Journal of Network Intelligence
Taiwan Ubiquitous Information
 ISSN 2414-8105 (Online)
Volume **6**, Number **2**, May **2021**

An Anonymous Authentication and Key Exchange Protocol in Smart Grid

Yi Luo

Fujian Provincial Key Laboratory of Big Data Mining and Applications
Fujian University of Technology
Fuzhou 350100,China
13961161139@163.com

Wei-min Zheng*

College of Computer Science and Engineering
Shandong University of Science and Technology
Qingdao 266590, P.R. China
* Corresponding author: zhengweimin@sdust.edu.cn

Yeh-Cheng Chen

Department of Computer Science
University of California, Davis
CA 95616,USA
ycch@ucdavis.edu

Received February 2020; revised April 2021

Abstract. *With the use of a large number of digital devices in smart grid, how to protect the security of communication in Advanced Metering Infrastructure (AMI) has become a difficult problem. AMI plays an important role in smart grid, which is used two-way communication between users and electricity companies. AMI includes smart meters(SM), data collectors, AMI Head-End(AHE), etc. In this paper, we present an authentication and key exchange protocol between the smart meter and the AMI Head-End in smart grid. The security of proposed scheme is proved by random oracle model and BAN logic. At the end of the paper, the performance analysis shows that the scheme is efficient and suitable for AMI.*
Keywords: Authentication, Key exchange, Smart grid, Cryptanalysis.

1. **Introduction.** Smart meter is a digital device in smart grid, which can provide energy measurement, energy monitoring and energy control. Smart meter collects all the consumption information of users and sends these information to the AHE regularly. The AHE is responsible for data collection and management, so as to further interact with other operating systems and management systems. As Figure 1 shows, messages are delivered via concentrators and possibly other meters. Smart grid can not only monitor users' electricity consumption habits to properly adjust the power generation, but also effectively control the use of electricity to ensure continuous power supply. It is difficult to design an appropriate authentication and key exchange protocol in smart grid because of the different security requirements for complexity and diversity. In the process of system data transmission, it can not only ensure that the instruction received by the smart meter is accurate, but also ensure the identity confidentiality of both sides [1], which is the

biggest challenge in terms of security at present.Compared with other encryption technologies, elliptic curve cryptosystem [2] is more suitable for smart grid environment. In

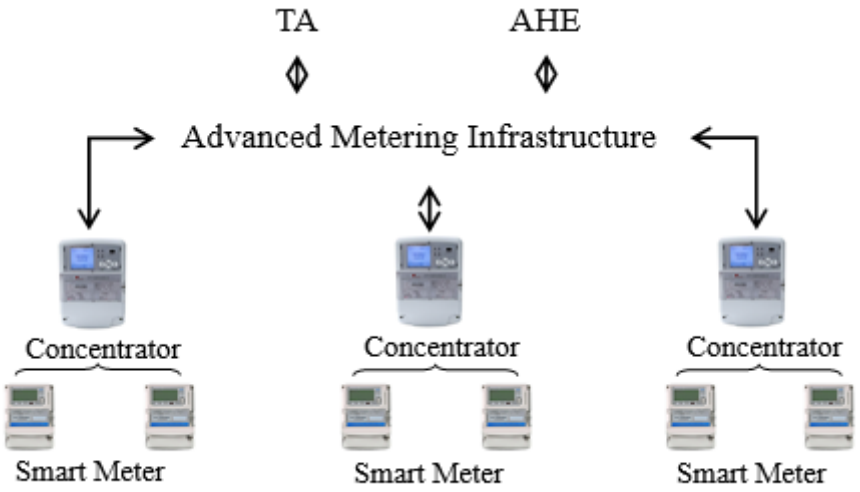

FIGURE 1. Demonstration of the Advanced Metering Infrastructure

2011, Nicanfar et al. [3] proposed an authentication and key exchange protocol deployed on smart meters. However, Mohamadali et al. [4] found that Nicanfar et al's scheme has a security vulnerability, which makes their scheme vulnerable to simulation attacks. Fouda et al. [5] also designed a lightweight scheme, which based on Diffie-Hellman, but their scheme is too complex to realize. In 2013, Nicanfar et al. [6] proposed another scheme using elliptic curve cryptography but the database used to save the password increases the cost of the scheme. In the same year, Liu et al. [7] proposed a key establishment scheme based on key graph. However, Wan et al. [8] analyzed their scheme and showed that it is vulnerable to desynchronization attack.In 2016, Tsai and Lo [9] published a scheme based on bilinear pairing. In their scheme, smart meters can quickly carry out identity verification without the help of trusted authorization. Odelu et al.'s [10] scheme is also based on bilinear pairing and their scheme can provide security under specific attack model. In the same year, Braeken et al. [11] designed a key agreement model using elliptic curve cryptography, which aims to protect the security of session key. Kumar et al. [12] proposed a lightweight scheme using hybrid encryption method. Their scheme used elliptic curve cryptography, symmetric encryption to improve the security in smart grid. In 2021, Wu et al. [13] proposed an enhanced authentication scheme for smart grid communications based on bilinear pairing.

In recent years, many key agreement protocols [14–17] have been proposed for different environments. Authentication and key exchange protocol can be divided into smart card based [18], password based [19] and biometric based [20]. Considering the complexity and delay sensitivity of smart grid, elliptic curve cryptography is more suitable for smart grid environment compared with other key agreement schemes. In this paper, we proposed an anonymous authentication and key exchange protocol based on elliptic curve cryptosystems in smart grid. We proved that our protocol is secure by random oracle model and BAN logic [21, 22].

The rest of this paper is organized as follows. Section 2 introduces the scheme in detail. Section 3 verifies the security of the scheme by using random oracle model and BAN logic. Section 4 analyzes the performance of the scheme and section 5 draws the conclusions.

2. **The proposed scheme.** In this section, we present a new authentication and key exchange based on elliptic curve cryptography in smart grid. The proposed protocol is divided into three parts, including Setup, Registration and Key exchange.The descriptions are given below:

a. Setup phase. The power supplier takes a system parameter value for k and the trusted authority (TA) does the following:

Chooses a k-bit prime q and constructs $\{F_q, E/F_q, G_q, P\}$.

Chooses a master key $x \in Z_q^*$,compute the system public key $P_{pub} = xP \in E/F_q$.

Chooses a hash function $H : \{0,1\}^* \times G_q \to Z_q^*$.

Publish $\{F_q, E/F_q, G_q, P, P_{pub}, H\}$ as the system parameters.

b. Registration phase.

(i) Registration of AHE

Step1. AHE chooses a random number $b \in Z_q^*$, computes $B_j = bP$ and sends ID_j, B_j, , to TA over a secure channel.

Step2. After receiving ID_j and B_j , TA computes $Q_j = qP$, $R_j = H(ID_j||B_j)x + q$ and sends it back to AHE.

Step3. AHE verifies whether the equation $R_jP = H(ID_j||B_j)P_k + Q_j$ holds.

(ii) Registration of SM

Step1. SM chooses a random number $a \in Z_q^*$, after computing $A_i = h(ID_i||a)$,$X_i = A_iP$,$V_i = aP$, SM sends X_i, V_i , ID_i to TA over a secure channel.

Step2. TA chooses a random number $d \in Z_q^*$,computes $D_i = H(ID_i||d)$, $C_i = D_i \oplus (dV_i)$, $V_T = dP$, $Y_i = D_iP$, $Z_i = X_i + Y_i$, then sends Z_i, C_i, V_T along with B_j back to SM.

Step3. SM computes $D_i = C_i \oplus (aV_T)$ and the private key $SK_i = A_i + D_i$, public key $PK_i = SK_iP$. Then SM verifies whether the equation $PK_i = Z_i$ holds.

c. Key exchange phase.

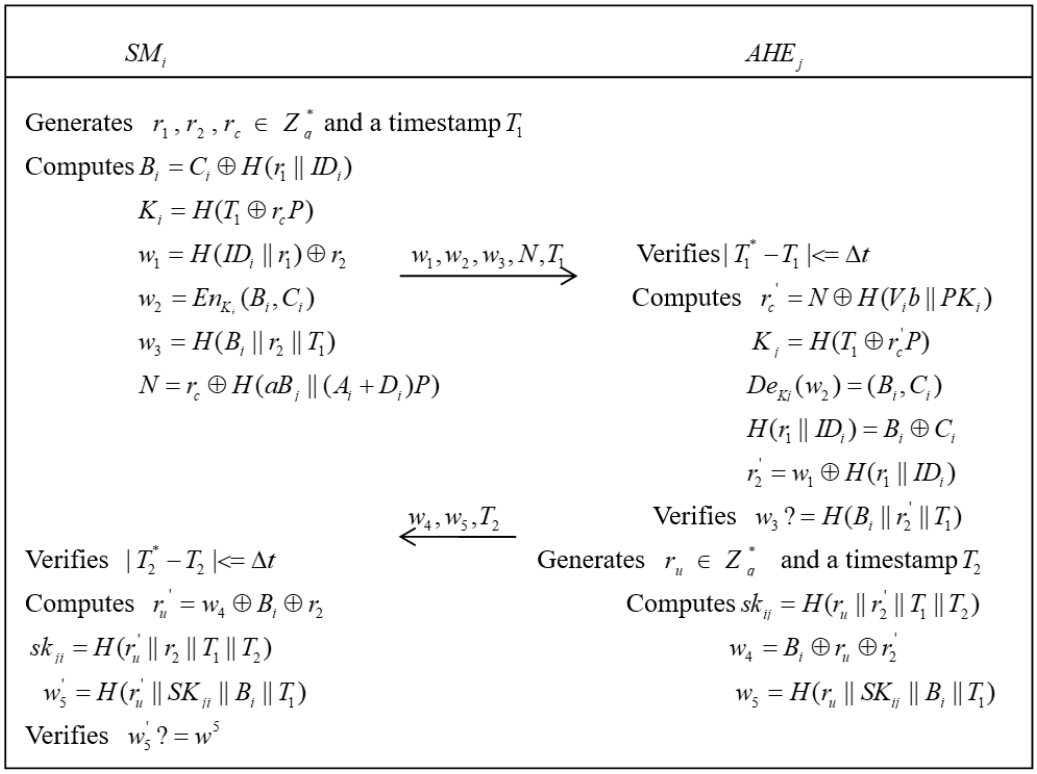

FIGURE 2. Key Exchange Phase

Step1. SM chooses three random number $r_1, r_2, r_c \in Z_q^*$, timestamp T_1 and computes $B_i = C_i \oplus H(r_1||ID_i)$, $K_i = H(T_1 \oplus aP)$,$w_1 = H(ID_i||r_1) \oplus r_2$, $w_2 = En_{K_i}(B_i, C_i)$, $w_3 = H(B_i||r_2||T_1)$, $N = r_c \oplus H(aB_j||(A_i + D_i)P)$, then sends $w_1, w_2, w_3, N, T_1$to AHE.

Step2. After receiving w_1, w_2, w_3, N, T_1 , AHE verifies the timestamp $|T_1^* - T_1| <= \Delta t$ and then computes $r_c^{'} = N \oplus H(V_i b||PK_i)$, $K_j = H(T_1 \oplus r_c^{'}P)$, $De_{Kj}(w_2) = (B_i, C_i)$,$H(r_1||ID_i) = B_i \oplus C_i$,$r_2^{'} = w_1 \oplus H(r_1||ID_i)$.

Step3. AHE verifies whether the equation $w_3 = H(B_i||r_2^{'}||T_1)$ holds. If $w_3 = H(B_i||r_2^{'}||T_1)$, AHE chooses a random number $r_u \in Z_q^*$ and a timestamp T_2.Then session key $sk_{ij} = H(r_u||r_2^{'}||T_1||T_2)$ is established.AHE computes $w_4 = B_i \oplus r_u \oplus r_2^{'}$, $w_5 = H(r_u||SK_{ij}||B_i||T_1)$ and sends w_4, w_5, T_2 back to SM.

Step4. SM verifies the timestamp $|T_2^* - T_2| <= \Delta t$ and computes $r_u{}^{'} = w_4 \oplus B_i \oplus r_2$, session key $sk_{ji} = H(r_u^{'}||r_2||T_1||T_2)$. SM computes $w_5^{'} = H(r_u^{'}||SK_{ji}||B_i||T_1)$ then verifies whether the equation $w_5^{'} = w^5$ holds. If $w_5^{'} = w^5$ holds, the session key is established successfully.

The steps are shown in Figure 2.

3. **Security analysis.** In this section, security of the proposed protocol is analyzed. The adversary A's capabilities are assumed that the adversary A has control over the content transmitted over the public channel.A can eavesdrop and modify the information transmitted in the public channel and send the modified information to the receiver.

3.1. **Formal security analysis. (a) BAN Logic.** The BAN logic is widely used to analyze the security of authentication and key agreement protocol. The detailed notations used in the following subsections.

BAN logic rules.

R_1 : Nonce verification rule $\dfrac{P| \equiv \#(X), P| \equiv Q| \sim X}{P| \equiv X}$

R_2 : Message meaning rule

$\dfrac{P| \equiv P \overset{K}{\longleftrightarrow} Q, P \triangleleft \{X\}_K}{P| \equiv Q| \sim X}$, $\dfrac{P| \equiv \overset{K}{\mapsto} Q, P \triangleleft \{X\}_{K^{-1}}}{P| \equiv Q| \sim X}$, $\dfrac{P| \equiv P \overset{K}{\rightleftharpoons} Q, P \triangleleft \{X\}_{K^{-1}}}{P| \equiv Q| \sim X}$

R_3 Jurisdiction rule $\dfrac{P| \equiv Q \mapsto X, P| \equiv Q| \equiv X}{P| \equiv X}$

R_4 Freshness rule $\dfrac{P| \equiv \#(X)}{P| \equiv \#(X, Y)}$

R_5 Belief rule $\dfrac{P| \equiv X, P| \equiv Y}{P| \equiv (X, Y)}$, $\dfrac{P| \equiv (X, Y)}{P| \equiv X}$,$\dfrac{P| \equiv Q| \equiv (X, Y)}{P| \equiv Q| \equiv X}$, $\dfrac{P| \equiv Q| \sim (X, Y)}{P| \equiv Q| \sim X}$

Goals. The proposed scheme should achieve the following 4 goals:

$G_1 : SM_i| \equiv SM_i \overset{sk}{\longleftrightarrow} AHE_j$, $G_2 : AHE_j| \equiv SM_i \overset{sk}{\longleftrightarrow} AHE_j$

$G_3 : SM_i| \equiv AHE_j| \equiv SM_i \overset{sk}{\longleftrightarrow} AHE_j$, $G_4 : AHE_j| \equiv SM_i| \equiv SM_i \overset{sk}{\longleftrightarrow} AHE_j$

Idealize the communication messages. Convert to the language that Ban logic can recognize.

$M_1 : SM_i \to AHE_j : \{w_1, w_2, w_3, N\}$, $M_2 : AHE_j \to SM_i : \{w_4, w_5\}$

Initial state assumptions. According to the protocol process, the assumptions are further extracted.

$A_1 : AHE_j| \equiv \#\{T_1, T_2, r_u, r_c\}$, $A_2 : AHE_j| \equiv \overset{(V_i, sk)}{\longrightarrow} SM_i$

According A_1 , A_2 , R_5 , we can obtain $A_3 : AHE_j| \equiv SM_i \overset{bV_i}{\rightleftharpoons} AHE_j$

$A_4 : AHE_j| \equiv SM_i \mapsto (B_i, C_i)$

$A_5 : AHE_j| \equiv SM_i \mapsto (r_2, r_c)$

$A_6 : SM_i| \equiv \#\{T_1, T_2, B_i, r_2\}$

Detailed description. The specific proof is as follows.

For G_1 . By M_2 we have $S_{10} : SM_i \triangleleft \{w_4, w_5\}$. According to S_{10} , A_7 we can obtain $S_{11} : SM_i| \equiv r_u$ applying R_5. $S_{12} : SM_i| \equiv SM_i \overset{sk}{\longleftrightarrow} AHE_j$ is proved due to $sk_{ij} = H(r_u||r_2||T_1||T_2)$.

For G_2 . By M_1 we have $S_1 : AHE_j \triangleleft \{w_1, w_2, w_3, N\}$. According to S_1, A_3 we can obtain $S_2 : AHE_j| \equiv SM_i| \sim r_c$ applying R_2. According S_2, A_1 we can obtain $S_3 : AHE_j| \equiv SM_i| \equiv r_c$ applying R_1 . According S_3, A_6 we can obtain $S_4 : AHE_j| \equiv r_c$ applying R_3 . Since $K_j = H(T_1 \oplus r_c P)$, According to S_4, A_1 ,we can obtain $S_5 : AHE_j| \equiv SM_i \overset{\#(K_j)}{\longleftrightarrow} AHE_j$. Since $w_2 = En_K(B_i, C_i)$, According to S_1, S_5 we can obtain $S_6 : AHE_j| \equiv SM_i| \equiv (B_i, C_i)$ applying R_1, R_2 . According to S_6, A_4 we can obtain $S_7 : AHE_j| \equiv (B_i, C_i)$ applying R_3 . Since $r_2 = w_1 \oplus H(r_1||ID_i) = w_1 \oplus B_i \oplus C_i$, according to S_7 we can obtain $S_8 : AHE_j| \equiv r_2$ applying R_5 . Since $sk_{ij} = H(r_u||r_2^{'}||T_1||T_2)$, according S_8, A_1 we can prove $S_9 : AHE_j| \equiv SM_i \overset{sk_{ij}}{\longleftrightarrow} AHE_j$ applying R_5 .

For G_3 . According to $S_{12} : SM_i| \equiv SM_i \overset{sk}{\longleftrightarrow} AHE_j$ and $S_{10} : SM_i \triangleleft \{w_4, w_5\}$ we can obtain $S_{13} : SM_i| \equiv AHE_j| \sim w_5$ applying R_2 . According to $SM_i| \equiv \#(w_5)$,$S_{13} : SM_i| \equiv AHE_j| \sim w_5$, we can obtain $SM_i| \equiv AHE_j| \equiv w_5$ applying R_1 . Since w_5 contains sk , we can prove $S_{14} : SM_i| \equiv AHE_j| \equiv SM_i \overset{sk}{\longleftrightarrow} AHE_j$ applying R_5 .

For G_4 . According to $S_9 : AHE_j| \equiv SM_i \overset{sk_{ij}}{\longleftrightarrow} AHE_j$, $S_1 : AHE_j \triangleleft \{w_1, w_2, w_3, N\}$ we can obtain $S_{15} : AHE_j| \equiv SM_i| \sim w_3$ applying R_2 . According to $AHE_j| \equiv \#(w_3)$, $S_{15} : AHE_j| \equiv SM_i| \sim w_3$, we can obtain $S_{16} : AHE_j| \equiv SM_i| \equiv w_3$ applying R_5 . Then we can obtain $S_{17} : AHE_j| \equiv SM_i| \equiv sk$ applying R_5,therefore we can prove $S_{18} : AHE_j| \equiv SM_i| \equiv SM_i \overset{sk}{\longleftrightarrow} AHE_j$.

(b) Security proof in random oracle model.

This section will prove the security in the random oracle model. Oracle query includes Hash query, Excute query, Send query, Real query, Corrupt query and Test query.

Security Model. We suppose there is a powerful attacker A who can intercept and modify the information transmitted in the public channel, but also can obtain the long-term key of both sides through some specific attack. We suppose that represents the i_{th} event of participant P, where P can be the SM or AMI. All possible oracle queries are listed below:

Hash(string): Using this query, A can obtain the value of the corresponding string after hash encoding.

Excute (SM_i, AHE_i): Using this query can simulate the eavesdropping attack, so that A can access the messages exchanged during the execution of the protocol.

Send (P^i, m): This query can simulate active attack. Using this query, A can send message m and receive a response according to the protocol definition.

Reaveal (P^i): Using this query, A can get the session key of P^i.

Corrupt (P^i): This query is used to define the semantic security of the session key. After receiving the query, flip the coin if c = 1, A will get the session key of P^i . If it is not equal to 1, A will get a equal length random number.

Proof. Let $Succ_A^{GM_x}$ indicates an event where A can easily guess the random bit b in Game G_x , while the corresponding advantage of A is $Adv_A^{GAME} = p_r[Succ_A^{GM_x}]$

The scheme proposed in this paper will be simulated by a series of simulations. The simulation process will be described by a "Game". In this game, A will issue multiple queries, and at the end of the game, attacker a will list the probability that this is a real session key or an equal length random number string.

Suppose p is a parameter in the protocol and p is a prime number, The period of $\{T_n(x)\}_{n\geq 0}$ is P+1.For attacker A, the advantage of attacking the protocol successfully is $Adv^{GAME_0}(A) = q_H^2/2^l + (q_S + q_E)^2/p + q_S/2^{l-1} + 2q_H Adv^{ECDLP}(A) + 2q_H Adv^{ECDLP}(A)$. Where q_H, q_E and q_S are defined as the times of*Hash* query, *Excute* query and *Send* query respectively, and l is the length of output. The specific game process is as follows:

$Game_0$: The simulation in $Game_0$ is the same as the real attack in the random oracle model, and the response of oracle is all from the actual operation. The game is simulated according to the real situation. The probability of A successfully breaking the session key is $Adv^{GAME_0}(A) = |2\Pr[Succ_A^{GM_0}] - 1|$.

$Game_1$: In $Game_1$, due to the oracle models of *Hash, Execute, Send, Reaveal, Corrupt, Test* are exactly the same as the simulation in the actual attack, it is impossible to distinguish the simulation in from the actual execution of the protocol, so we can get $\Pr[Succ_A^{GM_1}] = \Pr[Succ_A^{GM_0}]$.

$Game_2$: If there is a collision in the *Hash* query or in the transmission, the $Game_2$ will be aborted. According to the birthday paradox, the collision probability of *Hash* is at most $q_H^2/2^{l+1}$, and the collision probability of transmitted text is at most $(q_S + q_E)^2/2n$. Therefore $|\Pr[Succ_A^{GM_2}] - \Pr[Succ_A^{GM_1}]| \leq q_H^2/2^{l+1} + (q_S + q_E)^2/2p$.

$Game_3$: When A does not launch the corresponding Hash query, it can still guess the verification value correctly, so we can get $|\Pr[Succ_A^{GM_3}] - \Pr[Succ_A^{GM_2}]| \leq q_S/2^l$.

$Game_4$: In this game, the security of session key will be considered. The purpose of this game is to verify the perfect forward security and the ability to resist the temporary secret leakage attack. When attacker a uses the reveal query, attacker a will get the temporary secret value corresponding to the query. Due to A can't get both long-term secret value and temporary secret value at the same time. So that if A wants to break the session key, he must solve the elliptic curve discrete logarithm problem (ECDLP), so we can get $|\Pr[Succ_A^{GM_4}] - \Pr[Succ_A^{GM_3}]| \leq q_H Adv^{ECDLP}(A)$.

$Game_5$: In the last game, A attempts to obtain B_i, C_i by decrypting the w_2 which transmitted in the public tunnel to calculate the session key. Depending on the security of symmetric encryption, the probability of A winning this game under the IND-CPA(Indistinguishability under chosen-plaintext attack) is $|\Pr[Succ_A^{GM_5}] - \Pr[Succ_A^{GM_4}]| \leq Adv^{IND-CPA}(A)$, where $|\Pr[Succ_A^{GM_5}]| = 1/2$.

According to the five games mentioned above, we can get

$Adv^{GAME_0}(A) = 2\sum_{n=0}^{5} |\Pr[Succ_A^{GM_n}] - \Pr[Succ_A^{GM_{n-1}}]| = q_H^2/2^l + (q_S + q_E)^2/p + q_S/2^{l-1}$ $+2q_H Adv^{ECDLP}(A) + 2Adv^{IND-CPA}(A)$ .From the equation, this is a very small probability value. Therefore, the proposed scheme can ensure the security of session key between the SM and AHE.

3.2. **Informal security analysis.** (a) Man-in-the-middle attack: If A wants to impersonate as a SM to launch a impersonation attack on the AHE, A must obtain the random number r_1, r_2 . It is obvious that A can not obtain the random number because of $r_2' = w_1 \oplus H(r_1||ID_i)$,$w_3 = H(B_i||r_2||T_1)$. As the same, A can not obtain the random number r_u, r_2 so that A has no chance to launch a impersonation attack on the SM. Therefore, the proposed scheme can resist MITM attack.

(b) Replay attack: The establishment of session key depends on the generation of random numbers, so when the receiver receives the previously sent packets, it will not be able to complete the authentication process, so it can resist replay Attack.

(c) Insider privilege attack: The insider cannot obtain the random number a and b generated by the SM and AHE in the registration stage. A cannot obtain the random

number q because of $R_j = H(ID_j||B_j)x + q$, so the master key x of TA cannot be calculated directly.

(d) Anonymity: The identity of smart meter ID_i will be sent to AHE through XOR and hash calculation $B_i = C_i \oplus H(r_1||ID_i)$. As the same, the identity of AHE is not transmitted directly through public the public channel, therefore, A cannot obtain the identity directly.

(e) Perfect forward secrecy: In this scheme, the session key is not affected by the long-term key leakage. Because each session needs to generate a new random number, even if the attacker obtains the long-term key, the session key cannot be calculated. Therefore, the proposed scheme has perfect forward secrecy.

The security features of our protocol are compared with other protocols under various attacks in Table 1.

Table 1. Security Comparison.

Feature/Resistance	Replay Attack	Impersonation Attack	HITM Attack	Insider Attack	Anonymity
Nicanfar et al. [3]	✓	×	✓	✓	✓
Nicanfar et al. [6]	✓	✓	✓	✓	✓
Wan et al. [8]	✓	✓	✓	✓	✓
Mohammadali et al. [4]	✓	×	✓	×	×
Mohammadali et al. [4]	✓	×	✓	×	×
Proposed scheme	✓	✓	✓	✓	✓

3.3. **Verification by using ProVerif.** After using ProVerif to verify the proposed protocol, the results are shown in Figure 3. It shows that the protocol can ensure the security of SM and AHE, the random number r_1, r_2, r_c, r_u and the session key sk is also secure.

4. **Performance analysis.** Performance of the proposed scheme will be analyzed from computation cost and communication cost.

4.1. **Computation cost.** According to the description of each protocol, the complex operations involved in the protocol that need to calculate the time include bilinear pairing (C_P), point multiplication on elliptic curve (C_M), hash operation time (C_H), AES symmetric encryption and decryption ($C_{E(S)}, C_{D(S)}$) and RSA asymmetric encryption and decryption ($C_{E(P)}, C_{D(P)}$). There are also some simple operations such as XOR, multiplication and addition. Because the time cost of these simple operations tends to zero,the computation time is usually negligible. In order to calculate the computation cost of the protocol, MICAZ device is used as the SM and 2.7GHz,Intel(R) Xeon(R) E-2176M CPU is used as the AHE. The computation time of operations as in Table 2 . Computational costs of different key establishment as in Table 3.

Table 2. Computation Time of Operation.

Operation	C_P	C_M	C_H	$C_{E(S)}$	$C_{D(S)}$	$C_{E(P)}$	$C_{D(P)}$
SM	5.32s	2.45s	0.023ms	0.023ms	0.023ms	0.79s	21.5s
AHE	13ms	15ms	45ms	0.018ms	0.004ms	0.514ms	2.773ms

```
-- Query not attacker(skij[])
Completing...
200 rules inserted. The rule base contains 200 rules.
28 rules in the queue.
Starting query not attacker(skij[])
RESULT not attacker(skij[]) is true.
-- Query not attacker(skji[])
Completing...
200 rules inserted. The rule base contains 200 rules.
28 rules in the queue.
Starting query not attacker(skji[])
RESULT not attacker(skji[]) is true.
-- Query not attacker(x[])
Completing...
200 rules inserted. The rule base contains 200 rules.
28 rules in the queue.
Starting query not attacker(x[])
RESULT not attacker(x[]) is true.
-- Query not attacker(r1[])
Completing...
200 rules inserted. The rule base contains 200 rules.
28 rules in the queue.
Starting query not attacker(r1[])
RESULT not attacker(r1[]) is true.
-- Query not attacker(r2[])
Completing...
200 rules inserted. The rule base contains 200 rules.
28 rules in the queue.
Starting query not attacker(r2[])
RESULT not attacker(r2[]) is true.
-- Query not attacker(rc[])
Completing...
200 rules inserted. The rule base contains 200 rules.
28 rules in the queue.
Starting query not attacker(rc[])
RESULT not attacker(rc[]) is true.
-- Query not attacker(ru[])
Completing...
200 rules inserted. The rule base contains 200 rules.
28 rules in the queue.
Starting query not attacker(ru[])
RESULT not attacker(ru[]) is true.
-- Query inj-event(SMend(id)) ==> inj-event(SMstart(id))
Completing...
200 rules inserted. The rule base contains 200 rules. 40 rules in the queue.
400 rules inserted. The rule base contains 346 rules. 8 rules in the queue.
Starting query inj-event(SMend(id)) ==> inj-event(SMstart(id))
RESULT inj-event(SMend(id)) ==> inj-event(SMstart(id)) is true.
-- Query inj-event(AHEend(id_69)) ==> inj-event(AHEstart(id_69))
Completing...
200 rules inserted. The rule base contains 200 rules. 28 rules in the queue.
Starting query inj-event(AHEend(id_69)) ==> inj-event(AHEstart(id_69))
RESULT inj-event(AHEend(id_69)) ==> inj-event(AHEstart(id_69)) is true.
```

FIGURE 3. Results of ProVerif

TABLE 3. Computational Costs of Different Key Establishment Methods.

Protocol	SM	AHE	Total
Nicanfar et al. [3]	$3C_{E(P)} + 2C_{D(P)} + 4C_{D(S)} + 4C_{E(S)}$	$C_{E(P)} + 3C_{D(P)} + C_{E(S)}$	45.379s
Nicanfar et al. [6]	$2C_M + C_{E(S)} + C_{D(S)} + 2C_H$	$2C_M + C_{E(S)} + C_{D(S)} + 2C_H$	5.020s
Wan et al. [8]	$C_M + C_P$	$C_M + C_P$	7.798s
Mohammadali et al. [4]	$2C_M + 3C_H$	$3C_M + 4C_H$	5.125s
Mohammadali et al. [4]	$C_M + 3C_H$	$4C_M + 4C_H$	2.690s
Proposed scheme	$3C_M + 6C_H + C_{E(S)}$	$2C_M + 7C_H + C_{D(S)}$	7.695s

4.2. **Communication cost.** A protocol with low communication times can shorten the communication delay and improve the response speed. Therefore, reducing the communication times is also the key to improve the efficiency, so the communication cost is also an important indicator of the performance of the protocol. The communication cost is observed by determining the number of times and data transmitted during the execution of the protocol. The comparison of specific communication costs is shown in table 4.It can be seen from table 3 that the communication times of the scheme proposed in this paper is 2, and the number of new data transmission is 8, which has a lower communication times compared with other protocols

TABLE 4. Communication Costs of Different Key Establishment Methods.

Protocol	Communications	Messages
Nicanfar et al. [3]	9	9
Nicanfar et al. [6]	3	4
Wan et al. [8]	3	4
Mohammadali et al. [4]	3	7
Mohammadali et al. [4]	3	6
Proposed scheme	2	8

5. **Conclusion.** This paper proposed an anonymous authentication and key exchange scheme based on elliptic curve cryptosystems for smart grid. It is found that the computational cost of the proposed scheme are better than most schemes, but slower than Mohammadali et al.'s scheme. However, Mohammadali et al.'s scheme is vulnerable to insider privilege attack, impersonation attack, and lacks anonymity. The scheme designed in this paper not only makes up for the defects of Mohammadali et al.'s scheme, but also keeps similar computing cost and communication cost. The security of the scheme is proved by applying informal security analysis and formal security analysis. The formal security analysis is proved by random oracle model and BAN logic. We found that the proposed scheme can resist a variety of known attacks.

REFERENCES

[1] C. M. Chen, K. H. Wang, T. Y. Wu, E. K. Wang, Reconsidering a lightweight anonymous authentication protocol, *Journal of the Journal of the Chinese Institute of Engineers*, vol.42, no.1, pp.9-14, 2019.

[2] T. Y. Wu, L. Yang, Z. Y. Lee, C. M. Chen, J. S. Pan, S. H. Lslam, Improved ECC-based three-factor multiserver authentication scheme, *Security and Communication Networks*, vol.2021, 6627956, 2021.

[3] H. Nicanfar, P. Jokar, V. Leung, Smart grid authentication and key management for unicast and multicast communications,*IEEE PES Innovative Smart Grid Technologies Asia (ISGT)*, pp.1-8, 2011.

[4] A. Mohammadali, M. S. Haghighi, M. H. Tadayon, A. M. Nodooshan, A novel identity-based key establishment method for advanced metering infrastructure in smart grid,*IEEE Transactions on Smart Grid*, vol.9, no.4, pp.2834-2842, 2018.

[5] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. X. Lu, X. S. Shen, A lightweight message authentication scheme for smart grid communications, *IEEE Trans Smart Grid*, vol.2, no.4, pp.675-685, 2011.

[6] H. Nicanfar, V. Leung, Multilayer vonsensus ECC-based password authenticated key-exchange (MCEPAK) protocol for smart grid system,*IEEE Trans Smart Grid*, vol.4, no.1, pp.253-264, 2013.

[7] N. Liu, J. S. Chen, L. Zhu, J. H. Zhang, Y. L. He, A key management scheme for secure communications of advanced metering infrastructure in smart grid, *IEEE Transactions on Industrial Electronics*, vol.60, no.10, pp.4746-4756, 2013.

[8] Z. Wan, G. Wang, Y. Yang, S. Shi, Skm: scalable key management for advanced metering infrastructure in smart grids, *IEEE Transactions on Industrial Electronics*, vol.61, no.12, pp.7055-7066, 2014.

[9] J. L. Tsai, N. W. Lo, Secure anonymous key distribution scheme for smart grid, *IEEE Trans Smart Grid*, vol.7, no.2, pp.906-914, 2016.

[10] V. Odelu, A. K. Das, M. Wazid, M. Conti, Provably secure authenticated key agreement scheme for smart grid, *IEEE Trans Smart Grid*, vol.9, no.3, pp.1900-1910, 2016.

[11] A. Braeken, P. Kumar, A. Martin, Efficient and provably secure key agreement for modern smart metering communications, *Energies*, vol.11, no.10, 2662, 2018.

[12] P. Kumar, A. Gurtov, M. Sain, A. Marin, H. H. Phuong, Lightweight authentication and key agreement for smart metering in smart energy networks, *IEEE Transactions on Smart Grid*, vol.10, no.4, pp.4349-4359, 2019.

[13] T. Y. Wu, Y. Q. Lee, C. M. Chen, Y. Tian, N. A. Al-Nabhan, An enhanced pairing-based authentication scheme for smart grid communications, *Journal of Ambient Intelligence and Humanized Computing*, https://doi.org/10.1007/s12652-020-02740-2, 2021.

[14] S. Kumari, P. Chaudhary, C. M. Chen, M. K. Khan, Questioning key compromise attack on Ostad-Sharif et al.'s authentication and session key generation scheme for healthcare applications, *IEEE Access*, vol.7, pp.39717-39720, 2019.

[15] T. Y. Wu, Z. Y. Lee, L. Yang, J. N. Luo, R. Tso, Provably secure authentication key exchange scheme using fog nodes in vehicular Ad-Hoc networks, *The Journal of Super computing*, https://doi.org/10.1007/s11227-020-03548-9, 2021.

[16] C. M. Chen, B. Xiang, K. H. Wang, K. H. Yeh, T. Y. Wu, A robust mutual authentication with a key agreement scheme for session initiation protocol, *Applied Sciences*, vol.8, 1789, 2018.

[17] T. Y. Wu, T. Wang, Y. Q. Lee, W. M. Zheng, S. Kumari, S. Kumar, Improved authenticated key agreement scheme for fog-driven IoT healthcare system,*Security and Communication Networks*, vol. 2021, 6658041, 2021.

[18] C. M. Chen, B. Xiang, K. Hang. Wang, Y. Zhang, T. Y. Wu, An efficient and secure smart card based authentication scheme,*Journal of Internet Technology*, vol. 20, no.4, pp.1113-1123, 2019.

[19] J. C. Hsu, Y. S. Jheng, S. M. Rahman, R. Tso, Password-based authenticated key exchange from lattices for client server model,*Journal of Computer Security and Data Forensics*, vol.1, no.1, pp.1-17, 2021.

[20] Y. L. Wang, Y. Liu, H. B. Ma, Q. T. Ma, Q. Ding, The research of identity authentication based on multiple biometrics fusion in complex interactive environment, *Journal of Network Intelligence*, vol.4, no.4, pp.124-139, 2019.

[21] C. M. Chen, L. L. Xu, K. H. Wang, S. Liu, T. Y. Wu, Cryptanalysis and improvements on three-party-authenticated key agreement protocols based on chaotic maps,*Journal of Internet Technology*, vol.19, no.3, pp.679-687, 2018.

[22] T. Y. Wu, Z. Y. Lee, S. Mohammad, Obaidat, S. Kumari, C. M. Chen, An authenticated key exchange protocol for multi-server architecture in 5G networks,*IEEE Access*, vol.8, pp.28096-28018, 2020.