International Journal of Safety and Security Engineering
Vol. 10, No. 4, August, 2020, pp. 549-558
Journal homepage: http://iieta.org/journals/ijsse

# A Lightweight Authenticated Key Establishment Scheme for Secure Smart Grid Communications

Fatty M. Salem*, Elham Ibrahim, Osama Elghandour

Department of Electronics and Communications Engineering, Helwan University, Helwan, Cairo 11918, Egypt

Corresponding Author Email: Faty_ahmed@h-eng.helwan.edu.eg

https://doi.org/10.18280/ijsse.100415

**Received:** 3 July 2020
**Accepted:** 12 August 2020

***Keywords:***
*smart grid, key establishment, authentication, anonymity, untraceability*

## ABSTRACT

Smart grid is a great revolution in communications that has succeeded in overcoming traditional network problems. However, smart grid components may face many security challenges that make the smart grid vulnerable to many attacks such as impersonation and replay attacks and user privacy disclosure. To cope with these challenging problems, we propose a lightweight authenticated key establishment scheme depending on data aggregation by using elliptic curve cryptography to create shared keys between smart meter and data aggregator, and between data aggregator and service provider. The data aggregator reduces the burden on smart meters and transfers consumption data safely as it is the mediator between the smart meter and the service provider. The proposed scheme can provide mutual authentication, anonymity and untraceability of smart meter, and can resist impersonation and replay attacks. In addition, the proposed scheme reduces the overall computation costs compared to other recent related schemes.

## 1. INTRODUCTION

Nowadays, the most prominent defects that affect the traditional network are that it is one-way communication, blackouts resulting from human error that is due to damage in electric transmission lines, and other defects such as the increased demand for electricity. Hence, the trend towards the so-called smart grid begins.

Smart grid is the next generation of the electric power system that uses computer technology to improve communication between different components and increase the use of digital information to improve the reliability and security of the grid. Smart grids progress the most efficient electric grid operations based on the received client data via two-way communications between the different entities in the grid. Customers can choose the most appropriate way to use the energy facilities based on the dynamic price data obtained from the smart grid in every period [1].

Smart grids consist of many components, with three most distinct and main components: Smart meters, aggregators, and service providers. The smart meter is a solid-state programmable device that is responsible for recording the amount of energy consumed and provide the electricity price information for the customers [2]. Usually, smart meters record power frequently and report daily at least. Data aggregator is responsible for collecting data from different smart meters and forwards them to the service provider [3]. Then it directs the data coming from the service provider to the smart meters. Service provider is responsible for giving each user the required amount of power according to the message received from the smart meters through the aggregator [4].

Smart meters are usually placed outside of the home and protected with a box [5]. Therefore, the attacker could penetrate the box and get the data from the smart meter, in addition to the information exchange between the smart meter and the other components communicate with each other is via the wireless communication channel [1]. Due to the nature of the wireless connection, the smart grid is exposed to many security issues. These issues might allow attackers to threaten network security. Some of the most important of these types are: a) Impersonation attack: an attack in which the opponent tries to impersonate one of the legitimate components of the network, and b) Replay attack: it is a shape of network attack that occurs when an attacker tries to eavesdrop on messages that are exchanged between network components, intercept them, and then resend them again or delay them.

To protect the security of data transmission and maintain the network's privacy, several security services must be met. The most prominent of these services are that:

- Mutual authentication: it is a process in which both components authenticate each other. Usually, the authentication process takes place between the smart meter and the data collector, or between the data collector and the service provider.
- Anonymity of smart meter: this service prevents the attacker from knowing the identity of the smart meter that sent the metering data in the network.
- Untraceability of smart meter: this service prevents the attacker from monitoring the amount of power consumed by the smart meter that is collected and sent in the network. The anonymity and untraceability can protect the privacy of consumers.
- Forward secrecy: this service prevents any attacker from breaking into session keys even if the private key of the entity is compromised.

### 1.1 Related work

Many researchers have sought to provide many different schemes to achieve security services and get rid of different types of attacks. A secure Key distribution scheme [6] has been proposed between smart meter and service provider for the smart grid. The proposed scheme has succeeded to prevent replay attack; however, it has not only failed to achieve perfect secrecy, mutual authentication, anonymity, untractability, but also the authors claimed that their scheme could prevent impersonation attack; however, this was found to be incorrect. A fault-tolerant and scalable key management scheme [7] has been proposed; the proposed scheme combines symmetric key technique and elliptic curve public key technique. Although, it has failed to provide mutual authentication, anonymity, forward secrecy and intractability, but it has succeeded in preventing replay and impersonation attack.

Maier et al. [8] proposed a message authentication based on hash message authentication code and Diffie-Hellman key agreement protocol. The proposed scheme has achieved mutual authentication, but has not achieved anonymity and untractability, in addition to very high communication cost because of RSA. Mahmood et al. [9] achieved forward secrecy, mutual authentication between home area network gateways and building area network gateways using hybrid Diffie-Hellman key agreement protocol, and the authentication of message based on hash message authentication code by proposing a lightweight message authentication scheme. Although the proposed scheme has failed to achieve anonymity and un-traceability, it has succeeded in reducing the communication cost compared to Maier et al.'s scheme [8]. Aziz et al. [10] applied a lightweight scheme to achieve the authentication between the smart breaker and the control center and preventing several types of attacks in the smart grid. Although this scheme has succeeded in reducing the communication cost compared to Mahmood et al's scheme [9]. Despite that, the authors claimed to achieve anonymity, which is not true.

A new anonymous metering scheme [3] has been proposed based on direct anonymous attestation and identity-based signatures. The proposed scheme has succeeded in achieving the mutual authentication, anonymity and untraceability; however, the scheme has failed to resist replay attack and impersonation attack and has failed to achieve forward secrecy. An authentication scheme based on the Merkle hash tree technique [11] has been implemented to achieve the authentication and resist of replay attacks. This scheme is more efficient of the schemes depended on RSA. This scheme also has failed to achieve anonymity and un-traceability. The authentication between smart meters and the neighborhood gate way based on a lightweight authentication scheme and Lagrange interpolation formula [12]. The communication cost for this scheme is much better than the previous schemes. It also has succeeded in getting rid of replay attack.

An identity-based key establishment scheme [13] has been proposed to provide mutual authentication and forward secrecy in addition to preventing the replay attacks and impersonation attacks. However, it has failed to achieve anonymity and untraceability. Also, an anonymous key distribution scheme based on utilized identity-based encryption and signature [14] has been proposed to achieve the mutual authentication between the smart meter and service provider. Moreover, it can provide smart meters' anonymity and perfect forward secrecy. However, this scheme has failed to achieve the strong credentials' privacy of the smart meter and failed to resist against replay attack, impersonation attack, and the ephemeral secret leakage attack.

A new secure authenticated shared key establishment scheme [15] has been proposed to beat the security weaknesses of the pervious scheme, also it has succeeded in reducing the communication cost compared to the previous scheme. However, the authors claimed that their scheme has achieved untraceability of the smart meter and has prevented the impersonation attack, which has proved to be incorrect. Later, an anonymous authentication and key establish scheme has been proposed [16] to avoid the disadvantages of the previous scheme [15], but the computational cost of this scheme is very high where it depends on bilinear maps and the computational Diffie–Hellman problem.

A lightweight anonymous key distribution scheme [17] has been implemented based on Elliptic Curve Cryptography (ECC); the proposed scheme has achieved the mutual authentication between smart meter and service provider and also has achieved smart meter anonymity. Moreover, the scheme also has succeeded in preventing the replay attacks and impersonation attacks and provided less communication cost compared to scheme [14, 15]. Despite all the accomplishments of this scheme, it has failed to achieve untraceability of smart meter. Kumar et al. [5] proposed a different scheme of lightweight authentication and key agreement for smart metering in smart energy network. They have utilized hybrid cryptography (the ECC and symmetric encryption) to achieve the mutual authentication, anonymity, perfect forward secrecy, preventing the several types of attacks, and has provided less communication cost compared to the schemes [14, 15, 17]. Despite all the advantages and security services achieved by Kumar et al.'s scheme [5], it has failed to achieve untraceability of smart meter.

Zhang et al. [18] have applied ECC-based authentication with identity protection; their scheme is secure against replay attacks and impersonation attacks. Moreover, the scheme has achieved the mutual authentication between smart meter and control center, and anonymity. However, this scheme has failed to achieve forward secrecy. The proposed ECC-based lightweight authentication scheme [19] has succeeded in achieving several security services and provided less communication cost compared to the schemes [8, 18], but it failed to achieve anonymity.

Farhadi et al. [20] have approached a lightweight key management protocol for secure communication in smart grids based on time constraints for two sensitive protocols (GOOSE, SV) in communication between substations and a data center. This scheme has provided the mutual authentication and forward secrecy. Other features have been provided by this scheme such as anonymity, thwarting replay and impersonation attacks; however, it has failed to achieve the untraceability. Moreover, the authors claimed that their scheme has provided less communication cost compared to the schemes [8, 14, 17-19], which is untrue.

Abbasinezhad-mood [21] proposed an anonymous key distribution scheme based on ECC which counteracts against replay and impersonation attacks, and has provided mutual authentication, forward secrecy and anonymity, and reduced the communication cost compared to schemes [8, 14, 15, 17]; but it has failed to achieve untraceability. Garg et al. [22] proposed a lightweight authentication scheme which has provided less communication cost compared to Abbasinezhad-mood's scheme [21]. This scheme was also able to solve the problems of the pervious scheme, but it has failed to achieve untraceability of smart meter.

An EEC-based privacy preserving data aggregation scheme has been proposed [23]; the proposed scheme has succeeded in achieving privacy preserving and authentication, but it has failed to achieve anonymity and untraceability of smart meter, and forward secrecy. In addition, it could not resist against replay and impersonation attack. Kong et al. [24] proposed a group blind signature scheme for privacy protection in smart grid based on RSA; the proposed scheme relays on data aggregator to achieve anonymity and untraceability; the scheme could also provide mutual authentication, but it has failed to achieve forward secrecy and failed also in preventing replay attack and impersonation attack. Wu et al. [25] introduced a different approach to preserve privacy with identity traceable property; the scheme can provide less communication cost compared to Kong et al.'s scheme [24]. However, both schemes have failed to achieve untraceability and forward secrecy.

A Dynamic Membership Data Aggregation (DMDA) protocol [26] has been proposed based on the homomorphic encryption and ID-based signature; the proposed scheme has provided mutual authentication, privacy and forward secrecy, but it has failed to prevent replay and impersonation attacks and failed to achieve anonymity, untraceability. Tahir et al. [27] introduced a new scheme depending on data aggregation; the scheme has succeeded in preventing the replay attacks and impersonation attacks, but it has failed to achieve anonymity, untraceability and forward secrecy. Boudia et al. [28] implemented an ECC-based multidimensional aggregation scheme; the idea of the proposed scheme is based on determining the type of data and collecting readings from all smart meters. After that, the data aggregator sends data of all smart meters to the service provider. The proposed scheme has been proved to be more efficient compared to Tahir et al.'s scheme [27]. However, Boudia et al. [28] has failed to achieve anonymity, untraceability and forward secrecy.

A privacy-preserving scheme for data collection in smart grid has been proposed [29]; the proposed scheme is depending on the blind signature and the key distribution to achieve mutual authentication and forward secrecy and preventing the replay attacks, but it has failed to achieve anonymity, untraceability and could not prevent impersonation attack. Zhang and Shen [30] proposed an efficient privacy-preserving multi-dimensional data aggregation scheme; the performance evaluations of this scheme have showed that it is more efficient and low-computational cost for no map-to-point hash and bilinear pairing operations are used. However, it has failed to achieve anonymity, untraceability and forward secrecy.

### 1.2 Contributions

The proposed scheme in this paper succeeds in offering the following significant contributions in the field of smart grid communications.

- We utilized the elliptic curve cryptography to design a lightweight authenticated key establishment scheme depending on data aggregation.
- Our proposed scheme provides the required security services for smart grid communications and resists against impersonation attack and replay attack.
- The performance of the proposed scheme is also better than existing schemes that depend on data aggregation idea.

## 2. PRELIMINARIES AND COMMUNICATION MODEL

In this section, we will state the required preliminaries and describe the communication model.

### 2.1 Preliminaries

Elliptic Curve Cryptography (ECC) is used to achieve security for smart network entities and not only that, but also reduces the computational cost compared to other methods as the key size used in the cryptographic curve is much less than the size of the keys used in other techniques, such as RSA, digital signature algorithm and Diffie Hellman. ECC is applied to many different tasks, the most prominent of these tasks is encryption and the key agreement.

The equation of the elliptic curve $E_p(a,b): y^2 = x^3 + ax + b \; mod \; p$ is used to define the mathematical operations, where $a, b \in Z_p$ and $4a^3 + 27b^2 \; mod \; p \neq 0$ such that $p$ is a large prime number. The values $a$ and $b$ are used to specify the elliptic curve while the points $(x, y)$ inclusive a point at infinity depend on the elliptic curve if it satisfies the last given statement.

### 2.2 Communication model

In this paper, the communication model consists of a group of communities where each community has a number of smart meters; the model also has a group of aggregators, a group of service providers, and finally one TTP as shown in Figure 1.

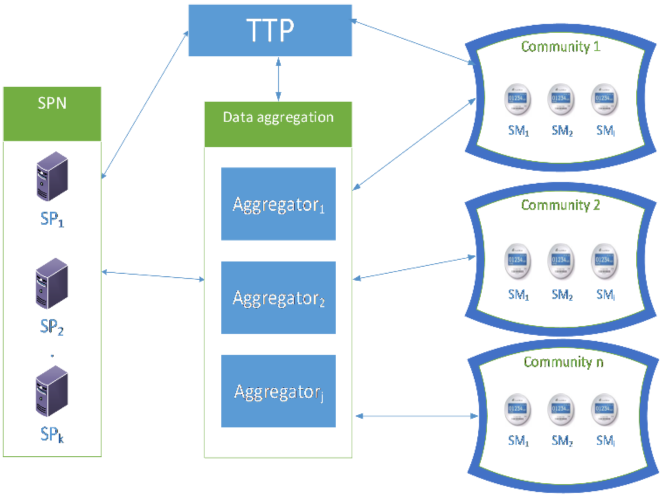


**Figure 1.** Communication model

In the following, we explain in detail every entity in this model.

- Trusted Third Party (TTP): It is the entity which is responsible for supporting the communication between two parties who both trust the third party as it distributes the keys for each party.
- Service Provider (SP): It is responsible for giving each user the required amount of energy according to the message received from the smart meters through aggregators.
- Data Aggregator (DA): It is a device that aggregates the information from different smart meters and forwards them to the SP, and it forwards the information from service provider to smart meter.

- Smart Meter (SM): It is an electronic device which is responsible for recording the amount of energy consumed periodically for the corresponding service provider through aggregators.

## 3. THE PROPOSED SCHEME

First, the required notations and their descriptions throughout the paper are listed in Table 1. The proposed scheme is consisted of three stages: initialization stage, registration stage, mutual authentication and key establishment stage which are explained as follows:

### 3.1 Initialization

In this stage, the TTP chooses an elliptic curve over a finite field $E(F_P)$, a random generator ($G$), a secret key ($S$), and one-way hash functions. The *TTP* computes its public key as:

$$\mathrm{PK} = \mathrm{SG} \tag{1}$$

And subsequently, the *TTP* broadcasts the parameters $\{PK, G, E(F_P), H(.)\}$.

### 3.2 Registration

In this stage, service providers, data aggregators, and smart meters are registered in the system.

3.2.1 SP registration

A service provider $SP_k$ chooses its identity $ID_k$ and computes $IDS_k$ according to Eq. (2), where TSP defines the entity type as service provider. Then it sends its $IDS_k$ to *TTP* in a secure channel.

$$\mathrm{IDS_k} = \mathrm{TSP}||\mathrm{ID_k} \tag{2}$$

The *TTP* chooses a nonce value $a_{SP_k} \in Z_p$ and computes the public and private keys of $SP_k$ according to Eq. (3) and Eq. (4). Then, the *TTP* sends the private key $\left(SK_{SP_k}\right)$ in a secure channel to $SP_k$, and broadcasts the public key $\left(PK_{SP_k}\right)$ of $SP_k$.

$$\mathrm{PK_{SP_k}} = \mathrm{a_{SP_k}G} \tag{3}$$

$$\mathrm{SK_{SP_k}} = \mathrm{a_{SP_k}} + \mathrm{S.H(IDS_k, PK_{SP_k})} \tag{4}$$

**Table 1.** Table of notations

| Icons | Descriptions |
|---|---|
| $F_P$ | A finite field that is decided by prime $p$ |
| $Z_P$ | Multiplicative group of integers modulo $p$ |
| $G$ | Random generator of $E(F_P)$ |
| $E(F_P)$ | An elliptic curve its equation $y^2=x^3+ax+b \bmod p$ |
| *TTP* | Trusted Third Party |
| *Pk,S* | Public key &Private key of the *TTP* |
| *H(.)* | One-way hash functions |
| $SM_i$ & $ID_i$ | i-th smart meter and its identity |
| $DA_j$ & $ID_j$ | j-th data aggregator and its identity |
| $SP_k$ & $ID_k$ | k-th service provider and its identity |

3.2.2 DA registration

A data aggregator $DA_j$ chooses its identity $ID_j$ and computes $IDA_j$ according to Eq. (5), where TDA defines the entity type as data aggregator. Then, it sends $IDA_j$ to *TTP* in a secure channel.

$$\mathrm{IDA_j} = \mathrm{TDA}\|\mathrm{ID_j} \tag{5}$$

The *TTP* chooses a nonce value $a_{DA_j} \in Z_p$ and computes the public and private keys of $DA_j$ as.

$$\mathrm{PK_{DA_j}} = \mathrm{a_{DA_j}G} \tag{6}$$

$$\mathrm{SK_{DA_j}} = \mathrm{a_{DA_j}} + \mathrm{S.H(IDA_j, PK_{DA_j})} \tag{7}$$

Then, the *TTP* sends the private key ($\mathrm{SK}_{DAj}$) in a secure channel to $DA_j$, and broadcasts the public key ($\mathrm{PK}_{DAj}$) of $DA_j$ and its certificate.

3.2.3 SM registration

A smart meter $SM_i$ chooses its identity $ID_i$ and computes $IDSM_i$ according to Eq. (8), where TSM defines the entity type as smart meter, and sends it to *TTP* in a secure channel.

$$\mathrm{IDSM_i} = \mathrm{TSM}||\mathrm{ID_i} \tag{8}$$

The *TTP* chooses a nonce value $a_{SM_i} \in Z_p$ and computes the public and private keys for $SM_i$ according to Eq. (9) and Eq. (10).

$$\mathrm{PK_{SM_i}} = \mathrm{a_{SM_i}G} \tag{9}$$

$$\mathrm{SK_{SM_i}} = \mathrm{a_{SM_i}} + \mathrm{S.H(IDSM_i\|PK_{SM_i})} \tag{10}$$

Then, the *TTP* sends the private key $\left(SK_{SM_i}\right)$ in a secure channel to $SM_i$, and encrypts and sends the identity and the public key $\left(PK_{SM_i}\right)$ of $SM_i$ $E_S\left(IDSM_i\|PK_{SM_i}\right)||\, H\left(IDSM_i\|PK_{SM_i}\right)$ to $DA_j$.

$DA_j$ verifies the identity and public key of each smart meter $SM_i$ in its community and stores the verified identities and public keys in its data base.

### 3.3 Authentication and key agreement

In this stage, an authenticated session key will be established between $SM_i$ and $DA_j$ (Figure 2 describes the steps of this stage), and another authenticated session key will be established between $DA_j$ and $SP_k$ (Figure 3 describes the steps of this stage).

3.3.1 Mutual authentication between $SM_i$ and $DA_j$

Firstly, $SM_i$ chooses a nonce value $w \in Z_p$ and computes $A_1$, $A_2$, $A_3$, and $C_1$ as:

$$A_1 = wG \tag{11}$$

$$A_2 = H\left(wPK_{DA_j} + wH\left(IDA_j\|PK_{DA_j}\right)PK\right) \oplus IDSM_i \tag{12}$$

| **Smart Meter $SM_i$** | | **Data Aggregator $DA_j$** |
|---|---|---|
| Choose $w \in Z_p$<br>$A_1 = wG$<br>$A_2 = H\left(wPK_{DA_j} + wH\left(IDA_j \| PK_{DA_j}\right)PK\right) \oplus IDSM_i$<br>$A_3 = H\left(A_1 \| PK_{SM_i} \| PK_{DA_j} \| IDSM_i \| IDA_j \| t_1\right)$<br>$C_1 = E_{a_{SM_i}}(A_3)$ | | |
| | $\xrightarrow{\{A_1, A_2, C_1, t_1\}}$ | |
| | | $t_1 - t_2 \leq \Delta t$, revokes if not fresh. Else,<br>$IDSM_i = A_2 \oplus H\left(SK_{DA_j}, A_1\right)$<br>Computes<br>$A_3{}^* = D_{PK_{SM_i}}(C_1)$<br>$A_3{}^* \overset{?}{=} H\left(A_1 \| PK_{SM_i} \| PK_{DA_j} \| IDSM_i \| IDA_j \| t_1\right)$<br>Chooses $x \in Z_p$<br>$A_4 = xG,$<br>$SK_{ji} = H(A_1 \| A_4 \| xA_1)$<br>$A_5 = H\left(xPK_{SM_i} + xH\left(IDSM_i \| PK_{SM_i}\right)PK\right) \oplus IDA_j$<br>$A_6 = H\left(IDSM_i \| IDA_j \| A_1 \| A_4 \| SK_{ji} \| t_2\right)$<br>$C_2 = E_{a_{DA_j}}(A_6)$ |
| | $\xleftarrow{\{A_4, A_5, C_2, t_2\}}$ | |
| $t_2 - t_3 \leq \Delta t$ , revokes if not fresh. Else,<br>$IDA_j = A_5 \oplus H\left(SK_{SM_i}, A_4\right)$<br>$SK_{ij} = H(A_1 \| A_4 \| wA_4)$<br>$A_6{}^* = D_{PK_{DAj}}(C_2)$<br>$A_6{}^* \overset{?}{=} H\left(IDSM_i \| IDA_j \| A_1 \| A_4 \| SK_{ij} \| t_2\right)$ | | |

**Figure 2.** Session key establishment between smart meter and data aggregator

$$A_3 = H\left(A_1 \| PK_{SM_i} \| PK_{DA_j} \| IDSM_i \| IDA_j \| t_1\right) \tag{13}$$

$$C_1 = E_{a_{SM_i}}(A_3) \tag{14}$$

Then, $SM_i$ sends $\{A_1, A_2, C_1, t_1\}$ to $DA_j$.

Secondly, when $DA_j$ receives the message from $SM_i$, it starts off checking $t_1 - t_2 \leq \Delta t$, it rejects the message if not fresh; otherwise, it extracts the identity of $SM_i$ and gets the public key of $SM_i$ from its data base to extract $A_3{}^*$ as:

$$IDSM_i = A_2 \oplus H\left(SK_{DA_j}, A_1\right) \tag{15}$$

$$A_3{}^* = D_{PK_{SM_i}}(C_1) \tag{16}$$

Then, it checks $D_{PK_{SM_i}}(C_1) \overset{?}{=} H\left(A_1 \| PK_{SM_i} \| PK_{DA_j} \| IDSM_i \| IDA_j \| t_1\right)$; if true, $DA_j$ chooses a nonce value $x \in Z_p$ and computes $A_4, SK_{ji}, A_5, A_6,$ and $C_2$ as:

$$A_4 = xG \tag{17}$$

$$SK_{ji} = H(A_1 \| A_4 \| xA_1) \tag{18}$$

$$A_5 = H\left(xPK_{SM_i} + xH\left(ID_i \| PK_{SM_i}\right)PK\right) \oplus IDA_j \tag{19}$$

$$A_6 = H\left(IDSM_i \| IDA_j \| A_1 \| A_4 \| SK_{DA_j}\right) \tag{20}$$

$$C_2 = E_{a_{DA_j}}(A_6) \tag{21}$$

Then, it sends $\{A_4, A_5, C_2, t_2\}$ to $SM_i$.

Finally, when $SM_i$ receives the message from $DA_j$, it starts off checking $t_2 - t_3 \leq \Delta t$ , it rejects the message if not fresh; otherwise, extracts the identity of $DA_j$ and extracts $A_6{}^*$ as:

$$IDA_j = A_5 \oplus H\left(SK_{SM_i}, A_4\right) \tag{22}$$

$$A_6{}^* = D_{PK_{DA_j}}(C_2) \tag{23}$$

Then, it checks if $A_6{}^* \overset{?}{=} H\left(IDSM_i \| IDA_j \| A_1 \| A_4 \| SK_{SM_i}\right)$; if true, $SM_i$ computes:

$$SK_{ij} = H(A_1 \| A_4 \| wA_4) \tag{24}$$

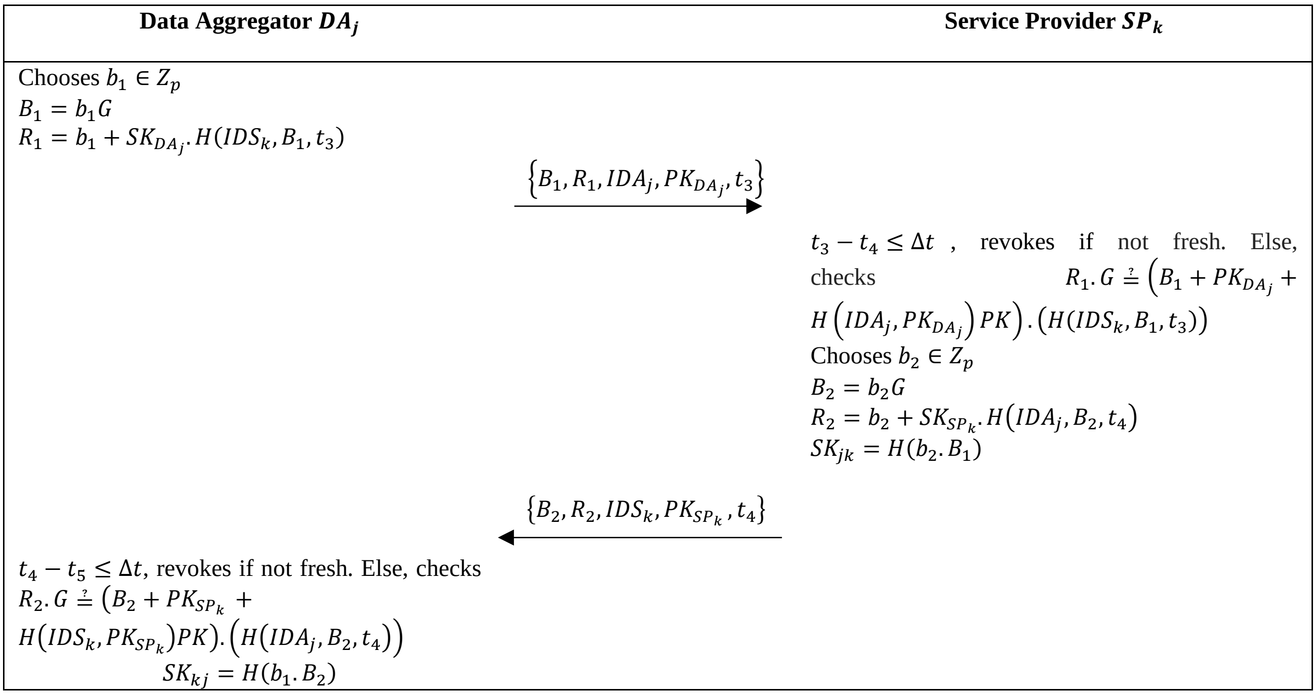
This shared key will be used to encrypt the messages and to provide secure communication between $SM_i$ and $DA_j$.

3.3.2 Mutual authentication between $DA_j$ and $SP_k$

Firstly, $DA_j$ chooses a nonce value $b_1 \in Z_p$ and computes $B_1$ and $R_1$ according to Eq. (25) & Eq. (26). Then, it sends $\left\{B_1, R_1, IDA_j, PK_{DA_j}, t_3\right\}$ to $SP_k$.

$$B_1 = b_1 G \tag{25}$$

$$R_1 = b_1 + SK_{DA_j}.H(IDS_k, B_1, t_3) \tag{26}$$



**Data Aggregator $DA_j$** **Service Provider $SP_k$**

Chooses $b_1 \in Z_p$
$B_1 = b_1G$
$R_1 = b_1 + SK_{DA_j}.H(IDS_k, B_1, t_3)$

$$\xrightarrow{\left\{B_1, R_1, IDA_j, PK_{DA_j}, t_3\right\}}$$

$t_3 - t_4 \le \Delta t$ , revokes if not fresh. Else, checks $R_1.G \overset{?}{=} \left(B_1 + PK_{DA_j} + H\left(IDA_j, PK_{DA_j}\right)PK\right).\left(H(IDS_k, B_1, t_3)\right)$
Chooses $b_2 \in Z_p$
$B_2 = b_2G$
$R_2 = b_2 + SK_{SP_k}.H\left(IDA_j, B_2, t_4\right)$
$SK_{jk} = H(b_2.B_1)$

$$\xleftarrow{\left\{B_2, R_2, IDS_k, PK_{SP_k}, t_4\right\}}$$

$t_4 - t_5 \le \Delta t$, revokes if not fresh. Else, checks $R_2.G \overset{?}{=} \left(B_2 + PK_{SP_k} + H\left(IDS_k, PK_{SP_k}\right)PK\right).\left(H\left(IDA_j, B_2, t_4\right)\right)$
$SK_{kj} = H(b_1.B_2)$

**Figure 3.** Session key establishment between data aggregator and service provider

Secondly, when $SP_k$ receives the message from $DA_j$, it starts off checking $t_3 - t_4 \le \Delta t$, it rejects the message if not fresh; otherwise, it checks $R_1.G \overset{?}{=} \left(B_1 + PK_{DA_j} + H\left(IDA_j, PK_{DA_j}\right)PK\right).\left(H(IDS_k, B_1, t_3)\right)$, if true, SP$_k$ chooses a nonce value $b_2 \in Z_p$ and computes $B_2, R_2$ and $SK_{jk}$ as:

$$B_2 = b_2G \tag{27}$$

$$R_2 = b_2 + SK_{SP_k}.H\left(IDA_j, B_2, t_4\right) \tag{28}$$

$$SK_{jk} = H(b_2.B_1) \tag{29}$$

Then, it sends $\left\{B_2, R_2, IDS_k, PK_{SP_k}, t_4\right\}$ to $DA_j$.

Finally, when DA$_j$ receives the message from $SP_k$, it starts off checking $t_4 - t_5 \le \Delta t$, it rejects the message if not fresh; otherwise, it checks $R_2.G \overset{?}{=} \left(B_2 + PK_{SP_k} + H\left(IDS_k, PK_{SP_k}\right)PK\right).\left(H\left(IDA_j, B_2, t_4\right)\right)$. Then, it computes $SK_{kj}$ *as*:

$$SK_{kj} = H(b_1.B_2) \tag{30}$$

This shared key will be used to encrypt the messages and to provide secure communication between $SP_k$ and $DA_j$.

## 4. SECURITY ANALYSIS

This section analyzes the security of the proposed authenticated key establishment scheme.

### 4.1 Mutual authentication

**Between $SM_i$ and $DA_j$:** In the proposed scheme, $DA_j$ authenticates $SM_i$ by computing $A_3{}^* = D_{PK_{SM_i}}(C_1)$ and then verifying $A_3{}^* \overset{?}{=} H\left(A_1 \| PK_{SM_i} \| PK_{DA_j} \| IDSM_i \| IDA_j \| t_1\right)$ as the attack cannot compute $C_1$ as the encryption depends on the secret nonce $a_{SM_i}$ of $SM_i$, and using the public key of $SM_i$ to decrypt $C_1$ ensures that the message is from the authorized $SM_i$. Likewise, $SM_i$ authenticates $DA_j$ by computing $A_6{}^* = D_{PK_{DAj}}(C_2)$ and then verifying $A_6{}^* \overset{?}{=} H\left(IDSM_i \| IDA_j \| A_1 \| A_4 \| SK_{ij} \| t_2\right)$ as the attack cannot compute $C_2$ as the encryption depends on the secret nonce $a_{DA_j}$ of $DA_j$, and using the public key $PK_{DA_j}$ of $DA_j$ to decrypt $C_2$ ensures that the message is from the authorized $DA_j$. Hence, the proposed scheme can provide the mutual authentication between $SM_i$ and $DA_j$.

**Between $DA_j$ and $SP_k$:** In the proposed scheme, $DA_j$ compute $B_1 = b_1G$ and $R_1 = b_1 + SK_{DA_j}.H(IDS_k, B_1, t_3)$ and sends $\left\{B_1, R_1, IDA_j, PK_{DA_j}, t_3\right\}$ to $SP_k$ , then $SP_k$ authenticates $DA_j$ by verifying $R_1.G \overset{?}{=} \left(B_1 + PK_{DA_j} + H\left(IDA_j, PK_{DA_j}\right)pk\right).\left(H(IDS_k, B_1, t_3)\right)$ as the computation of $R_1$ includes the private key $SK_{DA_j}$ of $DA_j$ which is difficult for the attack to know; therefore, the attack cannot compute a valid $R_1$. Likewise, $SP_k$ computes $B_2 = b_2G$ and $R_2 = b_2 + SK_{SP_k}.H\left(IDA_j, B_2, t_4\right)$ and sends $\left\{B_2, R_2, IDS_k, PK_{SP_k}, t_4\right\}$ to $DA_j$, then $DA_j$ authenticates $SP_k$ by verifying $R_2.G \overset{?}{=} \left(B_2 + PK_{SP_k} + H\left(IDS_k, PK_{SP_k}\right)PK\right).\left(H\left(IDA_j, B_2, t_4\right)\right)$ as the computation of $R_2$ includes the private key $SK_{SP_k}$ of $SP_k$ which it is difficult for the attack to know; therefore, the attack cannot compute a valid $R_2$. Hence, the proposed scheme can provide the mutual authentication between $DA_j$ and $SP_k$.

### 4.2 Anonymity of $SM_i$

The identity of smart meter i ($IDSM_i$) is hidden by using xor operation and secure hash function which is expressed as $H\left(wPK_{DA_j} + wH\left(IDA_j \| PK_{DA_j}\right)PK\right) \oplus IDSM_i$. Moreover, the extraction of IDSM$_i$ requires the secret key of $DA_j$ as

$IDSM_i = A_2 \oplus H\left(SK_{DA_j}, A_1\right)$; therefore, the identity of $SM_i$ is protected.

### 4.3 Untraceability of $SM_i$

During every session, a new nonce $w$ is generated by $SM_i$; hence, the message $\{A_1, A_2, C_1, t_1\}$ that is sent through the channel will be changed in each new session as the w is used to calculate $A_1 = wG,$ and $A_2 = H\left(wPK_{DA_j} + wH\left(IDA_j \| PK_{DA_j}\right)PK\right) \oplus IDSM_i$. Finally, $C_1 = E_{a_{SM_i}}(A_3)$ will be also changed every session as $A_3$ includes $A_1$ which depends on the new $w$. Thus, the attack cannot trace the messages sent by the same $SM_i$.

### 4.4 Forward secrecy

An authentication scheme satisfies the forward secrecy when the security of the shared keys created in preceding sessions is not affected due to disclosure of the private keys of the participant entities.

**Between $SM_i$ and $DA_j$:** Suppose the attack knows all the secret keys of $SM_i$ and $DA_j$, it is not easy for an attacker to calculate an agreed shared key $SK_{ji} = H(A_1\|A_4\|xA_1)$ or $SK_{ij} = H(A_1\|A_4\|wA_4)$ because the attack cannot obtain $w$ from $A_1 = wG$ nor $x$ from $A_4 = xG$ due to ECDLP. The random numbers $w$ and $x$ are created by $SM_i$ and $DA_j$ respectively. Therefore, it is hard for the attack to disclose the previously created shared keys without having multiple session parameters.

**Between $DA_j$ and $SP_k$:** Suppose the attack knows all the secret keys of $DA_j$ and $SP_k$, the attack cannot compute $SK_{jk} = H(b_2.B_1)$ because the attack cannot obtain $b_1$ from $B_1 = b_1G$ due to ECDLP. Alternately, the attack cannot compute $SK_{kj} = H(b_1.B_2)$ because the attack cannot obtain $b_2$ from $B_2 = b_2G$ also due to ECDLP. Every time both the participants use new random numbers, so it is hard for the attack to guess previous shared keys.

### 4.5 Impersonation attack

**Between $SM_i$ and $DA_j$:** Suppose that the attack tries to impersonate as a legal $SM_i$ to $DA_j$; to do that, the attack generates nonce number $w`$ and computes $A_1` = w`G$, $A_2` = H\left(w`PK_{DA_j} + w`H\left(IDA_j\|PK_{DA_j}\right)PK\right) \oplus IDSM_i`$ , and $A_3` = H\left(A_1`\|PK_{SM_i}`\|PK_{DA_j}\|IDSM_i`\|IDA_j\|t_1`\right)$, fabricates a false $C_1`$, and sends $\{A_1`, A_2`, C_1`, t_1\}$ to $DA_j$. The $DA_j$ extracts $IDSM_i` = A_2` \oplus H\left(SK_{DA_j}, A_1`\right)$ and obtains $SM_i's$ corresponding public key to decrypt $C_1`$, and checks if $D_{PK_{SM_i}}(C_1') \overset{?}{=} H\left(A_1`\|PK_{SM_i}`\|PK_{DA_j}\|IDSM_i`\|IDA_j\|t_1`\right)$. It is obvious that the equality will not be valid as it is difficult for the attack to know the secret parameter $a_{SM_i}$ of $SM_i$ that is used to encrypt $C_1$ where $C_1 = E_{a_{SM_i}}(A_3)$ even if the attack knew the identity and public key of the $SM_i$. Also, suppose that the attack tries to impersonate as a legal $DA_j$ to $SM_i$; to do that, the attack generates a nonce number $x`$ and computes $A_4` = x`G$ , $A_5 = H(x`PK_{SM_i} + x`H(IDSM_i\|PK_{SM_i})PK) \oplus IDA_j`$, $A_6` = H(IDSM_i\|IDA_j`\|A_1\|A_4`\|SK_{ji}`\|t_2`)$, fabricates a false $C_2`$, and sends $\{A_4`, A_5`, C_2`, t_2`\}$ to $SM_i$. The $SM_i$ decrypts $C_2`$ using the public key of $DA_j$ and checks if $D_{PK_{DAj}}(C_2`) \overset{?}{=} H(IDSM_i\|IDA_j`\|A_1\|A_4`\|SK_{ji}`\|t_2`)$. It is obvious that the equality will not be valid as it is difficult for the attack to know the secret parameter $a_{SM_i}$ of $SM_i$ that is used to encrypt $C_2$ where $C_2 = E_{a_{DA_j}}(A_6)$.

**Between $DA_j$ and $SP_k$:** Suppose the attack tries to impersonate as a $DA_j$ to $SP_k$; to do that, the attack generates a nonce number $b_1`$, computes $B_1` = b_1`G$, fabricates a false $R_1` = b_1` + SK_{DA_j}`.H(IDS_k, B_1`, t_3`)$ , and sends $\left\{B_1`, R_1`, IDA_j, PK_{DA_j}, t_3`\right\}$ to $SP_k$. The $SP_k$ checks if $R_1`.G \overset{?}{=} \left(B_1 + PK_{DA_j}H\left(IDA_j, PK_{DA_j}\right)PK\right).\left(H(IDS_k, B_1, t_3)\right)$ ; however, it is obvious that the equality will not be valid due to the fabricated $R_1`$as it is difficult for the attack to know the private key of the $DA_j$.

Also, suppose the attack tries to impersonate as $SP_k$ to $DA_j$; to do that, the attack generates a nonce number $b_2`$, computes $B_2` = b_2`G$ , fabricates a false $R_2` = b_2` + SK_{SP_k}`.H(IDA_j`, B_2`, t_4`)$ , and sends $\{B_2`, R_2`, IDS_k`, PK_{SP_k}`, t_4`\}$ to $DA_j$ . The $DA_j$ checks if $R_2`.G \overset{?}{=} (B_2 + PK_{SP_k} + H(IDS_k, PK_{SP_k})S.G).\left(H(IDA_j, B_2, t_4)\right)$ ; however, it is obvious that the equality will not be valid due to the fabricated $R_2`$ as it is difficult for the attack to know the private key of $SP_k$ .

### 4.6 Replay attack

**Between $SM_i$ and $DA_j$ :** when the request message $\{A_1, A_2, A_3, C_1, t_1\}$ is received and it is clear that $A_3 = H\left(A_1\|PK_{SM_i}\|PK_{DA_j}\|IDSM_i\|IDA_j\|t_1\right)$ includes the time stamp $t_1$, $DA_j$ starts checking the freshness of the timestamp by using $t_1 - t_2 \le \Delta t$. If the replay attack initiates at time $(t`)$, the attack resends $\{A_1, A_2, A_3, C_1, t`\}$ to $DA_j$, but this message will be rejected because of the verification of the time stamp, i.e., $t` - t_2 \le \Delta t$. Moreover, the request will fail to verify $D_{PK_{SM_i}}(C_1) \overset{?}{=} H\left(A_1\|PK_{SM_i}\|PK_{DA_j}\|IDSM_i\|IDA_j\|t`\right)$ . Likewise, replay attack will be prevented due to the existence of $t_2$ in response message $\{A_4, A_5, A_6, t_2\}$ and is also hidden in $A_6 = H\left(IDSM_i\|IDA_j\|A_1\|A_5\|SK_{DA_j}\|t_2\right)$ and $A_6 \overset{?}{=} H(IDSM_i\|IDA_j\|A_1\|A_4\|SK_{SM_i}\|t_2)$.

**Between $DA_j$ and $SP_k$ :** when the request message $\left\{B_1, R_1, IDA_j, PK_{DA_j}, t_3\right\}$is received and it is clear that $R_1 = b_1 + SK_{DA_j}.H(IDS_k, B_1, t_3)$ includes the time stamp $t_3$, $SP_k$ starts checking the freshness of the timestamp by using $t_3 - t_4 \le \Delta t$. If the replay attack initiates at time (t*), the attack resends $\left\{B_1, R_1, IDA_j, PK_{DA_j}, t^*\right\}$ to $DA_j$, but this message will be rejected because of the verification of the time stamp, i.e., $t^* - t_4 \le \Delta t$. Moreover, the request will fail to verify $R_1.G \overset{?}{=} \left(B_1 + PK_{DA_j} + H\left(IDA_j, PK_{DA_j}\right)S.G\right).(H(IDS_k, B_1, t^*))$. Likewise, replay attack will be prevented due to the existence of $t_4$ in response message $\left\{B_2, R_2, IDS_k, PK_{SP_k}, t_4\right\}$ and is also hidden in $R_2.G \overset{?}{=} (B_2 + PK_{SP_k} + H(IDS_k, PK_{SP_k})S.G).\left(H(IDA_j, B_2, t_4)\right)$.

## 5. PERFORMANCE ANALYSIS AND COMPARISON

In this section, we analyze the performance of the proposed scheme and compare it with a number of recent considerable schemes in terms of security services and complexity.

### 5.1 Performance analysis

The important notations required for performance analysis of our proposed scheme and for the comparison with the recent related schemes and its execution time are given in Table 2.

**Table 2.** Required notations and execution time for all the crypto-operation

| Notation | Description | Execution time (ms) |
|---|---|---|
| $T_s$ | Time of ECC Scalar multiplication. | 2.226 |
| $T_{PA}$ | Time of point addition. | 0.0288 |
| $T_h$ | Time of one-way hash function. | 0.0023 |
| $T_{AED}$ | Time of asymmetric key encryption/decryption. | 4.4808 |
| $T_{SED}$ | Time of symmetric key encryption/decryption. | 0.0046 |
| $T_{\mathrm{pr}}$ | Time of a bilinear pairing operation. | 5.811 |
| $T_{mul}$ | Time of bilinear scalar multiplication. | 2.2260 |
| $T_{\mathrm{exp}}$ | Time of a modular exponentiation. | 3.85 |
| $T_{\mathrm{hp}}$ | Time of the map-to-point function. | 12.418 |
| $T_{\mathrm{log}}$ | Time of Solving the DL operation mod p. | $190.189*10^6$ |
| $T_c$ | Time of Chebyshev map operation. | 1.113 |

The complexity at the four entities in each stage of our proposed scheme is indicated in Table 3. The role of TTP appears in the initialization stage and registration stage; in the initialization stage, TTP requires one ECC scalar multiplication operation; however, in the registration stage, TTP requires six ECC scalar multiplication, three points addition operations, four hash function operations, and one asymmetric key encryption/decryption operation.

**Table 3.** Complexity of our proposed scheme

| Stage | TTP | SM | DA | SP |
|---|---|---|---|---|
| Initialization stage | $\mathrm{T_s}$ | - | - | - |
| Registration stage | $6\,T_s$+$3T_{PA}$+4 $T_h + T_{AED}$ | - | - | - |
| Authentication and key agreement stage | - | $4T_s$+ $T_{PA}$ + $6T_h$+ $2T_{AED}$ | $9T_s$ $+ 4T_{PA}$ $+ 10T_h$ $+ 2T_{AED}$ | $5T_s$ + 3 $T_{PA}$ + $4T_h$ |

In the authentication and key agreement stage, each SM requires four ECC scalar multiplication operations, one-point addition operation, six hash function operations, and two asymmetric key encryption/decryption operations. DA requires nine ECC scalar multiplication operations, four-point addition operations, ten hash function operations, and two asymmetric key encryption/decryption operations. SP requires five ECC scalar multiplication operations, three-point addition operations, and four hash function operations.

### 5.2 Security comparison

As the proposed authenticated key establishment scheme depends on the idea of data aggregation to reduce the burden on smart meters and transfers consumption data safely, we compare our proposed scheme with the schemes that depend on data aggregation [3, 28] in Table 4. From Table 4, it is obvious that our scheme and the other schemes support the authentication service. However, only our scheme and the anonymous metering scheme [3] can provide anonymity and untraceability of SM, while only our proposed scheme and Boudia et al.'s scheme [28] can resist against impersonation attack and replay attack. Finally, only our scheme can provide forward secrecy. From the previous comparison, we can conclude that our proposed scheme can provide more security services than other schemes [3, 28] that depend on using the same idea of data aggregation.

**Table 4.** Security comparison

| Security service | [3] | [28] | Ours |
|---|---|---|---|
| Mutual Authentication | √ | √ | √ |
| Anonymity of SM | √ | x | √ |
| Untraceability of SM | √ | x | √ |
| Forward Secrecy | x | x | √ |
| Impersonation attack Resilience | x | √ | √ |
| Replay attack Resilience | x | √ | √ |

### 5.3 Complexity comparison

In Table 5, we compare our scheme with the anonymous metering scheme [3] and multidimensional aggregation scheme [28]. In our proposed scheme, SM requires four ECC scalar multiplication operations, one-point addition operation, six hash function operations, and two asymmetric key encryption/decryption operations. Hence the SM's complexity is $(4T_s + T_{PA} + 6T_h + 2T_{AED})$ which needs 17.9082 ms to be executed. For the anonymous metering scheme [3], SM requires one bilinear pairing operation, six bilinear scalar multiplication operations, one modular exponentiation operation, and three map-to-point function operations. Hence the SM's complexity is $\left(1T_{pr} + 6\,T_{mul} + 1T_{exp}\ + 3T_{hp}\right)$ which needs 60.271 ms to be executed. It is well known that bilinear pairing operation is very complex than any other computations. For the multidimensional aggregation scheme [28], SM requires $(2n + 2)$ ECC scalar multiplication operations where $n$ is the number of data types. Hence the SM's complexity is $(2n + 2)T_s$ which needs 4.452n+4.452 ms to be executed.

Secondly, the complexity of DA in each scheme is obtained. In our scheme, the DA requires nine ECC scalar multiplication operations, four-point addition operations, ten hash function operations, and two asymmetric key encryption/decryption operations. Hence, the DA's complexity is $(9T_s + 4T_{PA} + 10T_h + 2T_{AED})$ which will be executed in 29.1338 ms. In the anonymous metering scheme [3], the DA requires one bilinear pairing operation, six bilinear scalar multiplication operations, five modular exponentiation operation, and five map-to-point function operations. Hence, the DA's complexity is $\left(1T_{pr} + 6\,T_{mul} + 5T_{exp}\ + 5T_{hp}\right)$ which will be executed in 100.507

ms. In the multidimensional aggregation scheme [28], the DA requires ($w$+2) ECC scalar multiplication operations where $w$ is the number of SMs. Hence the DA's complexity is $(w+2)T_s$ which will be executed in 4.452w+4.452 ms.

Finally, the complexity at SP in each scheme is computed successively. In our scheme, SP requires five scalar multiplication operation in ECC, three-point addition operation, and four hash function operations. Hence the SP's complexity is $(5T_s + 3T_{PA} + 4T_h)$ which will be executed in 11.2256ms. In the anonymous metering scheme [3], SP requires one bilinear pairing operation, one bilinear scalar multiplication operation, one modular exponentiation operation, and two map-to-point function operations. Hence the SP's complexity is $\left(1T_{pr} + 1\,T_{mul} + 1T_{exp}\ + 2T_{hp}\right)$ which will be executed in 36.723 ms. In the multidimensional aggregation scheme [28], SP requires ($w$+2) ECC scalar multiplication operations and $n$ solving the DL operation $mod\, p$. Hence, the SP's complexity is $(w+2)T_s + nT_{\log}$. Solving the DL operation needs too long time to be executed; however, parallel Pollard‟s Rho method can be used to speed up the computations. By implementing the algorithm on a cluster of 256 octa-core computers having PFLOPs capacity, solving the ECDLP requires 190189.061 sec. Hence, the execution of Boudia et al.'s scheme [28] requires $4.4524.452(w+2) + 190189061$ ms.

The real time complexity of our proposed scheme, the anonymous metering scheme [3], and multidimensional aggregation scheme [28] are given in Table 6. The real time complexity of Boudia et al.'s scheme [28] at the SM is dependent on the number of data types $n$, and it will be equivalent to our scheme at $n$=3. However, the real time complexity of Boudia et al.'s scheme [28] at the DA is dependent on the number of SMs ($w$), and it will be equivalent to our scheme at $w$=6. Lastly, the time complexity of Boudia et al.'s scheme [28] at the SP is dependent on the number of data type, the number of SMs, and the complexity of solving the DL. However, the real time of solving the DL operation which too long compared to the real time complexity of our proposed scheme at the SP regardless of the number of data type or the number of SMs.

**Table 5.** Complexity comparison

| Scheme | SM | DA | SP |
|---|---|---|---|
| [3] | $(1T_{pr} + 6\,T_{mul} + 1T_{exp} + 3T_{hp})$ | $(1T_{pr} + 6\,T_{mul} + 5T_{exp} + 5T_{hp})$ | $(1T_{pr} + 1\,T_{mul} + 1T_{exp} + 2T_{hp})$ |
| [28] | $(2n+2)T_s$ | $(w+2)T_s$ | $(w+2)T_s + nT_{\log}$ |
| Ours | $(4T_s + T_{PA} + 6T_h + 2T_{AED})$ | $(9T_s + 4T_{PA} + 10T_h + 2T_{AED})$ | $(5T_s + 3T_{PA} + 4T_h)$ |

**Table 6.** Real-time complexity comparison

| Scheme | SM (ms) | DA (ms) | SP (ms) |
|---|---|---|---|
| [3] | 60.271 | 100.507 | 36.723 |
| [28] | 4.452(n+1) | 4.452(w+1) | 4.452(w+1) + 190189061n |
| Ours | 17.9082 | 29.1338 | 11.2256 |

The previous discussion and comparison indicate that our scheme can reduce the overall computation costs compared to other recent related schemes as it produces better performance than other schemes in terms of computation complexity and real-time complexity; especially if the number of data types $n$>3 and the number of SMs>6.

## 6. CONCLUSION

In this paper, we relied on the idea of data aggregator to maintain the user's privacy and reduce the burden on smart meters, which has made us proposing a scheme for establishing keys between the smart meter and the data aggregator, and also between the data aggregator and the service provider by using elliptic curve cryptography. The proposed scheme has managed to overcome all the safety problems that are exposed to the related schemes. The proposed scheme can achieve mutual authentication between the different entities in smart grid, anonymity and untraceability of SM, and get rid of replay attack and impersonation attack. We have analyzed the efficiency of the proposed scheme in term of complexity; the proposed scheme also has managed to reduce the complexity compared to related schemes at the meter side, data aggregator side, and service provider side. In conclusion, the results demonstrate that our proposed scheme is a suitable key establishment scheme considering both security and efficiency.

## REFERENCES

[1] Wu, F., Xu, L., Li, X., Kumari, S., Karuppiah M., Obaidat, S. (2019). A lightweight and provably secure key agreement system for a smart grid with elliptic curve cryptography. IEEE Systems Journal, 13(3): 2830-2838. https://doi.org/10.1109/JSYST.2018.2876226

[2] Zhang, H., Wang J., Ding, Y. (2019). Blockchain-based decentralized and secure keyless signature scheme for smart grid. International Journal of Energy, 180: 955-967. https://doi.org/10.1016/j.energy.2019.05.127

[3] Xie, S., Zhang, F., Lin, H., Tian, Y. (2019). A new secure and anonymous metering scheme for smart grid communications. International Journal of Energies, 12(24): 1-16. https://doi.org/10.3390/en12244751

[4] Aloul, F., Al-Ali, A.R., Al-Dalky, R., Al-Mardini M., El-Hajj. W. (2012). Smart grid security: threats, vulnerabilities and solutions. International Journal of Smart Grid Clean Energy, 1(1): 1-6. https://doi.org/10.12720/sgce.1.1.1-6

[5] Kumar, P., Gurtov, A., Sain, M., Martin, A., Ha, P.H. (2019). Lightweight authentication and key agreement for smart metering in smart energy networks. International Journal of IEEE Transactions on Smart Grid, 10(4): 4349-4359. https://doi.org/10.1109/TSG.2018.2857558

[6] Xia, J., Wang, Y. (2012). Secure key distribution for the smart grid. International Journal of IEEE Transactions on Smart Grid, 3(3): 1437-1443. https://doi.org/10.1109/TSG.2012.2199141

[7] Wu, D., Zhou, C. (2011). Fault-tolerant and scalable key management for smart grid. International Journal of IEEE Transactions on Smart Grid, 2(2): 375-381. https://doi.org/10.1109/TSG.2011.2120634

[8] Maier, M., Ghazisaidi, N., Maier, M., Ghazisaidi, N. (2012). A lightweight message authentication scheme for

smart grid communications. International Journal of FiWi Access Networks, 2(4): 207-217. https://doi.org/10.1016/j.compeleceng.2016.02.017

[9] Mahmood, K., Ashraf, S., Naqvi, H., Shon, T. (2016). A lightweight message authentication scheme for smart grid communications in power sector. International Journal of Computers and Electrical Engineering, 52: 114-124. https://doi.org/10.1016/j.compeleceng.2016.02.017

[10] Aziz, I.T., Jin, H., Abdulqadder, I.H. (2018). A lightweight scheme to authenticate and secure the communication in smart grids. Applied Sciences, 8(9): 1508. https://doi.org/10.3390/app8091508

[11] Li, H., Lu, R., Zhou, L., Yang, B., Shen, X.S. (2014). An efficient Merkle-tree-based authentication scheme for smart grid. International Journal of IEEE System, 8(2): 655-663. https://doi.org/10.1109/JSYST.2013.2271537

[12] Liu, Y., Cheng, C., Gu, T., Jiang, T., Member, S., Li, X. (2016). A lightweight authenticated communication scheme for smart grid. International Journal of IEEE Sensors, 16(3): 836-842. https://doi.org/10.1109/JSEN.2015.2489258

[13] Mohammadali, A., Haghighi, M.S. (2016). A novel identity-based key establishment method for advanced metering infrastructure in smart grid. International Journal of IEEE Transactions on Smart Grid, 9(4): 2834-2842. https://doi.org/10.1109/TSG.2016.2620939

[14] Tsai, J., Lo, N. (2015). Secure anonymous key distribution scheme for smart grid. International Journal of IEEE Transactions on Smart Grid, 7(2): 906-914. https://doi.org/10.1109/TSG.2015.2440658

[15] Odelu, V., Das, A.K., Wazid, M., Conti, M., Member, S. (2016). Provably secure authenticated key agreement scheme for smart grid. International Journal of IEEE Transactions on Smart Grid, 9(3): 1900-1910. https://doi.org/10.1109/TSG.2016.2602282

[16] Chen, Y., Castillejo, P. (2017). An anonymous authentication and key establish scheme for smart grid: FAuth. Energies, 10(9): 1354. https://doi.org/10.3390/en10091354

[17] He, D., Wang, H., Khan, M.K., Wang, L. (2016). Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography. IET Communications, 10(14): 1795-1802. https://doi.org/10.1049/iet-com.2016.0091

[18] Zhang, L., Tang, S., Luo, H. (2016). Elliptic curve cryptography-based authentication with identity protection for smart grids. PLoS ONE, 11(3): 1-15. https://doi.org/10.1371/journal.pone.0151253

[19] Mahmood, K., Ashraf, S., Naqvi, H., Kumari, S. (2018). An elliptic curve cryptography based lightweight authentication scheme for smart grid communication. Future Generation Computer Systems, 81: 557-https://doi.org/10.1016/j.future.2017.05.002

[20] Farhadi, M., Nikooghadam, M., Hossein, A. (2020). A lightweight key management protocol for secure communication in smart grids. Electric Power Systems Research, 178: 106024. https://doi.org/10.1016/j.epsr.2019.106024

[21] Abbasinezhad-mood, D. (2018). An anonymous ECC-based self-certified key distribution scheme for the smart grid. IEEE Transactions on Industrial Electronics, 65(10): 7996-8004. https://doi.org/10.1109/TIE.2018.2807383

[22] Garg, S., Kaur, K., Kaddoum, G., Rodrigues, J.J.P.C., Member, S., Guizani, M. (2020). Secure and lightweight authentication scheme for smart metering infrastructure in smart grid. IEEE Transactions on Industrial Informatics, 16(5): 3548-3557. https://doi.org/10.1109/TII.2019.2944880

[23] Vahedi, E., Bayat, M., Pakravan, M.R., Aref, M.R. (2017). A secure ECC-based privacy preserving data aggregation scheme for smart grids. International Journal of Computer Networks, 129: 28-36. https://doi.org/10.1016/j.comnet.2017.08.025

[24] Kong, W., Shen, J., Vijayakumar, P., Cho, Y., Chang, V. (2020). A practical group blind signature scheme for privacy protection in smart grid. Journal of Parallel and Distributed Computing, 136: 29-39. https://doi.org/10.1016/j.jpdc.2019.09.016

[25] Wu, F., Li, X., Xu, L., Kumari, S. (2020). A privacy-preserving scheme with identity traceable property for smart grid. Computer Communications, 157: 38-44. https://doi.org/10.1016/j.comcom.2020.03.047

[26] Song, J., Liu, Y., Shao J., Tang, C. (2020). A dynamic membership data aggregation (DMDA) protocol for smart grid. International Journal of IEEE System, 14(1): 900-908. https://doi.org/10.1109/JSYST.2019.2912415

[27] Tahir, M., Khan, A., Hameed, A., Alam, M., Khan, M.K., Jabeen, F. (2017). Towards a set aggregation-based data integrity scheme for smart grids. Annals of Telecommunications, 72: 551-561. https://doi.org/10.1007/s12243-017-0602-7

[28] Merad Boudia, O.R., Senouci, S.M., Feham, M. (2017). Elliptic curve-based secure multidimensional aggregation for smart grid communications. IEEE Sensor Journal, 17(23): 7750-7757. https://doi.org/10.1109/JSEN.2017.2720458

[29] Chen, J., Shi, J., Zhang, Y. (2015). EPPDC: An efficient privacy-preserving scheme for data collection in smart grid. International Journal of Distributed Sensor Networks, 11(5): 1-12. https://doi.org/10.1155/2015/656219

[30] Zhang, X., Shen, X. (2019). Efficient privacy-preserving multi-dimensional data aggregation scheme in smart grid. IEEE Access, 7: 32907-32921. https://doi.org/10.1109/ACCESS.2019.2903533