Two-Pass Privacy Preserving Authenticated Key Agreement Scheme for Smart Grid

Mingping Qi and Jianhua Chen

***Abstract*—The design of an authenticated key agreement protocol for securing the smart meter communications in smart grid networks has attracted growing attention recently. Typically, realizing mutual authentication and key agreement without active involvement of a trusted third party is expected in this field. Thus, to achieve this aim, several authenticated key agreement schemes for smart grid have been presented; while as investigated in the following section of this work, most of these schemes remain vulnerable to various attacks. Therefore, to design a truly secure authenticated key agreement protocol for smart grid and make some contributions to this field, this work presents our new authenticated key agreement scheme for smart grid using Elliptic Curve Qu-Vanstone (ECQV) implicit certificate as the building block. Our scheme is pairing-free and just uses two passes to realize mutual authentication and key agreement as well as strong credential privacy, making it with high efficiency in both computation and communication overheads. Moreover, its security is formally proved under the widely accepted Canetti and Krawczyk (CK) security model, and is further confirmed by a heuristic security analysis.**

***Index Terms*—Authenticated key agreement, Elliptic Curve Qu-Vanstone (ECQV), elliptic curve cryptography (ECC), smart grid.**

I. Introduction

SMART grid plays an important role in establishing smart city, and with its further development and evolution, the smart metering networks have evolved into an important component of smart grid, which enables power utilities to better control and manage power resources. Generally, in a smart metering network, a smart meter (SM) and the service provider (SP) should first register to a trusted authority (TA), and then SM can directly communicate with SP via wireless channel without involving TA, sending/receiving consumption data or commands, as shown in Fig. 1. Although the deployment of SMs in home can bring various notable benefits such as real-time monitoring of energy consumption, etc., it also poses various security and privacy challenges due to the openness of a public network communication channel. An adversary may perform various passive and active attacks on the communication channel between SM and SP, and even may compromise an SM by physical methods.

Manuscript received February 10, 2020; revised April 6, 2020; accepted April 25, 2020. This work was supported by the Fundamental Research Funds for the Central Universities under Grant 31020200QD011. *(Corresponding author: Mingping Qi.)*

Mingping Qi is with the School of Cybersecurity, Northwestern Polytechnical University, Xi'an 710072, China (e-mail: mpqi_math@163.com).

Jianhua Chen is with the School of Mathematics and Statistics, Wuhan University, Wuhan 430072, China (e-mail: chenjh_ecc@163.com).

Digital Object Identifier 10.1109/JSYST.2020.2991174

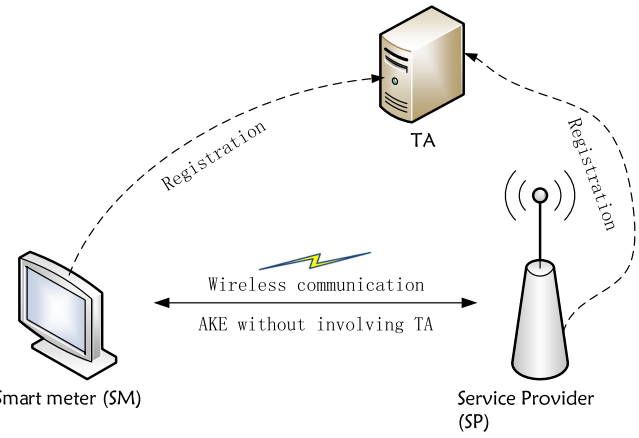

Fig. 1. Smart metering communication network.

A. Related Works

Authenticated key agreement protocols play a significant role in dealing with the security and privacy issues in smart metering networks, and recently, numerous authenticated key agreement protocols have been presented for smart grid with the aim to secure the communications between SM and SP.

Wu and Zhou [1] in 2011 introduced an elliptic curve cryptography (ECC) based key management scheme for smart grid, whereas Xia and Wang [2] pointed out later that the man-in-the-middle attack is available in this scheme, then they designed a new key distribution scheme. However, Xia and Wang's scheme was revealed by Park *et al.* [3] to be vulnerable to the impersonation attack and unable to provide SM anonymity and perfect forward secrecy. Later, Nicanfar *et al.* [4], Jo *et al.* [5], and Saxena *et al.* [6] presented an authenticated key management mechanism with different attributes for smart grid environment.

In 2016, an anonymous key distribution scheme designed by Tsai and Lo [7] for smart grid environment based on the identity-based cryptographic techniques [8], [9] was presented. However, considering the well-known Canetti and Krawczyk (CK) security model [10], Tsai and Lo's scheme was pointed out by Odelu *et al.* [11] that it is unable to ensure the session key security and preserve the privacy of SM credential. Then, Odelu *et al.* [11] proposed a new authenticated key agreement scheme for smart gird, in which the SMs secret credential is produced by using the ECC-based El-Gamal type signature techniques [12], [13] and SPs secret credential is produced by the identity-based encryption technique [8], and Odelu *et al.* [11] asserted that their scheme is provably secure under the CK model. However,

the private key escrow problem exists in Odelu *et al.*'s [11] scheme and may bring some security concerns. Later, Wazid *et al.* [14] presented a three-factor user authentication scheme for renewable-energy-based smart grid environment, while it can be easily found that Wazid *et al.*'s [14] scheme cannot resist the SM impersonation attack and has some design defects. Chen *et al.* [15] and Abbasinezhad-Mood and Nikoohgadam [16] also, respectively, presented an authenticated key agreement scheme and a self-certificated key distribution scheme for smart grid. Nevertheless, as reported by Braeken *et al.* [17], the scheme [15] may suffer from the denial-of-service attack, and the scheme [16] is also unable to ensure session key security under the CK adversary model and may also suffer from the denial-of-service attack. In [18], Gope and Sikdar presented an authenticated key agreement scheme for smart grid utilizing the physically unclonable function (PUF) with the claim that their scheme is robust under the CK security model, but the computational fuzzy extractor in PUF has limitations as reported in [19]. Thus, from the previous review, it can be easily known that designing a truly secure authenticated key agreement protocol for smart grid environment remains an urgent task, and we are dedicated to make some contributions to this field in this article.

B. Contributions

Our contributions mainly include the following three points.

1) We design a new authenticated key agreement protocol for smart grid environment using the Elliptic Curve Qu-Vanstone (ECQV) implicit certificate [20] as the building block. Unlike some existing schemes (such as [7], [11], etc.) that need to perform the relatively time-consuming pairing operation, our new scheme is pairing-free.
2) Our new scheme realizes mutual authentication with session key agreement as well as strong credential privacy within two communication flows, supporting perfect forward secrecy and resisting various known attacks, whereas some existing schemes (such as [7], [11], [14]–[16], etc.) suffer from some attacks and require at least three communication flows to achieve mutual authentication and session key agreement.
3) The security of our proposed new authenticated key agreement scheme for smart grid environment is formally proved under the CK security model, and also confirmed by heuristic analysis. In addition, we compare our new scheme with some other recently presented authenticated key agreement schemes for smart grid in the aspects of computation and communication costs, and from which it can be seen that our new scheme has quite an advantage in efficiency.

C. Outline

The next arrangement of this work is as follows. Section II presents some necessary preliminaries; our proposed two-pass authenticated key agreement scheme for smart grid environment is introduced in Section III; its formal security proof and heuristic security analysis are given in Section IV; the performance analysis is presented in Section V. Finally, Section VI concludes this article.

TABLE I
NOTATIONS USED IN THIS WORK

Notation	Description
TA	Trusted Authority
$E_p(a,b)$	An elliptic curve group defined over F_p
G	A generator on $E_p(a,b)$
n	G's big prime order
P_{pub}, k	TA's public-private key pair
SM_i, SP_j	The ith smart meter and jth service provider
ID_i, SID_j	The identity of SM_i and SP_j
$\mathbb{Z}_n^*$	The interval $[1,\ n-1]$
$\overline{h}(\cdot), h(\cdot), H_i(\cdot)\ (i=1,2,3)$	Secure one-way hash functions
Δt	Tolerance threshold value
$\|, \oplus$	Concatenation and bitwise XOR operations

II. PRELIMINARIES

This section presents some necessary background knowledge, and the notations used throughout this work are listed in Table I.

A. Elliptic Curve

The elliptic curve group $E_p(a,b)$ defined over the prime finite field F_p by the nonsingular elliptic curve equation E: $y^2 = x^3 + ax + b \bmod p$, $a, b \in F_p$, $\Delta = 4a^3 + 27b^2 \bmod p \neq 0$, together with the point at infinity $\mathcal{O}$, is concisely given as

$$E_p(a,b) = \left\{ (x,y) : \begin{array}{l} x, y \in F_p,\ y^2 = x^3 + ax + b \bmod p, \\ \Delta = 4a^3 + 27b^2 \bmod p \neq 0,\ a, b \in F_p \end{array} \right\} \cup \{\mathcal{O}\}.$$

A point P over $E_p(a,b)$ has order n if $nP = \mathcal{O}$ for the smallest integer $n > 0$, where the scalar multiplication is defined as $nP = P + P + \cdots + P$ (n times). Assume that $E_p(a,b)$ is with a big prime order n and G is its $generator$ point.

Definition 1: Elliptic curve discrete logarithm problem is defined as: Given $G \in E_p(a,b)$ with order n and $P = kG \in E_p(a,b)$, it is computationally intractable in polynomial-time to compute the integer $k \in [1, n-1]$.

Definition 2: Elliptic curve computational Diffie–Hellman (ECDH) problem is defined as: Given $G,\ aG,\ bG \in E_p(a,b)$, it is computationally infeasible in polynomial-time to compute $abG \in E_p(a,b)$.

III. OUR SCHEME

This section introduces our new proposed two-pass authenticated key agreement scheme for smart grid environment, and a high-level description of its authenticated key agreement phase is also depicted in Fig. 2.

A. Setup Phase

In this phase, the TA first chooses the secure elliptic curve domain parameters $\{E_p(a,b), G, n\}$ and five hash functions: $h : \{0,1\}^* \to \{0,1\}^{\lceil \log n \rceil}$, $\overline{h} : \{0,1\}^* \to \{0,1\}^{\lceil \log(n)/2 \rceil}$, $H_1 : \{0,1\}^* \to \{0,1\}^{\ell_1}$, $H_2 : \{0,1\}^* \to \{0,1\}^{\ell_2}$, $H_3 : \{0,1\}^* \to$

Smart meter (SM_i)		Service provider (SP_j)
Generates a random number $x \in \mathbb{Z}_n^*$		
$X = xG$		
$e = \overline{h}(X, SID_j)$		
$\overline{X} = X + eP_i$		
$T_1 = (x + es_i)P_s$		
$C_1 = (ID_i \Vert T_i \Vert X) \oplus H_1(T_1 \Vert SID_j \Vert t_1)$		
	$\xrightarrow{\overline{X}, C_1, t_1}$	
		Check $t_1^* - t_1 \ ? < \Delta t$, if true, proceed
		$T_1 = s_j \overline{X}$
		$ID_i \Vert T_i \Vert X = C_1 \oplus H_1(T_1 \Vert SID_j \Vert t_1)$
		$e = \overline{h}(X, SID_j)$
		Check $\overline{X} \ ? = X + e(h(ID_i \Vert T_i)T_i + P_{pub})$, if true, proceed
		Generates a random number $y \in \mathbb{Z}_n^*$
		$d = \overline{h}(X, ID_i)$
		$\overline{Y} = (y + ds_j)G$
		$C_2 = \overline{Y} \oplus T_1$
		$A = H_2(SID_j \Vert ID_i \Vert T_1 \Vert C_2 \Vert t_2)$
		$sk = H_3((y + ds_j)\overline{X})$
	$\xleftarrow{C_2, A, t_2}$	
Check $t_2^* - t_2 \ ? < \Delta t$, if true, proceed		
Check $A \ ? = H_2(SID_j \Vert ID_i \Vert T_1 \Vert C_2 \Vert t_2)$		
$\overline{Y} = C_2 \oplus T_1$		
$sk = H_3((x + es_i)\overline{Y})$		

Fig. 2. Summary of authenticated key agreement phase of our scheme.

$\{0,1\}^{\ell_3}$. Then, TA randomly generates a $k \in \mathbb{Z}_n^*$ as its private key and computes its corresponding public key $P_{\text{pub}} = kG$. Finally, TA publishes these public parameters $\{E_p(a,b), G, n, P_{\text{pub}}, h, \overline{h}, H_1, H_2, H_3\}$.

B. Registration Phase

The registration phases for both SM_i and SP_j are the same with the ECQV certificate scheme. Concretely, the registration steps for SM_i are as following.

Step 1: SM_i with identity ID_i generates a random $r_i \in \mathbb{Z}_n^*$ and computes $R_i = r_i G$, then sends $\{\text{ID}_i, R_i\}$ to the TA for registration via a secure channel.

Step 2: Upon receiving $\{\text{ID}_i, R_i\}$, TA generates a random $k_i \in \mathbb{Z}_n^*$ and computes $T_i = R_i + k_i G$. Then, TA computes $c_i = k + h(\text{ID}_i \Vert T_i)k_i \bmod n$. Finally, TA securely returns $\{T_i, c_i\}$ to SM_i.

Step 3: Upon receiving $\{T_i, c_i\}$, SM_i computes its private key $s_i = h(\text{ID}_i \Vert T_i)r_i + c_i$ and accepts the result of this registration if its corresponding public key P_i satisfies equality $P_i = s_i G = h(\text{ID}_i \Vert T_i)T_i + P_{\text{pub}}$. Thus, SM_i has the implicit certificate $\text{Cert}_{\text{SM}_i} = (\text{ID}_i, T_i)$, and any other party can reconstruct its public key by $P_i = h(\text{ID}_i \Vert T_i)T_i + P_{\text{pub}}$.

Similarly, SP_j can obtain, as above steps, its public–private key pair (P_s, s_j) and implicit certificate $\text{Cert}_{\text{SP}_j} = (\text{SID}_j, T_j)$, where $P_s = s_j G = h(\text{SID}_j \Vert T_j)T_j + P_{\text{pub}}$.

C. Authenticated Key Agreement Phase

As depicted in Fig. 2, this section gives a detailed description of the mutual authentication and session key agreement processes of our proposed new scheme.

Step 1: SM_i first generates a random nonce $x \in \mathbb{Z}_n^*$ and then computes $X = xG$, $e = \overline{h}(X, \text{SID}_j)$, $\overline{X} = X + eP_i$, $T_1 = (x + es_i)P_s$, $C_1 = (\text{ID}_i \Vert T_i \Vert X) \oplus H_1(T_1 \Vert \text{SID}_j \Vert t_1)$, where t_1 is its current timestamp. Then, SM_i sends $\{\overline{X}, C_1, t_1\}$ to SP_j.

Step 2: Upon receiving $\{\overline{X}, C_1, t_1\}$ at the time t_1^*, SP_j checks the freshness of t_1 by checking $t_1^* - t_1 \ ? < \Delta t$. If not, SP_j terminates the session, otherwise, SP_j proceeds to compute $T_1 = s_j \overline{X}$ by its static private key s_j, and then proceeds to compute $\text{ID}_i \Vert T_i \Vert X = C_1 \oplus H_1(T_1 \Vert \text{SID}_j \Vert t_1)$, $e = \overline{h}(X, \text{SID}_j)$. Then, SP_j

checks $\overline{X} \stackrel{?}{=} X + e(h(\mathrm{ID}_i\|T_i)T_i + P_{\mathrm{pub}})$, if false, SP_j breaks off this procedure, otherwise, SP_j generates a random number $y \in \mathbb{Z}_n^*$ and computes $d = \overline{h}(X, \mathrm{ID}_i)$, $\overline{Y} = (y + ds_j)G$, $C_2 = \overline{Y} \oplus T_1$, $A = H_2(\mathrm{SID}_j\|\mathrm{ID}_i\|T_1\|C_2\|t_2)$, and the session key $sk = H_3((y + ds_j)\overline{X})$. Finally, SP_j replies $\{C_2, A, t_2\}$ to SM_i.

Step 3: Upon receiving $\{C_2, A, t_2\}$ at the time t_2^*, SM_i checks the freshness of t_2 by verifying $t_2^* - t_2 \stackrel{?}{<} \Delta t$. If not, SM_i terminates the session, otherwise, SM_i checks $A \stackrel{?}{=} H_2(\mathrm{SID}_j\|ID_i\|T_1\|C_2\|t_2)$. If not, SM_i aborts the session, otherwise, SM_i computes $\overline{Y} = C_2 \oplus T_1$ and the session key $sk = H_3((x + es_i)\overline{Y})$.

Correctness: As long as both SM_i and SP_j perform correctly as the protocol specified, they can finally derive the same session key due to that

$$\begin{aligned}\mathrm{sk} &= H_3((x + es_i)\overline{Y}) = H_3((x + es_i)(y + ds_j)G) \\ &= H_3((y + ds_j)\overline{X}).\end{aligned}$$

IV. Security Analysis

In this section, the formal security proof of our new scheme under CK adversary model is first given, and then the further security attributes heuristic analysis for our scheme is attached.

A. Formal Security Proof

1) Security Model: CK security model [10] is a widely accepted adversary model designed for the formal security proof of authenticated key agreement schemes, in which an adversary $\mathcal{A}$ is supposed to have full control over the communication channel, i.e., $\mathcal{A}$ can freely intercept, replay, or modify (etc.) the communication messages, and $\mathcal{A}$ may be a legitimate user or *vice versa* and can further compromise private keys, session keys, session state information, etc.

SM_i, SP_j, and TA are the three roles in our scheme, and for convenience, we still denote by SM_i and SP_j, respectively, the ith and jth instances of the SM and SP in our protocol Π. An instance typically involves three states: *accept*, *reject,* and $\perp$, where *accept* means the oracle receives the final correct message, *reject* means the oracle does not receive the correct message, and $\perp$ means no response is output. Then, under the CK adversary model, $\mathcal{A}$ can interact with the instances in our protocol Π via the following oracle queries, with the aim to break through Π.

1) $Execute(\mathrm{SM}_i, \mathrm{SP}_j)$: This query simulates the passive attacks against the protocol Π, in which $\mathcal{A}$ can only eavesdrop onto the communication channels and learn the exchanged messages between the honest instances SM_i and SP_j.
2) $Send(\mathrm{SM}_i/\mathrm{SP}_j, m)$: This query simulates the active attacks against the protocol Π, in which $\mathcal{A}$ can generate any message m and send it to an instance $\mathrm{SM}_i/\mathrm{SP}_j$. As a result, $\mathcal{A}$ knows the corresponding instance's outputs according to Π's specification on receiving m.
3) $SSReveal(\mathrm{SM}_i/\mathrm{SP}_j)$: This query allows $\mathcal{A}$ to obtain the session state information such as the ephemeral private key, etc., held by the instance $\mathrm{SM}_i/\mathrm{SP}_j$.
4) $SKReveal(\mathrm{SM}_i/\mathrm{SP}_j)$: This query allows $\mathcal{A}$ to obtain the negotiated session key held by the instance $\mathrm{SM}_i/\mathrm{SP}_j$ in case it has been negotiated.
5) $Corrupt(\mathrm{SM}_i/\mathrm{SP}_j)$: This query captures the notion of forward secrecy, in which $\mathcal{A}$ is allowed to obtain the static private key of $\mathrm{SM}_i/\mathrm{SP}_j$.
6) $Test(\mathrm{SM}_i/\mathrm{SP}_j)$: This special query can be only queried by $\mathcal{A}$ at most once, by which the session key of $\mathrm{SM}_i/\mathrm{SP}_j$ or a random value with the same bit length with the session key will be returned, depending on the flipped coin $b \in \{0, 1\}$ in case the instance $\mathrm{SM}_i/\mathrm{SP}_j$ has accepted and is fresh, i.e., the real session key is returned if $b = 1$ or a random value with the same bit length is returned if $b = 0$.

2) Partnering: The accepted instances SM_i and SP_j are partners if the session id, session key, and partner id they hold (i.e., $(\mathrm{sid}; \mathrm{sk}; \mathrm{pid})$ of SM_i and $(\mathrm{sid}'; \mathrm{sk}'; \mathrm{pid}')$ of SP_j), respectively, satisfy $\mathrm{sid} = \mathrm{sid},'$ $sk = \mathrm{sk}'$ and $\mathrm{pid} = \mathrm{SP}_j \wedge \mathrm{pid}' = \mathrm{SM}_i$.

3) Freshness: An accepted instance is fresh if it or its partner has not been queried $SKReveal$, and it has never been queried $Send$ when it or its partner has been queried $Corrupt$.

Definition 3: Semantic security. Let b' be the guessed bit by $\mathcal{A}$ for the $Test$ oracle query to a fresh instance in which the random hidden bit $b \in \{0, 1\}$ is generated, then the advantage for $\mathcal{A}$ to violate the semantic security of the protocol Π is defined to be

$$Adv_{\Pi}(\mathcal{A}) = |2\Pr[b' = b] - 1|.$$

Consequently, Π is semantically secure under CK adversary model if $Adv_{\Pi}(\mathcal{A}) \leq \epsilon$, for a negligible $\epsilon > 0$.

Theorem 1: Let $\mathcal{A}$ be a probabilistic polynomial time adversary against the sematic security of our proposed protocol Π with a time bound t, making at most q_e $Execute$ queries, q_s $Send$ queries, and q_h random oracle queries. Then

$$\begin{aligned}\mathrm{Adv}_{\Pi}(\mathcal{A}) \leq\ & \frac{q_h^2 + 2q_s}{2^{\ell}} + \frac{(q_s + q_e)^2}{n - 1} \\ & + 2(q_s + q_e)^2 q_h \cdot \mathrm{Adv}_G^{\mathrm{ECDH}}(\mathcal{C})\end{aligned}$$

where $\ell = \min\{\ell_1, \ell_2, \ell_3\}$, $\mathrm{Adv}_G^{\mathrm{ECDH}}(\mathcal{C})$ means the success probability of solving an instance of ECDH problem by an algorithm $\mathcal{C}$.

Proof: A sequence of hybrid games G_i in which denote by $\mathrm{Succ}_i (i = 0, 1, 2, 3, 4)$ the event that $\mathcal{A}$ correctly guesses the random bit b in the $Test$ query, are defined to prove this theorem, starting from the real attack game G_0 and ending up with the final game G_4.

Game G_0: This game is the real attack situation against Π, as defined in the earlier semantic security definition, thus we have

$$\mathrm{Adv}_{\Pi}(\mathcal{A}) = 2|\Pr[\mathrm{Succ}_0] - \frac{1}{2}|. \tag{1}$$

Game G_1: In this game, the random oracles $\overline{h}$, h, H_1, H_2, H_3 are simulated as usual by maintaining a hash list $\mathcal{L}$ in which every entry is in the form of (u, v, f), and the other oracle queries

are simulated as in the real attack. On a hash query $f(u)$ where $f \in \{\overline{h}, h, H_1, H_2, H_3\}$, if the record (u, v, f) is already in $\mathcal{L}$, then return v directly, otherwise a random number v with the same bit length with the output of f is generated as the answer to this query, and then add the record (u, v, f) into the list $\mathcal{L}$. Obviously

$$\Pr[\text{Succ}_1] = \Pr[\text{Succ}_0]. \tag{2}$$

Game G_2: In this game, all oracle queries are simulated as the same as in the game G_1, while when collisions occur in the session transcripts or the output of the random oracles, G_2 aborts. Thus, it can be drawn from the birthday paradox that

$$|\Pr[\text{Succ}_2] - \Pr[\text{Succ}_1]| \leq \frac{q_h^2}{2^{\ell+1}} + \frac{(q_s + q_e)^2}{2(n-1)}. \tag{3}$$

Game G_3: In this game, the scheme is simply aborted in case that $\mathcal{A}$ successfully guesses C_1 or A without querying the random oracle H_1 or H_2, which means G_3 and G_2 are indistinguishable unless this case occurs. Thus

$$|\Pr[\text{Succ}_3] - \Pr[\text{Succ}_2]| \leq \frac{q_s}{2^{\ell}}. \tag{4}$$

Game G_4: In this game, a random session is exactly chosen as the test-session, and if not, abort this game. Moreover, the computation of the test-session key is modified into just choosing a random key from an appropriate range. Then, G_4 and G_3 are indistinguishable unless the event E occurs that $\mathcal{A}$ has queried $\sigma = (x + es_i)(y + ds_j)G$ in the test-session to the random oracle H_3. To bound this difference, the following four cases may be involved:

1) $Corrupt(\text{SM}_i)$ and $Corrupt(\text{SP}_j)$ are queried, from which, $\mathcal{A}$ obtains the static private keys s_i of SM_i and s_j of SP_j. To derive the session key
$$\begin{aligned} \text{sk} &= H_3((x + es_i)\overline{Y}) = H_3((y + ds_j)\overline{X}) \\ &= H_3((x + es_i)(y + ds_j)G) \end{aligned} \tag{*}$$
either the ephemeral private key x of SM_i or y of SP_j is required.
2) $SSReveal(\text{SM}_i)$ and $SSReveal(\text{SP}_j)$ are queried, from which, $\mathcal{A}$ obtains the ephemeral private keys x of SM_i and y of SP_j. To derive the session key, cf. equation (*), either the static private key s_i of SM_i or s_j of SP_j is required.
3) $SSReveal(\text{SM}_i)$ and $Corrupt(\text{SP}_j)$ are queried, from which, $\mathcal{A}$ obtains the ephemeral private key x of SM_i and static private key s_j of SP_j. To derive the session key, cf. equation (*), s_i, or y is required.
4) $Corrupt(\text{SM}_i)$ and $SSReveal(\text{SP}_j)$ are queried, from which, $\mathcal{A}$ obtains the static private key s_i of SM_i and ephemeral private key y of SP_j. To derive the session key, cf. equation (*), x, or s_j is required.

Then, for each of these four cases, if event E occurs, then refer to the method in [21], an algorithm $\mathcal{C}$ to solve an instance of ECDH problem can be built, and it holds that

$$|\Pr[\text{Succ}_4] - \Pr[\text{Succ}_3]| \leq (q_s + q_e)^2 q_h \cdot \text{Adv}_G^{\text{ECDH}}(\mathcal{C}). \tag{5}$$

Moreover, in the game G_4, it is obvious that the guess to the bit b involved in the $Test$ query is random and independent for all sessions. So

$$\Pr[\text{Succ}_4] = \frac{1}{2} \tag{6}$$

Finally, the theorem can be easily obtained by (1)–(6).

TABLE II
SECURITY ATTRIBUTES COMPARISON

	Scheme				
Security attributes	[7]	[11]	[15]	[16]	Our
Authentication and key agreement	√	√	√	√	√
Forward secrecy	√	√	√	√	√
Privacy preserving	×	√	√	√	√
Replay attack resistance	√	√	√	√	√
Impersonation attack resistance	√	√	√	√	√
Man-in-the-middle attack resistance	√	√	√	√	√
Denial of service attack resistance	√	√	×	×	√
Private key escrow avoidance	√	×	√	√	√
Session key security under CK model	×	√	√	×	√

B. Further Security Attributes Analysis

The security attributes contained in our new scheme are further confirmed in this section by heuristic analysis, and detailed descriptions are as follows.

1) Authentication and Key Agreement: First, SP_j can authenticate SM_i by checking whether $\overline{X} = X + e(h(\text{ID}_i \| T_i)T_i + P_{\text{pub}})$ holds or not, since only the legal SM_i has the corresponding static private key s_i and can use it to compute the shared secret parameter T_1, making SP_j decrypt the cipher text C_1 correctly. Then, SM_i can authenticate SP_j by verifying whether $A = H_2(\text{SID}_j \| \text{ID}_i \| T_1 \| C_2 \| t_2)$ holds or not, since only the legal SP_j can use its static private key s_j to derive the shared secret parameter T_1 by $T_1 = s_j\overline{X}$. It is obvious as depicted in Fig. 2 that after successfully mutual authentication, both the participants can derive the same session key $\text{sk} = H_3((x + es_i)(y + ds_j)G)$.

2) Forward Secrecy: The established session key in our new scheme is $\text{sk} = H_3((x + es_i)(y + ds_j)G)$, different in every session due to the ephemeral private keys x, y randomly generated in every session. The only way for an adversary $\mathcal{A}$ to compute sk is to obtain both the static private key s_i and ephemeral private key x, or both the static private key s_j and ephemeral private key y simultaneously, which is trivial and without consideration in the CK adversary model. Therefore, even both the static private key s_i and s_j of the participants SM_i and SP_j are all exposed to $\mathcal{A}$, $\mathcal{A}$ cannot derive any previous established session keys. Namely, forward secrecy holds in our new scheme.

3) Privacy Preserving: In our new scheme, SM_i's implicit certificate (ID_i, T_i) is encrypted by $C_1 = (\text{ID}_i \| T_i \| X) \oplus H_1(T_1 \| \text{SID}_j \| t_1)$ and then sent to SP_j in every session; moreover, the cipher text C_1 is dynamic and different in every session. Therefore, SM_i can preserve identity anonymity and is infeasible to be traced. Thus, privacy preserving is obviously supported in our new scheme.

4) Replay Attack Resistance: An adversary $\mathcal{A}$ may intercept some previous exchanged messages between SM_i and SP_j, and

TABLE III
COMPUTATION COSTS COMPARISON

scheme	SM_i	SP_j
[7]	$T_e + 4T_{pm} + T_{pa} + 5T_h \approx 12.794$ ms	$2T_b + T_e + 3T_{pm} + 2T_{pa} + 5T_h \approx 22.219$ ms
[11]	$2T_e + 2T_{pm} + T_{pa} + 6T_h \approx 12.195$ ms	$2T_b + T_e + 2T_{pm} + T_{pa} + 6T_h \approx 19.967$ ms
[15]	$T_e + 2T_{pm} + 5T_h \approx 8.314$ ms	$T_b + T_e + 3T_{pm} + T_{pa} + 6T_h \approx 16.382$ ms
[16]	$4T_{pm} + T_{pa} + 5T_h \approx 8.944$ ms	$4T_{pm} + T_{pa} + 5T_h \approx 8.944$ ms
Our scheme	$3.5T_{pm} + T_{pa} + 4T_h \approx 7.829$ ms	$4.5T_{pm} + 2T_{pa} + 6T_h \approx 10.088$ ms

TABLE IV
COMMUNICATION COSTS COMPARISON

scheme	Total communication costs	Communication flows
[7]	867 bits	3
[11]	1538 bits	3
[15]	1091 bits	3
[16]	867 bits	3
Our scheme	996 bits	2

then replay them to either of the participants later. However, due to the timestamp involved in all the transcripts, SM_i and SP_j are likely to discard these replayed messages for $t_i^* - t_i > \Delta t\,(i = 1, 2)$. Moreover, even if t_i is modified by $\mathcal{A}$ to satisfy $t_i^* - t_i < \Delta t$, SM_i or SP_j will abort the session due to the original timestamp t_i is embedded in $H_1(T_1 \| \mathrm{SID}_j \| t_1)$ or A. Thus, SM_i and SP_j will detect the modification of the received transcripts and then make a reasonable disposal. Hence, our new scheme can resist the replay attack.

5) Impersonation Attack Resistance: To impersonate SM_i, an adversary $\mathcal{A}$ needs to know the static private key s_i of SM_i, and then uses it to compute the shared secret parameter T_1 by $T_1 = (x + es_i)P_s$. Similarly, to impersonate SP_j, $\mathcal{A}$ needs to know the static private key s_j of SP_j, and then uses it to compute the shared secret parameter T_1 by $T_1 = s_j\overline{X}$. Obviously, obtaining the static private key s_i or s_j is almost impossible for $\mathcal{A}$. Hence, our new scheme can withstand the impersonation attack.

6) Man-in-the-Middle Attack Resistance: Passing all the checking test performed by SM_i and SP_j such that an adversary $\mathcal{A}$ can successfully deceive SM_i and SP_j simultaneously is needed for $\mathcal{A}$ to perform the man-in-the-middle attack, whereas this is impossible for $\mathcal{A}$ as analyzed in Sections IV-B4 and IV-B5. Hence, our new scheme is secure against the man-in-the-middle attack.

7) Denial-of-Service Attack Resistance: In our scheme, the timestamp is included in the exchanged messages from both SM_i and SP_j, and also is as the input of hash functions in both sides. Thus, upon arrival of messages from SM_i or SP_j, the receiver can immediately check their correctness in one single phase, as a result, no separated buffers need to be allocated for them and the receiver can immediately go to check the next received messages as long as the check failed. Hence, the denial-of-service attack is not available in our new scheme.

8) Private Key Escrow Avoidance: Due to the registration phase of ECQV implicit certificate is correctly applied, the problem of static private key escrow is avoided in our new scheme since the private key consists of two secret components contributed by SM_i/SP_j and TA, respectively. Thus, the private key escrow problem is not within our new scheme.

Finally, we compare the security attributes provided by our new scheme and some recently proposed authenticated key agreement schemes [7], [11], [15], [16] for smart grid in Table II. It is clear that our new scheme has perfect security attributes while each of these relevant schemes suffers from different vulnerabilities.

V. PERFORMANCE EVALUATION

This section evaluates the performance of our scheme from the computation and communication costs. For simplicity, we denote the time for executing the bilinear pairing operation by T_b, modular exponentiation operation by T_e, elliptic curve scalar multiplication operation by T_{pm}, elliptic curve point addiction operation by T_{pa}, and hash function by T_h. The experiment values for these operations have been given by Yanik and Kilinc [22] on a personal computer with a Intel Pentium Dual CPU E2200 2.20 GHz processor, 2048 MB of RAM and the Ubuntu 12.04.1 LTS 32 b operating system (i.e., $T_b \approx 5.811$ ms, $T_e \approx 3.850$ ms, $T_{\mathrm{pm}} \approx 2.226$ ms, $T_{\mathrm{pa}} \approx 0.0288$ ms, $T_h \approx 0.0023$ ms), which are referenced in this work to evaluate the computation efficiency.

Then, the computational costs for the SM_i and SP_j in our new scheme and some relevant schemes in [7], [11], [15], and [16] (where the scheme [18] does not rely on public key cryptography, and thus is omitted here) are compared in Table III, from which, it can be easily seen that the computation overhead consumed by SM_i in our scheme (i.e., $3.5T_{\mathrm{pm}} + T_{\mathrm{pa}} + 4T_h \approx 7.829$ ms) is the least, and by SP_j (i.e., $4.5T_{\mathrm{pm}} + 2T_{\mathrm{pa}} + 6T_h \approx 10.088$ ms) is much less than the schemes in [7], [11], and [15] and just slightly more than the scheme in [16]. Overall, our new scheme has quite an advantage over the other relevant schemes in the aspect of computation overhead, since SM_i just has constraint resources and consumes the least resources in our scheme.

As for the communication costs, we roughly assume the bit lengths of identity and timestamp are all 64 b, the random nonce and the output of hash function for authentication are all 160 b, an elliptic curve point is 161 b (with a sign bit), and an element in multiplicative group is 512 b. Then, the messages' bits sent by the SM_i and SP_j in our scheme are 611 b and 385 b, respectively, and thus, the total communication costs consumed by SM_i and SP_j in our scheme are 996 b. We also compare our scheme with the relevant schemes in [7], [11], [15], and [16] in the aspect of communication costs, as shown in Table IV, from which, it can be easily seen that our scheme just requires two communication flows, whereas the others require three, and the

total communication costs consumed in our scheme are just a little more than the schemes in [7] and [16]. Thus, in general, our new scheme has advantages in efficiency.

VI. Conclusion

In this article, we present a new two-pass authenticated key agreement scheme for smart grid, which is formally proved to be able to provide session key security in the widely accepted CK adversary model and can offer various anticipated security features including mutual authentication with session key security, privacy preserving, as well as securing against various known attacks, such as the impersonation, replay, man-in-the-middle attacks, etc. Moreover, our new scheme behaves quite well in terms of the computation and communication overhead. Therefore, whether it is from the security or efficiency point of view, our new scheme has advantages over the relevant schemes, and thus may be more suitable for the smart grid setting. Besides, due to the advantages of our new scheme, it obviously can be applied in smart home networks (such as remotely accessing the smart camera, intelligent audio, etc.) to provide security assurance.

Also, we remark here that although our new scheme is more efficient than other public key cryptography based relevant schemes, its time consumption is still more than twice that of the original Diffie–Hellman protocol. Therefore, how to further promote the computation efficiency of our new scheme is our future research related to this work. Also, how to make users efficiently and securely access the data in SMs may be another future research topic related to this work.

Acknowledgment

The authors would like to express great appreciation to the anonymous reviewers for their valuable comments, and the editors for the patience and hard work for this article.

References

[1] 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.

[2] 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.

[3] J. H. Park, M. Kim, and D. Kwon, "Security weakness in the smart grid key distribution scheme proposed by Xia and Wang," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1613–1614, Sep. 2013.

[4] H. Nicanfar, P. Jokar, K. Beznosov, and V. C. M. Leung, "Efficient authentication and key management mechanisms for smart grid communications," *IEEE Syst. J.*, vol. 8, no. 2, pp. 629–640, Jun. 2014.

[5] H. J. Jo, I. S. Kim, and D. H. Lee, "Efficient and privacy-preserving metering protocols for smart grid systems," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1732–1742, May 2016.

[6] N. Saxena, B. J. Choi, and R. Lu, "Authentication and authorization scheme for various user roles and devices in smart grid," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 5, pp. 907–921, May 2017.

[7] 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.

[8] P. S. L. M. Barreto, N. Mccullagh, and J. J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," in *Proc. Int. Conf. Theory Appl. Cryptology Inf. Secur.*, 2005, pp. 515–532.

[9] R. Sakai and M. Kasahara, "ID based cryptosystems with pairing on elliptic curve," 2003. [Online]. Available: https://eprint.iacr.org/2003/054

[10] C. Ran and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," *Lecture Notes Comput. Sci.*, vol. 2045, pp. 453–474, 2001.

[11] 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 2018.

[12] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. IT-31, no. 4, pp. 469–472, Jul. 1985.

[13] L. Harn and Y. Xu, "Design of generalised ElGamal type digital signature schemes based on discrete logarithm," *Electron. Lett.*, vol. 30, no. 24, pp. 2025–2026, 1994.

[14] M. Wazid, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "Secure three-factor user authentication scheme for renewable-energy-based smart grid environment," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3144–3153, Dec. 2017.

[15] Y. Chen, J.-F. Martínez, P. Castillejo, and L. López, "An anonymous authentication and key establish scheme for smart grid: Fauth," *Energies*, vol. 10, no. 9, 2017, Art. no. 1354.

[16] D. Abbasinezhad-Mood and M. Nikooghadam, "An anonymous ECC-based self-certified key distribution scheme for the smart grid," *IEEE Trans. Ind. Electron.*, vol. 65, no. 10, pp. 7996–8004, Oct. 2018.

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

[18] P. Gope and B. Sikdar, "Privacy-aware authenticated key agreement scheme for secure smart grid communication," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3953–3962, Jul. 2019.

[19] K. Yasunaga and K. Yuzawa, "On the limitations of computational fuzzy extractors," Cryptology ePrint Archive, Report 2014/605, 2014. [Online]. Available: https://eprint.iacr.org/2014/605

[20] M. Campagna, "Sec 4: Elliptic curve Qu-vanstone implicit certificate scheme (ECQV)," Certicom Res., Mississauga, ON, Canada, Tech. Rep, 2013.

[21] Krawczyk and Hugo, "HMQV: A high-performance secure Diffie-Hellman protocol," *Crypto*, vol. 3621, pp. 546–566, 2005.

[22] T. Yanik and H. H. Kilinc, "A survey of sip authentication and key agreement schemes," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 2, pp. 1005–1023, Apr.–Jun. 2014.

Mingping Qi received the Ph.D. degree in applied mathematics from Wuhan University, Wuhan, China, in 2019.

He is currently an Assistant Professor with Northwestern Polytechnical University, Xi'an, China. His research interests include public key cryptography especially elliptic curve cryptography, cryptographic protocols, and network security.

Jianhua Chen received the B.S. degree in applied mathematics from the Harbin Institute of Technology, Harbin, China, in 1983, and the M.S. and Ph.D. degrees in applied mathematics from Wuhan University, Wuhan, China, in 1989 and 1994, respectively.

He is currently a Professor with Wuhan University. His current research interests include number theory, cryptography, and information security.