MPDA-HPR: Multi-Dimensional Privacy-Preserving Data Aggregation Based on Homomorphic Proxy Re-Encryption for Industrial Internet of Things

Qingyang Zhang, Zhen Fang, Jie Cui, *Senior Member, IEEE*, Hulin Jin, Fengqun Wang, and Debiao He

***Abstract*—As modern communication technologies advance, the Industrial Internet of Things (IIoT) is progressively evolving towards greater intelligence. The extensive implementation of smart grids has significantly affected IIoT factories. Data aggregation is commonly used to protect the factory's privacy. However, existing multi-dimensional data aggregation schemes lack flexibility and are vulnerable to internal attacks, where private data from certain smart devices may be decrypted by insiders. Moreover, replacing related devices necessitates updating the keys of the entire system, which incurs heavy overhead. To address these issues, a multi-dimensional privacy-preserving data aggregation scheme based on homomorphic proxy re-encryption (MPDA-HPR) is proposed. Using a modified Paillier encryption algorithm supported by proxy re-encryption and super-increasing sequences, the proposed scheme enhances flexibility and scalability. Security analyses demonstrate that the proposed scheme can withstand various security threats and effectively preserve the privacy of devices. Finally, the prototype is implemented and evaluated, demonstrating that the proposed scheme is robust, efficient, and feature-rich.**

***Index Terms*—Privacy-preserving data aggregation, super-increasing sequences, homomorphic encryption, proxy re-encryption, IIoT.**

I. Introduction

THE smart grid is a crucial component of the modern Industrial Internet of Things (IIoT) [1], [2], [3]. It achieves a reliable, efficient, and sustainable operation of power systems using real-time data and intelligent control techniques [4] that are helpful for industrial production scheduling. Typically, the infrastructure of the smart grid in the IIoT includes smart sensors (SS), an aggregator gateway (AG), and an electricity control center (ECC) [5], [6]. The smart sensors in factories are deployed within industrial devices to collect electricity usage data and transmit it regularly to the aggregator gateways [7]. Aggregator gateways operate within industrial area networks, collect and consolidate data, reduce data transmission frequency, and lower system load and costs. Electricity control centers analyze this data using mathematical and statistical algorithms to support decisions such as load optimization, fault warning, electricity price regulation, and emergency response measures.

While the smart grid of the IIoT offers advantages in power management and dispatching, it also introduces significant privacy and security concerns [8]. Most data transmission in the smart grid of the IIoT occurs through wireless communication links, which may include sensitive information such as the factory's production capacity [9], [10], [11]. Attackers can exploit privacy breaches for gain [12]. Therefore, it is necessary to develop effective security schemes to preserve the granular data of IIoTs from unauthorized access.

Privacy-preserving data aggregation (PPDA) can ensure the effectiveness of data analyses and mining while minimizing the risk of privacy leaks. Studies have indicated that homomorphic encryption is an effective technique. Homomorphic encryption supports direct computation on ciphertext, enabling the processing of sensitive information without exposing the original data. However, most homomorphic encryption schemes focus solely on electricity consumption scenarios [13], [14], [15], [16], [17], [18], preventing electricity control centers from conducting multi-dimensional analyses and managing regional electricity usage patterns. In practical environments, multiple types of information regarding electricity usage exist. Existing single-dimensional aggregation schemes must handle multi-dimensional electricity usage data individually. Moreover, because smart sensors regularly report data to aggregator gateways, the reported plaintext data are generally significantly smaller than the plaintext space of the encryption algorithms, leading to significant computational resource waste when encrypting single-dimensional data [19]. In response to these challenges, some studies have proposed multi-dimensional data aggregation schemes [20], [21], [22]. A multi-dimensional

Received 22 July 2024; revised 18 October 2025; accepted 20 October 2025. Date of publication 31 October 2025; date of current version 12 March 2026. This work was supported in part by the National Natural Science Foundation of China under Grant 62202005, Grant 62272002, Grant U24A20243, Grant 62372002, and Grant 62325209, in part by the Natural Science Foundation of Anhui Province, China under Grant 2508085QF243, in part by the Fundamental Research Funds for the Central Universities under Grant 2042023KF0203, and in part by the China Postdoctoral Science Foundation under Grant 2025M771549. *(Corresponding author: Jie Cui.)*

Qingyang Zhang, Zhen Fang, Jie Cui, Hulin Jin, and Fengqun Wang are with the Key Laboratory of Intelligent Computing and Signal Processing of Ministry of Education, School of Computer Science and Technology, Anhui Engineering Laboratory of IoT Security Technologies, Anhui University, Hefei 230039, China (e-mail: cuijie@mail.ustc.edu.cn).

Debiao He is with the School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China, and also with the Shanghai Key Laboratory of Privacy Preserving Computation, MatrixElements Technologies, Shanghai 201204, China (e-mail: hedebiao@163.com).

Digital Object Identifier 10.1109/TDSC.2025.3626895

privacy-preserving data aggregation scheme refers to transmitting multiple dimensions of data in a single aggregation process, which typically relies on super-increasing sequences or the Chinese Remainder Theorem (CRT) for implementation [19], [21], which enables preliminary aggregation of multidimensional data into a single-dimensional form. The recipient can subsequently extract individual dimensional data from the aggregated result through specific algorithms for analytical computation. Such multidimensional aggregation schemes effectively mitigate redundant computational overhead inherent in single-dimensional aggregation approaches.

However, most existing schemes aim to defend systems against external attacks, whereas modern smart grid infrastructures also face risks from internal attacks. For example, in some schemes [17], [19], smart sensors encrypt plaintext data using the public key of the electricity control center. However, the semi-honest electricity control center holding the decryption private key can access the private energy consumption data of any individual smart sensor. Moreover, if insiders collude with attackers to steal the key, it could lead to large-scale privacy breaches of industrial equipment, which is highly dangerous for industrial IoT systems involving diverse devices and complex user communities. Mitigating internal attacks thus becomes a crucial challenge for ensuring smart grid security. Most existing multi-dimensional schemes based on traditional public-key encryption fail to defend against internal attacks or the risk of private key leakage [23], [24].

To address these internal attack issues, some studies [20], [22] have modified the Paillier cryptosystem, where smart sensors encrypt the collected data using their respective independent keys. Simultaneously, the electricity control center holds the aggregated key and can only decrypt the aggregated data. This design effectively prevents curious control centers from decrypting sensitive data from the registered devices. Even if an adversary compromises the private key of a single device, other device data remains secure from leakage. However, these public-key encryption schemes lack sufficient reliability and require significant additional overhead to recover the system in the case of missing aggregation participants. Smart sensors, typically deployed at the edge of a power grid system, are vulnerable along with their communication lines [25]. Furthermore, the addition, removal, and updating of entities within an industrial power grid system align more closely with real-world usage scenarios. Therefore, designed schemes should possess adequate fault tolerance and flexibility to adapt to real-world conditions. Proxy re-encryption enables a proxy to transform ciphertext encrypted under one key into ciphertext under another key without accessing the sensitive data itself. The introduction of proxy re-encryption enables the conversion of any sender's ciphertext into a decryptable form for the recipient, eliminating the dependence on aggregation keys in public-key algorithm variants and thereby enhancing the scheme's fault tolerance. This approach also provides effective support for dynamic updates of system participants. Even when some aggregation participants fail or new entities are added during system expansion, the remaining devices can still successfully perform aggregation operations.

To address the issues of existing multi-dimensional data aggregation schemes, a multi-dimensional privacy-preserving data aggregation scheme based on homomorphic proxy re-encryption (MPDA-HPR) is proposed. Specifically, the contributions of this study are listed as follows.

- Considering the low fault tolerance and poor scalability of the existing framework schemes, a reliable and flexible data aggregation framework is proposed based on super-increasing sequences, homomorphic encryption, and proxy re-encryption. The proposed framework supports multi-dimensional data aggregation and the dynamic management of smart sensors, aggregator gateways, and electricity control centers.
- Focusing on less-addressed internal attacks, a privacy-preserving data aggregation scheme is designed based on a modified Paillier cryptosystem with the support of proxy re-encryption. Thus, no entity can obtain individual plaintext, thereby preserving the privacy of factories in the IIoT.
- Correctness and security analyses are performed to validate the feasibility of the proposed scheme. The analysis results demonstrate that MPDA-HPR guarantees privacy, integrity, authenticity, resistance to internal attacks, and fault tolerance. The proposed scheme is implemented and evaluated. The experimental results demonstrate its effectiveness for the IIoT smart grid, offering more functionalities with a similar overhead compared to other schemes.

The remainder of this paper is organized as follows: Section II discusses related works on data aggregation. Section III introduces the prerequisite knowledge used in this study. Section IV outlines MPDA-HPR, including the system model, threat model, security model, and system workflow. Section V introduces the detailed design of the MPDA-HPR. The correctness and security of the proposed scheme are analyzed in Section VI, and the performance of MPDA-HPR is evaluated in Section VII. Finally, we summarize the study in Section VIII.

II. Related Work

Homomorphic encryption allows computations directly on ciphertexts, a feature well-suited for scenarios involving privacy-preserving data aggregation. Liu et al. [16] developed a 3PDA privacy-preserving data aggregation scheme independent of a trusted third party, where users with certain trust levels construct virtual aggregation regions to shield individual data and achieve accurate aggregation results instead of approximations. Chen et al. [21], combining the Chinese Remainder Theorem and the Paillier encryption algorithm, designed an efficient data aggregation method that uses Shamir's secret sharing to resist internal attacks and achieve fine-grained weight distribution for multi-dimensional data. Zhao et al. [26] constructed a lightweight fog-based privacy-preserving data aggregation scheme and proposed the PDA-SP aggregation scheme with intelligent pricing capabilities. Lyu et al. [27] introduced the PPFA privacy-preserving data aggregation system based on fog computing architecture, suggesting a provable differential noise generation method using

Gaussian noise stability and employing a dual-layer encryption mechanism under a partially trusted aggregator model to enhance system robustness. The PPFA framework leverages efficient stream ciphers and employs separate keys for additive homomorphism. Xue et al. [28] implemented an efficient and robust data aggregation scheme without relying on trusted authorities, using efficient additional homomorphic cryptosystems to avoid high complexity computations. MuDA, a multifunctional data aggregation scheme based on the BGN cryptosystem, was proposed to defend against differential privacy Chen et al. [29]. Bao et al. [30] enhanced the basic BGN cryptosystem to construct a fault-tolerant differential privacy data aggregation scheme (DPAFT), balancing privacy-preserving and fault tolerance. Zuo et al. [31] proposed an intelligent grid multi-dimensional privacy-preserving data aggregation scheme based on ElGamal homomorphic distributed decryption, independent of trusted authorities in the real world. Zhan et al. [17] introduced the EC-ElGamal encryption algorithm with a double trapdoor mechanism, proposing an efficient privacy-preserving query scheme for smart grids. Lu et al. [19] designed an efficient privacy-preserving data aggregation scheme (EPPA) based on the Paillier encryption algorithm and super-increasing sequence, significantly reducing overhead compared to traditional single-dimensional data aggregation. The existing schemes mentioned are based on traditional public key cryptography, where the sender encrypts plaintext data using the receiver's public key. However, they face risks of data leakage if the private key is compromised or if internal attacks occur.

Li et al. [20] modified the Paillier cryptosystem and, for the first time, implemented the PPMA privacy-preserving multi-subset data aggregation scheme for smart grids using super-increasing sequences. Zhang et al. [22] constructed a verifiable privacy-preserving multi-dimensional data aggregation scheme (VPMDA) using an enhanced Paillier scheme and super-increasing sequences. Saleem et al. [32] designed an efficient fog-supported privacy-preserving data aggregation scheme using a modified version of the Paillier cryptosystem. However, the reliability of these modified public key encryption algorithms is not sufficient, and in practical environments, registration, deletion, and update of participating entities require system restarts, which do not meet the production needs of the IIoT.

In recent years, researchers have begun to explore the potential of homomorphic proxy re-encryption in the field of privacy-preserving data aggregation. Derler et al. [33] introduced the concept of homomorphic proxy re-encryption into privacy-preserving data aggregation research for the first time, but their plaintext space was small and unsuitable for real IIoT environments. Ni et al. [34] designed the P2SM privacy-preserving data aggregation scheme using proxy re-encryption and homomorphic validators, but their scheme considers the computation center as a fully trusted entity, which slightly compromises security. In response to the above issues, this paper proposes a privacy-preserving data aggregation scheme based on homomorphic proxy re-encryption to address the security vulnerabilities and low usability found in existing schemes.

III. Preliminaries

A. Paillier Cryptosystem

The Paillier encryption algorithm is a probabilistic asymmetric algorithm based on the decisional composite residue assumption (DCRA) [35], and it possesses excellent additive homomorphic properties, making it widely used in various cryptographic systems. The Paillier cryptosystem can mainly be divided into three parts: key generation, encryption, and decryption. The description of the Paillier cryptosystem is given as follows:

- *Key Generation:* Given a security parameter k, select two independent large prime numbers p and q randomly, where $|p| = |q| = k$, satisfying $\gcd(pq, (p-1)(q-1)) = 1$. Compute $N = pq$ and $\lambda = \mathrm{lcm}(p-1, q-1)$, where denotes the least common multiple. Then choose a random integer g such that $g \in \mathbb{Z}^*_{N^2}$. Define the function $L(x) = \frac{x-1}{N}$, Ensure the existence of μ such that n divides the order of g by checking the existence of the modular multiplicative inverse $\mu = (L(g^\lambda \bmod N^2))^{-1} \bmod n$. Therefore, the public key of the cryptosystem is (N, g) and the private key is (λ, μ).
- *Encryption:* For a plaintext message $m \in \mathbb{Z}_N$, a random number r is selected such that $r \in \mathbb{Z}^*_N$ and $\gcd(r, N) = 1$. Then, compute the ciphertext $C = g^m \cdot r^N \bmod N^2$.
- *Decryption:* For a ciphertext $C \in \mathbb{Z}^*_{N^2}$, recover the plaintext using the formula $m = L(C^\lambda \bmod N^2) \cdot \mu \bmod N$.

The additive homomorphic property of the Paillier cryptosystem is one of its notable features. Its homomorphic property is described as follows:

$$D\left(E\left(m_1, r_1\right) \cdot E\left(m_2, r_2\right) \bmod N^2\right) = m_1 + m_2 \bmod N$$

The product of two ciphertexts decrypts to the sum of their respective plaintexts, that is:

$$\begin{aligned} E\left(m_1\right) \cdot E\left(m_2\right) &= \left(g^{m_1} \cdot r_1^N\right)\left(g^{m_2} \cdot r_2^N\right)\left(\mathrm{mod} N^2\right) \\ &= g^{m_1+m_2} \cdot \left(r_1 r_2\right)^N \left(\mathrm{mod} N^2\right) \\ &= E\left(m_1 + m_2\right) \end{aligned}$$

B. Super-Increasing Sequence

A sequence in which each element is greater than the sum of all preceding elements in the sequence is called a super-increasing sequence. Due to its unique super-increasing property, it is often applied in the field of cryptography. Super-increasing sequences are typically characterized by the following form:

$$S_n > \sum_{i=1}^{n-1} S_i (n > 1)$$

Super-increasing sequences are introduced to perform preliminary aggregation on initial multi-dimensional plaintext data. By combining each dimension's data with elements of the super-increasing sequence and then aggregating, the multi-dimensional plaintext can be aggregated into a single-dimensional plaintext that incorporates the super-increasing sequence. Subsequently, the multi-dimensional plaintext can

be recovered from the single-dimensional plaintext using Algorithm 1 proposed in the following sections, achieving the aggregation and recovery of multi-dimensional data.

C. Proxy Re-Encryption

Proxy re-encryption is an encryption technique that allows an agent (a third party) to transform data encrypted by one user into data decryptable by another user. In this process, the agent uses a re-encryption key to perform the transformation without accessing the plaintext or decryption key, thereby ensuring the security and privacy of the data during the conversion process. A general description of proxy re-encryption is given as follows:

- *Encryption:* The sender encrypts the plaintext message m using their public key pk_i to obtain the initial ciphertext $C_i : C_i \leftarrow \mathrm{Enc}(m, pk_i)$.
- *Proxy Re-encryption:* The proxy uses the re-encryption key $rk_{i\to j}$ to transform the initial ciphertext C_i into a re-encrypted ciphertext C_j encrypted under the recipient's public key: $C_j : C_j \leftarrow \mathrm{ReEnc}(C_i, rk_{i\to j})$.
- *Decryption:* The recipient decrypts the re-encrypted ciphertext C_j using their private key sk_j to obtain the original plaintext message $m : m \leftarrow \mathrm{Dec}(C_j, sk_j)$.

D. BLS Signature

BLS signature is a digital signature technique based on the Diffie-Hellman problem [36], employing elliptic curve pairing methods based on bilinear mappings [37]. BLS digital signatures offer excellent aggregation capabilities and verification efficiency, making them a suitable choice for ensuring data integrity in the transmission process. A general description of BLS digital signatures is given as follows:

- *Key Generation:* Define a bilinear mapping $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_T$, where both $\mathbb{G}_1$ and $\mathbb{G}_T$ are cyclic groups of prime order q. Choose a generator g for $\mathbb{G}_1$, select a collision-resistant hash function H, and choose a random number x as the signing private key. Compute the public key $p = g^x$;
- *Digital Signature:* Given a message m, compute the hash value of the message $h = H(m)$, use the signing private key to sign it, generating the signature $\sigma = h^x$;
- *Signature Verification:* Verify if the equation $e(\sigma, g) = e(H(m), p)$ holds. If the equation holds true, the signature is considered valid.

For the bilinearity of the bilinear pairing: $\forall g_1, g_2 \in \mathbb{G}_1$ and $\forall a, b \in Z_q^*$, we have $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$. Therefore, BLS digital signatures can achieve aggregated signature verification:

$$e(\sigma_1 + \sigma_2 + \ldots + \sigma_n, g) = e(H(m_1), p_1) * e(H(m_2), p_2) * \ldots * e(H(m_n), p_n)$$

IV. System Model

A. System Model

The system model diagram of the proposed scheme in this paper is shown in the Fig. 1, consisting of four main entities:

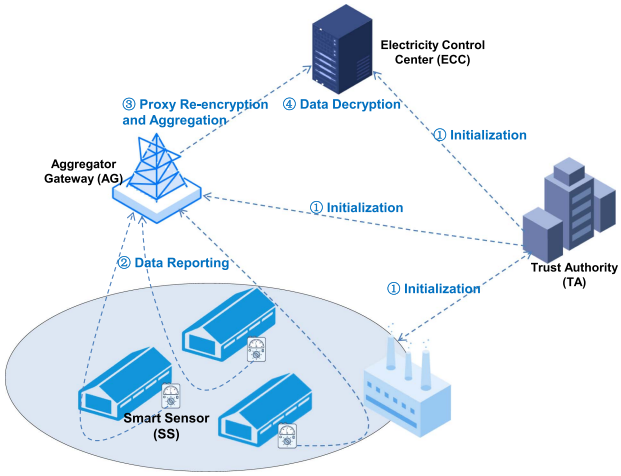


Fig. 1. System model.

smart sensor, aggregator gateway, electricity control center, and trusted authority.

- *Smart Sensor:* SS, edge devices in the smart grid of the IIoT, are responsible for collecting multi-dimensional electricity data generated by devices and aggregating it into initial plaintext using super-increasing sequences. They encrypt the initial plaintext with their own keys and send it to the aggregator gateway.
- *Aggregator Gateway:* The AG collects the initial ciphertext encrypted by SS, performs proxy re-encryption on it to transform it into a ciphertext form decryptable by ECC, then aggregates the re-encrypted ciphertext and sends it to ECC.
- *Electricity Control Center:* ECC is responsible for receiving the aggregated ciphertext sent by AG, decrypting it to obtain the aggregated plaintext, then using algorithms to obtain the sum of various dimensions of data and performing analyses and decision-making based on it.
- *Trusted Authority:* Trusted Authority (TA) is responsible for generating keys, re-encryption keys, signature keys, and publishing public parameters for each main entity. After the system initialization is completed, TA generally goes offline.

B. Threat Model

Data security is a crucial security metric for IIoT. In the proposed system architecture, TA is assumed to be completely trusted, while the ECC, AG, and SS are all honest but curious entities. They will faithfully execute the system's functions, but may be curious about other devices' data. The threat model considered in the proposed scheme includes the following potential threats:

- *Communication Privacy:* Based on the designed system model, most communication between entities occurs over public channels. Therefore, attackers may eavesdrop on data streams over public channels or forge and modify transmitted data.

- *Data Storage:* Attackers may launch attacks on the databases of AG and ECC to steal plaintext information stored in the storage space.
- *Edge Device Security:* Smart sensors, as edge devices far from the center, are vulnerable to attacks by attackers. Therefore, it is necessary to consider data aggregation in the absence of aggregation participants.

C. Security Goals

- *Data Privacy:* Devices' electricity consumption data may reveal production information and operational modes in the factory. Therefore, in the design of the proposed scheme in this paper, no plaintext information will be transmitted over the public channel, and the AG and ECC will not store devices' plaintext information.
- *Integrity and Authenticity:* Encrypted ciphertext data should not be tampered with or forged before decryption. Each entity can verify the correctness and integrity of the received data through signature verification.
- *High Fault Tolerance:* In practical IIoT applications, operational entities may need updates, decommissioning, or other changes due to external attacks or aging. Therefore, the proposed scheme should achieve high fault tolerance to accommodate changes in entities.
- *Mitigating Internal Attacks:* Service providers or third-party data centers may potentially misuse factory energy consumption information and operational modes, such as for confidential theft or targeted marketing. Therefore, in the proposed scheme design in this paper, ECC will not have access to plaintext information of device power consumption data.

D. System Workflow

The proposed scheme in this paper consists primarily of four algorithmic components: ***Initialization***, ***data reporting***, ***proxy re-encryption and aggregation***, and ***data decryption***. Taking the data aggregation of a factory region as an example, the process of the proposed scheme mainly involves n smart sensors $SS_i(i = 1, 2, \ldots, n)$, a regional AG, and the ECC.

- *Initialization:* In this phase, the trusted authority generates secret parameters for the system based on security parameters and distributes public parameters. Assuming SS_i collects k dimensional electricity data $D_i = \{d_{i1}, d_{i2}, \ldots, d_{ik}\}$, TA determines a super-increasing sequence $S = \{S_1, S_2, \ldots, S_k\}$ for preliminary aggregation of the raw data to generate plaintext.
- *Data Reporting:* In this phase, SS_i aggregates the raw data using the super-increasing sequence S to generate primary plaintext message m_i. Subsequently, the primary plaintext message is encrypted using the modified Paillier encryption algorithm proposed in this paper, resulting in the primary ciphertext. Then, SS_i signs the primary ciphertext and sends it along with the signature to AG.
- *Proxy Re-encryption and Aggregation:* In this phase, AG verifies the signatures of the reported uploads. Upon successful verification, AG first performs re-encryption of the primary ciphertext of $SS_i(i = 1, 2, \ldots, n)$ to generate a secondary ciphertext. The homomorphic proxy re-encryption proposed in this paper ensures that the ciphertext maintains its homomorphic properties after transformation. Subsequently, AG aggregates the transformed ciphertext to generate the regional aggregate ciphertext $C = \sum_{i=1}^{n} C_i$. AG signs the aggregated ciphertext and sends it along with the signature to ECC.
- *Data Decryption:* In this phase, ECC first verifies the signatures of the uploaded data. Upon successful verification, ECC decrypts the aggregated ciphertext. Due to the use of homomorphic proxy re-encryption, ECC can decrypt the aggregated ciphertext using its own key, obtaining the aggregated original plaintext. Subsequently, using an algorithm based on the super-increasing sequence, ECC calculates the sum of electricity usage data for each dimension j within the region, $D_j = \sum_{i=1}^{n} d_{ij}$.

V. Proposed MPDA-HPR Scheme

This paper takes smart sensor devices within a factory region as an example, consisting primarily of n smart sensors $SS_i(i = 1, 2, \ldots, n)$, an aggregator gateway AG, and an electricity control center ECC. The main workflow of the scheme is illustrated in Fig. 2.

Initialization: TA generates the system's public parameters and distributes secret parameters to ECC, AG, and $SS_i(i = 1, 2, \ldots, n)$. The specific details are given as follows:

- Based on the security parameter λ, the TA selects large prime numbers p and q. It calculates $N = pq$ and $g = N + 1$. It also chooses a random r_0 such that $r_0^N \bmod N^2 = g_0 \in \mathbb{Z}_{N^2}^*$. Simultaneously, it determines the bilinear mapping pairing $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_T$, where $\mathbb{G}_1$ and $\mathbb{G}_T$ are both prime-order cyclic groups of order v. It selects the generator g_1 for $\mathbb{G}_1$ and sets up a collision-resistant hash function $H : \{0, 1\}^* \to \mathbb{G}_1$.
- The TA selects a random number $x_{ecc} \in \mathbb{Z}_{N^2}^*$ as the private key for ECC. It also selects random numbers x_i as the private keys for each SS_i and x_{ag} as the private key for AG. Then it calculates the re-encryption keys $rk_{i\to ecc} = g_0^{x_{ecc}-x_i} \bmod N^2 (i = 1, 2, \ldots, n)$ for $i = 1, 2, \ldots, n$. Furthermore, it computes the signature public keys $p_i = g_1^{x_i} (i = 1, 2, \ldots, n)$ and $p_{ag} = g_1^{x_{ag}}$.
- The TA selects a super-increasing sequence $S = \{S_1, S_2, \ldots, S_k\}$, where each S_i satisfies $S_i = \sum_{j=1}^{i-1} (S_j \cdot M_j \cdot N)$, where k is the dimension of the reported data, M_j represents the upper limit of the $j - th$ dimension data, and N represents the upper limit of the number of smart sensors.
- The TA sends x_{ecc} to ECC through a secure channel, x_{ag} and $rk_{i\to ecc} (i = 1, 2, \ldots, n)$ to AG through a secure channel, and x_i to each $SS_i (i = 1, 2, \ldots, n)$ through a secure channel. It publishes the public parameters $\Omega = (N, g, g_0, g_1, e, q, \mathbb{G}_1, \mathbb{G}_T, H, p_{ag}, \{p_i\}_{i=1,2,\ldots,n}, \{S_i\}_{1\le i\le k})$.

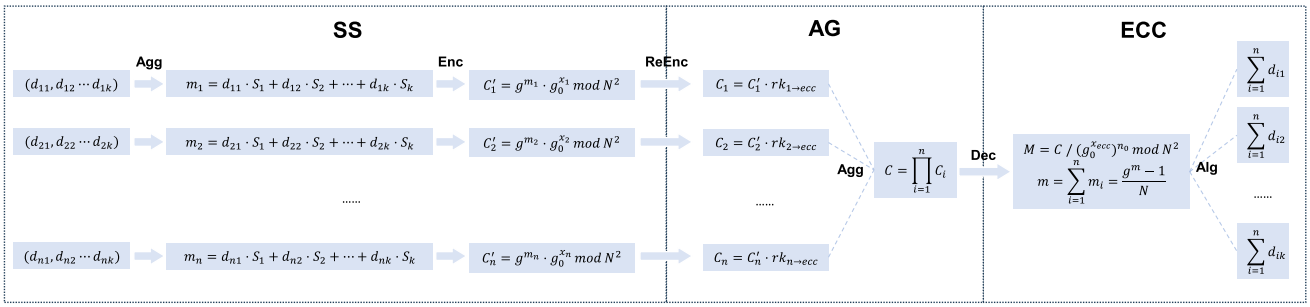


Fig. 2. MPDA-HPR system process.

After the initialization is complete, the TA goes offline and does not participate in the subsequent scheme processes.

Data Reporting: $SS_i(i = 1, 2, \ldots, n)$ encrypts the collected k-dimensional data, signs the ciphertext, and reports both the ciphertext and the signature to AG. Details are given as follows:

- SS_i aggregates the plaintext preliminarily:

$$m_i = d_{i1} \cdot S_1 + d_{i2} \cdot S_2 + \cdots + d_{ik} \cdot S_k$$

where d_{ij} represents the jth dimension data collected by SS_i;

- SS_i encrypts the original plaintext, computes the primary ciphertext C_i':

$$C_i' = g^{m_i} \cdot g_0^{x_i} \bmod N^2$$

- After generating the primary ciphertext, SS_i generates a signature $\sigma_i = H(C_i')^{x_i}$;
- SS_i packages $\{C_i', \sigma_i, T\}$ to the AG, where T is the current timestamp, which can resist the potential replay attack.

Proxy Re-encryption and Aggregation: After receiving data $\{C_i', \sigma_i, T\}(i = 1, 2, \ldots, n)$ from SS_i, AG performs the following operations:

- First, AG verifies whether the timestamp T is fresh. After the time validation passes, it verifies the validity of the digital signatures. If the equation $e(\sigma_i, g_1) = e(H(C_i'), p_i)$ holds true, the verification passes. To enhance the efficiency of signature verification, AG can perform batch signature verification: $e(\sum_{i=1}^{j} \sigma_i, g_1) = \prod_{i=1}^{j} e(H(C_i'), p_i)$, batch verification reduces the pairing operations from $2n$ to $n + 1$ times;
- AG performs proxy re-encryption on the validated ciphertexts. For each primary ciphertext C_i', it calculates the secondary ciphertext C_i using the re-encryption key $rk_{i\to ecc}(i = 1, 2, \ldots, n)$: $C_i = C_i' \cdot rk_{i\to ecc} = g^{m_i} \cdot g_0^{x_i} \cdot g_0^{x_{ecc}-x_i} \bmod N^2 = g^{m_i} \cdot g_0^{x_{ecc}} \bmod N^2$;
- After obtaining all the secondary ciphertexts, AG performs an aggregation operation on them. To prevent decryption failure due to malfunctioning edge devices, AG counts the devices involved in the aggregation. It calculates:

$$C = \prod_{i=1}^{n_0} C_i = g^{\sum_{i=1}^{n_0} m_i} \cdot (g_0^{x_{ecc}})^{n_0} \bmod N^2$$

Here, n_0 represents the number of correctly participating devices in the aggregation.

Algorithm 1: Procedure: Extracting Multi-Dimensional Data.

Input: $m,\ S = (S_1, S_2, \ldots, S_k)$
Output: $D_1, D_2, \ldots, D_k$
1: **for** i = k to 1 **do**
2: $D_i = (m - (m \bmod S_i))/S_i$
3: $m = m \bmod S_i$
4: **end for**
5: **return** $D_1, D_2, \ldots, D_k$

- After aggregating the ciphertexts, AG signs the aggregated ciphertext by computing $\sigma_{ag} = H(C)^{x_{ag}}$;
- AG packages $\{C, \sigma_{ag}, n_0, T\}$ and sends it to ECC.

Data Decryption: Upon receiving the data report $\{C, \sigma_{ag}, n_0, T\}$ from AG, ECC performs the following operations:

- ECC first verifies if the timestamp T is fresh. Upon successful time verification, it proceeds to signature verification. If the equation $e(\sigma_{ag}, g_1) = e(H(C), p_{ag})$ holds true, the verification passes. If ECC needs to receive data reports from multiple AGs, it can still employ batch verification to enhance the efficiency of signature verification;
- After the signature verification passes, ECC proceeds with decryption. It calculates:

$$C/\,(g_0^{x_{ecc}})^{n_0} \bmod N^2 = g^{\sum_{i=1}^{n} m_i} \bmod N^2$$

Let $m = \sum_{i=1}^{n} m_i$, According to binomial expansion, we have $g^m = (1 + N)^m \bmod N^2 = (1 + Nm) \bmod N^2$. Thus, we get

$$m = \sum_{i=1}^{n} m_i = \frac{g^m - 1}{N}$$

- ECC determines the plaintext message $m = \sum_{i=1}^{n} m_i = S_1 \cdot \sum_{i=1}^{n} d_{i1} + S_2 \cdot \sum_{i=1}^{n} d_{i2} + \cdots + S_k \cdot \sum_{i=1}^{n} d_{ik}$. Then, ECC uses Algorithm 1 to derive the sum of data values for each dimension $\sum_{i=1}^{n} d_{i1}, \sum_{i=1}^{n} d_{i2}, \ldots, \sum_{i=1}^{n} d_{ik}$. With the total values of data for each dimension, ECC can proceed with further analyses.

VI. Correctness and Security Analyses

In this section, the security issues of the proposed scheme will be analyzed in detail. The correctness of the proposed scheme is demonstrated from the following two aspects, and the privacy-preserving and data integrity of the proposed scheme are demonstrated by analyzing potential privacy leaks.

A. Correctness Proof

Correctness of Signature Verification: Single signature correctness verification is given as follows:

$$\begin{aligned} e(\sigma_i, g) &= e\left(H\left(C_i\right)^{x_i}, g\right) \\ &= e\left(H\left(C_i\right), g^{x_i}\right) \\ &= e\left(H\left(C_i\right), p_i\right) \end{aligned}$$

Batch signature aggregation authentication correctness verification is given as follows:

$$\begin{aligned} e(\sigma, g) &= e\left(\sigma_1 + \sigma_2 + \ldots + \sigma_n, g\right) \\ &= e\left(\sigma_1, g\right) * e\left(\sigma_2, g\right) * \ldots * e\left(\sigma_n, g\right) \\ &= e\left(H\left(C_1\right), p_1\right) * e\left(H\left(C_2\right), p_2\right) * \ldots * e\left(H\left(C_n\right), p_n\right) \\ &= \prod_{i=1}^{n} e\left(H\left(C_i\right), p_i\right) \end{aligned}$$

Correctness Verification of Decryption: The recipient performs decryption on the aggregated ciphertext. First, compute $g^m = \frac{C}{(g_0^{x_{ecc}})^{n_0}} (\mathrm{mod} N^2)$. Since $g = N + 1$, g^m can be written as $(1+N)^m$. According to the binomial expansion formula, we have $(1+N)^m = \sum_{i=1}^{m} \binom{m}{i} N^i$. Therefore, in modulo N^2, we have $(1+N)^m = 1 + Nm (\mathrm{mod} N^2)$, We can solve for m as $m = \frac{g^m - 1}{N} (\mathrm{mod} N^2)$.

After decrypting, the ECC obtains the aggregated plaintext $m = \sum_{i=1}^{n} m_i = S_1 \cdot \sum_{i=1}^{n} d_{i1} + S_2 \cdot \sum_{i=1}^{n} d_{i2} + \cdots + S_k \cdot \sum_{i=1}^{n} d_{ik}$. Then, executing Algorithm 1 and leveraging the properties of the super-increasing sequence, we can derive

$$\begin{aligned} & S_1 \cdot \sum_{i=1}^{n} d_{i1} + S_2 \cdot \sum_{i=1}^{n} d_{i2} + \cdots + S_{k-1} \cdot \sum_{i=1}^{n} d_{i(k-1)} \\ & \leq S_1 \cdot \sum_{i=1}^{n} M_1 + S_2 \cdot \sum_{i=1}^{n} M_2 + \cdots + S_{k-1} \cdot \sum_{i=1}^{n} M_{k-1} \\ & = \sum_{j=1}^{k-1} S_j \cdot M_j \cdot n < S_k \end{aligned}$$

Therefore, according to Algorithm 1, we have

$$\frac{m - (m \bmod S_k)}{S_k} = \frac{S_k \cdot \sum_{i=1}^{n} d_{ik}}{S_k} = \sum_{i=1}^{n} d_{ik}$$

As described above, we can obtain the sum of each dimension $\sum_{i=1}^{n} d_{ij} (j = 1, 2, \ldots, k)$.

B. Security Analyses

Encryption Algorithm Security: The proposed scheme employs a variant of the Paillier encryption algorithm constructed independently to encrypt plaintext data, referring to Li's scheme PPMA [20]. The detailed analyses are provided below:

Since $g_0 = r_0^N$, we have $C = g^m \cdot g_0^{x_i} = g^m \cdot r_0^{N \cdot x_i} = g^m \cdot (r_0^{x_i})^N$. Therefore, the ciphertext C can still be considered as a valid plaintext under the Paillier cryptosystem, satisfying the chosen plaintext attack on the semantic security implemented by the Paillier cryptosystem. Thus, the proposed encryption algorithm is secure and effective.

Privacy-Preserving of Entities Throughout the System (SS, AG, ECC): The analyses of devices' privacy-preserving within the system workflow mainly focus on the following three aspects:

First, at the individual devices' end, smart sensors encrypt the collected raw plaintext data on the edge device SS. $SS_i (i = 1, 2, \ldots, n)$ preliminarily aggregates and encrypts k types of plaintext data, obtaining ciphertext $C_i' = g^{m_i} \cdot g_0^{x_i} \bmod N^2$, which is then sent to AG via a public channel. Even if an adversary eavesdrops on the communication channel between SS_i and AG, they can only obtain ciphertext data. Based on the security analyses of the encryption algorithm mentioned earlier, adversaries cannot recover any plaintext information from ciphertext C. While powerful adversaries may have the capability to compromise the keys of certain devices within the region, all secret parameters in this paper are randomly generated by a trusted authority and are independent of each other. Therefore, compromising the keys of one or some devices still does not result in the leakage of privacy of other devices.

At the intermediary node AG, the ciphertext of multi-dimensional data is first subjected to a re-encryption process. Utilizing the homomorphic proxy re-encryption designed in this paper, ciphertext data under the keys of SS_i are transformed into ciphertext under ECC keys. During the re-encryption process, the proxy AG cannot obtain any effective information about the original plaintext. Moreover, the data is stored in AG in ciphertext form. Based on the homomorphic property, AG can directly perform ciphertext-based aggregation on the transformed primary ciphertext. According to the above analyses, the initial ciphertext before transformation, the primary ciphertext after transformation, and the aggregated ciphertext after aggregation all have the same form as the Paillier cryptosystem, achieving invisibility of plaintext information to the proxy AG. Even if an adversary compromises or intrudes upon AG's database, they still cannot obtain any plaintext information from the ciphertext. Smart sensors are typically located at the system's edge, far from the center. Therefore, there may be occurrences of natural device failures or physical damage to certain smart sensors by adversaries, rendering them unable to participate in aggregation normally. In the proposed scheme in this paper, the keys of each SS_i device are independently and randomly generated. Therefore, the system can continue to function properly even in the event of device failures.

For the receiving end ECC, upon receiving the aggregated ciphertext $C = \prod_{i=1}^{n_0} C_i$, where ciphertexts from multiple devices

TABLE I
PERFORMANCE COMPARISON

scheme	sp1	sp2	sp3	sp4	sp5	sp6	sp7
Xue *et al.* [28]	✓	×	×	×	✓	×	✓
Bao *et al.* [30]	✓	×	×	✓	✓	×	✓
Zhan *et al.* [17]	✓	✓	✓	✓	×	×	✓
Lu *et al.* [19]	✓	✓	✓	✓	×	✓	✓
Zhang *et al.* [22]	✓	✓	✓	×	✓	✓	×
Verma *et al.* [18]	✓	✓	✓	✓	×	×	✓
Ours	✓	✓	✓	✓	✓	✓	✓

sp1: Data privacy sp2: Data integrity sp3: Authenticated
sp4: Fault-tolerant sp5: Against internal attacks
sp6: Multi-dimensional aggregation sp7: Extensibility

TABLE II
ENCRYPTION PRIMITIVES

Notations	Operation
T_h	Hash
T_{mm}	Modular multiplication
T_{me}	Modular exponentiation
T_{pm}	Elliptic point addition
T_{pa}	Elliptic point multiplication

are aggregated into a single ciphertext, ECC cannot decipher the independent ciphertext of any individual device. This ensures that the privacy of devices is not compromised by the receiving end.

Identity Authentication and Integrity Verification: In the proposed scheme, identity and integrity verification are carried out using digital signatures. Digital signatures are typically constructed using the sender's private key and verified using the corresponding public key. The ciphertext data sent from SS and AG are both signed using the BLS signature method. This method is based on the Diffie-Hellman problem and can be proven secure under the random oracle model. For specific proofs, refer to the original BLS paper [36].

VII. PERFORMANCE EVALUATION

A. Functionality Comparison

First, several schemes have been compared with the proposed scheme in terms of functionality, and the comparison results are shown in Table I. These schemes have been comprehensively analyzed from various functional perspectives, including basic security functions (such as data privacy, data integrity, and authenticated), risk-resistance functions (such as fault-tolerance, against internal attacks), data analysis functions (such as multi-dimensional aggregation), and scheme extensibility. The proposed scheme in this paper introduces BLS short signatures, providing comprehensive data privacy protection, integrity verification, and identity authentication. Additionally, the scheme combining homomorphic encryption with proxy re-encryption is proposed. Homomorphic encryption enhances the scheme's resistance to internal attacks, while proxy re-encryption effectively improves fault-tolerance and extensibility. Furthermore, the scheme incorporates super-increasing sequences, enabling single-round computation for multi-dimensional data, significantly reducing overhead compared to traditional single-dimensional data aggregation.

B. Theoretical Analyses

To facilitate the comparison of computational costs, the execution time symbols for some cryptographic primitives are listed in Table II. Comparing the proposed scheme with schemes [17], [19], [22]. To address the inefficiency issues of traditional single-dimensional privacy-preserving data aggregation schemes and the low fault tolerance of public-key algorithm variants, we proposed a multi-dimensional privacy-preserving data aggregation scheme based on homomorphic proxy re-encryption and super-increasing sequences. Scheme [17] is a single-dimensional privacy-preserving data aggregation scheme based on EC-ElGamal, scheme [19] is a multi-dimensional privacy-preserving data aggregation scheme based on Paillier, and scheme [22] is a multi-dimensional privacy-preserving data aggregation scheme based on a modified Paillier algorithm. These three schemes employ different technical approaches to achieve privacy-preserving data aggregation; therefore, this paper selects schemes [17], [19], [22] for comparison. The following is a detailed theoretical analysis.

First, the encryption cost at the SS end is compared. In the proposed scheme, each SS_i initially performs preliminary aggregation, computing the plaintext message $m_i = d_{i1} \cdot S_1 + d_{i2} \cdot S_2 + \cdots + d_{ik} \cdot S_k$. During this process, SS_i needs to perform k modular multiplication operations. In the encryption process, SS_i needs to perform one modular multiplication operation and two modular exponentiation operations. Therefore, the total encryption computational cost for SS_i is $(k+1) \cdot T_{mm} + 2T_{me}$. It's worth noting that Zhan et al.'s scheme [17] only supports single-dimensional data aggregation, so in a multi-dimensional data aggregation scenario, Zhan et al.'s scheme [17] needs to handle each dimension separately. Zhan et al.'s scheme [17] uses the EC-ElGamal encryption algorithm, encrypting each single-dimensional data from a smart sensor using one modular multiplication operation and three point multiplication operations, with a total computational cost of $k \cdot (T_{mm} + T_{pm})$. Lu et al.'s scheme [19] combines the Paillier encryption algorithm with super-increasing sequences to achieve multi-dimensional data aggregation. Encrypting k-dimensional data from a smart sensor requires $k+1$ modular exponentiation operations and k modular multiplication operations, with a total computational cost of $k \cdot T_{mm} + (k+1) \cdot T_{me}$. Zhang et al.'s scheme [22] uses a modified version of the Paillier algorithm, where each encryption involves two modular exponentiation operations, $k+2$ modular multiplication operations, and one hash operation, with a total computational cost of $T_h + (k+2) \cdot T_{mm} + 2T_{me}$.

At the AG end, assuming the number of users participating in aggregation is n, the proposed scheme is discussed first. In the proposed scheme, AG first performs proxy re-encryption on the primary ciphertexts of n devices, calculating $C_i = C'_i \cdot rk_{i \to ecc}$. This process involves n modular multiplication

TABLE III
COMPUTATIONAL COST ANALYSES

Scheme	SS	AG	ECC
Zhan *et al.* [17]	$k \cdot (T_{mm} + 3T_{pm})$	$2(n-1) \cdot T_{pa}$	$T_{pm} + T_{pa}$
Lu *et al.* [19]	$k \cdot T_{mm} + (k+1) \cdot T_{me}$	$(n-1) \cdot T_{mm}$	$2T_{mm} + T_{me}$
Zhang *et al.* [22]	$T_h + (k+2) \cdot T_{mm} + 2T_{me}$	$(n-1) \cdot T_{mm}$	$T_h + 2T_{mm} + T_{me}$
Ours	$(k+1) \cdot T_{mm} + 2T_{me}$	$2(n-1) \cdot T_{mm}$	$2T_{mm} + T_{me}$

Set k to the plaintext dimension and n to the number of devices

operations. Then, AG aggregates the re-encrypted ciphertexts $C = \prod_{i=1}^{n_0} C_i$, which involves $n-1$ modular multiplication operations. The total computational cost is $2(n-1) \cdot T_{mm}$. For Zhan et al.'s scheme [17], the aggregation cost is $2(n-1) \cdot T_{pa}$. For Lu et al.'s scheme [19], the aggregation cost is $(n-1) \cdot T_{mm}$ and for Zhang et al.'s scheme [22], the aggregation cost is also $(n-1) \cdot T_{mm}$. In terms of time complexity, the proposed scheme is slightly higher than the comparison schemes due to the proxy re-encryption operation performed by AG. However, this addition of a fault tolerance mechanism makes the proposed scheme more robust compared to the comparison schemes.

When ECC receives the aggregated ciphertext sent by AG, it performs decryption. In the proposed scheme, ECC decrypts the ciphertext, calculating $C/(g_0^{x_{ecc}})^{n_0} \bmod N^2 = g^{\sum_{i=1}^{n} m_i} \bmod N^2$, which involves one modular exponentiation operation and two modular multiplication operations. The total computational cost is $2T_{mm} + T_{me}$. For Zhan et al.'s scheme [17], decryption of the aggregated data involves one point addition operation and one point multiplication operation, with a computational cost of $T_{pm} + T_{pa}$. For Lu et al.'s scheme [19], decryption involves one modular exponentiation operation and two modular multiplication operations, with a total computational cost of $2T_{mm} + T_{me}$. For Zhang et al.'s scheme [22], decryption involves one modular exponentiation operation, two modular multiplication operations, and one hash operation, with a total computational cost of $T_h + 2T_{mm} + T_{me}$.

The theoretical cost analyses of each scheme are shown in Table III, including the theoretical overhead at the SS, AG, and ECC ends.

C. Experimental Evaluation

In this section, the computational overhead at the SS, AG, and ECC ends is used to measure the performance of the proposed scheme. Specifically, the proposed scheme is implemented using the Python programming language and the miracl core library. The experiments are conducted on a computer with an AMD Ryzen 7 6800H 3.2GHz processor, 16GB of memory, and Windows 11 (64-bit) operating system. Schemes [17], [19], [22] are also chosen for comparison. At the same security level as the proposed scheme and the comparison schemes, the security parameters for both the Paillier cryptosystem and the modified version are set to 2048 bits. Additionally, the elliptic curve BLS12-383 is chosen for the EC-ElGamal cryptosystem.

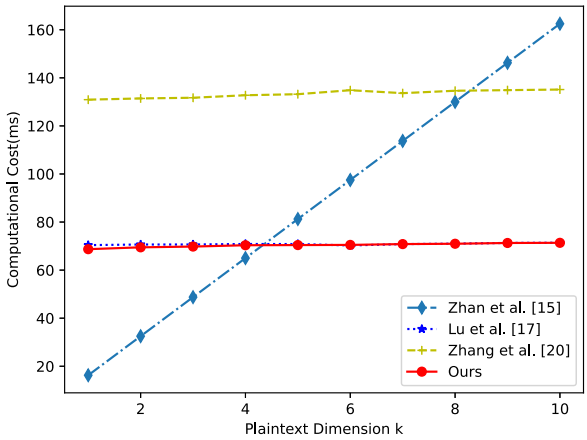


Fig. 3. Encryption costs on the SS side.

During the data reporting phase, the SS initially aggregates the collected multi-dimensional data and then encrypts the aggregated single plaintext data. The encryption time cost comparison chart for each smart sensor side in various schemes is shown in Fig. 3. Due to the introduction of the super-increasing sequence, it can be observed that as the data dimension continues to increase, the advantage of encryption time cost on the SS side in the proposed scheme becomes more prominent. Due to the modified encryption algorithm based on the Paillier cryptosystem, the encryption overhead at the SS end in the proposed scheme closely resembles that of using the Paillier cryptosystem for encryption, Lu et al.'s scheme [19]. But compared to Lu et al.'s scheme [19], the proposed scheme adds resistance against internal attacks.

During the proxy re-encryption and aggregation phase, AG first performs re-encryption operations on the reported ciphertext data after verifying signatures. Then, it aggregates the re-encrypted ciphertexts. The plaintext dimension is fixed at $k = 10$. Fig. 4. shows the time cost comparison chart of data operations at the aggregator gateway end in various schemes. Since Zhan et al.'s scheme [17] is a single-dimensional data aggregation scheme, in Zhan et al.'s scheme [17], the AG operation is repeated ten times to ensure it can achieve the same functionality as the multi-dimensional data aggregation scheme. Due to the choice of introducing proxy re-encryption to enhance the flexibility and reliability of the system framework, the time cost may be slightly higher compared to existing schemes. However, it remains at the millisecond level, which is acceptable for the practical implementation of the scheme.

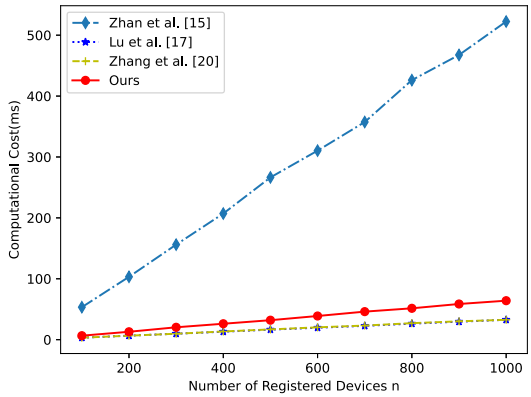


Fig. 4. Ciphertext computation costs on AG side.

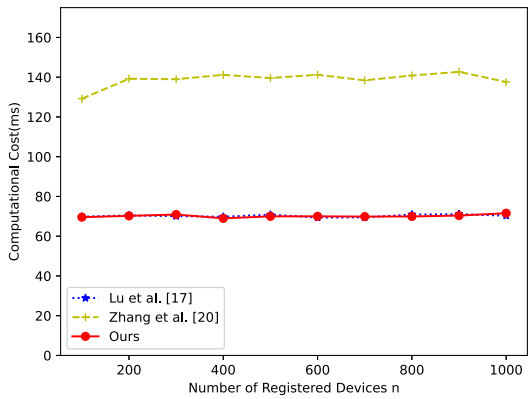


Fig. 5. Decryption costs on ECC side.

During the data decryption phase, ECC decrypts the received ciphertexts after verifying signatures and then uses an algorithm to extract the sum of the data for each dimension from the aggregated plaintext. The plaintext dimension is also fixed at $k = 10$. Fig. 5 shows the decryption time cost comparison chart at the power computation center end in various schemes. Since the decryption in Zhan et al.'s scheme [17] is only suitable for data in a smaller plaintext space, it was not included in the comparison. From the figure, the proposed scheme has a low decryption overhead. Compared to Zhang et al.'s scheme [22] and a similarly costly scheme like Lu et al.'s scheme [19], the framework can support updates to ECC.

D. Communication Costs Analyses

In this section, the communication overhead between SStoAG and AGtoECC has been theoretically analyzed. In the proposed scheme and the comparison schemes, the ciphertext size for both the Paillier cryptosystem and its variant algorithms is 4096 bits, while the ciphertext size for the EC-ElGamal cryptosystem is 392 bits. The signature algorithms for all schemes are implemented on the BLS12-383 curve, with a signature size of 392 bits. To ensure the correctness and consistency of the theoretical analyses' results, the size of identifiers and timestamps is set to 32 bits.

TABLE IV
THEORETICAL ANALYSES OF COMMUNICATION

Scheme	SStoAG	AGtoECC
Zhan *et al.* [17]	(1176k+848)n	784k + 848
Lu *et al.* [19]	4584n	4584
Zhang *et al.* [22]	4520n	4912
Ours	4520n	4552

First, the data reporting phase from SS to AG is analyzed. In the proposed scheme, each SS sends a data report $\{C, \sigma, T\}$ to AG, resulting in a communication cost of $(4096 + 392 + 32) \cdot n = 4520n$ bits for n SSs to AG. In Zhan et al.'s scheme [17], each SS sends a data report $\{T, ID, C, L, \sigma\}$ to AG, resulting in a communication cost of $(32 + 32 + 3923 + 392 + 392) \cdot n = 2024n$ bits. Since Zhan et al.'s scheme [17] is a single-dimensional data aggregation scheme, as plaintext dimensions increase, the communication cost becomes $(32 + 32 + 3923 \cdot k + 392 + 392) \cdot n = 1176kn + 848n$. In Lu et al.'s scheme [19], each SS sends a data report $\{C, RA, U, T, \sigma\}$ to AG, resulting in a communication cost of $(4096 + 32 + 32 + 32 + 392) \cdot n = 4584n$ bits. In Zhang et al.'s scheme [22], each SS packs $\{C, \sigma, T\}$ and sends it to AG, resulting in a communication cost of $(4096 + 392 + 32) \cdot n = 4520n$ bits.

Next, the data reporting phase from AG to ECC is analyzed. In the proposed scheme, AG sends a data report $\{C, \sigma, n, T\}$ to ECC, resulting in a communication cost of $(4096 + 392 + 32 + 32) = 4552$ bits. In Zhan et al.'s scheme [17], AG sends $\{t, ID, C, L, \sigma\}$ to ECC. Considering Zhan et al.'s scheme [17] is a single-dimensional scheme, the communication cost is $(32 + 32 + 3922 \cdot k + 392 + 392) = 784k + 848$ bits. In Lu et al.'s scheme [19], AG reports $\{C, RA, GW, T, \sigma\}$ to ECC, resulting in a communication cost of $(4096 + 32 + 32 + 32 + 392) = 4584$ bits. In Zhang et al.'s scheme [22], AG sends $\{C, \sigma, \xi, T\}$ to ECC, resulting in a communication cost of $(4096 + 392 + 392 + 32) = 4912$ bits.

The theoretical cost analyses of each scheme are shown in Table IV. From the figure, it can be seen that changes in plaintext dimensions affect the communication overhead of Zhan et al.'s scheme [17]. When the plaintext dimension is greater than or equal to 4, the $SStoAG$ communication overhead in Zhan et al.'s scheme [17] already exceeds that of the proposed scheme. When the plaintext dimension is greater than or equal to 5, the $AGtoECC$ communication overhead in Zhan et al.'s scheme [17] exceeds that of the proposed scheme. The proposed scheme achieves multi-dimensional data aggregation while consuming fewer communication resources.

VIII. CONCLUSION

In this study, we propose a privacy-preserving multi-dimensional data aggregation scheme based on homomorphic proxy re-encryption (MPDA-HPR). To enable the dynamic management of entities in the smart grid of IIoT, a modified Paillier cryptosystem with the support of proxy re-encryption is designed. The proposed scheme enhances privacy for sensitive device and electricity consumption data while increasing

resilience against internal attacks and fault tolerance. Security and performance analyses demonstrate the effectiveness and applicability of MPDA-HPR for smart grids of IIoT systems compared with other schemes, where the proposed scheme provides more security functionalities but a similar overhead.

ACKNOWLEDGMENT

The authors are very grateful to the anonymous referees for their detailed comments and suggestions regarding this paper.

REFERENCES

[1] J.-N. Liu, J. Weng, A. Yang, Y. Chen, and X. Lin, "Enabling efficient and privacy-preserving aggregation communication and function query for fog computing-based smart grid," *IEEE Trans. Smart Grid*, vol. 11, no. 1, pp. 247–257, Jan. 2020.

[2] J. Wang, L. Wu, S. Zeadally, M. K. Khan, and D. He, "Privacy-preserving data aggregation against malicious data mining attack for IoT-enabled smart grid," *ACM Trans. Sensor Netw.*, vol. 17, no. 3, pp. 1–25, 2021.

[3] Q. Zhang, Y. Fu, J. Cui, D. He, and H. Zhong, "Efficient fine-grained data sharing based on proxy re-encryption in IIoT," *IEEE Trans. Dependable Secure Comput.*, vol. 21, no. 6, pp. 5797–5809, Nov./Dec. 2024.

[4] Y. Liu, C. Yang, L. Jiang, S. Xie, and Y. Zhang, "Intelligent edge computing for IoT-based energy management in smart cities," *IEEE Netw.*, vol. 33, no. 2, pp. 111–117, Mar./Apr. 2019.

[5] J. Li, C. Gu, Y. Xiang, and F. Li, "Edge-cloud computing systems for smart grid: State-of-the-art, architecture, and applications," *J. Modern Power Syst. Clean Energy*, vol. 10, no. 4, pp. 805–817, 2022.

[6] H. Farhangi, "The path of the smart grid," *IEEE Power Energy Mag.*, vol. 8, no. 1, pp. 18–28, Jan./Feb. 2010.

[7] J. Su and M. Jiang, "A hybrid entropy and blockchain approach for network security defense in SDN-based IIoT," *Chin. J. Electron.*, vol. 32, no. 3, pp. 531–541, 2023.

[8] T. Haibo, L. Maonan, and R. Shuangyin, "ESE: Efficient security enhancement method for the secure aggregation protocol in federated learning," *Chin. J. Electron.*, vol. 32, no. 3, pp. 542–555, 2023.

[9] B. Jiang, M. Li, and R. Tandon, "Local information privacy and its application to privacy-preserving data aggregation," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 3, pp. 1918–1935, May/Jun. 2022.

[10] D. He, S. Chan, Y. Zhang, M. Guizani, C. Chen, and J. Bu, "An enhanced public key infrastructure to secure smart grid wireless communication networks," *IEEE Netw.*, vol. 28, no. 1, pp. 10–16, Jan./Feb. 2014.

[11] Q. Zhang, J. Wu, H. Zhong, D. He, and J. Cui, "Efficient anonymous authentication based on physically unclonable function in industrial Internet of Things," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 233–247, 2023.

[12] F. Wang, J. Cui, Q. Zhang, D. He, and H. Zhong, "Blockchain-based secure cross-domain data sharing for edge-assisted industrial Internet of Things," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 3892–3905, 2024.

[13] Y. Chen, J.-F. Martıńez-Ortega, P. Castillejo, and L. López, "A homomorphic-based multiple data aggregation scheme for smart grid," *IEEE Sensors J.*, vol. 19, no. 10, pp. 3921–3929, May 2019.

[14] Y. Ding, B. Wang, Y. Wang, K. Zhang, and H. Wang, "Secure metering data aggregation with batch verification in industrial smart grid," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6607–6616, Oct. 2020.

[15] C. Castelluccia, E. Mykletun, and G. Tsudik, "Efficient aggregation of encrypted data in wireless sensor networks," in *Proc. 2nd Annu. Int. Conf. Mobile Ubiquitous Syst.: Netw. Serv.*, 2005, pp. 109–117.

[16] Y. Liu, W. Guo, C.-I. Fan, L. Chang, and C. Cheng, "A practical privacy-preserving data aggregation (3PDA) scheme for smart grid," *IEEE Trans. Ind. Informat.*, vol. 15, no. 3, pp. 1767–1774, Mar. 2019.

[17] Y. Zhan, L. Zhou, B. Wang, P. Duan, and B. Zhang, "Efficient function queryable and privacy preserving data aggregation scheme in smart grid," *IEEE Trans. Parallel Distrib. Syst.*, vol. 33, no. 12, pp. 3430–3441, Dec. 2022.

[18] G. Verma, P. Gope, N. Saxena, and N. Kumar, "CB-DA: Lightweight and escrow-free certificate-based data aggregation for smart grid," *IEEE Trans. Dependable Secure Comput.*, vol. 20, no. 3, pp. 2011–2024, May/Jun. 2023.

[19] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1621–1631, Sep. 2012.

[20] S. Li, K. Xue, Q. Yang, and P. Hong, "PPMA: Privacy-preserving multi-subset data aggregation in smart grid," *IEEE Trans. Ind. Informat.*, vol. 14, no. 2, pp. 462–471, Feb. 2018.

[21] D. Chen, T. Zhou, W. Liu, R. Li, L. Wu, and X. Yang, "MDA-FLH: Multidimensional data aggregation scheme with fine-grained linear homomorphism for smart grid," *IEEE Internet Things J.*, vol. 11, no. 2, pp. 3524–3538, Jan. 2024.

[22] X. Zhang, C. Huang, Y. Zhang, and S. Cao, "Enabling verifiable privacy-preserving multi-type data aggregation in smart grids," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 6, pp. 4225–4239, Nov./Dec. 2022.

[23] N. Saxena, B. J. Choi, and R. Lu, "Authentication and authorization scheme for various user roles and devices in smart grid," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 5, pp. 907–921, May 2016.

[24] X. Zhang, C. Huang, C. Xu, Y. Zhang, J. Zhang, and H. Wang, "Key-leakage resilient encrypted data aggregation with lightweight verification in fog-assisted smart grids," *IEEE Internet Things J.*, vol. 8, no. 10, pp. 8234–8245, May 2021.

[25] M. Y. Mehmood et al., "Edge computing for IoT-enabled smart grid," *Secur. Commun. Netw.*, vol. 2021, pp. 1–16, 2021.

[26] S. Zhao et al., "Smart and practical privacy-preserving data aggregation for fog-based smart grids," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 521–536, 2020.

[27] L. Lyu, K. Nandakumar, B. Rubinstein, J. Jin, J. Bedo, and M. Palaniswami, "PPFA: Privacy preserving fog-enabled aggregation in smart grid," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3733–3744, Aug. 2018.

[28] K. Xue, B. Zhu, Q. Yang, D. S. Wei, and M. Guizani, "An efficient and robust data aggregation scheme without a trusted authority for smart grid," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 1949–1959, Mar. 2020.

[29] L. Chen, R. Lu, Z. Cao, K. AlHarbi, and X. Lin, "MuDA: Multifunctional data aggregation in privacy-preserving smart grid communications," *Peer-to-Peer Netw. Appl.*, vol. 8, pp. 777–792, 2015.

[30] H. Bao and R. Lu, "A new differentially private data aggregation with fault tolerance for smart grid communications," *IEEE Internet Things J.*, vol. 2, no. 3, pp. 248–258, Jun. 2015.

[31] X. Zuo, L. Li, H. Peng, S. Luo, and Y. Yang, "Privacy-preserving multi-dimensional data aggregation scheme without trusted authority in smart grid," *IEEE Syst. J.*, vol. 15, no. 1, pp. 395–406, Mar. 2021.

[32] A. Saleem et al., "FESDA: Fog-enabled secure data aggregation in smart grid IoT network," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6132–6142, Jul. 2020.

[33] D. Derler, S. Ramacher, and D. Slamanig, "Homomorphic proxy re-authenticators and applications to verifiable multi-user data aggregation," in *Proc. 21st Int. Conf. Financial Cryptogr. Data Secur.*, Sliema, Malta, Springer, 2017, pp. 124–142.

[34] J. Ni, K. Zhang, X. Lin, and X. S. Shen, "Balancing security and efficiency for smart metering against misbehaving collectors," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 1225–1236, Mar. 2019.

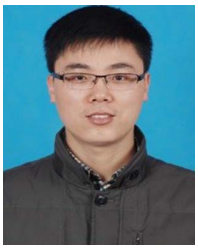
[35] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. Int. Conf. Theory Appl. Cryptographic Techn.*, Springer, 1999, pp. 223–238.

[36] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, Springer, 2001, pp. 514–532.

[37] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Proc. Annu. Int. Cryptol. Conf.*, Springer, 2001, pp. 213–229.

Qingyang Zhang received the BE and PhD degrees in computer science from Anhui University, in 2014 and 2021, respectively. He is currently an associate professor with the School of Computer Science and Technology, Anhui University. He was also a visiting student with Wayne State University. His research interest includes edge computing, computer systems, and security. He has more than 40 scientific publications in reputable journals (e.g., *Proceedings of the IEEE*, *IEEE Transactions on Dependable and Secure Computing*, *IEEE Transactions on Information Forensics and Security*, *IEEE Transactions on Parallel and Distributed Systems*, *IEEE Transactions on Computers*) and international conferences.

Zhen Fang is now working toward the degree with the School of Computer Science and Technology, Anhui University. His research focuses on the security of the Industrial Internet of Things (IIoT).



Jie Cui (Senior Member, IEEE) received the PhD degree from the University of Science and Technology of China, in 2012. He is currently a professor and PhD supervisor with the School of Computer Science and Technology, Anhui University. His current research interests include applied cryptography, IoT security, vehicular ad hoc network, cloud computing security and software-defined networking (SDN). He has more than 150 scientific publications in reputable journals (e.g., *IEEE Transactions on Dependable and Secure Computing*, *IEEE Transactions on Information Forensics and Security*, *IEEE Journal on Selected Areas in Communications*, *IEEE Transactions on Mobile Computing*, *IEEE Transactions on Parallel and Distributed Systems*, *IEEE Transactions on Computers*), academic books and international conferences.

Hulin Jin received the PhD degree from the Sejong University of Korea, in 2013. He is currently a professor and PhD supervisor with the School of Big Data and Statistics, Anhui University. His current research interests include Big Data, computer vision, and cloud computing. He has more than 100 scientific publications.

Fengqun Wang received the PhD degree in computer science from Anhui University, in 2024. He is currently a lecture with the School of Computer Science and Technology, Anhui University. His research interests include IoT security, blockchain and applied cryptography. He has multiple scientific publications in reputable journals (e.g., *IEEE Transactions on Information Forensics and Security*, *IEEE Transactions on Dependable and Secure Computing*, *IEEE Transactions on Network and Service Management*, *IEEE Transactions on Industrial Electronics*).

Debiao He received the PhD degree in applied mathematics from the School of Mathematics and Statistics, Wuhan University, Wuhan, China, in 2009. He is currently a professor with the School of Cyber Science and Engineering, Wuhan University, Wuhan, China, and the Shanghai Key Laboratory of Privacy Preserving Computation, MatrixElements Technologies, Shanghai 201204, China. His main research interests include cryptography and information security, in particular, cryptographic protocols. He has published more than 100 research papers in refereed international journals and conferences, such as *IEEE Transactions on Dependable and Secure Computing*, *IEEE Transactions on Information Security and Forensic*, and Usenix Security Symposium. He is the recipient of the 2018 IEEE Sysems Journal Best Paper Award and the 2019 IET Information Security Best Paper Award. His work has been cited more than 10000 times with Google Scholar. He is in the editorial board of several international journals, such as *Journal of Information Security and Applications*, *Frontiers of Computer Science*, and *Human-centric Computing & Information Sciences*.