IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 15, 2019, accepted February 2, 2019, date of publication February 11, 2019, date of current version March 4, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2898376

A Bilinear Map Pairing Based Authentication Scheme for Smart Grid Communications: PAuth

YUWEN CHEN, JOSÉ-FERNÁN MARTÍNEZ, PEDRO CASTILLEJO, AND LOURDES LÓPEZ
Departamento de Ingeniería Telemática y Electrónica, Escuela Técnica Superior de Ingeniería y Sistemas de Telecomunicación, Universidad Politécnica de Madrid, 28031 Madrid, Spain

Corresponding author: Yuwen Chen (yuwen.chen@upm.es)

The work in this study was supported in part by the European project "Sustainable-Smart Grid Open System for the Aggregated Control, Monitoring, and Management of Energy" (e-GOTHAM).

ABSTRACT Smart meters have been widely applied in the smart grid, and they enable two-way communication in the smart grid. User's electricity consumption data and other data are transmitted between the entities. It is necessary to ensure the security of this two-way communication. Several authentication schemes have been proposed to solve this problem. Recently, Mahmood *et al.* proposed an authentication scheme for the smart grid. However, we find that their scheme cannot provide the perfect forward secrecy and private key privacy as they have claimed. An improved version by Abbasinezhad is found to be subject to replay attack, too. In this paper, a bilinear map pairing-based authentication and key establish scheme is proposed, which can withstand the aforementioned attacks and achieves more security features, private key privacy, perfect forward privacy, and message integrity. We designed a simpler registration scheme, which implements the same functionalities, while the computation cost is reduced. We also conducted a formal security analysis of the proposed scheme, and the result shows that the proposed scheme is secure. Our simulation results show that the proposed scheme has a comparable communication cost and computation cost.

INDEX TERMS Smart grid, elliptic curve, bilinear map, authentication and key establishment, private key secrecy.

I. INTRODUCTION

Smart meters have been widely installed in the European Union. It is required that 200 million smart meters for electricity and 45 million smart meters for gas will be installed by the year 2020 [1]. An estimated amount of more than 200 million European households will have their smart meters by the year 2023 [2]. European Parliament and the European Council has required its member states to make sure the implementation of smart metering systems and to help consumers in the electricity supply and gas supply markets [3], it is foreseeable that smart meters will be deployed in large numbers in the near future.

Smart grid provides a way of mutual communication between the utility supplier and the consumer. Smart grid makes it possible for the utility supplier to monitor the consumers' electricity consumption behaviors, to adjust the amount of electricity supplement in real time. In order to achieve these functions, devices in smart grid need bidirectional communication to share information periodically [4], for example, every fifteen minutes [5]. To ensure the security of two-way communication between smart grid entities, authentication and key establishment is a necessary, which enables the entities to verify the the legitimacy of the entity with which they communicate, and to build a shared key with the legitimate entity for further communication.

Recently, Mahmood *et al.* [6] proposed an elliptic curve based lightweight authentication scheme for smart grid. However, their scheme is found to be unable to meet their design goals. Abbasinezhad-Mood and Nikooghadam [7] proposed an improved version claims to overcome the security risks. However, we found that their scheme suffers from replay attack and their scheme can not ensure the integrity of the first message, a detailed analysis is shown in Section VII, besides, the registration process in their scheme is cumbersome. We designed a simpler registration scheme that implements the same functionalities, however, the computation cost is reduced. In this study, we proposed a pairing based

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

authentication and key establishment scheme for smart grid. Our contributions are in three folds:

1) First, we analyzed the two existing schemes, we found both of them failed to provide all the security features as they claimed. The discussion is in Section VII.
2) Second, we designed a simpler registration scheme that implements the same functionalities, achieves the same or a higher security level, however, the computation cost is reduced.
3) We came up with a bilinear map pairing based mutual authentication scheme, the proposed scheme achieves more security features compared to related works, perfect forward privacy, message integrity, private key privacy etc., which means it can resist various attacks, replay attack, impersonate attack etc. We conducted a formal analysis of the security features of the proposed scheme, the result shows the proposed scheme is secure. We also validated the proposed scheme using Burrows-Abadi-Needham logic (BAN logic).

II. RELATED WORK

There are many studies focusing on the authentication problems in smart grid. Some of which are lightweight ones, while some are more secure ones based on asymmetric cryptography. Elliptic curve and bilinear map pairing are two of the most popular asymmetric cryptography suites used in the past studies.

Wu and Zhou's scheme [8] used both the symmetric encryption and the elliptic curve encryption, their scheme is partly based on the Needham-Schroeder authentication protocol. Xia and Wang [9] found that the scheme of Wu and Zhou is vulnerable to the man-in-the-middle attack, in the scheme of Xia and Wang (2012), a trusted third party is introduced. Besides, their scheme enables key revocation. The scheme of Mahmood et al. has been tested by ProVerif and BAN logic, however, their scheme is found to fail to provide perfect forward secrecy by Abbasinezhad and Nikooghadam, besides, in the scheme of Mahmood et al., the network manager knows the private key of the entities, and the shared session keys may be compromised if the ephemeral secrets are leaked. For the scheme of Abbasinezhad and Nikooghadam, we found that their scheme faces a replay attack, although the adversary can not get the session key, the adversary can make this entity inaccessible to its peer entities temporarily, besides, in the first message of their scheme, there is not a signature or a timestamp, a receiver of this message can not know if this message has been tampered or altered by an adversary or not. Liu *et al.* [10]

proposed a 1-RAAP scheme, which preserves anonymity, mutual authentication, non-repudiation and some other desirable security properties, while only requiring users to perform several low-cost computational operations. Li *et al.* [11] discovered several potential security risks in the scheme of Liu et al., for example, when the information stored in the server is leaked to an adversary, the adversary can mimic as a legitimate server and build a shared key with the user, Li et al. proposed an improved version. In the scheme of Kumari *et al.* [12], the private key of the user is generated by the server, so the server knows the private keys of all the users. Wu *et al.* [13] proposed a smart card based authentication scheme, their scheme can ensure identity anonymity. The scheme of Huang *et al.* [14] is a lightweight scheme, in their scheme, when a user registers with the server, the server will generate an encrypted identity for the user, and the user uses this new identity to log in next time. Thus the adversary is unable to get the true identity of a user.

The bilinear map pairing is another famous asymmetric cryptography suit used in the smart grid authentication schemes. The scheme of Tsai and Lo [15] is an authentication scheme based bilinear map pairing, the smart meter can be quickly authenticated without the help of a trusted anchor. The scheme of Odelu *et al.* [16] is also based bilinear map pairing, their scheme provides SK-security under the CK-adversary model. Tseng *et al.* [17] proposed a list free identity based mutual authentication scheme, the bilinear map pairing was used in their scheme, their scheme has an efficient revocation mechanism in multi-server architectures, the communication cost of this scheme is relatively lower compared with related works. Tsai and Lo [18] proposed an anonymous authentication scheme for the distributed mobile cloud services environment, which enables mobile users to access to different cloud services using only one single private key, the identity privacy is protected in this scheme. Li and Hong [19] proposed a signature scheme for wireless sensor networks and based on the signature scheme they devised a certificate-less access control scheme. The authentication scheme of Li *et al.* [20] enables batch verification in the message verification process, which significantly reduces the computation cost. Lu *et al.* [21] proposed a secure and privacy-preserving framework for healthcare emergency, the scheme enables two users to authenticate each other without the help of a trusted third party.

Mahmood *et al.* [22] proposed a Diffie–Hellman based authentication scheme for the smart grid, RSA and AES are used in their scheme, HMAC is also used in order to maintain message integrity. The scheme of Wang *et al.* [23] adopts the intrinsic idea of ElGamal encryption, and their scheme achieves user anonymity. Wazid *et al.* [24] proposed a lightweight authentication scheme, only hash, XOR, and some few symmetric encryption schemes are used. Horng *et al.* [25] discussed about a privacy-preserving signature scheme. Akhunzada *et al.* [26] discussed the ''Man-At-The-End attacks''.

This study is organized in the following way, in Section III we discussed the proposed scheme, Section IV is the formal security analyzation part, in Section V, we conducted a security analysis using BAN logic, we compared the proposed scheme with related works in Section VI and Section VII, Section VIII provides the conclusion of this study.

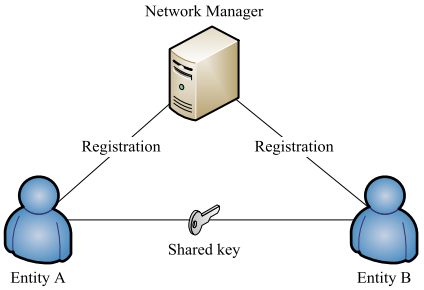


FIGURE 1. Entities in the system.

TABLE 1. Symbols used in the proposed scheme.

Symbol	Description
NM	The network manager
(d_x, R_x)	The public key pair of the network manager
V_i, Id_i	The i_{th} entity and its identity
V_j, Id_j	The j_{th} entity and its identity
(d_i, R_i)	The public key pair of the i_{th} entity
$\|\|$	String connector, connecting two strings together
G_1, G_2	Cyclic groups
$e: G_1 \times G_1 \rightarrow G_2$	A bilinear nondegenerate map
P	A random generator
T_1	A timestamp
H_1	Hash a string to a big integer
H	Hash to an element of G_1 operation
h	SHA-256 hash operation

III. THE PROPOSED SCHEME

Fig. 1 shows the entities in the system, there is a network manager (NM), which manages all the entities in this system. Every entity is registered with the network manager, the network manager will issue a key pair for each entity. With this key pair, the entity can verify if the peer entity is a legitimate one or not. After verification, the two can build a shared key for further communication. The notions used in this study are listed in Table 1.

A. INITIALIZATION AND REGISTRATION PHASE

The network manager generates the parameters for an elliptic curve and selects a random number d_x as its private key, its public key is computed as: $R_x = d_x \cdot P$, then the network manager publishes parameters of this elliptic curve and its public key to all the entities in the system.

When an entity V_i wants to join the system, it must be registered with the network manager to get its public key pairs. Here, we suppose the registration messages are sent in a private and secure channel.

1. Entity V_i selects a random number k_u, and gets $R_u = k_u \cdot P$.
2. Entity V_i sends $\{Id_i, R_u\}$ to the network manager.

After the network manager receives a registration request, it performs the following steps to complete the registration process.

TABLE 2. Registration process.

ENTITY V_i	NETWORK MANAGER
random k_u, $R_u = k_u \cdot P$	
$\{Id_i, R_u\}$ →	
	random k_n, $R_n = k_n \cdot P$ $R_{in} = (R_u + R_n)$ $e_i = H_1(R_{in}\|\|Id_i)$ $s_i = e_i \cdot k_n + d_x$
	← $\{s_i, R_n\}$
$R_{in} = (R_u + R_n)$ $e_i = H_1(R_{in}\|\|Id_i)$ $d_i = e_i \cdot k_u + s_i$ stores $\{d_i, R_{in}\}$	

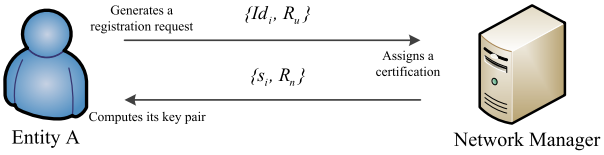


FIGURE 2. Registration process.

1. Network manager selects a random number k_n, and gets $R_n = k_n \cdot P$.
2. Network manager computes $R_{in} = (R_u + R_n)$.
3. Network manager computes $e_i = H_1(R_{in}||Id_i)$.
4. Network manager computes $s_i = e_i \cdot k_n + d_x$.
5. Network manager sends $\{s_i, R_n\}$ back to entity V_i.

When entity V_i receives $\{s_i, R_n\}$, it calculates R_{in} and its private key d_i, the registration process is depicted in Table 2 and Fig. 2.

1. Entity V_i computes $R_{in} = (R_u + R_n)$.
2. Entity V_i computes $e_i = H_1(R_{in}||Id_i)$, and its private key $d_i = e_i \cdot k_u + s_i$.

B. AUTHENTICATION AND KEY ESTABLISHMENT PHASE

When entity V_i and entity V_j want to communicate with each other, they must authenticate each other first and then build a shared key for further communication. Suppose entity V_i initializes the scheme, entity V_i generates a request message and sends this request to V_j.

1. Entity V_i selects a random number k_{i1}, and gets $R_{i1} = k_{i1} \cdot P$.
2. Entity V_i gets the current timestamp T_1 and an element of G_1 as $R_{it} = H(Id_i||R_{in}||R_{i1}||T_1)$.
3. Entity V_i generates a signature $R_{si} = d_i \cdot R_{it}$.
4. Entity V_i sends $\{Id_i, R_{in}, R_{i1}, R_{si}, T_1\}$ to entity V_j.

When V_j receives $\{Id_i, R_{in}, R_{i1}, R_{si}, T_1\}$ from V_i, V_j will check the correctness of this message by checking the timestamp and the signature. After this, V_j prepares a replay message. The detailed steps are described as follows:

1. Entity V_j checks the timestamp T_1, if T_1 is fresh, goes to the next step, otherwise, the scheme ends here.

TABLE 3. Authentication process.

ENTITY V_i	ENTITY V_j
random $k_{i1}, R_{i1} = k_{i1} \cdot P$ timestamp T_1 $R_{it} = H(Id_i \| R_{in} \| R_{i1} \| T_1)$ $R_{si} = d_i \cdot R_{it}$	
$\{Id_i, R_{in}, R_{i1}, R_{si}, T_1\}$ →	
	Check T_1 $e_i' = H_1(R_{in} \| Id_i)$ $R_{it}' = H(Id_i \| R_{in} \| R_{i1} \| T_1)$ if $e(P, R_{si}) = e(e_i' \cdot R_{in} + R_x, R_{it}')$ random $k_{j1}, R_{j1} = k_{j1} \cdot P$ $SK_{ij} = h(e(R_{it}', R_{i1})^{k_{j1}})$ $R_{jt} = d_j \cdot R_{i1}$ $h_j = h(Id_j \| R_{jn} \| R_{j1} \| SK_{ij} \| T_1 \| R_{jt})$
	← $\{Id_j, R_{jn}, R_{j1}, h_j\}$
$SK_{ij}' = h(e(R_{it}, R_{j1})^{k_{i1}})$ $e_j' = H_1(R_{jn} \| Id_j)$ $R_{jt}' = k_{i1} \cdot (e_j' \cdot R_{jn} + R_x)$ if $h_j = h(Id_j \| R_{jn} \| R_{j1} \| SK_{ij}' \| T_1 \| R_{jt}')$	
Both entities agree on the key $SK_{ij} = SK_{ij}'$	

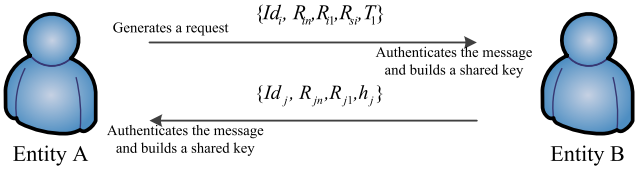


FIGURE 3. Authentication process.

2. Entity V_j gets an element of G_1 as $R_{it}^{'} = H(Id_i \| R_{in} \| R_{i1} \| T_1)$.
3. Entity V_j computes $e_i^{'} = H_1(R_{in} \| Id_i)$.
4. Entity V_j checks if $e(P, R_{si}) = e\left(e_i^{'} \cdot R_{in} + R_x, R_{it}^{'}\right)$, if they are equal, goes to the next step, otherwise, the scheme ends here.
5. Entity V_j chooses a random k_{j1}, and gets $R_{j1} = k_{j1} \cdot P$.
6. Entity V_j calculates the shared key as: $SK_{ij} = h(e\left(R_{it}^{'}, R_{i1}\right)^{k_{j1}})$.
7. Entity V_j computes $R_{jt} = d_j \cdot R_{i1}$.
8. Entity V_j generates a signature $h_j = h(Id_j \| R_{jn} \| R_{j1} \| SK_{ij} \| T_1 \| R_{jt})$.
9. Entity V_j sends the message $\{Id_j, R_{jn}, R_{j1}, h_j\}$ to entity V_i.

When V_i receives $\{Id_j, R_{jn}, R_{j1}, h_j\}$ from V_j. V_i first computes the shared key $SK_{ij}^{'}$, then V_i checks the correctness of the signature. If the signature is correct, V_i accepts the shared key $SK_{ij}^{'}$. The whole process is shown in Table 3 and Fig. 3.

1. Entity V_i calculates the shared key as: $SK_{ij}^{'} = h(e\left(R_{it}, R_{j1}\right)^{k_{i1}})$.
2. Entity V_i calculates $e_j^{'} = H_1(R_{jn} \| Id_j)$.
3. Entity V_i calculates $R_{jt}^{'} = k_{i1} \cdot (e_j^{'} \cdot R_{jn} + R_x)$.
4. Entity V_i checks if $h_j = h(Id_j \| R_{jn} \| R_{j1} \| SK_{ij}^{'} \| T_1 \| R_{jt}^{'})$, if they are equal, V_i accepts $SK_{ij}^{'}$ as the shared key.

Here is the proof of the correctness of the shared key $SK_{ij} = SK_{ij}^{'}$.

$$\begin{aligned} SK_{ij}^{'} &= h(e\left(R_{it}, R_{j1}\right)^{k_{i1}}) \\ &= h(e\left(R_{it}, k_{i1} \cdot R_{j1}\right)) \\ &= h(e\left(R_{it}, k_{i1} \cdot k_{j1} \cdot P\right)) \\ &= h(e\left(R_{it}, k_{j1} \cdot R_{i1}\right)) \\ &= h(e\left(R_{it}, R_{i1}\right)^{k_{j1}}) \\ &= h(e\left(R_{it}^{'}, R_{i1}\right)^{k_{j1}}) \\ &= SK_{ij} \end{aligned}$$

We prove the correctness of the validation process of a signature $R_{si} = d_i \cdot R_{it}$, after validation, entity V_j confirms that this message is from an entity V_i with identity Id_i and R_{in}. Suppose $R_{it} = H(Id_i \| R_{in} \| R_{i1} \| T_1) = R_{it}^{'}$ and $e_i = H_1(R_{in} \| Id_i) = e_i^{'}$, we can get the following proof.

$$\begin{aligned} e\left(P, R_{si}\right) &= e\left(P, d_i \cdot R_{it}\right) \\ &= e\left(P, R_{it}\right)^{d_i} \\ &= e\left(d_i \cdot P, R_{it}\right) \\ &= e\left(e_i \cdot (k_u + k_n) \cdot P + d_x \cdot P, R_{it}\right) \\ &= e\left(e_i \cdot (R_u + R_n) + R_x, R_{it}\right) \\ &= e\left(e_i^{'} \cdot R_{in} + R_x), R_{it}^{'}\right) \end{aligned}$$

IV. SECURITY ANALYSIS

In this section, we conduct a formal security analysis of the proposed scheme.

A. SECURITY OF THE REGISTRATION SCHEME

The security of the registration scheme is based on the computation hardness of the Elliptic Curve Discrete Logarithm (ECDL) problem. Suppose G_1 is a cyclic additive group of prime order q, P is a generator of G_1. Given an element Q of G_1, it is computationally intractable to find a $c \in Z_q^*$ such that $Q = cP$.

Theorem 1: The proposed registration scheme is secure against an external adversary if and only if the ECDL problem is unable to be solved in polynomial time.

Proof: ($\Rightarrow$) Suppose there is an efficient algorithm O_I that could break the ECDL problem in polynomial time. Suppose $R_x = Q$ and $d_x \cdot P = cP$, with algorithm O_I, an adversary is able to get the network manager's private key d_x. The adversary selects a random $R_{an} = (k_n + k_u) \cdot P$, with $R_n = k_n \cdot P$ and $R_u = k_u \cdot P$, now, the adversary can get a private key $d_a = H_1(R_{an} \| Id_a) \cdot (_n + k_u) + d_x$. With d_a and R_{an}, the adversary can pass the verification process at the authentication phase.

($\Leftarrow$) Suppose there is an external adversary could break the security of the registration scheme in polynomial time. For this adversary, given a random identity Id_a, he is able to find a $d_a = H_1(R_{an} \| Id_a) \cdot (k_n + k_u) + d_x$ and a $R_{an} = (k_n + k_u) \cdot P$, with which this adversary can pass the verification process at the authentication phase. Based on these information, we can

get: $d_a \cdot P = H_1(R_{an}||Id_a) \cdot (k_n + k_u) \cdot P + d_x \cdot P = H_1(R_{an}||Id_a) \cdot R_{an} + R_x$,. For the ECDL problem, suppose $c = d_a, H_1(R_{an}||Id_a) \cdot R_{an} + R_x = Q$, given an element of G_1: $Q = H_1(R_{an}||Id_a) \cdot R_{an} + R_x$, the adversary is able to find a $c = d_a$ such that $Q = cP$. This apparently contradicts the hardness of the ECDL problem.

B. MUTUAL AUTHENTICATION

The proposed scheme achieves mutual authentication, this is based on the computational hardness of the Elliptic Curve Computational Diffie–Hellman (ECCDH) problem. Suppose G_1 is a cyclic additive group of prime order q, P is a generator of G_1. For any $a, b, c \in Z_q^*$, given an instance $< aP, bP >$, it is computationally intractable to compute $cP = abP$.

Theorem 2: The proposed scheme achieves mutual authentication if and only if the ECCDH problem is unable to be solved in polynomial time.

We prove the proposed scheme achieves mutual authentication in two steps. First, we prove entity V_j can verify the legitimacy of entity V_i.

Proof: ($\Rightarrow$) Suppose there is an efficient algorithm O_I that could break the ECCDH problem. Given an random entity's identity Id_i, the corresponding public key $R_i = d_i \cdot P$ and R_{in}, an adversary can get a random $R_{i1} = k_{i1} \cdot P$, a timestamp T_1, and a $R_{it} = H(Id_i||R_{in}||R_{i1}||T_1)$. Suppose $aP = R_{it}$ and $bP = R_i = d_i \cdot P$, the adversary is able to compute $cP = abP = d_i \cdot R_{it} = R_{si}$ by using the algorithm O_I. Until now, the adversary can generate a message $\{Id_i, R_{in}, R_{i1}, R_{si}, T_1\}$, with which it can pass the verification of entity V_j.

($\Leftarrow$) Suppose there is an adversary could pass the verification process of entity V_j, which means the adversary could generate a message $\{Id_i, R_{in}, R_{i1}, R_{si}, T_1\}$, in which $R_{si} = d_i \cdot R_{it}, R_{it} = H(Id_i||R_{in}||R_{i1}||T_1)$ and $R_{i1} = k_{i1} \cdot P$, k_{i1} is a random number.

For the ECCDH problem, suppose $aP = R_{it}, bP = R_i = d_i \cdot P$ and $cP = abP = d_i \cdot R_{it} = R_{si}$, given aP, bP, the adversary is able to compute $cP = abP$ in polynomial time. This apparently contradicts to the hardness of the ECCDH problem.

Now, we have proved entity V_j can verify the legitimacy of entity V_i. Second, we prove entity V_i can verify the legitimacy of entity V_j.

Proof: ($\Rightarrow$) Suppose there is an efficient algorithm O_I that could break the ECCDH problem. Suppose $aP = R_j = d_j \cdot P$ and $bP = R_{i1} = k_{i1} \cdot P$, an adversary is able to compute $cP = abP = d_j \cdot R_{i1} = R_{jt}$ in polynomial time, which means the adversary can generate a message $\{Id_j, R_{jn}, R_{j1}, h_j\}$, in which $h_j = h(Id_j||R_{jn}||R_{j1}||SK_{ij}||T_1||R_{jt}), R_{j1} = k_{j1} \cdot P, SK_{ij} = h(e\left(R_{it}^{'}, R_{i1}\right)^{k_{j1}})$, k_{j1} is a random number. With this message, the adversary can pass the verification of entity V_i.

($\Leftarrow$) Suppose there is an adversary who could pass the verification process of entity V_i, which means the adversary could generate a message $\{Id_j, R_{jn}, R_{j1}, h_j\}$, in which $h_j = h(Id_j||R_{jn}||R_{j1}||SK_{ij}||T_1||R_{jt}), R_{jt} = d_j \cdot R_{i1}, R_{j1} = k_{j1} \cdot P, SK_{ij} = h(e\left(R_{it}^{'}, R_{i1}\right)^{k_{j1}}), R_{it}^{'} = H(Id_i||R_{in}||R_{i1}||T_1)$. With this message, the adversary can pass the verification process of entity V_i, as the SHA-256 is secure, the adversary must have got R_{jt}.

For the ECCDH problem, suppose $aP = R_j = d_j \cdot P, bP = R_{i1} = k_{i1} \cdot P$ and $cP = abP = R_{jt} = d_j \cdot R_{i1}$, an adversary is able to compute $cP = abP$ in polynomial time. This apparently contradicts to the hardness of the ECCDH problem.

Now, we have proved that entity V_i can verify the legitimacy of entity V_j, we get the conclusion that the proposed scheme achieves mutual authentication.

C. PERFECT FORWARD PRIVACY

Bilinear Computational Diffie–Hellman (BCDH) problem is thought to be a computational hardness, suppose G_1 is a cyclic additive group of prime order q, P is a generator of G_1. For any $a, b, c \in Z_q^*$, given an instance $< aP, bP, cP >$, it is computationally intractable to compute $e(P, P)^{abc}$.

Theorem 3: The proposed scheme achieves perfect forward privacy if and only if the BCDH problem is unable to be solved in polynomial time.

Proof: ($\Rightarrow$) Suppose there is an efficient algorithm O_I that could break the BCDH problem in polynomial time. Given $aP = k_{i1} \cdot P = R_{i1}, bP = k_{j1} \cdot P = R_{j1}$ and $cP = R_{it} = R_{it}^{'} = H(Id_i||R_{in}||R_{i1}||T_1)$ of an arbitrary past session, an adversary can compute $e(P, P)^{abc} = e\left(R_{it}^{'}, R_{i1}\right)^{k_{j1}} = e\left(R_{it}, R_{j1}\right)^{k_{i1}}$ by using algorithm O_I, which means the adversary is able to get the shared key of an arbitrary past session as: $SK_{ij} = h\left(e\left(R_{it}^{'}, R_{i1}\right)^{k_{j1}}\right) = h(e\left(R_{it}, R_{j1}\right)^{k_{i1}}) = SK_{ij}^{'}$.

($\Leftarrow$) Suppose there is an adversary who could get the session key of an arbitrary past session, for example, $SK_{ij} = h\left(e\left(R_{it}^{'}, R_{i1}\right)^{k_{j1}}\right) = h(e\left(R_{it}, R_{j1}\right)^{k_{i1}}) = SK_{ij}^{'}$, as the SHA-256 is secure, the adversary must have got $e\left(R_{it}^{'}, R_{i1}\right)^{k_{j1}} = e\left(R_{it}, R_{j1}\right)^{k_{i1}}$.

For the BCDH problem, suppose $aP = k_{i1} \cdot P = R_{i1}, bP = k_{j1} \cdot P = R_{j1}$ and $cP = R_{it} = H(Id_i||R_{in}||R_{i1}||T_1)$, an adversary is able to compute $e(P, P)^{abc}$ in polynomial time. This apparently contradicts to the hardness of the BCDH problem.

V. SECURITY ANALYSIS USING BAN LOGIC

BAN logic is a security analysis tool used to determine if the exchanged information is trustworthy, secure against eavesdropping etc [27], [28]. In this section, we conduct a security analysis of the proposed scheme using BAN logic. BAN logic can be easily applied and it can give us a quick insight of the authentication protocols. BAN logic makes it possible to reason in a very simple way over the authentication protocols in a formal way, it ensures all the publicly shared key primitives are formalized. When BAN logic is used in the design of an authentication protocol, it helps us to exclude potential faults.

TABLE 4. Symbols of BAN logic.

SYMBOL	MEANING
$P \mid\equiv X$	P believes X.
$P \lhd X$	P sees/receives X.
$P \mid\sim X$	P once said X (or P sent X).
$\#(X)$	X is fresh.
$PK(K,U)$	Entity U has associated a good public key K.
$\prod(U)$	Entity U has a good private key. This private key is only known to U.
$\sigma(X,U)$	Formula X is signed with the private key of U.
$\Delta(t_1, t_2)$	t_1, t_2 denotes a good interval.
$(\Theta(t_1, t_2), X)$	X holds in the internal between t_1 and t_2. The creator which uttered the timestamped message X, claims that X is, or was, good in the time interval between t_1 and t_2.

TABLE 5. Some primary BAN logic postulates.

RULE	BAN LOGIC FORM
#()-introduction	$\frac{P \text{ creates } X}{P \mid\equiv \#(X)}$
$\overset{k}{\longleftrightarrow}$ introduction	$\frac{P \mid\equiv \#(k),\ P \mid\equiv Q \mid\equiv X}{P \mid\equiv P \overset{k}{\longleftrightarrow} Q}$
promotion #	$\frac{P \mid\equiv \#(X)}{P \mid\equiv \#((X,Y))}, \frac{P \mid\equiv \#(X)}{P \mid\equiv \#(\alpha^X)}$
elimination of multipart messages	$\frac{P \mid\equiv Q \mid\sim (X,Y)}{P \mid\equiv Q \mid\sim X}, \frac{P \mid\equiv Q \mid\equiv (X,Y)}{P \mid\equiv Q \mid\equiv X}, \frac{P \mid\equiv (X,Y)}{P \mid\equiv X}, \frac{P \lhd (X,Y)}{P \lhd X}$
once-said for public key crypto systems	$\frac{P \mid\equiv PK(K,Q),\ P \mid\equiv \prod(Q),\ P \lhd \sigma(X,Q)}{P \mid\equiv Q \mid\sim X}$
reasoning about duration-stamps	$\frac{P \mid\equiv Q \mid\equiv \Delta(t_1,t_2),\ P \mid\equiv Q \mid\sim (\Theta(t_1,t_2),X)}{P \mid\equiv Q \mid\equiv X}$

TABLE 6. The idealized form of the messages.

MESSAGE	FLOW	IDEALIZED FORM
1	$V_i \rightarrow V_j$	$\sigma((\Theta(\delta_{t1}), X_i), V_i)$
2	$V_j \rightarrow V_i$	$\sigma((\Theta(\delta_{t2}), X_j), V_j)$

It also helps us to optimize the design, for example, to remove the unnecessary actions.

A. NOTIONS AND POSTULATES

First, some symbols and primary postulates are described in Table 4 and Table 5.

B. MESSAGES AND GOALS

We translate the messages into an idealized form of BAN logic, the results are shown in Table 6.

Let $\delta_{t1} = (t_1, t_2)$ be a time duration, we write $\Theta(\delta_{t1})$ for $\Theta(t_1, t_2)$. Let $\delta_{t2} = (t_1, t_3)$, we write $\Theta(\delta_{t2})$ for $\Theta(t_1, t_3)$. Let $X_i = \{Id_i, R_{in}, R_{i1}\}$, entity V_i claims X_i holds in the time interval δ_{t1}, we can get $(\Theta(\delta_{t1}), X_i)$. As $(\Theta(\delta_{t1}), X_i)$ is signed with the private key of entity V_i, we can get the idealized form of message 1: $\sigma((\Theta(\delta_{t1}), X_i), V_i)$. Let $X_j = \{Id_j, R_{jn}, R_{j1}, SK\}$, we can get the idealized form of message 2 as: $\sigma((\Theta(\delta_{t2}), X_j), V_j)$.

There are two goals for the proposed scheme: $V_i| \equiv V_i \overset{SK}{\longleftrightarrow} V_j$ and $V_j| \equiv V_i \overset{SK}{\longleftrightarrow} V_j$. These goals ensure entity V_i and entity V_j to agree on a shared key SK.

C. ASSUMPTIONS

First, entity V_i and entity V_j believes the opponent's timestamp, we get assumption A1: $V_i| \equiv V_j| \equiv \Delta(\delta_{t2})$ and assumption A2: $V_j| \equiv V_i| \equiv \Delta(\delta_{t1})$.

Second, after registration, entities have achieved the correct public key, we get assumptions A3: $V_i| \equiv PK(R_j, V_j)$ and A4: $V_j| \equiv PK(R_i, V_i)$. All entities believe that everyone else keeps their private keys private, we get assumptions A5: $V_i| \equiv \prod(V_j)$ and assumptions A6: $V_j| \equiv \prod(V_i)$.

D. PROOF OF THE PROPOSED SCHEME

First, we analyze the idealized form of message 1.

1. Message 1 gives us:
$$V_j \lhd \sigma((\Theta(\delta_{t1}), X_i), V_i) \tag{1}$$
2. According to (1), A4, A6 and the "once-said for public key crypto systems" rule:
$$V_j \mid\equiv V_i| \sim (\Theta(\delta_{t1}), X_i) \tag{2}$$
3. According to A2, (2) and the "reasoning about duration-stamps" rule:
$$V_j \mid\equiv V_i| \equiv X_i \tag{3}$$
4. According to (3) and " ','-elimination" rule:
$$V_j \mid\equiv V_i| \equiv R_{i1} \tag{4}$$
5. As k_{j1} is randomly created by V_j, according to "#()-introduction" rule:
$$V_j| \equiv \#(k_{j1}) \tag{5}$$
6. According to (5) and the "promotion #" rule:
$$V_j| \equiv \#(SK), SK = h\left(e\left(R'_{it}, R_{i1}\right)^{k_{j1}}\right) \tag{6}$$
7. According to (6), (4), and "$\overset{k}{\longleftrightarrow}$ introduction" rule:
$$V_j| \equiv V_j \overset{SK}{\longleftrightarrow} V_i \tag{7}$$

Second, we start to analyze the message 2.

8. Message 2 gives us:
$$V_i \lhd \sigma((\Theta(\delta_{t2}), X_j), V_j) \tag{8}$$
9. According to (8), A3, A5 and the "once-said for public key crypto systems" rule:
$$V_i \mid\equiv V_j| \sim (\Theta(\delta_{t2}), X_j)) \tag{9}$$
10. According to A1, (9) and the "reasoning about duration-stamps" rule:
$$V_i \mid\equiv V_j| \equiv X_j \tag{10}$$

TABLE 7. Assumptions.

NUMBER	ASSUMPTIONS	NUMBER	ASSUMPTIONS
A1	$V_i \mid\equiv V_j \mid\equiv \Delta(\delta_{t2})$	A2	$V_j \mid\equiv V_i \mid\equiv \Delta(\delta_{t1})$
A3	$V_i \mid\equiv PK(R_j, V_j)$	A4	$V_j \mid\equiv PK(R_i, V_i)$
A5	$V_i \mid\equiv \prod(V_j)$	A6	$V_j \mid\equiv \prod(V_i)$

TABLE 8. Computation time of basic operations in milliseconds.

TYPE	G_{bp}	G_{mul}	G_{add}	G_{h2e}	G_{h2b}	GT_{exp}	$hash$
Time	2.8419	4.6267	0.0168	0.9809	0.0043	0.4409	0.0037

11. According to (10) and " ','-elimination" rule:

$$V_i \mid\equiv V_j \mid\equiv R_{j1} \tag{11}$$

12. As k_{i1} is randomly created by V_i, according to "#()-introduction" rule:

$$V_i \mid\equiv \#(k_{i1}) \tag{12}$$

13. According to (12), and the "promotion #" rule:

$$V_i \mid\equiv \#(SK), SK = h(e\left(R_{it}, R_{j1}\right)^{k_{i1}}) \tag{13}$$

14. According to (13), (11), and "$\overset{k}{\longleftrightarrow}$ introduction" rule:

$$V_i \mid\equiv V_i \overset{SK}{\longleftrightarrow} V_j \tag{14}$$

Now, we have proved the two goals of the scheme. We can say that the proposed scheme is secure under BAN logic.

VI. COMPARISON

In this section, we compared the schemes in computational overhead and communication overhead.

A. COMPUTATIONAL PERFORMANCE ANALYSIS

We simulated the scheme in Java environment, the JDK version is 1.8. The cryptography library used in this study is the Java Pairing-Based Cryptography Library (JPBC) [29]. Type A pairings are constructed on the curve $y^2 = x^3 + x$ over the field F_q for some prime $q = 3mod4$. Both G_1, G_2 are the group of points $E(F_q)$. The computation cost of general hash operation is calculated based on the SHA-256. The experiment is conducted on a computer with a 64-bits Windows 7 enterprise operating system, with Intel(R) Core(TM) i73370K CPU 3.5 GHz processor, 8 GB memory. Part of the code has been uploaded to a public library in github.com [30]. The parameters of the curve are listed at Appendix A, q is 256 bit, and order r is 224 bit, we choose these parameters because the recommended elliptic curve key length is 256 bit for 2016-2030 by NIST [31], and for 2018 - 2028 by ECRYPR [32], the experiment results are shown in Table 8.

1. G_{bp} a bilinear map pairing operation
2. G_{mul} an element of G_1 multiply a big integer operation
3. G_{add} an element addition operation of G_1
4. G_{h2e} a hash to an element of G_1
5. G_{h2b} a hash to big integer operation
6. GT_{exp} an element exponentiation in G_T
7. $hash$ the SHA-256 operation

TABLE 9. Computation cost of the registration phase.

SCHEMES	G_{mul}	G_{add}	G_{h2b}	TIME
Mahmood [6]	1	0	1	4.63
Abbasinezhad [7]	4	2	3	18.55
Our scheme	2	2	2	9.30

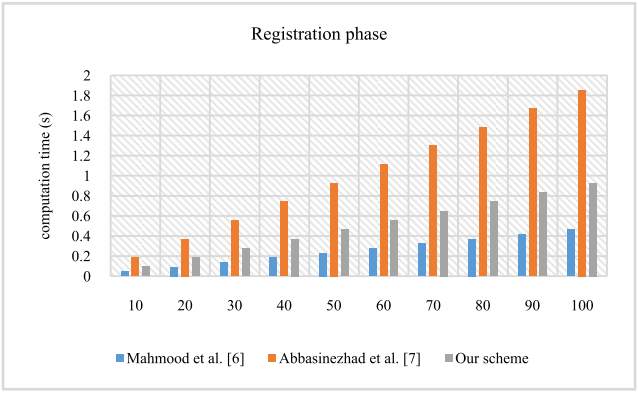


FIGURE 4. The computation overhead of registration phase.

TABLE 10. Computation cost of the authentication phase.

SCHEME	G_{bp}	G_{mul}	G_{add}	G_{h2e}	G_{h2b}	GT_{exp}	$hash$	TIME
Mahmood [6]	0	10	4	0	6	0	2	46.37
Abbasinezhad[7]	0	8	4	0	2	0	6	37.11
Our scheme	4	7	2	2	2	2	4	46.65

We compared the computation costs in the form of security operations per phase. At registration phase, the scheme of Mahmood et al. needs $1G_{mul}$, $1G_{h2b}$ operations. The scheme of Abbasinezhad et al. requires $4G_{mul}$, $2G_{add}$ and $3G_{h2b}$ operations. The proposed scheme requires $2G_{mul}$, $2G_{add}$ and $2G_{h2b}$ operations. The results are shown in Table 9.

Fig. 4 shows the computation costs of the registration phase in milliseconds, the horizontal axis indicates the number of registration times; the vertical axis indicates the computation time in milliseconds. Compared to the scheme of Mahmood et al., the proposed scheme needs more computation time, however, in their scheme, the private key of an arbitrary entity is known to the network manager, for the proposed scheme, the network manager is unable to learn the private key of an arbitrary entity, for this reason, the proposed scheme needs more computation time. Compared to the scheme of Abbasinezhad et al., the proposed scheme is more efficient, and the two schemes achieve the same security level.

For the authentication phase, the scheme of Mahmood et al. needs $10G_{mul}$, $4G_{add}$, $6G_{h2b}$ and $2hash$ operations. The scheme of Abbasinezhad et al. requires $8G_{mul}$, $4G_{add}$, $2G_{h2b}$ and $6hash$ operations. The proposed scheme requires $4G_{bp}$, $7G_{mul}$, $2G_{add}$, $2G_{h2b}$, $2G_{h2e}$, $2GT_{exp}$ and $4hash$ operations. The results are shown in Table 10.

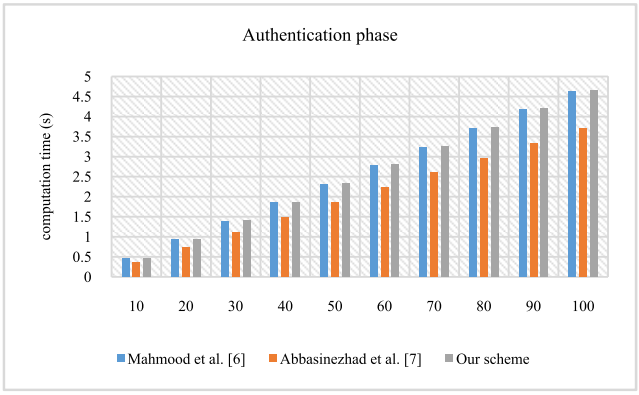


FIGURE 5. The computation overhead of authentication phase.

Fig. 5 shows the computation costs of authentication phase in milliseconds; the horizontal axis indicates the number of authentication times; the vertical axis indicates the computation time, the unit is a second. Compared to the proposed scheme, the computation cost of the scheme of Abbasinezhad et al. needs less computation time, about 9.54ms per phase. This is mainly because in their scheme, the first message is not signed by the sender, however, in the proposed scheme, for security reason, every message is signed by the sender, thus the receiver can verify the correctness of the messages. Compared to the scheme of Mahmood et al., the proposed scheme needs almost the same computation time.

However, if we consider the differences and particularities of the implementation of the schemes in different environments, the computation costs of different operations may be different. Let the total running time of Abbasinezhad et al. be $T_A = 8G_{mul} + 4G_{add} + 2G_{h2b} + 6hash$, the total running time of Mahmood et al. be $T_M = 10G_{mul} + 4G_{add} + 6G_{h2b} + 2hash$ the total running time of the proposed scheme be $T_p = 4G_{bp} + 7G_{mul} + 2G_{add} + 2G_{h2e} + 2G_{h2b} + 2GT_{exp} + 4hash$. We can get: $T_A - T_p = G_{mul} + 2G_{add} + 2hash - 4G_{bp} - 2GT_{exp} - 2G_{h2e}$ and $T_M - T_p = 3G_{mul} + 2G_{add} + 4G_{h2b} - 4G_{bp} - 2G_{h2e} - 2GT_{exp} - 2hash$, when $(T_A - T_p) \geq 0$ or $(T_M - T_p) \geq 0$, the proposed scheme is more efficient.

B. COMMUNICATION OVERHEAD

The SHA-256 is used in this study, the result of the general hash operation is 256 bit. The bit lengths of an element in G_1 is 512 bit, the order is 224 bit. The bit size of a timestamp is 32 bit, the bit size of an identity is 32 bit.

For the scheme of Mahmood et al., the messages sent at the registration phase are $\{Id_i\}$ and $\{K_{ip}, K_{is}\}$, Id_i is an identity, it is 32 bit, K_{is} is a modulo of the order, it is 224 bit, K_{ip} is an element of G_1, it is 512 bit. The communication cost is 32 + 512 + 224 = 768 bit. At authentication phase, the messages sent between the two entities are $\{Id_i, X_i, Y_i, K_{ip}, t_i\}$ and $\{Id_j, X_j, Y_j, K_{jp}, t_j\}$, Id_i and Id_j are identities, the bit length are both 32 bit, respectively, X_i, K_{ip}, X_j, K_{jp} are elements of G_1, the bit length is 512 bit, Y_i, Y_j are modulus of the order, they are both 224 bit, t_i, t_j are timestamps. The communication cost of the authentication phase is 32*2+512*4+224*2+32*2 = 2624 bit.

TABLE 11. Communication costs.

Schemes	Registration	Authentication
Mahmood [6]	768 bit/ 2 messages	2624 bit/ 2 messages
Abbasinezhad [7]	1280 bit/ 2 messages	2656 bit/ 3 messages
Our scheme	1280 bit/ 2 messages	2912 bit/ 2 messages

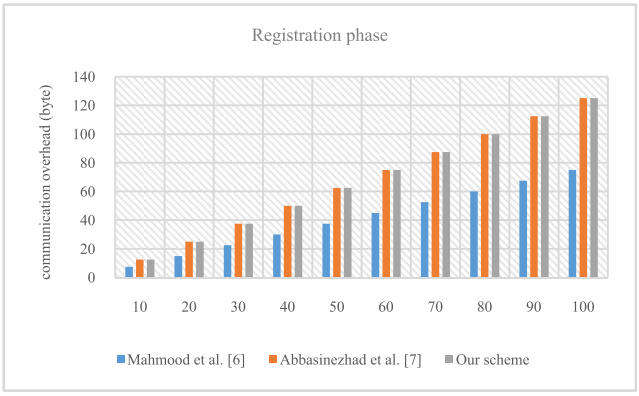


FIGURE 6. Communication overhead of registration phase.

For the scheme of Abbasinezhad et al., the messages sent at the registration phase are $\{Id_x, R_x\}$ and $\{y_x, WT_x\}$, Id_x is an identity, it is 32 bit, y_x is a modulo of the order, it is 224 bit, R_x and WT_x are elements of G_1, they are both 512 bit. The communication cost is 32 + 512*2 + 224 = 1280 bit. At authentication phase, the messages sent between the two entities are $\{Id_A, R_A, WT_A\}$, $\{Id_B, R_B, V_B, WT_B\}$ and $\{Id_A, V_A\}$, Id_A and Id_B are identities, the bit length is 32 bit, R_A, WT_A, R_B, WT_B are elements of G_1, the bit length is 512 bit, V_B, V_A are the results of SHA-256, the bit length is 256 bit, the communication cost of authentication phase is 32*3 + 512*4 + 256*2 = 2656 bit.

For the proposed scheme, the messages sent at the registration phase are $\{Id_i, R_u\}$ and $\{s_i, R_n\}$, Id_i is an identity, it is 32 bit, s_i is a modulo of the order, it is 224 bit, R_u and R_n are elements of G_1, they are both 512 bit. The communication cost is 32 + 512*2 + 224 = 1280 bit. At authentication phase, the messages sent between the two entities are $\{Id_i, R_{in}, R_{i1}, R_{si}, T_1\}$ and $\{Id_j, R_{jn}, R_{j1}, h_j\}$. Id_i and Id_j are both identities, the bit length is 32 bit, $R_{in}, R_{i1}, R_{jn}, R_{j1}, R_{si}$ are elements of G_1, the bit length is 512 bit, h_j is the result of SHA-256, it is 256 bit, T_1 is a timestamp, the communication cost of the authentication phase is 32*2+512*5+256+32 = 2912 bit. The results are shown in Table 11.

Fig. 6 shows the communication overhead of the registration phase, although the communication cost of the scheme of Mahmood et al. is lower, however, in their scheme, the private key of an arbitrary entity is known to the network manager. Fig. 7 shows the communication overhead for authentication phase, the horizontal axis indicates the number of times;

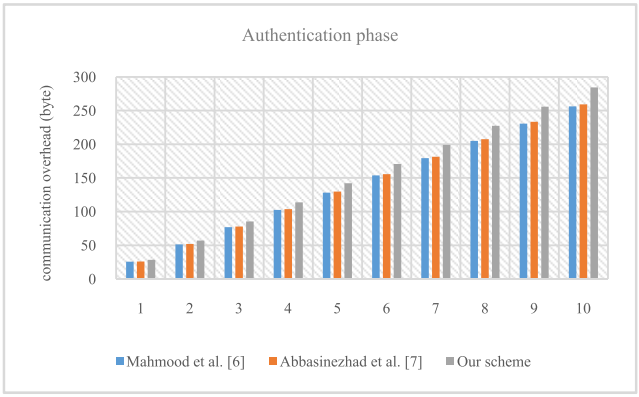


FIGURE 7. Communication overhead of authentication phase.

TABLE 12. Security features.

Comparison	Mahmood [6]	Abbasinezhad [7]	Our
Replay attack	√	×	√
Private key privacy	×	√	√
Private key leakage	×	√	√
Perfect forward privacy	×	–	√
Early detection of illegal entities	×	×	√
Impersonate attack	√	√	√
Man in middle attack	√	√	√
Message integrity	√	×	√
Round of messages	2	3	2

the vertical axis indicates the communication cost in bits, although the communication cost of the proposed scheme is higher. However, compared to the scheme of Mahmood et al., the proposed scheme have more security features; compared to the scheme of Abbasinezhad et al., in the proposed scheme only two messages needs to be sent, while in their scheme 3 messages need to be sent, besides, in the message 1 of their scheme, there is not a timestamp or a signature, the receiver cannot check the integrity and the source of this message.

VII. SECURITY FEATURES COMPARISON

We compare the security features of different schemes, the result is shown in Table 12.

A. REPLAY ATTACK

When it comes to replay attack, in the proposed scheme, there is a timestamp T_1 in the message $\{Id_i, R_{in}, R_{i1}, R_{si}, T_1\}$, besides, the timestamp T_1 is also concealed in R_{si}, if an adversary sends a former message, the entity will abandon this message after checking the timestamp. However, if the adversary replaces the old timestamp with a new one, the entity will find it out by checking the signature R_{si}.

For the scheme of Abbasinezhad et al., as there is not a signature or a timestamp in message Id_A, R_A, WT_A, if an adversary sends a former message to a legitimate entity, this entity will accept this message. If an adversary keeps sending former messages to this entity, the entity has to deal with these messages and it will not be accessible to the other legitimate entities in the system.

B. MESSAGE INTEGRITY

For the scheme of Abbasinezhad et al., as there is not a signature in message Id_A, R_A, WT_A, if this message is tampered or altered by an adversary, and sent to a legitimate entity, the receiver is unable to find out if this message has been tampered with or altered by an adversary. Thus, their scheme cannot ensure the integrity of the message. Besides, as there is not a signature in this message, their scheme cannot ensure authentication on this message neither.

C. PRIVATE KEY PRIVACY

For the private key privacy, in the proposed scheme, the private key of an arbitrary entity is $d_i = e_i \cdot (k_n + k_u) + d_x$, the network manager knows d_x, e_i and k_n, however, it does not know k_u, it is unable to know the private key of an arbitrary entity, the probability the network manager learns the private key of an entity by guessing is $\frac{1}{2^{224}}$. On the other hand, the probability an entity learns the private key of the network manager by guessing is $\frac{1}{2^{224}}$, too. This is the same as that of the scheme of Abbasinezhad et al, which means the two schemes have the same security level.

However, in the scheme of Mahmood et al., the private key of an arbitrary entity is generated by the network manager, the network manager knows the private key of all the entities.

D. PRIVATE KEY LEAKAGE PROBLEM

For the scheme of Mahmood et al., once an adversary learns the session ephemeral information x_i, and the public information $\{Id_i, X_i, Y_i, K_{ip}, t_i\}$ and $\{Id_j, X_j, Y_j, K_{jp}\}$, the adversary is able to get the private key of an entity as: $(Y_i - x_i) \cdot H_2^{-1}(Id_j, X_i, t_i)$. In this way, their scheme has the potential private key leakage problem.

E. PERFECT FORWARD PRIVACY

For the scheme of Mahmood et al., once the private key of an entity is compromised, for example, if an adversary coincidentally learns a private key K_{is}, the adversary is able to compute the shared key $SK = H_3(x_i X_j)$, as $x_i = Y_i - K_{is} \cdot H_2(Id_j, X_i, t_i)$, based on public messages of the past sessions $\{Id_i, X_i, Y_i, K_{ip}, t_i\}$ and $\{Id_j, X_j, Y_j, K_{jp}\}$.

For the scheme of Abbasinezhad et al., once the private key of the two entities are compromised, which means if an adversary gets the private key sk_a and sk_b. The adversary is able to compute the shared key $SSK_{AB} = H_3(Id_A||Id_B||(sk_b \cdot R_A + sk_a \cdot R_B))$ based on the public messages of the past sessions: $\{Id_A, R_A, WT_A\}$, $\{Id_B, R_B, V_B, WT_B\}$ and $\{Id_A, V_A\}$.

For the proposed scheme, even if the private keys of both entities are leaked, the adversary is unable to get the shared key of the past sessions.

F. EARLY DETECTION OF ILLEGAL MESSAGE

In some cases, an adversary sends fake messages to a legitimate entity to deplete its computation ability, thus the ability to find out if a message is a fake one or not is important. For the scheme of Mahmood et al., if an adversary send a fake message $\{Id_1, X_1, Y_1, K_1, t_1\}$ to an entity, Id_1 is a random identity, X_1 and K_1 are random elements of G_1, and Y_1 is a random number, the recipient entity cannot know if this is a legitimate message or not, he will conducts the same steps as he does in the normal way.

For the scheme of Abbasinezhad et al. If an adversary sends a fake message $\{Id_1, R_1, WT_1\}$ to a legitimate entity V_j, where Id_1 is a random identity, R_1 and WT_1 are random elements of G_1. Entity V_j is unable to judge whether this is a legitimate message or not. However, if an adversary keeps sending these messages, entity V_j will get busy dealing with these messages, and it will not be accessible to other legitimate entities.

For the proposed scheme, if an adversary sends a fake message $\{Id_i, R_{in}, R_{i1}, R_{si}, T_1\}$ to entity V_j. V_j can find out this message is not a legitimate one by checking the timestamp and the signature in the following steps. If an adversary keeps sending fake messages, V_j will reject the messages from this source.

1. Entity V_j checks the timestamp T_1.
2. Entity V_j gets $R_{it}^{'} = H(Id_i||R_{in}||R_{i1}||T_1)$, which is an element of G_1, and $e_i^{'} = H_1(R_{in}||Id_i)$.
3. Entity V_j checks if $e(P, R_{si}) = e\left(e_i^{'} \cdot R_{in} + R_x, R_{it}^{'}\right)$, if they are equal, V_j accepts the message, otherwise, V_j abandons the messages.

VIII. CONCLUSION

In this study, we first analyzed existing schemes, we found the two of them failed to provide all the security features as they claimed, and both of them have potential security issues, for example, private key leakage problem. Thus, we proposed a pairing based authentication scheme for smart grid scenario, which gains more security features compared to related works, for example, the proposed scheme ensures private key privacy, perfect forward privacy and message integrity etc. We designed a simpler registration scheme, the computation cost is reduced. However, compared to related work, the proposed registration scheme implements the same functionalities, and achieves the same or a higher security level. We conducted a formal security analysis of the proposed authentication scheme, the result shows the scheme is secure. The analysis of BAN logic also shows that the proposed scheme is secure. In addition, we implemented the scheme in a Java environment, we validate our analysis of communication overhead and computation overhead. In all, the proposed scheme gains an advantage as it has more security features and a comparable computation cost and communication cost.

APPENDIX

Here are the parameters of the elliptic curve used in the experiment.

TABLE 13. Parameters of the elliptic curve.

Name	Data
q	75844028390781998704593395418996586982331 5
	82100438383475677635183597129065931
r	13479973333575319897344925525051463 0
	15867038499025882201642867097601
h	5626422732

ACKNOWLEDGMENT

The proposal presented in this paper is part of the work made in the European project "Sustainable-Smart Grid Open System for the Aggregated Control, Monitoring and Management of Energy" (e-GOTHAM).

REFERENCES

[1] *Smart Metering Deployment in the European Union | JRC Smart Electricity Systems and Interoperability*. Accessed: Dec. 1, 2018. [Online]. Available: http://ses.jrc.ec.europa.eu/smart-metering-deployment-european-union

[2] *Smart Metering in Europe*. Accessed: Dec. 1, 2018. [Online]. Available: http://www.berginsight.com/ReportPDF/ProductSheet/bi-sm13-ps.pdf

[3] *Commission Recommendation of 10 October 2014 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems' 32014H0724*. Accessed: Oct. 19, 2017. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.300.01.0063.01.ENG

[4] Y. Kabalci, "A survey on smart metering and smart grid communication," *Renew. Sustain. Energy Rev.*, vol. 57, pp. 302–318, May 2016. doi: 10.1016/j.rser.2015.12.114.

[5] D. Abbasinezhad-Mood and M. Nikooghadam, "An ultra-lightweight and secure scheme for communications of smart meters and neighborhood gateways by utilization of an ARM Cortex-M microcontroller," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6194–6205, Nov. 2018. doi: 10.1109/TSG.2017.2705763.

[6] K. Mahmood, S. A. Chaudhry, H. Naqvi, S. Kumari, X. Li, and A. K. Sangaiah, "An elliptic curve cryptography based lightweight authentication scheme for smart grid communication," *Future Gener. Comput. Syst.*, vol. 81, pp. 557–565, Apr. 2018.

[7] D. Abbasinezhad-Mood and M. Nikooghadam, "Design and hardware implementation of a security-enhanced elliptic curve cryptography based lightweight authentication scheme for smart grid communications," *Future Gener. Comput. Syst.*, vol. 84, pp. 47–57, Jul. 2018.

[8] D. Wu and C. Zhou, "Fault-tolerant and scalable key management for smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 375–381, Jun. 2011.

[9] J. Xia and Y. Wang, "Secure key distribution for the smart grid," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1437–1443, Sep. 2012.

[10] J. Liu, L. Zhang, and R. Sun, "1-RAAP: An efficient 1-round anonymous authentication protocol for wireless body area networks," *Sensors*, vol. 16, no. 5, p. 728, May 2016.

[11] X. Li, "An enhanced 1-round authentication protocol for wireless body area networks with user anonymity," *Comput. Elect. Eng.*, vol. 61, pp. 238–249, Jul. 2017. doi: 10.1016/j.compeleceng.2017.02.011

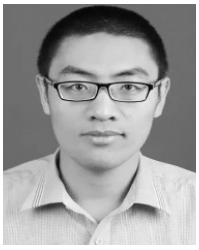
[12] S. Kumari, S. A. Chaudhry, F. Wu, X. Li, M. S. Farash, and M. K. Khan, "An improved smart card based authentication scheme for session initiation protocol," *Peer-Peer Netw. Appl.*, vol. 10, no. 1, pp. 92–105, Jan. 2017.

[13] S. Wu, Y. Zhu, and Q. Pu, "Robust smart-cards-based user authentication scheme with user anonymity," *Secur. Commun. Netw.*, vol. 5, no. 2, pp. 236–248, Feb. 2012.

[14] X. Huang, X. Chen, J. Li, Y. Xiang, and L. Xu, "Further observations on smart-card-based password-authenticated key agreement in distributed systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 7, pp. 1767–1775, Jul. 2014.

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

[16] V. Odelu, A. K. Das, M. Wazid, and M. Conti, "Provably secure authenticated key agreement scheme for smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1900–1910, May 2016.
[17] Y.-M. Tseng, S.-S. Huang, T.-T. Tsai, and J.-H. Ke, "List-free ID-based mutual authentication and key agreement protocol for multiserver architectures," *IEEE Trans. Emerg. Topics Comput.*, vol. 4, no. 1, pp. 102–112, Jan./Mar. 2016.
[18] J.-L. Tsai and N.-W. Lo, "A privacy-aware authentication scheme for distributed mobile cloud computing services," *IEEE Syst. J.*, vol. 9, no. 3, pp. 805–815, Sep. 2015.
[19] F. Li and J. Hong, "Efficient certificateless access control for wireless body area networks," *IEEE Sensors J.*, vol. 16, no. 13, pp. 5389–5396, Jul. 2016.
[20] D. Li, Z. Aung, J. R. Williams, and A. Sanchez, "Efficient and fault-diagnosable authentication architecture for AMI in smart grid," *Secur. Commun. Netw.*, vol. 8, no. 4, pp. 598–616, Mar. 2015.
[21] R. Lu, X. Lin, and X. Shen, "SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 3, pp. 614–624, Mar. 2013.
[22] K. Mahmood, S. A. Chaudhry, H. Naqvi, T. Shon, and H. F. Ahmad, "A lightweight message authentication scheme for smart grid communications in power sector," *Comput. Elect. Eng.*, vol. 52, pp. 114–124, May 2016. doi: 10.1016/j.compeleceng.2016.02.017.
[23] D. Wang, N. Wang, P. Wang, and S. Qing, "Preserving privacy for free: Efficient and provably secure two-factor authentication scheme with user anonymity," *Inf. Sci.*, vol. 321, pp. 162–178, Nov. 2015.
[24] M. Wazid, A. K. Das, M. K. Khan, A. A. D. Al-Ghaiheb, N. Kumar, and A. V. Vasilakos, "Secure authentication scheme for medicine anti-counterfeiting system in IoT environment," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1634–1646, Oct. 2017.
[25] S.-J. Horng, S.-F. Tzeng, P.-H. Huang, X. Wang, T. Li, and M. K. Khan, "An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks," *Inf. Sci.*, vol. 317, pp. 48–66, Oct. 2015.
[26] A. Akhunzada *et al.*, "Man-at-the-end attacks: Analysis, taxonomy, human aspects, motivation and future directions," *J. Netw. Comput. Appl.*, vol. 48, pp. 44–57, Feb. 2015.
[27] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," *Proc. Roy. Soc. London A, Math., Phys. Eng. Sci.*, vol. 426, no. 1871, pp. 233–271, Dec. 1989. doi: 10.1098/rspa.1989.0125.
[28] K. Gaarder and E. Snekkenes, "Applying a formal analysis technique to the CCITT X.509 strong two-way authentication protocol," *J. Cryptol.*, vol. 3, no. 2, pp. 81–98, Jan. 1991.
[29] *The Java Pairing Based Cryptography Library (JPBC)*. Accessed: Feb. 13, 2019. [Online]. Available: http://gas.dia.unisa.it/projects/jpbc/#.Wc0m51uCyUl
[30] *Source Code of This Study*. Accessed: Feb. 13, 2019. [Online]. Available: https://github.com/SevenBruce/JPBC
[31] *Recommendation for Key Management, Part 1: General, SP 800-57 Part 1 Rev. 4*, NIST, Gaithersburg, MD, USA, Jan. 2016. [Online]. Available: https://www.keylength.com/en/compare/
[32] *Algorithms, Key Size and Protocols Report (2018)*, document H2020-ICT-2014-Project 645421, D5.4, ECRYPT-CSA, Feb. 2018.



YUWEN CHEN received the M.S. degree in computer software and theory from Zhengzhou University, Zhengzhou, China, in 2015. He is currently pursuing the Ph.D. degree in telematic engineering with the Technical University of Madrid, Madrid, Spain.

His research interests include the IoT security and privacy, and smart grid privacy and security.

JOSÉ-FERNÁN MARTÍNEZ received the Ph.D. degree in telematic engineering from the Technical University of Madrid, Madrid, Spain, in 2001, where he is currently an Associate Professor with the Department of Engineering and Telematic Architectures.

He is responsible for different Spanish and European public-funded research projects and also research contracts with different IT companies. His main research interests include ubiquitous computing and the Internet of Things, smart cities and wireless sensor and actuators networks, next-generation telematic network and services, software engineering and architectures, distributed applications and intermediation platforms (middleware), and high-performance and fault-tolerant systems. He has authored several national and international publications included in the Science Citation Index in his interest areas. He has participated in several international and European projects.

Dr. Martínez is a Technical Reviser and the Chair of technical national and international events on telematics and a member of different international and scientific committees.

PEDRO CASTILLEJO received the Ph.D. degree in telematic engineering from the Universidad Politécnica de Madrid (UPM), Madrid, Spain, in 2015.

He is a member of the Group of Next-Generation Networks and Services, UPM, where he is also a Researcher in different European projects, such as LIFEWEAR, DEMANES, E-GOTHAM, I3RES, and SWARMs. He has several conference presentations and paper published in indexed journals. He has also participated as an invited Lecturer in different bachelor's, master's, and doctoral courses. His current research interests include wireless sensor networks, network security algorithms, network protocols, knowledge management, and tiny devices middleware.

LOURDES LÓPEZ received the degree in mathematical sciences from the Universidad Complutense de Madrid, in 1985, and the Ph.D. degree in computers engineering from the Universidad Politécnica de Madrid (UPM), in 1998.

Since 1991, she has been a Professor with the Department of Engineering and Telematics Architectures, UPM. From 2000 to 2009, she has been the Director of the Department of Engineering and Telematics Architectures, EUIT de Telecomunicación, UPM. In 1992, she initiated her research and development activity at the Group of Information and Network Security, EUIT de Telecomunicación, UPM. She joined the Group of Telematics Services for the Information Society, in 2005. In 2010, she launched a new research group whose work is focused on new telematic networks, GRyS (Group of Next-Generation Networks and Services). Since 2012, she has been the Secretary of the Research Center for Software Technology and Multimedia Systems for Sustainability.