Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 9988170, 10 pages
https://doi.org/10.1155/2021/9988170

Research Article

A Blind Signature-Aided Privacy-Preserving Power Request Scheme for Smart Grid

Weijian Zhang,[1] Zhimin Guo,[2] Nuannuan Li,[2] Mingyan Li ,[2] Qing Fan,[3] and Min Luo [3]

[1]*State Grid Henan Electric Power Company, Zhengzhou, China*
[2]*State Grid Henan Electric Power Research Institute, Zhengzhou, China*
[3]*Wuhan Lianweitu Software Co., Ltd., Wuhan, China*

Correspondence should be addressed to Mingyan Li; limingyan@stu.xjtu.edu.cn

Received 22 March 2021; Revised 4 May 2021; Accepted 6 June 2021; Published 1 July 2021

Academic Editor: Ding Wang

Smart grid is an emerging power system capable of providing appropriate electricity generation and distribution adjustments in the two-way communication mode. However, privacy preservation is a critical issue in the power request system since malicious adversaries could obtain users' daily schedule through power transmission channel. Blind signature is an effective method of hiding users' private information. In this paper, we propose an untraceable blind signature scheme under the reputable modification digital signature algorithm (MDSA). Moreover, we put forward an improved credential-based power request system architecture integrated with the proposed blind signature. In addition, we prove our blind signature's blindness and unforgeability under the assumption of Elliptic Curve Discrete Logarithm Problem (ECDLP). Meanwhile, we analyze privacy preservation, unforgeability, untraceability, and verifiability of the proposed scheme. Computational cost analysis demonstrates that our scheme has better efficiency compared with other two blind signatures.

1. Introduction

The concept of "Intelligrid" is first proposed by the American Electric Power Research Institute in 2001 [1], and exploration of smart grid is becoming more and more popular. Since the notion of industry 4.0 is put forward, operation and management of smart grid are optimized through connection of various facilities, equipment, and devices [2]. Smart grid is regarded as the next-generation power grid infrastructure capable of promoting secure and effective electricity transmission from power operators to electric appliance. Power operation and management in smart grid are upgraded by integrating advanced bidirectional communications and widespread computing capabilities for efficient control, distribution, reliability, and safety [3]. Smart grid not only eliminates barriers between users and power producers but also ensures continuous electricity supply for users due to intelligently monitoring electricity consumption behaviour of users to realize suitable adjustments in the amount of power deployment [4].

In general, a smart grid network is roughly comprised of three layers: control center, substations, and smart appliances (i.e., smart meters) [5]. Figure 1 depicts a simplified architecture of the smart grid network. As a kind of physical carrier, smart meters are installed in each electricity appliance system and users could send power request to substation with the help of smart meters. Moreover, smart meters will push appliance information to substations periodically. Substations could collect users' real-time demand and forward it to the control center via the Supervisory Control and Data Acquisition (SCADA) system [6, 7]. Then, the power control center will make further power deployment analysis and distribute proper electricity amount to substations as various requirements. Finally, users could obtain the required electricity through substations.

It should be noted that the major differences between traditional power network and smart grid are that smart meters bearing users' application information communicate with substations via wired or wireless networks. Specifically, one of the main information is the users' real-time electricity

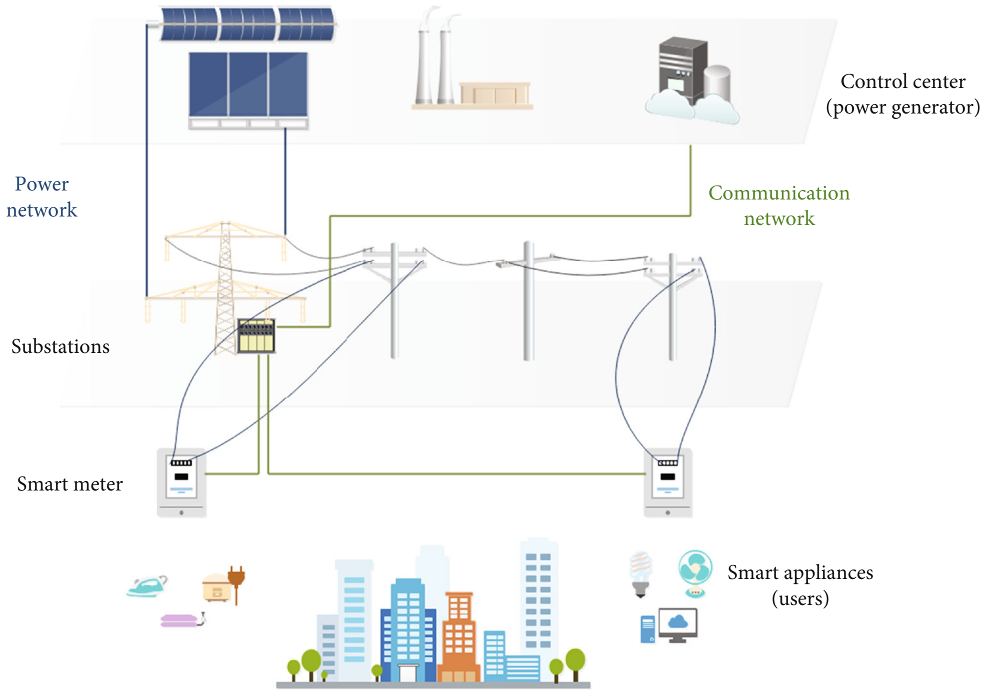

Figure 1: Model of the smart grid.

consumption and demands. Due to the power request which has the potential of leaking users' daily schedule, which is private, we devote to the privacy and security issues of electricity request communication. Furthermore, power demands are not only related to users' privacy directly but also related to the charging policy and fairness. How to take effective measures to guarantee genuineness of power demand sources and the user's privacy is a significant issue. The former problem could be solved by identity authentication, and the latter needs privacy preservation techniques to be settled [8].

The digital signature is an important cryptographic protocol for ensuring the authenticity and the integrity of messages [9–11]. The blind signature is a special digital signature, which is an effective method for user's privacy preservation. The pioneer of blind signature conception is from Chaum et al.'s research [12], in which they established a user's privacy-preserved electric payment system based on blind signature. The blind digital signature generation process contains two parties: a signer $\mathcal{S}$ and a user $\mathcal{U}$. On receiving a blind signature request from a user $\mathcal{U}$, the signer $\mathcal{S}$ generates a random element and sends it to $\mathcal{U}$. Then, the user utilizes received element and produced blind factors to blind the original message m. The blinded message denoted by $\tilde{m}$ is sent to $\mathcal{S}$. Actually, $\mathcal{S}$ signs $\tilde{m}$ as a secure signature scheme. Finally, $\mathcal{U}$ unblinded signature values from $\mathcal{S}$ to obtain the ultimate blind signature. In the above process, $\mathcal{S}$ cannot recognize the real signing message even if he saves all the signature scripts that he has signed. The unmatchability between output of blind signature and signer's signature scripts is viewed as untraceability.

Amounts of blind signature schemes have been proposed [13–19], but they cannot hold untraceability, where the signer $\mathcal{S}$ can find a match between his signature scripts and blind signature outputs. Thus, $\mathcal{S}$ can distinguish the original message he has signed and privacy of user could not be ensured. In this paper, we improved Bütün and Demirer's scheme and proposed a secure blind signature. Based on the advanced blind signature, we put forward a power request system model. Contributions of this paper are as follows:

(i) We put forward an improved blind signature-aided power request privacy preservation system model, in which smart meters (i.e., users) could send power request, a blindly signed credential with a certain amount, to substations, and the control center cannot identify the real user identity through blind signature verification

(ii) We analyze Bütün and Demirer's scheme and point out its weakness, that is a malicious signer could find a match message between his signing scripts and user's blind signature outputs

(iii) We propose a secure blind signature scheme under the reputable MDSA digital signature. What is more, blindness and unforgeability of our proposed blind signature are proved under difficulty assumption of ECDLP

1.1. Organizations of This Paper. Some works related to blind signature and smart grid privacy preservation are described in Section 2. Section 3 are preliminaries of this paper, which introduces our proposed system model, fundamental knowledge, definition of blind signature, and security model of blind signature. In Section 4, we review Bütün and Demirer's scheme. Then, we point out the linkability attack on the reviewed scheme in Section 5, that is, a signer can find an original message he has signed. In Section 6, we proposed our improved blind signature with untraceability. In Section 7, we prove our scheme's blindness and unforgeability and analyze properties of privacy preservation, unforgeability, untraceability, and verifiability. Section 8 gives comparisons of security properties and computational costs with Bütün and Demirer's scheme [13] and Verma and Singh's scheme [16].

2. Related Works

Since the advent of "smart grid" concept, a flow of smart grid surveys has sprung up [3, 20–26]. Fang et al. explore three major systems and gave the future expectations for smart grid [20]. This paper has an important reference value for the following smart grid survey. Alshehri gives further research for smart grid and studied multiperiod demand response management [21]. Wen et al. [25] and Makhadmenh et al. [26], respectively, conducted researches on smart meters and smart homes. However, some sensitive information of users may leak through the two-way communication channel. Therefore, privacy preservation is especially significant.

Si et al. analyze the existing privacy problems and enumerate some solutions from a global perspective for smart grid [27]. Mahmood et al. propose an elliptic curve-based authentication to provide communication security between customers and substations [28]. Blind signature is an effective way of hiding users' sensitive information and first proposed by Camenisch et al. [29]. Blind signature could guarantee anonymity of participants. Tseng put forward a specific privacy-preserving communication protocol utilizing the restrictive partially blind signature [30]. Sarde and Banerjee propose an incentive-based demand response privacy-preserving scheme for the smart grid [14]. Yang et al. make an attempt to identify the privacy-preserving issues and put forward a reward architecture for V2G networks [31]. Yu et al. propose a power request scheme to satisfy the security requirements [32]. Han and Xiao give a thorough and deep survey on the privacy preservation for smart grid and point out that the blind signature is a universal method for users' security issues [33], but they do not give a detailed blind signature based privacy preservation scheme.

In conclusion, the above papers have great effects on the smart grid privacy preservation research. But they either give a general description or lack of a comprehensive blind signature scheme. In this paper, we proposed an integrated blind signature-aided privacy-preserving power request scheme for smart grid.

3. Preliminaries

In this section, we introduce the system model, fundamental knowledge, definition of blind signature, and security model of blind signature.

3.1. The System Model. In this subsection, we propose an improved system model of Cheung et al.'s architecture [34]. A smart grid network can be simplified into a hierarchical structure consisting of three basic layer-control centers, substations, and smart meters. It can be shown that they have different characteristics.

(i) A control center (CC) is at the top level and maintained by the power operator. It can be a single server inside the power plant or be distributed servers at different locations responsible for parameter generation, entity registration, and issuing credentials for smart meters. In this paper, we assume that the control center is trusted

(ii) Substations (SS) are at the middle of the structure and fixed in a particular geographic location as it contains expensive electric devices. They could communicate with users directly

(iii) Smart meters (SM) are at the lowest level and installed in the power application positions such as users' homes. They could send power requests to the control center

In our system construction, the main idea is that the control center makes good use of the proposed blind signature scheme to sign credentials for users. In this case, identities of users cannot be recognized when he or she sends a request to the control center, while the user's identity can be validly verified due to only legal user could have requested control center for blind signatures.

The workflow of the system model is shown in Figure 2 [5]. In the system setup phase, the control center (CC) generates a pair of public and private keys and assigns a unique identifier $\mathrm{ID}_{\mathrm{SM}}$ for each smart meter (SM) to be registered. In the smart meter registration phase, the CC first authenticates the SM's identity and decides to accept or reject this SM. Then, each user submits the blinded credential information to the CC. Each credential consists of a unique identity CID, issuance date T, a substation identifier $\mathrm{ID}_{\mathrm{SS}}$, and a value of power amount v that a credential holder could request. Then, the CC generates a blind signature for the credential and sends it to SM. Eventually, the SM unblinds the signature and obtains a signed credential. In the power requesting phase, smart meters of a user request for more power when it finds the electric appliances cannot be satisfied. The SM chooses a signed credential of required value and transmits it to the SS with identity $\mathrm{ID}_{\mathrm{SS}}$ noted in the credential. Then, SS sends the signature credential to CC. If the signature is valid and the credential's identity CID is not in the credential revocation list, CC distributes proper power as the credential to the SS. Meanwhile, CC adds CID in the credential revocation list. Finally, the SM receives required power amount.

In the above process, the control center cannot recognize the real user identity through blind signature. Therefore, the power consumption information is not disclosed to CC. In the next subsection, we will introduce blind signatures related to knowledge.

3.2. Fundamental Knowledge

3.2.1. Elliptic Curve. Given a large prime p and the finite field F_p, the elliptic curve equation is defined by $E(F_p)$: $y^2 = x^3$

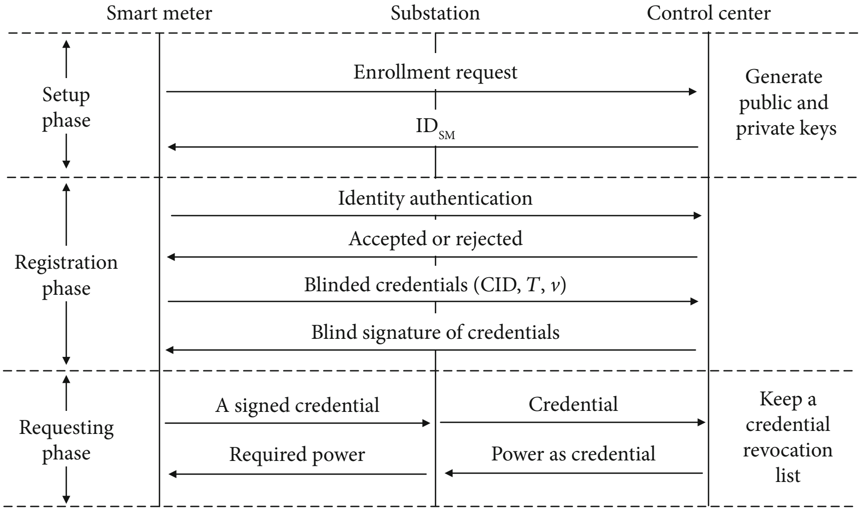

Figure 2: System architecture.

$+ ax + b$ mod p, where $a, b \in F_p$. All points satisfying the elliptic curve equation together with a point at infinity $\mathcal{O}$ are composed of an Abelian group. Order of the group is denoted by n.

Elliptic Curve Discrete Logarithm Problem (ECDLP). Suppose that G is a generator on $E(F_p)$ and Q is a possible point on the elliptic curve, it is difficult to find an $x \in Z_n^*$ such that the equation $Q = x \cdot G$ holds.

3.2.2. The Modification Digital Signature Algorithm (MDSA). As cited, the MDSA is mainly composed of three phases as follows: key generation, signing, and verifying.

(i) *Key Generation*. The signer randomly chooses an $x \in Z_n$ as the private key and computes $Q = x \cdot G$ as the public key

(ii) *Signing*. The user selects a random number $k \in Z_n$ and computes $R = k \cdot G = (x_1, y_1)$. x_1 mod n is denoted by r. Then, he calculates $e = H(m)$ and $s = ke + xr$ mod n. The signature output is (s, R)

(iii) *Verifying*. Upon receiving m, s, R, the verifier first computes $e = H(m)$ and extracts $r = x_1$ mod n. Then, he verifies the equation $s \cdot G = H(m)R + r \cdot Q$. If it is the case, (s, R) is a valid signature

3.3. Definition of Blind Signature. A complete blind signature is composed of setup phase, key generation phase, blind signature phase, and verification phase [29]. Specifically, the blind signature phase consists of two probabilistic polynomial-time (PPT) interactive algorithms in the respective party of signer $\mathcal{S}$ and user $\mathcal{U}$.

(i) *Setup Phase* (params $\longleftarrow$ Setup(λ)). On inputting a security parameter λ for expected security level, a series of public parameters are output in this phase

(ii) *Key Generation Phase* ((pk, sk) $\longleftarrow$ Gen(λ)). This is a probabilistic polynomial-time (PPT) algorithm. Taking the security parameter λ as input, outputting a public and private key (pk, sk)

(iii) *Blind Signature Phase*. This phase includes two interactive PPT algorithms Signer(pk, sk) and User (pk, m)

(a) complete or uncomplete $\longleftarrow$ Signer(pk, sk). Upon inputting a public key pk and the corresponding secret key sk generated by Gen($\cdot$), the signer $\mathcal{S}$ outputs complete or uncomplete through blind signature interactive process

(b) $\sigma(m)$ or fail $\longleftarrow$ User(pk, nonce, m). Upon inputting a common public key pk of $\mathcal{S}$, selected blind factors nonce, and the message m to be signed, the user $\mathcal{U}$ selects the demanded blind outputs fail or $\sigma(m)$ through blind signature interactive process

(iv) *Verification Phase* (accept or reject $\longleftarrow$ Verify(pk, $m, \sigma(m)$)). This is a deterministic polynomial-time algorithm. On inputting public key pk, message m, and the signature $\sigma(m)$, it always outputs accept with the condition that both signer $\mathcal{S}$ and user $\mathcal{U}$ follows the blind signature and $\mathcal{S}$ outputs complete, $\mathcal{U}$ outputs complete

3.4. Security Model of Blind Signature. We refer to Okamoto who proposed a security model for blind signatures and consider the following two properties: blindness and unforgeability [35].

3.4.1. Blindness. The blindness of blind signature is depicted by the following game between an adversarial signer $\mathcal{S}^*$ and a simulator $\mathcal{B}$ which controls two honest users $\mathcal{U}_0, \mathcal{U}_1$.

(i) An adversary $\mathcal{S}^*$ inputs the security parameter λ to obtain the public key pk and two ordered messages denoted by (m_0, m_1). Then, (m_0, m_1) are transmitted to the simulator $\mathscr{B}$

(ii) $\mathscr{B}$ randomly chooses a bit $b \in \{0, 1\}$ to reorder the two messages (m_b, m_{1-b}) and, respectively, distributes m_b and m_{1-b} to $\mathscr{U}_0$ and $\mathscr{U}_1$ as secret information. Then, $\mathscr{U}_0(\mathscr{U}_1)$ selects proper blind factors nonce and inputs corresponding message $m_b(m_{1-b})$ and pk to run User(pk, nonce, m) algorithm

(iii) $\mathscr{S}^*$ engages in these two parallel interactive blind signatures separately with $\mathscr{U}_0, \mathscr{U}_1$

(iv) If $\mathscr{U}_0, \mathscr{U}_1$, respectively, outputs valid blind signatures $(m_b, \sigma(m_b))$ and $(m_{1-b}, \sigma(m_{1-b}))$, send the two signatures to $\mathscr{S}^*$ in random order. Otherwise, output $\perp$

(v) Finally, $\mathscr{S}^*$ outputs a guess bit $b' \in \{0, 1\}$

We define

$$\mathrm{Adv}_{\mathrm{BS}}^{\mathrm{blind}} = 2 \cdot \Pr\left[b' = b\right] - 1, \tag{1}$$

where $\mathrm{Adv}_{\mathrm{BS}}^{\mathrm{blind}}$ is the advantage of adversary $\mathscr{S}^*$ breaking the blindness property.

Definition 1 (blindness property). A blind signature protocol is recognized to be (t, ε)-blind if no PPT adversary $\mathscr{S}^*$ breaks the blindness property in time at most t, and $\mathrm{Adv}_{\mathrm{BS}}^{\mathrm{blind}}$ is at least ε.

3.4.2. Unforgeability. The unforgeability of blind signature is described by the following game between an honest signer $\mathscr{S}$ and a malicious user $\mathscr{U}^*$.

(i) Gen(λ) is run to obtain public and private keys (pk , sk). Then, pk is sent to $\mathscr{U}^*$ and sk is secretly held by $\mathscr{S}$

(ii) $\mathscr{U}^*$ adaptively engages in polynomially parallel interactive blind signatures by User(pk, m) algorithm with $\mathscr{S}$ executing Signer(pk, sk) algorithm

(iii) Let l denote the number of executions among $\mathscr{U}^*$ and $\mathscr{S}$, where $\mathscr{S}$ outputs complete

(iv) $\mathscr{U}^*$ wins the game if he outputs l^* valid signature ($m_1, \sigma(m_1), \cdots, (m_{l^*}, \sigma(m_{l^*}))$ such that they are different signatures for l^* different messages and $l^* l$

We define $\mathrm{Adv}_{\mathrm{BS}}^{\mathrm{unforge}}$ is the probability that U^* wins the above game. Then, we give the definition of blind signature unforgeability.

Definition 2 (unforgeability). A blind signature is (t, q_S, ε) -unforgeable if there does not exist PPT adversary $\mathscr{U}^*$ win the above game, where t is the most time, q_S is the most times U^* motivates the blind signature, and ε is the least $\mathrm{Adv}_{\mathrm{BS}}^{\mathrm{unforge}}$.

Notations used in this paper are explained in Table 1.

Table 1: Notations.

Notations	Description
p	A large prime number
F_p	A finite field with the order p
a, b	Coefficients defining the elliptic curve
G	A generator point
n	The prime order of generator G
Z_n^*	Nonzero integers not larger than n
$H(\cdot)$	One-way hash function
$\mathscr{S}$	The signer
$\mathscr{U}$	The user asking for blind signature
d	Private key of $\mathscr{S}$
Q	Public key of $\mathscr{S}$, where $Q = d \cdot G$
m	The original message to be signed
$\tilde{m}$	The blinded message
s	Digital signature for m
$\tilde{s}$	Blind signature
$R, \tilde{R}$	Points on the elliptic curve
r	x-coordinate of point R
$\tilde{r}$	x-coordinate of point $\tilde{R}$
α, β	The blind factors
k	The random integer number

4. Review of Bütün and Demirer's Scheme

In this section, Bütün and Demirer's scheme [13] will be briefly reviewed. Their scheme comprises the following five phases, including initialization, blinding, signing, unblinding, and verifying. Each phase of Bütün and Demirer's scheme is presented in the following subsection.

(i) *Initialization Phase*. The elliptic curve parameters are params $= \{p, F_p, a, b, G, n\}$, where F_p is a finite field defined by the big prime number p; a, b defines the elliptic curve $E(F_p)$: $y^2 = x^3 + ax + b \bmod p$; G is a base point on $E(F_p)$ with the order n

The signer randomly selects an integer $d \in Z_n^*$ as the secret key and calculates $Q = d \cdot G$ as the public key. For each blind signature request from a user, the signer chooses a random number $k \in Z_n^*$ and computes the point $\tilde{R} = kG = (x_1{}',$ $y_1{}')$ and $\tilde{r} = x_1{}' \bmod n$. If $\tilde{r} = 0$, the signer reselects the nonce k; otherwise, he transmits $\tilde{R}$ to the user.

(ii) *Blinding Phase*. Upon receiving $\tilde{R}$, the user first extracts $\tilde{r}$ from $\tilde{R}$ and chooses two blind factors α, $\beta \in Z_n^*$. Then, he calculates $R = \alpha\tilde{R} + \beta G = (x_1, y_1)$, r $= x_1 \bmod n$ and blinds message m through $\tilde{m} = \alpha H$ $(m)\tilde{r}r^{-1} \bmod n$. Finally, the user transmits the blinded message $\tilde{m}$ to the signer

(iii) *Signing Phase*. On receiving the blinded message, the signer uses his private key d to sign tildem. He computes $\tilde{s} = d\tilde{r} + k\tilde{m} \bmod n$ and sends $\tilde{s}$ to the user

(iv) *Unblinding Phase*. On receiving $\tilde{s}$, $\mathscr{U}$ verifies whether $\tilde{s}$ is in the range of Z_n^*. If it holds, the signature is unblinded as follows:

$$s = \tilde{s} r \tilde{r}^{-1} + \beta H(m) \ \bmod\ n. \tag{2}$$

Eventually, $\mathscr{U}$ outputs the digital signature $\{s, R\}$ on message m

(v) *Verifying Phase*. On receiving $\{s, R\}$, the verifier, respectively, calculates $f_1 = s \cdot G \bmod n$ and $f_2 = r \cdot Q + H(m) \cdot R$. Then, he verifies the equation $f_1 = f_2$. If the equation holds, $\{s, R\}$ is a valid signature of the message m; otherwise, the signature is invalid

Correctness. The correctness can be verified by the following equations:

$$\begin{aligned} s &= \tilde{s} r \tilde{r}^{-1} + \beta H(m) \ \bmod\ n = (d\tilde{r} + k\tilde{m}) r \tilde{r}^{-1} + \beta H(m) \ \bmod\ n \\ &= dr + k\tilde{m} r \tilde{r}^{-1} + \beta H(m) \ \bmod\ n \\ &= dr + k\left(\alpha H(m) \tilde{r} r^{-1}\right) r \tilde{r}^{-1} + \beta H(m) \ \bmod\ n \\ &= dr + \alpha k H(m) + \beta H(m) \ \bmod\ n, \\ f_1 &= s \cdot G = (dr + \alpha k H(m) + \beta H(m)) \cdot G \\ &= rd \cdot G + H(m)\left(\alpha \cdot \tilde{R} + \beta \cdot G\right) = r \cdot Q + H(m) \cdot R = f_2. \end{aligned} \tag{3}$$

5. Attack on Bütün and Demirer's Scheme

In this section, we show a malicious signer $\mathscr{M}$ can find a link between the blind signature s' and the original message m. Suppose that the signer saves all the transcripts $\{k, \tilde{R}', \widetilde{m'}, \tilde{s}\ '\}$ of his signatures. Using the unblinded signature $\{m, R, s\ \}$, $\mathscr{M}$ can match a blinded signature he has signed to an original message m. Detailed procedures are as follows:

(i) Extracting $r = x_1 \ \bmod\ n, \tilde{r}' = x_{1'} \ \bmod\ n$ from $R = (x_1, y_1), \tilde{R}' = (x_1{}', y_1{}')$

(ii) Calculating $\widetilde{m'} r \tilde{r}'^{-1}$ denoted as $\alpha' H(m')$

(iii) Calculating $s - \tilde{s}' r \tilde{r}'^{-1}$ denoted as $\beta' H(m')$

(iv) Using the private key d to verify whether the following equation $dr + k\alpha' H(m') + \beta' H(m') = s$ holds

$$dr + k\alpha' H\left(m'\right) + \beta' H\left(m'\right) = s \tag{4}$$

If equation (4) holds, $\mathscr{M}$ is able to find the linkage between the blind signature and his signed blind message m ; otherwise, going through all transcripts $\{k, R', m', s'\}$ and repeating the above process. This shows Bütün and Demirer's scheme is insecure, because there is absence of untraceability. The next section is our improvement of Bütün and Demirer's scheme.

6. Our Proposed Scheme

In this section, an untraceable blind signature scheme is completely described. Our blind signature scheme comprises four phases: setup phase, key generation phase, blind signing phase, and verification phase.

6.1. Setup Phase. On inputting the security parameter λ to reach the expected security magnitude, the elliptic curve parameters are output as params $= \{p, F_p, a, b, G, n\}$, where p is a large prime that specifies the finite field F_p; $a, b \in F_p$ defines the elliptic curve $E(F_p)$: $y^2 = x^3 + ax + b \bmod p$; G is a base point on $E(F_p)$, and n is the prime order of G.

6.2. Key Generation Phase. The private and public key of the signer $\mathscr{S}$ is generated by the following steps: First, generating a random nonce d from Z_n^*. Second, calculating the elliptic curve point $Q = d \cdot G = (x_Q, y_Q)$. Finally, $\mathscr{S}$ keeps the private key d secret and the public key Q published.

6.3. Blind Signing Phase. As shown in Figure 3, the user and the signer execute the following steps to generate a signature.

(i) For each blind signature request, a random integer k is generated by $\mathscr{S}$ and the elliptic curve point $\tilde{R}$ is computed as follows:

$$\begin{aligned} \tilde{R} &= k \cdot G = (x_{1'}, y_{1'}), \\ \tilde{r} &= x_1{}' \bmod n. \end{aligned} \tag{5}$$

Moreover, the signer checks $\tilde{r} \neq 0$. If the inequation holds, $\mathscr{S}$ transmits the elliptic curve point $\tilde{R}$ to the user $\mathscr{U}$; otherwise, $\mathscr{S}$ reselects k and repeats (5) to fulfill $\tilde{r} \neq 0$

(ii) Upon receiving $\tilde{R}$, $\mathscr{U}$ performs the following operations to obtain the blinded message $\tilde{m}$. Firstly, extracting $\tilde{r} = x_1{}' \bmod n$ from $\tilde{R}$. Secondly, randomly selecting two factors $\alpha, \beta \in Z_n^*$ and computes $R = (\alpha + \beta H(m)^{-1})\tilde{R} + (\alpha^{-1}\tilde{r}^{-1} + \alpha\beta)G = (x_1, y_1)$. Thirdly, extracting $r = x_1 \bmod n$ from R. Finally, calculating $\tilde{m} = (\alpha H(m) + \beta) r^{-1} \tilde{r} \ \bmod\ n$ to blind the original message. Having executed the above steps, $\mathscr{U}$ sends the blinded message $\tilde{m}$ to $\mathscr{S}$

(iii) Upon receiving $\tilde{m}$, $\mathscr{S}$ first extracts $\tilde{r} = x_1{}' \bmod n$ from $\tilde{R}$. Then, he uses private key d and selects a random nonce k to compute the blind signature $\tilde{s} = d\tilde{r} + k\tilde{m} \bmod n$. Finally, $\mathscr{S}$ transmits the blinded signature $\tilde{s}$ to $\mathscr{U}$

(iv) On receiving $\tilde{s}$, $\mathscr{U}$ verifies whether $\tilde{s} \in Z_n^*$ satisfies. If it holds, the signature is unblinded as follows:

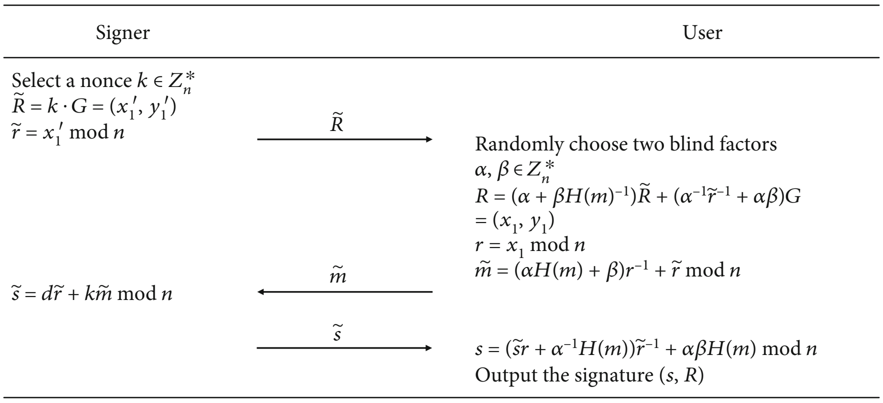
Signer
User
Select a nonce $k \in Z_n^*$
$\tilde{R} = k \cdot G = (x_1', y_1')$
$\tilde{r} = x_1' \bmod n$
$\tilde{R}$
Randomly choose two blind factors
$\alpha, \beta \in Z_n^*$
$R = (\alpha + \beta H(m)^{-1})\tilde{R} + (\alpha^{-1}\tilde{r}^{-1} + \alpha\beta)G$
$= (x_1, y_1)$
$r = x_1 \bmod n$
$\tilde{m} = (\alpha H(m) + \beta)r^{-1} + \tilde{r} \bmod n$
$\tilde{m}$
$\tilde{s} = d\tilde{r} + k\tilde{m} \bmod n$
$\tilde{s}$
$s = (\tilde{s}r + \alpha^{-1}H(m))\tilde{r}^{-1} + \alpha\beta H(m) \bmod n$
Output the signature (s, R)

Figure 3: The proposed scheme.

Table 2: Comparison of security properties.

Properties	Schemes				
	Ours	[13]	[16]	[36]	[37]
Correctness	✓	✓	✓	✓	✓
Verifiability	✓	✓	✓	✓	✓
Impersonality resistance	✓	✓	✓	✓	✓
Privileged insider resistance	✓	✓	✓	✓	×
Privacy preservation	✓	×	✓	✓	✓
Unforgeability	✓	✓	✓	✓	✓
Untraceability	✓	×	✓	✓	✓
Unlinkability proof	✓	×	✓	×	×

Table 3: Performance comparisons.

Protocol	Computation cost	Communication cost (bit)
Ours	$3T_{\text{pm}} + 4T_{\text{mi}} = 6.663$ ms	1024
Ref. [13]	$3T_{\text{pm}} + 2T_{\text{mi}} = 6.579$ ms	1024
Ref. [16]	$2T_{\text{H}} + 3T_{\text{pm}} + 1T_{\text{mi}} = 17.523$ ms	1280
Ref. [36]	$5T_{\text{pm}} = 10.825$ ms	2368
Ref. [37]	$9T_{\text{pm}} = 19.485$ ms	3136

Table 4: Running time of basic operations (ms).

Notations	Description	Running time
T_{H}	Hash-to-point	5.493
T_{pm}	Point multiplication	2.165
T_{mi}	Modular inversion	0.042

$$s = \left(\tilde{s}r + \alpha^{-1}H(m)\right)\tilde{r}^{-1} + \alpha\beta H(m) \bmod n. \tag{6}$$

Eventually, $\mathcal{U}$ outputs the digital signature $\{s, R\}$ on message m

6.4. Verification Phase. Any verifier can verify the validity of the signature $\{s, R\}$. First, using the public parameter G and signature s to compute $g_1 = s \cdot G \bmod n$; second, extracting $r = x_1 \bmod n$ from $R = (x_1, y_1)$; third, using the signer's public key Q and signature value R to calculate $g_2 = r \cdot Q + H(m) \cdot R$; finally, verifying whether the equation $g_1 = g_2$ holds. If the equation holds, $\{s, R\}$ is a valid signature of message m; otherwise, the signature is invalid.

Correctness. The correctness can be verified by the following equations:

$$\begin{aligned} s &= \left(\tilde{s}r + \alpha^{-1}H(m)\right)\tilde{r}^{-1} + \alpha\beta H(m) \bmod n \\ &= \left((d\tilde{r} + k\tilde{m})r + \alpha^{-1}H(m)\right)\tilde{r}^{-1} + \alpha\beta H(m) \bmod n \\ &= dr + k\tilde{m}r\tilde{r}^{-1} + \alpha^{-1}H(m)\tilde{r}^{-1} + \alpha\beta H(m) \bmod n \\ &= dr + H(m)\left(\alpha + \beta H(m)^{-1}\right)k + H(m)\left(\alpha^{-1}\tilde{r}^{-1} + \alpha\beta\right) \bmod n, \end{aligned}$$

$$\begin{aligned} g_1 &= s \cdot G = rd \cdot G + H(m)\left(\left(\alpha + \beta H(m)^{-1}\right)\tilde{R} + \left(\alpha^{-1}\tilde{r}^{-1} + \alpha\beta\right) \cdot G\right) \\ &= r \cdot Q + H(m) \cdot R = g_2. \end{aligned} \tag{7}$$

7. Security

In this section, we give the formal security proof of our blind signature scheme's blindness property and unforgeability.

7.1. Security Proof. According to the security model of blindness in Section 3.4, the blindness is to guarantee that an adversarial signer $\mathcal{S}^*$ cannot distinguish signatures from two different messages. We will show that our scheme's signature values are independent from the view of $\mathcal{S}^*$.

Theorem 3 (blindness property). *Our proposed blind signature keeps blindness property.*

Proof. For any public key output Q from the malicious signer $\mathcal{S}^*$, $(k, \tilde{m})$ is perfectly independent from (m, α, β) in the blind signature process in the view of $\mathcal{S}^*$. On the one hand, the k is a completely random number chosen from Z_n^*. On the other hand, $\tilde{m} = (\alpha H(m) + \beta)r^{-1}\tilde{r} \bmod n$, where $\tilde{r}$ is the

x-coordinate of $\tilde{R} = k \cdot G$. Due to the randomness of k, $\tilde{m}$ is independent of (m, α, β). □

Next, we will prove that the signature (m, s, R) is independent from the view of $\mathcal{S}^*$. Since $s = (\tilde{s}r + \alpha^{-1}H(m))\tilde{r}^{-1} + \alpha\beta H(m) \mod n$ and (m, α, β) cannot be obtained from $(k, \tilde{m})$, s is perfectly independent. Moreover, $R = (\alpha + \beta H(m)^{-1})\tilde{R} + (\alpha^{-1}\tilde{r}^{-1})G + \alpha\beta G$ and (α, β) is not related to $(k, \tilde{m})$. Therefore, the signature values (m, s, R) are independent in the view of $\mathcal{S}^*$.

Above all, our blind signature scheme keeps perfectly blindness property.

Theorem 4 (unforgeability). *If the ECDLP assumption holds, our proposed blind signature is existential unforgeability against chosen-message attacks (EU-CMA).*

Proof. Suppose that $\mathcal{A}$ is an adversary delegated for a malicious user that forges the proposed blind signature scheme, there exists a challenger $\mathcal{C}$ that can break unforgeability of the MDSA. Then, it is contradictory to the ECDLP assumption. □

In this proof, Signer(pk, sk) algorithm is modelled as a signing oracle and forging process of the proposed blind signature is depicted as follows.

(i) $\mathcal{C}$ runs the Gen(λ) to generate a pair of public and private keys $(Q = x \cdot G, \mathrm{sk} = x)$. Then, $\mathcal{B}$ sends Q to $\mathcal{A}$ as the public key

(ii) $\mathcal{C}$ executes signing oracle following the proposed blind signature, that is, the signing oracle outputs $\tilde{R}$ and $\tilde{s}$ with the corresponding $\tilde{m}$ from $\mathcal{A}$

(iii) $\mathcal{A}$ could adaptively request l times $\mathcal{C}$ to sign different $\tilde{m}$ as the proposed interactive blind signature

(iv) If $\mathcal{A}$ outputs l^* different signatures $\Sigma = ((m_1, s_1, R_1), \cdots, (m_{l^*}, s_{l^*}, R_{l^*}), l^* l)$, there exists one signature $(m_f, s_f, R_f) \in \Sigma$ forged by $\mathcal{A}$. In addition, $\mathcal{A}$ cannot obtain the secret key x through $\tilde{R}, \tilde{s}$ due to $\tilde{R}$ is unrelated to x and the private key cannot be recovered by the equation $\tilde{s} = x\tilde{r} + k\tilde{m} \mod n$ with k unknown to $\mathcal{A}$

Moreover, the signature (s, R) is a variant of MDSA since $s = (\tilde{s}r + \alpha^{-1}H(m))\tilde{r}^{-1} + \alpha\beta H(m) \mod n = xr + H(m)(\alpha + \beta H(m)^{-1} + \alpha^{-1}\tilde{r}^{-1} + \alpha\beta) = xr + H(m)z$ where $z = \alpha + \beta H(m)^{-1} + \alpha^{-1}\tilde{r}^{-1} + \alpha\beta$ and the signature is verified by the equation $s \cdot G = r \cdot Q + H(m) \cdot R$. Therefore, unforgeability of the proposed blind signature is reduced to the security of MDSA. Under the difficulty assumption of ECDLP, MDSA is existential unforgeability.

7.2. Security Analysis. According to references, we analyze identity privacy preservation, unforgeability, untraceability, and verifiability of the proposed scheme.

(i) *Privacy Preservation*. We have proven blindness of our proposed blind signature in 7.1. Therefore, nobody including the control center and substations could recognize the real identity of users when they request for more power. Thus, identity and electricity consumption privacy of users could be protected

(ii) *Unforgeability*. As shown in 7.1, the proposed blind signature scheme is existential unforgeability. Thereby, any users (i.e., smart meters) cannot unforge blind signatures for credentials with desired values

(iii) *Untraceability*. Suppose that a control center attempts to find linkage among the credential he signed and signature. For this, he could preserve all the transcripts $(k, \tilde{m}, \tilde{s})$. Even after the blind signature (m, s, R) is made public by the user, the control center is still unable to find the blind factors α, β. Moreover, $(k, \tilde{m}, \tilde{s})$ and (m, s, R) are independent of each other. Above all, it is impossible for the control center to link the signature (m, s, R) with corresponding transcript $(k, \tilde{m}, \tilde{s})$

(iv) *Verifiability*. The *correctness* of proposed blind signature insures that the control center can verify validity of credentials by checking equation $s \cdot G = r \cdot Q + H(m) \cdot R$

8. Performance Analysis

In this section, we compare the proposed scheme with Bütün and Demirer's [13], Verma and Singh's [16], Chaudhry et al.'s [36], and Mahmood et al.'s [37] in terms of security properties, computational cost, and communication cost. The results are listed in Tables 2 and 3 separately.

8.1. Security Properties. As we have analyzed in this paper, Bütün and Demirer's scheme [13] cannot resist that a malicious signer traces the original message he has signed, which means there is no untraceability in Bütün and Demirer's scheme. Furthermore, traceability provides opportunities for adversaries to recognize users' daily schedule and privacy preservation does not hold. In addition, [36] does not provide unlinkability proof and [37] does not have privileged insider resistance and unlinkability proof.

8.2. Performance Analysis

8.2.1. Computational Cost. In this subsection, we mainly consider the more time-consuming operations hash-to-point (T_{H}), point multiplication (T_{pm}), and modular inversion (T_{mi}) and adopt the executing time in [38] as shown in Table 4. It can be seen that the proposed scheme requires 3 point multiplication operations and 4 modular inversions, i.e., 6.663 ms, which is only slightly larger than that of [13] and smaller than the other three schemes' computational cost.

8.2.2. Communication Cost. We set the size of point on $E(F_p)$ is 512 bits, size of n is 256 bits, output size of general hash function is 256 bits, and size of timestamp is 32 bits. Then, we have the communication cost comparison in Table 3. We can see that our scheme and Ref. [13] have the least communication cost, i.e., 1024 bits than the other three literatures. Therefore, our scheme needs the least communicational bandwidth.

Above all, the proposed scheme has better security properties than Bütün and Demirer's [13] although performing two more modular inversions and has better computational costs with the same security properties of Verma et al.'s scheme.

9. Conclusion

Our scheme provided values of theory and application to some extent. On the one hand, the proposed untraceable blind signature is constructed under the noted MDSA algorithm and proof of which gave theoretical insurance of blindness and unforgeability. On the other hand, we put forward a new credential-based privacy-preserving power request model for smart grid. In this system model, the user's daily schedule could not leak outside with the help of blind signature since blinded factors hide the real signed message for the signer and verifiers cannot identify the real sources of messages. Moreover, it was shown that this scheme has better security or computational costs compared with other blind signatures under the same background or cryptographic infrastructure.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] J. W. Hughes, "IntelliGrid architecture concepts and IEC61850," in *Transmission and Distribution Conference and Exhibition, 2005/2006 IEEE PES*, pp. 401–404, 2006.

[2] W. Kong, J. Shen, P. Vijayakumar, Y. Cho, and V. Chang, "A practical group blind signature scheme for privacy protection in smart grid," *Journal of Parallel and Distributed Computing*, vol. 136, pp. 29–39, 2020.

[3] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: motivations, requirements and challenges," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 5–20, 2013.

[4] Q. Gao, Y. Wang, X. Cheng, J. Yu, X. Chen, and T. Jing, "Identification of vulnerable lines in smart grid systems based on affinity propagation clustering," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5163–5171, 2019.

[5] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "Pass: privacy-preserving authentication scheme for smart grid network," in *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Brussels, Belgium, 2011.

[6] A A Group, "Scada systems for smart grid," http://www.arcweb.com/Research/Studies/Pages/SCADA-Power.aspx.

[7] R. Li, C. Sturtivant, J. Yu, and X. Cheng, "A novel secure and efficient data aggregation scheme for IoT," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1551–1560, 2019.

[8] R. Liu, Y. Wang, S. Wu, C.-X. Wang, and W. Zhang, "Energy efficiency and area spectral efficiency tradeoff for coexisting wireless body sensor networks," *Science China Information Sciences*, vol. 59, no. 12, pp. 1–15, 2016.

[9] D. He, Y. Zhang, D. Wang, and K.-K. R. Choo, "Secure and efficient two-party signing protocol for the identity-based signature scheme in the IEEE P1363 standard for public key cryptography," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 5, pp. 1124–1132, 2020.

[10] Q. Feng, D. He, Z. Liu, D. Wang, and K.-K. R. Choo, "Distributed signing protocol for IEEE P1363-compliant identity-based signature scheme," *IET Information Security*, vol. 14, no. 4, pp. 443–451, 2020.

[11] Y. Zhang, D. He, X. Huang, D. Wang, K.-K. R. Choo, and J. Wang, "White-box implementation of the identity-based signature scheme in the IEEE P1363 standard for public key cryptography," *IEICE Transactions on Information and Systems*, vol. E103.D, no. 2, pp. 188–195, 2020.

[12] D. Chaum, R. L. Rivest, and A. T. Sherman, *Blind signatures for untraceable payments*, Springer, 1983.

[13] İ. Bütün and M. Demirer, "A blind digital signature scheme using elliptic curve digital signature algorithm," *Turkish Journal of Electrical Engineering & Computer Sciences*, vol. 21, 2013.

[14] P. Sarde and A. Banerjee, "A secure ID-based blind and proxy blind signature scheme from bilinear pairings," *Journal of Applied Security Research*, vol. 12, no. 2, pp. 276–286, 2017.

[15] C. Popescu, "Blind signature schemes based on the elliptic curve discrete logarithm problem," *Studies in Informatics and Control*, vol. 19, no. 4, pp. 397–402, 2010.

[16] G. K. Verma and B. B. Singh, "Efficient identity-based blind message recovery signature scheme from pairings," *IET Information Security*, vol. 12, no. 2, pp. 150–156, 2018.

[17] G. K. Verma and B. B. Singh, "Efficient message recovery proxy blind signature scheme from pairings," *Transactions on Emerging Telecommunications Technologies*, vol. 28, no. 11, 2017.

[18] H. Chen, L. Zhang, J. Xie, and C. Wang, "New efficient certificateless blind signature scheme," in *2016 IEEE Trustcom/BigDataSE/ISPA*, Tianjin, 2016.

[19] G. K. Verma, B. B. Singh, and H. Singh, "Provably secure certificate-based proxy blind signature scheme from pairings," *Information Sciences*, vol. 468, pp. 1–13, 2018.

[20] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid — the new and improved power grid: a survey," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 944–980, 2012.

[21] K. M. A. Alshehri, "Multi-period demand response management in the smart grid: a stackelberg game approach," http://hdl.handle.net/2142/88959.

[22] R. Zafar, A. Mahmood, S. Razzaq, W. Ali, U. Naeem, and K. Shehzad, "Prosumer based energy management and sharing in smart grid," *Renewable & Sustainable Energy Reviews*, vol. 82, pp. 1675–1684, 2018.

[23] M. H. Rehmani, A. Davy, B. Jennings, and C. Assi, "Software defined networks based smart grid communication: a

comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 99, 2019.

[24] N. I. Nimalsiri, C. P. Mediwaththe, E. L. Ratnam, M. Shaw, and S. K. Halgamuge, "A survey of algorithms for distributed charging control of electric vehicles in smart grid," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 99, pp. 1–19, 2019.

[25] L. Wen, K. Zhou, S. Yang, and L. Li, "Compression of smart meter big data: a survey," *Renewable & Sustainable Energy Reviews*, vol. 91, pp. 59–69, 2018.

[26] S. N. Makhadmeh, A. T. Khader, M. A. al-Betar, S. Naim, A. K. Abasi, and Z. A. A. Alyasseri, "Optimization methods for power scheduling problems in smart home: survey," *Renewable & Sustainable Energy Reviews*, vol. 115, article 109362, 2019.

[27] G. Si, Z. Guan, J. Li, P. Liu, and H. Yao, "A comprehensive survey of privacy-preserving in smart grid," in *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*, Zhangjiajie, China, 2016.

[28] 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 Generations Computer Systems*, vol. 81, pp. 557–565, 2018.

[29] J. L. Camenisch, J. M. Piveteau, and M. A. Stadler, "Blind signatures based on the discrete logarithm problem," in *Workshop on the Theory and Application of of Cryptographic Techniques*, Perugia, Italy, 1994.

[30] H. R. Tseng, "A secure and privacy-preserving communication protocol for V2G networks," in *2012 IEEE Wireless Communications and Networking Conference (WCNC)*, Paris, France, 2012.

[31] Z. Yang, S. Yu, W. Lou, and C. Liu, "P^2: privacy-preserving communication and precise reward architecture for V2G networks in smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 697–706, 2011.

[32] C. Yu, C. Chen, S. Kuo, and H. Chao, "Privacy-preserving power request in smart grid networks," *IEEE Systems Journal*, vol. 8, no. 2, pp. 441–449, 2014.

[33] W. Han and Y. Xiao, "Privacy preservation for V2G networks in smart grid: a survey," *Computer Communications*, vol. 91-92, pp. 17–28, 2016.

[34] J. C. L. Cheung, T. W. Chim, S. M. Yiu, V. O. K. Li, and L. C. K. Hui, "Credential-based privacy-preserving power request scheme for smart grid network," in *2011 IEEE Global Telecommunications Conference - GLOBECOM 2011*, pp. 1–5, Houston, TX, USA, 2011.

[35] T. Okamoto, "Efficient blind and partially blind signatures without random oracles," in *Theory of Cryptography*, S. Halevi and T. Rabin, Eds., pp. 80–99, Springer, Berlin, Heidelberg, 2006.

[36] S. A. Chaudhry, H. Alhakami, A. Baz, and F. Al-Turjman, "Securing demand response management: a certificate-based access control in smart grid edge computing infrastructure," *IEEE Access*, vol. 8, pp. 101235–101243, 2020.

[37] K. Mahmood, J. Arshad, S. A. Chaudhry, and S. Kumari, "An enhanced anonymous identity-based key agreement protocol for smart grid advanced metering infrastructure," *International Journal of Communication Systems*, vol. 32, no. 16, 2019.

[38] Q. Fan, J. Chen, L. J. Deborah, and M. Luo, "A secure and efficient authentication and data sharing scheme for internet of things based on blockchain," *Journal of Systems Architecture*, vol. 117, article 102112, 2021.