adapt complex and computation intensive cryptographic algorithms for such devices. Second, the infrastructure of metering networks has long life span compared to other IT systems which requires the security techniques to ensure sufficient security level that survive for long period of time taking into consideration that any upgrade procedure may not be feasible to such large-scale networks. Third, the majority AMI programs require real-time communication with minimum delay and latency. However, deploying security solutions introduces extra overhead that may result in annulling the functionality of these programs. Fourth, in opposite to most distributed systems that possess static interconnections, the implementation of certain AMI functions such as Demand-Response requires the customers to move virtually from one group to another. In order to ensure forward and backward secrecy of groups' information an efficient key management schemes must be deployed. Finally, uplink and downlink transmission flows that build up the two-way communication feature have different security goals. In uplink transmission, consumption information is transmitted from the smart meters to the utility headend. The main security goal for this single-recipient communication is protecting the privacy of consumers' information. On the other hand, downlink transmission propagates information and control information from the utility headend towards a group of smart meters. For this communication, the main security goals are to maintain data integrity and ensure anonymous fine-grained access control mechanism to utility data.

In summary, secure data communication in AMI networks is an indispensable requirement to ensure reliable and efficient power grid operations; however, the unique communication and architectural characteristics of these networks poses great challenges on designing security mechanisms.

1.4 Research Objectives

In this thesis, we aim to improve the dependability of the smart grid metering networks by designing secure cryptographic-based data exchange protocols for the two-way communication in AMI networks. Our main objective is to ensure confidentiality and integrity of messages exchanged between the smart meters and the utility headend over the insecure communication channels. Another principal objective we intend to achieve is the high computational and communication efficiency. We want our security protocols to incur low computation and communication overhead to accommodate the constraints of AMI networks. In the effort of achieving the aforementioned goals, we studied the communication scenarios needed to implement the different AMI programs and functions. We realized that uplink data collection and downlink data communication have different security goals and transmission modes. Consequently, efforts will be geared towards handling each communication pattern independently. For the uplink communication, we intend to design a secure data exchange protocol to preserve customer privacy when reporting energy consumption readings to the utility headend. In order to achieve high computational efficiency, we aim to exploit hybrid encryption that incorporates the efficiency of symmetric cryptography with the security of public-key cryptography (particularly Elliptic Curve Cryptography). The resiliency of the scheme could be improved by considering additional cryptographic functions such as Message Integrity Codes. In order to address the security issues of downlink data transmission, we propose to design a secure communication protocol to provide fine-grained access control for control center messages multicasted to a group of smart meters. The proposed scheme should permit the control center to regularize access to the encrypted data based on certain criteria. Attribute-Based Encryption (ABE) is a promising recent encryption scheme that provides such functionality. However, this encryption technique is not adapted widely due to its high computation complexity. Therefore, we aim to design an efficient ABE that tackles the performance limitation of the traditional ABE schemes. We aim to strengthen the resiliency of the protocol by integrating additional cryptographic function to ensure authenticity of control center messages.

We anticipate that the two cryptographic-based protocols can together offer an integrated security solution that is capable of handling most of the security threats encountered in the two-way data exchange carried on AMI networks.

1.5 Thesis Contribution

In this thesis, there are three major contributions in which other sub-contributions are emerged from. First, we addressed the need for secure data exchange in AMI networks by introducing requirements-driven security schemes. By requirements-driven we mean that the design goals of our schemes are driven from the key security requirements needed to address the major cyber threats targeting the communication. We realized that the two-way communication in AMI networks constitutes uplink single-recipient communication and downlink multi-recipient communication, where each one of them has different transmission modes and security requirements. Preserving customer privacy is the most important security goal for uplink data communication, therefore we designed a new hybrid encryption scheme to protect metering data in while in transit to utility headend. In contrast, enforcing robust access control mechanism for utility messages is the principle security goal for downlink communication. Thus, we proposed a novel Attribute-Based Encryption (ABE) scheme to enable the control center efficiently regularize access to the data. Most of the related work in the literature are goal-oriented, meaning they propose schemes to impose certain security goals without considering the importance of the goal to the underlying communication pattern which makes many of the schemes impractical.

Second, we considered efficiency and security an equally consequential requirements when designing our cryptographic-based data exchange schemes and we focused on balancing these contradicting requirements. Given the resource constraints of the smart devices and the limited shared bandwidth of AMI communication channels, the computational complexity and communication overhead are the main factors that determine the efficiency of security protocols. In fact, we encountered many schemes in the literature that are proven to be secure against many attacks, but in the context of AMI networks they are computationally inefficient. In this regard, the construction of the proposed hybrid encryption scheme utilizes Elliptic Curve Cryptography (ECC) that is known to yield small cryptographic key sizes. Additionally,

we incorporated a precomputation phase to improve the computation speed of our scheme. Similarly, our novel ABE scheme is constructed without using the slow bilinear pairing operation.

Third, we provide security analysis for each one of the proposed schemes to demonstrate its resiliency in mitigating the attacks that jeopardize the data exchange.

1.6 Thesis Outline

The remainder of this thesis is organized as follows. In Chapter 2, we present background information about different public-key cryptosystems followed by illustrating the literature review for several cryptographic-based schemes to secure uplink and downlink communication in AMI networks. In Chapter 3, we propose a hybrid encryption scheme that incorporates elliptic curve cryptography with symmetric key cryptography to achieve a secure single-recipient uplink data exchange in AMI networks. In Chapter 4, we present our initial effort to address multicast communication by proposing a lightweight encryption and signature scheme to secure uplink and downlink communication in AMI networks. In Chapter 5, we present a signcryption scheme that stands on the concept of attribute-based encryption to attain secure multicast downlink communication in AMI networks. In Chapter 6, we conclude the work presented in this thesis and give some directions for future work.

CHAPTER 2

BACKGROUND INFORMATION AND LITERATURE VIEW

This Chapter introduces the literature review on security protocols used to ensure secure two-way communication in AMI networks. Based on the underlying communication model, the related work is classified into single-recipient uplink communication or multiple-recipient downlink data communication. For each one of these two categories, further classification is done based on the underlying cryptosystem. In order to make this chapter self contained and to provide the necessary knowledge needed to understand the rest of it easily, Section 2.1 presents three approaches related to the public-key cryptography approaches; Elliptic Curve Cryptography (ECC) and Pairing-Based Cryptography (PBC) and Paillier cryptosystem.

2.1 Background

This section introduces three security concepts that some of the related work in the next two sections are built upon. As major work of this thesis is built upon the concept of elliptic curve cryptography, Appendix I presents more details about the basic mathematics of elliptic curves.

2.1.1 Elliptic Curve Cryptography (ECC)

Public Key cryptography or Asymmetric key cryptography, is a cryptographic system in which the communicating parties utilize a pair of keys to realize two security features: data encryption and digital signature generation. The pair of keys consists of a public key known to all parties and used for encryption or signature verification and a private key used for decryption or signature generation. Most of the systems and standards that employ public key cryptography use the well-know Rivest–Shamir–Adleman (RSA) algorithm for encryption and digital signatures. In order to retain its secrecy, the key length of RSA algorithms kept increasing over years resulting in increased storage and processing requirements.

Elliptic Curve Cryptography (ECC) was discovered by Victor Miller and Neal Koblitz in 1985 as an alternative approach for implementing public key cryptography (Koblitz, 1987). This

cryptosystem makes use of elliptic curve which is a set of points that satisfy a specific mathematical equation. Elliptic curves are basically defined by an equation with two variables with coefficients where these variables are coefficients are all restricted to elements of a finite field. There exist two types of elliptic curves that is used in the cryptographic applications: **prime curves over $\mathbb{Z}_p$** and **binary curves over $\mathbb{GF}(2^m)$** . Prime curves use cubic functions in which the variables and coefficients are restricted to the set of integers between 0 and $p - 1$ and the calculations are performed *modulo* p . For binary curves, the variables and coefficients are restricted to values in $\mathbb{GF}(2^m)$ and the calculations are performed over $\mathbb{GF}(2^m)$. As pointed out in (Stallings, 2016), prime curves achieve better performance in software application while binary curves are best for hardware applications.

Public key cryptography is powered by trapdoor functions and ECC is not an exception. The trapdoor function that operates this kind of cryptosystems is called elliptic curve discrete logarithmic function. The strength of elliptic curve cryptosystems lies behind the fact that despite more than decades of continuous research, mathematicians still are not able to find an algorithm to solve the *Elliptic Curve Discrete Logarithmic Problem (ECDLP)*. Actually, for numbers of the same size, solving the ECDLP is significantly harder than solving problems associated with other public key cryptosystems such as factoring associated with RSA (Hankerson, Vanstone, & Menezes, 2004). Compared to other public key cryptosystems, ECC achieves smaller key sizes for the same security level and incurs more efficient implementation (Lenstra & Verheul, 2001) and thus has emerged as an attractive cryptosystem for many wireless and mobile environments.

2.1.2 Pairing-Based Cryptography (PBC)

We believe that there is no short easy way to introduce the basic concept of pairing-based cryptography, yet we will try to keep this introductory background as simple as possible. In this section we demonstrate bilinear pairings as the central building block for any pairing-based cryptography. Then we discuss two encryption schemes systems that utilize pairings in their constructions namely Identity-based and attribute-based encryption.

2.1.2.1 Bilinear Pairing

In the context of pairing-based cryptography, pairing is a map between elements of two cyclic additive groups G_1 and G_2 of order q to a destination cyclic multiplicative group G_T of the same order. The pairing is *symmetric* if the same group is used as source groups, otherwise the mapping is *asymmetric*, where both have their use in cryptography. Menezes, Vanstone and Okamoto were the first to introduce the use of pairing in cryptography as tool to solve ECDLP on some elliptic curves (Menezes, Okamoto & Vanstone, 1993). Since then, bilinear pairings have attracted great attention as the only available tool to solve many cryptographic problems such as three-way Diffie Hellman (Joux, 2000). and collision-free broadcast encryption (Boneh, Gentry, & Waters, 2005). In addition, pairings are advantageous in implementing new encryption schemes in modern cryptography such as Identity-Based and attribute-based encryption.

2.1.2.2 Identity-Based Encryption (IBE)

Certificate authority (CA) is a central entity used in many large-scale systems that implement public key cryptography. CA is responsible for issuing digital certificate for the public keys used in encryption and signature generation. Each certificate corresponds to a single user and contains his identifying information and public key along with CA signature. Any party who possesses a certificate can ensure authenticity of the corresponding public key by verifying CA signature on the certificate. Despite being simple, this scheme has many shortcomings in terms of certificates management. Parties rely on certificates to establish secure communication but they may not know how to obtain the certificate of a certain entity. In addition, they may not be able to tell if a public key is still valid (i.e. certificate has not been not revoked).

The notion of identity-based cryptography was introduced first by Adil Shamir (Shamir, 1985). to tackle the difficulties of certificate-based public key cryptosystems. The idea was to allow the users generate public keys based on identifying information such as the Email address or account name. Trusted third party usually referred as Private Key Generator (PKG) is required to generate user's private keys from using the same identifying information and PKG private key. In this implementation, a party can encrypt a message using a certain public key even

before PKG generates the corresponding private one. In addition, IBE allows the public key to be generated using composite identifiers, therefore by including time or date as an identifier the system can control keys revocation. In general, an IBE is composed of the following four randomized algorithms:

- **SETUP** (λ). This algorithm takes the security parameter λ as input and outputs: set of global parameters $param$ (such as message and ciphertext spaces), PKG master secret key SK that will be used to generate user's secret keys based on their identifiers and PKG master public key PK ;
- **EXTRACT** ($param, SK, ID$). This algorithm takes the system global parameter $param$, PKG master secret key SK and user identifier ID and outputs the user secret key k_{ID} ;
- **ENCRYPT** ($param, PK, ID, m$). The encryption algorithm accepts as an input the global system parameter $param$, PKG master public key PK , user identifiers ID , and the message m to produce the ciphertext C ;
- **DECRYPT** ($param, k_{ID}, C$). The decryption algorithm takes the global system parameters $param$, the user secret key k_{ID} and the ciphertext C to recover the corresponding message m .

The first feasible IBE implementation was proposed by Dan Boneh and Matthew Franklin in 2001 (Boneh & Franklin, 2003). They used asymmetric bilinear pairing as the constructors for their scheme. Since then, many schemes based on their IBE have been proposed.

2.1.2.3 Attribute-Based Encryption (ABE)

Traditional public key cryptosystems and the aforementioned identity-based encryption allow a user to decrypt a ciphertext if and only if the ciphertext was generated using his own public key. However, in many real-life scenarios, we may end up in a situation that requires us to encrypt some data and store it in a place (database or cloud) where multiple parties are granted the right to access it. For such scenarios, public key cryptosystems (and even IBE) would require encrypting the data multiple times each with a public key corresponding to a single user, resulting in a poor implementation and performance.

Attribute Based Encryption (ABE) is relatively recent approach introduced first by Sahai and Waters as a Fuzzy Identity-Based Encryption scheme (Sahai & Waters, 2005). The term fuzzy came from the fact that multiple private keys are linked to a single public key in a way that is new to public key cryptography. Despite the name, public keys are constructed from a set of attributes rather than identities. The primary incentive for ABE schemes is to provide encryption and fine grain access control by reconsidering the concept of public key cryptography. In ABE systems, ciphertexts are not encrypted to one particular user as in traditional public key schemes. The motivation behind introducing this scheme was the need to control data access in systems where data users are not known in priori. In such encryption scheme, attributes are a key component in which they are created and managed by an entity called “attribute authority”. In Sahai’s model, the data owner can define access to the data based on a boolean formula defined over a set of attributes. For each user, the attribute authority assigns private key corresponding to the attributes he holds. The data user can decrypt the ciphertext if and only if his private key is associated with attributes that satisfy the boolean formula chosen by the data owner. Bethencourt et al. (Bethencourt, Sahai, & Waters, 2007). proposed Ciphertext-Policy Attribute Based Encryption (CP-ABE) as a new ABE scheme that permits more expressive access policies over attributes to build the ciphertext. The data user is assigned multiple keys, one for each attribute he owns. Still, the data user can decrypt the ciphertext if the owns a set of keys corresponding to attributes that satisfy the access policy. (Lewko & Waters, 2011) proposed a CP-ABE that supports the existence of multiple independent authorities in which users’ private keys are linked to the authority issued them. Key Policy Attribute Based Encryption (KP-ABE) (Goyal, Pandey, Sahai, & Waters, 2006) is the dual of CP-ABE in which the ciphertext is labeled with set of attributes and the users private keys are associated with the access structure. CP-ABE is more convenient in many real-world scenarios as normally users are defined with the attributes. Practically, CP-ABE schemes consist of the following algorithms:

- 1- **SYSTEM SETUP** (λ). This algorithm takes a security parameter λ as an input and output the global system parameters $param$ required by the ABE system;
- 2- **AUTHORITY SETUP** ($param$) $\rightarrow k_x, k_y$. This is a randomized algorithm run by attribute authority to generate it’s public/private key pair. The public key is shared with

other system entities while the secret key is kept secret. Additionally, a public/private key pair is generated for each attribute in the attribute universe;

- 3- **ENCRYPT** ($param, m, A, k_x$) $\rightarrow CT$. This randomized algorithm run by data owner to generate the ciphertext CT . The algorithm takes as input the global parameters $param$, the message to be encrypted m , access policy A defined over a set of attributes and authority public key k_x ;
- 4- **KEY GENERATION** ($param, ID, i, k_y$) $\rightarrow SK_i$. The attribute authority runs this algorithm to generate a private decryption key corresponding to attribute i owned by the user identified as ID;
- 5- **DECRYPT** ($param, CT, \{SK_i\}$). A user with a set of attributes that satisfy the access policy use this algorithm with the corresponding secret keys $\{SK_i\}$ to decrypt the ciphertext CT and recover the message m .

The majority of ABE schemes (CP-ABE and KP-ABE) are constructed using bilinear pairing operations. As we will discuss in Chapter5, such pairing operations incurs high computation overhead. This will hinder utilizing such ABE schemes in many applications that have strict processing time requirements.

2.1.3 The Paillier Cryptosystem

It is a public-key cryptography approach that was first introduced by Pascal Paillier in 1999 (Paillier 1999). The security of Paillier encryption scheme is derived from an assumption related to the hardness of factoring. For this cryptosystem, the encryption scheme uses a multiplicative group of elements in the range $\{1, \dots, N\}$ that are relatively prime to N , that is a product of two large distinct primes. Being an additive homomorphic cryptosystem, the most interesting feature of this cryptosystem is the support of Homomorphic encryption. This sort of encryption permits computation on ciphertexts resulting in an encrypted result that when decrypted matches the results of the operations as if performed on the plaintexts. This feature is highly desirable in some settings where at some point it is important to perform some operations on the ciphertext without revealing the content of the ciphertexts. For example, a gateway may need to aggregate multiple encrypted packets without revealing their content. For

this reason, homomorphic encryption is attracting great attention for privacy preserving applications.

2.2 Literature Review

This section sheds lights on the different security schemes proposed to achieve secure communication in AMI networks. In section 2.2.1, we present the schemes that support single-recipient uplink communication. Section 2.2.2 surveys the schemes designed to secure multi-recipient downlink communication.

2.2.1 Security Schemes for Uplink Data Communication

This section is dedicated to present few cryptographic-based approaches to achieve secure unicast communication in AMI networks.

2.2.1.1 Schemes Based on Secret Key Encryption

Very few schemes suggested using symmetric key cryptography to secure downlink communications in AMI networks due to the high management overhead for maintaining secret keys.

In (Bartoli et al., 2010), a secure data aggregation scheme for delivering metering information is proposed. The protocol adopts tree-based network connectivity where the leaves (smart meters) report their data to the root node (gateway) for aggregation. The scheme achieves secure data collection by employing end-end and hop-hop security schemes. For this purpose, a secret key is shared between the root nodes and every leaf node. In addition, a pairwise key is maintained by every one-hop pair of smart meters. The major limitation of this scheme is the high management cost of shared keys in addition to the need for key revocation strategy which is missing.

A dynamic secret-based encryption scheme between the utility and smart meters is presented in (Liu et al., 2014). Sender and receiver synchronously and continuously monitor packets loss

and retransmissions in the link layer in order to build a Retransmission sequence (RS) that is used to update the secret key. Every retransmitted packet is coded as 1 in RS, whereas a non-retransmitted packet is coded as 0. When RS reaches a predetermined length, it is used to update the shared secret using simple bitwise *xor* operation. Authors prove that errors in link layer are inevitable and demonstrate that it is very difficult for the adversary to obtain correct RS by simply eavesdropping on the communication channel. Despite being a lightweight protocol, it is by no means a scalable solution.

(Li, Lu, Zhou, Yang & Shen, 2014) proposed an authentication scheme based on Merkle-Tree hashing for Home Area Networks. The proposal exploits Merkle hashing by constructing a binary tree where the utility is considered the root and smart meters as the leaves. Smart meters are authenticated using their hash codes and the Authentication Path Information (APIs). HAN gateway creates a database to store the smart meters IDs in addition to set of hashes information that helps to associate the origin of the messages received. When a smart meter generates an electricity consumption report, it attaches the identification and authentication information to the report and encrypts it. Upon receiving it, the gateway checks if the report is being maliciously replayed or altered in transit and authenticates its origin. In spite of being resilient against analysis, replay, message injection and message modification attacks the proposed technique is able to sign limited number of messages.

2.2.1.2 Schemes Based on Elliptic Curve Encryption

(Mahmood et al., 2018) proposed an elliptic curve cryptography based lightweight authentication scheme for smart grid communication. The protocol runs in three phases: initialization, device registration and authentication. In the initialization phase, the Trusted Third Party (TTP) computes own private key and generates the global system parameters. Afterwards, the smart grid device registers with TTP to obtain a pair of public and private keys. In the authentication phase, a pair of AMI devices utilize ECC and one-way hashing functions to mutually authenticate each other. Once authenticated, the devices can communicate securely. The proposed scheme achieves perfect forward secrecy and guards against replay, man-in-the middle, impersonation, and privileged insider attack.

A lightweight authentication and key agreement to attain authentication, anonymity, and integrity in smart metering networks is proposed in (Kumar, Gurtov, Sain, Martin & Ha, 2019). The protocol supports hierarchical energy network where HAN meters are connected to a NAN gateway that in turn is connected to the utility server. The scheme exploits ECC, MAC, and hashing to achieve mutual authentication and key establishment between the smart meters and gateways. Moreover, it utilizes symmetric cryptography to ensure confidentiality of metering messages. Pseudonymity is used to improve customer privacy and guard against identity spoofing. The authors prove that their scheme is resilient against replay, impersonation and Man-in-the-Middle attacks.

A work that is very similar to the aforementioned one is presented in (Garg, Kaur, Kaddoum, Rodrigues & Guizani, 2020). Utilizing the features of Fully Hashed Menezes-Qu-Vanstone (FHMV) and ECC, the scheme achieves mutual authentication, confidentiality, and integrity in smart metering infrastructure.

2.2.1.3 Schemes Based on Identity-Based Encryption

(Wang, 2017) proposed an identity-based data aggregation protocol to ensure the privacy of customer fine-grained power usage data. A Private Key Generation (PKG) is used to initialize the private keys of smart devices, collectors and Energy Service Provider (ESP). Whenever data is requested by the collector, the smart devices encrypt their metering readings using a random number, sign it and forward it to the collector. The collector in turn constructs the total electricity data by aggregating the smart devices ciphertexts and forwards the data signed with his private key to ESP. The proposed protocol is resilient against man-in-the-middle, external, internal and replay attacks but incurs high computation cost due to the use of bilinear pairing operations.

A zero-configuration Identity-based Signcryption scheme for end-to-end communication in the Advanced Metering Infrastructure (AMI) networks is presented in (So, Kwok, Lam, & L, 2010). The scheme utilizes Boneh-Franklin Identity-Based encryption (IBE) scheme (Boneh & Franklin, 2001) for encryption and the Identity-Based Signature (IBS) scheme proposed in

(Hess, 2002) for authenticating AMI data packets. The proposal has two phases of operation: registration phase and data transmission phase. In the registration phase, every smart device uses a pair of device-registration keys embedded into the device during the manufacturing process to register with Key Generation Server (KGS) to obtain a secret key that will be used subsequently to communicate with other AMI devices. In the transmission phase, the sender encrypts the data using the receiver's public key that is derived from his identifying information without the need for further setup. A key caching mechanism is incorporated into the scheme to minimize its computation cost by reducing the number of Tate-pairing calculations for needed for every packet.

An efficient privacy-preserving scheme to thwart privacy leakage attacks in smart grid specifically metering networks is proposed by (Farrag, 2017). The network model comprises HAN, BAN, and NAN networks with distinct gateways supporting each one. The proposed technique achieves data and gateway privacy by utilizing bilinear pairing Identity-Based Encryption scheme with updating certificates strategy. The protocol operates in four phases: gateways initialization, party registration, privacy preserving energy consumption, and updating certificates. The author proves that the scheme is robust against several attacks such as replay, man-in-the-middle and Sybil, however it possesses weak performance against collusion attack.

(Soykan, Ersoz & Soykan 2017) proposed a signcryption scheme to secure the unicast communication between the smart meters and the Data Management Center (DMC) at the utility side. The scheme incorporates symmetric encryption with bilinear pairing to construct the Identity- Based signcryption scheme. The authors argue that their scheme achieves data confidentiality, authentication, integrity and non-repudiation. They haven't shown the potential improvements gained by combining secret key cryptography with pairing over traditional IBE schemes.

2.2.1.4 Schemes Based on Homomorphic Encryption

(Rug & Nayyak, 2013) a secure smart grid communication framework that provides access control and privacy preserving data aggregation based on Paillier cryptosystem Attribute-Based

Encryption. In order to retain customer privacy, each smart meter encrypts the metering information using Paillier cryptosystem. The smart meter specifies the entities entitled to access the ciphertext by attaching a set of attributes to the ciphertext before sending it to the corresponding gateway. Based on the received attributes, the gateway in turns aggregates the collected metering data before sending it to the Remote Terminal Units (RTUs) at the utility side.

An end-to-end security scheme to ensure the privacy and integrity of aggregated data based on homomorphic encryption and signature is proposed in (Li & Luo, 2012). In the proposed scheme, an aggregation tree is constructed from all the smart meters on the neighbourhood where the collector being the root of the tree. Every smart meter aggregates his data to the data collected from its children before sending it towards the collector. Along with the aggregation process, homomorphic signature based on paillier cryptosystem is generated on every intermediate smart meter on path towards the collector.

SEDA (Ni, Alharbi, Lin & Shen, 2015), a security-enhanced data aggregation scheme for metering data collection in smart grid networks. The proposal ensures data confidentiality and integrity by incorporating trapdoor hash functions (Shamir & Tauman, 2001), Paillier cryptosystem and homomorphic authenticators (Shacham & Waters, 2008). The scheme guards against malicious aggregators as gateways aggregate the ciphertexts of the reports received from many residential users without be able to disclose the metering content. The operation center obtains the sum of power usage by decrypting the aggregated ciphertexts received from the gateways. The proposal incurs low computation and communication overhead as it is capable of aggregating ciphertexts, signatures and authentication responses simultaneously.

Authors in (Fan, Huang & Lai, 2014) proposed a secure metering information collection that is resilient against internal attacks. The scheme prevents electricity suppliers from getting individual metering information, rather they can obtain consumption reports for a group of users to infer the total energy consumption. This is achieved by giving every user a blinding factor that is used during the homomorphic encryption process. The blinding factor forces the utility suppliers to process all aggregated ciphertexts to obtain the total consumption.

In (Li, Xue, Yang & Hong, 2018), the authors proposed PPMA, a privacy preserving multi-subset data aggregation scheme. Different from the aforementioned techniques, the scheme allows the aggregation of user consumption data of different ranges. The users are classified into different subsets and a single aggregated data per subset is generated. The proposed scheme utilizes homomorphic encryption based on Paillier cryptosystem with two super-increasing sequences to realize multi-subset aggregation.

2.2.2 Security Schemes for Downlink Data Communication

In this section, we illustrate the cryptographic-based schemes employed to ensure secure multi-recipient downlink communications in AMI networks. The schemes are based on group key management or attribute-based encryption.

2.2.2.1 Schemes Based on Group Key Management

Liu et al., (Liu, Chen, Zhu, Zhang & He , 2013) classified the messages exchanged in AMI networks based on the transmission modes and presented a centralized key management technique to accommodate each mode. The utility generates symmetric keys, group keys and cryptographic parameters and distributes them to the smart meters through secure channel. Accordingly, the meters generate a session key for broadcast encryption, a session key for unicast encryption and session key(s) for multicast encryption. The proposal ensures data confidentiality and integrity with low computation overhead. The scheme requires perfect synchronization between the parties and lacks scalability.

A scalable end-end security for AMI networks is proposed in (Nabeel, Ding, Seo & Bertino, 2015). The proposal is designed to provide a key management scheme to achieve secure end-to-end communication in AMI. The model is based on using weak Physically Unclonable Functions (PUFs) as a security primitive to provide strong hardware-based authentication for smart meters and collectors. Due to the fact that PUF responses are never stored anywhere, Pedersen commitment and Zero-knowledge proof of knowledge schemes are used by smart meters to commit to their values. In order to support broadcast and multicast communications,

the proposal utilizes Broadcast Group Key Management (BGKM) (Shang, Nabeel, Paci & Bertino, 2010) scheme.

An efficient and Scalable multi-group key management protocol for AMI named eSKAMI is proposed in (Benmalek & Challal, 2015). The proposal is built to support the management of DR projects, where every node has to subscribe to at least one mandatory DR project. Every smart meter obtains a key from the MDMS that is used for encryption or deriving the multi-group keys. logical key hierarchy tree is used to model the structure of multi-group keys. The main contribution of this protocol is the sharing of group keys between multiple DR projects. In this case, if a device is subscribed to multiple DR projects it will only need to hold the group key corresponding to the last subscription.

The authors in (Kim & Choi, 2012) proposed an efficient and versatile key management protocol for secure smart grid communication. A binary tree is utilized to manage the secret keys for secure unicast, multicast, and broadcast communications. The secret broadcast key that is known to all communication parties is used for broadcast encryption, whereas a secret key that is shared only between DR project members is used to secure unicast and multicast communications. The proposed scheme incurs high revocation cost whenever a node is compromised or leave the broadcast domain.

2.2.2.2 Schemes Based on Pairing Based Cryptography

Hierarchical Identity-Based Signature Scheme for AMI downlink transmission named HIBaSS is proposed in (Ye, Qian & Hu, 2015). The scheme aims to ensure data integrity and sender authentication for two types of downlink traffic. Type I is the downlink traffic from utility concentrator to Data Aggregate Point (DAP) which carries control information. Type II is the downlink traffic from DAP to smart meters which carries information to customers. Type I is signed by an authentication server (AS), whereas union of DAPs signs type II messages with a group signature. The scheme utilizes symmetric bilinear pairing to construct the Identity-based signature model.

(Hu et al., 2018) proposed a Ciphertext-Policy Attribute Based Signcryption (CP-ABSC) to secure multicast communication in smart grids. The scheme ensures the security of broadcast commands to a group of smart meters (push-based multicast) and retrieval of data from repository (pull-based multicast). The scheme adapts Shamir's secret sharing (Shamir 1979) scheme and the threshold-based access tree structure to construct the access policy. The main difference between this scheme and the traditional ABE schemes is the use of bitwise *xor* operation to blind the plaintext. Yet, it still employs bilinear pairing to construct the underlying signcryption scheme. The authors showed that the proposed CP-ABSC resists integrity, authenticity and collision attacks. However, when compared with the basic CP-ABE, the proposed CP-ABSC achieves higher computation cost to perform designcryption.

A recent multi-authority attribute based signcryption scheme to ensure confidentiality, authenticity and non-repudiation for downlink communication in the smart grid networks is proposed in (Alsharif, Shafee, Nabil, Mahmoud & Almasmary, 2019). It is a CP-ABE that is based on Linear Secret Sharing and matrix access policy, yet it incorporates signer identity attribute to the monotone boolean formula to generate the signcrypted text. The grid user can obtain a valid message if: he owns the verification key required to authenticate the signer and possess the non-revoked attributes that satisfy the access policy. Authors showed that their scheme is resilient against collusion attack and signature forgery.

Liu et al., proposed MAAC-AR (Liu, Li, Yang & Yang, 2014), a multi-authority access control with attribute revocation in smart grid. The protocol utilizes symmetric encryption and pairing-based CP-ABE to realize secure and fine-grained access control for the downlink communication between the control center and the energy market. In this scheme, control center aggregates the smart meters readings and encrypts them using CP-ABE based on Linear Secret Sharing Scheme (LSSS) matrix. Legal market interested in electricity data can obtain a decryption token from a Third Party Auditor (TPA) if and only if it possesses the attributes that satisfy the access policy embedded in the ciphertext. Without the token, the market will never be able to compute the secret key required to decipher the encrypted electricity data. MAAC-AR supports attribute revocation and has the strength to thwart collision attack.

CHAPTER 3

HE-SSRU: A HYBRID ENCRYPTION SECURE SIGLE-RECIPIENT UPLINK COMMUNICATION SCHEME FOR AMI NETWORKS¹

3.1 Overview

Smart meters are deployed in customer's premises to collect energy consumption readings and communicate the information over uplink channels to the utility control center. Due to the inherited power grid characteristics and the integration of Information and Communication Technologies (ICT), metering networks are subject to numerous security threats. Therefore, the security of the fine-grained smart meters data is crucial for achieving accurate customer billing and maintaining balanced grid operation.

In this Chapter, a secure communication scheme for single-recipient uplink communication in AMI networks is proposed. The proposed scheme aims to provide an efficient technique to ensure the privacy and integrity of smart metering information while in transit to the utility control center. Given the resource constraints of the metering devices and the limited channels bandwidth, the proposed security scheme has been designed to be lightweight by imposing low computation, communication and storage requirements.

3.2 Mechanism Description and Design Goals

The proposed scheme ensures metering data confidentiality and integrity by considering the concept of Hybrid Cryptosystems (HC). In such cryptosystems, two modes of encryptions are utilized to combine the strength of public key cryptography with the efficiency of symmetric Cryptography. HC is composed of two subsystems namely: data encapsulation and key encapsulation systems. Data encapsulation system is a symmetric key cryptosystem, where the

¹ The work presented in this chapter has been already published in (Khasawneh et al. 2018). Some of the figures, tables, and pseudocodes are taken from the previously published paper.

plaintext is encrypted with an arbitrary key using one of the symmetric encryption algorithms. On the other hand, key encapsulation system is a public key cryptosystem that is used to encrypt the arbitrary secret key using one of the asymmetric encryption algorithms. The secure message is formed by merging the results of the two encapsulation systems to form what is so called a digital envelop. The receiver of the digital envelop will use asymmetric decryption to recover the secret key that will be used to recover the plaintext. In particular, HC is public key cryptosystems that inherits the efficiency of the symmetric cryptography with the security of the public key cryptography. Figure 3.1 shows high level description of the hybrid cryptosystems.

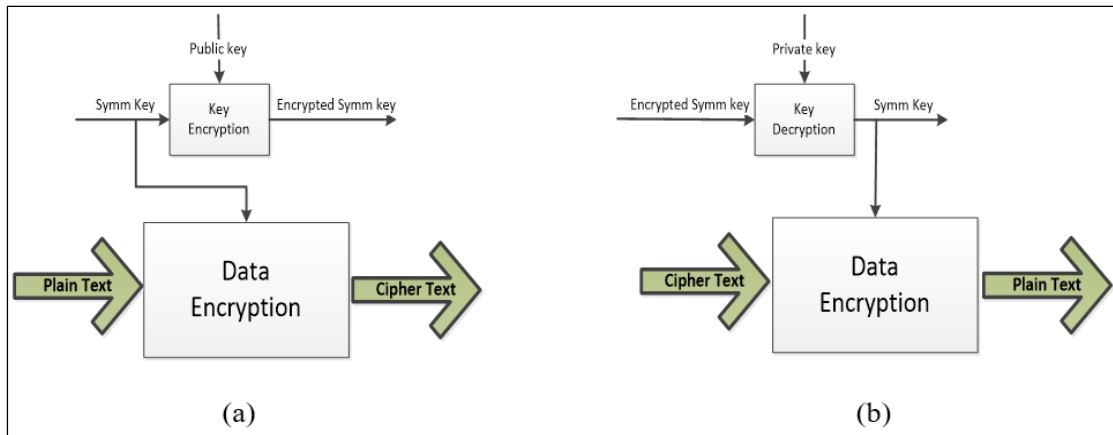


Figure 3.1: The structure of hybrid cryptosystem. (a) Encryption. (b) Decryption

Smart meters are solid state devices that are equipped with limited processing and storage capabilities. In addition, the meters utilize communication channels with low bandwidth. Consequently, the encryption algorithms for data and key encapsulation systems must be designed appropriately to achieve the desired security level without having the performance of metering networks degraded. In our scheme, we will use Advance Encryption standard (AES) for the data encapsulation system and Elliptic Curve Integrated Encryption Scheme (ECIES) for the key encapsulation system. AES is used in most of US federal government organization, has different key sizes, and is known to be efficient in hardware and software. ECIES is used instead of the well-known RSA algorithm because elliptic curve encryption appears to offer equal security with smaller key sizes (Lenstra, 2001).

The main design goals of the proposed protocol are:

- Maintaining the integrity and confidentiality of the smart metering information with high efficiency by combining the strength of public key cryptography with the speed of private key cryptography;
- Providing an efficient and lightweight mechanism to setup the cryptographic keys and parameters between the smart meters and the gateways that will route the meters' data to the final mile networks;
- Optimizing the performance of the hybrid cryptosystem by designing low overhead data and key encapsulation systems that accommodate the meters' limited hardware capabilities;
- Mitigating the critical threats that can cripple the performance of the smart metering functions such as replay, data modification, and spoofing attacks.

3.3 Preliminaries

3.3.1 Elliptic Curve Cryptography (ECC)

ECC is a branch of public-key cryptography that utilizes certain mathematical curves called elliptic curves to construct numerous cryptosystems for encryption, digital signature, pseudo-random generations, and key sharing schemes. ECC is no longer a new scheme as it is showing up in many standards such as IEEE P1363. In opposite to other public-key cryptography schemes that use integer or polynomial arithmetic, ECC uses elliptic curve arithmetic over different fields. The most interesting feature of ECC-based cryptosystems is that they can achieve the same security level of other public-key cryptosystems, such as RSA but with much shorter size of cryptographic parameters. Table 3.1 shows a comparison between the key sizes required to achieve the same security level for different cryptographic approaches. By the same security level, we mean the same computational overhead for cryptanalysis.

In general, ECC has the following advantages over other public-key schemes:

- Utilizes smaller size keys and results in smaller size ciphertext and signatures;

- Supports faster key generation;
- Requires less computational hardware resources such as CPU cycles and memory capacity.

Table 3.1 The size of cryptographic parameters to achieve the same security level

Symmetric key Algorithms	DH-DSA	RSA (size of n in bits)	ECC (modules size in bits)
80	L = 1024 N = 160	1024	160-223
112	L = 2048 N = 224	2048	224-255
128	L = 3072 N = 256	3072	256-383
192	L = 7680 N = 384	7680	384-511
256	L = 15360 N = 512	15360	512+

3.3.2 Elliptic Curve Discrete Logarithmic Problem (ECDLP) and Keys Generation

(ECDLP): Let E be an elliptic curve defined over the finite field $\mathbb{F}_q$. Suppose $P \in E(\mathbb{F}_q)$ be the generator (base point) of order n and $Q \in E(\mathbb{F}_q)$ a point on the curve such that $Q \in \langle G \rangle$. Find x such that $Q = x.P$.

The discrete logarithm problem for elliptic curves requires that it should be computationally easy to compute Q given x and P ; however, it should be very hard to determine x given P and Q . The security of the of ECC is based upon the hardness of solving the Elliptic Curve Discrete Logarithmic Problem (ECDLP). There are no general purpose subexponential time algorithm for solving ECDLP given that the elliptic groups are chosen suitably (Katz and Lindell, 2014). This implies that elliptic curve-based cryptosystems can achieve smaller cryptographic operands compared to other public key cryptosystems.

For the elliptic curve $E(\mathbb{F}_q)$ and point $G \in E(\mathbb{F}_q)$ of prime order n , then the cyclic subgroup of $E(\mathbb{F}_q)$ generated by G is given by:

$$\langle G \rangle = \{O, G, 2G, 3G, \dots, (n-1)G\} \quad (3.1)$$

Utilizing elliptic curves to construct public and private key pair is quite easy and fast. The procedure is depicted in Algorithm 3.1. x represents the private key that is kept secret while P is the public key that is shared with the other nodes to enable them construct an encrypted message.

Algorithm 3.1 Cryptographic keys generation using elliptic curves

INPUT: Elliptic curve domain parameters (E, q, G, n)
OUTPUT: Public-private key pair

1. Randomly pick $x \in [1, q - 1]$
2. Compute $P = x \cdot G$
3. Output (x, P)

3.3.3 The Road to Elliptic Curve Integrated Encryption Scheme (ECIES)

Several elliptic curve-based encryption algorithms have been analyzed in the literature. They all utilize the same arithmetic to generate a ciphertext corresponds to a given plaintext. However, the algorithms have different hardware requirements which can give a preference for one algorithm over another since we are dealing with resource constrained AMI devices. In this section, we will evaluate three elliptic curve encryption algorithms to show the motivation behind choosing ECIES as a building block in our proposed hybrid cryptosystem.

Scheme 1: Encode-then-Encrypt:

This scheme is presented in (Stallings, 2011) and is considered the simplest yet the least secure encryption scheme. The first step to encrypt a message using this scheme is to encode the message into an elliptic curve point. By encoding we mean that the plaintext (or part of it) is represented as an (x, y) coordinates of a point in the elliptic curve. Once the plaintext is encoded into a point P_m , the ciphertext C_m could be calculated using (3.2).

$$C_m = \{C_1, C_2\} = \{kG, P_m + kP_B\} \quad (3.2)$$

Where, G : is the curve generator, k : is a random integer $\in Z_q$, P_B : receiver public key

The plaintext could be recovered by decrypting C_2 , however, the value of k is generated randomly at the sender side and it is not known to the receiver. For this reason, the ciphertext

is sent as two components: C_1 that is used to recover k and C_2 that will be used afterwards to recover the plaintext. The ciphertext is decrypted using (3.3).

$$P_m + kP_B - n_B(kG) \quad (3.3)$$

Where, n_B receiver private key.

This encryption technique requires an encoding strategy, so that both parties obtain correct text to point mapping. One way to do this is to construct a lookup table that stores all encoding possibilities. However, for the resource constrained AMI devices, such table can introduce considerable storage overhead. For example, if the size of the plaintext is 32Kbyte, the lookup table needs to store 2^{18} entry in the lookup table. The size of each entry depends on the elliptic curve characteristics. For example assume the recommended curve “secp112r1” presented in (Certicom Research, 2010), where the size of modulus parameter, x -coordinate, and y -coordinate is 112 bits each. The size of the lookup table will be :

$$= \underbrace{2^{18}}_{\text{No. of entries}} * \underbrace{(18 + 224)}_{\text{input size in bits + bits to represent } x-y \text{ coordinates}}$$

$$= 7.5625 \text{ MByte}$$

Therefore, the lookup table requires very large storage and this will greatly diminish the efficiency of the scheme. We tried to tackle this drawback by splitting the plaintext string into smaller substrings, each substring will be mapped to an elliptic curve point as shown below.

$$\underbrace{100001}_{(x_1, y_1)} / \underbrace{000001}_{(x_2, y_2)} \dots \dots \dots \underbrace{111111}_{(x_n, y_n)}$$

Although this technique can reduce the storage requirement of the lookup table considerably, the substring length must be chosen appropriately. In order to apply this technique, we need to determine the number of points on the elliptic curve, because the number of permutations

produced by substrings should not be larger than the number of points in the elliptic curve. The formula given in (3.4) determine the correct choices of the substring length.

$$l \leq \lfloor \log_2 E_q(a, b) \rfloor \quad (3.4)$$

Due to the fact that there is no mathematical formula that determines the exact number of points in the elliptic curve, we developed a C# software to calculate the number of points on the elliptic curve and accordingly determine the optimal choice for the substrings length. The interface of the application is shown in Figure 3.2.

Lets now recalculate the size of the lookup table assuming the length of the substring is l and for the same recommended elliptic curve (secp112r1):

$$\begin{aligned} &= 2^l * (l + (2 * \text{size of field prime})) \\ &= 2^l * (l + 224) \end{aligned}$$

As this curve has very large number of points, choosing $l = 8$ (for byte strings) will definitely satisfies (3.4) and the corresponding lookup table size will be:

$$\begin{aligned} &= 2^8 * (8 + 224) \\ &= 7.25 \text{ Kbyte} \end{aligned}$$

The reduced size of the lookup table is considered acceptable even for devices with limited storage capabilities such as the smart maters. However, there is another factor that must be taken into consideration which is the communication overhead. In cryptography, the communication overhead is the extra bits that are added to the original message to secure it before the transmission. For the hybrid cryptosystem shown in Figure 3.1, the extra bits that are added to the message represent the encrypted arbitrary key. In order to blind the arbitrary key using Encode-then-Encrypt scheme, the following actions are taken:

Figure 3.2: Elliptic curve points calculator

- 1-Divide the arbitrary key into substrings of length l ;
- 2-Represent each substring as an elliptic curve point;
- 3-For each point generated in step 2, obtain the corresponding ciphertext based on (3.2);
- 4-In order to optimize the size of the result, keep one copy of C_1 only, since all key substrings will have the same value for C_1 .

In order to encrypt $1KByte$ plaintext using Encode-then-Encrypt, we have to use symmetric encryption algorithm to encrypt the plaintext using the key k_{sym} , and then we will use Encode-then-Encrypt to encrypt k_{sym} . Assume we used AES algorithm to encrypt the plaintext, k_{sym} is encrypted using the elliptic curve-based Encode-then-Encrypt algorithm according to the steps explained earlier. The communication overhead is calculated as:

$$= \frac{\text{key size}}{l} * (2 * \text{coordinate length in bits})$$

For 128bits AES, $l = 1\text{byte}$ and the elliptic curve “secp192k1”, the communication overhead will be:

$$= \frac{128}{8} * (384) = 0.75KByte$$

The resulting communication overhead is huge. In fact, RSA that is known to add considerable overhead to sign messages (a minimum of 1024 bits) achieves much better performance in terms on communication overhead.

In summary, elliptic curve encryption based on Encode-then-Encrypt scheme requires mapping tables to store bits to points mapping. Such lookup tables incur large storage requirement. We were able to enhance the storage requirement by partitioning the key into smaller-size substrings. Although the partitioning technique improves the storage requirement, it introduces considerable communication overhead. For these reasons, Encode-then-Encrypt incurs poor performance in terms of storage and communication overhead making this scheme infeasible for AMI networks.

Scheme 2: Encoding-Free Hashed ElGamal Elliptic Curve Encryption:

Another elliptic curve encryption algorithm is analyzed in (Abdalla, Bellare, & Rogaway, 2001). In opposite to the previous scheme this algorithm does not require encoding, which means that the plaintext is encrypted without mapping it to a point on the elliptic curve. Symmetric encryption algorithm is used to encrypt the plaintext using a key generated by a Key Derivation Function (KDF). The input to the KDF is a point on the curve calculated by multiplying the generator by a random integer. Suppose that Alice wants to send an encrypted text to Bob using the Hashed ElGamal Elliptic Curve Encryption, Alice needs to know Bob's public key P to generate the encrypted message.

Bob: Key Generation

1. Pick a private value $\alpha \in [1, n - 1]$ and compute the public key $P = \alpha G$.
2. Broadcast P to all parties.

Alice: Encrypting a message to Bob

1. Choose a random integer $r \in [1, n - 1]$ and compute $Q = r G$.
2. Generate the symmetric key k such that $k = KDF(r P)$.
3. Encrypt the message $M' = SYMM_ENC_k(M)$.
4. The ciphertext is (Q, M') .

Where, G : curve generator of order n , $SYMM_ENC$: symmetric encryption algorithm

The ciphertext generated using this scheme is not M' only because the receiver needs extra information to recover the encryption key k (encryption key is the same as decryption key). The receiver will use Q and his private key α to recover the encryption key k as

$$k = KDF(\alpha Q) \quad (3.6)$$

The plaintext is obtained by decrypting M' using k . The size of the ciphertext is determined by the size of the plaintext and the choice of the elliptic curve.

The storage overhead of this scheme is very small compared to Encode-then-Encrypt described earlier since it does not require a lookup table to encode the message. The information that need to be stored to recover the ciphertext is the private key α . Furthermore, the communication overhead of this scheme is small as well. In order to integrate this algorithm in our hybrid encryption scheme, key encapsulation is done using ElGamal hashed elliptic curve. In this case, the communication overhead is Q in addition to the encrypted secret key. The main limitation of this encryption algorithm is the lack of support to authentication services.

Scheme 3: Elliptic Curve Integrated Encryption Scheme (ECIES):

ECIES is an elliptic curve encryption algorithm that is part of the ANSI X9.63 standard (Accredited Standards Committee X9, 2001). This scheme is very similar to ElGamal hashed elliptic curve, except for the addition of message authentication functionalities. Integrating authentication codes can protect against integrity and authenticity violations. Given the receivers' public key P , the encryption procedure in ECIES is shown under.

1. Choose a random integer $r \in [1, n - 1]$ and compute $Q = r G$.
2. Generate the symmetric keys $(k_a, k_b) = KDF(r P)$.
3. Encrypt the message, $M' = SYMM_{ENC_{k_a}}(M)$.
4. Attach the authentication code, $AUTH = MAC_{k_b}(M')$.
5. The ciphertext is $(M', AUTH, Q)$.

Where, MAC_{K_b} : Message Authentication Code based on key k_b

In this scheme, the ciphertext that needs to be sent to the receiver consists of the variable Q , the encrypted message M' and the authentication code $AUTH$. Q is used to recover the encryption and authentication keys, whereas the authentication code is used to verify the message integrity (if it has been tampered with) and authenticity (if it has been sent by an unauthorized entity). Upon receiving the ciphertext, the receiver computes the value of $AUTH$ and compares it with the received one, if the values are found equal the ciphertext is processed to obtain the plaintext, otherwise the information is ignored. The decryption procedure is shown in Algorithm 3.2. As with the previous model, the scheme has small storage overhead. Yet, the communication overhead is larger for this scheme as it adds authentication information to the encrypted message.

Algorithm 3.2 ECIES decryption procedure

INPUT: Private key α , $(M', AUTH, Q)$
OUTPUT: M

1. Generate the symmetric keys $(k'_a, k'_b) = KDF(\alpha Q)$
2. **IF** $(AUTH \neq MAC_{k'_b}(M'))$
3. Ignore message and stop
4. **ELSE**
5. $M = SYMM_{DEC_{k'_a}}(M')$
6. **END IF**
7. **Output** M

It should be obvious that ECIES incurs an acceptable performance overhead and provides the best functionalities among the elliptic curve-based encryption schemes. Consequently, we will utilize it for building the proposed hybrid encryption cryptosystem that is described in the next section.

3.4 The Proposed Hybrid Encryption Secure Single-Recipient Uplink Communication Scheme (HC-SSRU)

In this section we will demonstrate the proposed hybrid encryption in details. However, we will present first the assumed network and adversarial models.

3.4.1 The Network Model

Figure 3.3 shows the architecture of the AMI network we employ in our scheme. Every HAN, BAN, and IAN comprises a smart meter that is deployed in customers' premises. The meter is responsible for measuring energy consumption and reporting the readings to the utility for billing purposes.

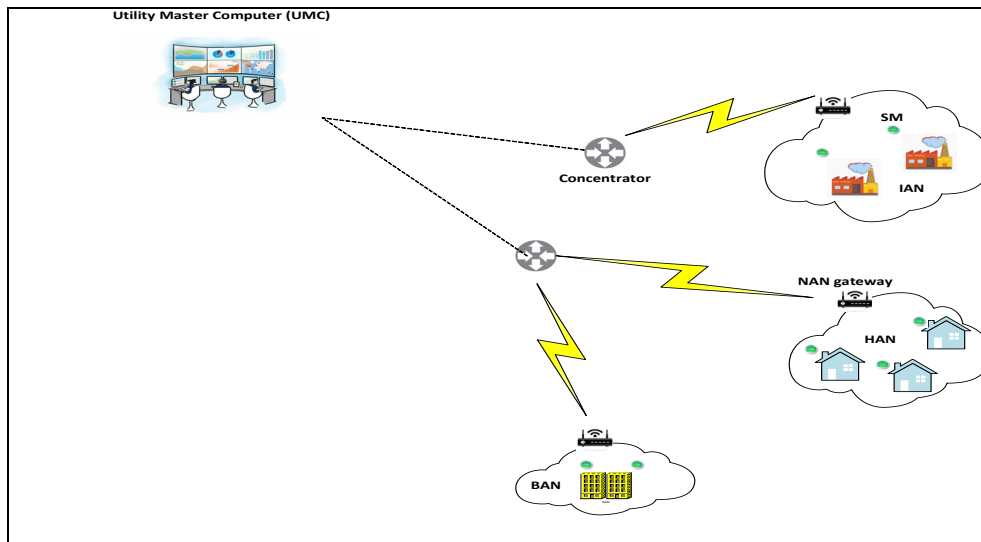


Figure 3.3 AMI network model assumed in HE-SSRU

In addition, the meters receive pricing information and control commands from the utility, but in this chapter we concentrate on the uplink data transmitted from the smart meters towards the utility premises. There is no direct connection between the meters and the Utility Master Computer (UMC), therefore the meters utilize public insecure communication channels to transport the readings to NAN gateways that act as intermediators. The connection between the meters and gateways is hierarchal in a sense that one NAN gateway collects the readings of multiple smart meters. Similarly, every data concentrator collects and aggregates the data received from multiple gateways before routing it to the final destination. For this infrastructure, the communication between the smart meters and NAN gateways are the most vulnerable (Fouda et al., (2011)). Accordingly, we will adopt the simplified network model shown in Figure 3.4 to discuss our proposed security protocol. We assume that the smart meters and UMC are one hop in distance. UMC is equipped with high storage and powerful processing

capabilities in opposite to the smart meters and gateways that have very limited storage and communication capabilities.

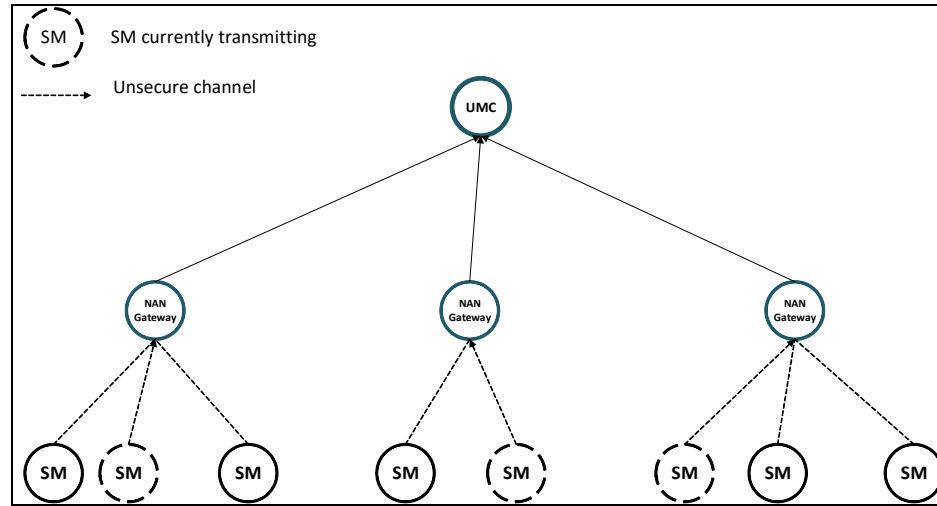


Figure 3.4 The simplified AMI network model

3.4.2 The Threat Model

For the communication between smart meters and gateway, the adopted threat model is assuming a powerful external adversary that is capable of:

- 1- Capturing the smart meter messages by intercepting on the two-way communication channels between the meters and NAN gateway;
- 2- Acting as a legitimate smart meter to maliciously replay outdated metering messages or inject falsified messages to the NAN gateway. The falsified messages could be new or forged from a previous communication;
- 3- Spoofing smart meter identities to initiate communication with other parties.

3.4.3 Optimizing the Computation Overhead of ECIES

The proposed hybrid encryption system utilizes ECC and symmetric cryptography in its construction. As we have demonstrated in section 3.3.2, ECIES is the most desirable elliptic curve-based encryption scheme, therefore we will use it as the public-key encryption module.

Encryption using ECIES requires two scalar-point multiplications while decryption requires one scalar-point multiplication. Several research articles pointed out that scalar-point multiplication is the most computation intensive operation for the elliptic curve-based encryption schemes (Almimi, Samsudin & Jahani, 2014) (Azarderakhsh & Reyhani-Masoleh, 2013). In this regard, we have developed a C++ code to assess the time required to perform scalar-point multiplication over the prime finite field Z_q for some of the recommend elliptic curves presented in (Certicom Research, 2010). The simulation results shown in Table 3.2 indicate that the computational overhead increases with the size of elliptic curve. In addition, the results show that the time required to perform one scalar-point multiplication is significant compared to other cryptographic operations. For example, RSA encryption and decryption requires 0.16ms and 6.08 respectively (Dai,2009) compared to 0.98ms for single point multiplication using the curve secp224k1.

Table 3.2 Computation time for single scalar-point multiplication

Elliptic Curve	secp112r1	secp160k1	secp192k1	secp224k1	secp384r1
Time (ms)	0.56	0.63	0.74	0.98	2.07

For AMI networks, the impact of point multiplication overhead will be greater than what is shown in the table for two reasons: 1) ECIES requires two scalar-point multiplications for encryption, therefore the encryption overhead at the smart meter is the double. 2) In AMI networks, NAN gateway will be responsible for hundreds or thousands of smart meters, therefore it encrypts/decrypts several messages for each connected meter thereby the impact of multiplications overhead on encryption/decryption performance will be substantial.

Considering the fact that scalar-point multiplication is independent of the message to be encrypted or decrypted, we found that the computation overhead of ECIES could be improved by precomputing the scalar-point multiplication in advance. During an initialization phase, every one of the communicating parties (smart meter or NAN gateway) chooses the private value r , precomputes $Q = r \cdot G$, and sends the result to the node it wishes to communicate with. The receiving node precomputes KDF input by multiplying the received value by his private key and stores the obtained result. The stored result is used in future communications. With

the precomputation technique, the parties do not generate new secret values for each communication session. Rather, they utilize the stored value to drive the symmetric keys K_a and K_b . The proposed scheme allows the parties to frequently generate new secret values to improve the resiliency of the protocol. In the next section, the precomputation procedure is explained in the context of the proposed hybrid encryption scheme.

3.4.4 Message Format

The messages exchanged under HE-SSRU have the format shown in Figure 3.5. The payload field stores the information that the smart meter needs to report for the UMC through NAN gateway. The size of this field is variable and determined by the amount of information that needs to be reported. Synch and clock tolerance fields are used to guard against replay attack as we will discuss shortly. Synch is 128 bits that stores the message timestamp corresponding to the message creation time, whereas clock tolerance (θ) is 32 bits that indicates for how long (in milliseconds) the message will remain valid. The choice of clock tolerance value depends on many factors such as computation speed, network bandwidth, network congestion status and the packet delay requirements. The precomputation parameter (Q) is used to improve the security of the proposed protocol by frequently updating the precomputed values that are used to derive the cryptographic keys. The input to KDF is updated once a new precomputation parameter is received by multiplying the value of Q with the private key. Zeros in the precomputation field indicates that the sender wants to keep using the old KDF inputs, thus no update to KDF keys is required. The size of this field depends on the elliptic curve in use. As explained, hybrid cryptosystems encrypt the secret key used to construct the ciphertext and append it to the ciphertext. The symmetric secret key is stored in key field. The size of this field depends on: original key size and the public key algorithm used to encrypt the key. Message Integrity Code (MIC) is used to protect message integrity and authenticity. A message that is tampered with or originated from an unauthorized source is detected when MIC field is checked. The shaded fields on Figure 3.5 represent encrypted information.

<i>Payload</i>	<i>Synch</i>	<i>Clock Tolerance (θ)</i>	<i>precomputation parameter (Q)</i>	<i>key</i>	<i>MIC</i>
----------------	--------------	--	--	------------	------------

Figure 3.5 The message format of the proposed hybrid cryptosystem

3.4.5 Details of HE-SSRU

This section elaborates the proposed hybrid encryption scheme in details. The operation of the proposal can be divided into three phases illustrated as follows:

a) Initialization

Whenever a new smart meter joins the AMI network, it needs to contact the corresponding NAN gateway to register itself and initialize the cryptographic parameters and keys needed for further communication. The initialization procedure is illustrated in Figure 3.6. The smart meter requests to register himself with the NAN gateway by sending a join message with his ID included. The ID is any unique identification information such as the MAC address. In our scheme, the smart meter is not allowed to register with more than one gateway to prevent identity spoofing. Therefore, once the gateway receives the join message, it contacts the other NAN gateways to verify whether the meter is already a member of another NAN network or not. If the meter is found a member of another NAN network, the request will be denied and the connection is aborted. Otherwise, it will approve the join request.

Then, the smart meter and the NAN gateway generate a pair of public/private keys after agreeing on the elliptic curve parameters. As shown in the figure, α and P_1 are the gateway private and public keys respectively. Whereas, β and P_2 are the meter private and public keys respectively. They also agree on the precomputation parameters that they will use as an input to KDF to drive ECIES keys. In order to do so, they independently choose random points on the elliptic curve and exchange these points with each other ($Y.G$ and $X.G$). Finally, they will calculate the precomputation parameters needed to drive the encryption and decryption keys. For example, the smart meter will use $X.P_1$ to derive encryption and authentication keys and $\beta.Y.G$ to derive decryption and authentication keys. These precomputation parameters will not remain the same during all communications between the meter and gateway, rather they will be changed frequently to improve the resiliency of ECIES.

b) Message Encryption at smart meter

The structure of the proposed hybrid encryption scheme is shown in Figure 3.7. The scheme is composed of three models: symmetric encryption module, asymmetric encryption module and message integrity module (keyed hashing module). Before encrypting the message, the smart meter decides if it needs to change the precomputation parameters currently in use by flipping a random coin. If it decides to update the parameter, it picks a random point on the elliptic curve and includes it in the precomputation parameter field Q on the message.

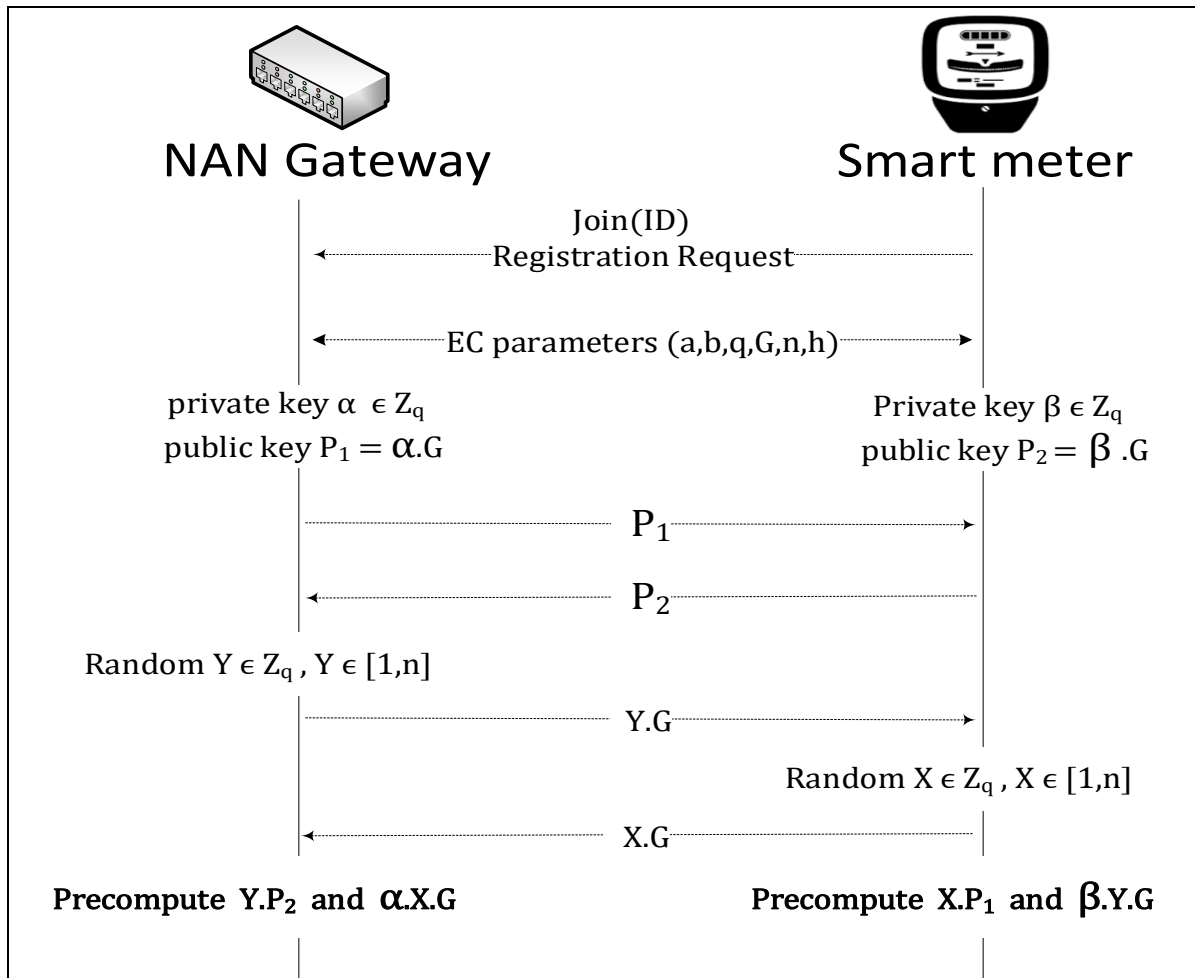


Figure 3.6 The initialization phase of HE-SSRU

The smart meter then constructs the message to be encrypted by combining the payload, timestamp (synch), clock tolerance (θ) and the updated precomputation parameter Q . Then,

the message is encrypted in the symmetric encryption module with 128bits AES and an arbitrary key (k_r) produced by the random generation unit. The precomputation parameter ($X.P_1$) established during the initialization phase is used as an input to key derivation function to generate the encryption key K_e and the authentication key K_h . In our scheme, we used SHA-256 hashing function as a key derivation function. After that, the asymmetric encryption module is used to encrypt the secret key k_r using the elliptic curve-based ECIES algorithm with the key K_e to produce the encrypted key k'_r . With the authentication key K_h , the keyed hashing module produces Message Integrity Code (MIC) for the encrypted message M' and the encrypted secret key k'_r . The ciphertext is formed by combining the encrypted message M' , the encrypted secret key k'_r and the integrity code MIC .

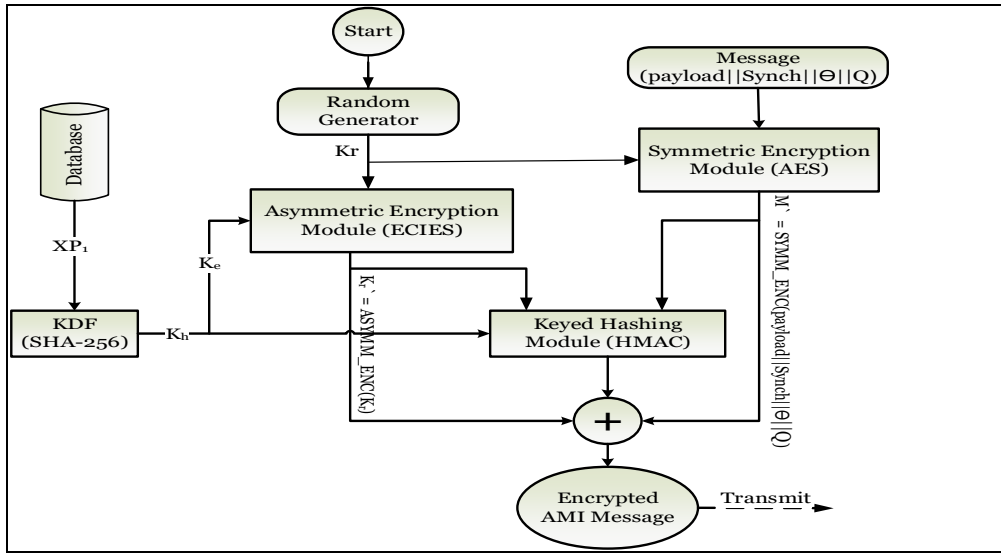


Figure 3.7 Message encryption procedure

c) Message Decryption at NAN gateway

When the encrypted metering information is received at the NAN gateway, it is decrypted and verified before the gateway acts on it or transmits it to UMC. Algorithm 3.3 illustrates the process of decrypting messages using the proposed hybrid protocol. Firstly, the gateway retrieves the precomputation parameter associated with the source meter and generates the authentication and decryption keys (lines 1,2). Then, the gateway recomputes the value of the integrity code ($HMAC_{K_h}(M' || K'_r)$) and compares it with the received one to check against any

integrity or authenticity violations. If the values are found different, it means the message is invalid (has been tampered with or is originated from an unauthorized entity) and thus it will be dropped (lines 3 and 21).

The key field of a valid message is decrypted using K_e to obtain the secret key (line 4), this key is used to recover the message M by decrypting M' (Lines 5-7). Then, the message timestamp is compared with the current time to determine whether the message has been replayed or not (line 10). The message is considered replayed if the difference between the message timestamp and the local time is greater than the clock tolerance. Replayed messages are dropped with no further action (line 17). The gateway processes the message if and only if it passes the aforementioned checks. Finally, the receiver checks whether the sender is willing to update the precomputation parameter by inspecting Q field (line 12). The value of zero in the Q field indicates that the sender is not willing to modify the precomputation parameter for the next communication.

Algorithm 3.3 Decryption procedure in HE-SSRU

INPUT: Encrypted message M', Encrypted secret key K'_r, Message Integrity Code MIC OUTPUT: Message M or $\perp$ <pre> 1 $\alpha XG \leftarrow \text{get_param}(\text{DEC})$ 2 $(K_e, K_h) \leftarrow H(\alpha XG)$ //Verify message integrity and authenticity 3 IF (MIC == $\text{HMAC}_{K_h}(M' K'_r)$) 4 $K_r = \text{AES_D}(K'_r, K_e)$ 5 FOREACH ($B_i \in \{B_0, B_1, \dots, B_{\text{SIZE}-1}\}$) LOOP 6 $m = \text{AES_D}(B_i, K_r)$ 7 $M = [M m]$ 8 END FOREACH 9 ($\text{Payload}, \text{SYNCH}, \theta, Q$) = PARTITION($M$) 10 IF ($\text{TIMEOFDAY}() - \text{SYNCH} < \theta$) 11 //process message 12 IF ($Q \neq 0$) 13 UPDATE_PRECOMM_PARA(Q) 14 END IF 15 END IF 16 ELSE 17 // ignore replayed message 18 END ELSE 19 END IF 20 ELSE 21 // ignore invalid message 22 END ELSE </pre>
--

3.5 Performance Analysis

In this section, we will evaluate the performance of the proposed scheme in terms of computation, communication, and storage overhead. We implemented the proposed hybrid encryption scheme (HE-SSRU) in software (C++) using 128bits AES and ECIES with precomputation phases. The proposed scheme is compared with RSA and the Merkle-Tree-Based Authentication scheme (MTBA) presented in (Li et al., 2014). The simulation parameters are shown in Table 3.3.

Table 3.3 Simulation environment parameters

Processor Speed	2.7 GHz
CPU cores	5
Memory Capacity	8 GB
Operating system	Linux Mint 18.1 mate
Kernel Version	4.4.0-53
GCC compiler version	4.6.3
Degree of multithreading	Single
KDF	SHA-256
Symmetric Encryption Module	AES128
Elliptic curve specs	Variable
No. of DR projects	1
Message Size	32Kbyte

3.5.1 Computation Overhead

Computation overhead is the time required to generate all the ciphertext components in the format that will be transmitted to the network or the time required to decrypt the ciphertext to recover the plaintext. The main factor that determine the computation time is the algorithm structure and complexity. For the proposed protocol (HE-SSRU), the computation overhead is the processing time of symmetric encryption, asymmetric encryption and message integrity modules plus the processing time of any complementary units such as pseudo random generation unit and KDF. In this experiment, we used the recommend elliptic curve *secp160r1* that offers the same security level of 1024bits RSA (as shown in Table 3.1). In addition, we assume that the precomputation parameters are established during the initialization phase and

are not changed later ($Q = 0$). Figure 3.8, shows a comparison of computation overhead incurred by NAN gateway to decrypt multiple metering ciphertexts for the different encryption schemes. We assume that each smart meter is sending only one encrypted message, thus for 1000 connected smart meters, the time plotted represents the cost of decrypting 1000 messages. In the figure, we can see that RSA requires considerable computation overhead compared to the other protocols. As shown in the figure, the proposed protocol achieves almost the same computation cost of the lightweight Markle-tree hashing scheme due to the use of the precomputation phases that significantly reduced the decryption overhead. With the implementation of the precomputation phase, the computation overhead of the proposed scheme can achieve the efficiency of symmetric cryptosystems.

3.5.1 Communication Overhead

Communication overhead is measured by the number of extra bits added to the message in order to secure it. Due to the fact that AMI networks have limited bandwidth; cryptographic schemes should consider minimizing the communication overhead a priority. In our proposed scheme, three fields are added to the message: the precomputation parameter (Q), the encrypted secret key K'_r and the integrity codes (MIC). The size of the precomputation parameter depends on the elliptic curve used. The size of K'_r is determined by the size of key used by the symmetric encryption algorithm, while the size of MIC field depends on the choice of the keyed hashing function. In the simulations conducted, we implemented 128bits AES in the symmetric encryption module and SHA-224 in the key hashed module. Consequently, the communication overhead will be 352 bits plus the size of elliptic curve point.

In MTBA, authentication path information (API) is added to every report generated by the smart meter. API is seven hash digests added together, where the size of each digest is 128 bits. Consequently, 896 bits are added to every smart meter report so that the message authenticity could be verified at the destination. On the other hand, the size of ciphertext or digital signature generated by RSA equals to the key used for encryption and signature generation where the minimum possible size of ciphertext or signature is 1024 bits

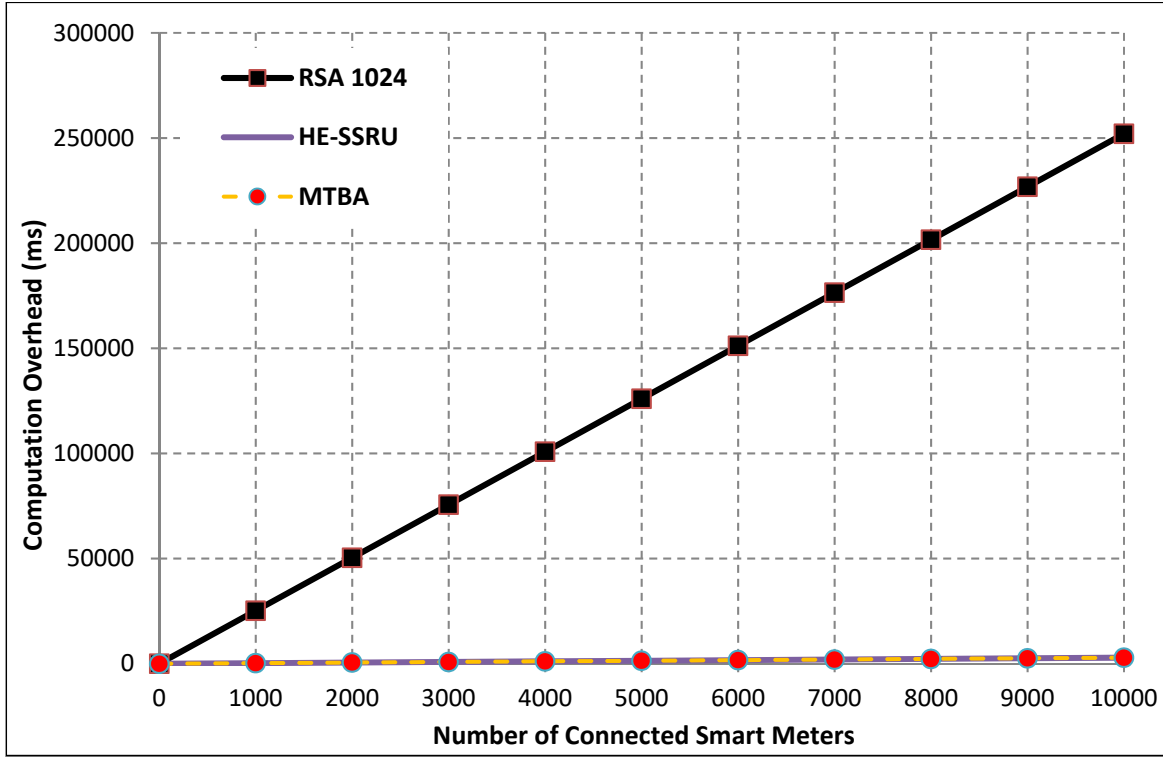


Figure 3.8 Comparison of decryption Time incurred By NAN gateway

Figure 3.9, shows the communication overhead resulted from the three encryption schemes and for different number of smart meters, each transmitting single encrypted metering information. It is evident that the implementations of the proposed protocol using different elliptic curves (112, 160, 192, and 224 bits) achieves the lowest communication overhead. RSA results in the highest communication overhead due to the large signature size.

3.5.2 Storage Overhead

In the context of cryptography, the storage overhead is the total size of keys, parameters, identifiers that need to be stored in order to implement the cryptographic scheme. As shown in section 3.4.1, the simplified AMI network model comprises UMC, gateways and smart meters. In opposite to UMC and gateways, smart meters are equipped with limited storage capabilities. Since gateways and smart meters are not supposed to store large amount of cryptographic information, the storage requirement of any cryptosystem is crucial. In this section, we analyze

the storage requirement for our protocol and compare it with the storage requirements of MTBA and RSA.

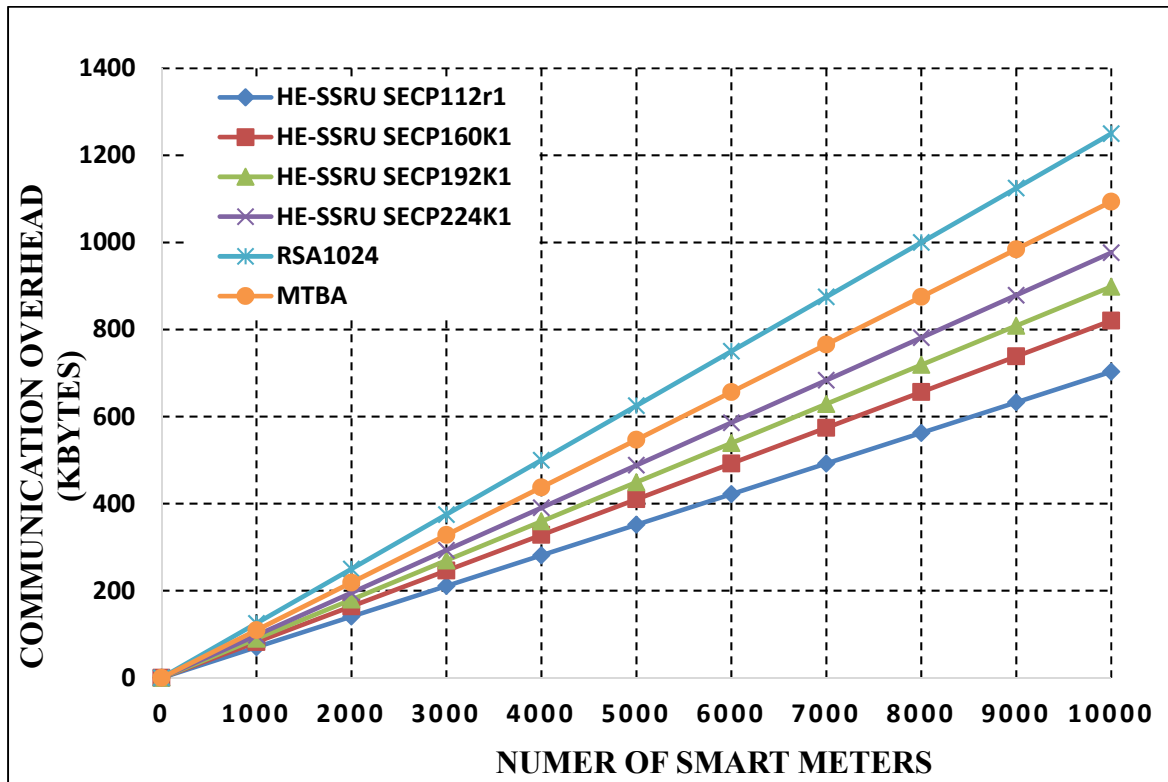


Figure 3.9 The Communication overhead for different number of smart meters

First, we measured the storage overhead incurred by the smart meters to implement the different encryption schemes. In our scheme, smart meters need to store elliptic curve parameters, public/private key pair and precomputed encryption/decryption parameters. The size of these parameters depends on the underlying elliptic curve. RSA on the other hand, requires the smart meters to store three keys in addition to the parameters needed to generate the keys (such as p , q , n and $\emptyset$). The implementation of Merkle-tree based scheme requires the smart meters to store a special table called electricity report collection table. Every tuple in this table stores identification information, timestamp and authentication path information. The storage overhead comparison for the three schemes is illustrated in Table 3.4.

Table 3.4 Storage overhead on smart meters

Scheme	HE-SSRU secp112r1	HE-SSRU secp160k1	HE-SSRU secp192k1	HC-SSRU secp224K1	HE-SSRU Secp256r1	RSA1024	RSA2048	MTBA
Storage (bits)	1344	1920	2304	2688	3072	3072	6144	$13 * 2^{13}$

Next, we demonstrate the storage overhead on NAN gateway to ensure secure communication with the smart meters. NAN gateway must store cryptographic information related to each one of the smart meters belongs to the same DR project to enable the gateway recovering the encrypted metering information. In the proposed scheme, the gateway stores the identifier, elliptic curve parameters, public key and the precomputation parameters associated with every meter registered with it. In addition, it stores his own public-private key pair. Figure 3.10, shows the storage overhead on NAN gateway to ensure secure communication with a group of smart meters for the different encryption schemes. The figure illustrates that the storage overhead is directly proportional to the number of smart meters connected to the same gateway to accommodate the need to store more cryptographic information. As depicted in the figure, RSA possess considerable storage requirement compared to the other schemes. On the other hand, MTBA has the lowest overhead as most of the cryptographic information is stored at the meters and API is attached to the messages themselves. The main factor that controls the storage requirement of the proposed protocol is the elliptic curve size, therefore the choice of elliptic curve size must be chosen wisely to ensure balancing the security level needed with the storage overhead introduced.

3.6 Security Analysis

Having us illustrated the efficiency of the proposed protocol in terms of the computation, communication and storage overhead, we now discuss its competence in providing secure uplink communication between the smart meters and the NAN gateway. In this regard, we will illustrate HE-SSRU ability to fulfil security requirements and thwart multiple attacks. The analysis is based on the security services provided by the underlying cryptosystem.

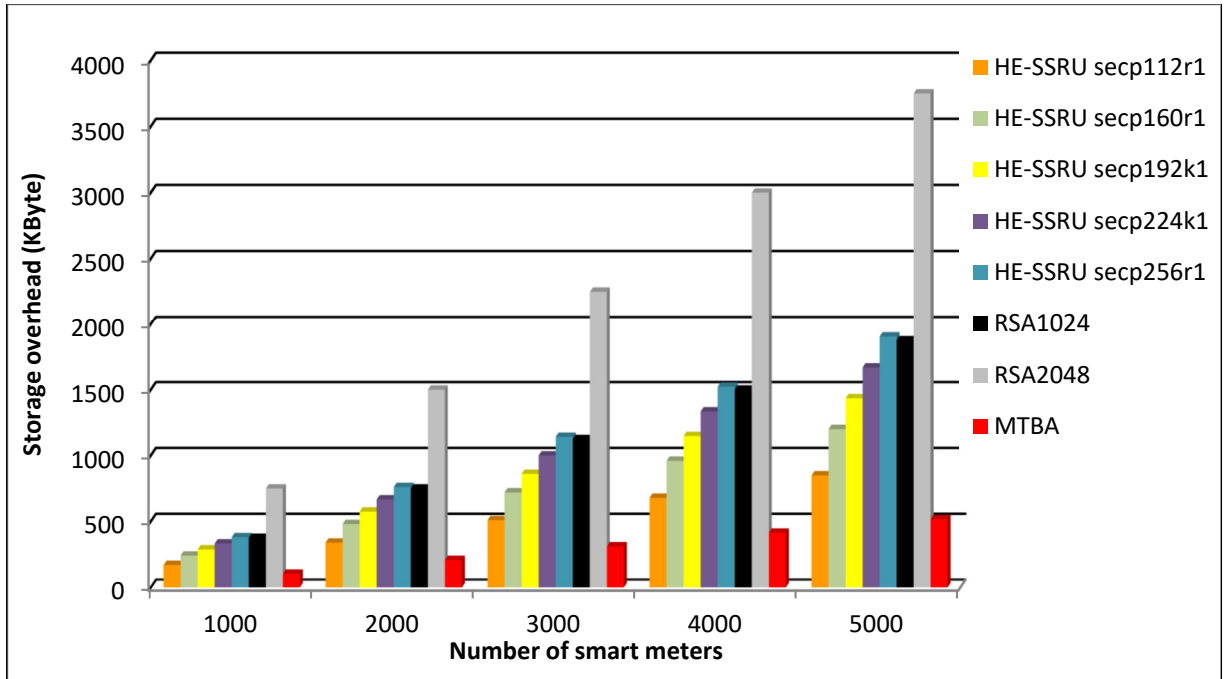


Figure 3.10 Storage overhead on NAN gateway for variable number of smart meters

1. Data Confidentiality and Customer privacy

In the proposed scheme, messages exchanged between the smart meters and the gateway are always encrypted using symmetric encryption algorithm with a random one-time key (K_r). This key is encrypted using ECIES and attached to the message in a way that ensures only the designated gateway in which the meter is registered with can recover the message. An unauthorized entity who does not pose the private key (but still needs to drive the decryption key (K_e)) must solve ECDLP to obtain the private key (say α) from the known public key ($\alpha \cdot G$) which is known to be a computationally infeasible operation. Thus, unauthorized entities will never be able to reveal the content of encrypted messages. Therefore, the proposed scheme ensures data confidentiality and protects customer privacy.

2. Data Integrity and data manipulation attack

Ensuring data integrity requires protecting data against unauthorized modification. In the proposed scheme, keyed hashing module appends integrity code (*MIC*) for every message to ensure unauthorized modification to the message does not go undetected. The integrity code is

recomputed at the receiving side and is compared with the one included in the message. If the two are found unequal, the receiver can infer that the message is maliciously modified and should be ignored. Therefore, the proposed protocol maintains data integrity and mitigates data manipulation attacks.

3. Data authenticity

Attaching *MIC* to messages ensures data authenticity as well. If the recomputed MIC does not match the one stored in the message ($MIC \neq HMAC_{K_h}(M' || K'_r)$), the receiver will deduce that the message is originated from an unauthorized source. This is because only legitimate smart meters hold the accurate precomputation parameters needed to drive the right authentication key (K_h).

4. Replay attack

This attack occurs when the adversary captures legitimate network message for the purpose of intentionally and maliciously injecting it back into the network at a later point of time. The proposed protocol guards against this attack by including synch and clock tolerance fields with every message. After decrypting the message, the receiver compares the current time against synch and θ field to determine if the message is replayed or not. If $((TIMEOFDAY() - SYNCH) > \theta)$ the receiver infers that the message is maliciously replayed and ignore it.

5. Spoofing attack

This attack occurs when the intruder snatches the identity of legitimate user to act on his behalf. In the context of the proposed scheme, the intruder may launch spoofing attack by snatches the identity of a legitimate smart meter. In order to do so, the intruder must eavesdrop on the communication channels to capture the smart meter identity (*ID*) at the beginning of the initialization phase. However, the intruder will not be able to use the identity to register himself with the NAN gateway because the gateway keeps track of the smart meters registered with it by storing their identities. In addition, the gateway checks the identity of the smart meter before registering it to make sure its not registered with another gateway. Failing to register with the gateway will prevent the intruder from generating the correct precomputation parameters

needed to drive the keys (K_e, K_h) . Therefore, a spoofing attack can not succeed in our encryption scheme.

3.7 Chapter Summary

Smart meters are central components of AMI networks that enable the power utility to remotely collect energy consumption readings through uplink communication channels. However, the utilization of public and insecure communication links to transmit massive amount of data that include sensitive customers information jeopardizes the metering networks to countless number of security threats that can ruin billing and profiling functions. Therefore, its quite important to ensure secure smart metering operations.

In this Chapter, we consider the concept of hybrid cryptosystem to design an efficient protocol to secure single-recipient uplink communication in AMI networks. The proposed scheme requires that every smart meter register with a NAN gateway before it can report any information to the utility. The registration process aims to prevent identity spoofing and ensures the meter obtain the necessary cryptographic parameters needed to communicate securely with the gateway. In order to protect customer privacy, metering information is encrypted using symmetric encryption algorithm with random session key. The key is encrypted using ECIES and is attached to the encrypted message. We implemented a precomputation procedure to reduce the overhead of ECIES by reducing the scalar-point multiplication time. The cryptographic parameters established during the registration stage enables the gateway to recover the encrypted session key and thus recover the encrypted metering data. Additionally, the proposed protocol maintains data integrity by attaching MIC to every smart meter message. Simulation results show that the proposed protocol incurs low computation and communication costs and requires small storage space. Security analysis illustrates that the proposal can ensure data integrity and confidentiality in addition to mitigating several attacks. In the next chapter, we present a secure data exchange scheme for uplink and downlink communication in AMI networks

CHAPTER 4

ESUD: AN ENCRYPTION AND SIGNATURE SCHEME TO SECURE UPLINK AND DOWNLINK COMMUNICATIONS IN AMI NETWORKS

4.1 Mechanism Description and Design goals

In this chapter, we propose a simple technique to ensure secure data exchange between the different entities in the AMI networks. In opposite to the scheme presented in the previous chapter, the technique we are presenting here accommodates both single-recipient uplink communication and multi-recipient downlink communication. The scheme utilizes symmetric cryptography to protect data confidentiality and customer privacy against passive adversaries. It also aims to warrant data integrity and origin authentication by implementing an elliptic curve signature scheme. The proposed protocol ensures that when a new AMI device joins the network, he is granted the necessary cryptographic parameters needed to establish secure communication with the device in the higher level of network hierarchy.

In particular, the proposed technique aims to achieve the following design goals:

- *Confidentiality and privacy preservation.* The proposed scheme enforces data encryption to prevent unauthorized AMI participants from disclosing messages content;
- *Data Integrity:* The proposed scheme must guarantee that maliciously injected or modified AMI messages must not go undetected;
- *Origin Authentication.* The receiver of a message should be able to tell that the source of the message is indeed verified;
- *Efficiency.* The proposed scheme should be able to provide secure unicast, multicast, and broadcast communication without posing significant computation overhead on AMI devices or communication overhead on the underlying communication channels.

4.2 Preliminaries : Elliptic Curve Digital Signature Algorithm (ECDSA)

The proposed scheme exploits digital signature to ensure data authenticity and non repudiation. It has been shown that the performance of RSA specially for resource constrained devices is not up to the mark (Suarez-Albela, Fernández-Caramés, Fraga-Lamas, & Castedo, 2018) . With

the increasing need for greater security levels, RSA yields large key sizes leading to inefficient implementations. ECDSA (Johnson, Menezes, & Vanstone, 2001) is a public-key algorithm that was accepted as an ANSI standard as a variation of Digital Signature Algorithm (DSA) that utilizes elliptic curves for signature generation and verification. Thus, it can achieve similar security levels as of RSA but with significantly smaller key sizes.

Given an elliptic curve E defined over the finite field $\mathbb{F}_q$, $G \in E(\mathbb{F}_q)$ is the generator point of order n and the hash function $H: \{0,1\}^* \rightarrow \mathbb{Z}_n$. The signer generates a random value α such that $1 \leq \alpha < n - 1$ and computes $Q = \alpha \cdot G$. The private key α is kept secret while the public key Q is published. The procedure for signing message m is as follows:

1. Choose a random value k in the interval $1 \leq k < n$, and compute the point $(r_1, r_2) = k \cdot G$;
2. Compute $s = k^{-1}(H(m) + \alpha r_1) \bmod n$;
3. The signature $\sigma = (r_1, s)$

The receiver can verify the signature by computing:

1. IF $((0 < r_1 < n) \&\& (0 < s < n))$, proceed;
2. Compute the point $(t_1, t_2) = (s^{-1} \bmod n)(H(m)G + r_1Q)$;
3. The signature is valid if and only if $t_1 = r_1$, otherwise the signature is invalid

4.3 The proposed Scheme

In this section we present the models used to implement the proposed scheme, then we will demonstrate the proposed scheme in details.

4.3.1 Network and Communication Mode

We assume two-way communication AMI network that comprises three devices namely: smart meters (SMs), gateways (GWs) and the utility Supervisory Control Center (SCC). SMs are located in customer side and are responsible for collecting energy consumption and reporting the readings to the utility for billing purposes. Meanwhile, SCC communicates variety of data and control commands to the meters such as pricing information, peak shaving, DR announcements, and remote load control. This two-way communication between the utility

and customers is the smart grid flagship feature this is empowered by AMI networks. The gateways play an important rule in this communication by routing information in bidirectional paths from/to smart meters to/from SCC.

Having us examined the messages exchanged in AMI networks (Liu et al.,2013), we have found that communication between the AMI devices can fall in one of two categories:

a) Uplink communication

This communication is carried out when a lower layer device D_{LL} sends message to a higher layer device D_{HL} . For example, a smart meter transmitting to the corresponding gateway or a gateway that routes message to SCC. The transmission mode for such communication is unicast only.

-Unicast ($GW_i \rightarrow SSC, SM_i \rightarrow GW_i$)

Figure 4.1(a) shows an example of this case when a smart meter is reporting the customers' energy consumption to the corresponding gateway.

b) Downlink communication

In this case, a higher layer device D_{HL} sends message to a lower layer device(s) D_{LL} . It could be the SCC transmitting to the corresponding gateway(s) or a gateway is routing messages to the corresponding smart meters(s). The transmission mode for such communication is unicast, multicast or broadcast.

-Unicast ($SSC \rightarrow GW_i, GW_i \rightarrow SM_i$)

Remote load control is an example of this communication scheme. The supervisory node continuously monitors customer's consumption and can issue special command to enforce peak management.

-Multicast ($SSC \rightarrow GW_i, GW_i \rightarrow SM_i$) $i \in \{0,1, \dots \mathcal{M}\} \mathcal{M} < L$

An example of downlink multicast AMI communication is shown in Figure 4.1(b). Price updating and remote load control commands are triggered by the supervisory node and disseminated to certain Demand-Response projects in multicast transmission mode.

-Broadcast ($SSC \rightarrow GW_i, GW_i \rightarrow SM_i$) $i \in \{0,1, \dots L\}$

This case is similar to the previous one, except having the AMI headend (supervisory node) or gateway transmits the command to all AMI devices. Publishing of DR projects is an example of this communication style.

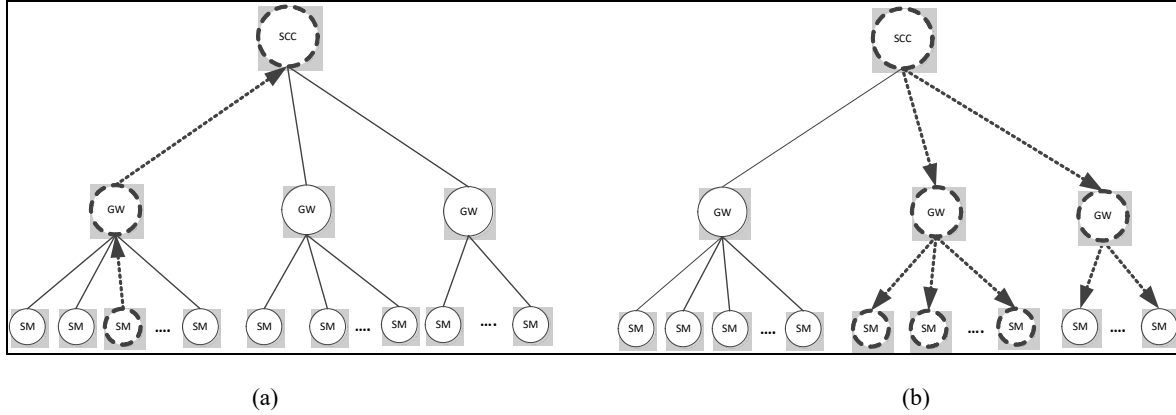


Figure 4.1 The AMI communication model assumed in the proposed security scheme. a) unicast uplink Communication. b) multicast downlink communication

4.3.2 Adversarial Model

In our threat model, we assume an external polynomial time adversary $\mathcal{A}$ with a sufficient knowledge and computation power. The adversary $\mathcal{A}$ can access the public communication channels and capture network messages. Accordingly, he can eavesdrop, analyze, inject, replay, modify data exchanged over the communication channels. Additionally, $\mathcal{A}$ may try to forge the signature of a legitimate AMI entity “B” by obtaining B’s signature on a collection of messages. We assume that gateways and supervisory node (SCC) is securely suited within the utility premises and could not be compromised by the attacker.

4.3.3 The Proposed Scheme to Ensure Secure Uplink and Downlink Communication

In the light of the conceivable communication scenarios discussed in section 4.3.1, we demonstrate the proposed scheme to ensure secure bidirectional communication between the smart meters and the utility headend. Data generated by the meters are mainly household consumption readings, thereby carries massive amount of personal information. Therefore, the major security goal is to protect consumer privacy for uplink communication. On the other hand, utility-generated messages contain critical commands to maintain accurate and reliable grid operation. Thus, ensuring integrity and authenticity are equally important security goals

for downlink traffic. Taking into consideration these security requirements, we designed a crossbred encryption and signature scheme to confront confidentiality, integrity and authentication threats for both communication patterns in AMI network. The operation of the proposed mechanism is divided into two phases: initialization and secure communication.

a- Registration phase

This phase is required whenever a new smart meter or gateway joins the AMI network to setup the necessary parameters needed to establish secure communication with the rest of AMI network. The new device initiates the registration phases with the device in the higher layer of the communication hierarchy (i.e. a new smart meter makes the request to the corresponding gateway or a new gateway makes the request to SCC). We will refer to the new device as *Lower Layer Device* (D_{LL}) which makes the request to the *Higher Layer Device* D_{HL} . This phase is essential to enable D_{LL} and D_{HL} securely set up the cryptographic parameters (keys and hash functions) over the inherently insecure two-way AMI channels. D_{HL} assembles the elliptic curve parameters and shares them with D_{LL} to enable both deriving a shared secret key K_{sh} . Once they agree on the shared key, they proceed exchanging other cryptographic parameters encrypted using K_{sh} .

As discussed in the communication model, downlink traffic is generated by D_{HL} and is transmitted to one or more D_{LL} devices in unicast, multicast and broadcast mode. In order to make sure they can exchange encrypted messages, D_{HL} generates a secret key k_U and shares the set of secret keys $\{k_U, k_M, k_B\}$ securely with D_{LL} . The shared key k_U is used to secure the communication (uplink and downlink) between D_{LL} and D_{HL} , whereas k_M and k_B are group keys used to secure downlink multicast and broadcast messages, respectively. k_U is generated using the identity of D_{LL} device and the symmetric key generation function ($SGen(b)^1$). Similarly, D_{HL} utilizes asymmetric key generation function ($PGen(b)^1$) to generate a pair of asymmetric keys (KP_{UD}, KS_{UD}) and securely shares a set of three public keys $\{KP_{UD}, KP_{MD}, KP_{BD}\}$ with D_{LL} to enable it verifying signatures constructed using the private keys $\{KS_{UD}, KS_{MD}, KS_{BD}\}$. Additionally, D_{HL} randomly chooses an initial nonce (Number Only Used Once) value N_0 and shares it with D_{LL} . As we will discuss later in section 4.6, using nonce is an efficient mechanism to detect replay attack.

On the other hand, uplink traffic is generated by D_{LL} and is transmitted to a single D_{HL} in unicast mode only. D_{LL} messages are encrypted using the secret key k_U received from D_{HL} . A single public key PK_{UU} need to be shared with D_{HL} to enable it verifies the signatures constructed by D_{LL} private key SK_{UU} . Table 4.1 presents the list of cryptographic notations used in the registration process shown in Figure 4.2.

Table 4.1 Notation guide used in section 4.3

Notation	Description
$h_1(.), h_2(.)$	Hashing functions
k_{sh}	shared symmetric key
k_U, k_M, k_B	Symmetric encryption keys for unicast, multicast, broadcast
$KP_{UD}, KP_{MD}, KP_{BD}$	Public downlink unicast, multicast, broadcast keys for signature verification
$KS_{UD}, KS_{MD}, KS_{BD}$	Private downlink unicast, multicast, broadcast keys for signature generation
KP_{UU}	Public uplink unicast signature verification key
KS_{UU}	Private uplink unicast, multicast, broadcast keys for signature verification

b- Secure Communication Phase

Once the essential cryptographic parameters are established during the registration phase, AMI devices can communicate securely by exchanging encrypted and signed messages. Messages are constructed by concatenating nonce $N_t (N_t = N_{t-1} + 1)$ to the payload (if the sender decides to change his private key, he can include the corresponding public key with the message to enable the receiver correctly verifying forthcoming messages). For single-recipient communication, the messages are encrypted using the secret key K_U and signed using either KS_{UD} for downlink communication or KS_{UU} for uplink communication. Multi-recipient messages originated from the SCC or gateways are encrypted using one of the group keys K_M or K_B , depending on the transmission mode. Such messages are digitally signed using KS_{MD} or KS_{BD} . In the proposed scheme, symmetric cryptography is utilized for encryption and decryption, while ECDSA is used to construct and verify message signature.

Example:

Suppose the multicast domain $\{D_{HL_1} \rightarrow D_{LL_i}, D_{LL_j} \dots D_{LL_M}\}$, in which the gateway ($D_{HL_1} = GW_i$) is propagating a remote load control message securely to a group of smart meters $\{SM_i, SM_j, \dots \dots SM_M\}$. The communication shall proceed as follows:

Step 1: Message Encryption ($D_{HL_1}: \{\overline{M}_t\}$)

In the proposed model, the message to be encrypted has three components: the data content D , the nonce value N_t and an optional public key (multicast public key $KP_{MD_{t+1}}$ in this case).

The nonce value is used to keep the parties in sync to ensure withstanding replay attack. Therefore, the transmitted nonce value is $N_t = N_{t-1} + 1$, where N_{t-1} is the nonce used in the previous session. The encrypted message $\overline{M}_t$ is $SYMM.ENC_{K_M}(D||N_t||KP_{MD_{t+1}})$.

Step 2: Signature generation ($D_{HL_1}: \{\sigma_t\}$)

The signature σ_t is constructed using the secret key KS_{MD_t} , the hash function $h_2(.)$, and the one way signature generation function **Sign** as $\sigma_t = \mathbf{sign}_{KS_{MD_t}}(h_2(\overline{M}_t))$.

Step 3: Multicast Transmission ($D_{HL_1} \rightarrow D_{LL_i}, D_{LL_j} \dots D_{LL_M}: \{\overline{M}_t, \sigma_t\}$)

D_{HL_1} transmits the encrypted message $\overline{M}_t$ along with the signature σ_t for each $D_{LL} \in \{D_{LL_i}, D_{LL_j} \dots D_{LL_M}\}$.

Step 4: Signature verification ($D_{LL_i}, D_{LL_j} \dots D_{LL_M}: \mathbf{Vrfy}_{PK}(.))$

Every D_{LL} in the multicast domain $\{D_{LL_i}, D_{LL_j} \dots D_{LL_M}\}$ that receives the message will use the multicast public key KP_{MD_t} , the hashing function $h_2(.)$ and the one way signature verification function **Vrfy** to verify the signature. The signature is accepted if and only if $\mathbf{Vrfy}_{KP_{MD_t}}(h_2(\overline{M}_t), \sigma_t) = 1$, otherwise the signature is rejected and “invalid message” is reported.

Step 5: Message decryption $D_{LL_i}, D_{LL_j} \dots D_{LL_M}: \{D, N_t, KP_{MD_{t+1}}\}$

If the signature σ_t is accepted, the multicast domain members $\{D_{LL_i}, D_{LL_j} \dots D_{LL_M}\}$ individually decrypts $\overline{M}_t$ using the multicast downlink key K_{MD} to obtain $M_t = SYMM.DEC_{K_M}(\overline{M}_t)$. Then, the received nonce value N_t is checked to detect if the message is replayed. Replay attack is detected if $N_t \leq N_{t-1}$ and in this case the message is ignored and replay attack is reported.

Otherwise, the data content D is processed and the received public key $KP_{MD_{t+1}}$ is stored to enable verifying the message that will be received next. The current nonce value (N_{t-1}) is updated with N_t as well.

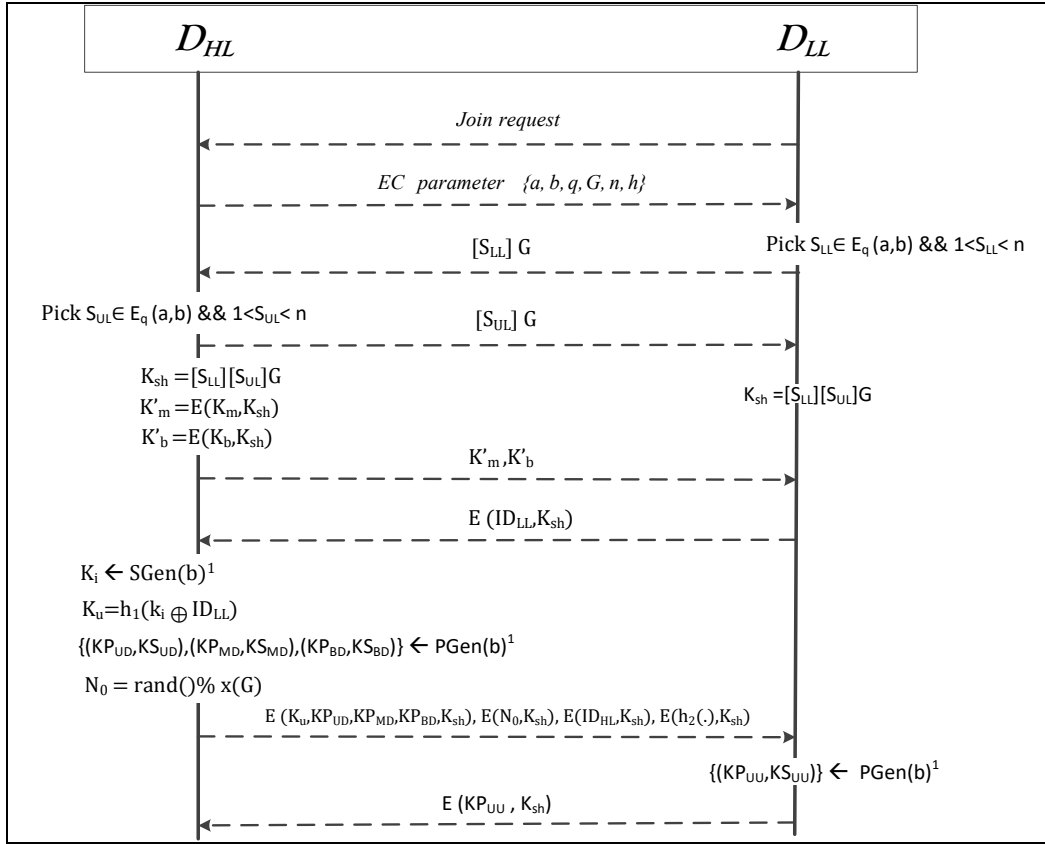


Figure 4.2 The details of registration phase

4.4 Performance Evaluation and Security Analysis

This section is dedicated to evaluate the performance of the proposed encryption and signature scheme in terms of computation cost, ciphertext size, and storage overhead. we evaluate the performance of the proposed scheme and compare it with the Identity-Based Signcryption (IBS) model presented in (Alharbi & Lin, 2016). In addition, we illustrate the strength of the proposed protocol in mitigating several attacks in this section. The notation used in this section shown in Table 4.2.

Table 4.2 List of notations used in section 4.4

Notation	Description
T_{symm}	Time to perform encryption of decryption using symmetric key algorithm ($SYMM_{END}$ or $SYMM_{DEC}$)
T_{mul}	Time to execute scalar-point multiplication (such as $K.G$ or $H(m).G$)
T_{pair}	Time to perform bilinear pairing operating (such as $e(Q_s, P_{pub})$)
$ point $	The size of an elliptic curve point in bits
$\hat{C}$	A digitally signed ciphertext
$ \mathcal{M} $	Multicast domain size
$ L $	Broadcast domain size
N	Number of multicast domains

4.4.1 Performance Evaluation

The performance analysis of the proposed protocol in terms of computation cost, ciphertext size and storage overhead is discussed in this section.

4.4.1.1 Computation Cost

With respect to the proposed protocol, the computation cost is the time overhead required to encrypt and sign the plaintext message at the sender side or the time incurred to verify the signature and decrypt the ciphertext at the receiver side. $SYMM.ENC$ and $SYMM.DEC$ are symmetric key cryptography algorithms that have very low computation cost. On the other hand, Signature generation and verification is implemented using the ECC-based ECDSA where elliptic curve point multiplication dominates signing and verification times. Therefore, the computation overhead of our scheme is determined mainly by the time incurred to construct or verify the signature. The identity-based signcryption (IBS) scheme exploits bilinear pairing over elliptic curves to realize encryption and signature generation for AMI downlink traffic. Scalar-point multiplication and pairing are the two operations that determine the computation overhead of IBS.

Table 4.3 illustrates a comparison between the proposed scheme and the identity-based signcryption scheme in terms of the computation overhead. The time required to generate a signed ciphertext in our model is $T_{symm} + T_{mul}$ compared to $4 \times T_{mul} + T_{pair}$ for the other scheme. Moreover, the time needed to verify the signature and recover the plaintext in our scheme is $2 \times T_{mul} + T_{symm}$ compared to $T_{mul} + 4 \times T_{pair}$ for the other bilinear based signcryption model.

Table 4.3 Computation overhead comparison between ESUD and IBS

Operation	Symmetric Cryptography		EC point multiplication (T_{mul})		pairing computation (T_{pair})	
	ESUD	IBS	ESUD	IBS	ESUD	IBS
Signed Ciphertext generation	T_{symm}	-	1	4	-	1
Plaintext recovering	T_{symm}	-	2	1	-	4

In order to compare the efficiency of the two schemes in experimental aspect and to examine the performance in a larger scale, we used PBC (Pairing Based Cryptography) library (Lynn, 2006) to implement elliptic curves and bilinear pairing functions. The implementation was for *secp160r1* elliptic curve with embedding degree = 6 and a base field of 512bits size. The simulation was executed on an Intel Pentium IV 3.1GHz machine with 8GB RAM. We found that the overhead of scalar-point multiplication T_{mul} is 0.6ms and the bilinear pairing T_{pair} is 4.5ms. As explained before, the scalar-point multiplication and pairing operations are the two operations that dominate the execution time of the schemes (ESUD is pairing free). Therefore, we are considering these two operations only when calculating the total computation overhead.

- **Uplink unicast Communication**

Figure 4.3, shows the computation overhead incurred on AMI devices to transmit multiple secure messages or recover multiple plaintexts for the two schemes. From Table 4.3 and Figure 4.3, we can conclude that our proposed protocol is more efficient than IBS in terms of computation speed for supporting secure uplink communication. This is due to the less complex algorithms used for constructing the signed ciphertext or decrypting the ciphertext.

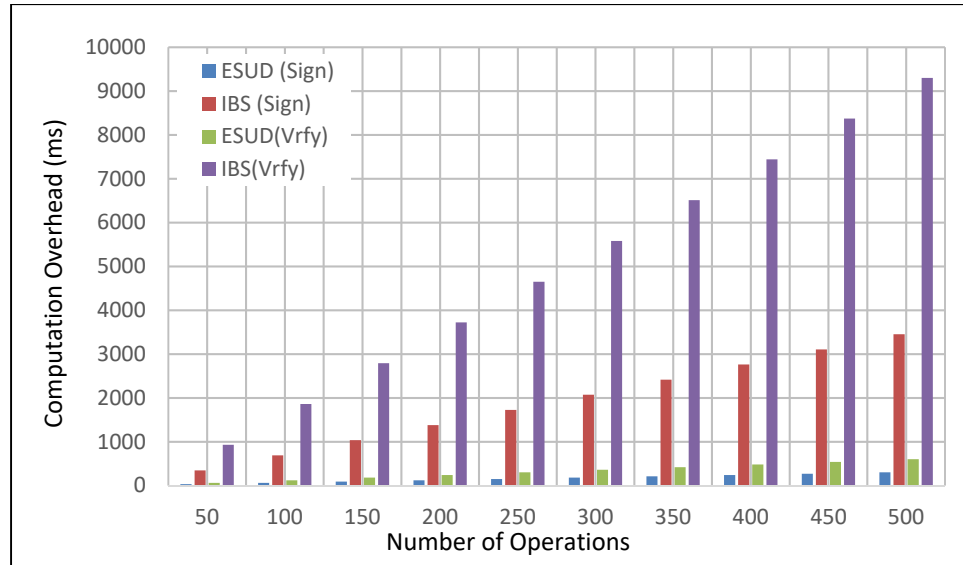


Figure 4.3 The Computation Overhead for Transmitting or Receiving Multiple Secure Uplink Messages

- **Downlink multicast Communication**

The results reported in Table 4.3, show the computation cost for a single encryption/signing or decryption/verification operation. Our proposed scheme is designed to support downlink traffic that can take multicast or broadcast forms. One version of the ciphertext is constructed by encrypting the messages using the multicast key K_m and signing it with the private key KS_{MD} . Then, the ciphertext is propagated to all the users in the multicast domain. The encryption computation overhead is $T_{symm} + T_{mul}$. On the other hand, IBS supports unicast communication only. Therefore, to construct a secure multicast message using IBS scheme, a distinct ciphertext must be generated for each user individually, using the credentials shared between the source and the user. Therefore, the computation cost of signcryption is directly proportional to the multicast domain size. Consequently, the proposed scheme is more efficient than IBS in securing multi-recipient downlink communication.

4.4.1.2 Ciphertext Size

Ciphertext ($\hat{C}$) size is the total size of secure message transmitted to the network including: the encrypted data, signature and any additional cryptographic parameters attached to enable

recovering the plaintext. In the proposed scheme, the ciphertext $\hat{C} = (\bar{M}, \sigma)$, where $\bar{M}$ is the encrypted data and σ is the ECDSA signature. AES encryption does not enlarge data size; therefore M and $\bar{M}$ both have the same size. The signature σ has two components (as per ECDSA details discussed in section 4.3); hence the signature size is twice the length of the elliptic curve. Therefore, the ciphertext size is $|M| + |point|$. On the other hand, the ciphertext produced by IBS is $\hat{C} = (C, C_{enc}, C_{sign})$. C and C_{sign} are each twice the size of the elliptic curve as they are points on the curve. The scheme does not expand encrypted data too, therefore the size of the plaintext and C_{enc} are the same. The total length of the ciphertext under signcryption scheme will be $|M| + 2|point|$. Assuming a plaintext size of 16KB, Figure 4.4 illustrates the length of the resulting ciphertext under the proposed scheme and IBS when using different elliptic curve standards. The figure shows that the proposed scheme incurs lower ciphertext size.

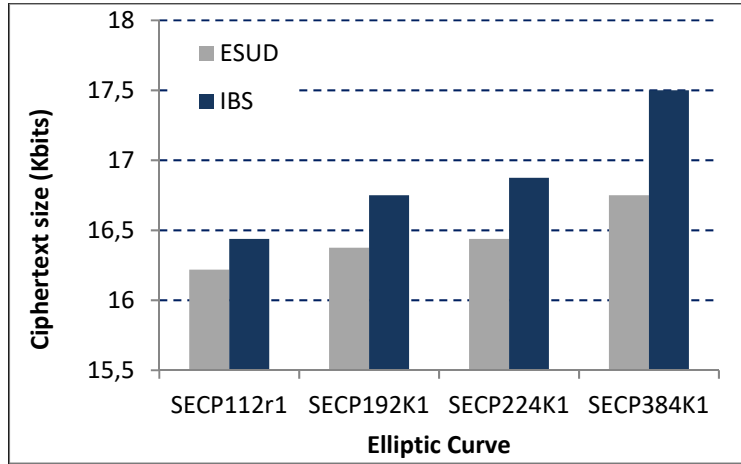


Figure 4.4 A comparison between our scheme and IBS in terms of ciphertext size

4.4.1.3 Storage Overhead

Storage overhead is the size of cryptographic information the communicating parties need to store so that they can establish a secure communication. First, we analyze the storage overhead of the two schemes in terms of the total number of keys D_{LL} and D_{HL} need to store. In our scheme, symmetric keys are used for encryption or decryption, while asymmetric keys are used

for signature generation and verification. In IBS symmetric keys are used to derive asymmetric keys that in turns used for encryption/decryption and signature generation/verification.

Table 4.4, shows the number of symmetric and asymmetric keys stored in each scheme. Our scheme requires to store more keys since it supports secure communication for unicast, multicast and broadcast transmission modes. However, IBS supports unicast downlink communication only. Therefore, the increase storage overhead is justified to accommodate extra transmission modes.

Table 4.4 Comparison of Keys Storage Overhead

	<i>SM</i>		<i>GW</i>	
	Symmetric keys	Asymmetric keys	Symmetric keys	Asymmetric keys
ESUD	4	$3 KP + 1 KS$	$2 L + N + 1$	$(L + N + 1)KS + L KP$
IBS	-	2	1	$1 PK + L SK$

Figure 4.5, shows the storage overhead on smart meters taking into consideration all cryptographic information that need to be stored including identifiers, nonce value, symmetric and asymmetric keys. In this simulation we assume that the size of identifier and nonce is 128bits each.

Obviously, the proposed protocol incurs high storage overhead as it supports uplink and downlink communication. In addition, our protocol requires the smart meters to store its identifier and nonce value to mitigate spoofing and replay attacks. IBS is not resilient against spoofing and replay attacks. Thus, we would like to think that the increased storage overhead is to support extra functionalities.

4.4.2 Security Analysis

The proposed scheme ensures the integrity, confidentiality and origin authentication for downlink and uplink communication in AMI network. This section demonstrates the security analysis of the proposed scheme under the adversarial model presented in section 4.4.2 by

examining its resiliency against known attacks. The analysis is based on the security services provided by the underlying cryptosystem.

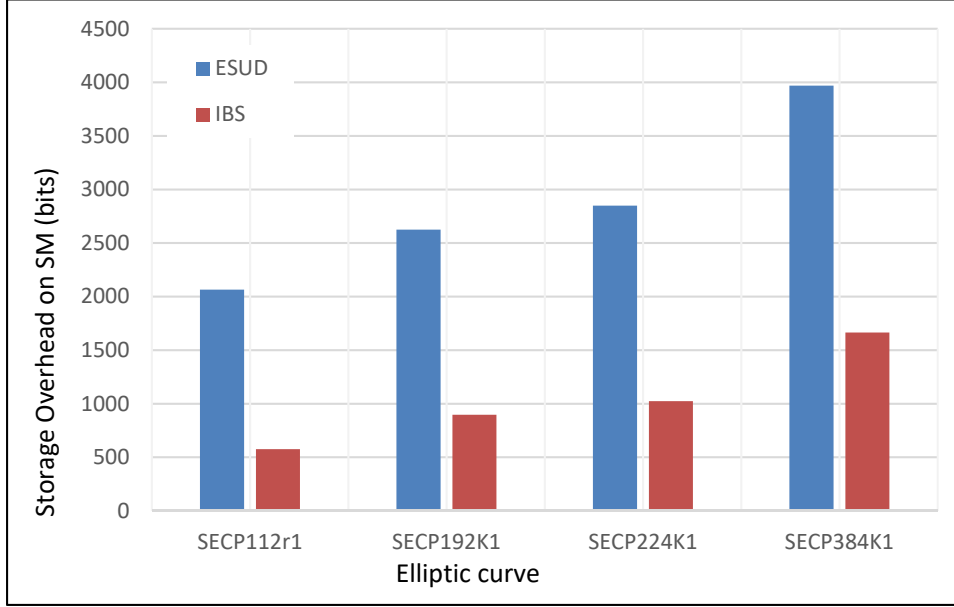


Figure 4.5 Storage overhead comparison

4.4.2.1 Resiliency Against Passive Attacks

The proposed protocol utilizes symmetric key cryptography to implement the encryption algorithm *SYMM.ENC* in order to guarantee data confidentiality. During the initialization phases, D_{HL} and D_{LL} computes a shared secret key K_{sh} to enable D_{HL} sharing the set of secret key $\{k_U, k_M, k_B\}$ securely with D_{LL} . Thus, a passive adversary $\mathcal{A}$ intercepting on the AMI communication channels will never be able to deduce the decryption keys necessary to reveal the content of any message. Accordingly, the proposed protocol maintains data confidentiality and customer privacy by guarding against passive adversaries.

4.4.2.2 Resiliency Against Impersonation Attack

An active adversary $\mathcal{A}$ can impersonate the identity of any network device if he manages to forge its' signature. In the proposed protocol, D_{HL} and D_{LL} exchanges the public keys $\{KP_{UD}, KP_{MD}, KP_{BD}, KP_{UU}\}$ securely before the beginning of any communication. In addition,

if any one of them decides to regenerate his public key pair, the new public key is never sent in clear. Thereby, $\mathcal{A}$ is not even given the chance to gather and cryptanalyze combinations of legitimate public keys/signatures for the purpose of forging valid signatures. Consequently, the proposed scheme is resilient against impersonation attack.

4.4.2.3 Resiliency Against Replay Attacks

Assuming a reliable communication protocol such as TCP/IP, the proposed protocol can easily thwart replay attack by using nonce. D_{HL} and D_{LL} should not encounter the same nonce value twice as the values are generated in an increasing order from an initial nonce N_0 . Therefore, a replayed message by the adversary $\mathcal{A}$ is detected when $N_t \leq N_{t-1}$. It should be noted that the attacker can't predict the current nonce value as the values are exchanged encrypted from an initial random nonce.

4.4.2.4 Resiliency Against Message Modification Attack

ECDSA is a secure public key algorithm because it is computationally infeasible to modify the message $\overline{M}_t$ and its signature σ_t to construct a new message with a valid signature (assuming the secure setup discussed in section 4.3). Therefore, with the use of collision free hashing function, $\mathbf{Vrfy}_{PK}(h_2(\overline{M}_t), \sigma_t)$ will output zero if the message or the signature (or both) are altered in transit. Hence, an adversarial attempt to manipulate signed ciphertext will not go undetected and message modification attack can't succeed against the proposed scheme.

4.4.3 Limitation of the proposed scheme

The proposed protocol achieves secure communication in the hierarchal AMI network by considering each traffic mode separately. Uplink traffic originated from D_{LL} need to be propagated to a single recipient, therefore one secret key with a pair of public keys are utilized to secure such traffic. In contrast, multi-recipient traffic originated from D_{HL} requires two symmetric group keys (k_M and k_B) to realize encryption and three pairs of asymmetric keys

to implement efficient authentication mechanism. Given that customers move dynamically from one demand response project to another, the proposed scheme may be not up to the mark in terms of the resulted key management overhead. Whenever a meter SM_i changes his preferred DR project, the corresponding multicast group key must be revoked. Meters in the original DR project should be assigned a new multicast group key to ensure the secrecy of future messages. In addition, SM_i is assigned new unicast and multicast group keys corresponds to the new DR he joined. Furthermore, when a meter is not longer a member of any DR projects (disconnected user), broadcast and multicast group keys must be revoked and new set must be generated. Knowing that AMI network is highly dynamic with the millions of users connected, these scenarios are not unreal at all. In fact, this is what motivated us to explore more efficient techniques for tackling the security threats of downlink communication in AMI networks.

4.5 Chapter Summary

AMI is the main automated architecture that empowers the smart grid brings the most efficient operation by implementing two-way communication between the utility headend and customers. This complex architecture comprises millions of heterogenous devices interconnected using wired and wireless communication technologies. This, in addition to the inherited weaknesses of the power grid opens the door for novel security threats that never existed in any other infrastructure. Therefore, security is an indispensable requirement to ensure reliable AMI operation.

In this Chapter, we provided a cryptographic based solution to ensure secure uplink and downlink communication in AMI networks. The proposed scheme takes into consideration the possible transmission mode of each communication scenario. Thus, AMI participants exchange secret keys and group secret keys in addition to other cryptographic parameters during setup phase. The proposed protocol maintains confidentiality of control center commands and the privacy of the metering reports by utilizing symmetric encryption. Furthermore, the protocol implements elliptic curve signature scheme to protect integrity and authenticity of AMI messages. Simulation results show that the proposed scheme is efficient

in terms of the computation overhead and ciphertext size. In addition, the scheme is resilient against passive, data modification, impersonation, and replay attacks.

The security of the proposed protocol requires keying procedure when a new user joins the multicast group and rekeying procedure when a user leaves the group. Knowing that AMI network is very dynamic as the customers respond to utility incentives by changing their consumption patterns and thereby the DR projects they are participating in, the performance of the proposed scheme may not be up to par in terms of key management overhead. Therefore, in the next chapter we propose a new mechanism to address the problem of secure data exchange for downlink AMI communication by utilizing attribute-based encryption.

CHAPTER 5

S-CP-ABE: A SIGNCRYPTION SCHEME BASED ON CP-ABE TO SECURE DOWNLINK MULTICAST COMMUNICATION IN AMI NETWORKS

5.1 Overview

Achieving secure data exchange is a key concern for AMI networks given the numerous attacks threatening this infrastructure. There are many researches to address the security issues in AMI networks, yet very few consider downlink communication. Most of the proposed schemes are designed to safeguard customer energy consumption reports to protect the consumer privacy and attain accurate billing. Downlink transmission transports control center pricing and management commands to customers for the purpose of ensuring reliable and efficient grid operation, thus requires equivalent or higher degree of security. In fact, this transmission occurs mainly in multicast mode between the utility headend and a group of smart meters and has different security requirements than uplink communication. The main security goal for this transmission is supporting efficient and anonymous access control. In many scenarios, the control center communicates information without knowing which users are eligible to view or act on this information. For example, the utility may trigger firmware update event without knowing which smart meters are qualified for this update. Therefore, an efficient multicast security scheme must ensure that the authorized group of smart meters only can decrypt the secure control center messages. Another important security goal is data integrity. In opposite to uplink data collection schemes where customer privacy is the main security concern, data integrity is crucial in downlink transmission as threats targeting data integrity can produce catastrophic results on the grid performance. In addition, the development of versatile key management protocols is an important security goal. There must exist a lightweight key management scheme to efficiently distribute and revoke the cryptographic keys according to the users joining and leaving the multicast domain. As we demonstrated in the previous chapter, the use of symmetric key cryptography to secure downlink transmission can result in a considerable key management overhead. For the reasons aforementioned, addressing security

issues for downlink transmission in AMI network competently requires taking into consideration different requirements and goals.

5.2 Mechanism Description and Design goals

In this chapter, we propose a new Signcryption scheme based on Ciphertext Policy Attribute Based Encryption (S-CP-ABE) to secure downlink data transmission in AMI networks. CP-ABE is promising relatively new encryption algorithm that features simplified key generation and distribution to permit efficient access control of the shared data. The proposed scheme is a variant of CP-ABE in which the ciphertext is constructed based on a Boolean formula over a set of attributes. For this encryption system, every user is assigned a set of attributes and the secret keys of each user are generated according to those attributes. Attributes are managed by a central entity called attribute authority that is responsible for the generation, distribution, and revocation of attributes. Figure 5.1 shows the architecture of a typical ABE system.

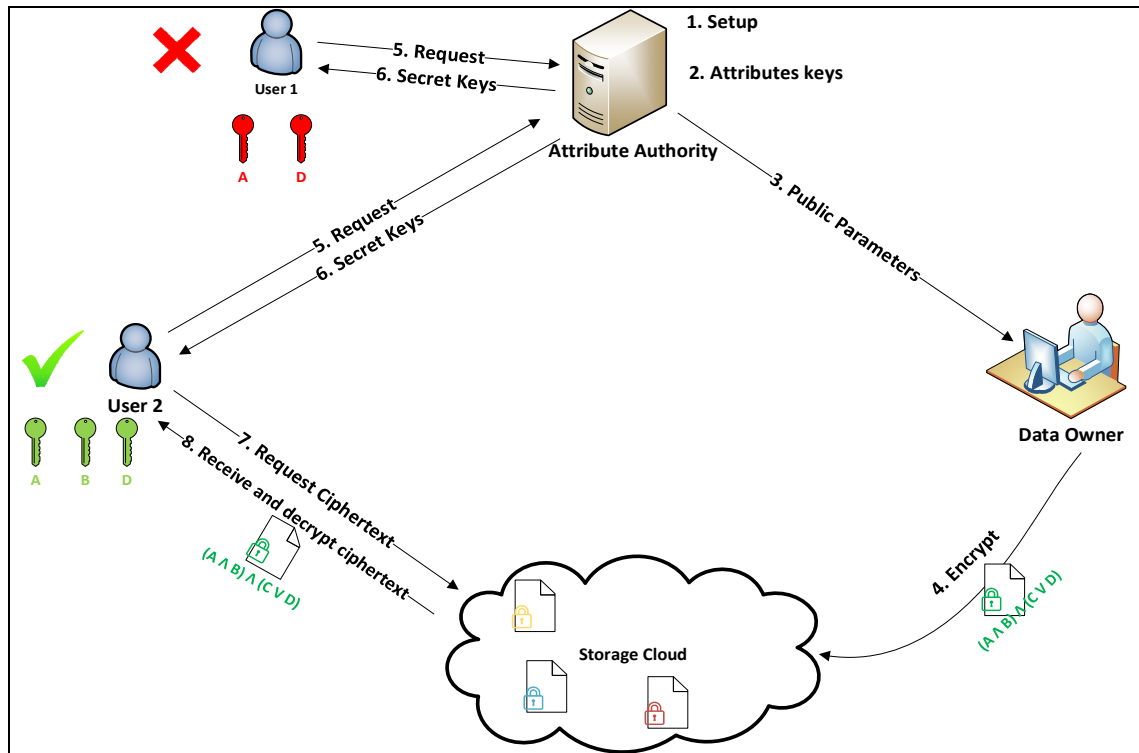


Figure 5.1 The typical architecture of CP-ABE scheme

Most ABE schemes found on the literature utilize bilinear pairings to construct or decrypt the ciphertext. This operation is known to be computation intensive and slow (Hong & Sun, 2016), (Li, Chen, Jiang, Li, & Li, 2016), (Li, Chen, & Sun, 2005). Thus the computation overhead of these ABE schemes is considered high compared to other public key cryptosystems. The proposed scheme is implemented without using bilinear pairing for encryption or decryption, yet it can achieve the same features of the traditional ABE schemes. In the context of our scheme, the control center is the data owner that will utilize the proposed signcryption algorithm to construct a ciphertext that will be propagated to a group of smart meters. Every smart meter owns a set of private decryption keys assigned to him from the attribute authority based on his attributes. A smart meter can decrypt the ciphertext if and only if he owns the secret keys correspond to the attributes that satisfies the Boolean formula used to generate the ciphertext. The proposed CP-ABE has the following principal prerequisite design goals:

1. Protect control center confidential data against unauthorized access by encrypting the data at the source and enforcing fine-grained access control so that eligible smart meters only can disclose the content of messages;
2. Implement the necessary cryptographic functions needed to enable the smart meters verify the integrity and authenticity of control center messages;
3. Defend against collusion attack by preventing multiple users from combining their private keys to recover a ciphertext that they cannot individually decrypt;
4. Redesign the traditional CP-ABE to tackle its computation efficiency by replacing the computation intensive pairing operations with faster elliptic curve scalar multiplications. Yet, the new ABE scheme utilizes flexible and expressive monotonic Boolean formulas for constructing the ciphertext;
5. Improve the overhead of attribute/user revocation of the traditional CP-ABE schemes by introducing centralized mechanism to rescind invalid users or attributes.

5.3 Preliminaries

Definition 1 (Access Structure (Beimel, 1996)). Let $\{P_1, P_2, \dots, P_n\}$ be a set of parties. A collection $\mathbb{R} \subseteq 2^{\{P_1, P_2, \dots, P_n\}}$ is monotone if $\forall B, C : \text{if } B \in \mathbb{R} \text{ and } B \subseteq C \text{ then } C \in \mathbb{R}$. A

monotone access structure is a monotone collection $\mathbb{R}$ of non-empty subsets of $\{P_1, P_2, \dots, P_n\}$ (i.e. $\mathbb{R} \subseteq 2^{\{P_1, P_2, \dots, P_n\}} \setminus \{\emptyset\}$).

- The sets in $\mathbb{R}$ are called the authorized sets, whereas the sets not in $\mathbb{R}$ are called unauthorized sets. In ABE schemes, parties' role is given by attributes, therefore the access structure comprises the authorized set of attributes. Throughout this chapter, access structure whenever mentioned refers to a monotone access structure.

- **Definition 2 (Linear Secret Sharing Scheme (LSSS) (Beimel, 1996)):** A secret sharing scheme π over a set of parties (P) is a linear secret scheme if:

- a. A vector over Z_q is generated from the shares of each party (P_i).
- b. There exists a matrix A of size $n \times l$ used to generate the shares. For each row x of the matrix ($x = 1, \dots, n$), the mapping function $\rho(i)$ with $\rho: \{1, \dots, n\} \rightarrow P$ maps the x th row of the matrix A to a party P for labeling purposes. Assuming the column vector $\vec{V} = \{s, r_2, r_3, \dots, r_l\}$, where s is the secret to be shared, $(r_2, r_3, \dots, r_l)$ are chosen randomly and $(s, r_1, r_2, \dots, r_l) \in Z_q$. Then $A\vec{V}$ is the vector of the n shares of secret s according to π . In this scheme, each party $\rho(i)$ holds the share $\lambda_i = (A\vec{V})_i$.

As discussed in (Beimel, 1996), every LSSS defined as above, enjoys linear reconstruction property. Assuming an LSSS for the access structure $\mathbb{A}$ and the authorized set P_A . Let I be the corresponding set of row number of the access structure $\mathbb{A}$ such that $I = \{i: \rho(i) \in P_A\}$. Then, according to the Monotone Span Program (MSP) (Beimel, 1996), the vector $(1, 0, 0, \dots, 0)$ is in the span of matrix A rows. Consequently, there exist constants $\{c_i \in Z_q\}_{i \in I}$ such that if $\{\lambda_i\}$ are the valid shares of the secret, then the secret s can be reconstructed by computing $s = \sum_{i \in I} c_i \lambda_i$ (since $\sum_{i \in I} c_i A_i = (1, 0, \dots, 0)$). LSSS matrices are advantageous in implementing monotone access structures in CP-ABE schemes. In the proposed scheme, the encryption algorithm accepts an access matrix A of secret shares. This matrix is constructed from an access tree that represents the monotonic boolean formula. We adapt the technique presented in (Lewko et al., 2011) to convert the access tree into a share matrix of size $n \times l$. The details of this technique are explained in Appendix A.

• Ciphertext-Policy Attribute Based Encryption (CP-ABE)

CP-ABE is a public key encryption scheme that exploits attributes to realize encryption, key generation and decryption. In this scheme, the ciphertext is generated using an access policy defined over a set of attributes. Every user is assigned a set of private decryption keys according to the attributes he owns, where an authorized user possesses set of attributes satisfying the access policy can decrypt the ciphertext. Practically, CP-ABE schemes consist of the following algorithms:

- 1- System Setup (Υ). This algorithm takes a security parameter Υ as an input and output the global system parameters $param$ required by the CP-ABE system;
- 2- Authority Setup ($param$) $\rightarrow k_x, k_y$. This is a randomized algorithm run by attribute authority to generate its asymmetric key pair. The public key is shared with other system entities while the secret key is kept secret. Additionally, every attribute in the attribute universe is assigned an asymmetric key pair;
- 3- Encrypt ($param, m, A, k_x$) $\rightarrow CT$. This randomized algorithm run by data owner (control center in the context of our scheme paper) to generate the ciphertext CT . The algorithm takes as input the global parameters $param$, the message to be encrypted m , access policy A defined over a set of attributes and authority public key k_x ;
- 4- Key Generation ($param, ID, i, k_y$) $\rightarrow SK_i$. The attribute authority runs this algorithm to generate a private decryption key corresponding to attribute i owned by the user identified as ID ;
- 5- Decrypt ($param, CT, \{SK_i\}$). A user with a set of attributes that satisfy the access policy use this algorithm with the corresponding secret keys $\{SK_i\}$ to decrypt the ciphertext CT and recover the message m .

5.4 The Proposed CP-ABE Signcryption Scheme

In order to maintain confidentiality, integrity, and authenticity of control center messages and provide the smart meters with fine-grained data access, we present a new attributed-based signcryption scheme. In the proposed scheme, the control center is the data owner that utilizes our ABE to encrypt his messages using an access matrix A that is obtained from a monotonic access structure defined over a set of attributes. To do so, the control center uses a random secret

s to pair his plaintext with using *bitwise xor* operator and then encrypts the secret using our new CP-ABE scheme that we will discuss later in this section. The constructed ciphertext is signed using an elliptic curve signature scheme in order to guarantee its' authenticity and integrity.

On the other hand, smart meters represent data users in which each smart meter is labeled with a set of descriptive attributes and is assigned a set of private keys corresponding to those attributes. As in any ABE scheme, the attribute authority is the entity responsible for creating, distributing and managing system attributes. Every smart meter that owns a set of attributes satisfying the access policy used in encryption can recover the secret s (and thus decrypt the ciphertext) if and only if it receives a token from the attribute authority. The novelty of the proposed CP-ABE scheme lies behind the fact that it is an elliptic curve cryptosystem that is pairing free, in opposite to most ABE schemes. Instead of the complex bilinear pairing operations, we exploited faster elliptic curve scalar-point multiplication operations to construct the proposed CP-ABE signcryption model. In this section, we discuss the presumed network and threat models and present a detailed description of the proposed scheme. The list of notations used in this section is depicted in Table 5.1.

5.4.1 The Network Model

We assume the AMI network model depicted in Figure 5.2, in which there are four main entities in this network:

- 1- Smart Meters (SM_s): they are electronic devices equipped with limited processing and storage capabilities. The meters mainly measure customers power consumption and report the readings to the company. In addition, they receive data and control messages from the last mile entities. In our scheme we assume downlink multicast communication, therefore smart meters are the data users as they try to decrypt the ciphertext multicasted from the utility control center;
- 2- Supervisory Control Center (SCC): this unit enables the service provider controlling the power grid by gathering the information reported from the smart meters. It can issue variety of power control commands to maintain the smart grid performance at the desired level;

Table 5.1 List of notations used in section 5.4

Notation	Meaning
σ	Ciphertext signature
$\rho()$	Function to map a row from matrix A to an attribute
θ	Threshold value to determine message validity
δ	Elliptic curve based signature algorithm (ex. ECDSA)
$\mathbb{G}$	Group of order q
$\mathcal{U}$	Attributes universe
$\mathcal{M}$	Multicast domain
$\mathcal{US}$	Set of all user attributes
$\mathcal{SS}$	Set of user attributes satisfying the access policy
v	Message (plaintext) size
m	Message (plaintext) generated by the control center
SID	The identifier assigned to the smart meter
PK	Attribute authority public key
A	LSSS access matrix of dimension $n \times l$
γ	Security parameter
$\hat{C}$	Ciphertext signed by control center
$ $	Concatenation operation
ω_A, Y_A	Attribute authority secret keys
τ_m	Timestamp assigned to message m
k_v	Signature verification public key
k_s	Control center private signing key
a_i, Y_A	The private key of attribute i
$SK_{i,SID}$	Secret key of attribute i given to smart meter SID
H_1, H_2, F	Hash functions
$C_0, C_{1,x}$	Ciphertexts generated by control center
AK_i	The public key of attribute i
D_x	Decryption token of attribute x
s	Secret value
i	Attribute identifier

For example, it can issue a load shedding command to avoid the installation of capacity to supply the peaks of a highly variable loads. As well, SCC enables the service provider controlling the energy cost by multicasting pricing information updates. As we will explain in the next sections, *SCC* signcrypts data before multicasting it to the smart meters.

3- Gateways (GW_s): these intermediary entities bidirectionally route data between the smart meters and SCC;

4- **Attribute Authority (AA):** In our scheme, we use attribute-based encryption to ensure secure and fine-grained data access for the smart grid downlink multi-recipient communication. In this case, data owner (*SCC*) will encrypt the data using a predefined access policy and only data users (smart meters) who owns the attributes that satisfy the access policy can decrypt the ciphertext. Therefore, attribute authority plays a significant role in our proposed scheme since it's the unit responsible for assigning attributes to users. For each smart meter, it generates a set of private keys based on the assigned attributes and securely communicates the keys with him. Besides, (*AA*) controls the process of revoking users who leave the multicast domain or attributes that are no longer supported.

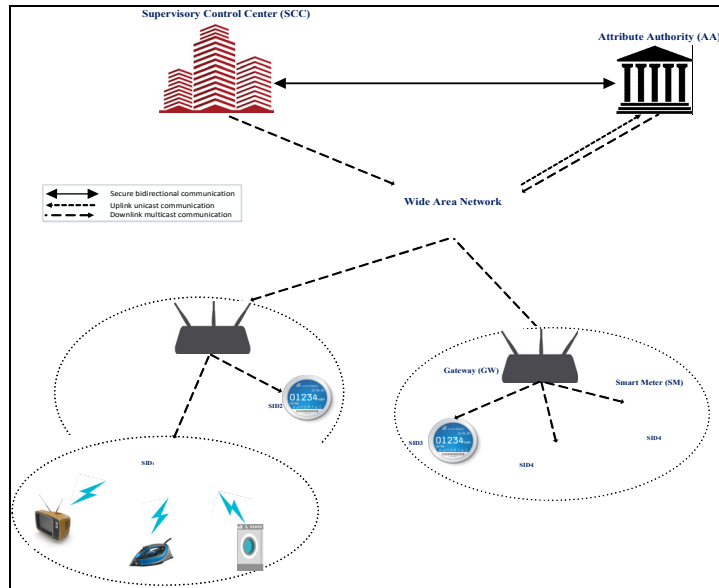


Figure 5.2 AMI network model for the proposed signcryption scheme

5.4.2 The Adversarial Model

There exists a polynomial time adversary $\mathcal{A}$ who possess the knowledge and the computation power to launch numerous passive and active attacks. $\mathcal{A}$ may try to breach customer privacy by eavesdropping on the communication channels. He may try to reveal the content of control center

messages multicasted to a group of smart meters. In addition, $\mathcal{A}$ may try to fabricate falsified messages and inject them into the network. The adversary (or any user) may collude with other users so as to decrypt a ciphertext that they cannot decrypt individually. Finally, $\mathcal{A}$ may fraudulently replay outdated network messages to produce undesirable effects. For instance, $\mathcal{A}$ may replay obsolete control or pricing information related to peak shaving to force the power grid customers reduce their energy consumption. In the proposed scheme we assume that the control center and attribute authority are both fully trustful entities.

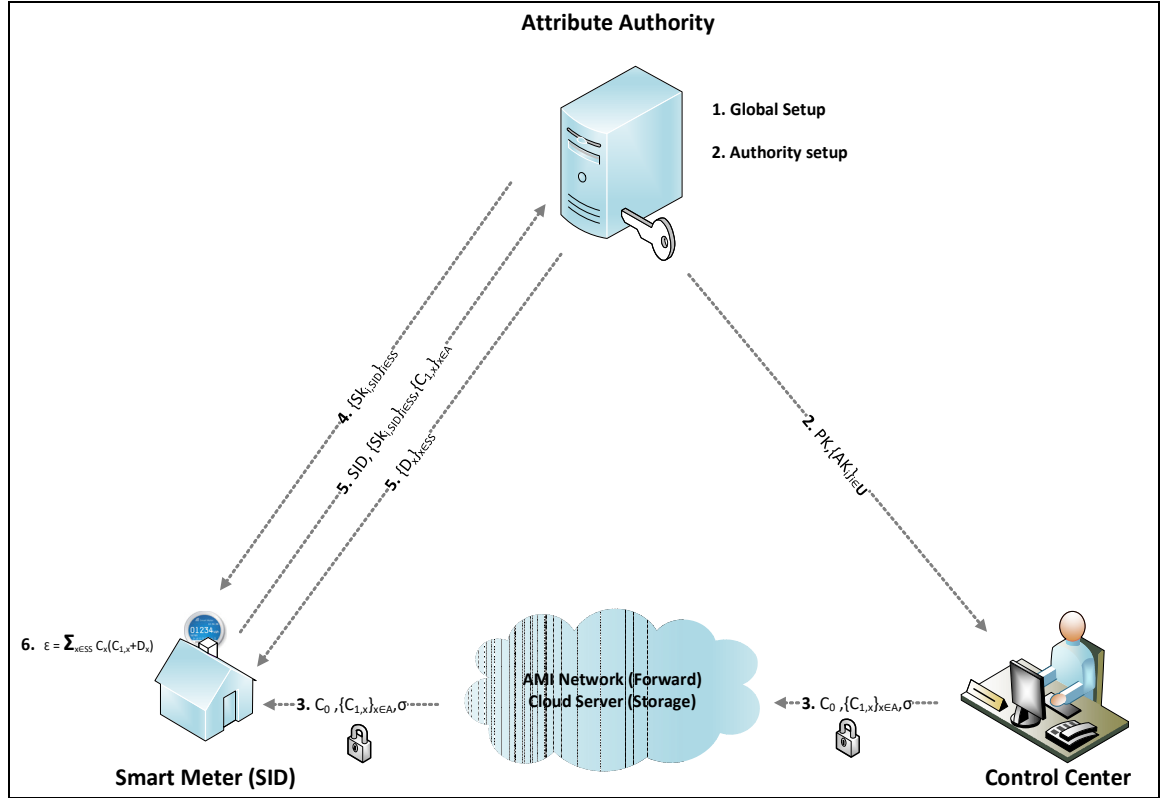


Figure 5.3 The steps of the proposed signcryption scheme

5.4.3 The Details of the Proposed S-CP-ABE

The proposed S-CP-ABS scheme runs in six stages: global setup, authority Setup, control center setup, signcryption, key generation, and designcryption. In this section, we demonstrate the

details of each one of those steps. Figure 5.3 summarizes the operation of the proposed signcryption scheme.

5.4.3.1 Global System Setup ($\mathcal{Y}$)

At this stage, a randomized algorithm takes the security parameter ($\mathcal{Y}$) and outputs the system global parameters such as the elliptic curve parameters, the hashing functions, and the smart meters identifiers SID_j . The details of this algorithm are shown in Algorithm 5.1.

Algorithm 5.1 Global Setup($\mathcal{Y}$)

1. Choose a multiplicative cyclic subgroup $\mathbb{G}$ of an elliptic curve with prime order q where G is the group generator
2. Select three hash functions as a random oracle
 $H_1: \mathbb{G} \rightarrow \{0,1\}^v$, $H_2: \mathbb{G} \rightarrow \{0,1\}^*$, $F: \{0,1\}^* \rightarrow Z_q$
3. Select a mapping function $\rho(i)$ with $\rho: \{1, \dots, n\} \rightarrow i$
4. Choose a signature algorithm δ
5. **for** each smart meter j in multicast domain $\mathcal{M}$ **do**
6. assign a unique global identifier SID_j
7. **end for**
8. **Publish** the global parameters
 $GP = \{ \mathbb{G}, G, q, H_1, H_2, F, \delta, \{SID_j\} \forall j \in \mathcal{M} \}$

5.4.3.2 Authority Setup (GP)

As discussed previously, the attribute authority is a main entity in any ABE system since it's the entity responsible for creating and managing attributes; the building block of such encryption systems. In this stage, the authority generates its public key (PK) and the private key (MK) that is used to drive the users' decryption keys. Additionally, the authority defines the attributes universe $\mathcal{U}$ and assigns a set of attributes $\mathcal{US}$ for each smart meter SID_j . The details of authority setup stage are shown in Algorithm 5.2.

5.4.3.3 Supervisory Control Center Setup (GP)

In the proposed model, the Supervisory Control Center is the data owner that will generate and signcrypt the messages that will be multicasted to a group of smart meters. Therefore, during this phase the control center generates a private signing key k_s and a publish the corresponding public verification key k_v to all smart meters $SID_j, j \in \mathcal{M}$.

Algorithm 5.2 Authority_Setup(GP)

1. Choose two random secret values $\omega_A, Y_A \in Z_q$ such that $\omega_A \neq Y_A \neq 0$
2. **for** each attribute i in $\mathcal{U}$ **do**
3. choose random secret $a_i \in Z_q$
4. attribute i secret key is $a_i \cdot Y_A$
5. compute $AK_i = a_i \cdot Y_A \cdot G$
6. **end for**
7. **Publish** attributes public keys $\{AK_i\} \forall i \in \mathcal{U}$
8. The authority public key is published as $PK = Y_A G$
9. The authority master secret key is $MK = (\omega_A, Y_A)$

5.4.3.4 Signcryption: Ciphertext and Signature Generation (GP, m, PK, A, k_s)

The control center runs this randomized algorithm to generate the signed ciphertext that will be multicasted to the group of smart meters in $\mathcal{M}$. The algorithm takes as an input the global parameters GP , message m to be signcrypted of size v bits, authority public key PK which is embedded in all attributes keys $\{AK_i\}$, access matrix A of size $n \times l$ and the control center private signature key k_s . The signcryptor first constructs the access matrix A that is driven from a particular monotonic boolean formula defined over a set of attributes. We exploit the procedure presented in (Lewko et al., 2011) to convert the boolean formula into an access matrix. Then, it computes the ciphertext C_0 by blinding the message with a random point generated from a secret s . Next, for each attribute in the access policy, the control center computes a ciphertext $C_{1,x}$ using the corresponding row vector of the access matrix A_x , the column vector V , the attribute public key $AK_{\rho(x)}$ and a random value r . As we will see later, the set of ciphertexts $\{C_{1,x}\}$ enable the authorized set of smart meters recover the blinding factor required to decrypt the ciphertext

C_0 . The control center signs the ciphertext with his private key k_s using an elliptic curve signature algorithm. Finally, it shares the tuple $\{\rho(x), \{C_{1,x}\}, r\}_{\forall \rho(x) \in A}$ with the attribute authority to enable it generates decryption tokens for data users with satisfying set of attributes. The ciphertext $\hat{C}$ that is propagated to the smart meters comprises three components: $C_0, \{C_{1,x}\}$ and the signature σ . As pointed out earlier, we do not use any bilinear pairing operations in generating the signencrypted text, and thus no such operations are required for designcryption. Algorithm 5.3 describes the details of the signencryption procedure.

Algorithm 5.3 Signencryption (GP, m, PK, A, k_s)

1. Let A be the access matrix embedding the access policy
2. Choose the random secret $s \in Z_q$;
3. Compute $C_0 = m \oplus H_1(sG)$;
4. Choose the vector $V = (s, v_2, v_3, \dots, v_l)$ such that $(v_2, v_3, \dots, v_l) \xleftarrow{R} Z_q^{l-1}$
5. pick random $r \in Z_q$
6. **For** each row x in A **do**
7. Compute $V_x = A_x V$
8. Compute $C_{1,x} = V_x \cdot G - rAK_{\rho(x)}$;
9. **End For**
10. Generate the signature $\sigma = \delta \left(F \left(C_0 || H_2 \left(\{C_{1,x}\}_{\forall x \in A} \right) \right), k_s \right)$;
11. Securely share $\{\rho(x), \{C_{1,x}\}, r\}_{\forall \rho(x) \in A}$ with the attribute authority;
12. The signencrypted text is

$$\hat{C} = (C_0, \{C_{1,x}\}_{\forall x \in A}, \sigma)$$

5.4.3.5 Key Generation (GP, SID, MK, i)

In order to generate a key for attribute i that belongs to smart meter with identity SID , the attribute authority uses its secret key MK and the global parameters GP and the meter identifier SID . The user secret decryption key is computed as:

$$SK_{i,SID} = a_i Y_A F(SID)^{\omega_A} G \quad (5.1)$$

The term $F(SID)^{\omega_A}$ is included in the private key to prevent multiple users colluding their keys to gain access to a ciphertext that they can not decrypt individually. The authority securely shares the set of keys $\{SK_{i,SID}\}_{\forall i \in \mathcal{US}}$ with the corresponding smart meter SID .

5.4.3.6 Designcrypton: Signature Verification and Decryption ($GP, \hat{C}, \{SK\}_{i,SID}, k_v$)

The data user (smart meter) runs this algorithm to recover the signcrypted message m . The algorithm takes as an input: the global system parameters GP , the signed ciphertext $\hat{C}$, the set of decryption keys $\{SK\}_{i,SID}$ and the signer public key k_v . The message m could be recovered successfully if 1) The ciphertext is signed by control center secret key k_s 2) the signed ciphertext is not altered in transit 3) the designcryptor owns the decryption keys $\{SK_{i,SID}\}$ corresponding to the set of attributes $\{i\}_{i \in \mathcal{SS}}$ that satisfy the access policy used in encryption 4) the signcrypted text is not fraudulently replayed by an adversary. In the event that any of these four conditions is not met, the designcrypton algorithm outputs $\perp$. The details of signcrypton algorithm is depicted in Algorithm 5.4.

The decrypting smart meter first verifies the signatures (Algorithm 5.4: line 1) to make sure the message is indeed originated from the control center and its not altered while in transit. The meter then invokes Search function (Algorithm 5.4: line 6) to check $\mathcal{US}$ to identify a subset of attributes with secret keys $\{SK_{i,SID}\}$ for a subset of rows $\{A_x\}$ of A such that $(1,0,0, \dots, 0)$ is in the span of these rows. Accordingly, the satisfying set $\mathcal{SS} \subseteq \mathcal{US}$ is constructed with those attributes satisfying the access policy if no satisfying set is found the meter will not be able to decrypt the ciphertext. Next, the smart meter uses the generated set to request a decryption token from the attribute authority. The authority verifies the validity of the request by checking whether the submitted set $\mathcal{SS}$ satisfies the access policy and if the smart meter SID indeed possesses the attributes in the submitted set. If the request is found to be valid, the authority securely shares the decryption token $\{D_x\}_{x \in \mathcal{SS}}$ with the corresponding smart meter SID (Algorithm 5.4: line 7). The smart meter can then decrypt the ciphertext by computing $C_{1,x} + D_x$ for each attribute in $\mathcal{SS}$ (Algorithm 5.4: line 11). Using the reconstruction property discussed in section 5.3, the smart meter finds constants $\{C_x\}_{x \in \mathcal{SS}}$ such that $\sum_{i \in \mathcal{SS}} c_{i \in \mathcal{SS}} A_{i \in \mathcal{SS}} = (1,0, \dots, 0)$ to calculate the value ϵ that enables him to recover the message m (Algorithm 5.4: line 13-15). Finally, the smart meter checks the recovered message to determine if the message is maliciously replayed by examining the timestamp (τ_m) and validity (θ) fields.

Algorithm 5.4 Designcrypton ($GP, \hat{C}, \{SK\}_{i,SID}, k_v$)

```

1. IF ( $\delta^{-1} \left( F \left( C_0 || H_2 \left( \{C_{1,x}\}_{\forall x \in A} \right) \right), k_v, \sigma \right) == 1$ )
2.     Go to step 6
3. ELSE
4.     Output  $\perp$ 
5. END IF ELSE
6.  $\mathcal{SS} \leftarrow \text{Search}(A, \{SK_{i,SID}\}_{\forall i \in \mathcal{US}})$ 
7.  $\{D_x\}_{x \in \mathcal{SS}} \leftarrow \text{Request\_Token}(SID, \{SK_{i,SID}\}_{\forall i \in \mathcal{SS}}, \{C_{1,x}\}_{\forall x \in A})$ 
8. IF ( $\{D_x\}_{x \in \mathcal{SS}} == \{\emptyset\}$ )
9.     Output  $\perp$ 
10. ELSE
11.     Calculate  $\sum_{x \in \mathcal{SS}} (C_{1,x} + D_x)$ 
12. END IF ELSE
13. Select constants  $C_x \in Z_q$  such that  $\sum_x C_x A_x = (1, 0, 0, \dots, 0) \quad \forall x \in \mathcal{SS}$ 
14. Calculate  $\epsilon = \sum_{x \in \mathcal{SS}} C_x (V_x G - rAK_{\rho(x)} + D_x)$ 
15. recover the plaintext  $m = C_0 \oplus H_1(\epsilon)$ 
16. IF ( $\tau > \tau_m + \theta$ )
17.     Output  $\perp$ 
18. ELSE
19.     Output plaintext  $m$ 
20. END IF ELSE

```

5.5 The Correctness Proof of The Proposed Scheme

Upon verifying the signature σ and receiving a valid decryption token from the attribute authority, the smart meter can proceed in decrypting the ciphertext. Here, we show that the proposed protocol is correct in recovering message m .

The decryption token corresponds to attribute x in the satisfying set $\mathcal{SS}$ is given by

$$D_x = rF(SID)^{-\omega_A} SK_{x,SID} \quad (5.2)$$

Using the attribute set $\mathcal{SS}$ and the decryption token $\{D_x\}_{x \in \mathcal{SS}}$, the smart meter first computes:

$$\sum_{x \in \mathcal{SS}} C_{1,x} + D_x \quad (5.3)$$

$$= \sum_{x \in \mathcal{SS}} V_x \cdot G - rAK_{\rho(x)} + rF(SID)^{-\omega_A} SK_{x,SID} \quad \text{By Substituting (5.2)}$$

$$= \sum_{x \in \mathcal{SS}} V_x \cdot G - rAK_{\rho(x)} + rF(SID)^{-\omega_A} (a_i Y_A F(SID)^{\omega_A} G) \quad \text{By Substituting (5.1)}$$

$$= \sum_{x \in \mathcal{SS}} V_x \cdot G - rAK_{\rho(x)} + r a_i Y_A G \quad (5.4)$$

The two terms $r_x AK_{\rho(x)}$ and $r a_i Y_A G$ are equal as $AK_{\rho(x)}$ represents the public key of attribute x used during the signcryption operation and $a_i Y_A G$ represents the public key of attribute i in the satisfying set $\mathcal{SS}$. Therefore, (5.4) can be rewritten as

$$\epsilon = \sum_{x \in \mathcal{SS}} V_x \cdot G \quad (5.5)$$

Then, for the satisfying set of attributes $\mathcal{SS}$, the smart meter finds constants $\{C_x\} \in Z_q$ according to the reconstruction property discussed in section 5.3, so that the $(1,0,0,\dots,0)$ is in the span of the satisfying set of attributes (i.e. $\sum_x C_x A_x = (1,0,0, \dots, 0)$, where A_x is row x in access matrix A which corresponds to the same attribute in the satisfying set $\mathcal{SS}$. It then computes,

$$= \sum_{x \in \mathcal{SS}} C_x V_x \cdot G$$

$$= \sum_{x \in \mathcal{SS}} C_x A_x \cdot V \cdot G$$

$$= (1,0, \dots, 0) \cdot V \cdot G$$

$$= s \cdot G$$

Finally, the smart meter can recover the message as:

$$C_0 \oplus H_1(\epsilon)$$

$$= m \oplus H_1(s \cdot G) \oplus H_1(\epsilon)$$

$$= m$$

5.6 Performance Analysis

In this section, we evaluate the efficacy of the proposed signcryption scheme in terms of messages size, communication overhead and computation cost. We compare the performance of our protocol with the two CP-ABE schemes designed to secure AMI communications presented in (Ruj et al., 2013) and (Alsharif et al., 2019). We will refer to the former scheme as DSF and the later one as MA-ABSC. The notations used in this section is shown in Table 5.2.

Table 5.2 List of new notations used in section 5.5

Notation	Meaning
$ \mathbb{G} $	The size of an element in $\mathbb{G}$
$ \mathbb{G}_p $	The size of an element in the pairing group $\mathbb{G}_p$
$ \cdot $	Length of attribute set (given as $ \mathcal{U} $, $ \mathcal{US} $ or $ \mathcal{SS} $)
T_G	Time to perform exponentiation or multiplication in $\mathbb{G}$
T_{GT}	Time to perform exponentiation or multiplication in $\mathbb{G}_T$
T_P	Time to calculate one bilinear pairing operating

5.6.1 Message Size

As explained in the previous sections, ABE schemes run in multiple phases. Usually, system setup is done once and before any communication takes place, while designcryption is done without the need to exchange any messages with other entities. Therefore, we analyze the size of parameters and messages exchanged during authority setup, private keys generation and signcryption stages. In the proposed scheme and during authority setup phase, the secret values $(MK, \{a_i\}_{i \in \mathcal{U}})$ and the public values $(PK, \{AK\}_{i \in \mathcal{U}})$ are generated. Since only public keys are shared with other entities in the network, the total size of parameters exchanged during this phase is $(|\mathcal{U}| + 1)|\mathbb{G}|$. In key generation phase, each smart meter will receive a key $SK_{i, SID}$ for every attribute i he owns. Therefore, the total size of keys every meter will receive from the attribute authority is $|\mathcal{US}| \cdot |\mathbb{G}|$. During signcryption phase, the control center multicasts the signcrypted cipher $\hat{C}$ to the smart meters in the multicast domain $\mathcal{M}$. Fig 5.4 shows the format of this cipher that is generated by algorithm 5.3. The ciphertext size is $n|\mathbb{G}|$ and the signature

size is $|\mathbb{G}|$. Therefore, the total size of the signcrypt text published in the network is $(n + 1)|\mathbb{G}|$.

C_0	$\{C_{1,x}\}$				σ
  	$C_{1,1}$	$C_{1,2}$		$C_{1,n}$	$H_MAC_{k_s}(C_0, \{C_{1,x}\})$

Figure 5.4 Ciphertext format in the proposed signcryption scheme
shaded fields are encrypted.

Table 5.3 shows a comparison between our protocol, DSF, and MA-ABSC in terms of messages size generated during different phases of CP-ABE. It is easy see that the proposed S-CP-ABE scheme achieves the smallest message size during all phases of CP-ABE. knowing that the communication channels in AMI networks are shared between millions of users, achieving small messages size is important in avoiding congestion. In addition, the data owner may construct the ciphertext and upload it to a cloud server so that it remains available for a long time. Therefore, a small ciphertext size is a very desirable feature for many applications.

Table 5.3 Comparison of messages size for different CP-ABE schemes

Scheme \ Step	MA-ABSC	DSF	S-CP-ABE
Authority Setup	$ \mathcal{U} (\mathbb{G} + \mathbb{G}_P)$	$ \mathcal{U} (\mathbb{G} + \mathbb{G}_P)$	$(\mathcal{U} + 1) \mathbb{G} $
Encryption	$(n + 1) \mathbb{G}_P + 2n \mathbb{G} $	$(n + 1) \mathbb{G}_P + 2n \mathbb{G} $	$n \mathbb{G} $
Key Generation	$2 \mathbb{G} $	$ \mathbb{G} $	$ \mathbb{G} $
Signcryption	$(n + 1) \mathbb{G}_P + (2n + 1) \mathbb{G} $	—	$(n + 1) \mathbb{G} $

5.6.2 Communication and Revocation Overhead

In our scheme, the control center shares $\{\rho(x), \{C_{1,x}\}, r\}_{\forall \rho(x) \in A}$ with the attribute authority in signcryption phase to enable it construct the decryption tokens for eligible users. Furthermore, an authorized user can decrypt the ciphertext if and only if he obtains a decryption token $\{D_i\}_{i \in \mathcal{SS}}$ from the attribute authority during designcryption phase. Apparently, this will introduce additional communication cost compared to the conventional ABE schemes.

However, the proposed scheme substantially reduces the communication overhead in the event of attribute/user revocation. Traditional ABE schemes incur considerable communication overhead to update the decryption keys of all system users in the event of attribute revocation. The cost is incredibly higher to revoke a user by invalidating all of his attributes. However, our scheme supports simple and efficient centralized revocation without incurring any communication cost on the data users. The attribute authority in our scheme can effectively revoke attribute/user by simply updating the corresponding attribute list without the need to modify the keys of other users in the system. In accordance to that, no decryption token will ever get issued to a revoked user or attribute. As a result, it is evident that our scheme achieves better performance in terms of the overall communication overhead.

5.6.3 Computation Overhead

In the context of AMI security, the computation overhead of the security protocols is an important performance factor for mainly two reasons: 1) the smart meters are equipped with limited storage and processing capabilities which makes them intolerant to large spectrum of complex and computation intensive encryption schemes 2) most of the applications implemented in AMI networks are time-critical requiring minimal processing delays. In this subsection, we evaluate the computation overhead of the proposed scheme and we compare it with the other two CP-ABE protocols. The three protocols are CP-ABE schemes that support monotone access structure and they use standard techniques to convert it into an LSSS matrix (Lewko et al., 2011).

Firstly, we are analyzing the complexity of the CP-ABE schemes by considering their cryptographic operations. The only cryptographic operations that we are taking into consideration are: exponentiation or multiplication in $\mathbb{G}$, exponentiation or multiplication in $\mathbb{G}_T$ and bilinear pairing operation. The time required to compute each one of these operations is represented as T_G , T_{GT} and T_p respectively. Compared to these three operations, other operations such as hashing, bitwise XOR and exponentiation or multiplication in Z_q are computationally inexpensive (Dai, 2009) and thus will be ignored.

In our scheme:

- **Authority Setup.** In this phase, the attribute authority computes public/private key pair for itself and for every attribute in the system. Generation a pair of keys requires one scalar multiplication in $\mathbb{G}$, therefore the total time required to run this setup phase is $(|\mathcal{U}| + 1)T_G$;
- **Key generation:** the attribute authority performs one scalar multiplication in $\mathbb{G}$ to compute the decryption key $SK_{i,SID}$ for each attribute i owned by user SID . The total time required to generate all secret keys for a single user is $|\mathcal{US}|T_G$;
- **Signcryption:** the control center (data owner) performs: one scalar multiplication in $\mathbb{G}$ to compute C_0 , another two multiplications to calculate each $C_{1,x}$ and additional multiplication to compute the signature σ . Therefore, the computation overhead for generating the signcrypted text is $(2n + 2)T_G$;
- **Designcryption:** the smart meter (data user) performs two scalar multiplications in $\mathbb{G}$ to authenticate data origin. Next, the meter can request a decryption token from attribute authority if he manages to find a set of attributes $\mathcal{SS}$ satisfying the access policy. If meters' request is valid, the authority performs one multiplication in $\mathbb{G}$ for each attribute in $\mathcal{SS}$ to compute the decryption token. After receiving the token, the meter computes additional multiplication in $\mathbb{G}$ per attribute in satisfying set $\mathcal{SS}$ to recover the blinding value ϵ . Thus, the total computation overhead to validate the ciphertext and recover the message m is $(2 + 2|\mathcal{SS}|)T_G$.

Table 5.4 shows the results of the computational complexity comparison between our S-CP-ABE scheme and the other CP-ABE schemes. According to the rough estimate used in (Yao, Chen, & Tian, 2015), the computation overhead of one bilinear pairing operation is equivalent to 20 scalar multiplications in $(i.e. T_p = 20 T_G)$. Moreover, exponentiation in $\mathbb{G}_T$ is approximately four times slower than scalar multiplications in $\mathbb{G}$ (*i.e.* $T_{GT} = 4 T_G$) (Liu, Li, Yang, & Yang, 2014). By referring to Table IV, it should be evident that the proposed scheme outperforms the other two ABE schemes in terms of the computation overhead. This is because our proposal utilizes scalar-point multiplications on elliptic curves and do not employ slow pairing operations as in other protocols.

Table 5.4 Comparison of computation overhead for different CP-ABE schemes

Step \ Scheme	MA-ABSC **	DSF *	S-CP-ABE **
Authority Setup	$ \mathcal{U} (T_{GT} + T_G)$	$ \mathcal{U} (T_{GT} + T_G)$	$(\mathcal{U} + 1)T_G$
Encryption/Signcryption	$n(2T_{GT} + 3T_G) + T_P$	$2n(T_G + T_{GT}) + T_P$	$(2n + 2)T_G$
Key Generation	$2T_{GT}$	T_{GT}	T_G
Decryption/Designcryption	$ \mathcal{SS} T_{GT} + T_P$	$5 \mathcal{SS} T_{GT} + (2 \mathcal{SS} + 1)T_P$	$(2 + 2 \mathcal{SS})T_G$

* The scheme supports encryption

** The scheme supports Signcryption

In order to compare the computation overhead of the three schemes for different access policy sizes in experimental aspect, we implemented the protocols using Charm-Crypto library (Akinyele, German, Miers, Pagano, Rushanan, Green, & Rubin, 2013). It is a hybrid framework written in Python and C languages to enable rapid prototyping of advanced cryptosystems. For the experiments, we used a laptop equipped with Intel I7 processor running at 2.8GHz and 16GB RAM. We choose Type 1 symmetric pairing $(G_1 \times G_1 \rightarrow G_T)$ with 512-bits SuperSingular curve to implement the pairing-based protocols. For the implementation of our protocol, we used the 160-bits curve “*secp160k1*” $E: y^2 = x^3 + 7$ with the recommended parameters in (Certicom Research, 2010) over a base field of 512-bits.

Next, we run several experiments to evaluate encryption and decryption times for the different CP-ABE schemes and with variable access policy sizes. Figure 5.5, shows signcryption and designcryption time (encryption and decryption for the scheme in (Ruj et al., 2013) versus the number of attributes embedded in the access policy. In the context of our scheme, signcryption time is the time required by the control center to produce a signed ciphertext including the construction of C_0 , $\{C_{1,x}\}_{x \in A}$, and the signature σ . Whereas, designcryption time is the time incurred by the data user to recover the message m that includes signature verification time, the time incurred by attribute authority to generate the decryption token and the overhead of computing ϵ .

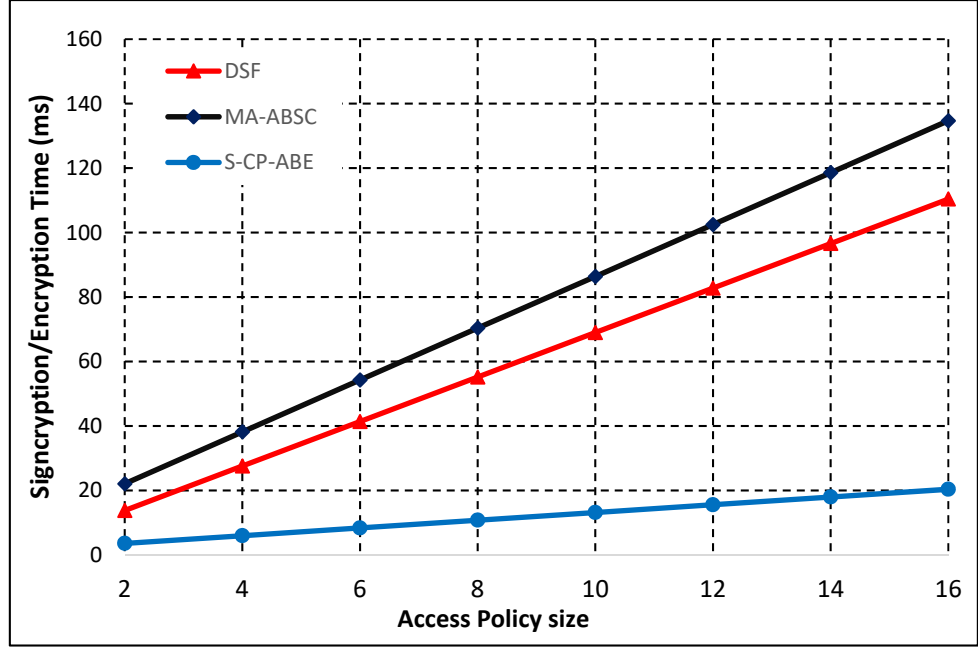


Figure 5.5 Signcryption/Encryption overhead comparison for different access policy sizes

Clearly, the encryption time increases as the number of attributes in the access policy increases because in ABE schemes the ciphertext is constructed over the set of attributes in the access policy. In our scheme, there exists a ciphertext $C_{1,x}$ for each attribute in the access policy, therefore increasing access policy size results in increasing the computation cost to produce the set $\{C_{1,x}\}_{x \in A}$.

Similarly, the decryption time increases as the number of attributes satisfying the access policy increases. As shown in Figure 5.6, the proposed scheme incurs the lowest computation time for signcryption and designcryption as we replaced the computation intensive pairing operations with much faster elliptic curve scalar multiplications. For this reason, the proposed scheme scales better with larger access policies and thus it suits the smart grid applications best as such applications require minimal processing delays.

5.7 Security Analysis

The proposed signcryption scheme purposes to maintain data confidentiality of control center messages by preventing unauthorized entities from disclosing the messages content.

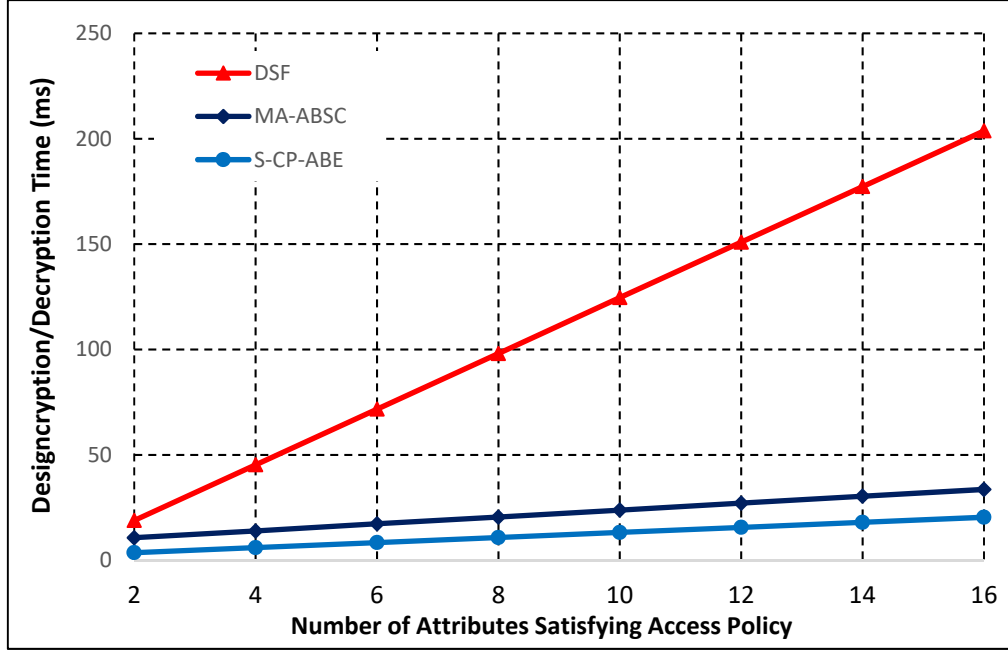


Figure 5.6 Designcrypton/Decryption overhead comparison for different access policy sizes

Only certain smart meters owning satisfying set of attributes can request decryption token from the attribute authority. Moreover, the signcrypton algorithm enables the transmitter signing the ciphertext so that the decrypting smart meter can verify data authenticity and infer if the data is not maliciously altered while in transit. In this subsection, we illustrate the security strength of the proposed signcrypton scheme by showing its resilience against several attacks. The analysis is based on the security services provided by the underlying cryptosystem.

5.7.1 Collusion Attack Resistance

This attack occurs if two or more data users try to combine their decryption keys to decrypt a ciphertext that no one of them can decrypt individually. In the proposed protocol, the user global identifier SID is involved in generating the secret decryption keys $\{SK_{i,SID}\}_{i \in US}$ and decryption tokens $\{D_i\}_{i \in ES}$. This ID is exclusive and can uniquely identify each smart meter in the network. As shown in the previous section, user secret keys and decryption tokens received from the attribute authority will always embed a single identifier SID . Therefore, if two or more data users combine their decryption keys, the decryption token D_x will not reduce to $(r a_i Y_A G)$ and in

this case the terms $\sum_x r AK_{\rho(x)}$ and $\sum_x r a_i Y_A G$ will not be equal and thus will not cancel out from $\{C_{1,x}\}$. In this case, Algorithm 5.4 will not output the term $\sum_{x \in \mathcal{S}} V_x \cdot G$ required for recovering the message (rather it will output $\perp$). Consequently, the proposed protocol thwart collusion attack.

5.7.2 Data Confidentiality

The proposed ABE protocol encrypts control center messages based on an access matrix A generated from a monotone boolean formula. As explained, authorized users with valid set of attributes can decrypt the ciphertext only after receiving a decryption token from the attribute authority. Before sharing a decryption token with a user, the authority determines if the user truly owns the secret keys corresponding to the submitted attributes. Therefore, unauthorized users will never be able to reveal ciphertext content which ensures the confidentiality of control center messages. Consequently, the proposed protocol is resilient against passive attacks.

5.7.3 Data Integrity and Signature Forgery

In addition to the fine-grained data access, our proposed protocol ensures data integrity of control center messages. An active adversary $\mathcal{A}$ may try to a) capture, modify and retransmit control center messages b) inject falsified messages to the AMI network c) launch replay attack by capturing valid control center messages to maliciously retransmit them later. In our scheme, we implemented hash-and-sign (algorithm 4.3) technique in which the signature $\delta\left(F\left(C_0 || H_2\left(\{C_{1,x}\}_{v_x \in A}\right)\right), k_s\right)$ is attached to every ciphertext generated by the control center. Therefore, any adversarial attempt to manipulate control center signcrypted messages will not go undetected. The data user will reject any message if the signature verification fails. In addition, algorithm 4.3 can detect fabricated messages injected by the adversary $\mathcal{A}$, because in our scheme the control center owns the private signing key k_s and thus it is the only entity capable of producing ciphertexts with valid signatures. Forging control center signature requires solving ECDLP to compute the private signing key k_s from the public key k_p which is infeasible. Finally, our scheme resists replay attack by including timestamp τ_m and threshold value θ in

every message. During signcryption, τ_m is examined to check whether the message was maliciously replayed or not. A message is considered obsolete and marked as replayed if $(\tau_m < \tau - \theta)$ where τ represents the current time. Therefore, replay attack cannot succeed in our scheme.

5.8 Chapter Summary

The security of AMI networks has been addressed in the literature, however the vast majority of the researches considered uplink single-recipient communication. However, In AMI networks, the utility headend utilizes downlink communication links to multicast necessary data and control information to a group of smart meters. The security of this type of communication requires enforcing efficient access control mechanism to ensure only authorized meters can retrieve control centers data. Secure multicast communication is a problem that is barely investigated in the context of AMI networks.

In this chapter, we proposed S-CP-ABE, an efficient signcryption scheme that integrates CP-ABE with additional security features to guarantee secure AMI downlink communication. The control center represents the data owner that exploits the proposed scheme to construct a ciphertext according to a certain access matrix that is obtained from a monotonic access structure defined over a set of attributes. The ciphertext is hashed and signed before disseminated into the network towards a group of meters. With the help of attribute authority, eligible smart meters who own a set of private keys correspond to the attributes that satisfy the access policy can decrypt the ciphertext. The novelty of the proposed signcryption scheme lies behind the fact that we improved the efficiency of the traditional ABE schemes by replacing the computation intensive bilinear operations with faster scalar-point multiplication over elliptic curves. We evaluated the efficiency of the proposed scheme in terms of computation overhead and messages size by comparing it with two CP-ABE schemes designed for AMI networks and the results prove the efficacy of the proposal. In addition, we demonstrated the strength of our protocol in defending against passive, collusion, reply, data modification and signature forgery attacks.

CONCLUSIONS AND FUTURE WORKS

Conclusions

Advanced Metering Infrastructure (AMI) is a central smart grid architecture that plays a vital role in realizing numerous modernized applications such as demand response, automated metering reading and remote management control by empowering bi-directional communication between the utility and its' customer. This architecture relies on violable devices such as smart meters and semi-open communication channels to exchange massive amount of sensitive information. This, in addition to the inherited weakness of the power grid paves the way to countless number of security threats that never existed in the legacy power grid. Being a part of an electricity system, AMI possess unique characteristics that puts challenging constraints on designing efficient security protocols to protect data exchange in its' networks. In this thesis, we address the need for secure data exchange in AMI networks by proposing cryptographic-based solutions to protect single and multiple recipient communications. In order to ensure the competency of the proposed schemes, we examined the transmission modes, types of messages exchanged, and security requirements for each one of these two communications.

Single-recipient communication represents the unicast data transmission of energy consumption reports from the smart meters towards the utility headend to ensure correct customer billing. We proposed HE-SSRU, a hybrid encryption scheme that exploits the strength of public-key cryptography with the efficiency of symmetric cryptography to secure uplink communication between the smart meters and Utility Master Computer (UMC). The proposed scheme optimizes the performance of ECIES algorithm by introducing precomputation procedure to reduce the computation overhead of the scalar multiplication operations. HE-SSRU is designed to protect customer privacy, ensure integrity of metering data and mitigates several attacks such as relay and spoofing. Performance analysis shows that the proposed protocol is efficient in terms of computation, communication and storage overhead.

On the other hand, the control center utilizes multicast downlink communication channels to propagate critical control and data messages to a group of smart meters. This multi-recipient communication is harder to secure as it needs sophisticated key management protocols and efficient fine-grained access control mechanisms. In order to address the need for secure multicast transmission in AMI networks, we proposed a new signcryption scheme based on Ciphertext-Policy Attribute-Based Encryption (CP-ABE). The main security goal of the proposed scheme is to achieve anonymous access control with low key management overhead. The scheme permits the control center to determine the smart meters eligible for accessing the secure data by constructing the ciphertext according to an access policy defined over a set of attributes. Authorized meters with attributes satisfying the access policy can decrypt the ciphertext by obtaining a decryption token from the attribute authority. The protocol is different from most of the ABE schemes in the sense that we built it without using the complex bilinear pairing operations. Our scheme maintains confidentiality and authenticity of control center messages and is resilient against collusion, replay, and signature forgery attacks. In addition, it is efficient in terms of computation overhead and ciphertext size.

Future Work

In this thesis, we focused on cryptographic based approaches to secure AMI communications, however there exist other non cryptographic techniques to enhance network security. Here are some of the potential future research directions based on non cryptographic approaches:

- We plan to study the efficiency of non-cryptographic privacy preserving methods such as anonymization, obfuscation, and perturbation to determine if such methods can achieve the same security level of the cryptographic based schemes;
- There are some researches that investigated the efficiency of network coding in improving AMI security as the work in (Tonyali, Akkaya, Saputro, & Cheng, 2017), but these researches are still in the baby steps. We would like to investigate the efficiency of applying network coding strategies to achieve peer-to-peer authentication between AMI devices and improve the security of metering data collection schemes;

- Nowadays, Intrusion Detection Systems (IDSs) are indispensable in any large-scale distributed computing environments for detecting unusual traffic. Knowing that smart meters are usually installed unattended at the customers' premises, they are subject to compromise. Therefore, IDS could be beneficial in detecting abnormal traffic generated by a compromised node. We would like to investigate the efficiency of implementing anomaly-based IDSs constructed specifically using Support Vector Machines (SVMs) and Neural Networks (NNs).

APPENDIX I

ELLIPTIC CURVE ARITHMETIC

An elliptic curve is defined by a cubic equation with two variables and some coefficients. In cryptography, the variables and coefficients have to be limited to elements of finite field. The cubic equation that controls elliptic curves takes a form known as *Weierstrass* equation that is given by:

$$y^2 + axy + by = x^3 + cx^2 + dx + e \quad (\text{A1.1})$$

In this research, we will limit ourselves to the prime elliptic curves that are defined over $\mathbb{F}_q$ (non negative integers less than the prime number q) using a reduced Weierstrass equation given by A1.2

$$y^2 \bmod q = (x^3 + ax + b) \bmod q \quad (\text{A1.2})$$

For these curves, variables and coefficients take values in the range of $[0, q - 1]$ and the discernment $\Delta \neq 0$ such that:

$$\Delta = (4a^3 + 27b^2) \bmod q \neq 0 \bmod q \quad (\text{A1.3})$$

The notation of $E_q(a, b)$ is used to describe the elliptic curve defined over $\mathbb{F}_q$ with the coefficients a and b . Such curve consists of all pairs of integers (x, y) , in addition to the point of infinity (O) as given in equation A1.4.

$$E(Z_q) \stackrel{\text{def}}{=} \{(x, y) | x, y \in Z_q \text{ and } y^2 = x^3 + ax + b \bmod q\} \cup \{O\} \quad (\text{A1.4})$$

For instance, $E_{37}(-5, 8)$ has 45 points, the point of infinity (O) in addition to the set of numeric points as shown in Figure A1.1

For the points $P, Q, R \in E_q(a, b)$, the following algebraic rules are used for addition and multiplication:

$$1- P + O = P; \quad (\text{A1.5})$$

$$2- P + (-P) = (X_p, Y_p) + (X_p, -Y_p) = O; \quad (\text{A1.6})$$

$$3- P + Q = (X_p, Y_p) + (X_q, Y_q) = R;$$

$$X_R = (\lambda^2 - X_p - X_q) \bmod q \quad (\text{A1.7})$$

$$Y_R = (\lambda(X_p - X_R) - Y_p) \bmod q \quad (\text{A1.8})$$

$$\lambda = \left(\frac{Y_q - Y_p}{X_q - X_p} \right) \bmod q \quad (\text{A1.9})$$

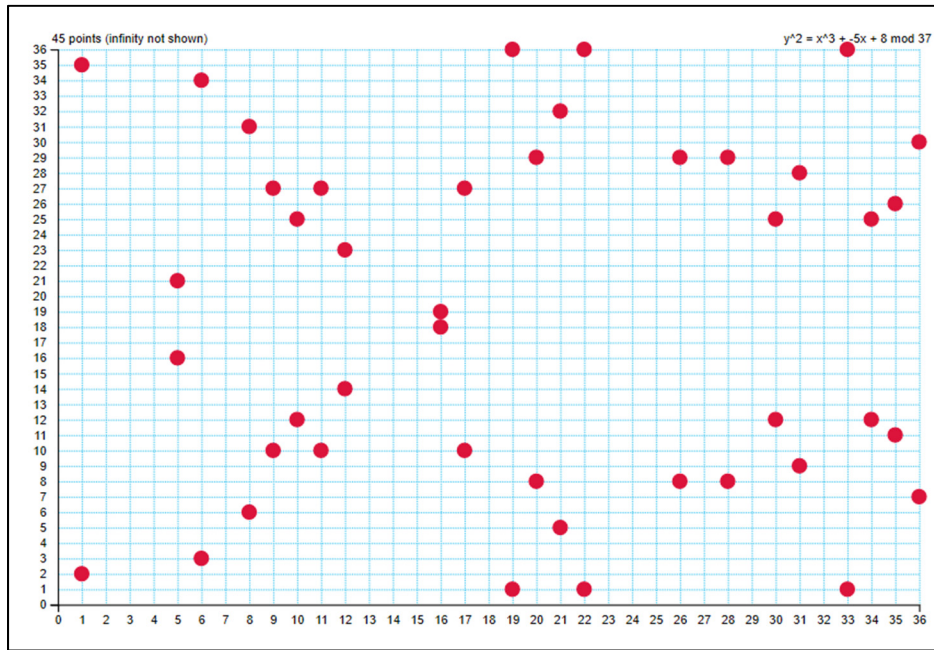


Figure A1.1 The points of Elliptic Curve $E_{37}(-5,8)$

4- Point Doubling: $P + P = 2P = 2(X_p, Y_p) = R$

$$\begin{aligned} X_R &= \lambda^2 \pmod{q} \\ Y_R &= (\lambda(X_p - X_R) - Y_p) \pmod{q} \\ \lambda &= \frac{3X_p^2 + a}{2Y_p} \pmod{q} \end{aligned} \quad (\text{A1.10})$$

5- Point multiplication: defined as repeated addition. For example: $4P = P + P + P + P$. In such way, we need 9 steps to calculate $200P$ as follows

- 1: $P + P \rightarrow 2P$
- 2: $2P + 2P \rightarrow 4P$
- 3: $4P + 4P = 8P$
- 4: $8P + 8P = 16P$
- 5: $16P + 16P = 32P$
- 6: $32P + 32P = 64P$
- 7: $64P + 64P = 128P$
- 8: $128P + 64P = 192P$
- 9: $192P + 8P = 200P$

APPENDIX II

CONVERTING MONOTONIC BOOLEAN FORMULA INTO LSSS MATRIX

The proposed ABE scheme exploits an access policy in the form of an access matrix to encrypts a message using a set of attributes. We used the algorithm presented in (Lewko et al., 2011) to convert an access tree (representing an access policy) into the equivalent LSSS matrix. The access tree is composed of nodes representing attributes and binary gates pairing the attributes. Leaf nodes in the access tree represent the attributes whereas the root and interior nodes are AND and OR gates. The algorithm labels the tree nodes and constructs the LSSS matrix from the labels assigned to the attributes. It starts by initializing a global counter to 1 and labeling the root node with a vector having value and length of 1. Then, every node (top to down) is assigned a vector (label) determined by parent's vector and as follows:

- a) Parent is an AND gate. The algorithm pads parents' vector by "0" if its length is smaller than counter value. Then, one of the children is labeled by parents vector concatenated with "1" and the other child is labeled by $(0,0,\dots,0)|-1$ where $(0,0,\dots,0)$ has a length equals to counter's value. Finally, the value of counter is incremented by 1;
- b) Parent is an OR gate. The algorithm labels both of its children by parent vector. The value of the counter is not updated. As an example, suppose we have the following monotonic boolean formula

$$(A \wedge E) \vee (B \wedge (C \vee D)) \quad (\text{AII.1})$$

The algorithm labels the root OR node by vector 1 and initializes the global counter to 1, as well. The two child's AND gates are labeled by the same vector (1) and the counter value remains the same.

Since left AND gate is labeled with a vector of same length as counter, it needs not to be padded with "0". Attribute A is labeled first by (1,1) while attribute E is assigned the vector (0,-1).

Then, the value of counter is incremented to 2. The vector's length of right AND gate has a length less than counter's value, so its padded with "0". Then, attribute B is assigned the vector (1,0,1) while OR gate is labeled by (0,0,-1). After that, the counter's value is incremented to 3. Attributes C and D are labeled by (0,0,-1) as their parent. The resulted labeled tree is shown in Figure A2.1.

Accordingly, the resulting LSSS matrix A is:

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & -1 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{bmatrix}$$

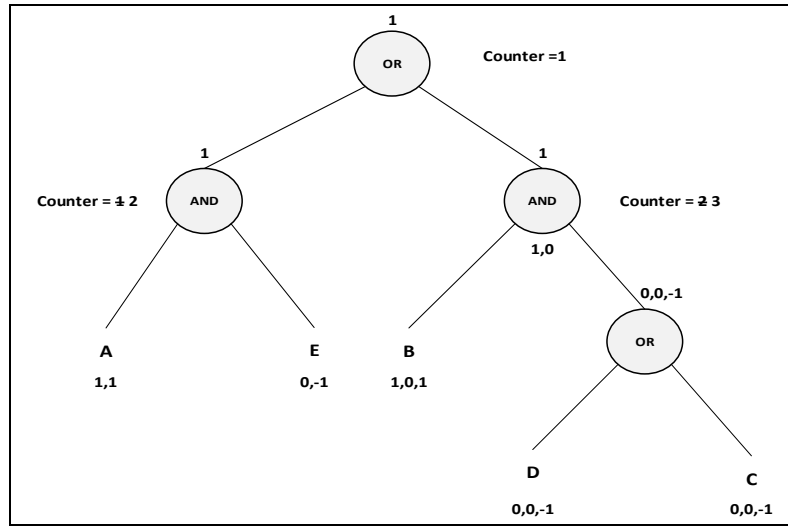


Figure A2.1 Access Tree Corresponding to Boolean Formula

Where the rows of LSSS matrix corresponds to attributes A, B, C, D and E respectively and the mapping function $\rho()$ is used to carry this mapping. Any subset of the rows includes (1,0,0) in its span, if the corresponding attributes in this subset satisfies the Boolean formula given in AII.1

APPENDIX III

LIST OF PUBLICATIONS

Journals:

Accepted and Published:

Khasawneh, S., & Kadoch, M. (2018). Hybrid Cryptography Algorithm with Precomputation for Advanced Metering Infrastructure Networks. *Mobile Networks And Applications*, 23(4), 982-993. DOI: 10.1007/s11036-017-0956-0

Submitted:

Khasawneh, S., & Kadoch, M. (2020). A Signcryption Scheme Based on CP-ABE to Secure Downlink Multicast Communication in AMI Networks. *Transactions on Emerging Telecommunications Technologies*.

Conferences:

Khasawneh, S., & Kadoch, M. (2017, Aug). *A Hybrid Encryption Scheme for Advanced Metering Infrastructure Networks*. Proceedings of the 1st EAI International Conference on Smart Grid Assisted Internet of Things, Sault Ste. Marie, Ontario, Canada. (PP. 982-993). DOI: 10.4108/eai.7-8-2017.152990.

Khasawneh, S., & Kadoch, M. (2018, Jul). *A Chain Based Signature Scheme for Uplink and Downlink Communications in AMI Networks*. International Conference on Smart Grid and Internet of Things, Niagara Falls, ON, Canada. (PP. 85-99).

LIST OF BIBLIOGRAPHICAL REFERENCES

- Abdalla, M., Bellare, M. & Rogaway, P. (2001, April). Cryptographers Track at the RSA Conference-CT-RSA 2001: Topics in Cryptology — CT-RSA 2001, San Francisco, CA, USA. (PP. 143-158)
- Abdullah, M. D. H., Hanapi, Z. M., Zukarnain Z. A., & Mohamed, M. A. (2015). Attacks, Vulnerabilities and Security Requirements in Smart Metering Networks. *KSII Transactions On Internet And Information Systems*, 9(4). DOI: 10.3837/tiis.2015.04.013
- Albu, M., Sanduleac, M., & Stanescu, C. (2017). Syncretic Use of Smart Meters for Power Quality Monitoring in Emerging Networks. *IEEE Transactions On Smart Grid*, 8(1), 485-492. DOI: 10.1109/tsg.2016.2598547
- Alharbi, K. & Lin, X. (2016, Dec). Efficient and Privacy-Preserving Smart Grid Downlink Communication Using Identity Based Signcryption. 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, USA. (PP. 1-6). DOI: 10.1109/GLOCOM.2016.7841770.
- Almimi, H., Samsudin, A., & Jahani, S. (2014). Elliptic-curve scalar multiplication algorithm using ZOT structure. *Security And Communication Networks*, 8(6), 1141-1154. doi: 10.1002/sec.1047
- Alohali B., Kifayat K., Shi Q., & Hurst W. (2016, May) *Replay Attack Impact on Advanced Metering Infrastructure (AMI)*. First International Conference, SmartGIFT 2016, Liverpool, UK. (pp. 52-59). DOI: 10.1007/978-3-319-47729-9_6
- Alsharif, A., Shafee, A., Nabil, M., Mahmoud, M., & Alasmary, W. (2019, July). A multi-authority attribute-based signcryption scheme with efficient revocation for smart grid downlink Communication. 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCoM) and IEEE Smart Data (SmartData), Atlanta, GA, USA, USA. (PP. 1025-1032). DOI: 10.1109/iThings/GreenCom/CPSCoM/SmartData.2019.00178.

- American National Standard for Financial Service. (2001). Public Key Cryptography for the Financial Services Industry Key Agreement and Key Transport Using Elliptic Curve Cryptography. (Report number X9.63–2001). Retrieved from <https://standards.globalspec.com/std/26827/X9.63>
- Ancillotti, E., Bruno, R., & Conti, M. (2013). The role of communication systems in smart grids: Architectures, technical solutions and research challenges. *Computer Communications*, 36(17-18), 1665-1697. DOI: 10.1016/j.comcom.2013.09.004
- Azarderakhsh, R., & Reyhani-Masoleh, A. (2013). High-Performance Implementation of Point Multiplication on Koblitz Curves. *IEEE Transactions On Circuits And Systems II: Express Briefs*, 60(1), 41-45. doi: 10.1109/tcsii.2012.2234916
- Bartoli, A., Hernández-Serrano, U., Soriano, M., Dohler, M., Kountouris, A. & Barthel D. (2010, Oct). *Secure Lossless Aggregation for Smart Grid M2M Networks*. 2010 First IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, USA. (pp. 333-338). DOI: 10.1109/SMARTGRID.2010.5622063
- Beimel, A. (1996). *Secure schemes for secret sharing and key distribution*. (PhD thesis, Israel Institute of Technology, Israel). Retrived from <https://www.cs.bgu.ac.il/~beimel/Papers/thesis.pdf>
- Benmalek, M. & Challal, Y. (2015, Aug). eSKAMI: *Efficient and Scalable Multi-group Key Management for Advanced Metering Infrastructure in Smart Grid*. 2015 IEEE Trustcom/BigDataSE/ISPA, Helsinki, Finland. (PP. 782-789). DOI:10.1109/Trustcom.2015.447
- Blazquez, J., Fuentes-Bracamontes, R., Bollino, C., & Nezamuddin, N. (2018). The renewable energy policy Paradox. *Renewable And Sustainable Energy Reviews*, 82, 1-5. DOI: 10.1016/j.rser.2017.09.002
- Boneh, D., & Franklin, M. (2003). Identity-Based Encryption from the Weil Pairing. *SIAM Journal On Computing*, 32(3), 586-615. DOI: 10.1137/s0097539701398521
- Boneh, D., Gentry, C. & Waters, B. (2005, Aug). Collusion Resistant Broadcast Encryption With Short Ciphertexts and Private Keys. 25th Annual International Cryptology Conference, Santa Barbara, California, USA. (PP. 258-275).

- Brown, D. (2000). The exact security of ECDSA. (Report Number CORR 2000-54). Retrived from https://uwaterloo.ca/combinatorics-and-optimization/sites/ca.combinatorics-and-optimization/files/uploads/files/2000_54.pdf
- Bthencourt, J., Sahai, A. & Waters, B. (2007,May). *Ciphertext-Policy Attribute-Based Encryption*. IEEE Symposium on Security and Privacy (SP '07), Berkeley, CA, USA. (PP.321-334). DOI: 10.1109/SP.2007.11
- Certicom Research. (2000). Standards for Efficient Cryptography SEC 2: Recommended Elliptic Curve Domain Parameters. (Report number SEC2.V1.0). Retrieved from <https://www.secg.org/SEC2-Ver-1.0.pdf>
- Clements S. & Kirkham H. (2010,Jul). *Cyber-security considerations for the smart grid*. IEEE PES General Meeting, Providence, RI, USA. (pp. 1-5). DOI: 10.1109/PES.2010.5589829
- Cleveland, F. M. (2008,Jul). *Cyber security issues for Advanced Metering Infrastructure (AMI)*. 2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, Pittsburgh, PA, USA. (PP. 1-5). DOI: 10.1109/PES.2008.4596535.
- Duan, R., & Deconinck, G. (2010, April). *Future electricity market interoperability of a multi-agent model of the Smart Grid*. 2010 International Conference on Networking, Sensing and Control (ICNSC), Chicago, IL, USA . (pp. 625-630). DOI:10.1109/ICNSC.2010.5461588
- Fan, C., Huang, S., & Lai, Y. (2014). Privacy-Enhanced Data Aggregation Scheme Against Internal Attackers in Smart Grid. *IEEE Transactions On Industrial Informatics*, 10(1), 666-675. DOI: 10.1109/tii.2013.2277938
- Ferrag, M. (2017). EPEC: an efficient privacy-preserving energy consumption scheme for smart grid communications. *Telecommunication Systems*, 66(4), 671-688. DOI: 10.1007/s11235-017-0315-2
- Finster, S., & Baumgart, I. (2015). Privacy-Aware Smart Metering: A Survey. *IEEE Communications Surveys & Tutorials*, 17(2), 1088-1101. DOI: 10.1109/comst.2015.2425958

- Fouda, M., Fadlullah, Z., Kato, N., Rongxing Lu, & Xuemin Shen. (2011). A Lightweight Message Authentication Scheme for Smart Grid Communications. *IEEE Transactions On Smart Grid*, 2(4), 675-685. DOI: 10.1109/tsg.2011.2160661
- Garg, S., Kaur, K., Kaddoum, G., Rodrigues, J., & Guizani, M. (2020). Secure and Lightweight Authentication Scheme for Smart Metering Infrastructure in Smart Grid. *IEEE Transactions On Industrial Informatics*, 16(5), 3548-3557. DOI: 10.1109/tii.2019.2944880
- Goyal, V., Pandey, O. Sahai, A. & Waters, B. (2006, Oct). *Attribute-based encryption for fine-grained access control of encrypted data*. Proceedings of the 13th ACM conference on Computer and communications security, Virginia, USA. (PP.89-98). DOI: 10.1145/1180405.1180418
- Hankerson, D., Vanstone, S., & Menezes, A. (2004). *Guide to elliptic curve cryptography*. New York: Springer.
- Hisock, J., and Beauvais, D. (2013). *Smart Grid in Canada 2012-2013*. (Report number 2013-171 RP-ANU 411-SGPLAN). Retrieved from <https://www.nrcan.gc.ca/sites/www.nrcan.gc.ca/files/canmetenergy/files/pubs/smart-grid-annual-report2012-2013-eng.pdf>
- Hong, H., & Sun, Z. (2016). High efficient key-insulated attribute based encryption scheme without bilinear pairing operations. *Springerplus*, 5(1). doi: 10.1186/s40064-016-1765-9
- Hu, C., Yu, J., Cheng, X., Tian, Z., Akkaya, K., & Sun, L. (2018). CP ABSC: an attribute based signcryption scheme to secure multicast communications in smart grids. *Mathematical Foundations of Computing*, vol. 1 (1), pp. 77-100.
- Järventausta, P., Repo, S., Rautiainen, A., & Partanen, J. (2010). Smart grid power system control in distributed generation environment. *Annual Reviews In Control*, 34(2), 277-286. DOI: 10.1016/j.arcontrol.2010.08.005
- Johnson, D., Menezes, A., & Vanstone, S. (2001). The Elliptic Curve Digital Signature Algorithm (ECDSA). *International Journal Of Information Security*, 1(1), 36-63. DOI: 10.1007/s102070100002

- Joux A. (2000,July).A One Round Protocol for Tripartite Diffie–Hellman.Algorithmic Number Theory - International Algorithmic Number Theory Symposium, Leiden, The Netherlands. (PP,385-393).
- Katz, J. & Lindell, Y. (2014). *Introduction to Modern Cryptography* . 2nd edition. United States: CRC Press Taylor & Francis group
- Khan R., McLaughlin K., Lavery J. H. D., David H. & Sezer S. (2018, Aug). *Demonstrating Cyber-Physical Attacks and Defense for Synchrophasor Technology in Smart Grid*. 16th Annual Conference on Privacy, Security and Trust (PST), Belfast, UK. (pp. 1-10). DOI: 10.1109/PST.2018.8514197
- Kim, J.& Choi, H. (2012, April). *An efficient and versatile key management protocol for secure smart grid communications*.2012 IEEE Wireless Communications and Networking Conference (WCNC),Paris, France. (PP. 1823-1828). DOI:10.1109/WCNC.2012.6214081.
- Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics Of Computation*, 48(177), 203-203. DOI: 10.1090/s0025-5718-1987-0866109-5
- Komninos, N., Philippou, E., & Pitsillides, A. (2014). Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures. *IEEE Communications Surveys & Tutorials*, 16(4), 1933-1954. DOI: 10.1109/comst.2014.2320093
- Kumar, P., Gurtov, A., Sain, M., Martin, A., & Ha, P. (2019). Lightweight Authentication and Key Agreement for Smart Metering in Smart Energy Networks. *IEEE Transactions On Smart Grid*, 10(4), 4349-4359. DOI: 10.1109/tsg.2018.2857558
- Kumar, P., Lin, Y., Bai, G., Paverd, A., Dong, J., & Martin, A. (2019). Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues. *IEEE Communications Surveys & Tutorials*, 21(3), 2886-2927. DOI: 10.1109/comst.2019.2899354
- Lenstra, A., & Verheul, E. (2001). Selecting Cryptographic Key Sizes. *Journal Of Cryptology*, 14(4), 255-293. DOI: 10.1007/s00145-001-0009-4

- Lewko, A. & Waters, B. (2011,May). *Decentralizing Attribute-Based Encryption*.EUROCRYPT: Annual International Conference on the Theory and Applications of Cryptographic Techniques,Tallinn, Estonia. (PP. 568-588).
- Li, F. & Luo, B. (2012,Nov). *Preserving data integrity for smart grid data aggregation* .2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm),Tainan,Taiwan.(PP.366-371). DOI:10.1109/SmartGridComm.2012.6486011.
- Li, H., Lu, R., Zhou, L., Yang, B., & Shen, X. (2014). An Efficient Merkle-Tree-Based Authentication Scheme for Smart Grid. *IEEE Systems Journal*, 8(2), 655-663. DOI: 10.1109/jsyst.2013.2271537
- Li, L., Chen, X., Jiang, H., Li, Z. & Li, K. (2016,Jun). P-CP-ABE: Parallelizing Ciphertext-Policy Attribute-Based Encryption for Clouds.2016 17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD),Shanghai, China. (PP. 575, 580). DOI: 10.1109/SNPD.2016.7515961
- Li, S., Xue, K., Yang, Q., & Hong, P. (2018). PPMA: Privacy-Preserving Multisubset Data Aggregation in Smart Grid. *IEEE Transactions On Industrial Informatics*, 14(2), 462-471. DOI: 10.1109/tii.2017.2721542
- Li, X., Chen, K., & Sun, L. (2005). Certificateless signature and proxy signature schemes from bilinear pairings. *Lithuanian Mathematical Journal*, 45(1), 76-83. DOI: 10.1007/s10986-005-0008-5
- Liu, D., Li, H., Yang, Y., & Yang, H. (2014,Jun). Achieving multi-authority access control with efficient attribute revocation in smart grid.2014 IEEE International Conference on Communications (ICC), Sydney, NSW, Australia. (PP.634-639). DOI: 10.1109/ICC.2014.6883390.
- Liu, N., Chen, J., Zhu, L., Zhang, J., & He, Y. (2013). A Key Management Scheme for Secure Communications of Advanced Metering Infrastructure in Smart Grid. *IEEE Transactions On Industrial Electronics*, 60(10), 4746-4756. DOI: 10.1109/tie.2012.2216237

- Liu, N., Chen, J., Zhu, L., Zhang, J., & He, Y. (2013). A Key Management Scheme for Secure Communications of Advanced Metering Infrastructure in Smart Grid. *IEEE Transactions On Industrial Electronics*, 60(10), 4746-4756. DOI: 10.1109/tie.2012.2216237
- Liu, T., Liu, Y., Mao, Y., Sun, Y., Guan, X., Gong, W., & Xiao, S. (2014). A Dynamic Secret-Based Encryption Scheme for Smart Grid Wireless Communication. *IEEE Transactions On Smart Grid*, 5(3), 1175-1182. DOI: 10.1109/tsg.2013.2264537
- Lu, Z., Lu, X., Wang, W. & Wang, C. (2010,Nov). Review and Evaluation of Security Threats on the Communication Networks in the Smart Grid.2010 Military Communications Conference,San Jose, CA, USA. (pp. 1830-1835). DOI:10.1109/MILCOM.2010.5679551
- Lynn, B. (2006). PBC Library. Retrieved from <https://crypto.stanford.edu/pbc/>
- Mahmood A., Aamir M. & Anis M. I. (2008, Oct). *Design and implementation of AMR Smart Grid System*. IEEE Canada Electric Power Conference, Vancouver, BC, Canada. (pp. 1-6). DOI: 10.1109/EPC.2008.4763340
- Mahmood, K., Chaudhry, S., Naqvi, H., Kumari, S., Li, X., & Sangaiah, A. (2018). An elliptic curve cryptography based lightweight authentication scheme for smart grid communication. *Future Generation Computer Systems*, 81, 557-565. DOI: 10.1016/j.future.2017.05.002
- Menezes, A., Okamoto, T., & Vanstone, S. (1993). Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions On Information Theory*, 39(5), 1639-1646. DOI: 10.1109/18.259647
- Nabeel, M., Ding, X., Seo, S., & Bertino, E. (2015). Scalable end-to-end security for advanced metering infrastructures. *Information Systems*, 53, 213-223. DOI: 10.1016/j.is.2015.01.004
- Najafabadi, S.G., Naji, H. R., Mahani, A. (2013,Dec). *Sybil attack Detection: Improving security of WSNs for smart power grid application* . 2013 Smart Grid Conference (SGC), Tehran, Iran. (pp, 273-278). DOI: 10.1109/SGC.2013.6733831

- Newburger, E.(2019). More than 2 million people expected to lose power in PG&E blackout as California wildfires rage. Retrived from <https://www.cnbc.com/2019/10/26/pge-will-shut-off-power-to-940000-customers-in-northern-california-to-reduce-wildfire-risk.html>
- Ni, J., Alharbi, K., Lin, X. & Shen, X. (2015,Dec). *Security-Enhanced Data Aggregation against Malicious Gateways in Smart Grid*. 2015 IEEE Global Communications Conference (GLOBECOM),San Diego, CA, USA. (PP 1-6).DOI:10.1109/GLOCOM.2015.7417140
- Paillier, P. (1999,April). Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. EUROCRYPT International Conference on the Theory and Applications of Cryptographic Techniques, Prague, Czech Republic. (PP. 223-238)
- Panda, A., Mishra, D., & Ratha, H. (2016). Implementation of SCADA/HMI system for real-time controlling and performance monitoring of SDR based flight termination system. *Journal Of Industrial Information Integration*, 3, 20-30. DOI: 10.1016/j.jii.2016.07.001
- Rashed Mohassel, R., Fung, A., Mohammadi, F., & Raahemifar, K. (2014). A survey on Advanced Metering Infrastructure. *International Journal Of Electrical Power & Energy Systems*, 63, 473-484. DOI: 10.1016/j.ijepes.2014.06.025
- Ruj, S., & Nayak, A. (2013). A Decentralized Security Framework for Data Aggregation and Access Control in Smart Grids. *IEEE Transactions On Smart Grid*, 4(1), 196-205. DOI: 10.1109/tsg.2012.2224389
- Sahai, A. & Waters B. (2005, May). *Fuzzy Identity-Based Encryption scheme*. EUROCRYPT: Annual International Conference on the Theory and Applications of Cryptographic Techniques,Aarhus, Denmark. (PP. 457-473)
- Saputro, N., Akkaya, K., & Uludag, S. (2012). A survey of routing protocols for smart grid communications. *Computer Networks*, 56(11), 2742-2771. DOI: 10.1016/j.comnet.2012.03.027

- Shacham, H. & Waters, B. (2008,Dec). *Compact Proofs of Retrievability*. ASIACRYPT: International Conference on the Theory and Application of Cryptology and Information Security, Melbourne, Australia. (PP. 90-107)
- Shamir, A. & Tauman, Y. (2001, Aug). *Improved Online/Offline Signature Schemes*. CRYPTO 2001: Annual International Cryptology Conference -Advances in Cryptology, Santa Barbara, California, USA. (PP. 355-367).
- Shamir, A. (1979). How to share a secret. *Communications Of The ACM*, 22(11), 612-613. DOI: 10.1145/359168.359176
- Shamir, A. (1985, Aug). *Identity-based cryptosystems and signature schemes*. Proceedings of CRYPTO 84 : Workshop on the Theory and Application of Cryptographic Techniques, Santa Barbara, CA, USA. (PP.47-53)
- So, H. K.-H., Kwok, S. H. M., Lam, E. Y. & L, K. S. (2010, Oct). Zero-Configuration Identity-Based Signcryption Scheme for Smart Grid .2010 First IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, USA. (PP.321-326) DOI:10.1109/SMARTGRID.2010.5622061
- Sorebo, G. N. & Echols, M. C. (2011). *Smart Grid Security an End-to-End View of Security in The New Electrical Grid*. (First Edition) United States: Taylor & Francis Group
- Soykan, E. U., Ersoz, S. D. & Soykan, G. (2015, April) *Identity based signcryption for advanced metering infrastructure*. 2015 3rd International Istanbul Smart Grid Congress and Fair (ICSG), Istanbul, Turkey. (PP.1-5). DOI: 10.1109/SGCF.2015.7354933
- Stallings, W. (2011). *Cryptography and Network Security: principles and practice*. 5th edition. England: Pearson.
- Stallings, W. (2016). *Cryptography and Network Security: principles and practice*. 7th edition. England: Pearson.
- Suarez-Albela, M., Fernández-Caramés, T. M., Fraga-Lamas, P. & Castedo, L. (2018, Jun). A Practical Performance Comparison of ECC and RSA for Resource-Constrained IoT Devices. 2018 Global Internet of Things Summit (GloTS), Bilbao, Spain. (PP. 1-6). DOI: 10.1109/GIOTS.2018.8534575

- Tonyali, S., Akkaya, K., Saputro, N. & Cheng, X. (2017, Aug). *An Attribute & Network Coding-Based Secure Multicast Protocol for Firmware Updates in Smart Grid AMI Networks*. 2017 26th International Conference on Computer Communication and Networks (ICCCN), Vancouver, BC, Canada. (PP.1-9). DOI: 10.1109/ICCCN.2017.8038415
- Wang, W., & Lu, Z. (2013). Cyber security in the Smart Grid: Survey and challenges. *Computer Networks*, 57(5), 1344-1371. DOI: 10.1016/j.comnet.2012.12.017
- Wang, Z. (2017). An Identity-Based Data Aggregation Protocol for the Smart Grid. *IEEE Transactions On Industrial Informatics*, 13(5), 2428-2435. doi: 10.1109/tii.2017.2705218
- White, D., Roschelle, A., Peterson, P., Schlissel, D., Biewald, B., & Steinhurst, W. (2003). The 2003 Blackout: Solutions that Won't Cost a Fortune. *The Electricity Journal*, 16(9), 43-53. DOI: 10.1016/j.tej.2003.10.002
- W. Dai, W. (2009). cryptopp 5.6.0 benchmarks. Retrieved from <https://www.cryptopp.com/benchmarks.html>.
- Xie L., Mo Y. & Sinopoli B. (2010, Oct). *False Data Injection Attacks in Electricity Markets*. IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, USA. (pp. 226-231). DOI: 10.1109/SMARTGRID.2010.5622048
- Yao, X., Chen, Z., & Tian, Y. (2015). A lightweight attribute-based encryption scheme for the Internet of Things. *Future Generation Computer Systems*, 49, 104-112. DOI: 10.1016/j.future.2014.10.010
- Ye, F., Qian, Y., & Hu, R. (2015). HIBaSS: hierarchical identity-based signature scheme for AMI downlink transmission. *Security and Communication Networks*, 8(16), 2901-2908. DOI: 10.1002/sec.1217