The ISC Int'l Journal of Information Security

November 2022, Volume 14, Number 3 (pp. 101–112)

http://www.isecure-journal.org

Presented at the ISCISC'2022 in Rasht, Iran.

Light-Weight Privacy-Preserving Data Aggregation Protocols in Smart Grid Metering Networks ☆

Afshin Karampour [1,*], Maede Ashouri-Talouki [1], and Behrouz Tork Ladani [2]

[1] *Department of IT Engineering, Faculty of Computer Engineering University of Isfahan, Isfahan, Iran.*

[2] *Department of Software Engineering, Faculty of Computer Engineering University of Isfahan, Isfahan, Iran.*

ARTICLE INFO.

Keywords:
Smart Grid, Smart Meter, Data Aggregation, Privacy-Preserving, Elliptic Curve Cryptography, AV-Net Mask

Type:
Research Article

doi:
10.22042/isecure.2022.14.3.11

dor:
20.1001.1.20082045.2022.14.3.11.5

ABSTRACT

Smart grids using information technology (IT) and communication networks control smart home appliances to reduce costs and increase reliability and transparency. Preserving the privacy of the user data is one of the biggest challenges in smart grid research; by disclosing user-related data, an internal or external adversary can understand the habits and behavior of the users. A solution to address this challenge is, however, a data aggregation mechanism in which the aggregated data of all of the users in a residential area. The security and efficiency of the data aggregation approach are important. The drawback of the previous works is leaking fine-grained user data or the high computation and communication overhead. In this paper, we present an efficient privacy-preserving data-aggregation protocol, called PPDA, based on the Elliptic Curve Cryptography (ECC) and Anonymous Veto network protocol. The PPDA protocol aggregates metering data efficiently and securely so that it becomes applicable for resource-constraint metering devices. We also present an improved multi-cycle proposal of PPDA, called MC-PPDA. In the improved approach, the system initialization step runs only at the first cycle of the protocol which increases the efficiency of the protocol. Evaluation results show that the proposed approaches preserve the privacy of the fine-grained user data against an internal and external adversary; the improved multi-cycle approach is also secure against collusion. Compared to the previous approaches, the proposed approaches incur less computation and communication overhead.

1 Introduction

Privacy-preserving of metering data is one of the biggest challenges in the smart grid [1]. In smart grids amount of data is collected by smart meters (SMs) and sensors then it is sent to the control center (CC) to apply, monitor, and control tasks. The control center can apply to monitoring and controlling

* Corresponding author.

☆ The ISCISC'2022 program committee effort is highly acknowledged for reviewing this paper.

Email addresses: afshinkarampour@gmail.com, m.ashouri@eng.ui.ac.ir, ladani@eng.ui.ac.ir

ISSN: 2008-2045

duty by analysis of received data from SMs. Specially SM devices cyclically measure power consumption (e.g., 15 minutes) and report the metering data to the CC [2]. The connection between SMs and the CC is established through one or many interface stations like a gateway (GW). Indeed, SM devices send their metering data to the next station on the network or to the GW. Then the GW performs collecting and preprocessing (e.g., aggregation operation) on received data and sends the processed data to the next station or to the CC (unless there is another station). The CC analyses and processes the received data to extract statistical reports for further use. In such a system, privacy-preserving of metering data is very important and this means that fine-grained metering data by SMs should not be disclosed for any intermediate station and even the CC. Because by disclosing the metering data, the internal or external adversary can understand the habits and behaviors of the users [3]. In addition, privacy should be preserved in case of eavesdropping by an adversary or collusion. Data aggregation is a solution to protect users' fine-grained data from the middle nodes of the network and even from the CC, so by using aggregation, metering data is aggregated before sending it to the CC. In addition, data aggregation improves the network efficiency and reduces the network traffic, by sending each SM's data to the GW, and the GW aggregates them to send to the CC. Data aggregation has two benefits, including privacy-preserving metering data and increasing network efficiency [2]. In this paper, we consider the problem of aggregation of metering data by SMs with privacy-preserving as efficient and secure. In these networks, privacy-preserving of metering data is one of the important problems that in some of the proposed schemes data are disclosed to the semi-honest adversary. Also because of using weak process power by smart devices in the smart grid, computation and communication of the data aggregation schemes should be optimized. Our proposed approaches achieve privacy-preserving features for internal and external adversaries and give the promise to incur less computation and communication costs compared to previous works. In this paper, we propose a data aggregation scheme with the aim of privacy-preserving fine-grained data in the smart grid based on the Elliptic Curve Cryptography (ECC) and AV-net protocol called PPDA. This protocol is a third-trusted party (TTP) free, using elliptic curve cryptography and AV-net mask to solve the data aggregation problem. Also in this paper, we improved our PPDA protocol in a multi-cycle manner called MC-PPDA. During multi-cyclic execution, the initialization step runs only once in the first cycle which leads to an increase in the efficiency of the protocol. Evaluation results show that the proposed approaches preserve the privacy of fine-grained user data against an internal and external adversary; the improved multi-cycle approach is also secure against collusion. Compared to previous approaches, the proposed approaches incur less computation and communication costs. The remainder of this paper is organized as follows. We discuss the related works in Section 2. In Section 3, the system model and the threat model are explained. The preliminary background of the proposed approaches is discussed in Section 4. Then, we present the PPDA scheme and its security and performance analysis in Section 5. In Section 6, we explain and analyze an improved version of the PPDA protocol in a multi-cycle execution. In Section 7, the security and efficiency of our approaches are compared with the previous works and finally, the conclusion and future works are explained in Section 8.

2 Related Work

The existing works in the context of privacy-preserving data aggregation in smart grids are divided into two categories: TTP-based approaches and TTP-free approaches. In the following, we discuss them in more detail.

In 2017, Lu *et al.* [4] proposed a data aggregation approach (LPDA) based on the Paillier encryption system and the Chinese remainder theorem. Their system model consists of N IoT (Internet of Things) devices that generate data, a fog device that is located in a network bridge and a CC. They consider a semi-honest threat model. This scheme implements sender authentication using a hash chain to avoid fake data injection. Smart meters generate their ciphertext as $c_{is} = [1 + n \cdot \alpha_j \cdot (x_i \cdot \alpha_0 + x_i^2)] \cdot H(T_s)^{n \cdot s_i} \mod n^2$ using their metering data (x_i), the public key of the CC ($n = p \cdot q$), their private key (s_i), the received random number from the TTP (α_0) and the Chinese remainder theorem parameter (α_j) and then send them to the CC via the GW.

In 2016, Abdallah *et al.* [5] proposed a scheme for privacy-preserving data aggregation in a smart grid using the homomorphic encryption system (HES). In this scheme, a residential device is chosen as the aggregator of each round based on its ID. Then, all of the residential devices encrypt their data with the CC's public key and send them to the selected aggregator. The aggregator then aggregates the data and sends it to the CC. However, a semi-honest CC can eavesdrop on the SM's traffic and obtain the encrypted fine-grained data; then he can decrypt it and get the plain fine-grained data. Therefore, the privacy of the user-related data doesn't preserve from the CC's point of view.

In 2015, Chen *et al.* [6] presented a fault-tolerance scheme for privacy-preserving data aggregation called PDAFT. Their scheme aims to prevent data leakage even if a powerful adversary has compromised d servers out of k existing servers on the CC side ($d = k/2 - 1$). In this scheme, the CC extracts the aggregated data from at least $d + 1$ servers. Also, if an SM cannot send its data to the GW, the aggregator can still extract the aggregated data correctly; so, the fault tolerance property would be supported.

In 2017, Bao and Lu [7] introduced a scheme to meet the objectives of privacy and data integrity. Their system model consists of clusters where each cluster consists of many home area networks (HAN), and each HAN has one SM. Each cluster has a cluster head. Unlike most of the data, aggregation approaches in that SM are directly connected to GW, in this approach the cluster head is directly connected to GW. Therefore, the data aggregation operation is hierarchically done in two steps: firstly, the cluster head aggregates the received data from the connected HANs and then sends it to the GW. Second, the GW aggregates all the received data and sends it to the CC.

In 2015, Bao and Lu [8] proposed a data aggregation scheme using the Boneh-Goh-Nissim (BGN) encryption system [9] which is a homomorphic cryptography system. At the beginning of the protocol, the CC sends an aggregation request to the SMs via the GW ($A_1 = g^r, A_2 = h^{s_0 \cdot r}$). Then, the GW chooses a random number t and sends the aggregation request to the SMs ($A_3 = A_1^t, A_4 = A_2^t$); each SM encrypts its metering data using its private key (s_i) as $C_i = A_3^{m_i} \cdot A_4^{s_i}$ and sends it to the CC. Because the aggregated metering data is small, the CC can solve the discrete logarithm problem and find the aggregated data. This scheme leads to a high communication and computation overhead.

In 2013, Fan *et al.* [10] presented a data aggregation scheme to improve privacy and confront the internal adversaries in the semi-honest model. In this scheme, a TTP generates $n+1$ blinding factors where the sum of them is equal to zero. It sends the first blinding factor to the aggregator and the others to the SMs. To avoid the attack of internal adversaries, each SM is authenticated for the GW. This scheme incurs heavy computation overhead in the data aggregation phase.

In 2017, Tahir *et al.* [11] used a homomorphic encryption system and a hash chain to support privacy-preserving data integration in the smart grid. After generating data m_i by the i-th smart meter, it compares it with the threshold value (th). If $m_i > th$, then m_i computes c_i as $c_i = g^{m_i} \cdot h_1 \cdot H(t)^{x_i}$, otherwise it computes c_i as $c_i = h_0^{m_i} \cdot H(t)^{x_i}$ where t is the current time and x_i is the private key of SM_i.

In 2016, Knirsch *et al.* [12] proposed a data aggregation scheme using random noises. In each cycle of the data aggregation, CC chooses a random number and sends it to the first SM in the network (SM_i). After generating m_i by SM_i, it chooses a random number and computes the sum of its data and its random number and sends the result to the CC. Also, SM_i computes the sum of its random number and the received random number from the CC and sends it to the next SM on the network. This process continues until the CC receives the summation of all random numbers from the last SM. Finally, it can obtain the aggregated data by subtracting the received random numbers from the summation of noisy data. This proposed scheme is insecure against a collusion attack: the collusion of CC, SM_{i-1} and SM_{i+1}, would reveal the metering data of SM_i.

In 2017, li *et al.* [13] introduced a data aggregation scheme for several residential areas (RA) as PPMA. In this scheme, the whole RA is divided into several RAs and the CC can receive the aggregated data from some subset of RAs. In the generation data phase, each SM generates its cipher text as $c_i = g^{a_j \cdot \Delta \cdot m_i} \cdot g^{b_j} \cdot H(t)^{N \cdot x_i} \mod N^2$, using its private key (x_i) and the encryption parameters (g^{a_j}, g^{b_j}). This scheme imposes a heavy computational burden on the CC and SMs.

In 2015, Chen *et al.* [14] proposed a multifunctional data aggregation scheme by considering differential privacy. In this scheme, the CC can determine the function to apply to the aggregated data. The CC defines three functions consisting of average aggregation, variance aggregation, and one-way ANOVA aggregation. The GW performs a data aggregation process based on the CC request. In the case of the average aggregation function, the CC can eavesdrop on the SM's traffic and obtain the encrypted fine-grained data; then he can decrypt it and get the plain fine-grained data.

In 2018, Baran and Demir [15] presented a data aggregation scheme using data perturbation. Their scheme has four layers. In the first layer, SMs locate and generate their metering data. The second layer contains a task scheduler that performs data aggregation and transmits the metering data to PPNs (Privacy-Preserving Nodes). In the third layer the metering data is reconstructed and decrypted by PPNs and finally in the last layer utilities use the decrypted data.

In 2018, Braeken *et al.* [16] proposed a data aggregation scheme that supports price determining and

dynamic billing for different time slots. Their scheme considers the CC as a trusted node and contains eight steps including system initialization, smart meter deployment, customer registration phase, report generation, report aggregation, price determination and dynamic billing. However, they don't consider a collision attack.

In 2019, Karampour *et al.* [17] proposed a TTP-free data aggregation scheme based on the Paillier encryption system and AV-net mask. In their approach, at each cycle of sending metering data, a new AV-net mask must be created, otherwise, if the AV-net mask of the i-th and the $(i-1)$-th cycle are the same, then an adversary can catch the metering data. In this paper, we use a multiple-cycle approach to avoid this flaw and reduce the overhead of AV-net mask creation.

In 2020, Zhao *et al.* [18] presented a smart and practical privacy-preserving Data Aggregation (PDA) scheme that achieves multifunctional statistics; the authors have used homomorphic encryption (SHE) to preserve the user's privacy. However, their proposal incurs high overheads in terms of communication and computation.

In 2021, Khan *et al.* [19] proposed a TTP-based fault-tolerant privacy-preserving data aggregation scheme in a fog-enabled Boneh-Goh-Nissam (BGN) cryptosystem. In this scheme, the authors have applied fog nodes as the aggregator and put them between the SM layer and Cloud Control Center (CCC).

In 2022, Darzi *et al.* [20] proposed a TTP-based and multi-dimensional data aggregation scheme that used CC's public key to encrypt SM's data named LPM2DA. This approach has used lattice-based homomorphic encryption and Chinese remainder theorem (CRT) where based on polynomial CRT, each smart meter gathers all its multidimensional data into a single appropriate data and then encrypts and sends it to CC.

In 2022, Wu *et al.* [21] used ElGamal encryption to support privacy-preserving data aggregation in the smart grid while preserving user anonymity. Their adversary model is honest-but-curious and the internal node can eavesdrop on the channel. This scheme used the cloud as the aggregator that collects SM's data and sends it to the power station generating electricity as CC.

In 2021, Mohammadali and Haghighi [22] presented a TTP-based privacy-preserving homomorphic scheme with multiple dimensions and fault tolerance property for metering data aggregation in the smart grid based on the Paillier encryption system.

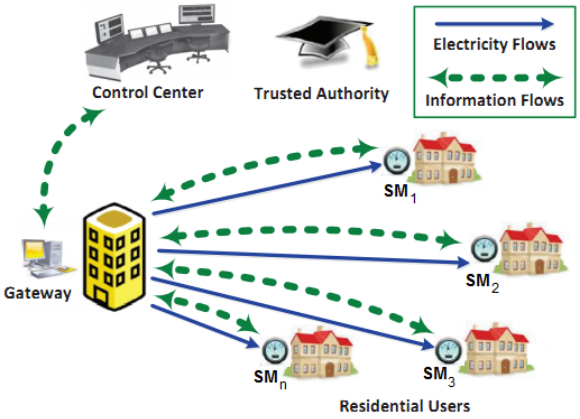

Figure 1. System model

3 System Model

In this section, we present the assumption and system model of our study. We assume that there is a residential area consisting of a set of n user $U = \{u_1, u_2, \ldots, u_n\}$ in smart home form and a gateway (as shown in Figure 1). Each user (u_i) is equipped with a smart meter (sm_i) that measures the power consumption and sends it to the gateway. The gateway is responsible for collecting and aggregating the metering data and sending it to the control center. Similar to most of the previous works [4, 5, 10, 18–21], we consider a semi-honest model as the protocol threat model and allow the existence of passive adversaries. Note that, this paper primarily focuses on the privacy of SM's data, so we only consider privacy disclosure attacks and leave other attacks as future work. Based on the above assumptions, the proposed protocol aims to compute the aggregate metering data without disclosing user fine-grained data to the control center, to the gateway and even to the smart metering devices, in case of partial collusion.

4 Preliminaries

The main building blocks used in designing the PPDA protocol are the AV-net and ECC schemes. The AV-net scheme was presented by Hao to solve the problem of anonymous vetoing [23, 24]. In this scheme, each participant selects a random number $x_i \in Z_q^*$, computes g^{x_i} and publishes it to all members. Doing so, each member can compute g^{y_i} through Equation 1.

$$g^{y_i} = \prod_{j=1}^{j=i-1} g^{x_i} / \prod_{j=i+1}^{n} g^{x_i} \quad (i = 1, 2, \ldots, n) \quad (1)$$

In the second round, each participant publishes $g^{c_i y_i}$ where c_i is equal to x_i if the user does not veto; or a random number otherwise. Upon computing $\prod g^{c_i y_i}$, if no user vetoes, the result is equal to 1 because of canceling the AV-net exponents; otherwise the result

is a random number without disclosing the vetoing user. We assume all entities agree on an ECC group $E(F_p)$ of prime order q and the AV-net generator G. CC chooses a random number k (from $[1, q-1]$) as its private key and then computes $K = k \cdot G$ as its public key. Also, all smart meters and the gateway know the public key of the control center in an elliptic curve cryptography system.

5 PPDA Protocol

The PPDA protocol applies the homomorphic feature [25] of elliptic curve cryptography to aggregate the fine-grained data at the gateway. It also applies the AV-net mask to hide the fine-grained data from the gateway point of view.

5.1 Scheme Description

As shown in Figure 2, the PPDA protocol has four major phases: *Initialization phase*, *Masking phase*, *Aggregation phase* and *Decryption phase*.

In the initialization phase, all smart meters in a residential area compute the AV-net mask to hide their metering data from all the inside or outside attackers including other smart meters, the gateway and the control center. To achieve this, each SM (SM_i) chooses a random number $x_i \in_R Z_q^*$ and publishes $x_i \cdot G$. Then, SM_i computes $y_i.G$ using received $x_j s$ from another SMs on the residential area according Equation 2:

$$y_i \cdot G = \sum_{j=1}^{i-1} x_j \cdot G - \sum_{j=i+1}^{n} x_j \cdot G \tag{2}$$

In the masking phase, each meter (SM_i) firstly maps its metering data (m_i) to a point (M_i) of the elliptic curve (E) using a map function [25, 26]. Then the i-th meter masks and encrypts its metering data using the AV-net mask and the control center public key and sends (C_1^i,C_2^i) to the gateway, as Equation 3:

$$\begin{aligned} C_1^i &= r_i \cdot G \\ C_2^i &= x_i \cdot y_i \cdot G + r_i \cdot K + M_i \end{aligned} \tag{3}$$

where r_i is a random number chosen by the i-th meter and K is the public key of the control center. After receiving all messages, GW computes their summation, as Equation 4 which results in canceling the AV-net mask [23] and computing the aggregate metering data encrypted by the public key of the control center. Then the gateway sends the result to the control center.

$$\begin{aligned} C_1 &= \textstyle\sum_{i=1}^{n} C_1^i = G \cdot \sum_{i=1}^{n} r_i \quad (i = 1, 2, \ldots, n) \\ C_2 &= \textstyle\sum_{i=1}^{n} C_2^i = K \cdot \sum_{i=1}^{n} r_i + \sum_{i=1}^{n} M_i \end{aligned} \tag{4}$$

PPDA Protocol

Phase 1 (Initialization phase):

I. $SM_i \rightarrow *$: $x_i.G$ where $x_i \in_R Z_q^*$

II. SM_i computes $y_i.G = \sum_{j=1}^{i-1} x_j.G - \sum_{j=i+1}^{n} x_j.G$

Phase 2 (Masking phase):

I. $SM_i \rightarrow GW$: (C_1^i, C_2^i) where $C_1^i = r_i.G$, $C_2^i = x_i.y_i.G + r_i.K + M_i$, M_i is the result of map function [23] of metering data (m_i), K is the CC's public key and r_i is a chosen random number

Phase 3 (Aggregation phase):

I. $GW \rightarrow CC$: (C_1, C_2) where $C_1 = \sum C_1^i = G.\sum r_i$ and $C_2 = \sum C_2^i = K.\sum r_i + \sum M_i$

Phase 4 (Decryption phase): k is the CC's private key: $K = k.G$

I. CC computes: $C = C_2 - k.C_1 = C_2 - k.G.\sum r_i = \sum r_i.K + \sum M_i - \sum r_i.K = \sum M_i$

→ * indicates message broadcast in the residential area

Figure 2. PPDA protocol

In the fourth phase, to find the aggregate metering data, the control center decrypts (C_1,C_2) using its private key applying Equation 5. Then, the CC obtains $\sum m_i$ by applying the inverse of map function [25] to the result of Equation 5 ($\sum M_i$) [24].

$$\begin{aligned} C &= C_2 - k \cdot C_1 = C_2 - k \cdot G \cdot \textstyle\sum r_i \ (i = 1, 2, \ldots, n) \\ &= \textstyle\sum r_i \cdot K + \sum M_i - \sum r_i \cdot K = \sum M_i \end{aligned} \tag{5}$$

5.2 Correctness Analysis

To prove the correctness of the PPDA protocol, it is enough to show that it generates the summation of all metering data encrypted by the public key of the control center. Without loss of generality, consider the i-th smart meter. The structure of i-th meter's message sent to the gateway contains $x_i \cdot y_i \cdot G$ (i-th mete's AV-net mask) to ensure the metering data privacy; $r_i \cdot K$ (i-th meter's random point to encrypt M_i); M_i and $r_i \cdot G$ to allow the decryption by the control center. Adding all C_2^i results in addition of all the AV-net masks ($\sum x_i \cdot y_i \cdot G$) plus $\sum r_i \cdot K$ and $\sum M_i$. Because of the vanishing property of AV-net mask [23], we have $\sum x_i \cdot y_i = 0$, so the result is ($G \sum r_i, \sum r_i \cdot K + \sum M_i$) which is the aggregate metering data encrypted by the public key of the control center.

5.3 Security Analysis

To analyze the security of the PPDA protocol, firstly, the privacy of the metering data against internal and

external adversary are assessed and then, the protocol behavior against the collusion attack is analyzed.

Property 1. PPDA protocol preserves the privacy of fine-grained metering data against internal adversaries.

Learning the metering data of a smart meter, a malicious meter or a gateway requires canceling the AV-net mask and also computes the control center's private key, but according to CDH problem, the attacker fails to compute the AV-net mask [23]. He also cannot compute the private key of the control center in the elliptic curve cryptography system [27]. In addition, a malicious control center, which eavesdrops on the communication channel between the meters and the gateway, is unable to learn the metering data because of the CDH property of the AV-net mask. Thus, no inside attacker learns the metering data.

Property 2. The PPDA protocol preserves the privacy of fine-grained metering data against external adversaries.

Similar to an internal attacker, an outside attacker who eavesdrops on the communication channel does not learn the metering data and the PPDA protocol preserves the metering data privacy against outsider attackers.

Property 3. The PPDA protocol preserves the privacy of the aggregate data.

The secrecy of the aggregated metering data is preserved in the PPDA protocol because the result of phase 3 is the aggregated data encrypted by the control center's public key in the elliptic curve cryptography system. Based on the security of the ECC, attackers could not reveal the aggregated data.

Property 4. The PPDA protocol is resistant to partial collusion attacks.

A partial collusion attack involves some participants but not all. Assume only one smart meter (SM_k) does not participate in a partial collusion attack against SM_i. Finding the metering data, the colluding meters should first decrypt (C_i^i, C_2^i) using the CC's private key. Doing so requires the CC to participate in the collusion, otherwise, it will fail. Considering the CC's participation, the colluding meters should compute the SM's AV-net mask $(x_i \cdot y_i \cdot G)$. However, the attackers cannot learn the AV-net mask in a partial collusion attack, because of the security of the AV-net scheme [23].

5.4 Performance Analysis

Computation cost: In PPDA protocol, each SM performs two-point multiplications and $(n-2)$ point-additions for computing the AV-net mask $(2T_{mulp} + (n-2)T_{addp})$ and two point-multiplications and two point-additions for generating its ciphertext. The GW does $2n-2$ point-additions to aggregate the data $((2n-2)T_{addp})$ and the CC performs two point-multiplications and one point-addition $(2T_{mulp} + T_{addp})$ to decrypt and access the aggregate data.

Communication cost: To analyze the communication cost of PPDA, we consider the parameters of NIST-P192 [26] and count the number of transmitted bits in different phases. SM-to-SM communication: In phase 1 of the protocol, each SM publishes $x_i \cdot G$ which results in a communication cost of 192 bits. SM-to-GW communication: In phase 2 of the PPDA protocol, data is masked and encrypted. The result is two points in the elliptic curve (E) which leads to the communication cost of 384 bits $(2 * 192 = 384)$. GW-to-CC communication: Considering the communication line between the GW and the CC, sending the aggregated data as two points in the elliptic curve by the GW results in the communication cost of 384 bits.

6 MC-PPDA Protocol

The PPDA scheme and other reviewed schemes of Section 2 assume a single execution of the protocol. Actually, in these schemes, the whole protocol should be repeated in each execution round. Considering a periodic data aggregation, each SM periodically sends its metering data to the CC at each predefined time slot. Considering w time slots in each time interval [7, 8], each SM should prepare and send its metering data in w rounds. In this section, we improve the PPDA scheme to efficiently work in a multi-cycle execution and call it the MC-PPDA.

6.1 Scheme Description

In the MC-PPDA protocol, the SMs generate the AV-net masks only at the first round of the protocol; the remaining rounds just use them. Similar to PPDA, MC-PPDA utilizes elliptic curve cryptography to protect the aggregated data from internal and external adversaries. Also, the MC-PPDA protocol uses a hash chain function [4] to avoid subtracting attacks. As shown in Figure 3 the MC-PPDA approach has four major phases consisting of *initialization phase*, *masking phase*, *aggregation phase* and *decryption phase* while the initialization phase runs only at the first round. In the first phase of MC-PPDA, the SMs generate the AV-net masks (as PPDA). Also, the GW chooses a hash function $(H_1 : \{0,1\}^* \rightarrow E(F_p))$ to compute a hash chain function. Considering a time interval consists of w time slots and SMs in RA, the GW

MC-PPDA Protocol

First cycle

Phase 1 (Initialization phase):

I. $SM_i \rightarrow *: x_i.G$ where $x_i \in_R Z_q^*$

II. SM_i computes $y_i.G = \sum_{j=1}^{i-1} x_j.G - \sum_{j=i+1}^{n} x_j.G$

III. GW $\Longrightarrow$ $*: H_{i0}$

w cycles

Phase 2 (Masking phase):

I. $SM_i \rightarrow GW: (C_1^{ij}, C_2^{ij})$ where

$C_1^{ij} = r_{ij}.G, C_2^{ij} = (x_i.y_i.G + r_{ij}.K + M_{ij}) + H_{ij}$

M_i is the result of map function [23] of metering data (m_i), K is the CC's public key and r_i is a chosen random number

Phase 3 (Aggregation phase):

I. GW computes:

$C_2^{ij} = C_2^{ij} - H_{ij} = (x_i.y_i.G + r_{ij}.K + M_{ij}) + H_{ij} - H_{ij}$

$= x_i.y_i.G + r_{ij}.K + M_{ij}$

II. $GW \rightarrow CC: (C_1^j, C_2^j)$ where $C_1^j = \sum C_1^{ij} = G.\sum r_{ij}$ and

$C_2^j = \sum C_2^{ij} = K.\sum r_{ij} + \sum M_{ij}$

Phase 4 (Decryption phase): k is the CC's private key: $K = k.G$

I. CC computes:

$C^j = C_2^j - k.C_1^j = C_2^j - k.G.\sum r_{ij}$

$= \sum r_{ij}.K + \sum M_{ij} - \sum r_{ij}.K = \sum M_{ij}$

$\rightarrow$ * Indicates message broadcast in the residential area

$\Longrightarrow$ Indicates secure channel

Figure 3. MC-PPDA protocol

chooses n hash chains $(HC_1, HC_2, \ldots, HC_n)$ where each hash chain include $w+1$ values determined as follow: $HC_i = \{H_{i0}, H_{i1}, \ldots, H_{iw}\}, i = 1, 2, \ldots, n$.

The first value of each hash chain function is selected at random ($H_{i0} \in E(F_q)$) and other values are computed as Equation 6 where T_j is the j-th time slot. Finally, the GW sends h_{i0} to the i-th meter through a secure channel.

$$H_{ij} = H_1(H_{i(j-1)}|T_j) \quad j = 0, \ldots, w \tag{6}$$

In the masking phase, each SM (i-th SM) in the j-th cycle of sending data, firstly uses a map function (invertible function) to map its metering data (m_{ij}) to a point of the elliptic curve $M_{ij} \in E$ [21, 24]. Then, he computes and sends C_1^{ij}, C_2^{ij}, T_j to the CC where C_1^{ij} and C_2^{ij} are computed according to Equation 7. Where r_{ij} is a random number chosen by the i-th meter, $K = k \cdot G$ is the public key of the CC, k is the private key of CC, $x_i \cdot y_i \cdot G$ is the generated AV-net mask and H_{ij} is the j-th value of i-th SM hash chain.

$$\begin{aligned} C_1^{ij} &= r_{ij}.G \\ C_2^{ij} &= (x_i \cdot y_i \cdot G + r_{ij} \cdot K + M_{ij}) + H_{ij} \end{aligned} \tag{7}$$

In phase 3, after receiving all values in the j-th time slot, the GW aggregates the data. Achieving this, he firstly computes and removes H_{ij} from C_2^{ij} of each SMs (Equation 8), and he then computes the aggregate data through Equation 9. Notice that the summation of all AV-net values is equal to zero in this equation ($\sum x_i \cdot y_i = 0$) [23]. Finally, the GW sends the result (C_1^j and C_2^j) to the CC.

$$\begin{aligned} C_2^{ij} &= C_2^{ij} - H_{ij} \\ &= (x_i \cdot y_i \cdot G + r_{ij} \cdot K + M_{ij}) + H_{ij} - H_{ij} \\ &= x_i \cdot y_i \cdot G + r_{ij} \cdot K + M_{ij} \end{aligned} \tag{8}$$

$$\begin{aligned} C_1^j &= \sum C_1^{ij} = G \cdot \sum r_{ij} \\ C_2^j &= \sum C_2^{ij} = K \cdot \sum r_{ij} + \sum M_{ij} \end{aligned} \tag{9}$$

In the decryption phase, the CC decrypts the result through Equation 10 and gets the aggregated data of j-th time slot. The CC can achieve $\sum m_{ij}$ by decoding $\sum M_{ij}$ [24].

$$\begin{aligned} C^j &= C_2^j - k \cdot C_1^j = C_2^j - k \cdot G \cdot \sum r_{ij} \\ &= \sum r_{ij} \cdot K + \sum M_{ij} - \sum r_{ij} \cdot K = \sum M_{ij} \end{aligned} \tag{10}$$

6.2 Correctness Analysis

Similar to PPDA, to prove the correctness of the MC-PPDA it suffices to show that MC-PPDA generates the summation of all metering data encrypted by the public key of CC in ECC. In j-th round, each SM generates $(r_{ij} \cdot G, x_i \cdot y_i \cdot G + r_{ij} \cdot K + M_{ij} + H_{ij})$ and sends it to the GW. The GW firstly eliminates the hash chain from the second part of the received data, then he aggregates the first part of all messages and also the second part of all messages which results in canceling the AV-net mask and getting the aggregated metering data encrypted by the CC's public key ($G \cdot \sum r_{ij}, K \cdot \sum r_{ij} + \sum M_{ij}$) and the proof is complete.

6.3 Security Analysis

To evaluate the security of the MC-PPDA, we show that it preserves the privacy of the metering data generated by each SM against internal and external adversaries and also its resistance against the collusion attack. Due to the multiple rounds of the MC-PPDA, we also analyze the protocol behavior against the subtraction attack.

Property 1. MC-PPDA protocol preserves the privacy of the fine-grained metering data against internal adversaries.

Because of applying the ECC and the AV-net mask, the GW and the CC cannot access the fine-grained data. If a malicious SM or a malicious CC eavesdrops on the communication between an SM and the GW, he cannot learn any information about the metering data. This is because he cannot cancel the AV-net mask [23]. In addition, a malicious SM requires the

CC's private key which cannot be computed [25]. Thus, no insider learns the metering data.

Property 2. MC-PPDA protocol preserves the privacy of fine-grained data against external adversaries. Similar to the internal adversary scheme, an external adversary does not learn the metering data because he is not able to compute the AV-net mask and CC's private key. So, the MC-PPDA provides metering data privacy against outsider attackers.

Property 3. The MC-PPDA protocol preserves the privacy of the aggregate data.

External adversaries or GW does not learn the aggregated metering data. This is because of producing the encrypted aggregated data by the GW. Based on the security of the ECC, attackers could not reveal the aggregated data.

Property 4. The MC-PPDA protocol is resistant to partial collusion attacks.

Assume the collusion of $n-2$ SMs against SM_i. Finding the metering data, the colluding meters should firstly remove the hash chain value, secondly decrypt (C_1^i, C_2^i) using the CC's private key and finally remove the AV-net mask. Removing the hash chain and decrypting the result requires the GW and the CC to participate in the attack, otherwise, it will fail. Considering the GW and the CC participation, the colluding meters should compute the SM_i's AV-net mask $(x_i \cdot y_i \cdot G)$ which is not possible in a partial collusion attack [23]. Therefore, the MC-PPDA is secure against a partial collusion attack.

Property 5. The MC-PPDA protocol is secure against the subtracting attack.

If a malicious adversary eavesdrops on the two consecutive communication rounds, he cannot learn any useful information. Without loss of generality, consider the SM_k's metering data in j-th and $(j+1)$-th rounds. If an adversary eavesdrops on these two messages and subtracts them, then he obtains a random number:

$$
\begin{aligned}
&C_2^k j - C_2^{(kj+1)} \\
&= (x_k \cdot y_k \cdot G + r_{kj} \cdot K + M_{kj}) + H_{kj} \\
&-[(x_k \cdot y_k \cdot G + r_{(kj+1)} \cdot K + M_{(kj+1)}) + H_{(kj+1)}] \\
&= (r_{kj} - r_{(kj+1)})K + (M_{kj} - M_{(kj+1)}) \\
&+(H_{kj} - H_{(kj+1)}) \equiv random
\end{aligned}
$$

Even if the GW performs this attack, he cannot learn any useful data, because he gets the differential of the metering data in an encrypted form by the CC's public key:

$$
\begin{aligned}
&x_k \cdot y_k \cdot G + r_{kj} \cdot K + M_{kj} - x_k \cdot y_k \cdot G \\
&+r_{(kj+1)} \cdot K + M_{(kj+1)} \\
&= (r_{kj} - r_{(kj+1)})K + M_{kj} - M_{(kj+1)} \\
&\equiv random
\end{aligned}
$$

The same is true for the CC: he cannot learn anything except a random number in a subtraction attack. Only in case of collusion of the GW and the CC, they can achieve the differential metering data of two consecutive rounds; in this case, there is no point for the SM to participate in the protocol.

6.4 Performance Analysis

Computation cost: To analyze the computation cost of the MC-PPDA, we count the number of operations of each entity. In the first phase of the protocol, each SM performs two-point multiplications and $(n-2)$ point additions to compute the AV-net mask; this phase runs only once. In each cycle of the second phase, each SM does two point-multiplications, three point-additions and one hash function to generate its ciphertext $(2T_{mulp} + 3T_{addp} + T_{hash})$. The GW does $2n-1$ point-additions and n hash functions to aggregate the data $((2n-1)T_{addp} + T_{hash})$; finally, the CC performs one point-multiplication and one point-addition $(T_{mulp} + T_{addp})$ to decrypt the aggregate data.

Communication cost: The communication cost of MC-PPDA is the same as PPDA because publishing data are points of an elliptic curve. Thus, we have a communication cost of 192 bits for the SM-to-SM path and 384 bits $(2 * 192 = 384)$ for SM-to-GW and GW-to-CC.

7 Comparison

The proposed protocols are compared with [4, 6–8, 13, 18–22, 26] schemes in Table 1. These protocols are selected because all of them preserve privacy against external attackers and are more efficient than other approaches introduce in Section 2.

Regarding the security comparison, we consider the privacy against the internal and external adversary and also the collusion of network entities against a victim SM. As shown in Table 1, two schemes that do not preserve privacy against an internal adversary are [20, 26]. In particular, in [20, 26] if the CC eavesdrops on the communication between a victim SM and the GW in the data generation phase, and sends the eavesdropping data to the victim SM in the distributed decryption phase, then, he can extract the fine-grained data and violate the privacy. The schemes of [4, 8] are vulnerable to a full collusion attack while the schemes of [6, 7, 13] are vulnerable to a partial collusion attack: the collusion of $n-1$ SMs and the

CC would reveal the victim SM's fine-grained data.

To have a fair efficiency comparison, we ignore the authentication cost of the approaches of [4, 6–8, 13, 18–22, 26]. So, the communication cost of Bao *et al.* [8] is 2560 bits for each SM-to-GW and 2560 bits for GW-to-CC communication, considering N as a 1024-bit length integer. The communication costs of [6, 13] are the same and are 2048 bits for each SM-to-GW and GW-to-CC communication. In [4] the communication cost is 2208 bits for each SM-to-GW and 2048 bits for GW-to-CC, same as [6, 13]. The communication cost of [7] is 2196 bits and 2176 bits for each SM-to-GW and GW-to-CC communication, respectively. In [19–21] the communication cost of SM-to-GW and GW-to-CC are 1024 bits. The communication cost of SM-to-GW in [18] is 2048 bits, while it is 1024 bits for GW-to-CC. In [20] the cost of SM-to-GW is 1024 bits and 3072 bits for GW-to-CC. Similar to our schemes, Liu *et al.* [26] incurs the communication cost of 352 bits for each SM. In this scheme, the communication cost is 896 bits for each SM-to-GW and 896 bits for GW-to-CC communication. In comparison, the communication cost of the proposed schemes is less than other schemes for SM-to-GW and GW-to-CC communications and is less than [26] for SM-to-SM communication. To analyze the computation cost, we count the number of operations of each entity and present it in Table 1. In Liu *et al.* [26], each SM performs five point-multiplications and $(n-1)$ point additions. The GW performs $(2n-2)$ point-additions and the CC does n point-additions and one logarithm function. In Bao *et al.* [8], each SM does two exponents, the GW performs three exponents and $(n-1)$ multiplications and finally, the CC performs three exponents and two multiplications and one logarithm function. In [4] each SM runs one exponent, five multiplications, two additions, one hash function and one AES-encryption function. The GW does one exponent, $(n-1)$ multiplications, two hash functions and n AES-decryption functions. The CC performs one exponent and one multiplication. In [6] each SM performs two exponents and one hash function. The GW runs $(n-1)$ multiplications for aggregation and the CC does three exponents and $(2d+2)$ multiplications. In [7], each SM does three exponents, three hash functions and one AES-encryption function. The GW runs n multiplications, two hash functions, n AES-decryption functions and one AES-encryption and the CC performs two exponents, one multiplication, two hash functions, one AES-decryption function and one logarithm function. In [13] each SM performs two exponents, four multiplications, one addition and one hash function. The GW runs $(n-1)$ multiplications for aggregation and the CC does three exponents, $(4n+3)$ multiplications, $(5n+1)$ additions and one hash function. In [18], SM performs two multiplications and three additions; GW performs $(k+nk+1)$ multiplications and $(n+k+2nk-4)$ additions where k is the security parameter; CC performs n exponents, n multiplications and n additions. In [19], SM performs two exponents and four multiplications; GW performs n multiplications while CC performs one multiplication and one logarithm. In [20], SM performs $(3n+3)$ multiplications and two additions; GW performs n multiplications and $3n$ additions and CC performs three multiplications. In [21], SM performs two exponents, two multiplications and one addition; GW performs two exponents, $(n-1)$ multiplications and two hash functions and CC performs three multiplications and two hash functions. In [22], SM performs two exponents, one multiplication, two additions and one hash function; GW performs $(n-1)$ multiplications and CC performs one exponent and n hash functions. In summary, the proposed schemes incur less computation cost for the smart meters, the gateway and the CC. In particular, the computation cost of MC-PPDA is less than other approaches, because all of the phases of the previous works should be completely repeated for each execution of the protocol. For example, to adopt the Liu *et al.* [26] in multi-execution, it is necessary to run w instances of the protocol which results in a computation cost of $w(5T_{mulp}+(n-1)T_{addp})$ per smart meter. However, the MC-PPDA only incurs $w(2T_{mulp}+3T_{addp}+T_{hash})$ computation cost per smart meter. It should be noted that the computation cost of the initialization phase of MC-PPDA only incurs once which makes the protocol more efficient.

8 Conclusion

Recently, privacy-preserving data aggregation in smart grids has attracted a lot of concerns. Disclosing the fine-grained metering data would reveal users' habits and behavior, thus, many researchers work on preserving the privacy of fine-grained metering data. In most of the proposed approaches, homomorphic encryption systems like Paillier and BGN are used. These approaches impose a heavy computational cost on the SMs which are resource-constraint devices. In this paper, we presented an efficient approach for privacy-preserving data aggregation using the AV-net mask and the ECC, named PPDA. The PPDA is a TTP-free protocol. We have also improved our PPDA protocol to efficiently work in a multi-cycle execution, called MC-PPDA. Security analysis shows that the proposed schemes are secure against collusion and preserve the privacy of the fine-grained metering data against internal and external adversaries.

In future work, we aim to add fault tolerance properties to our schemes and support multifunctional and multidimensional data.

Table 1. Comparing of security and performance

Performance						Security			Scheme
Communication overhead			Computational overhead			Security against collusion	Privacy		
GW to CC	SM to GW	SM to SM	CC	GW	SM		External attacker	Internal attacker	
2048	2208	–	$T_{exp}+T_{mul}$	$T_{exp}+(n+1)T_{mul}$ $+2T_{hash}+nT_{AES}$	$T_{exp}+5T_{mul}+2T_{add}$ $+T_{hash}+T_{AES}$	*Full*	✓	✓	[4]
2048	2048	–	$3T_{exp}+(2d+2)T_{mul}$	$(n-1)T_{mul}$	$2T_{exp}+T_{hash}$	$(n-1)SM$ $,CC$	✓	✓	[6]
2176	2196	–	$2T_{exp}+T_{mul}+2T_{hash}$ $+T_{AES}+T_{log}$	$nT_{mul}+2T_{hash}$ $+(n+1)T_{AES}$	$3T_{exp}+3T_{hash}+T_{AES}$	$(n-1)SM$ $,CC$	✓	✓	[7]
2560	2560	–	$3T_{exp}+2T_{mul}+T_{log}$	$3T_{exp}+(n-1)T_{mul}$	$2T_{exp}$	*Full*	✓	✓	[8]
2048	2048	–	$3T_{exp}+(4n+3)T_{mul}$ $+(5n+1)T_{add}+T_{hash}$	$(n-1)T_{mul}$	$2T_{exp}+4T_{mul}$ $+T_{add}+T_{hash}$	$(n-1)SM$ $,CC$	✓	✓	[13]
1024	2048	–	$nT_{exp}+nT_{mul}+nT_{add}$	$(k+nk+1)T_{mul}+$ $(n+k+2nk-4)T_{add}$	$2T_{mul}+3T_{add}$	$(n-1)SM$ $,CC$	✓	✓	[18]
1024	1024	–	$T_{mul}+T_{log}$	nT_{mul}	$2T_{exp}+4T_{mul}$	$(n-1)SM$ $,CC$	✓	✓	[19]
3072	1024	–	$3T_{mul}$	$nT_{mul}+3nT_{add}$	$(3n+3)T_{mul}+2T_{add}$	CC	✓	×	[20]
1024	1024	–	$3T_{mul}+2T_{hash}$	$2T_{exp}+(n-1)T_{mul}$ $+2T_{hash}$	$2T_{exp}+2T_{mul}+T_{add}$	$(n-1)SM$ $,CC$	✓	✓	[21]
1024	1024	–	$T_{exp}+nT_{hash}$	$(n-1)T_{mul}$	$2T_{exp}+T_{mul}$ $+2T_{add}+T_{hash}$	*Full*	✓	✓	[22]
896	896	352	$T_{log}+nT_{addp}$	$(2n-2)T_{addp}$	$5T_{mulp}+(n-1)T_{addp}$	CC	✓	×	[26]
384	384	192	$2T_{mulp}+T_{addp}$	$(2n-2)T_{addp}$	$4T_{mulp}+nT_{addp}$	$(n-1)SM$ $,CC$	✓	✓	PPDA
384	384	192	$T_{mulp}+$ $w(T_{mulp}+T_{addp})$	$w((2n-1)T_{addp}$ $+T_{hash})$	$(2T_{mulp}+(n-2)T_{addp})$ $+w(2T_{mulp}+3T_{addp}$ $+T_{hash})$	*Full*	✓	✓	MC-PPDA

References

[1] Ye Yan, Yi Qian, Hamid Sharif, and David Tipper. A survey on cyber security for smart grid communications. *IEEE communications surveys & tutorials*, 14(4):998–1010, 2012.

[2] Rongxing Lu. *Privacy-enhancing aggregation techniques for smart grid communications*. Springer, 2016.

[3] Elias Leake Quinn. *Smart Metering & Privacy: Existing Law and Competing Policies: a Report for the Colorado Public Utilities Commission*. Colorado Public Utilities Commission, 2009.

[4] Rongxing Lu, Kevin Heung, Arash Habibi Lashkari, and Ali A Ghorbani. A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced iot. *IEEE access*, 5:3302–3312, 2017.

[5] Asmaa Abdallah and Xuemin Sherman Shen. A lightweight lattice-based homomorphic privacy-preserving data aggregation scheme for smart grid. *IEEE Transactions on Smart Grid*, 9(1):396–405, 2016.

[6] Le Chen, Rongxing Lu, and Zhenfu Cao. Pdaft: A privacy-preserving data aggregation scheme with fault tolerance for smart grid communications. *Peer-to-Peer networking and applications*, 8(6):1122–1132, 2015.

[7] Haiyong Bao and Rongxing Lu. A lightweight data aggregation scheme achieving privacy

preservation and data integrity with differential privacy and fault tolerance. *Peer-to-Peer Networking and Applications*, 10(1):106–121, 2017.

[8] Haiyong Bao and Rongxing Lu. A new differentially private data aggregation with fault tolerance for smart grid communications. *IEEE Internet of Things Journal*, 2(3):248–258, 2015.

[9] Dan Boneh, Eu-Jin Goh, and Kobbi Nissim. Evaluating 2-dnf formulas on ciphertexts. In *Theory of cryptography conference*, pages 325–341. Springer, 2005.

[10] Chun-I Fan, Shi-Yuan Huang, and Yih-Loong Lai. Privacy-enhanced data aggregation scheme against internal attackers in smart grid. *IEEE Transactions on Industrial informatics*, 10(1):666–675, 2013.

[11] Mouzna Tahir, Abid Khan, Abdul Hameed, Masoom Alam, Muhammad Khurram Khan, and Farhana Jabeen. Towards a set aggregation-based data integrity scheme for smart grids. *Annals of Telecommunications*, 72(9):551–561, 2017.

[12] Fabian Knirsch, Günther Eibl, and Dominik Engel. Error-resilient masking approaches for privacy preserving data aggregation. *IEEE Transactions on Smart Grid*, 9(4):3351–3361, 2016.

[13] Shaohua Li, Kaiping Xue, Qingyou Yang, and Peilin Hong. Ppma: Privacy-preserving multisubset data aggregation in smart grid. *IEEE Transactions on Industrial Informatics*, 14(2):462–471, 2017.

[14] Le Chen, Rongxing Lu, Zhenfu Cao, Khalid Alharbi, and Xiaodong Lin. Muda: Multifunctional data aggregation in privacy-preserving smart grid communications. *Peer-to-peer networking and applications*, 8(5):777–792, 2015.

[15] Ulas Baran Baloglu and Yakup Demir. Lightweight privacy-preserving data aggregation scheme for smart grid metering infrastructure protection. *International Journal of Critical Infrastructure Protection*, 22:16–24, 2018.

[16] An Braeken, Pardeep Kumar, and Andrew Martin. Efficient and privacy-preserving data aggregation and dynamic billing in smart grid metering networks. *Energies*, 11(8):2085, 2018.

[17] Afshin Karampour, Maede Ashouri-Talouki, and Behrouz Tork Ladani. An efficient privacy-preserving data aggregation scheme in smart grid. In *2019 27th Iranian Conference on Electrical Engineering (ICEE)*, pages 1967–1971. IEEE, 2019.

[18] Shuai Zhao, Fenghua Li, Hongwei Li, Rongxing Lu, Siqi Ren, Haiyong Bao, Jian-Hong Lin, and Song Han. Smart and practical privacy-preserving data aggregation for fog-based smart grids. *IEEE Transactions on Information Forensics and Security*, 16:521–536, 2020.

[19] Hayat Mohammad Khan, Abid Khan, Farhana Jabeen, and Arif Ur Rahman. Privacy preserving data aggregation with fault tolerance in fog-enabled smart grids. *Sustainable Cities and Society*, 64:102522, 2021.

[20] Saleh Darzi, Bahareh Akhbari, and Hassan Khodaiemehr. Lpm2da: a lattice-based privacy-preserving multi-functional and multi-dimensional data aggregation scheme for smart grid. *Cluster Computing*, 25(1):263–278, 2022.

[21] Liang Wu, Wenzheng Zhang, and Wei Zhao. Privacy preserving data aggregation for smart grid with user anonymity and designated recipients. *Symmetry*, 14(5):847, 2022.

[22] Amin Mohammadali and Mohammad Sayad Haghighi. A privacy-preserving homomorphic scheme with multiple dimensions and fault tolerance for metering data aggregation in smart grid. *IEEE Transactions on Smart Grid*, 12(6):5212–5220, 2021.

[23] Maede Ashouri-Talouki, Ahmad Baraani-Dastjerdi, and Ali Aydın Selçuk. Glp: A cryptographic approach for group location privacy. *Computer Communications*, 35(12):1527–1533, 2012.

[24] Feng Hao and Piotr Zieliński. A 2-round anonymous veto protocol. In *International Workshop on Security Protocols*, pages 202–211. Springer, 2006.

[25] Ming-quan Hong, Peng-Yu Wang, and Wen-Bo Zhao. Homomorphic encryption scheme based on elliptic curve cryptography for privacy protection of cloud computing. In *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, pages 152–157. IEEE, 2016.

[26] Yining Liu, Wei Guo, Chun-I Fan, Liang Chang, and Chi Cheng. A practical privacy-preserving data aggregation (3pda) scheme for smart grid. *IEEE Transactions on Industrial Informatics*, 15(3):1767–1774, 2018.

[27] Victor S Miller. Use of elliptic curves in cryptography. In *Conference on the theory and application of cryptographic techniques*, pages 417–426. Springer, 1985.

Afshin Karampour received his bachelor's degree in computer engineering from the Jahade Daneshgahi of Kermanshah University (JDKU), Kermanshah, Iran, in 2011 and an M.Sc. degree in information security from the University of Isfahan (UI), Isfahan, Iran, in 2019. His research interests are privacy and data hiding.

Maede Ashouri-Talouki is an Assistant Professor in the IT Engineering department of the University of Isfahan (UI). She received her B.Sc., M.Sc., and Ph.D. degrees from the University of Isfahan in 2004, 2007, and 2012, respectively. In 2013, she joined the University of Isfahan. Her research interests include mobile networks security, user privacy and anonymity, cryptographic protocols, and network security.

Behrouz Tork Ladani received his bachelor's degree in computer engineering from the University of Isfahan (UI), Isfahan, Iran, in 1996, M.Sc. degree in software engineering from the Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran, in 1998, and a Ph.D. degree in software engineering from the University of Tarbiat Modarres, Tehran, in 2005. His research interests are around modeling, analysis, and verification of security in information systems, including software security (vulnerability detection and malware analysis) and soft security (computational trust and rumor control in social networks). Dr. Tork Ladani is a member of the Iranian Society of Cryptology (ISC) and has been a Program Committee Member of the International ISC Conferences on Cryptology and Information Security (ISCISC). He is the Managing Editor of the Journal of Computing and Security (JCS) and a member of the Editorial Board of the International Journal of Information Security Science (IJISS).