*mathematics*

MDPI

*Article*

# An Efficient Lightweight Authentication Scheme for Smart Meter

**Jingqi Du [1], Chengjing Dai [2], Pinshang Mao [3], Wenlong Dong [4], Xiujun Wang [4] and Zhongwei Li [5,*]**

[1] Industrial Control Expansion Department, CLP Great Wall Internet System Application Co., Ltd., Beijing 100088, China; 13759598180@163.com
[2] Energy Planning Research Center, China Energy Engineering Group Yunnan Electric Power Design Institute Co., Ltd., Kunming 650051, China; dcj13988983323@163.com
[3] Marketing Center, NR Electric Co., Ltd., Nanjing 210000, China; maops@nrec.com
[4] College of Data Science and Technology, Heilongjiang University, Harbin 150080, China; 2232680@s.hlju.edu.cn (W.D.); 2232702@s.hlju.edu.cn (X.W.)
[5] School of Electrical Engineering and Automation, Harbin Institute of Technology, Harbin 150001, China
* Correspondence: lzw@hit.edu.cn

**Abstract:** With the rapid development of the information age, smart meters play an important role in the smart grid. However, there are more and more attacks on smart meters, which mainly focus on the identity authentication of smart meters and the security protection of electricity consumption data. In this paper, an efficient lightweight smart meter authentication scheme is proposed based on the Chinese Remainder Theorem (CRT), which can realize the revocation of a single smart meter user by publishing a secret random value bound to the smart meter identity. The proposed scheme not only protects the security of smart meter electricity consumption data by using encryption, but also resists identity attacks from both internal and external adversaries by using hash functions and timestamps. Experiment shows that the proposed scheme has lower computation overhead and communication overhead than other authentication schemes and is more suitable for smart meter authentication.

**Keywords:** smart meters; authentication; Chinese remainder theorem; collusion attack; revocation

**MSC:** 94A62



**Citation:** Du, J.; Dai, C.; Mao, P.; Dong, W.; Wang, X.; Li, Z. An Efficient Lightweight Authentication Scheme for Smart Meter. *Mathematics* **2024**, *12*, 1264. https://doi.org/10.3390/math12081264

Academic Editors: Arijit Karati and Chun-I Fan

Received: 25 March 2024
Revised: 14 April 2024
Accepted: 19 April 2024
Published: 22 April 2024



## 1. Introduction

With the rapid development of the information age, the smart grid has become more and more popular in our lives. The smart meter has an important application in smart grid. Power companies can plan production and allocation of power resources based on the data of smart meters, which is conducive to the efficient use of power resources and ensures the stable operation of the power grid. In the data transmission process between smart meters and power companies, there are frequent incidents of illegal users impersonating legal identities to steal electricity resources. Therefore, effective identity authentication for both parties is extremely important. Additionally, attackers may exploit users' personal habits and privacy to attack their electricity data, so the security protection of electricity usage data is also crucial. Current technologies for privacy protection in identity authentication mainly include HMAC [1], Zero-Knowledge Proofs [2], the Chinese Remainder Theorem (CRT) [3], Blind Signatures [4], Group Signatures [5], and Certificates [6]. Compared to other technologies, identity authentication schemes based on the CRT are relatively less demanding in terms of computation overhead, transmission consumption, and memory usage, making them more suitable for smart meter identity authentication. Compared to other technologies, identity authentication schemes constructed based on the CRT have relatively small computation overhead and communication overhead, making them more suitable for identity authentication of smart meters.

In 2016, Jiang et al. [7] proposed an efficient anonymous batch authentication scheme using HMAC, ensuring the security and confidentiality of Vehicular Ad hoc Networks

(VANETs). By using hash functions to check message integrity before batch processing, the scheme efficiently handled invalid request messages, making the batch authentication more effective. In 2019, Amine et al. [8] proposed a lightweight HMAC mutual authentication protocol specifically for IoT. Considering the resource constraints of IoT devices, this protocol, employing HMAC functions and XOR operations, ensures secure communication between IoT devices and fog nodes. This lightweight HMAC protocol addresses the challenge of secure communication on resource-limited devices, particularly against common network threats like replay and man-in-the-middle attacks. In 2017, Tian et al. [9] proposed a smart meter identity authentication scheme based on the CRT, which has low computational and memory requirements and allows dynamic user management through secret value updates. In 2019, Rasheed et al. [2] introduced a new, lightweight, adaptive group-based VANET zero-knowledge proof protocol. Using zero-knowledge proof technology, vehicles can prove their identity to base stations without revealing any sensitive information. In 2021, Dwivedi et al. [10] proposed a privacy-preserving identity authentication scheme using non-interactive zero-knowledge proofs, suitable for various IoT-based applications. For enhanced security, a password-authenticated key exchange protocol was used to create each session. Utilizing zero-knowledge proofs in this scheme ensures that if the statement is correct, the verifier cannot learn anything other than that the statement is true.

In 2019, Zhang et al. [11] designed a conditionally privacy-preserving authentication based on CRT. This scheme ensured communication security while also reducing the probability of personal information, including real identities, being leaked. Using the CRT significantly lowered the computational complexity for the trusted center. In 2020, Kong et al. [12] proposed an efficient and privacy-preserving solution suitable for resource-limited environments, especially in smart grids. Blind signature technology played an important role in this scheme which allows data to be authenticated and signed while maintaining user anonymity, enabling fine-grained analysis of consumption data without revealing user identities. In 2020, Jiang et al. [13] proposed a scheme named AAAS for anonymous authentication in VANETs. This scheme aimed to allow vehicles in VANETs to authenticate each other and communicate with roadside infrastructure while protecting the driver's privacy. The scheme combined alias mechanisms with group signature mechanisms to achieve a distributed solution, where no single authority could directly resolve the real identity of the vehicles. In 2021, Pathak et al. [14] proposed an identity verification scheme based on zero-knowledge proofs which can prove ownership of an identity to a verifier without revealing any sensitive information. In 2023, Zhu et al. [15] proposed a privacy-preserving data aggregation scheme based on the CRT and homomorphic encryption technology, effectively balancing communication and computation overhead. In this scheme, any entity can verify the integrity of data, effectively preventing data tampering, and abandoned bilinear and point-to-point hash functions, thus enhancing efficiency. In 2023, Sui et al. [4] employed blind signatures and anonymous authentication to propose a privacy protection scheme for smart grids. This scheme could not only track electricity thieves but also effectively protect the security of the electricity purchasing process using smart meters. In 2023, Lu et al. [16] constructed a new certificateless group signature scheme to achieve the vehicle identity hiding and secure communication between vehicles, thereby protecting the privacy of vehicle information.

In the smart meter authentication scheme proposed by Tian et al. [9], because each smart meter user has private $(X, n_i)$, and these smart meter users have the same $X$, and $n_1, \ldots, n_n$ are mutual coprime. Thus, when some users (assume $n_1, \ldots, n_n$) collude to attack the legal user identity, there is a high probability of guessing $n_j \in \{n_1, \ldots, n_n\}, j \neq 1, \ldots, k$. Therefore, they can take on user identity $n_j$ to forge electricity consumption data. In addition, since the region managers know the user's authentication information $(X, n_i)$, a dishonest region manager can take on user identity and forge electricity consumption information. Therefore, internal users of scheme [9] can carry out a collusion attack on identity, and the dishonest region managers can take on the smart meters identities and

tamper with power usage data. An efficient lightweight authentication scheme for a smart meter is proposed in this paper, which has the following specific contributions:

(1) In order to meet lightweight requirements, each smart meter has a hash value $H(n_i, a_i)$ and a random number $n_i$. According to the randomness, unidirectionality, and collision resistance of the hash function, even if multiple smart meter users conspire to know multiple $n_i$ and $H(n_i, a_i)$, they cannot guess the random number or hash values of other smart meters. Therefore, the scheme can resist collision attack by internal users on identity.

(2) Due to the fact that the user's random number $a_i$ is hidden in the hash function $h = H(a_i, P_{ow}, T^{'}_{s})$ during the electricity consumption data charging phase, RM cannot obtain the corresponding $a_i$ and therefore cannot calculate a valid hash value. Even if RM forges the bill, the OC can verify the authenticity of the electricity consumption data and detect false bills from RM through comparison of hash values. Therefore, the scheme can resist attacks from dishonest region managers who forge electricity consumption data.

(3) Because OC knows the secret random value $a_i$ corresponding to the user, when a smart meter is revoked, OC can disclose its $a_i$. Thus, during the authentication phase, RM can verify whether the corresponding hash values $H(n_i, a_i)$ are equal through $a_i$. If equal, reject user authentication, achieving authentication revocation for the user. Therefore, the scheme can efficiently achieve authentication revocation for a single user.

(4) Experiment shows that the proposed authentication scheme has lower communication and computation overhead compared to other schemes.

The remainder of this paper is organized as follows: Section 2 introduces preliminaries such as the CRT and elliptic curves. Section 3 describes the system model and threat model. Section 4 details the proposed authentication scheme for smart meter. Section 5 discusses the correctness and security of the scheme. Section 6 presents the performance analysis. Finally, Section 7 concludes the paper.

## 2. Preliminaries

This section mainly introduces CRT, elliptic curve, and ECDSA signature algorithms. CRT is used to assign shared secret values to smart meters, while elliptic curve and ECDSA signature algorithms are used to protect the security of transmitted data and verify the sender, respectively.

### 2.1. Chinese Remainder Theorem

If the numbers $m_1, m_2, \ldots, m_n$ are mutual prime, then for any numbers $a_1, a_2, \ldots, a_n$, the system of congruent equations $\begin{cases} x \equiv a_1 (\bmod m_1) \\ x \equiv a_2 (\bmod m_2) \\ \cdots \\ x \equiv a_n (\bmod m_n) \end{cases}$ has exactly one solution $x \equiv (\sum_{i=1}^{n} a_i t_i M_i) \bmod M$, where $M = \prod_{i=1}^{n} m_i$, $M_i = M/m_i$, $t_i = M_i^{-1}$ are the number-theoretic inverse element such that $M_i t_i \equiv 1 (\bmod m_i)$, $i \in \{1, 2, 3, \ldots, n\}$.

The method to construct the solution is described as follows: (1) The total modulus $M$ is calculated as the product of all moduli. (2) For each modulus $m_i$, $M_i = M/m_i$ is calculated. (3) The multiplicative inverse $t_i$ of $M_i$ is calculated such that $M_i t_i \equiv 1 (\bmod m_i)$. (4) The solution $x$ can be found as a weighted sum $x = \sum_{i=1}^{n} a_i M_i t_i$ modulo $M$.

An example to further illustrate this theorem involves solving a system of three equations: $\begin{cases} x \equiv 2 (\bmod 3) \\ x \equiv 3 (\bmod 4) \\ x \equiv 1 (\bmod 5) \end{cases}$. The following steps are performed: (1) Calculate $M = 3 \times 4 \times 5 = 60$. (2) For each modulus $m_i$ , calculate$M_i = \frac{M}{m_i}$, that is, $M_1 = \frac{M}{m_1} = \frac{60}{3} = 20$,

$M_2 = \frac{M}{m_2} = \frac{60}{4} = 15$, $M_3 = \frac{M}{m_3} = \frac{60}{5} = 12$. (3) Find the multiplicative inverses $t_i$ of $M_i$ such that $M_i t_i \equiv 1(\mathrm{mod}\, m_i)$, that is $20^{-1} \equiv 2(\mathrm{mod}3)$, $15^{-1} \equiv 3(\mathrm{mod}4)$, $12^{-1} \equiv 3(\mathrm{mod}5)$. (4) Calculate the solution $x = (a_1 M_1 t_1 + a_2 M_2 t_2 + a_3 M_3 t_3) \bmod M$ to get $x \equiv 11 \bmod 60$.

### *2.2. Elliptic Curves*

An elliptic curve over a finite field $\mathbb{F}_p$ of prime order $p$ is the Weierstrass equation $y^2 = x^3 + ax + b(\mathrm{mod}\, p)$, where $a, b \in \mathbb{F}_p$ and $(4a^3 + 27b^2) \bmod p \neq 0$, which ensures the absence of singular points. A group on the elliptic curve $E$ over $\mathbb{F}_p$, denoted as $\mathbb{G} = E_p(a, b)$, includes a generator $P$ of the group, the order $q$ of the group, and the infinity point $\mathcal{O}$.

The point addition and scalar multiplication operations on elliptic curve are defined as follows:

(1) Point addition: For points $R, W \in \mathbb{G}$ , if $P \neq W$ , then there exists $R \in \mathbb{G}$ such that $R = P + W$ . If $P = W$ , then $R = 2P$ . If $P + W = O$, then $P = -W$. Point addition is illustrated in Figure 1.The red solid line represents the elliptical curve, while the black dashed line represents the demonstration of the addition operation on the elliptical curve.

(2) Scalar multiplication: $mP = \underbrace{P + P + \ldots + P}_{m}$ , where $m \in \mathbb{Z}_q^*$.

Elliptic curve operations have the following properties. For any $P, Q, R \in \mathbb{G}$, there are (1) $P + Q = Q + P$. (2) $(P + Q) + R = P + (Q + R)$. (3) $P = P \oplus (\mathcal{O} \oplus \mathcal{O})$.

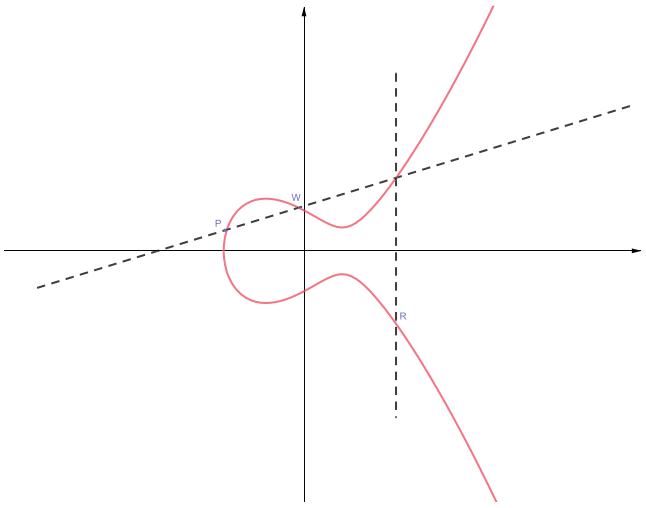


**Figure 1.** Addition operation in ECC.

### *2.3. ECDSA Signature Algorithm*

The ECDSA (Elliptic Curve Digital Signature Algorithm) [17] includes key generation, signing, and verification processes. The steps of the ECDSA signature algorithm are illustrated in Figure 2 and constructed as follows:

(1) Key generation. Let $\mathbb{F}_p$ be a finite field, $E$ be the elliptic curve on $GF(p)$. Choose Randomly $G \in E$. Let the order of $G$be prime $n$. Choose randomly $d \in [1, n-1]$, compute $Q$ such that $Q = dG$. Output the public key $pk = (n, Q)$ and private key $sk = d$.

(2) Signature. For the message to be signed, choose randomly $k \in [1, n-1]$, compute $kG = (x, y)$, $r \equiv x(\mathrm{mod}\, n)$, $s \equiv (e + rd)k^{-1}(\mathrm{mod}\, n)$. If $r = 0$ or $s = 0$, select another random number and repeat the above process. Output Signature $(r, s)$

(3) Verification. For Signature $(r, s)$ and message $e$, compute $u \equiv s^{-1}e(\mathrm{mod}\, n)$, $v \equiv s^{-1}r(\mathrm{mod}\, n)$, $(x_1, y_1) = uG + vQ$, $r_1 \equiv x_1(\mathrm{mod}\, n)$. If $r = r_1$, the signature is valid; Otherwise, the signature is invalid.

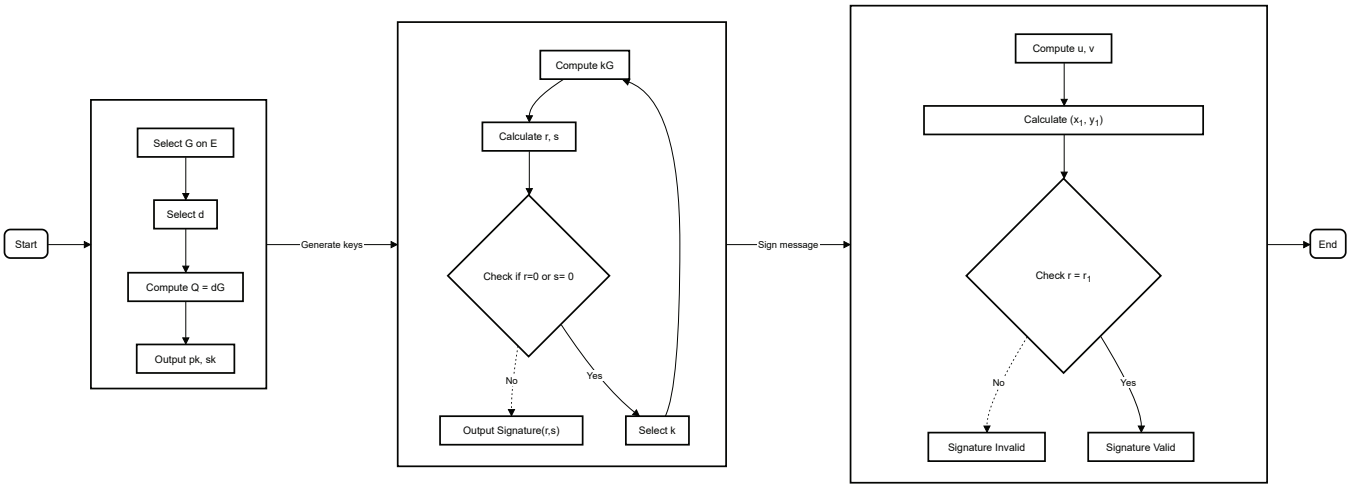


**Figure 2.** Flowchart of the ECDSA signature algorithm.

## 3. System Model and Threat Model

The smart meter authentication system includes four parties, as shown in Figure 3.

(1) Trust Authority (TA). There is only one TA in the system, who is responsible for initializing the system and injecting identity information into OC, RM, and SM.

(2) Operation Center (OC). There is only one OC in the system, which is responsible for billing the electricity consumption data forwarded by RMs and verifying the identity of SMs.

(3) Region Manager (RM). The system includes multiple RMs. The number of RMs is set by OC according to actual needs, for example, it can be divided by region, and each region has an RM. The RM is tasked with verifying the identity authentication of SMs in its region and forwarding their electricity consumption data to the OC.

(4) Region Manager (RM). The system includes multiple SMs, but each RM can manage up to n SMs. SM authenticate their identity with the RM and connect to the power grid.

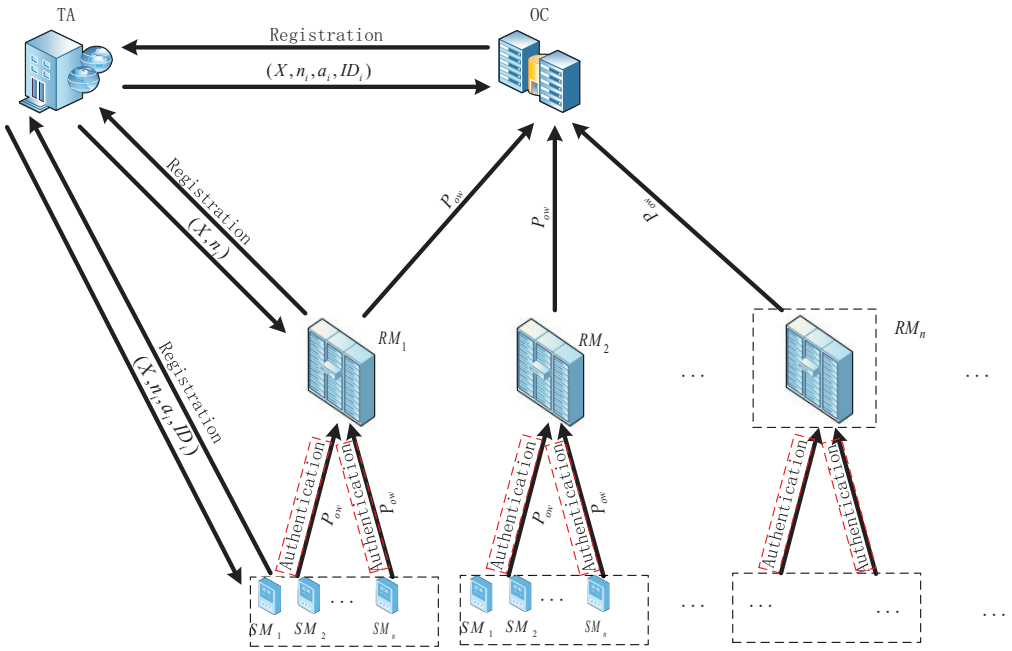


**Figure 3.** The smart meter authentication system.

It should be noted that in large-scale smart grids environments, identity authentication is required for millions of smart meters. Therefore, SMs can be registered according to their respective regions, meaning that the smart meter can communicate with the local RM instead of directly communicating with the OC. The proposed smart meter authentication system is a simplified one with only one layer of the RM. In practical deployment, the RM can be divided into multiple levels, which can reduce the burden of centralized authentication servers and improve the scalability of the system. In addition, the SM's identity authentication scheme needs to be deployed in actual power infrastructure and integrated with existing power systems. This may involve multiple stakeholders, technical standards, and security requirements, such as encryption algorithm standards, as well as management and maintenance, such as updating, monitoring, and troubleshooting authentication servers and smart meter software.

The threat model for smart meter authentication system is based on the threat model of [18]. In the smart grid, security issues may arise due to system compromises or vulnerabilities. Threats come from internal SM, dishonest RM, and external attacker. The following are threats related to smart meter authentication scheme.

(1) Passive Attack. Attackers illegally monitor data transmitted on the smart grid, compromising data confidentiality.
(2) Replay attack. The attacker repeatedly sends data that the receiver has already received, in order to deceive the receiver into accepting the message and disrupt the identity authentication.
(3) Collusion Attack. Internal SMs collude to attack the identity of other smart meters and then use that identity to carry out attacks.
(4) Forging Electricity Ledger Attack. The dishonest RM takes on SM identity and forges electricity consumption data for attacks.
(5) Identity Spoofing Attack. Attackers take on an identity that has been successfully authenticated and carry out attacks.

## 4. The Authentication Scheme for Smart Meter

The authentication scheme is divided into six phases: system initialization, key generation, smart meter registration, smart meter authentication, electricity consumption data charging, and smart meter revocation.

(1) System initialization phase.
① TA selects an elliptic curve: $E : y^2 \equiv x^3 + ax + b(\mathrm{mod}\, p)$ and an elliptic group $E_p(a, b)$, and randomly choose a generator $G \in E_p(a, b)$. Suppose the order of G is n. Randomly choose a hash function $H\{01\}^* \rightarrow E_p(a, b)$. Output public parameters $pp = \{E_p(a, b), G, H, n\}$.
② TA chooses randomly mutual prime numbers $n_1, n_2, \ldots, n_n$, a secret value $S$, and numbers $a_1, a_2, \ldots, a_n$, computes $p_i = E_{pk_{RM}}(S, n_i) + H(n_i, a_i)$, constructs the system of equations $\begin{cases} X \equiv p_1(\mathrm{mod}\, n_1) \\ X \equiv p_2(\mathrm{mod}\, n_2) \\ \cdots \\ X \equiv p_n(\mathrm{mod}\, n_n) \end{cases}$, and uses the CRT to compute the solution $X$.
(2) Key generation phase.
① OC randomly selects number $n_{OC} \in [1, n-1]$ as its private key and computes its public key $pk_{OC} = n_{OC}G$. OC outputs the public key $pk_{OC}$ and keeps the private key $sk_{OC} = n_{OC}$ secret.
② RM randomly selects number $n_{RM} \in [1, n-1]$ as its private key and calculates its public key $pk_{RM} = n_{RM}G$. RM outputs the public key $pk_{RM}$ and keeps the private key $sk_{RM} = n_{RM}$ secret.
(3) Smart meter registration phase.
When the $i$-th smart meter $SM_i$ is registered with TA, TA loads $(X, n_i, a_i)$ into $SM_i$ if $(X, n_i, a_i, ID_i)$ exists in TA's database. Otherwise, TA randomly selects $(X, n_i, a_i)$,

loads $(X, n_i, a_i, ID_i)$ into the smart meter $SM_i$. Then, TA secretly sends $(X, n_i, a_i, ID_i)$ to OC, and finally secretly sends $(X, n_i)$ to the corresponding RM.

(4) Smart meter authentication phase.

① The $SM_i$ authentication process to the RM is shown in Figure 4. $SM_i$ performs the following operations.

- Encode the registration information $(X, n_i, H(n_i, a_i), T_s)$ into point $P_m \in E_p(a, b)$, where $T_s$ is the timestamp selected by the $SM_i$.
- Randomly select the number $k_{SM} \in [1, n-1]$, compute $C_i = \{k_{SM}G, P_m + k_{SM}pk_{RM}\}$, and send $C_i$ to RM.

② After receiving $C_i$, the RM performs the following operations.

- Compute $P_m = P_m + k_{SM}pk_{RM} - sk_{RM}k_{SM}G$ by $sk_{RM}$ and get $(X, n_i, H(n_i, a_i), T_s)$ by decoding $P_m$.
- Check if the timestamp $T_s$ is valid, If it is invalid, return $\delta = 0$, indicating that the authentication of the SM to the RM has failed. If it is valid, compute $p_i = X \bmod n_i$ and $(\overline{S}, \overline{n_i}) = D_{sk_{RM}}(p_i - H(n_i, a_i))$.
- Compare whether $\overline{S}$ is equal to the system preset, and whether $\overline{n_i}$ is equal to $n_i$. If both are equal, return $\delta = 1$, indicating that $SM_i$ has successfully authenticated to RM. Otherwise, return $\delta = 0$.

(5) Electricity consumption data charging phase.

① Electricity consumption data charging is shown in Figure 5. The SM performs the following operations.

- summarize the electricity consumption data over a period of time (usually one month) and obtains $P_{ow}$.
- Choose a timestamp $T^{'}{}_s$ and encode $T_s^{'}, p_{ow}$ as a point $P_m{}' \in E_p(a, b)$.
- Compute $h = H(a_i, P_{ow}, T^{'}{}_s)$.
- Choose randomly number $k'_{RM} \in [1, n-1]$ and compute $C'_1 = \{k'_{SM}G, P'_m + k'_{SM}pk_{RM}\}$.
- Send ($h$,$C'_1$) to the RM.

② After receiving ($h$,$C'_1$), RM performs the following operations.

- Compute $P'_m = P'_m + k'_{SM}pk_{RM} - sk_{RM}k'_{SM}G$ by $sk_{RM}$ and get $T_s^{'}, p_{ow}$ by decoding $P'_m$.
- Check if the timestamp $T_s^{'}$ is valid, and exit if it is not. Otherwise, do the following.
- Encode the message $\left(X, n_i, P_{ow}, T_S^{'}\right)$ as point $P''_m \in E_p(a, b)$.
- Randomly choose number $k_{RM} \in [1, n-1]$ and compute $C'_2 = \{k_{RM}G, P''_m + k_{RM}pk_{OC}\}$.
- Signing $C'_2$ using the ECDSA signature algorithm yields $C_3^{'} = sig_{sk_{RM}}(H\left(C_2^{'}\right))$.
- Send $(C'_2, C'_3, h)$ to the OC.

③ OC performs the following operations.

- The OC verifies the validity of the signature $C_3{}^{'}$, and exits if it is invalid. Otherwise, proceed with the following operations.
- Compute $P''_m = P''_m + k_{RM}pk_{OC} - sk_{OC}k_{RM}G$ by $sk_{OC}$ and get $\left(X, n_i, P_{ow}, T_S^{'}\right)$ by decoding $P'_m$.
- Check if the timestamp $T_s^{'}$ is valid, and exit if it is not. Otherwise, do the following.
- Find the $a_i$ corresponding to $(X, n_i)$ in the local database and calculate whether $H(a_i, P_{ow}, T_S^{'})$ and $h$ are consistent. If they are consistent, it indicates that the Electricity consumption data are valid.

- By using $(X, n_i, a_i)$, the real identity of the $SM_i$ can be confirmed, thereby completing the electricity consumption data charging.

(6) SM revocation phase.
When $a_i$ is leaked or $SM_i$ logs out of the system, the OC can revoke $SM_i$ by broadcasting $a_i$ to the RM. If a revoked user $SM_i$ registers with RM, $SM_i$ needs to send registration information $(X, n_i, H(n_i, a_i), T_s)$ to the RM. After receiving the registration information, the RM can use the received revocation message $a_i$ from the OC and $n_i$ from $SM_i$ to calculate the hash value $H(n_i, a_i)$. If the hash value is equal to the hash value sent by $SM_i$, then the authentication is refused, indicating that the $SM_i$ has been revoked.

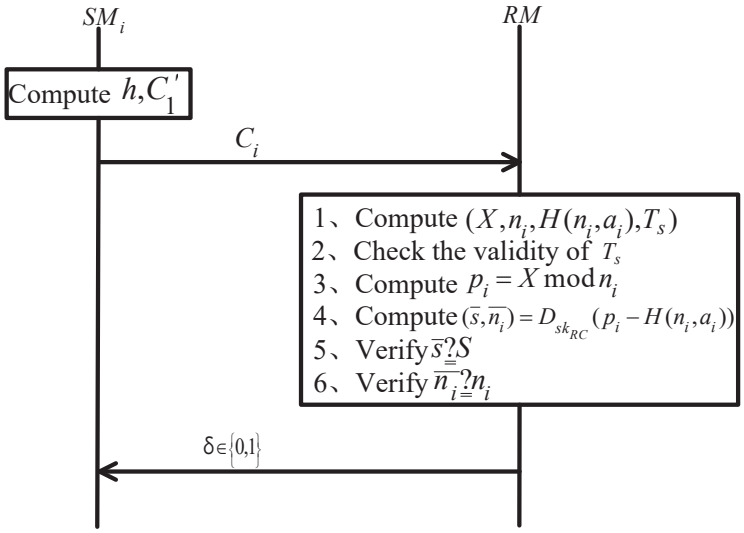


**Figure 4.** Authentication process to the RM.

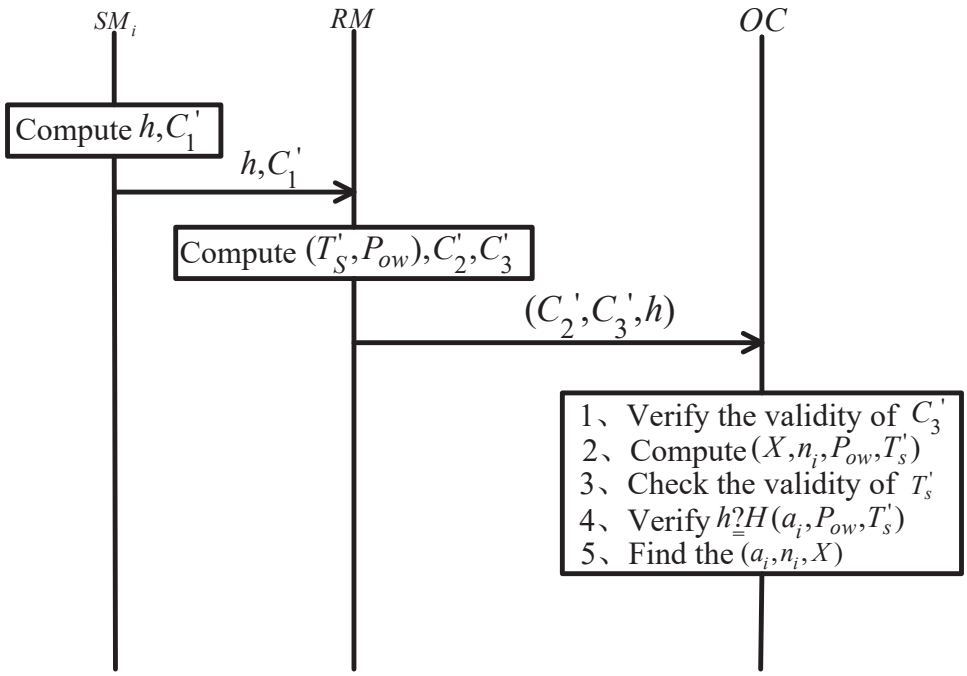


**Figure 5.** Electricity consumption data charging.

## 5. Correctness and Security Analysis

The correctness and security of the proposed scheme are analyzed in this section.

### *5.1. The Correctness Analysis*

The correctness of the scheme includes the correctness of smart meter authentication, electricity consumption data charging, and smart meter revocation.

(1) In the smart meter authentication phase, the smart meter sends a ciphertext $C_i = \{k_{SM}G, P_m + k_{SM}pk_{RM}\}$ to the RM, The RM calculates

$$\begin{aligned} & P_m + k_{SM}pk_{RM} - sk_{RM}k_{SM}G \\ &= P_m + k_{SM}pk_{RM} - k_{SM}(sk_{RM}G) \\ &= P_m + k_{SM}pk_{RM} - k_{SM}(pk_{RM}) \\ &= P_m. \end{aligned}$$

Thus, the RM can get $(X, n_i, H(n_i, a_i), T_s)$ by decoding $P_m$, and compute $p_i = X \bmod n_i$. Because $p_i = E_{pk_{RM}}(S, n_i) + H(n_i, a_i)$, the RM can decrypt $E_{pk_{RM}}(S, n_i) = p_i - H(n_i, a_i)$ and get $(\overline{S}, \overline{n_i})$. Therefore, it is possible to correctly output $\delta \in \{0, 1\}$ based on whether $\overline{S}$ and $S$, $\overline{n_i}$ and $n_i$ are equal.

(2) In the electricity consumption data charging phase, the RM can similarly decrypt the ciphertext $C^{'}{}_1$ to get $(T_S^{'}, P_{ow})$. The OC can verify the validity of $C_3{}^{'}$ by the validity verification of the signature and can decrypt it to get $(X, n_i, P_{ow}, T_S^{'})$. Because the hash function has collision resistance, verifying whether $H(a_i, P_{ow}, T_S^{'})$ and $h$ are equal can confirm the validity of the ledger and the real identity of the smart meter $SM_i$, thereby completing the billing of $ID_i$ electricity consumption $P_{ow}$.

(3) In the smart meter revocation phase, the OC can revoke $SM_i$ by broadcasting $a_i$ to RM. During the smart meter authentication phase, RM can obtain $(X, n_i, H(n_i, a_i), T_s)$. RM calculates the hash value by $a_i$ and $n_i$, and compares it with $H(a_i, n_i)$. If the hash values are equal, the authentication of $SM_i$ is rejected, resulting in $SM_i$ being revoked. The OC deletes the relevant information of $a_i$ from the local database, thereby revoking the $SM_i$.

### *5.2. The Security Analysis*

The smart meter authentication scheme involves six phases. Since the system initialization phase and the smart meter registration phase are completed offline or through secure channel transmission, there is no need to consider adversary. Smart meter revocation phase is operated by OC and does not require consideration of adversary. In the remaining three phases, security analysis is required because the information is transmitted over an open network. We analyze the security of the constructed scheme from two aspects: internal and external adversaries.

(1) Resist passive attack, coming from the internal SM or dishonest RM or external adversary. In the smart meter authentication phase, the message sent by the smart meter is the ciphertext $C_i$. In electricity consumption data charging phase, the message transmitted over the open network is the hash value H and the ciphertext $C^{'}{}_1, C_2^{'}, C_3{}^{'}$. From the security of the ECC (discrete logarithm problem on elliptic curve) and the property of the hash value (unidirectionality and collision resistance), it is known that the adversary cannot obtain any useful message from the hash value and the ciphertext, and thus the authentication scheme is secure for passive attack.

(2) Resist replay attack, coming from internal dishonest SM or dishonest RM or external adversary. In the smart meter authentication phase and electricity consumption data charging phase, if the smart meter forwards the intercepted ciphertext $C_i = \{k_{SM}G, P_m + k_{SM}pk_{RM}\}$, $C'{}_1 = \{k'{}_{SM}G, P'{}_m + k'{}_{SM}pk_{RM}\}$ to RM, the RM can obtain timestamp $T_s$ and $T^{'}{}_s$ by decoding $P_m$ and $P_m{}'$, which are get by decrypting $C_i$ and $C'{}_1$. Since the RM needs to check the validity of timestamps $T_s$ and $T^{'}{}_s$, it can resist replay attacks.

(3) Resist collusion attack, coming from the internal dishonest SM and external adversary. In the smart meter authentication phase, the smart meter $SM_i$ needs to provide the

hash value $H(n_i, a_i)$ additionally when performing authentication. Because even if smart meter users collude to attack and obtain $n_j$, due to the unidirectionality and collision resistance of the hash function, they cannot guess $a_i$ or the hash value. Therefore, it can resist collusion attack.

(4) Resist forging electricity ledger attack, coming from the dishonest RM. In the electricity consumption data charging phase, the dishonest RM takes on the identity of the successfully authenticated smart meter and forges the smart meter electricity consumption data $P_{ow}$ to send to the OC. Due to the unidirectionality of the hash function, $a_i$ cannot be calculated from $h = H(a_i, P_{ow}, T^{'}{}_s)$. Therefore, the RM does not know the secret value $a_i$ of the smart meter that has been successfully authenticated, and cannot calculate the corresponding hash value $h$. Therefore, RM can only randomly select a hash value to send to the OC. When the OC searches for corresponding to $(X, n_i)$ in the local database, it can calculate that $H(a_i, P_{ow}, T_S^{'})$ and $h$ are not equal, thus rejecting the ledger and resisting the forging electricity ledger attack.

(5) Resist identity spoofing attack, coming from internal SM or external adversary. An unauthenticated smart meter takes on the identity of a successfully authenticated smart meter and forges the smart meter electricity consumption data $P_{ow}$ sent to the RM. Because the unauthenticated smart meter does not know the secret value $a_i$ of the authenticated smart meter, it cannot calculate the real hash value $h = H(a_i, P_{ow}, T^{'}{}_s)$. Similar to the forging electricity ledger attack, when the OC searches for $a_i$ corresponding to $(X, n_i)$ in the local database, it can calculate that $H(a_i, P_{ow}, T_S^{'})$ and $h$ are not equal, thus rejecting the ledger and resisting identity spoofing attack.

Specifically, in the proposed scheme, when illegal users want to enter the system, they first need to perform identity authentication. In the identity authentication phase, smart meter users need to send registration information $(X, n_i, H(n_i, a_i), T_s)$ to RM. However, the message is sent in ciphertext form during the sending process, so the adversary cannot obtain valid information (in this case, it is a passive attack, that is, even if the attacker intercepts the ciphertext message, they cannot decipher the valid information). If the adversary replays the intercepted message, it is known from the timestamp $T_s$ that the system will reject it (in this case, it is a replay attack).

If the adversary wants to impersonate other legitimate users for identity authentication, the adversary needs to know the secret random number $a_i$ of the legitimate user or its corresponding hash value $H(n_i, a_i)$. However, the user's $a_i$ is hidden in the hash function, and the one-way and anti-collision properties of the hash function indicate that the secret random number $a_i$ of other legitimate users cannot be found. Therefore, it is not possible to impersonate other users (at this time, it is an identity spooning attack).

If the adversary conspires with some dishonest users to impersonate other legitimate users, then the adversary and dishonest users also need to conspire to calculate the secret random number $a_i$ or its corresponding hash value $H(n_i, a_i)$ of other legitimate users. Although there is a high probability of calculating mutually prime integers $n_i$, the input to the hash function still has an $a_i$, and the random number $a_i$ is hidden in the hash function, with each user's $a_i$ being independent of each other, resulting in the failure of the collusion attack.

Even if the adversary is very powerful and obtains all the registration information $(X, n_i, H(n_i, a_i), T_s)$, that is, the adversary has obtained a valid hash value $H(n_i, a_i)$ and passed identity authentication (because the hash value is random, this probability can be ignored unless the attacker is dishonest RM). However, according to the unidirectionality of the hash function, adversaries cannot obtain the true $a_i$, and, therefore, cannot calculate $h = H(a_i, P_{ow}, T^{'}{}_s)$. Therefore, adversaries cannot forge electricity ledger, and, therefore, cannot cause economic losses to users within the system (in this case, it is forging electricity ledger attack).

## 6. Performance Analysis and Comparison

This section compares the proposed scheme with some related schemes in terms of property and performance.

### *6.1. Property Comparison*

At present, the identity authentication schemes for smart meters include [9,19–22]. Table 1 compares these schemes from six aspects: Passive Attack, Replay attack, Collusion attack, Forging Electricity Ledger Attack, Identity Spoofing Attack, and Revoke a single user. Due to the use of ciphertext or hash values for transmission and the use of timestamps, these schemes can resist passive attack and replay attacks. Except for scheme [9], all other schemes can resist identity spooning attack. Refs. [20,21] and the proposed scheme can resist collusion attacks, but only the proposed scheme has the property of revoking a single user.

**Table 1.** Comparison of properties.

| | [9] | [19] | [20] | [21] | [22] | Proposed |
|---|---|---|---|---|---|---|
| Passive Attack | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Replay attack | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Collusion attack | × | × | ✓ | ✓ | × | ✓ |
| Forging Electricity Ledger Attack | × | × | × | – | – | ✓ |
| Identity Spoofing attack | × | ✓ | ✓ | ✓ | ✓ | ✓ |
| Revoke a single user | × | × | × | × | × | ✓ |

"✓" represents the scheme with this property, " × " represents the scheme without this property, and " – " represents the scheme without considering this property.

### *6.2. Computational Overhead*

The proposed authentication scheme involves operations such as congruent equations, ECC encryption/signature algorithm, and hash functions. The solution of the congruence equation system based on the CRT can be carried out offline by the TA. Therefore, in efficiency analysis, we only need to consider the ECC encryption/signature algorithm and hash function in the online authentication phase. The efficiency of these algorithms determines the computational efficiency of our scheme. In the data transmission process, only the hash $h$ and ciphertext $C_i$, $C^{'}{}_1, C_2^{'}, C_3{}^{'}$, are included. Therefore, compared to authentication schemes based on HMAC, zero-knowledge proofs, blind signatures, group signatures and certificates techniques, our proposed scheme has less computational and communication overhead, and is more suitable for smart meter authentication.

For comparison, the time required for the execution of operations in [11,23] is used, which was obtained by running the Windows 7 operating system on a hardware platform with an Intel I7-4770 processor, a clock frequency of 3.40 GHz, and 4 GB of memory using the library MIRACL, as shown in Table 2. Compared with the authentication scheme based on the CRT, such as the schemes of Xiong et al. [3] and Zhang et al. [11], our scheme also has advantages in terms of computation and communication overhead, as shown in Table 3.

**Table 2.** Time cost of referring cryptographics.

| Symbol | Meaning | Time (ms) |
|---|---|---|
| $T_{sm}$ | Time of scalar multiplication on elliptic curves | 0.4420 |
| $T_{s-sm}$ | Time of small scalar multiplication on elliptic curves [1] | 0.0138 |
| $T_{pa}$ | Time of point addition on elliptic curves | 0.0018 |
| $T_h$ | Time of hash function | 0.0001 |

[1] The time to execute the small-scale multiplication operation $v_i \bullet P$ using the small exponent test technology, where $P \in G$ , $v_i \in [1, 2^t]$ , and $t$ is a small integer.

**Table 3.** Comparison of computational overhead and communication overhead.

| Scheme | Computational Overhead | Communication Overhead |
|---|---|---|
| [3] | $5T_{sm} + 4T_{s-sm} + 4T_{pa} + 3T_h$ | $3\|\mathbb{G}\|+\|q\|$ |
| [9] | $4T_{sm} + T_h$ | $\|\mathbb{G}\|+ 1$ |
| [11] | $5T_{sm} + 3T_h + 2T_{pa}$ | $\|\mathbb{G}\| + 2\|q\|$ |
| [21] | $5T_{sm} + 3T_h$ | $2\|\mathbb{G}\|$ |
| [22] | $4T_{sm} + 8T_h$ | $2\|\mathbb{G}\|$ |
| Ours | $4T_{sm} + T_h$ | $\|\mathbb{G}\|+ 1$ |

In the scheme of Xiong et al. [3], one elliptic curve scalar multiplication, three small-scale multiplications, and three hash functions are required in the message signature phase, and four scalar multiplications and four point additions on elliptic curve, and one small-scale multiplication are required in the single-message authentication phase. Therefore, the total time cost is $5T_{sm} + 4T_{s-sm} + 4T_{pa} + 3T_h \approx 2.2727$ ms. In the scheme of Tian et al. [9], the identity authentication phase for the electricity meter requires four elliptic curve scalar multiplications and one hash operation. Therefore, the total time cost is $4T_{sm} + T_h \approx 1.7681$ ms. In the scheme of Zhang et al. [11], two elliptic curve scalar multiplications as well as two hash functions are required in the anonymous identity and signature phases, and three elliptic curve scalar multiplications, two elliptic curve point additions as well as one hash function are required in the single-message authentication phase. Therefore, the total time cost is $5T_{sm} + 3T_h + 2T_{pa} \approx 2.2139$ ms. In the scheme introduced by Garg et al. [21], the identity authentication phase involves five elliptic curve scalar multiplications and three hash operations. Therefore, the total time cost is $5T_{sm} + 3T_h \approx 2.2103$ ms. In the scheme of Sureshkumar et al. [22], the authentication phase needs four elliptic curve scalar multiplications and eight hash operations. Therefore, the total time cost is $4T_{sm} + 8T_h \approx 1.7688$ ms. In our scheme, four elliptic curve scalar multiplications, one hash function, and one modulo computation are required in the smart meter authentication phase. Therefore, the total time cost is $4T_{sm} + T_h \approx 1.7681$ ms. As shown in Figure 6, our proposed scheme has the lowest Computation overhead in the identity authentication phase.

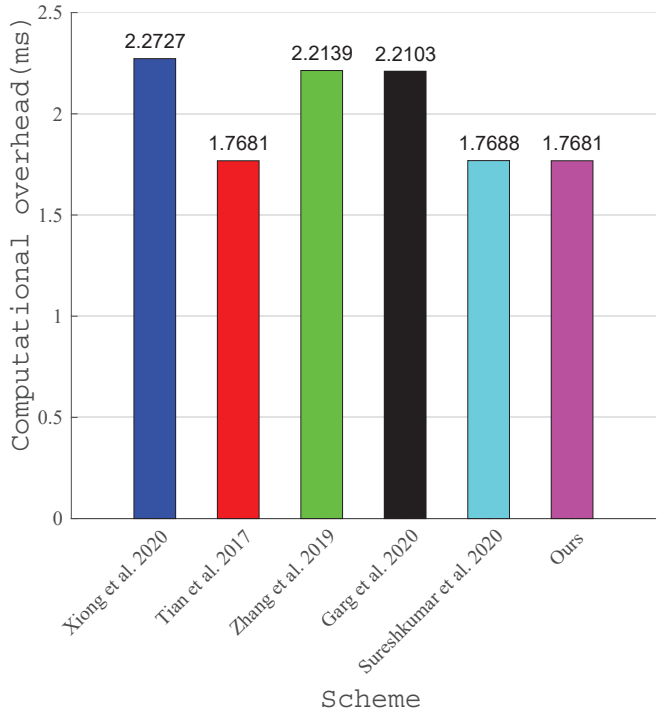


**Figure 6.** Time cost of computation in the identity authentication phase compared with [3,9,11,21,22].

### 6.3. Communication Overhead

The comparison of the communication overhead during the identity authentication phase is shown in Table 3, where $|\mathbb{G}|$ represents the bit length of the group on the elliptic curve and $|q|$ represents the element bit length in $\mathbb{Z}_q$. We adopt the same assumption as in [11], i.e., the size of p is 20 bytess, hence the size of elements in G is 40 bytess. As shown in Figure 6, compared to other schemes, our proposed scheme also has the smallest communication overhead in the identity authentication phase. In the scheme of Xiong et al. [3], vehicles are required to send $(M_i, PSID_{i_k}, ID_{i_k}, T_i, \sigma_i)$ to the roadside unit during the authentication phase, including three elements on the elliptic curve and one element in an integer group, hence the communication overhead is approximately $3|\mathbb{G}| + |q| \approx 140$ bytess. In the scheme of Tian et al. [9], the smart meter's authentication phase needs the sending of one elliptic curve element and a one-bit message, resulting in a communication overhead of approximately $|\mathbb{G}| + 1 \approx 41$ bytess. In the scheme of Zhang et al. [11], vehicles need to send to the roadside unit for identity authentication, including one elliptic curve element and two elements in integer groups, hence the communication overhead is approximately $|\mathbb{G}| + 2|q| \approx 80$ bytes. In the scheme of Garg et al. [21], smart meters are required to send $(I_{SM}, r_{SM}, \mathcal{R}_{SM}, \mathcal{T}_{SM})$ to the gateway, including one elliptic curve element and one element in an integer group, and the gateway sends $(r_{NAN}, \mathcal{R}_{NAN}, \mathcal{T}_{NAN}, Auth_{NAN})$ to the smart meter, including one elliptic curve element and one element in an integer group, leading to a communication overhead of approximately $2|\mathbb{G}| + 2|q| \approx 120$ bytes. In the scheme by Sureshkumar et al. [22], smart meters are required to send $(D_2, D_4, D_5, TS2_k)$, including two elliptic curve elements, thus the communication overhead is approximately $2|\mathbb{G}| \approx 80$ bytes. In the proposed scheme, during the meter's authentication phase, message $C'_1$ along with a one-bit confirmation message is required to be sent, leading to a communication overhead of approximately $|\mathbb{G}| + 1 \approx 41$ bytes. The communication overhead is shown in the Figure 7.

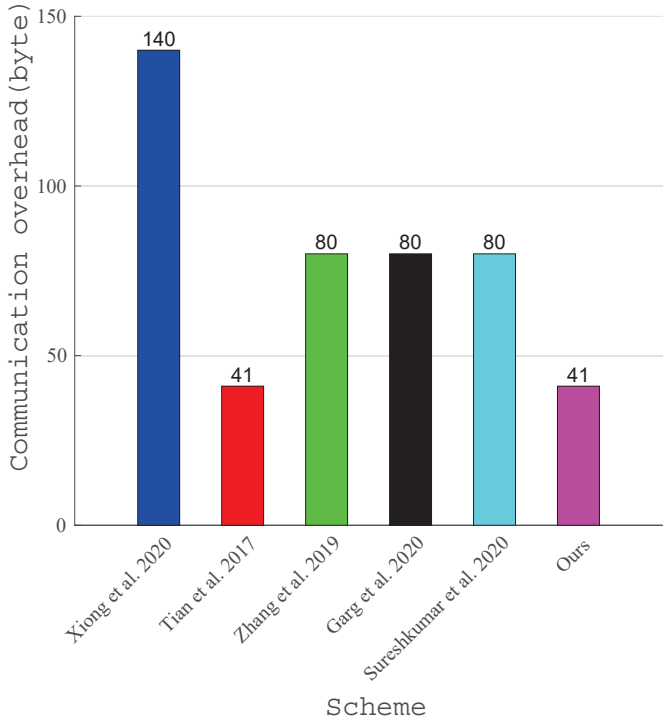


**Figure 7.** Time cost of communication in the identity authentication phase compared with [3,9,11,21,22].

### 6.4. Energy Consumption

Ref. [21] showed the energy consumption calculation formula $vol \times cur \times T$, where $vol$ represents voltage and $cur$ represents current, with $(vol = 3\ \text{V}, cur = 1.8\ \mu\text{A})$ . The energy consumed for sending and receiving one-bit messages is 0.72 μJ and 0.81 μJ, respectively.

In the scheme of Xiong et al. [3], the energy consumption related to computation is approximately 3 V × 1.8 μA × $(5T_{sm} + 4T_{s-sm} + 4T_{pa} + 3T_h) \approx 12.2725$ μJ, and the energy required for communication is approximately $(3|\mathbb{G}| + |q|) \times 0.72$ μJ $\approx 100.8000$ μJ, totaling approximately 113.0725 μJ. In the scheme of Tian et al. [9], the energy consumption related to computation is approximately 3 V × 1.8 μA × $(4T_{sm} + T_h) \approx 9.5477$ μJ and the energy required for communication is approximately $(|\mathbb{G}| + 1) \times 0.72$ μJ $\approx 29.5200$ μJ, totaling approximately 39.0677 μJ. In the scheme of Zhang et al. [11], the energy consumption related to computation is approximately 3 V × 1.8 μA × $(5T_{sm} + 3T_h + 2T_{pa}) \approx 11.9550$ μJ and the energy required for communication is approximately $(|\mathbb{G}| + 2|q|) \times 0.72$ μJ $\approx$ 57.6 μJ, totaling approximately 69.5550 μJ. In the scheme of Garg et al. [21], the energy consumption related to computation is approximately 3 V × 1.8 μA × $(5T_{sm} + 3T_h) \approx$ 11.9356 μJ, and the energy required for communication is approximately $(|\mathbb{G}| + |q|) \times$ 0.72 μJ + $(|\mathbb{G}| + |q|) \times 0.81$ μJ $\approx 91.8000$ μJ, totaling approximately 103.7356 μJ. In the scheme of Sureshkumar et al. [22], the energy consumption related to computation is approximately 3 V × 1.8 μA × $(4T_{sm} + 8T_h) \approx$ 9.5515 μJ and the energy required for communication is approximately $(2|\mathbb{G}|) \times 0.72$ μJ $\approx 57.6000$ μJ, totaling approximately 67.1515 μJ. Since other schemes do not include a meter confirmation phase, for the sake of unified comparison, only the energy consumption of sending messages is considered in the proposed scheme. The energy consumption related to computation is approximately 3 V × 1.8 μA × $(4T_{sm} + T_h) \approx 9.5477$ μJ and the energy required for communication is approximately $|\mathbb{G}| \times 0.72$ μJ $= 40 \times 0.72$ μJ $\approx 28.8000$ μJ, totaling approximately 38.3477 μJ. The comparison of energy consumption related to computation is illustrated in Figure 8, the comparison of energy consumption related to communication is shown in Figure 9, and the total energy consumption comparison is depicted in Figure 10.

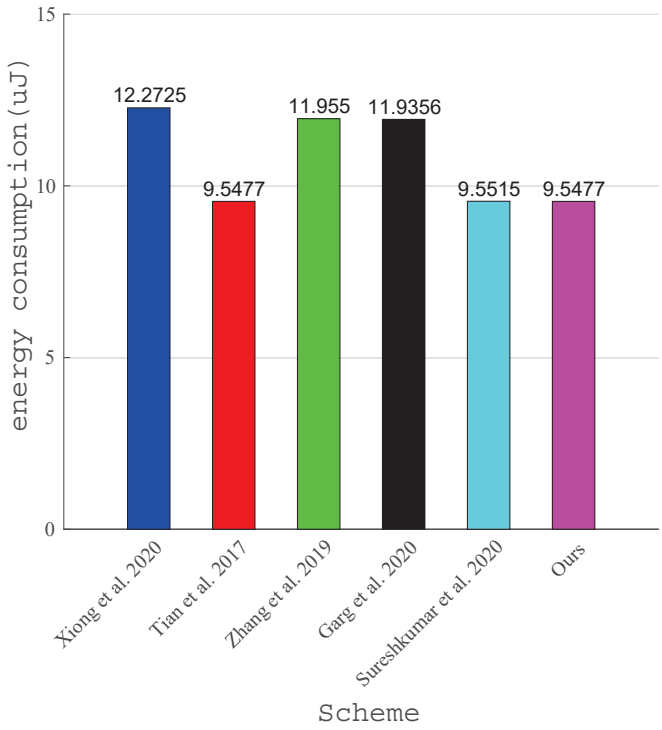


**Figure 8.** Calculation-related energy consumption compared with [3,9,11,21,22].

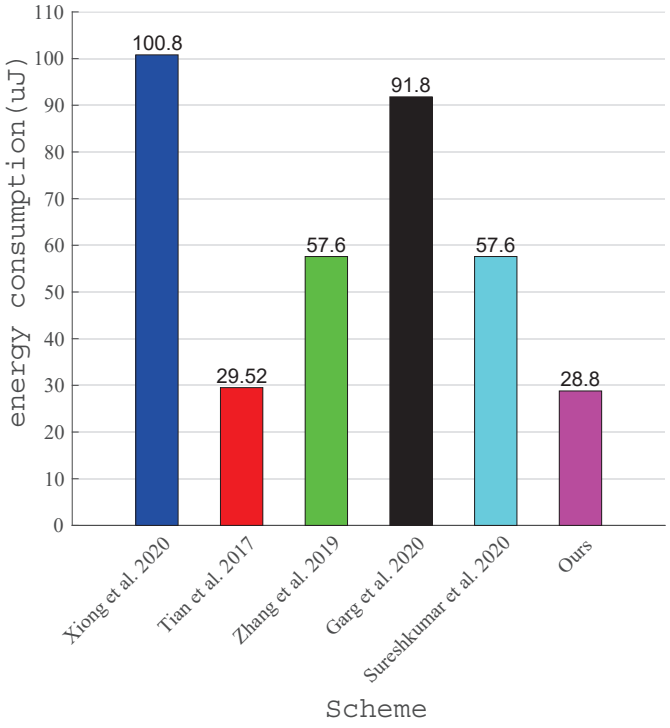


**Figure 9.** Communication-related energy consumption compared with [3,9,11,21,22].

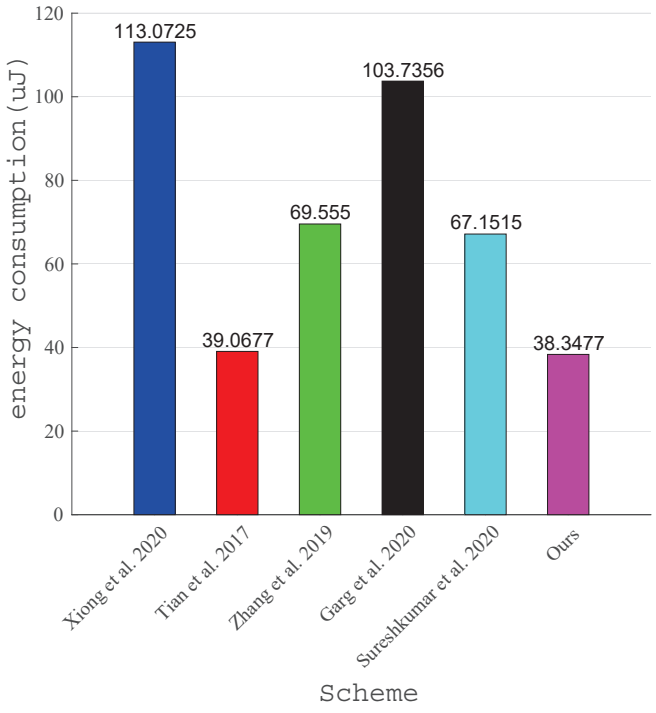


**Figure 10.** Total Compare total energy consumption with [3,9,11,21,22].

## 7. Conclusions

A lightweight authentication scheme for smart meters is proposed in this paper, which uses the Chinese Remainder Theorem for identity authentication, reduces the computation and communication overhead during the authentication phase, and effectively revokes a single smart meter user by exposing the random secret number in the hash function. In addition, the ECC encryption algorithm is used for confidential transmission of electricity consumption data. The security of the proposed scheme was analyzed from both internal

and external adversaries, which shows that the proposed scheme can resist passive attack, replay attack, collusion attack, false electronic ledger attack, and identity deception attack. However, the mutual authentication was not considered in the authentication phase. In our future work, we will consider more robust system models and stronger security requirements, such as mutual authentication and hierarchical authentication, to adapt to more complex real-world requirements.

**Author Contributions:** Conceptualization and methodology, J.D. and C.D.; writing—original draft J.D. and P.M.; software and validation, W.D. and X.W.; writing—review and editing, Z.L. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no funding

**Data Availability Statement:** Data are contained within the article.

**Conflicts of Interest:** Jingqi Du was employed by CLP Great Wall Internet System Application Co., Ltd.; Chengjing Dai was employed by China Energy Engineering Group Yunnan Electric Power Design Institute Co., Ltd.; Pinshang Mao was employed by NR Electric Co., Ltd. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest. The companies had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

## References

1. Panasenko, S. A Lightweight Blockchain for the Internet of Medical Things Using Hash-based Message Authentication Codes. In Proceedings of the 2023 International Wireless Communications and Mobile Computing (IWCMC), Marrakesh, Morocco, 19–23 June 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 1095–1100.
2. Rasheed, A.A.; Mahapatra, R.N.; Hamza-Lup, F.G. Adaptive group-based zero knowledge proof-authentication protocol in vehicular ad hoc networks. *IEEE Trans. Intell. Transp. Syst.* **2019**, *21*, 867–881. [CrossRef]
3. Xiong, H.; Chen, J.; Mei, Q.; Zhao, Y. Conditional privacy-preserving authentication protocol with dynamic membership updating for VANETs. *IEEE Trans. Dependable Secur. Comput.* **2020**, *19*, 2089–2104. [CrossRef]
4. Sui, Z.; Li, J. An Auditable and Efficient Prepaid Scheme with Privacy Preservation in Smart Grids. In Proceedings of the 2023 IEEE International Conference on Big Data and Smart Computing (BigComp), Jeju, Republic of Korea, 13–16 February 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 48–55.
5. Wasef, A.; Shen, X. Efficient group signature scheme supporting batch verification for securing vehicular networks. In Proceedings of the 2010 IEEE International Conference on Communications, Cape Town, South Africa, 23–27 May 2010; IEEE: Piscataway, NJ, USA, 2010; pp. 1–5.
6. Garba, A.; Khoury, D.; Balian, P.; Haddad, S.; Sayah, J.; Chen, Z.; Guan, Z.; Hamdan, H.; Charafeddine, J.; Al-Mutib, K. LightCert4IoTs: Blockchain-Based Lightweight Certificates Authentication for IoT Applications. *IEEE Access* **2023**, *11*, 28370–28383. [CrossRef]
7. Jiang, S.; Zhu, X.; Wang, L. An efficient anonymous batch authentication scheme based on HMAC for VANETs. *IEEE Trans. Intell. Transp. Syst.* **2016**, *17*, 2193–2204. [CrossRef]
8. Erroutbi, A.; El Hanjri, A.; Sekkaki, A. Secure and lightweight HMAC mutual authentication protocol for communication between IoT devices and fog nodes. In Proceedings of the 2019 IEEE International Smart Cities Conference (ISC2), Kansas City, MO, USA, 14–17 October 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 251–257.
9. Tian, F.L.; Tian, X.X.; Song, Q.; Xue, J.H. Smart Meter Identity Authentication Scheme Based on Chinese Residual Theorem. *J. Shanghai Univ. Electr. Power* **2017**, *33*, 397–401.
10. Dwivedi, A.D.; Singh, R.; Ghosh, U.; Mukkamala, R.R.; Tolba, A.; Said, O. Privacy preserving authentication system based on non-interactive zero knowledge proof suitable for Internet of Things. *J. Ambient. Intell. Humaniz. Comput.* **2021**, *13*, 4639–4649. [CrossRef]
11. Zhang, J.; Cui, J.; Zhong, H.; Chen, Z.; Liu, L. PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks. *IEEE Trans. Dependable Secur. Comput.* **2019**, *18*, 722–735. [CrossRef]
12. Kong, W.; Shen, J.; Vijayakumar, P.; Cho, Y.; Chang, V. A practical group blind signature scheme for privacy protection in smart grid. *J. Parallel Distrib. Comput.* **2020**, *136*, 29–39. [CrossRef]
13. Jiang, Y.; Ge, S.; Shen, X. AAAS: An anonymous authentication scheme based on group signature in VANETs. *IEEE Access* **2020**, *8*, 98986–98998. [CrossRef]
14. Pathak, A.; Patil, T.; Pawar, S.; Raut, P.; Khairnar, S. Secure authentication using zero knowledge proof. In Proceedings of the 2021 Asian Conference on Innovation in Technology (ASIANCON), Pune, India, 27–29 August 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–8.

15. Zhu, B.; Li, Y.; Hu, G.; Zhang, M. A Privacy-Preserving Data Aggregation Scheme Based on Chinese Remainder Theorem in Mobile Crowdsensing System. *IEEE Syst. J.* **2023**, *17*, 4257–4266. [CrossRef]
16. Lu, Y.; Cao, S.; He, Q.; Fang, Z.; Yan, J.; Guo, Y. Group Signature Authentication Scheme with Credit Evaluation Mechanism in VANET. In Proceedings of the 2023 26th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Rio de Janeiro, Brazil, 24–26 May 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 1703–1709.
17. Johnson, D.; Menezes, A.; Vanstone, S. The elliptic curve digital signature algorithm (ECDSA). *Int. J. Inf. Secur.* **2001**, *1*, 36–63. [CrossRef]
18. Singh, J.; Gimekar, A.; Venkatesan, S. An efficient lightweight authentication scheme for human-centered industrial Internet of Things. *Int. J. Commun. Syst.* **2023**, *36*, e4189. [CrossRef]
19. Hur, J.B.; Koo, D.Y.; Shin, Y.J. Privacy-Preserving Smart Metering with Authentication in a Smart Grid. *Appl. Sci.* **2015**, *17*, 1503–1527. [CrossRef]
20. Hegde, M.; Anwar, A.; Kotegar, K.; Baig, Z.; Robin Doss, R. A novel multi-stage distributed authentication scheme for smart meter communication. *PeerJ Comput. Sci.* **2021**, *7*, e643. [CrossRef] [PubMed]
21. Garg, S.; Kaur, K.; Kaddoum, G.; Rodrigues, J.J.P.C.; Robin Doss, M. Secure and Lightweight Authentication Scheme for Smart Metering Infrastructure in Smart Grid. *IEEE Trans. Ind. Inform.* **2020**, *16*, 3548–3557. [CrossRef]
22. Sureshkumar, V.; Anandhi, S.; Amin, R.; Selvarajan, N.; Madhumathi, R. Design of robust mutual authentication and key establishment security protocol for cloud-enabled smart grid communication. *IEEE Syst. J.* **2020**, *15*, 3565–3572. [CrossRef]
23. He, D.; Zeadally, S.; Xu, B.; Huang, X. An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 2681–2691. [CrossRef]