IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 5 July 2023, accepted 17 July 2023, date of publication 3 August 2023, date of current version 16 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3301570

RESEARCH ARTICLE

A Blockchain-Enabled Authentication and Conserved Data Aggregation Scheme for Secure Smart Grids

CHIEN-DING LEE[1], JHIH-HONG LI[2], AND TZUNG-HER CHEN[2]
[1]Department of Management and Information, National Open University, New Taipe 24701, Taiwan
[2]Department of Computer Science and Information Engineering, National Chiayi University, Chiayi 60004, Taiwan

Corresponding author: Tzung-Her Chen (thchen@mail.ncyu.edu.tw)

This work was supported in part by the Ministry of Science and Technology of Taiwan under Grant MOST 110-2221-E-415-006-MY2, and in part by the National Science and Technology Council of Taiwan under Grant NSTC 112-2221-E-415-005.

ABSTRACT The construction of smart grids provides many benefits. Computational cost, however, drastically grows with an increase in scale since a large amount of data is generated, transmitted, collected, and treated. Although data aggregation technology is helpful when adopting smart grid applications, corresponding security and performance issues should be considered while implementing the mechanism. In this paper, a blockchain-enabled authenticated conserved data aggregation scheme is proposed to balance security concerns and the computational cost of the smart grid. Furthermore, several functions are developed in our scheme to highlight the contributions. First, efficient cryptographic algorithms are integrated instead of computationally-expensive ones. Second, the proposed scheme seamlessly incorporates a blockchain system into a smart grid for better decentralization which can avoid the possible threats and high cost of a centralized system. Third, the scheme is scalable, which can be adapted to manage a great number of metering devices. Fourth, the aggregational operations in our design combine power data and signature, which is more practical. Finally, the proposed scheme covers a one-time key pair and signature mechanism, thus upgrading the privacy protection of blockchain applications in the smart grid.

INDEX TERMS Blockchain, data aggregation, elliptic curve cryptography, smart grids.

I. INTRODUCTION

Over the last decades, electricity consumption has grown considerably due to the development of technology and associated increasing demand, especially for the mass deployment of electrical devices. Smart grids are electronic energy networks used to connect a great number of electronic devices and establish a two-way flow infrastructure of electricity-relevant data, which contrasts with a typical system. There are many advantages to constructing a smart grid, such as digitization, efficiency enhancement, reliability improvement, cost savings, renewables integration, fast demand response, etc. Moreover, smart grids are a key modern infrastructure that has been tied together with the standardization and technologies related to Industry 4.0 [1].

The associate editor coordinating the review of this manuscript and approving it for publication was Mouloud Denai.

There are several major components involved in a smart grid. In particular, a smart meter is a crucial component used to automatically measure and collect energy consumption readings from different sources including a Subject Matter Expert (SME) and household appliances. It replaces traditional manual meters and is associated with the advanced metering infrastructure (AMI) which is being promoted by many countries. For instance, the installation number of electricity smart meters in the European Union (EU) countries will be approximately 223 million and 266 million (corresponding to 77% and 92% penetration rates) in 2024 and 2030, respectively [2].

The control center is another important component that collects and analyzes the power-related data received from smart meters. The evaluated results can be used to make further improvements, such as power demand forecasting, load monitoring, resource allocation, billing, etc. [3]. This

bidirectional characteristic from the analyzed result of consumption data can be fed back to consumers and power companies from the control center. Thus, customers and power companies can arrange individual consumption plans that minimize electricity costs and optimize energy management, respectively. Furthermore, by leveraging integration and analysis of real-time electricity consumption data, smart grid development can obtain more advanced functionalities [4], [5] such as self-healing, self-resilience, autonomous demand response, renewable energy resource, peak-time electricity consumption control, etc.

A. RELATED WORK

To gain benefits from smart grids, the dominant issues regarding security and privacy have to be carefully considered since the devices are widely distributed, and energy consumption data are usually transmitted via public networks, which raises high potential risks. Important focuses of attention include false data injection attacks [6], cyber security issues [7], [8], data analysis concerns [9], malicious data mining attacks [10], etc. As a result, a security mechanism should be properly established to protect the system from any possible risks. Such a mechanism needs to safeguard associated privacy-related information, e.g. household living patterns and economic situation [11], [12], while also protecting data that may impose on privacy.

In a smart grid, privacy-preserving data aggregation is one of the common solutions to securely handle integrated consumption data. In [13], Fan et al. proposed a privacy-enhanced data aggregation scheme in which blinding factors and batch verification are both involved against the internal attacker. Their scheme requires an offline trusted third party (TTP) which is responsible to generate and distribute blinding factors to the aggregator and all users. However, the need of the blinding factor may raise scalable concerns because the overall computation and distribution for blinding factors are needed if new meters join or broken meters have to be removed. In [14], He et al. developed a data aggregation scheme by applying a Boneh-Goh-Nissim cryptosystem against internal attackers; Vahedi et al. [15] and Chen et al. [16] respectively proposed elliptic curve-based aggregation schemes that [16] contain a scalable function since smart meters in their design can be added to or removed out without affecting the services; and Zhang et al. [17] proposed a data aggregation method, which takes the lightweight advantage into account while implemented in a resource-constrained environment. Akgun et al. [18] presented a customer-oriented aggregation scheme for privacy protection in the smart grid. In their approach, Trusted Execution Environment (TEE) is a crucial role since it is assigned to concentrate various core tasks, such as the distribution of customer keys, decryption operations, load monitoring, billing, and other types of added value services. Rather than placing an aggregator, the research [18] layouts the aggregation function over the selected customer within the selected period. It may restrict the scalability of the system because the update of meters may break the operations of aggregation, especially when some customers have been selected as aggregators and their meters has to be adjusted for some purposes.

Those schemes [13], [14], [15], [16], [17], [18], however, rely on a trusted third party (TTP) to carry out complex authentication and/or certificate-related operations, which is inefficient and costly. Such centralized architectures may be vulnerable to some threats, such as insider attacks, external attacks, or single points of failure. Hence, some research has aimed to remove TTP or certificate authority (CA) for smart grids. For instance, based on the idea of certificateless public key cryptography [19], Wang et al. [20] designed an ID-based certificateless aggregation signcryption scheme. However, the users' keys are managed in a key generation center (KGC) which is still centralized even if certificates are not used in the scheme. Zuo et al. [21] proposed a privacy-preserving multidimensional data aggregation method based on the ElGamal homomorphic cryptosystem. In their approach, certificates need to be issued and managed by the control center, and as such, similar concerns exist because the control center is centralized.

In the present era, blockchain technology has the capability to eliminate the reliance on a trusted authority and address the challenges inherent in centralized approaches. This is due to its provision of decentralized, tamper-proof, and traceable services. With the recent proliferation of digital currencies, e.g. Bitcoin [22], Ethereum [23], and Hyperledger [24], the benefits of blockchain have attracted the attention of both academia and industry. In a smart grid application, there are several approaches employing blockchain technology to accomplish privacy-preserving data aggregation mechanisms. Fan et al. [25] proposed a privacy-preserving data aggregation scheme under a blockchain architecture. In their design, the Paillier cryptosystem is employed, and mining nodes, determined from all smart meters, are required to handle the generation of system parameters and the authenticity of data transmitted. Since crucial data and complex operations must be handled on the mining nodes, centralized problems such as malicious threats and cost concerns may transfer to those nodes. In [26], Li et al. proposed a dual-blockchain-based lightweight scheme for a smart grid environment with a scenario regarding sales, pricing, and payment, in which a user's private information is protected by applying identity-based proxy re-encryption and signature mechanisms. A trusted authority, however, is still required in the method even if dual blockchains are developed for private and shared aspects respectively.

B. MOTIVATION AND CONTRIBUTION

There are several areas of improvement that can be addressed in existing works. Firstly, some of the current approaches rely on computationally-expensive cryptographic algorithms. The higher the computational cost required, the greater the operational burden becomes, especially when dealing with a large number of meters.

Secondly, the reliance on a trusted third-party and public key infrastructure (PKI) presents security and cost challenges. In contrast, a decentralized blockchain network offers a means to mitigate various potential threats and maintain lower costs compared to a centralized structure, provided that the blockchain and cryptographic mechanisms are effectively combined.

Thirdly, scalability is a notable challenge in certain existing works, such as [13] and [18]. Scalability refers to a system or network's ability to easily adapt to increasing demands [27]. By incorporating scalability, smart meters can be efficiently added or removed as needed, ensuring that a smart grid system does not go offline when some meters are broken and require replacement [16].

Fourthly, the aggregation task should encompass more than just electronic consumption data; it should also include data and signature processes. Aggregating the signatures alongside the consumption data enables verification of the aggregated consumption data using the aggregated signatures.

Lastly, it is important to consider that when a block transaction containing a sender's information is transmitted over a public channel, there is a risk that an adversary may gather enough clues to infer, induce, or even expose someone's energy usage behavior.

In this paper, we present an novel scheme called Blockchain-enabled Authenticated and Conserved Data Aggregation (BACDA), which addresses the aforementioned concerns comprehensively. Our scheme seamlessly integrates blockchain technology with appropriate cryptographic mechanisms to ensure authentication, confidentiality, anti-tampering, and data aggregation along with the corresponding signatures. This integration guarantees security and privacy protection in the scenario of a smart grid environment.

The main contributions of this study are summarized below.

1) Compared with existing aggregation schemes, the proposed scheme, based on Elliptic Curve Cryptography (ECC), facilitates a smaller key size while retaining a similar security level, which also reduces the total computational cost.
2) The algorithms for encryption/decryption and signature proposed in this scheme are based on the elliptic curve, that is, ECC encryption and ECDSA, which can seamlessly interoperate with a blockchain. The combination of a blockchain and smart grid also guarantees full decentralization, thus minimizing possible security risks and the additional high costs of maintaining a trusted third party as well as PKI.
3) The proposed scheme considers scalability, which means that the whole crucial information used to support smart grid operations is not held by any one specific party. Moreover, the transactions generated at each time are independent of one another, thus satisfying that some meter devices can be replaced without interrupting the services.
4) In our design, the aggregational subjects cover ciphertext data and signatures, which improves communication and computational performance. Moreover, based on the blockchain, the proposed scheme supports an infrastructure where the aggregator does not need to process the time-consuming verification of signatures.
5) Derived from the idea of a one-time address [28], the proposed scheme assures that each smart meter's public/private key pair is frequently updated for at least each transaction. Although all information saved in a blockchain is public, it is significantly harder for an adversary to track customer privacy-related information. A one-time signature is also developed in the proposed scheme.

C. PAPER ORGANIZATION

The rest of this manuscript is organized as follows. In Section II, relevant background knowledge is briefly reviewed. Section III provides the proposed system model and the proposed BACDA schemes. Security analysis is shown in Section IV. Functionality features as well as performance analysis are discussed in Section V. The research is concluded in Section VI.

II. PRELIMINARY

This section gives a brief overview of the essential relevant background of the proposed scheme including cryptographic primitives, blockchain technology, Elliptic Curve Digital Signature Algorithm (ECDSA), Elliptic Curve Cryptography (ECC)-based encryption algorithm, and Homomorphic encryption.

A. CRYPTOGRAPHIC PRIMITIVES

There are several cryptographic primitives involved in the proposed scheme, including hash function, digital signature, and encryption algorithm. To facilitates understanding of our design, the properties of those techniques are briefly introduced.

1) HASH FUNCTION

A hash function is a one-way mathematical operation in which a fixed-size digest is generated from inputting a variable-size message. The one-way property guarantees that inferring the original long string from a given digest and finding two different messages that can generate the same hashed result is both computationally infeasible. It also achieves the collision-resistant feature. A hash function is denoted as H: $\{0,1\}^* \rightarrow F_n$.

2) DIGITAL SIGNATURE

In a digital signature system, a signer signs messages by using a specific private key, and then its origin and whether the message has been illegally modified can be verified with the corresponding public key, which provides authenticity, data integrity, and non-repudiation since the private key is unique and only held by the signer. For example, Elliptic Curve

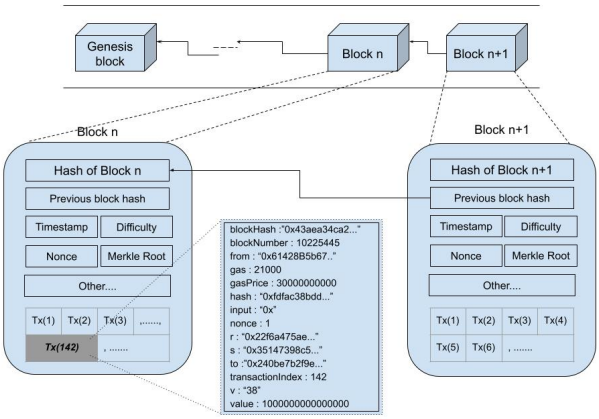

FIGURE 1. Ethereum blockchain structure.

Digital Signature Algorithm (ECDSA) [29] is a signature algorithm generally applied in the blockchain. The detail of ECDSA will be stated in the later section.

3) ENCRYPTION ALGORITHM

An encryption method called a cryptosystem, is applied to convert plaintexts into unreadable ciphertexts to prevent unauthorized disclosure. The algorithm provides a way to achieve confidentiality property since only the authorized user with the correct decryption key can obtain the original plaintexts. Several common algorithms applied for encryption include the Advanced Encryption Standard (AES) [30], RSA [31], Paillier [32], Elliptic Curve Cryptography (ECC) [33], etc.

Furthermore, homomorphic encryption [34] is a specific encryption technique that provides some extended features than conventional encryption and will be described in detail in the later section.

B. BLOCKCHAIN TECHNOLOGY

Blockchain is a distributed ledger technology that consists of an ordered list of continuously appended blocks maintained by all participating nodes. An example of the Ethereum blockchain structure is depicted in Figure 1. In Ethereum, a transaction (Tx) is composed of a group of data including the sender's message, the sender's address, and the recipient's address recorded in the fields of "*input*", "*from*" and "*to*", respectively. The signature of a transaction is recorded in the fields of "r" and "s" and the value in the "v" field can be employed to restore a sender's public key.

Based on cryptographic technologies, all blocks are chained together and the information placed in entire blocks is tamperproof, which guarantees the immutability of the blockchain. In general, the Elliptic Curve Digital Signature Algorithm (ECDSA) is applied to assure the security properties in popular blockchain systems. To facilitate an understanding of our proposed blockchain-enabled scheme, ECDSA will be briefly introduced in the next section.

C. ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM (ECDSA)

The Elliptic Curve Digital Signature Algorithm (ECDSA) [29], based on the group of points on elliptic curves, is a type of signature algorithm and consists of four stages: setup, key generation, signature generation, and verification. The stages are as follows:

1) SETUP PHASE

Assume E is an elliptic curve over the finite field F_q where q is a prime number such that all the points on E denote a finite group G with the prime multiplicative order n and a base point P.

2) KEY GENERATION PHASE

The signer generates a key pair by performing the following operations.

Step 1: Select an integer d as the private key, where $0 < d < n$.

Step 2: Compute $Q = d\,G$ as the public key corresponding to the private key d.

3) SIGNATURE GENERATION PHASE

To sign the message m, the signer does the following steps.

Step 1: Choose an integer k as a secure random number, where $0 < k < n$.

Step 2: Compute $e = H(m)$ and the curve point $(x_1, y_1) = kG$.

Step 3: Compute $r = x_1 \bmod n$.

Step 4: Compute $s = k^{-1}\,(e + dr) \bmod n$.

4) VERIFICATION PHASE

The verifier confirms the signature by using the public key as follows.

Step 1: Compute $e = H(m)$.

Step 2: Compute

$$w = s^{-1} \bmod n,$$
$$u_1 = e\,w \bmod n,$$
$$\text{and } u_2 = r\,w \bmod n.$$

Step 3: Compute $X = u_1\,g + u_2 Q$.

Step 4: Check whether $v = r$ to ensure the validity of the signature, where v is the x-coordinate of X.

D. ECC-BASED ENCRYPTION ALGORITHM

Based on the elliptic curve, the ECC-based encryption algorithm is performed as follows.

1) ENCRYPTION PHASE

The receiver has a key pair (d, Q), and the sender encrypts a plaintext message by doing the following operations.

Step 1: Assume plaintext m maps to a point P_m on the elliptic curve.

Step 2: Choose an integer r as a secure random number, where $0 < r < n$.

Step 3: Compute the curve point $C_1 = rG$.
Step 4: Compute the curve point $C_2 = P_m + rQ$.
The receiver then gets the ciphertext C_1 and C_2.

2) DECRYPTION PHASE

After receiving, the receiver decrypts the ciphertext by doing the following operations to obtain its corresponding plaintext.
Step 1: Compute the curve point $P_m = C_2 - d\ C_1$.
Step 2: Decode the plaintext m from point P_m.

E. HOMOMORPHIC ENCRYPTION

Homomorphic encryption [34] is a specific encryption method that allows users to computationally operate the ciphertext without performing decryption. The result is the same as if the ciphertexts were still in their original form. The technology provides a way to achieve better data usage while protecting confidentiality and privacy.

Let *Enc* be the encryption function, *Dec* be the decryption function and f be an operation function. A cryptosystem is homomorphic if the encryption and decryption functions satisfy the equation

$f(M_1, M_2) = Dec(f(Enc(M_1), Enc(M_2)))$.

If $f(.)$ is an addition operator, then the scheme is said to be additive homomorphic, if f is a multiplicative operator, then it is multiplicatively homomorphic. ECC homomorphic encryption can realize the additive homomorphic and multiplicative homomorphic. The addition homomorphic operation is given below, while the ciphertexts are (C_{1_i}, C_{2_i}).

1) ENCRYPTION PHASE

$$\sum_{i=1}^{n} C_{1_i} = \sum_{i=1}^{n} r_i G = G \sum_{i=1}^{n} r_i$$

$$\sum_{i=1}^{n} C_{2_i} = \sum_{i=1}^{n} (r_i Q + P_{M_i}) = Q \sum_{i=1}^{n} r_i + \sum_{i=1}^{n} P_{M_i}$$

2) DECRYPTION PHASE

$$\sum_{i=1}^{n} C_{2_i} - d \sum_{i=1}^{n} C_{1_i} = Q \sum_{i=1}^{n} r_i + \sum_{i=1}^{n} P_{M_i} - dG \sum_{i=1}^{n} r_i$$

$$= \sum_{i=1}^{n} P_{M_i}$$

The result $\sum_{i=1}^{n} P_{M_i}$ can be decoded into $\sum_{i=1}^{n} M_i$.

III. BLOCKCHAIN-ENABLED AUTHENTICATED AND CONSERVED DATA AGGREGATION SCHEME (BACDA)

In this section, the system model, adversarial model, and security requirements are given to depicting the basic organization of our scheme. Then, the proposed BACDA scheme involving major five phases is described in detail.

A. SYSTEM MODEL

The system model consists of four major entities: smart meter (*SM*), aggregator (*Agg*), control center (*CC*), and blockchain

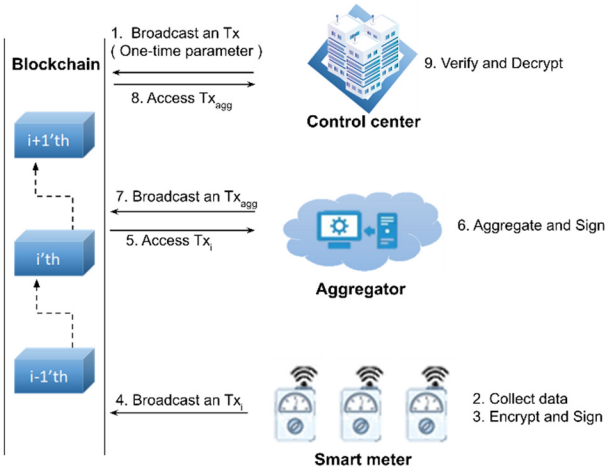

FIGURE 2. System model of the proposed scheme.

network. Those entities and their crossing procedures are depicted in Figure 2.

- Smart meter (*SM*): Compared to traditional electronic meters, a smart meter has a communication capability that allows the exchange of information between users and the control center. A smart meter regularly gathers real-time power consumption, performs encryption as well as the digital signature, and sends the encrypted data to the blockchain. Generally, it is a resource-restricted device because of limited storage and computing ability.
- Aggregator (*Agg*): *Agg* deals with the aggregation of encrypted power consumption data sent from smart meters. It then signs and transmits the aggregated ciphertext to the blockchain for further handling by the control center.
- Control center (*CC*): With the private key, a *CC* can decrypt the aggregated ciphertext sent from *Agg*. After obtaining the aggregated consumption data, *CC* has sufficient resources to perform business administrative tasks, such as billing, dynamic pricing, power generation plan adjustment, trend analysis, and appropriate feedback for users.
- Blockchain: A blockchain stores all transactions as well as the ciphertext and the aggregated ciphertext sent from the *SM* and *Agg*, respectively. The properties of a blockchain guarantee that no one can modify data once it has been sent to the blockchain network, which is conducive to traceability.

A scenario of the system is described as follows. First, *CC* broadcasts to the blockchain a transaction with a one-time parameter. Once the home appliance is active and establishes a connection with *SM*, its power consumption M_i starts to be transferred to the *SM*. To guarantee data confidentiality, *SM* performs encryption by using *CC*'s public key Q_c to generate the ciphertext of M_i, denoted as (C_{1_i}, C_{2_i}). The *SM* periodically broadcasts new transaction T_{xi} with (C_{1_i}, C_{2_i})

TABLE 1. Important notations used in BACDA scheme.

Notation	Description
SM_i, $i = 1,2,\ldots,n$	Identity of smart meter
Agg	Identity of aggregator
CC	Identity of the control center
E, F_q, q, G, n, F_n^*	Elliptic curve parameters
$H(.)$	One-way hash function
(d_i, Q_i)	SM_i's key pair
(d_c, Q_c)	CC's key pair
(d_{Agg}, Q_{Agg})	Agg's key pair
M_i, $i = 1,2,\ldots,n$	Power consumption data of SM_i
T_{xi}, $i = 1,2,\ldots,n$	The Transaction generated by SM_i
(C_{1_i},C_{2_i})	M_i's key pair
(r, s_i)	T_{xi}'s signature
(C_1,C_2)	Aggregated ciphertext (C_{1_i},C_{2_i})
(r, s)	Aggregated signature (r, s_i)
k	A secure number for a one-time signature

and the corresponding signature (r, s_i) signed by SM to the blockchain. Hereafter, the Agg aggregates each ciphertext and signature into (C_1, C_2) and (r, S), respectively, and further broadcasts the transaction to the blockchain. Finally, CC obtains the aggregated ciphertext and verifies the aggregated signature. If it is valid, CC decrypts the ciphertext (C_1, C_2) by using its private key d_c and thus gets the original aggregated plaintext $\sum_{i=1}^{n} M_i$.

A brief description of the important notations used in the proposed BACDA scheme is summarized in Table 1.

B. ADVERSARY MODEL AND SECURITY REQUIREMENTS

Herein, we consider an adversarial model in which the essential participants of the system model including SM_i Agg, CC, and blockchain network are honest and curious. Adversary $\mathcal{A}$ is a dishonest but non-intrusive entity, that may break the system rules, and try to learn meter and aggregated data respectively sent from SM_i and Agg by eavesdropping on the public communication network. $\mathcal{A}$ is also attempting to infer the customers' private information by analyzing the consumption data that has been collected. Moreover, $\mathcal{A}$ has no way to insert, modify, or delete the data which are stored. Challenger $\mathcal{C}$ is an entity that operates the cryptographic system and interacts with $\mathcal{A}$.

Confidentiality and unforgeability are two essential security requirements of our scheme and are formalized as follows.

1) CONFIDENTIALITY

Confidentiality property assures that the meter and the aggregated data have been protected and can only be accessed by authorized parties. An experiment is used to prove the property under chosen plaintext attacks.

- ***Setup***: $\mathcal{C}$ generates the system parameters and sends them to $\mathcal{A}$.
- ***Queries***: $\mathcal{A}$ generates several Oracle queries to $\mathcal{C}$ and $\mathcal{C}$ then returns the corresponding information.
- ***Challenge***: $\mathcal{A}$ submits two messages m_0 and m_1 with the same length to $\mathcal{C}$, and $\mathcal{C}$ randomly chooses a bit $b \in \{0, 1\}$, computes the ciphertext c_b of the challenge message m_b, and sends c_b to $\mathcal{A}$.
- ***Guess***: $\mathcal{A}$ outputs a bit $b' \in \{0, 1\}$ and wins the experiment if $b' = b$. The advantage of $\mathcal{A}$ is $ADV_{\mathcal{A}}^{IND-CPA} = |P(b' = b)\text{-}1/2|$.

Definition 1: The proposed scheme is secure against indistinguishability under the chosen plaintext attacks (IND-CPA) if there is no probabilistic polynomial time adversary $\mathcal{A}$ with a non-negligible advantage.

2) UNFORGEABILITY

Unforgeability is a property required to guarantee that the signature is secure against an adaptive chosen plaintext attack. The following is an experiment used to prove the property under message attacks.

- ***Setup*: $\mathcal{C}$** generates the system parameters and sends them to $\mathcal{A}$.
- ***Queries*: $\mathcal{A}$** generates several Oracle queries to $\mathcal{C}$, and $\mathcal{C}$ then returns the corresponding information. The following queries are allowed:
  - **Key Generation queries**: $\mathcal{A}$ sends d_A to $\mathcal{C}$, and then $\mathcal{C}$ executes a key generation algorithm and returns the key Q_A to $\mathcal{A}$.
  - **Encryption queries**: $\mathcal{A}$ sends (m, Q_C) to $\mathcal{C}$, and then $\mathcal{C}$ executes an encryption algorithm and returns the ciphertext (C_1, C_2) to $\mathcal{A}$.
  - **Signature queries**: $\mathcal{A}$ sends (C_1, C_2) to $\mathcal{C}$, and then $\mathcal{C}$ executes a signature algorithm and returns (r, s) to $\mathcal{A}$.
  - **Verification queries**: $\mathcal{A}$ sends (r, s) to $\mathcal{C}$, and then $\mathcal{C}$ executes a verification algorithm to check if the result accepts or rejects to $\mathcal{A}$.
- ***Forgery***: $\mathcal{A}$ can forge a signature (r^*, s^*) of message m^*, and we can say that $\mathcal{A}$ wins the experiment if the two conditions hold: (1) (r^*, s^*) is valid; (2) $\mathcal{A}$ never makes signature queries with m^*.

Definition 2: The scheme is secure against existential unforgeability under the chosen messages attacks (EUF-CMA) if there is no probabilistic polynomial time adversary $\mathcal{A}$ with a non-negligible advantage.

Definition 3: Elliptic Curve Discrete Logarithm problem (ECDLP): Given two points G and Q in elliptic curve E, where $Q = kG$. The number k is the discrete logarithm of Q to the base point G. It is difficult to compute k from G and Q.

Definition 4: Elliptic Curve Decisional Diffie–Hellman problem (ECDDHP): Given a point G in the elliptic curve E, and three points aG, bG, and cG. The problem is to determine whether $abG = cG$.

C. PROPOSED BACDA SCHEME

The proposed BACDA scheme consists of five phases: setup, key generation, data conservation, aggregation, and data restoration. Their details are described as follows.

1) STEUP PHASE

Given that E is an elliptic curve defined by an equation and default field, we can determine the multiplicative order n of the base point G on the curve. furthermore, we are provided with the hash function H:{0, 1}$^* \rightarrow Fn$. Assuming that all the smart meters involved have registered with the control center CC and become certificated devices.

2) KEY GENERATION PHASE

Using elliptic curve cryptography, every smart meter SM_i select a random number d_i as a private key and computes $Q_i = d_i G$ as the corresponding public key. similarly, the aggregator agg randomly chooses d_{Agg} as the private key and computes $Q_{Agg} = D_{Agg} G$ as its corresponding public key. The control center CC also randomly selects d_C as the private key and calculate $Q_C = d_c G$ as its corresponding public key. subsequently, CC randomly chooses a secure number k and broadcasts a transaction with k to the blockchain, representing process 1 in the system model.

3) DATA CONSERVATION PHASE

The data conservation process aligns with processes 2 to 4 of the system model (Figure 2). During this phase, SM_i collects the power consumption data M_i from equipment and then performs the following encryption and signing steps:

Step 1: Choose a random value k_i.

Step 2: Compute ciphertext $C_i = (C_{1_i}, C_{2_i})$ as

$$C_{1_i} = k_i G, \tag{1}$$

and

$$C_{2_i} = P_{M_i} + k_i Q_c, \tag{2}$$

where P_{M_i} is a point on the elliptic curve mapped from M_i.

Step 3: Generate the signature (r, s_i) of the transaction data by computing

$$(x, y) = kG, \tag{3}$$
$$e_i = H(C_{1_i}, C_{2_i}, Eth(field)), \tag{4}$$
$$r = x \bmod n, \text{ and} \tag{5}$$
$$s_i = k^{-1}(e_i + d_i r), \tag{6}$$

where k is obtained from the blockchain and $Eth(field)$ denotes the transaction field except for "r", "s" and "*input*".

Step 4: Build and broadcast the transaction $Tx_i = (Eth\,(field)\,, C_{1_i}, C_{2_i}, r, s_i)$ to the blockchain, where ciphertexts C_{1_i} and C_{2_i} are put in the field "*input*".

4) AGGREGATION PHASE

This phase corresponds to processes 5-7 in the system model. The aggregator Agg periodically extracts n transactions from the blockchain. Based on the property that transactions have been verified by blockchain miners, Agg does not need to perform verification again while handling the following procedures.

a: AGGREGATION PROCESS

Agg aggregates each ciphertext (C_{1_i}, C_{2_i}) and signature (r, s_i) into (C_1, C_2) and (r, S) by computing $C_1 = \sum_{i=1}^{n} C_{1_i}$, $C_2 = \sum_{i=1}^{n} C_{2_i}$, and $S = \sum_{i=1}^{n} s_i$, respectively. in addition, all hash values of E_I are aggregated into e by computing E= $\sum_{i=1}^{n} e_i$.

b: PUBLIC KEY EXTRACTION

Based on the elliptic curve, Agg finds two points R and R' which have the same value r as the x-coordinate. then, the public key is extracted from the signature (r, s_i) placed in the transaction TX_i by computing

$$Q_i = r^{-1}\,(s_i R - e_i G) \bmod n, \tag{7}$$

and

$$Q'_i = r^{-1}\,(s_i R' - e_i G) \bmod n. \tag{8}$$

Then, the parameter "v", included in the Ethereum block structure (Figure 1), is employed here to determine which one is the proper point and then obtains the corresponding public key from either Q_i or Q'_i.

c: PUBLIC KEY AGGREGATION

All SM_i's public keys Q_i (OR Q'_i) are aggregated into Q by computing $Q = \sum_{i=1}^{n} Q_i$ OR $Q = \sum_{i=1}^{n} Q'_i$.

Then, the aggregator Agg broadcasts the transaction $T_{x_{Agg}}$ with the input field including (C_1, C_2, r, S, e, Q) to the blockchain.

5) DATA RESTORATION PHASE

This phase corresponds to processes 8, 9, and 1 in the system model. Upon receiving transaction $T_{x_{Agg}}$, control center CC does not need to perform verification due to the blockchain property. Then, CC handles the following procedure to restore the secret data (C_1, C_2, r, S, e, Q) from $T_{x_{Agg}}$:

Step 1: Compute

$$u_1 = S^{-1} e, \tag{9}$$
$$u_2 = r S^{-1}, \text{ and} \tag{10}$$
$$X = u_1 G + u_2 Q. \tag{11}$$

Step 2: Check whether the value of the x-coordinate of X equals r. if it holds, the aggregated signature is valid; otherwise, the data restoration phase terminates.

Step 3: Decrypt the aggregated ciphertext by CC's private key d_c as

$$\sum\nolimits_{i=1}^{n} P_{M_i} = d_c C_2 - C_1. \tag{12}$$

Step 4: Map the point $\sum_{i=1}^{n} P_{M_i}$ to its corresponding aggregated plaintext $\sum_{i=1}^{n} M_i$.

Step 5: Choose a new secure number k' and broadcast it to replace the original k.

IV. SECURITY ANALYSIS

In this section, security concerns, including confidentiality and unforgeability, are analyzed based on the well-known computational difficulty problem from an elliptic curve.

Theorem 1: the proposed scheme is secure against IND-CPA if the Decisional Diffie–Hellman (DDH) problem is hard.

Proof. Assume a polynomial-time adversary $\mathcal{A}$ wins the experiment in **Definition 1** with a non-negligible advantage ϵ, and there is an algorithm that can break the DDH problem under the chosen plaintext attack. Given an instance (G, k G, d_c G, Z) of the DDH problem, determine whether $Z = k\ d_c\ G$, where $G, kG, d_cG, kd_cG \in G$ and $k, d_c \in Z_q^*$ are unknown for challenger $\mathcal{C}$. Let the recipient's public key be $Q_c = d_c G$. The following is described to show that if $\mathcal{A}$ can break the proposed scheme based on that algorithm, the DDH problem can be solved by $\mathcal{C}$.

- ***Setup*** $\mathcal{A}$ transmits parameters $(E, F_q, q, G, n, P, F_n^*)$ to $\mathcal{A}$.
- ***Queries*****:** After $\mathcal{A}$ makes a series of encryption queries m_i, $\mathcal{A}$ randomly selects k_i, encrypts m_i, and sends the ciphertext (C_{1_i}, C_{2_i}) to $\mathcal{A}$.
- ***Challenge***: Assume that $\mathcal{A}$ is capable of recognizing ciphertext after queries. $\mathcal{A}$ randomly picks two messages m_0 and m_1 with the same length and sends them to $\mathcal{C}$. Then, $\mathcal{C}$ chooses a random bit $b \in \{0,1\}$, encrypts it with Z, and sends the ciphertext (C_{1_b}, C_{2_b}) to $\mathcal{A}$.
- ***Guess***: Upon receiving (C_{1_b}, C_{2_b}), $\mathcal{A}$ outputs its guess b' to $\mathcal{C}$. If $b' = b$, $\mathcal{A}$ successes, otherwise, $\mathcal{A}$ fails. As a result, the success probability of solving the DDH problem is determined as:

$$
\begin{aligned}
&Pr[\mathcal{C}\text{succeeds}] \\
&= \frac{1}{2} Pr[\mathcal{A}\ \text{succeeds}|(kG, d_cG, Z), \text{where } Z \text{ satisfies } kd_cG] \\
&\quad + \frac{1}{2} Pr\ [\mathcal{A}\ \text{succeeds}|Z\text{is a random element of } G] \\
&= \frac{1}{2}(\frac{1}{2} + \epsilon) + \frac{1}{2}\frac{1}{2} \\
&= \frac{1}{2} + \frac{1}{2}\epsilon.
\end{aligned}
$$

The portability of solving the DDP problem is $Adv_c = Pr[\text{C } succeeds] - \frac{1}{2} = \frac{1}{2}\epsilon$, where the advantage ϵ cannot be ignored. It contradicts the hardness assumption of the DDH problem. Therefore, the hypothesis does not hold, which infers that the proposed scheme is secure against indistinguishability under the chosen-plaintext attack (IND-CPA).

Theorem 2: The proposed scheme is secure against EUF-CMA if the discrete logarithm (DL) problem is secure against the adaptively chosen message attack.

Proof. Assume a polynomial-time adversary $\mathcal{A}$ wins the experiment in **Definition 2** with a non-negligible advantage. There is an algorithm that solves the DL problem under a chosen message attack. Given an instance (G, Q) of the DL problem, where $G, Q \in Z_q^*$, the goal of $\mathcal{A}$ is to find $x \in Z_q^*$, such that $Q = xG$.

- ***Setup***: $\mathcal{C}$ transmits parameters $(E, F_q, q, G, n, P, F_n^*)$ to $\mathcal{A}$.
- ***Queries*****:** $\mathcal{A}$ is assumed to make a series of Oracle queries to $\mathcal{C}$, and $\mathcal{C}$ sends the corresponding information to $\mathcal{A}$. The following queries are allowed in this experiment:
  - **Key Generation queries**: When receiving this query, $\mathcal{C}$ checks whether the tuple (d_i, Q_i) exists in the table L_k which is kept by $\mathcal{C}$. If so, $\mathcal{C}$ returns Q_i to $\mathcal{A}$; otherwise, $\mathcal{C}$ generates Q_i, appends (d_i, Q_i) into L_K, and returns Q_i to $\mathcal{A}$.
  - **Encryption queries**: When receiving this query, $\mathcal{C}$ checks whether the tuple $(m_i, Q_i, C_{1_i}, C_{2_i})$ exists in the table L_E which is kept by $\mathcal{C}$. If so, $\mathcal{C}$ returns (C_{1_i}, C_{2_i}) to $\mathcal{A}$; otherwise, $\mathcal{C}$ generates (C_{1_i}, C_{2_i}), appends $(m_i, Q_i, C_{1_i}, C_{2_i})$ into L_E, and returns (C_{1_i}, C_{2_i}) to $\mathcal{A}$.
  - **Signature queries**: When receiving this query, $\mathcal{C}$ checks whether the tuple $(r_i, s_i, C_{1_i}, C_{2_i})$ exists in the table L_S which is kept by $\mathcal{C}$. If so, $\mathcal{C}$ returns (r_i, s_i) to $\mathcal{A}$; otherwise, $\mathcal{C}$ generates (r_i, s_i), appends $(r_i, s_i, C_{1_i}, C_{2_i})$ into L_S, and returns (r_i, s_i) to $\mathcal{A}$.
  - **Verification queries**: When receiving this query, $\mathcal{C}$ checks whether the tuple $(r_i, s_i, C_{1_i}, C_{2_i}, true/reject)$ exists in table L_V which is kept by $\mathcal{C}$. If so, $\mathcal{C}$ returns *true/reject* to $\mathcal{A}$; otherwise, $\mathcal{A}$ generates *true/reject*, appends $(r_i, s_i, C_{1_i}, C_{2_i}, true/reject)$ into L_V and returns *true/reject* to $\mathcal{A}$.
- ***Forgery***: $\mathcal{A}$ forges a signature (r^*, s^*) of the ciphertext (C_1^*, C_2^*) and $\mathcal{C}$ gets the solution of the DL problem instance G and Q where $Q = xG$. To calculate the advantage of $\mathcal{C}$, two events are defined: (1) E_1: $\mathcal{C}$ is not terminated when performing a query. (2) E_2: $\mathcal{A}$ outputs a valid signature. Thus, we have $\mathbf{Pr}[E_1] \geq \left(1 - \frac{1}{q_H}\right)^{q_H}$, and $\Pr[E_2 \mid E_1 \geq \epsilon$, where q_H is a signature query. The advantage of solving the DL problem is $\mathbf{Pr}[E_1 \bigwedge E_2] \geq \mathbf{Pr}[E_2 \Pr[E_1] \epsilon \left(1 - \frac{1}{q_H}\right)^{q_H}$, where the advantage ϵ cannot be ignored based on the above assumption.

The DL problem is solved with the probability $\mathbf{Pr}[E_1 \bigwedge E_2] = \epsilon \left(1 - \frac{1}{q_H}\right)^{q_H}$. However, it contradicts the hardness assumption that the DL problem cannot be solved in practice. Our hypothesis thus does not hold, which infers that the proposed scheme is secure against existential unforgeability under the chosen-message attack (EUF-CMA).

V. DISCUSSION

This section aims to demonstrate the contributions of this research by discussing and comparing the functionality features provided in the proposed scheme with those in the related work. Moreover, a performance analysis is conducted to evaluate the computational cost for all crucial participants in the system, including the smart meter, aggregator, and control center. The following comparison of computational costs highlights the efficiency of our scheme.

A. FUNCTIONALITY FEATURES

1) CRYPTOGRAPHIC ALGORITHMS ISSUE

The performance of cryptographic algorithms employed for a smart grid is crucial due to the resource-restricted property of a metering device. Elliptic curve cryptography has been proven as efficient in performance with a smaller key size [35], [36] For example, ECDSA achieves a similar security level to that of RSA (with a 3072-bits key size), but the key size of ECDSA is 256-bits [35], [36]. Accordingly, the computational effort can be reduced if the key size is smaller. In the proposed scheme, ECC encryption/decryption and ECDSA are used to protect the consumption data collected from smart meters SM_i. Moreover, a comparison of computational costs among related work and our proposal is detailed in the next chapter.

2) FULLY DECENTRALIZED ARCHITECTURE

Blockchain architecture is key to implementing full decentralization. The critical components executed throughout the whole scheme depend on blockchain technology. ECC-based cryptographic mechanisms, such as encryption and signature, involved in the scheme are one of the fundamental elements of a blockchain. The field of transaction TX_i is used to store the essential data of our design including ciphertext (C_{1_i}, C_{2_i}), and produced signature (r, s_i) in the data conservation phase. Depending on the peer-to-peer connection of blockchain clients, the validity of TX_i with the appended ciphertext (C_{1_i}, C_{2_i}) and signature (r, s_i) can be confirmed. Therefore, the proposed scheme no long requires TTP, KGC, or PKI, and as such, our scheme can prevent possible malicious intrusions into a centralized system, avoid the cost of system maintenance, and accomplish zero downtime for smart grid services.

3) SCALABILITY

The proposed scheme is scalable. The management of smart meters is based on the independent nature of each transaction without breaking the smart grid service. In the design, registered smart meters can be easily added by regenerating a public/private key pair in the phase of key generation. The newer round of TX_i from a different meter can be decrypted by using CC's private key, and the aggregated signature can be verified by presenting the public key extracted from the signature (r, s_i) placed in the transaction TX_i. Similarly, the replacement of a smart meter can be handled by removing an old meter and then adding a new one into the smart grid system.

4) AGGREGATIONAL EFFECTIVENESS

The proposed scheme involves data and signature aggregation aspects to guarantee the integrity of the aggregation result. That is, in the phase of data restoration, the parameters kept in the transaction $T_{x_{Agg}}$ can be ascertained as long as the aggregated signature is valid. It is ascertained only when the parameter X computed in $Eq.$ (11) is the same as the signature

TABLE 2. The comparison of functionality features.

Functionality Features / Scheme	F1	F2	F3	F4	F5
Fan et al. [13]	Bilinear pairing, RSA	N	N	N	N
He et al. [14]	Boheh-Goh-Nissim [37]	N	N	N	N
Vahedi et al. [15]	ElGamal, BLS short signature [38]	N	N	N	N
Chen et al. [16]	Elliptic curve based	N	Y	N	Y
Zhang et al. [17]	Paillier, BLS short signature	N	Y	Y	N
Zuo et al. [21]	ElGamal	N	N	Y	N
Fan et al. [25]	Paillier, BLS short signature	N	N	N	N
Li et al. [26]	Bilinear pairing, Identity-based proxy re-encryption	N	N	Y	N
Ours	ECC encryption, ECDSA	Y	Y	Y	Y

F1: Applied cryptographic algorithms F2: Fully decentralized architecture
F3: Scalability F4: Aggregational Effectiveness
F5: One-time key pair and signature
Y: Covers the property
N: Does not cover the property

TABLE 3. Notations of operation.

Symbol	Description
t_m	Execution time of scalar multiplication in F_n^*
T_P	Execution time of bilinear pairing operation
T_E	Execution time of exponentiation operation
T_M	Execution time of elliptic curve scalar point multiplication operation
T_A	Execution time of elliptic curve scalar point addition operation

(x, y) generated in $Eq.$ (3) in the phase of data conservation. To show the aggregated effectiveness, the correctness of the aggregated signature is demonstrated as follows.

$$
\begin{aligned}
X &= u_1 G + u_2 Q \\
&= S^{-1} eG + rS^{-1} \sum_{i=1}^{n} Q_i \\
&= S^{-1} eG + rS^{-1} \sum_{i=1}^{n} d_i G \\
&= (\sum_{i=1}^{n} s_i)^{-1} \sum_{i=1}^{n} e_i G + r(\sum_{i=1}^{n} s_i)^{-1} \sum_{i=1}^{n} d_i G \\
&= G(\sum_{i=1}^{n} s_i)^{-1} (\sum_{i=1}^{n} e_i + r \sum_{i=1}^{n} d_i) \\
&= G(k^{-1}(\sum_{i=1}^{n} e_i + r \sum_{i=1}^{n} d_i)^{-1} (\sum_{i=1}^{n} e_i + r \sum_{i=1}^{n} d_i) \\
&= G(k^{-1})^{-1} (\sum_{i=1}^{n} e_i + r \sum_{i=1}^{n} d_i)^{-1} (\sum_{i=1}^{n} e_i + r \sum_{i=1}^{n} d_i) \\
&= Gk = (x', y').
\end{aligned}
$$

TABLE 4. The comparison of computational cost.

Scheme	Smart Meter	Aggregator	Control Center	Total Execution Time
Vahedi et al. [15]	$n(4T_M+2T_A)$ $\approx (116.24n)\ t_m$	$(n+1)T_P+(2n+1)T_A+2T_M$ $\approx (87.24n+145.12)\ t_m$	$2T_P+T_M+T_A$ $\approx 203.12\ t_m$	$\approx (203.48n+348.24)\ t_m$
Chen et al. [16]	$n(T_P+T_E+2T_M+2t_m)$ $\approx (168n)\ t_m$	$2T_P+T_M+t_m$ $\approx 204\ t_m$	$3T_P+nT_E+T_M$ $\approx (21n+290)\ t_m$	$\approx (189n+494)\ t_m$
Zhang et al. [17]	$n(10T_M+4t_m)$ $\approx (294n)\ t_m$	$9T_P+T_E$ $\approx 804\ t_m$	$T_P+8T_E+2t_m$ $\approx 257\ t_m$	$\approx (294n+1061)\ t_m$
Zuo et al. [21]	$n(2T_P+7T_E+2t_m)$ $\approx (323n)\ t_m$	$3n\ t_m+(n+1)T_P+T_E$ $\approx (90n+108)\ t_m$	$2T_P+(n+1)t_m+T_E$ $\approx (1n+196)\ t_m$	$\approx (414n+304)\ t_m$
Fan et al. [25]	$n(2T_E+2t_m)$ $\approx (44n)\ t_m$	$2nT_P+2T_E+(n+1)t_m$ $\approx (175n+43)\ t_m$	$2T_P$ $\approx (174n)t_m$	$\approx (219n+217)\ t_m$
Li et al. [26]	$n(T_P+5T_E+2t_m)$ $\approx (194n)\ t_m$	$(2n+1)T_P+(2n+3)T_E+(4n+1)t_m$ $\approx (220n+151)\ t_m$	$3T_P+T_E+t_m$ $\approx 283\ t_m$	$\approx (414n+434)\ t_m$
Ours	$n(3T_M+T_A+2t_m)$ $\approx (89.12n)\ t_m$	$n(T_M+4T_A)+T_M+2t_m$ $\approx (87.48n+31)\ t_m$	$3T_M+2T_A+2t_m$ $\approx 89.24\ t_m$	$\approx (176.6n+120.24)\ t_m$

5) ONE-TIME KEY PAIR AND SIGNATURE

The proposed scheme constructs a one-time key pair method. In the phase of key generation, the public key of all participants including each smart meter SM_i, aggregator Agg, and control center CC, are computed by themselves using the private key derived from a random number. Each registered smart meter has its key pair (d_i, Q_i) and is granted authorization for accessing the blockchain. Once a new transaction is produced or a short period passes, the key pair of SM_i is different, which follows the one-time key concern [28].

Furthermore, a secure number k is developed and involved in s_i to guarantee a one-time signature in *Eq.* (6). When CC broadcasts a new transaction or a specific short period passes, the secure number k will be updated to another new one. Hence, the freshness of aggregated signature (r, S) can be confirmed since only the signature aggregated by the signature (r, s_i) with knowledge of a valid k can result in the validity of X computed by *Eq.* (11), so the one-time signature objective can be achieved.

Table 2 summarizes a comparison between related work and our scheme in terms of functionality features.

B. PERFORMANCE ANALYSIS

In this section, performance is presented by comparing the computational cost among relevant works and our proposal.

Table 3 presents several crucial time-consuming cryptographic operations derived from the referenced approaches [39], [40]. The time costs associated with these operations can be approximated as follows: $T_P \approx 87t_m$, $T_E \approx 21t_m$, $T_M \approx 29t_m$, $T_A \approx 0.12t_m$, where t_m represents the computational cost required for a modular multiplication operation. On the other hand, certain negligible operations such as hash functions and scalar additions have been excluded from the discussion as they have minimal impact on the overall computational performance.

The comparison of computational cost is presented in Table 4. In order to assess the computational load of each entity, including the smart meter, aggregator, and control center, the operational count and its corresponding approximate execution time are summarized. In [17], the edge server, denoted as ES, is utilized to handle the majority of tasks performed by the aggregator. Therefore, it can be considered as an evaluation of the aggregator's capabilities. Additionally, the total execution time is calculated and provided in the table, with n denoting the number of smart meters.

In terms of individual entities, our proposal for the smart meter requires $n(3T_M + T_A+2t_m)$ operations, approximately equivalent to $(89.12n)t_m$. This computational requirement exceeds most of the relevant works, except for Fan et al. [25], which necessitates $n(2T_E+2t_m)$ operations, translating to $(44n)t_m$ of execution time. Significantly, our scheme reduces

the needs on handling the linear time generated from the smart meter count in both the aggregator and control center, effectively mitigating computational bottlenecks.

Considering the overall execution time, our proposed scheme demonstrates high efficiency. With an approximate total execution time of $(176.6n + 120.24)t_m$, it shows better result among all relevant approaches in terms of both linear time (dependent on the smart meter count) and constant time.

VI. CONCLUSION

This paper proposed a blockchain–enabled authenticated and conserved data aggregation scheme (BACDA) to provide security and privacy in a smart grid. The proposed BACDA scheme fully integrates ECC-based cryptography and blockchain technology to improve comprehensive performance and eliminate issues associated with a centralized system. Based on the well-known computational difficulty problem from an elliptic curve, two essential security concerns including confidentiality and unforgeability are discussed in this research. Moreover, the functionalities necessary to establish a secure smart grid were developed, such as scalability, aggregational effectiveness, and one-time key pair and signature. Compared to related work, the contribution of our proposed scheme is highlighted in terms of functionality features and efficiency.

Our future work aims to the improvement of key management for the BACDA scheme. In the BACDA scheme, various cryptographic primitives are employed, and all of them need to complement each other to accomplish the protection. For such a streamlined work, it is necessary to integrate the interoperations, and a variety of cryptographic keys are essential throughout all those technologies. Undoubtedly, an elaborative key management solution covering all participants' key pairs and aggregated public keys is critical to guarantee the protection provided by the cryptographic mechanisms. It can also advance security level while satisfying the practical requirements.

REFERENCES

[1] N. Suhaimy, N. A. M. Radzi, W. S. H. M. W. Ahmad, K. H. M. Azmi, and M. A. Hannan, "Current and future communication solutions for smart grids: A review," *IEEE Access*, vol. 10, pp. 43639–43668, 2022.

[2] C. Alaton and F. Tounquet. (2020). *Benchmarking Smart Metering Deployment in the EU-28: Final Report, Publications Office*. European Commission, Directorate-General for Energy. [Online]. Available: https://data.europa.eu/doi/10.2833/492070

[3] S. Sultan, "Privacy-preserving metering in smart grid for billing, operational metering, and incentive-based schemes: A survey," *Comput. Secur.*, vol. 84, pp. 148–165, Jul. 2019.

[4] Z. Liu, C. Zhang, M. Dong, B. Gu, Y. Ji, and Y. Tanaka, "Markov-decision-process-assisted consumer scheduling in a networked smart grid," *IEEE Access*, vol. 5, pp. 2448–2458, 2017.

[5] B. Li, R. Lu, K.-K. R. Choo, W. Wang, and S. Luo, "On reliability analysis of smart grids under topology attacks: A stochastic Petri net approach," *ACM Trans. Cyber Phys. Syst.*, vol. 3, no. 1, p. 10, Aug. 2018.

[6] B. Li, R. Lu, W. Wang, and K.-K.-R. Choo, "Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system," *J. Parallel Distrib. Comput.*, vol. 103, pp. 32–41, May 2017.

[7] G. De La Torre Parra, P. Rad, and K.-K.-R. Choo, "Implementation of deep packet inspection in smart grids and industrial Internet of Things: Challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 135, pp. 32–46, Jun. 2019.

[8] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," *Int. J. Electr. Power Energy Syst.*, vol. 99, pp. 45–56, Jul. 2018.

[9] S. Ge, P. Zeng, R. Lu, and K.-K.-R. Choo, "FGDA: Fine-grained data analysis in privacy-preserving smart grid communications," *Peer-Peer Netw. Appl.*, vol. 11, no. 5, pp. 966–978, Sep. 2018.

[10] H. Shen, Y. Liu, Z. Xia, and M. Zhang, "An efficient aggregation scheme resisting on malicious data mining attacks for smart grid," *Inf. Sci.*, vol. 526, pp. 289–300, Jul. 2020.

[11] G. Wood and M. Newborough, "Dynamic energy-consumption indicators for domestic appliances: Environment, behaviour and design," *Energy Buildings*, vol. 35, no. 8, pp. 821–841, Sep. 2003.

[12] E. L. Quinn, "Privacy and the new energy infrastructure," Center Energy Environ. Secur. (CEES), Univ. Colorado, CO, USA, Tech. Rep. 09-001, Feb. 2009. [Online]. Available: http://ssrn.com/abstract=1370731.

[13] C.-I. Fan, S.-Y. Huang, and Y.-L. Lai, "Privacy-enhanced data aggregation scheme against internal attackers in smart grid," *IEEE Trans. Ind. Informat.*, vol. 10, no. 1, pp. 666–675, Feb. 2014.

[14] D. He, N. Kumar, S. Zeadally, A. Vinel, and L. T. Yang, "Efficient and privacy-preserving data aggregation scheme for smart grid against internal adversaries," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2411–2419, Sep. 2017.

[15] E. Vahedi, M. Bayat, M. R. Pakravan, and M. R. Aref, "A secure ECC-based privacy preserving data aggregation scheme for smart grids," *Comput. Netw.*, vol. 129, pp. 28–36, Dec. 2017.

[16] Y. Chen, J.-F. Martínez-Ortega, P. Castillejo, and L. López, "An elliptic curve-based scalable data aggregation scheme for smart grid," *IEEE Syst. J.*, vol. 14, no. 2, pp. 2066–2077, Jun. 2020.

[17] J. Zhang, Y. Zhao, J. Wu, and B. Chen, "LVPDA: A lightweight and verifiable privacy-preserving data aggregation scheme for edge-enabled IoT," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4016–4027, May 2020.

[18] M. Akgün, E. U. Soykan, and G. Soykan, "A privacy-preserving scheme for smart grid using trusted execution environment," *IEEE Access*, vol. 11, pp. 9182–9196, 2023, doi: 10.1109/ACCESS.2023.3237643.

[19] S. S. Al-Riyami and K. G. Paterson, "Certifiateless public key cryptography," in *Asiacrypt*, vol. 2894. New York, NY, USA: Springer, 2003, pp. 452–473.

[20] B. Wang, L. Liu, S. Zhang, and J. Huang, "Research on privacy protection scheme based on certificateless aggregation signcryption in AMI," *Internet Things (IoT) Eng. Appl.*, vol. 4, no. 1, pp. 7–12, 2019.

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

[22] S. Nakamoto. (2008). *BitCoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[23] V. Buterin. (2013). *Ethereum White Paper*. [Online]. Available: https://ethereum.org/en/whitepaper/

[24] C. Cachin, "Architecture of the hyperledger blockchain fabric," in *Proc. Workshop Distrib. Cryptocurrencies Consensus Ledgers*, 2016, vol. 310, no. 4, pp. 1–6.

[25] H. Fan, Y. Liu, and Z. Zeng, "Decentralized privacy-preserving data aggregation scheme for smart grid based on blockchain," *Sensors*, vol. 20, no. 18, p. 5282, 2020.

[26] K. Li, Y. Yang, S. Wang, R. Shi, and J. Li, "A lightweight privacy-preserving and sharing scheme with dual-blockchain for intelligent pricing system of smart grid," *Comput. Secur.*, vol. 103, Apr. 2021, Art. no. 102189.

[27] S. Ma, H. Zhang, and X. Xing, "Scalability for smart infrastructure system in smart grid: A survey," *Wireless Pers. Commun.*, vol. 99, pp. 161–184, Jan. 2018.

[28] W. van der Linde, P. Schwabe, A. Hülsing, Y. Yarom, and L. Batina, "Post-quantum blockchain using one-time signature chains," Radboud Univ., Nijmegen, The Netherlands, Tech. Rep., 2018.

[29] C. F. Kerry and P. D. Gallagher, "Digital signature standard (DSS)," in *Proc. FIPS*, 2013, pp. 186–192.

[30] *Advanced Encryption Standard*, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2001.

[31] R. Rivest, A. Shamir, and L. Adleman, "Cryptographic communications system and method," U.S. Patent 4 405 829, Sep. 20, 1983.

[32] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. Int. Conf. Appl. Cryptograph. Techn.* Cham, Switzerland: Springer, 1999, pp. 1–12.

[33] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.
[34] C. Gentry, *A Fully Homomorphic Encryption Scheme*. Stanford, CA, USA: Stanford Univ., 2009.
[35] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 6th ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2013.
[36] M. Al-Zubaidie, Z. Zhang, and J. Zhang, "Efficient and secure ECDSA algorithm and its applications: A survey," *Int. J. Commun. Netw. Inf. Secur.*, vol. 11, no. 1, pp. 7–35, Apr. 2022.
[37] D. Boneh, E.-J. Goh, and K. Nissim, "Evaluating 2-DNF formulas on ciphertexts," in *Proc. Theory Cryptogr. Conf.* Berlin, Germany: Springer, 2005, pp. 325–341.
[38] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," in *Proc. 7th Int. Conf. Appl. Cryptol. Inf. Secur.*, 2001, pp. 514–532.
[39] A. Karati, S. H. Islam, G. P. Biswas, M. Z. A. Bhuiyan, P. Vijayakumar, and M. Karuppiah, "Provably secure identity-based signcryption scheme for crowdsourced industrial Internet of Things environments," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2904–2914, Aug. 2018.
[40] A. Karati, S. Hafizul Islam, and G. P. Biswas, "A pairing-free and provably secure certificateless signature scheme," *Inf. Sci.*, vol. 450, pp. 378–391, Jun. 2018.

CHIEN-DING LEE received the B.S. degree from the Department of Information Management, Chaoyang University of Technology, Taichung, Taiwan, in 2000, and the M.S. and Ph.D. degrees from the Department of Information Engineering and Computer Science, Feng Chia University, Taichung, in 2005 and 2014, respectively. He has been with the Department of Management and Information, National Open University, New Taipei, Taiwan, since 2020, where he is currently an Associate Professor. His current research interests include cryptography, blockchain technology, software development, and smart healthcare. He is an honorary member of the Phi Tau Phi Scholastic Honor Society.

JHIH-HONG LI received the M.S. degree from the Department of Computer Science and Information Engineering, National Chiayi University, in 2021. His current research interests include blockchain techniques and cryptography.

TZUNG-HER CHEN was born in Tainan, Taiwan, China, in 1967. He received the B.S. degree from the Department of Information and Computer Education, National Taiwan Normal University, in 1991, the M.S. degree from the Department of Information Engineering, Feng Chia University, in 2001, and the Ph.D. degree from the Department of Computer Science, National Chung Hsing University, in 2005. He has been a Professor with the Department of Computer Science and Information Engineering, National Chiayi University, since August 2011. His current research interests include information hiding, multimedia security, digital rights management, and blockchain technology. He is an honorary member of the Phi Tau Phi Scholastic Honor Society.