# Security-Enhanced Lightweight Anonymous Authentication Scheme for Smart Grid Postprint

**Authors:** Ding Zhifan, Hu Hongbo, Yang Qingyu, Xiao Siyuan

**Date:** 2022-06-06T00:00:00+00:00

## Abstract

Existing identity authentication schemes for smart grids mostly suffer from high computational costs and complex authentication processes, making them unsuitable for resource-constrained smart devices in smart grids. However, some lightweight schemes have various security vulnerabilities, and these schemes cannot achieve the required trade-off between efficiency and security. To address the aforementioned issues, an enhanced provably secure lightweight anonymous authentication scheme for smart grids is designed based on elliptic curve cryptographic algorithms. By introducing auxiliary verifiers, the scheme eliminates reliance on electricity suppliers during the authentication phase, and achieves mutual authentication between gateways and smart meters while protecting the real identities of smart meters. Meanwhile, malicious smart meters can be traced and revoked through their pseudo-identities. Security analysis under the random oracle model and simulation tool ProVerif demonstrate that the scheme possesses strong security properties. Performance analysis shows that the proposed scheme can meet the requirements for security and efficiency in smart grid environments.

## Full Text

## Preamble

**Vol. 39 No. 10**
**Application Research of Computers**
**ChinaXiv Cooperative Journal**

**Security Enhanced Lightweight Anonymous Authentication Scheme for Smart Grid**

**Ding Zhifan[1] , Hu Hongbo[1] , Yang Qingyu[1] , Xiao Siyuan[1]**

[1](a. College of Electronic Information & Automation; b. Network & Information Management Center, Xiangtan University, Xiangtan Hunan 411105, China)

**Abstract:** Most existing smart grid authentication schemes suffer from high computational costs and complex authentication processes, making them unsuitable for resource-constrained smart devices in smart grids. Meanwhile, some lightweight schemes exhibit various security vulnerabilities, and none can achieve the required trade-off between efficiency and security. To address these issues, this paper designs an enhanced provably secure lightweight anonymous authentication scheme for smart grids based on elliptic curve cryptography. By introducing an auxiliary validator, the scheme eliminates dependency on the power supplier during the authentication phase and achieves mutual authentication between the gateway and smart meters while protecting their real identities. Additionally, malicious smart meters can be traced and revoked through pseudo-identities. Security analysis under the random oracle model and simulation using the ProVerif tool demonstrate that the proposed scheme possesses high security properties. Performance analysis shows that the scheme meets the security and efficiency requirements of smart grid environments.

**Keywords:** smart grid; identity authentication; elliptic curve; random oracle model; ProVerif

---

## 0 Introduction

Traditional power systems are no longer sufficient to address the challenges posed by emerging industrial production and socio-economic development due to their inherent limitations. As the next-generation power system, smart grids embed advanced technologies such as sensing, computing, and communication into the grid infrastructure to provide feasible, efficient, sustainable, economically viable, and secure power supply, significantly improving the efficiency of existing grids [**?**]. At the generation side, smart grids enable more accurate monitoring, power flow optimization, and greener energy production by integrating renewable energy sources [**?**]. At the user side, smart meters and other intelligent metering infrastructure are deployed to enable real-time monitoring of user power consumption. Each user is equipped with a smart meter that periodically collects consumption data, while gateways aggregate data from groups of users within their regions. Power suppliers analyze the aggregated consumption data and dynamically update pricing to implement demand-side management [**?**].

Despite these advantages, the interconnectivity, dynamic nature, and heavy reliance on information communication technologies make smart metering infrastructure vulnerable to numerous security threats, including man-in-the-middle attacks, impersonation attacks, and replay attacks [**?**]. Since communication between power suppliers, gateways, and smart meters is bidirectional, attackers can infiltrate the smart grid system from multiple entry points to steal user consumption data and further invade the power supplier' s databases. Con-

sequently, cybersecurity has become the most critical issue in smart grids [**?**]. However, traditional cybersecurity technologies such as password protection, anti-malware, and firewalls have their own limitations [**?**]. To address these challenges, secure and efficient authentication mechanisms must be integrated into smart grid communication systems to support secure information exchange among communication entities while protecting their privacy. Identity authentication and key agreement schemes serve as such mechanisms, enabling secure remote communication among smart grid parties, ensuring data confidentiality, user privacy, and message integrity, thereby providing reliable power services.

To tackle security issues in smart grids, researchers have proposed numerous identity authentication and key agreement schemes in recent years. However, two major problems persist: (a) Most existing schemes have been shown to contain various security vulnerabilities, making them susceptible to known attacks, and they fail to provide session key security or smart meter anonymity, thus cannot meet security requirements in smart grid environments. (b) Some existing schemes incur high computational and communication costs due to expensive operations such as exponentiation or bilinear pairing, which resource-constrained smart meters cannot accommodate.

Recently, Gope et al. [**?**] proposed a spatial data aggregation scheme for securely obtaining power demand in smart grids. The scheme consists of two phases: authentication and data aggregation. The authors claim their scheme is secure, achieves secure authentication and key agreement during the authentication phase, and resists known attacks, making it optimal for smart grid environments. However, this paper demonstrates that their scheme cannot resist key compromise impersonation attacks and that its session keys are insecure, which seriously compromises the security of smart grid communication systems.

To address these issues, this paper proposes a new provably secure lightweight anonymous authentication scheme for smart grids based on elliptic curve cryptography that meets security requirements while offering superior performance. The main contributions are: (a) Security analysis of the authentication phase in Gope et al.' s scheme, proving it cannot resist key compromise impersonation attacks and lacks session key security. (b) Design of an identity authentication and key agreement scheme for smart grids that introduces an auxiliary validator, eliminating the power supplier' s involvement in the authentication phase. (c) The proposed scheme protects smart meter identity information during message authentication, ensuring anonymity and untraceability. It uses symmetric encryption for lightweight pseudo-identity updates and enables tracing and revocation of malicious smart meters through pseudo-identities when necessary. (d) Proof of session key security and resistance to various known attacks using the random oracle model and ProVerif simulation tool. Comparative analysis with related schemes shows advantages in security, computational cost, and communication overhead.

## 1 Related Work

Numerous cryptographic protocols have been proposed as solutions to protect smart grid security in academia and industry, including digital signatures, encryption, data aggregation, secure data storage, and identity authentication schemes [?]. Among these, identity authentication schemes constitute the first line of defense for ensuring data security and privacy protection in smart grids and represent an important requirement for smart grid deployment. In 2015, Tsai and Lo [?] proposed identity-based signature and encryption schemes using bilinear pairing to achieve mutual authentication between service providers and smart meters. In 2016, Odelu et al. [?] pointed out that Tsai and Lo' s scheme [?] could not guarantee the privacy of smart meter secret credentials or session key security, and proposed a secure and efficient authenticated key agreement scheme that successfully addressed potential privacy leakage issues. In 2017, Chen et al. [?] demonstrated that Odelu et al.' s scheme [?] was vulnerable to impersonation attacks and allowed smart meter tracing through the key generation center. To solve these problems, Chen et al. modified the smart meter registration process at the key generation center by encrypting smart meter identities before transmission and preventing private key leakage to the key generation center, thus making it immune to various potential attacks from the key generation center. However, these schemes [?, ?, ?] used bilinear pairing and exponentiation, and suffered from key escrow problems, resulting in high computational costs.

To meet lightweight requirements, increasing numbers of researchers have adopted elliptic curve cryptography (ECC) to construct smart grid authentication schemes. In 2016, He et al. [?] proposed a lightweight anonymous key agreement scheme based on ECC to reduce the high computational costs caused by bilinear pairing and exponentiation in Tsai and Lo' s scheme [?], achieving mutual authentication between smart meters and service providers without a trusted third party. In 2018, Abbasinezhad et al. [?] pointed out that He' s scheme [?] could not resist known-session temporary information attacks or temporary secret value leakage attacks, and proposed an ECC-based key agreement scheme that provided session key security and solved key escrow issues, though it was later noted to lack smart meter anonymity [?]. In 2020, Garg et al. [?] proposed a secure authentication scheme combining the Fully Hashed Menezes-Qu-Vanstone (FHMQV) key exchange mechanism with ECC, which could resist various known attacks at low computational cost, but was proven unable to achieve smart meter anonymity and untraceability [?]. In 2021, Srinivas et al. [?] designed a new anonymous signature-based authenticated key exchange scheme combining ECC with Schnorr' s signature scheme that supported dynamic addition of new smart meters after initial deployment, but was shown to be vulnerable to man-in-the-middle and impersonation attacks and did not provide anonymity [?].

To protect smart meter anonymity, pseudo-identity generation techniques have continuously evolved. In 2021, Azeem et al. [?] proposed a lightweight

authenticated key scheme for smart grid demand response management that used hash functions to generate pseudo-identities to ensure anonymity and supported pseudo-identity updates. However, due to the one-way irreversibility of hash functions, their scheme did not support pseudo-identity tracing. In 2022, Safkhani et al. [**?**] proposed an authentication and key agreement scheme for smart grids that used physically unclonable functions (PUF) and symmetric encryption to construct user pseudo-identities, ensuring anonymity, but their scheme did not support pseudo-identity updates or tracing. Gope et al.' s scheme [**?**] performed identity authentication among power suppliers, smart meters, and third-party aggregators before smart meters uploaded user consumption data, ensuring communication entity legitimacy. The scheme used symmetric encryption to construct pseudo-identities for smart meter anonymity, resisted common known attacks, and achieved lightweight authentication among communication entities using low-cost cryptographic primitives. However, this paper' s security analysis reveals that Gope et al.' s scheme cannot resist key compromise impersonation attacks and has weak session key security.

---

## 2 Preliminaries

This section introduces the computational hardness assumptions and system model required to understand the proposed scheme.

### 2.1 Computational Hardness Assumptions

**Elliptic Curve Discrete Logarithm Problem (ECDLP):** Let $p$ be a large prime and $G$ be an additive cyclic group of order $q$. For given $P, aP \in G$, computing $a \in Z_q^*$ is hard.

**Elliptic Curve Diffie-Hellman Problem (ECDHP):** For given $P, aP, bP \in G$, computing $abP \in G$ is hard, where $a, b \in Z_q^*$.

### 2.2 System Model

As shown in Figure 1, based on existing models [**?**, **?**], this paper proposes a system model containing four communication entities: Power Supplier ($PS$), Gateway ($GW$), Smart Meter ($SM_i$) in the corresponding home local area network, and Auxiliary Validator ($AV$).

[Figure 1: see original paper] System model

a) **Power Supplier ($PS$).** As the administrator of the entire smart grid, $PS$ is primarily responsible for generating and distributing security parameters, monitoring and analyzing aggregated consumption data from gateways, and adjusting electricity prices. Compared with [**?**, **?**], $PS$ in this scheme only provides registration services and does not participate

in identity authentication and key agreement between smart meters and gateways.

b) **Gateway ($GW$).** With large storage space and excellent computing capabilities, $GW$ collects and aggregates encrypted consumption data from smart meters in its responsible area and sends the processed data to $PS$. This is a semi-trusted third-party entity that is honest but curious about encrypted consumption data from smart meters. After receiving aggregation requests from $AV$, $GW$ authenticates $AV$' s identity and initiates mutual authentication with smart meters to establish session keys.

c) **Smart Meter ($SM_i$).** As terminal devices in smart grids, smart meters periodically collect and encrypt user consumption data. These are resource-constrained intelligent devices with limited storage space and computing capabilities.

d) **Auxiliary Validator ($AV$).** This is a third-party tamper-resistant intelligent device that registers with $PS$ to obtain relevant security parameters. After receiving consumption data collection instructions from $PS$, $AV$ sends aggregation requests to $GW$. $GW$ must authenticate $AV$ before negotiating session keys with smart meters.

### 2.3 Security Goals

A secure and efficient smart grid identity authentication and key agreement scheme should provide robust security for communication entities and achieve the following security objectives:

a) **Mutual Authentication:** To ensure that smart meter data is uploaded to authorized gateways and that gateways receive encrypted consumption data from legitimate smart meters, mutual authentication should be provided between smart meters and gateways.

b) **Smart Meter Anonymity and Untraceability:** Ensure that attackers cannot trace the real identity of smart meters or any activities of smart meters in the communication network.

c) **Session Key Forward Secrecy:** Ensure the security of previously established session keys even if attackers obtain long-term secret parameters of gateways and smart meters.

d) **Resistance to Key Compromise Impersonation Attacks:** Even if the private key of either the gateway or smart meter is compromised, attackers cannot impersonate the compromised party to communicate with the other party.

e) **Resistance to Various Known Attacks:** The scheme should resist impersonation attacks, replay attacks, man-in-the-middle attacks, and smart meter temporary secret value leakage attacks.

### 2.4 Attacker Model

This paper combines the Dolev-Yao threat model and CK attacker model to construct a powerful attacker with the following capabilities within probabilistic polynomial time:

a) Can arbitrarily eavesdrop, intercept, modify, delete, and inject messages on communication channels.

b) Can obtain previous session keys of the system.

c) When evaluating resistance to key compromise impersonation attacks, can obtain private keys of communication entities.

---

## 3 Security Analysis of Gope et al.' s Scheme

This section reviews the authentication phase of Gope et al.' s scheme and analyzes its security vulnerabilities.

### 3.1 Review of Gope et al.' s Authentication Phase

The Power Supplier ($PS$) generates pseudo-identities $PID_i$ and private keys $k_i$ for each smart meter ($SM_i$) in the home local area network, and shares private key $K_{as}$ with the Third-Party Aggregator ($TPA$). Before collecting user consumption data, $PS$, $TPA$, and $SM_i$ perform mutual authentication among the three parties through the following process:

a) $SM_i$ generates random number $r_i$, computes $TID_i = h(T_i||ID_{SM_i}||r_i)$, $V_1 = h(TID_i||s_i||k_i)$, and sends message $M_1 = \{TID_i, V_1, T_i\}$ to $TPA$.

b) $TPA$ generates random number $r_a$, computes $TID_a = h(T_a||ID_{TPA}||r_a)$, $V_2 = h(TID_a||s_a||K_{as})$, $V_3 = h(TID_i||TID_a||K_{as})$, and sends message $M_2 = \{TID_i, TID_a, V_2, V_3, T_a\}$ to $PS$.

c) $PS$ locates the real identity $ID_{SM_i}$ corresponding to pseudo-identity $PID_i$ in its database, verifies the correctness of $V_2$ and $V_3$, and upon successful verification, authenticates $TPA$' s identity. $PS$ generates a new pseudo-identity $PID_i^{new}$ for $SM_i$, computes session key $SK = h(TID_i||TID_a||K_{as})$, $V_4 = h(TID_i||SK)$, encrypts $SM_i$' s temporary identity using $SK$ to obtain $E_{SK}[PID_i^{new}]$, and sends message $M_3 = \{V_4, E_{SK}[PID_i^{new}]\}$ to $TPA$.

d) $TPA$ verifies the correctness of $V_4$, and upon successful verification, authenticates $PS$' s identity, computes session key $SK = h(TID_i||TID_a||K_{as})$, generates a set $Q_i = q_i \cdot P$, uses $SK$ to encrypt $SM_i$' s temporary identity $PID_i^{new}$ and stores it, then sends message $M_4 = \{Q_i, TID_i, T_a\}$ to $SM_i$.

e) $SM_i$ verifies the correctness of $V_1$, and upon successful verification, authenticates $TPA$' s aggregator identity, computes session key $SK = h(TID_i||TID_a||k_i)$, and finally uses $SK$ to decrypt $E_{SK}[PID_i^{new}]$ and stores the parameters.

### 3.2 Security Vulnerabilities in Gope et al.' s Scheme

This section demonstrates that Gope et al.' s authentication phase cannot resist key compromise impersonation attacks launched by the attacker $\mathcal{A}$ constructed in Section 2.4, nor can it provide session key security.

The attacker $\mathcal{A}$ eavesdrops on communication channels between $SM_i$ and $TPA$ and between $TPA$ and $PS$, and obtains parameters $\{TID_i, V_1, T_i, TID_a, V_2, V_3, T_a, V_4, E_{SK}[PID_i^{new}], Q_i\}$. Assuming [**?**] that $\mathcal{A}$ can obtain the shared private key $K_{as}$ between $PS$ and $TPA$, $\mathcal{A}$ can impersonate $TPA$ to communicate with $SM_i$ and $PS$. The specific attack process is as follows:

a) $\mathcal{A}$ eavesdrops and intercepts message $M_2$, generates random number $r_a^*$, computes $TID_a^* = h(T_a^*||ID_{TPA}||r_a^*)$, $V_2^* = h(TID_a^*||s_a||K_{as})$, $V_3^* = h(TID_i||TID_a^*||K_{as})$, and sends message $M_2^* = \{TID_i, TID_a^*, V_2^*, V_3^*, T_a^*\}$ to $PS$.

b) Based on pseudo-identity $PID_i$, $PS$ locates the real identity $ID_{SM_i}$ and verifies the correctness of $V_2^*$ and $V_3^*$. Successful verification indicates that $PS$ authenticates $TPA$' s aggregator identity. $PS$ generates a new pseudo-identity $PID_i^{new}$ for $SM_i$, computes session key $SK^* = h(TID_i||TID_a^*||K_{as})$, $V_4^* = h(TID_i||SK^*)$, encrypts $SM_i$' s temporary identity using $SK^*$ to obtain $E_{SK^*}[PID_i^{new}]$, and sends message $M_3^* = \{V_4^*, E_{SK^*}[PID_i^{new}]\}$ to $\mathcal{A}$.

c) $\mathcal{A}$ verifies the correctness of $V_4^*$, and upon successful verification, authenticates $PS$' s identity, computes session key $SK^* = h(TID_i||TID_a^*||K_{as})$, forges a temporary identity set $\{Q_i^*, TID_i, T_a^*\}$ for $SM_i$, encrypts $PID_i^{new}$ using $SK^*$ and stores it, then sends message $M_4^* = \{Q_i^*, TID_i, T_a^*\}$ to $SM_i$.

d) $SM_i$ verifies the correctness of $V_1$, and upon successful verification, authenticates $\mathcal{A}$' s identity, computes session key $SK = h(TID_i||TID_a||k_i)$, and finally uses $SK$ to decrypt $E_{SK}[PID_i^{new}]$ and stores the parameters.

In summary, $\mathcal{A}$ successfully impersonates $TPA$ to communicate with $PS$ and $SM_i$, demonstrating that Gope et al.' s scheme cannot resist key compromise impersonation attacks. Moreover, when the shared private key $K_{as}$ between $PS$ and $TPA$ is compromised, $\mathcal{A}$ can successfully compute the session key $SK$, proving that Gope et al.' s scheme cannot provide session key security.

---

## 4 Proposed Scheme and Correctness Proof

To resist the security vulnerabilities in [**?**] and ensure communication security in smart grids, this paper proposes an enhanced provably secure identity authentication and key agreement scheme. The scheme consists of four phases: initialization, registration, identity authentication and key agreement, and malicious smart meter revocation.

### 4.1 Initialization

In this phase, the Power Supplier $PS$ initializes and generates the following parameters:

a) Select large primes $p$ and $q$, choose an elliptic curve $E$ over finite field $F_p$ based on $p$, and select point $P$ as the base point of order $q$ on elliptic curve $E$.

b) Select random number $sk_{PS} \in Z_q^*$ as $PS$' s private key and compute $pk_{PS} = sk_{PS} \cdot P$ as $PS$' s public key.

c) Select secure one-way hash function $h(\cdot)$ and symmetric encryption/decryption algorithm $(Enc_k(\cdot), Dec_k(\cdot))$, where $k$ is the encryption/decryption key.

Finally, $PS$ publishes parameters $\{p, q, E, P, pk_{PS}, h(\cdot), Enc_k(\cdot), Dec_k(\cdot)\}$.

### 4.2 Registration

In this phase, the Auxiliary Validator ($AV$), Gateway ($GW$), and the $i$-th Smart Meter ($SM_i$) register with $PS$ to obtain parameters for the next phase, transmitted through secret channels.

#### 4.2.1 $AV$ Registration

a) $AV$ selects identity identifier $ID_{AV}$ and sends registration request $\{ID_{AV}\}$ to $PS$.

b) $PS$ selects random number $r_{AV} \in Z_q^*$ as $AV$' s private key, computes $R_{AV} = r_{AV} \cdot P$, and sends $\{r_{AV}, R_{AV}\}$ to $AV$ through a secret channel.

c) After registration, $AV$ stores parameters $\{ID_{AV}, r_{AV}, R_{AV}\}$.

#### 4.2.2 $GW$ Registration

a) $GW$ selects identity identifier $ID_{GW}$ and sends registration request $\{ID_{GW}\}$ to $PS$.

b) $PS$ computes $B_1 = h(ID_{GW}||pk_{PS})$, selects random number $s_{GW} \in Z_q^*$ as $GW$' s private key, computes $sk_{GW} = s_{GW} + pk_{PS} \cdot B_1$ as $GW$' s private key and $pk_{GW} = sk_{GW} \cdot P$ as $GW$' s public key, and sends $\{sk_{GW}, pk_{GW}\}$ to $GW$ through a secret channel.

c) After registration, $GW$ stores parameters $\{ID_{GW}, sk_{GW}, pk_{GW}\}$.

#### 4.2.3 $SM_i$ Registration

a) $SM_i$ selects identity identifier $ID_{SM_i}$ and sends registration request $\{ID_{SM_i}\}$ to $PS$.

b) $PS$ selects random number $s_i \in Z_q^*$ as $SM_i$' s authentication token, selects random number $r_i \in Z_q^*$ as $SM_i$' s private key, computes $sk_{SM_i} = r_i + pk_{PS} \cdot s_i$ as $SM_i$' s private key and $pk_{SM_i} = sk_{SM_i} \cdot P$ as $SM_i$' s public key, encrypts $SM_i$' s real identity identifier $ID_{SM_i}$ using $sk_{SM_i}$ to obtain $PID_i = Enc_{sk_{SM_i}}(ID_{SM_i}||r_i)$ as $SM_i$' s pseudo-identity, and sends $\{s_i, sk_{SM_i}, pk_{SM_i}, PID_i\}$ to $SM_i$ through a secret channel.

c) After registration, $SM_i$ generates its own private and public keys, and finally stores parameters $\{ID_{SM_i}, s_i, sk_{SM_i}, pk_{SM_i}, PID_i\}$.

### 4.3 Identity Authentication and Key Agreement

In this phase, the Auxiliary Validator $AV$ sends a user consumption data aggregation request to Gateway $GW$. $GW$ authenticates $AV$' s identity, and upon successful verification, initiates mutual authentication with Smart Meter $SM_i$ and negotiates a session key.

a) $AV$ generates random number $N_{AV} \in Z_q^*$, computes $Q_{AV} = N_{AV} \cdot P$, $V_{AV} = h(ID_{AV}||R_{AV}||Q_{AV})$, and sends message $M_1 = \{ID_{AV}, Q_{AV}, V_{AV}\}$ to $GW$.

b) $GW$ verifies whether $V_{AV} = h(ID_{AV}||R_{AV}||Q_{AV})$ holds. If valid, $AV$' s identity is authenticated. $GW$ generates random number $N_{GW} \in Z_q^*$, computes $Q_{GW} = N_{GW} \cdot P$, $V_{GW} = h(ID_{GW}||pk_{GW}||Q_{GW})$, and sends message $M_2 = \{ID_{GW}, Q_{GW}, V_{GW}\}$ to $SM_i$.

c) $SM_i$ verifies whether $V_{GW} = h(ID_{GW}||pk_{GW}||Q_{GW})$ holds. If valid, $GW$' s identity is authenticated. $SM_i$ performs pseudo-identity update, uses its private key $sk_{SM_i}$ to decrypt $PID_i$ and obtain its real identity identifier $ID_{SM_i}$, generates a new pseudo-identity $PID_i^{new} = Enc_{sk_{SM_i}}(ID_{SM_i}||r_i^{new})$ for the next session, computes session key $SK = h(Q_{GW}||Q_{SM_i}||sk_{SM_i} \cdot Q_{GW})$, generates authentication token $V_{SM_i} = h(PID_i^{new}||SK)$, and sends message $M_3 = \{PID_i^{new}, V_{SM_i}\}$ to $GW$.

d) $GW$ generates session key $SK = h(Q_{GW}||Q_{SM_i}||sk_{GW} \cdot Q_{SM_i})$, verifies whether $V_{SM_i} = h(PID_i^{new}||SK)$ holds. If valid, $SM_i$' s identity is authenticated, and $GW$ updates its pseudo-identity to $PID_i^{new}$ for the next authentication.

$GW$ and $SM_i$ store session key $SK$ for further interactions between them.

### 4.4 Malicious Smart Meter Revocation

When $GW$ detects malicious behavior from a smart meter in its jurisdiction, such as sending incorrect authentication information or abnormal power consumption data, it sends a traceability request to $PS$. After reviewing the smart meter' s data and behavior, $GW$ sends the malicious smart meter' s pseudo-identity $PID_i$ to $PS$ for tracing. Since smart meter pseudo-identities are generated by $PS$, only $PS$ can trace them.

$PS$ decrypts the malicious smart meter' s pseudo-identity $PID_i$ to reveal its real identity and transmits this information through a secret channel to $GW$. $GW$ adds the malicious smart meter' s real identity and pseudo-identity to a revocation list, which can be queried by all members of the communication system to avoid interaction with listed malicious smart meters.

### 4.5 Correctness Proof

To prove that the session key $SK_{GW}$ generated by $GW$ equals the session key $SK_{SM_i}$ generated by $SM_i$, we need to prove that $h(Q_{GW}||Q_{SM_i}||sk_{GW}\cdot Q_{SM_i}) = h(Q_{GW}||Q_{SM_i}||sk_{SM_i}\cdot Q_{GW})$. The proof is shown by the following equations:

$$sk_{GW}\cdot Q_{SM_i} = sk_{GW}\cdot(N_{SM_i}\cdot P) = N_{SM_i}\cdot(sk_{GW}\cdot P) = N_{SM_i}\cdot pk_{GW}$$

$$sk_{SM_i}\cdot Q_{GW} = sk_{SM_i}\cdot(N_{GW}\cdot P) = N_{GW}\cdot(sk_{SM_i}\cdot P) = N_{GW}\cdot pk_{SM_i}$$

Since $pk_{GW} = sk_{GW}\cdot P$ and $pk_{SM_i} = sk_{SM_i}\cdot P$, we have:

$$sk_{GW}\cdot Q_{SM_i} = N_{SM_i}\cdot pk_{GW} = N_{SM_i}\cdot(sk_{GW}\cdot P) = sk_{GW}\cdot(N_{SM_i}\cdot P) = sk_{GW}\cdot Q_{SM_i}$$

$$sk_{SM_i}\cdot Q_{GW} = N_{GW}\cdot pk_{SM_i} = N_{GW}\cdot(sk_{SM_i}\cdot P) = sk_{SM_i}\cdot(N_{GW}\cdot P) = sk_{SM_i}\cdot Q_{GW}$$

Therefore, $SK_{GW} = SK_{SM_i}$, and the correctness is proven.

---

## 5 Formal Security Analysis in Random Oracle Model

Using security models for formal analysis has become one of the most powerful security proofs in modern cryptography. Among existing security models, this paper employs the random oracle model to conduct formal analysis of the proposed scheme.

### 5.1 Security Model

In the identity authentication and key agreement phase of this scheme, $GW$ and $SM_i$ are the two main participants. Assume each $GW$ and $SM_i$ can run multiple sessions. Let $\Pi_{GW}^{i}$ denote $GW$' s $i$-th session instance and $\Pi_{SM_i}^{j}$ denote $SM_i$' s $j$-th session instance. Each session instance is called an oracle. When an attacker queries an oracle, the oracle must return corresponding response parameters.

Define instance $\Pi_U^i$, where $U \in \{GW, SM_i\}$. In the random oracle model, $\Pi_U^i$ represents one of the two session instances $\Pi_{GW}^i$ and $\Pi_{SM_i}^j$. A probabilistic polynomial-time attacker $\mathcal{A}$ can arbitrarily eavesdrop, intercept, modify, delete, and inject messages on communication channels. Its attack capabilities are demonstrated through the following oracle queries:

- **Execute($\Pi_U^i$):** This query simulates $\mathcal{A}$' s passive attacks, allowing $\mathcal{A}$ to obtain all messages from communication parties on public channels.
- **Send($\Pi_U^i$, $M$):** This query simulates $\mathcal{A}$' s active attacks. $\mathcal{A}$ sends message $M$ obtained from communication channels to $\Pi_U^i$, which returns corresponding messages.
- **Corrupt($\Pi_U^i$):** This query enables $\mathcal{A}$ to obtain instance $\Pi_U^i$' s long-term secret parameters.
- **Test($\Pi_U^i$):** This query simulates the semantic security of instance $\Pi_U^i$' s session key. After the Test query, $\Pi_U^i$ flips a coin $b$. If $b = 1$ (heads), $\Pi_U^i$ returns the real session key to $\mathcal{A}$; if $b = 0$ (tails), it returns a random string of equal length.

**Security Definition:** This scheme' s security is evaluated through game $G_i$ ($i = 0, 1, 2, 3, 4, 5$). In the game, $\mathcal{A}$ can launch multiple queries to $\Pi_U^i$. $\mathcal{A}$ flips a coin $b$ (resulting in 0 or 1). If $\mathcal{A}$ correctly guesses the $b$ value, it wins the game. The advantage of attacker $\mathcal{A}$ in breaking this scheme' s security is defined as $Adv_{\mathcal{A}}^S = |2 \cdot Pr[Succ_{\mathcal{A}}] - 1|$, where $Pr[Succ_{\mathcal{A}}]$ is the probability that $\mathcal{A}$ correctly guesses the coin value $b$ in game $G_i$, and $\varepsilon$ is a negligible value.

### 5.2 Security Analysis

**Theorem 1.** The probability that attacker $\mathcal{A}$ wins game $G_i$ within probabilistic polynomial time is negligible. If $\mathcal{A}$ can execute at most $q_h$ hash queries and $q_{send}$ Send queries, the maximum advantage of $\mathcal{A}$ in breaking scheme $S$' s security is $Adv_{\mathcal{A}}^S \leq \frac{q_h^2}{2 \cdot |Hash|} + \frac{q_{send}^2}{2 \cdot |Hash|} + 2 \cdot Adv_{\mathcal{A}}^{ECDLP}$, where $|Hash|$ is the hash query size and $Adv_{\mathcal{A}}^{ECDLP}$ represents $\mathcal{A}$' s advantage in solving ECDLP.

**Proof.** Let $Pr[Succ_{\mathcal{A}}^{G_i}]$ denote the probability that $\mathcal{A}$ correctly guesses the coin value $b$ in game $G_i$, and $Adv_{\mathcal{A}}^S$ denote $\mathcal{A}$' s advantage in breaking scheme $S$.

**Game $G_0$:** This game simulates a real attack scenario, yielding $Pr[Succ_{\mathcal{A}}^{G_0}] = Pr[Succ_{\mathcal{A}}]$.

**Game $G_1$:** This game simulates $\mathcal{A}$' s passive attacks through Execute queries. $\mathcal{A}$ obtains messages $M_1 = \{ID_{AV}, Q_{AV}, V_{AV}\}$, $M_2 = \{ID_{GW}, Q_{GW}, V_{GW}\}$, and $M_3 = \{PID_i^{new}, V_{SM_i}\}$ through eavesdropping, but cannot compute session key $SK$ from these messages. Therefore, compared with the real attack scenario, $\mathcal{A}$ gains no additional advantage in this game, so $Pr[Succ_{\mathcal{A}}^{G_1}] = Pr[Succ_{\mathcal{A}}^{G_0}]$.

**Game $G_2$:** This game removes two collision scenarios present in $G_1$ and simulates $\mathcal{A}$' s active attacks.

- **Scenario 1:** According to the birthday paradox [**?**], the probability of hash query output collisions is less than or equal to $\frac{q_h^2}{2\cdot|Hash|}$.
- **Scenario 2:** The probability of collisions in selected random numbers is less than or equal to $\frac{q_{send}^2}{2\cdot|Hash|}$.

Unless the above collisions occur, $G_2$ and $G_1$ are indistinguishable. Therefore:

$$|Pr[Succ_{\mathcal{A}}^{G_2}] - Pr[Succ_{\mathcal{A}}^{G_1}]| \leq \frac{q_h^2}{2\cdot|Hash|} + \frac{q_{send}^2}{2\cdot|Hash|}$$

**Game $G_3$:** This game removes from $G_2$ the scenario where $\mathcal{A}$ guesses authentication tokens $V_{SM_i}$ or $V_{GW}$ without hash queries. The probability of this scenario is less than or equal to $\frac{q_{send}}{|Hash|}$.

**Game $G_4$:** This game removes from $G_3$ the scenario where $\mathcal{A}$ successfully decrypts to obtain $ID_{SM_i}$. Therefore:

$$|Pr[Succ_{\mathcal{A}}^{G_4}] - Pr[Succ_{\mathcal{A}}^{G_3}]| \leq Adv_{\mathcal{A}}^{E_k}$$

**Game $G_5$:** This game modifies $G_4$ to simulate $\mathcal{A}$' s key compromise impersonation attacks. $\mathcal{A}$ executes Corrupt queries to obtain long-term secret parameters of $GW$ and $SM_i$. Under the condition that $\mathcal{A}$ obtains $sk_{GW}$ and $sk_{SM_i}$, to obtain $SM_i$' s session key, $\mathcal{A}$ must compute $sk_{GW} \cdot Q_{SM_i}$ from $Q_{SM_i}$, which requires solving the Elliptic Curve Discrete Logarithm Problem (ECDLP). The same applies to $GW$. Therefore, comparing this game with $G_4$, we need to compute:

$$|Pr[Succ_{\mathcal{A}}^{G_5}] - Pr[Succ_{\mathcal{A}}^{G_4}]| \leq Adv_{\mathcal{A}}^{ECDLP}$$

In this game, $\mathcal{A}$ gains no advantage in guessing the $b$ value, so:

$$Pr[Succ_{\mathcal{A}}^{G_5}] = \frac{1}{2}$$

From equations (3) and (4), we obtain:

$$Pr[Succ_{\mathcal{A}}^{G_4}] \leq \frac{1}{2} + Adv_{\mathcal{A}}^{ECDLP}$$

From equations (5) to (8) and the triangle inequality, we obtain:

$$Adv_{\mathcal{A}}^{S} = |2 \cdot Pr[Succ_{\mathcal{A}}] - 1| \leq \frac{q_h^2}{2\cdot|Hash|} + \frac{q_{send}^2}{2\cdot|Hash|} + 2 \cdot Adv_{\mathcal{A}}^{ECDLP}$$

Thus, Theorem 1 is proved. The above proof process means that $\mathcal{A}$'s probability of winning the game is negligible. Therefore, this scheme is secure under the random oracle model.

## 6 ProVerif Simulation Analysis

ProVerif is a widely used automated cryptographic protocol verification tool that supports various cryptographic primitives such as encryption, decryption, digital signatures, and hash functions, along with specified rewriting rules and equations. The tool can prove reachability, authentication, and observational equivalence. It consists of three components: protocol input, system processing, and result output. The system input uses Pi calculus or Horn logic to encode protocols, the system processing uses first-order logic to derive security properties of encoded protocols, and the result output can provide corresponding attack sequences when the encoded protocol fails to satisfy specific security properties. Additionally, ProVerif includes an attacker model capable of eavesdropping, intercepting, modifying, or retransmitting messages, with these actions limited only by encryption methods.

This paper models the proposed scheme in ProVerif across four different scenarios to prove its resistance to known attacks and further verify its smart meter anonymity and session key forward secrecy.

**Scenario 1:** Without leaking any secret parameters, the scheme is modeled in ProVerif and queried for common attacks. This proves smart meter anonymity and scheme reachability. The simulation results are shown in Figure 2 [Figure 2: see original paper]. Result  queries scheme reachability, proving session key security; Result  proves smart meter anonymity; Results  and  demonstrate that smart meters and gateways can achieve mutual authentication and resist common attacks such as impersonation, replay, and man-in-the-middle attacks.

**Scenario 2:** This scenario verifies that the scheme provides session key forward secrecy. Using the command to leak long-term secret parameters of the session key to the attacker, the query results are shown in Figure 3 [Figure 3: see original paper]. The attacker fails to obtain the session key.

**Scenario 3:** This scenario verifies the scheme' s resistance to key compromise impersonation attacks. Using the command to leak the private keys of smart meters and gateways to the attacker, the query results are shown in Figure 4 [Figure 4: see original paper]. The attacker fails to obtain the session key.

**Scenario 4:** This scenario verifies the scheme' s resistance to smart meter temporary secret value leakage. Using the command to leak temporary secret values of smart meters to the attacker, the query results are shown in Figure 5 [Figure 5: see original paper]. The attacker fails to obtain the session key.

---

## 7 Performance Analysis

This section analyzes the proposed scheme' s performance in terms of security, computational cost, and communication overhead, comparing it with schemes from [?, ?, ?, ?, ?, ?, ?].

As shown in Table 1 , in terms of security, the proposed scheme provides mutual authentication, smart meter anonymity and untraceability, session key security, and resistance to various known attacks. Gope et al.'s scheme [**?**] cannot provide mutual authentication or session key security and cannot resist key compromise impersonation attacks. Other schemes [**?**, **?**, **?**, **?**, **?**, **?**] also have various security flaws. Therefore, the proposed scheme is superior to existing schemes in terms of security.

Computational costs are compared using experimental results from [**?**] obtained on Ubuntu 12.04.1 LTS 32-bit operating system. The computational costs are: hash operation $T_h \approx 0.0023$ms; symmetric encryption/decryption $T_e \approx 0.0046$ms; ECC point multiplication $T_m \approx 2.226$ms; ECC point addition $T_a \approx 0.0288$ms; exponentiation $T_{exp} \approx 3.85$ms; bilinear pairing $T_p \approx 5.811$ms. Some operations with negligible costs are ignored [**?**]. Communication overhead is the total number of bits transmitted during protocol execution. Lower communication overhead enables faster data transmission and reduced latency. To calculate communication overhead, we assume identity identifiers, random numbers, hash outputs, timestamps, and symmetric encryption/decryption blocks are 160 bits; points on elliptic curves are 320 bits; and bilinear mapping group generators are 1024 bits. Table 2 shows the comparison results for computational cost and communication overhead.

In terms of computational cost, the proposed scheme primarily uses lightweight operations such as hash functions and binary operations, supplemented by ECC point multiplication and symmetric encryption/decryption, achieving a computational cost of 8.9523ms. Schemes [**?**, **?**] adopt bilinear pairing and exponentiation operations, significantly increasing computational overhead. Schemes [**?**, **?**, **?**] mainly use ECC point multiplication, but the number of ECC point multiplication operations exceeds that of the proposed scheme. The proposed scheme reduces computational cost by 74.4%, 70.8%, 60.0%, 33.4%, and 42.7% compared with [**?**, **?**, **?**, **?**, **?**], respectively. Although Gope et al.' s scheme [**?**] primarily uses hash functions without additional high-cost operations, resulting in lower computational cost, Table 1 shows that their scheme' s use of lightweight cryptographic primitives leads to insufficient security, making it vulnerable to attacks. Moreover, Gope et al.' s scheme does not support pseudo-identity updates and tracing, whereas the proposed scheme can generate new smart meter pseudo-identities during sessions and distribute them to *GW* for use in the next session. Additionally, the proposed scheme can trace the real identity of malicious smart meters through pseudo-identities and revoke them.

In terms of communication overhead, the proposed scheme reduces message transmission rounds during authentication to 3, achieving streamlined communication with only 1760 bits. In contrast, Gope et al.' s scheme [**?**] requires 4 message transmissions during authentication, resulting in 3040 bits of communication overhead. The proposed scheme reduces communication overhead by 42.1%, 50.5%, 52.6%, 21.4%, 15.4%, and 9.0% compared with [**?**, **?**, **?**, **?**, **?**, **?**], respectively, significantly reducing communication latency.

## 8 Conclusion

This paper addresses the problems of insufficient security and low efficiency in existing smart grid communication authentication schemes. It analyzes and proves security vulnerabilities in Gope et al.' s scheme and proposes an identity authentication and key agreement scheme for smart grids based on elliptic curve cryptography. The proposed scheme' s security is verified through the ProVerif simulation tool and theoretical analysis. Comparison with similar authentication schemes demonstrates advantages in security, computational cost, and communication overhead, meeting smart grid requirements for security and efficiency in communication processes.

The proposed scheme only supports one-to-one single-point authentication from gateway to smart meter, where the gateway' s computational cost grows linearly with the number of smart meters in its jurisdiction. As smart meter deployment becomes more comprehensive, gateways may need to provide large numbers of authentication services simultaneously, resulting in high network latency and posing a significant challenge to gateway computing capabilities. Future work will investigate batch authentication where a single gateway authenticates multiple smart meters simultaneously to reduce gateway computational burden.

## References

[1] Sadhukhan D, Ray S, Obaidat M S, et al. A secure and privacy preserving lightweight authentication scheme for smart-grid communication using elliptic curve cryptography [J]. Journal of Systems Architecture, 2021, 114: 101938.

[2] Ferrag M A, Maglaras L A, Janicke H, et al. A systematic review of data protection and privacy preservation schemes for smart grid communications [J]. Sustainable Cities and Society, 2018, 38: 806–835.

[3] Mahmood K, Chaudhry S A, Naqvi H, et al. A lightweight message authentication scheme for smart grid communications in power sector [J]. Computers & Electrical Engineering, 2016, 52 (C): 114-124.

[4] Li Xiong, Wu Fan, Saru K, et al. A provably secure and anonymous message authentication scheme for smart grids [J]. Journal of Parallel and Distributed Computing, 2019, 132: 242-249.

[5] Dua A, Kumar N, Singh M, et al. Secure message communication among vehicles using elliptic curve cryptography in smart cities [C]// Proc of International Conference on Computer Information Telecommunication Systems. Kunmin, NJ: IEEE Press, 2016: 1–6.

[6] Wang Wenye, Lu Zhou. Cyber security in the smart grid: survey and challenges [J]. Computer Networks, 2013, 57 (5): 1344–1371.

[7] Gope P, Sikdar B. Lightweight and privacy-friendly spatial data aggregation for secure power supply and demand management in smart grids [J]. IEEE Trans on Information Forensics and Security, 2019, 14 (6): 1554-1566.

[8] Wu Libing, Wang Jing, Sherali Z, et al. Anonymous and efficient message authentication scheme for smart grid [J]. IEEE Access, 2021, 9: 4425-4436.

[9] Tsai J L, Lo N W. Secure anonymous key distribution scheme for smart grid [J]. IEEE Trans on Smart Grid, 2016, 7 (2): 906-914.

[10] Odelu V, Das A K, Wazid M, et al. Provably secure authenticated key agreement scheme for smart grid [J]. IEEE Trans on Smart Grid, 2018, 9 (3): 1900-1910.

[11] Chen Yuwen, Martínez J F, Castillejo P, et al. An anonymous authentication and key establish scheme for smart grid: FAuth [J]. Energies, 2017, 10 (9): 1354-1377.

[12] He Debiao, Wang Huaqun, Khan M K, et al. Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography [J]. Iet Communications, 2016, 10 (14): 1795-1802.

[13] Abbasinezhad M D, Ostad S A, Nikooghadam M. et al. A secure and efficient key establishment scheme for communications of smart meters and service providers in smart grid [J]. IEEE Trans on Industrial Informatics, 2020, 16 (3): 1495-1502.

[14] Fan Wu, Xu Lili, Li Xiong, et al. A lightweight and provably secure key agreement system for a smart grid with elliptic curve cryptography [J]. IEEE Systems Journal, 2019, 13 (3): 2830-2838.

[15] Garg S, Kaur K, Kaddoum G, et al. Secure and lightweight authentication scheme for smart metering infrastructure in smart grid [J]. IEEE Trans on Industrial Informatics, 2020, 16 (5): 3548-3557.

[16] Fatty S, Osama E. A lightweight authenticated key establishment scheme for secure smart grid communications [J]. International Journal of Safety and Security Engineering, 2020, 10 (4): 549-558.

[17] Srinivas J, Das A K, Li Xiong, et al. Designing anonymous signature-based authenticated key exchange scheme for internet of things-enabled smart grid systems [J]. IEEE Trans on Industrial Informatics, 2021, 17 (7): 4425-4436.

[18] Tanveer M, Khan A U, Shah H, et al. ARAP-SG: Anonymous and reliable authentication protocol for smart grids [J]. Security and Communication Networks, 2019: 1-12.

[19] Azeem I, Shehzad A C, Mamoun A, et al. A secure demand response management authentication scheme for smart grid [J]. Sustainable Energy Technologies

and Assessments, 2021, 48: 101571.

[20] Safkhani M, Kumari S, Shojafar M, et al. An authentication and key agreement scheme for smart grid [J]. Peer-to-Peer Networking and Applications, 2022, 15: 1595–1616.

[21] Huang Chengpeng, Wang Xiaoming, Gan Qingqing, et al. A lightweight and fault-tolerable data aggregation scheme for privacy-friendly smart grids environment [J]. Cluster Computing, 2021, 24: 3495–3514.

[22] Daniel R M, Rajsingh E B, Silas S. An efficient eCK secure identity based two party authenticated key agreement scheme with security against active adversaries [J]. Information and Computation, 2020, 275: 104603.

[23] 齐小晨, 黎妹红, 杜晔. 多服务器环境下基于动态 ID 的轻量级身份认证协议 [J]. 北京航空航天大学学报, 2021, 47 (12): 2632-2640. (Qi Xiaochen, Li Meihong, Du Ye. Lightweight identity authentication protocol based on dynamic ID in multi-server environment [J]. Journal of Beijing University of Aeronautics and Astronautics, 2021, 47 (12): 2632-2640.)

[24] Kilinc H H, Yanik T. A survey of sip authentication and key agreement schemes [J]. IEEE Communications Surveys & Tutorials, 2014, 16 (2): 998-1017.

[25] 李晓天, 陈建华. 更安全的匿名三因子多服务器身份认证协议研究 [J]. 计算机应用研究, 2020, 37 (9): 2781-2788. (Li Xiaotian, Chen Jianhua. Research on security-enhanced three-factor multi-server authentication scheme with anonymity [J]. Application Research Of Computers, 2020, 37 (9): 2781-2788.)

*Note: Figure translations are in progress. See original paper for figures.*