Hindawi
Security and Communication Networks
Volume 2021, Article ID 5531505, 16 pages
https://doi.org/10.1155/2021/5531505

Research Article

Generalized Proxy Oblivious Signature and Its Mobile Application

Shin-Yan Chiou [1,2] **and Yi-Xuan He** [1]

[1]*Department of Electrical Engineering, College of Engineering, Chang Gung University, Kwei-Shan, Taoyuan, Taiwan*
[2]*Department of Nuclear Medicine, Linkou Chang Gung Memorial Hospital, Taoyuan, Taiwan*

Correspondence should be addressed to Shin-Yan Chiou; ansel@mail.cgu.edu.tw

Received 19 February 2021; Revised 17 April 2021; Accepted 3 May 2021; Published 25 May 2021

Academic Editor: Manjit Kaur

Oblivious signature ensures users select from the specified candidates. However, users can choose only one candidate. This paper proposes a generalized oblivious signature scheme with proxy function. The scheme can be applied to many applications such as multichoice e-voting or e-lottery. Since there have been many applied research studies on e-voting, in this paper, we decided to apply this scheme to e-lottery, which is fair, secure, efficient, multiselect, and agent-based. In the lottery system, the server cannot cheat after a user makes a choice, and no one even the proxy can get any benefits. The signature scheme along with the lottery system is proved secure in the random oracle model. The lottery system is also implemented on Android smartphones. To the best of our knowledge, this is the first work done on a generalized proxy oblivious signature along with a fair and secure multiple-choice e-lottery system.

1. Introduction

In recent years, network transactions for applications such as Internet auctions and banking have increased greatly. Network and mobile security technologies play important roles in protecting users' privacy [1–4]. In this regard, digital signatures have attracted considerable attention. By using public key cryptography, a signer can sign a message using his or her private key, which is owned only by the signer, to create a digital signature for the message. Then, any verifier can validate the correctness of this signature by using the signer's public key.

However, it is necessary to protect the privacy of signature receivers in some situations, such as the contents of signed message in a digital cash system or the choices from candidates in an e-voting situation. In 1982, Chaum [5] introduced a blind signature scheme to offer blindness which protects the signee's privacy. In 2013, Nayak et al. [6] proposed a blind signature scheme based on an elliptic curve discrete logarithm problem. In 1981, Rabin [7] introduced the concept of oblivious transfer. In 1994, Chen [8] proposed the concept of oblivious signatures and considered two types of oblivious signature schemes. In 2008, Tso et al. [9] provided formal definitions and security requirements for an oblivious signature scheme. In 2012, Chou [10] proposed a more efficient and secure k-out-of-n oblivious transfer scheme. In 2018, Zhang et al. [11] proposed a new post-quantum blind signature from lattice assumptions. In 2019, Wang et al. [12] introduced a new construction of blind signatures from braid groups.

In 1996, Mambo et al. [13] proposed the concept of proxy signature. Various proxy-based schemes have been proposed [14, 15]. In 2000, Lin et al. [16] proposed the first proxy blind signature scheme that combines the functionalities of both proxy signatures and blind signatures. In 2002, Tan et al. [17] proposed a proxy blind signature scheme; however, in 2003, Lal et al. [18] showed this scheme to be insecure and further proposed a new scheme that is secure and more efficient than Tan's scheme. In 2013, Yang et al. [19] proposed a new proxy blind signature scheme that allows revocation.

In 2017, Chiou et al. [20] proposed two novel 1-out-of-n blind (oblivious) and proxy signature schemes that combine the advantages of oblivious signatures and proxy signatures and satisfy the security properties of these two signature schemes. In 2018, Lin et al. [21] proposed a short linearly

homomorphic proxy signature scheme, and Li et al. [22] proposed a blind proxy resignature scheme based on isomorphisms of polynomials. In 2019, Tso [23] proposed a two-in-one oblivious signature that combines message oblivious and signer oblivious into one scheme.

For electronic voting systems, in 2001, Ray et al. [24] introduced an online anonymous e-voting protocol that allows a voter to cast his or her ballot anonymously by exchanging untraceable authentic messages. In 2013, Pan et al. [25] proposed an e-voting scheme that is based on the ring signature and is resistant to a clash attack. Several schemes with delegated voting functionality have been proposed. In 2013, Zwattendorfer et al. [26] proposed a proxy voting scheme that allows a voter to delegate his or her voting power to a proxy who actually casts the ballots for all represented voters. Norway has used an Internet-based voting protocol for some years, and the vote privacy and correctness of this scheme have been demonstrated [27]. In 2016, Kulyk et al. [28] proposed a new coercion-resistant proxy voting scheme by extending the coercion-resistant JCJ/Civitas theme, aiming to prevent direct voter coercion, delegation coercion, and proxy coercion. They also proposed a new proxy voting scheme [29] and extended the Helios voting system [30] with delegated voting functionality. In 2017, Cohensius et al. [31] considered a social choice problem and demonstrated that the mechanism using proxy voting better approximates the optimal outcome. In the end of 2017, Chiou et al. [20] proposed an anonymous e-voting system with proxy signer based on their proposed 1-out-of-n blind and proxy signature schemes.

For electronic lottery systems, many scholars have proposed protocols [32–37] in attempts to achieve true fairness and satisfy security requirements. However, these measures suffer from security issues including insufficient fairness or privacy concerns. For example, in some protocols (e.g., [32, 35, 36]), the trusted third party mechanism is required to maintain system fairness. In other methods (e.g., [34]), one side can decide key parameters for determining the winner. Moreover, some schemes (e.g., [33]) fail to account for player privacy concerns.

Paper Motivation. Compared with a blind signature scheme, an oblivious signature scheme used in e-voting or e-lottery provides one more property: ambiguity in selected messages. A signer cannot find out which message a voter or a player has selected while signing the messages, but the signer can be certain that the message the voter/player chooses is one or some of the predetermined messages; otherwise, the signature would not be accepted by a verifier. Therefore, in oblivious signature systems, which differ from blind signature schemes, the limited signed contents can prevent potential malicious users from obtaining valid signatures of some candidates for unauthorized purposes.

In addition, because each unit of a group (such as each state of a country, each county of a state, each campus of a school, or each approved bank of a group) may use different methods to authorize their members (using different keys), polling/betting booths with proxy ability are required. Additional benefits include reducing the load at voting centers or lottery owners and avoiding network jams. Moreover, the mobility of the voting/lottery functionality allows people to vote/play from anywhere using their mobile devices, thereby making the electronic voting/lottery system more convenient.

The goal in this research is a design of a generalized oblivious signature scheme with proxy function and extend the designed schemes to applications such as e-voting and e-lottery systems.

Paper Contribution. This paper proposes a generalized t-out-of-n proxy oblivious signature, which combines the advantages of proxy signature [13, 38] and 1-out-of-n oblivious signature [8, 9, 38, 39] and satisfies the security properties of the signature scheme. By using the concept proposed in [40], we conduct security analyses and proofs. The performance comparisons show that our scheme is efficient. Our scheme can be easily applied to an anonymous t-out-of-n e-voting system with proxy signer using Chiou's method [20]. Based on our scheme, we also design a proxy-based fair e-lottery system which provides a multiple-prize multiple-choice function and satisfies the fairness and security properties of a lottery. There security analyses and feature comparisons are conducted, and the results showed that our scheme has better performance. Finally, the system is implemented on a smart phone to provide the player with a more convenient digital experience while participating in game activities which take place in a truly fair environment. The user studies for college students indicate that most users think the e-lottery is convenient and more than half persons are willing to play the game again. To the best of our knowledge, this is the first work done on t-out-of-n proxy blind signature scheme and fair multiple-choice e-lottery system.

Paper Structure. The rest of this paper is organized as follows. Section 2 reviews the relevant literature, and Sections 3 and 4 provide definitions of security and system requirements of the proposed signature algorithm and lottery scheme along with descriptions of the protocol and the systems. Section 4 provides a comparison analysis in terms of system security and fairness for the proposed protocol and our system and demonstrates their security features. Section 5 describes the system implementation, and Section 6 provides conclusions.

2. Related Works

2.1. Proxy Signature Scheme. The proxy signature method was first proposed by Mambo in 1996 [13]. The method includes three roles: original signer, proxy signer, and verifier. The original signer can authorize the proxy signer to represent him/her in signing public-facing documents.

Delegation [35] can be categorized as full delegation, partial delegation, and delegation by warrant, as follows:

(1) *Full Delegation*. The proxy signer obtains a copy of the original signer's signature key to produce a proxy signature value identical to the signature of the original signer.

(2) *Partial Delegation*. The proxy signer's signature key is obtained through a calculation based on the original signer's private key. However, the proxy signature key cannot be used to obtain information related to the original signer's private key. Partial delegation can be categorized as one of two types: proxy-unprotected or proxy-protected. In the former, the original signer and proxy signer can both provide valid proxy signatures. In the latter, only the proxy signer can provide a valid proxy signature.

(3) *Delegation by Warrant*. A warrant based on the original signer's signature is used to validate the proxy signer's signing authority. The proxy signer's authorization message and proxy signature content are included in the proxy signature, and the verifier is used to determine the legitimacy of the authorization.

2.2. Oblivious Signature Scheme. Oblivious signature is a variation of digital signature and was first proposed by Chen [8]. The method includes three roles: the signer, recipient, and verifier. Oblivious signature seeks to ensure that the recipient can only receive plaintext values specified by the signer, selecting one or more of the plaintext values for signing. When the signer signs, he/she remains unaware of the selected plaintext content.

Tso et al.'s oblivious signature protocol [9] provided the first clear definition of oblivious signature security requirements as completeness, unforgeability, and ambiguity.

(1) *Completeness*. If the signer and recipient follow the protocol steps, the signature information received by the final recipient must be from the signer's valid signature

(2) *Unforgeability*. Given a public signature algorithm, attackers will still have difficulty forging a usable signature in a reasonable or acceptable amount of time

(3) *Ambiguity*. When the recipient requests the signer's signature, the signer is unable to determine the content of the signed plaintext message, thus maintaining the recipient's privacy

In 2017, Chiou et al. [38] proposed a novel oblivious signature which is integrated with proxy signature. Their protocol defines seven security requirements: completeness, unforgeability, unlinkability, undeniability, verifiability, distinguishability, and ambiguity. Except completeness, unforgeability, and ambiguity, the other four requirements are shown as follows:

(1) *Unlinkability*. The proxy signer can identify neither the message nor the proxy signature he or she generates associated with the scheme after the signature is revealed when necessary

(2) *Undeniability*. Neither the original signer nor the proxy signer can deny the signature they have created after signature generation

(3) *Verifiability*. The signature that the receiver receives should be able to convince the verifier of the agreement from the original signer and the proxy signer

(4) *Distinguishability*. The proxy signature is distinguishable from a normal one

In 2018, Chiou and Chen [39] presented a novel t-out-of-n oblivious signature, which is applied to multiple-choice e-voting scheme on the mobile system. Their scheme satisfies not only the security requirements but also t-out-of-n selection restriction and nonreduplication making such scheme well suited for multiple-choice e-voting applications. The added two requirements are shown as follows:

(1) *Selection Restriction*. The recipient is unable to get a valid signature of any message except the n messages

(2) *Nonreduplication*. The recipient cannot get more than one signature on the same message in a signing process

2.3. Fair Online Game System. In the virtual world of digital communications, a wide range of security requirements has driven the continuous development of new digital signature techniques [41–44]. The real-world equivalent of the game includes probability factors which impact winning conditions (e.g., luck) in competitive activities. With the rapid development of the Internet, electronic game environments [45–49] have gradually achieved mass market penetration, and the fairness of online games has received increased attention, prompting the development of many protocols since the 1990s.

Zhao et al. proposed a fair online game protocol [32] using the trusted third party (TTP) mechanism to maintain system fairness where the key parameters (banker vs. player) are entirely determined by the banker. In actual practice, however, this can potentially create an unfair situation for the Player.

Kushelevitz et al. proposed a fair lottery system [33] which does not require TTP, but the protocol does not take into account player privacy issues and only discusses factors impacting the generation of a winning random number in the context of one-on-one competitions, frequently raising fairness issues due to potential cheating on the part of the banker.

In 2004, Blundo et al. proposed a secure electronic game platform [34] featuring the comprehensive design of an online game system architecture including payment mechanisms between players, player anonymity, and player privacy options. However, the key parameters for determining the winner are decided exclusively by one side, thus again raising fairness issues in the practical application of the game.

2.4. Proxy Partially Blind Signature Scheme with Proxy Revocation. Yang and Liang [19] indicated that Liu et al.'s scheme [50] is unable to provide untraceability and is susceptible to the attacks of counterfeit signatures. They

proposed a new proxy blind signature scheme that improves Liu et al.'s scheme [50] and allows revocation. Their scheme combines the techniques of Schnorr signature [51], partially blind signature [52], and proxy signature [53] that can terminate proxy privileges and simultaneously provide untraceability, unforgeability, and the other security features required of proxy signatures. The scheme provides seven requirements: distinguishability, nonrepudiation, verifiability, unforgeability, identifiability, prevention of misuse, and unlinkability.

3. Proposed *t*-out-of-*n* Proxy Blind Signature Protocol

The proposed *t*-out-of-*n* proxy blind signature is based on the security requirement in Definition 1.

3.1. Attacker Model. The proposed signature schemes consist of four entities: an original signer **A**, a proxy signer **B**, a receiver **R**, and a verifier **V**. In our scheme, we assume the channels between **A** and **B** are secure. Any identity (i.e., **R** or **V**) communicates with **B** via an insecure public channel, offering adversaries opportunities to intercept. In the following, we present the assumptions of the attacker model [54, 55]:

(1) An adversary may eavesdrop on all communications between protocol actors over the public channel
(2) An attacker can modify, delete, resend, and reroute the eavesdropped message
(3) An attacker cannot intercept a message over a secure channel
(4) An attacker cannot be a legitimate original signer or proxy signer
(5) The attacker knows the protocol description, which means the protocol is public

3.2. Security Requirements. System requirements [13, 36, 56] of the proposed signature system are described as Definition 1.

Definition 1 (system requirements of t-out-of-n proxy blind signature protocol). Assume an original signer, a proxy signer, a recipient, and a verifier interact in *t*-out-of-*n* proxy blind signature protocol. The protocol is secure if it achieves the following conditions. (1) Completeness: recipient obtains a signer's signature to verify the message completeness. (2) Distinguishability: from the signature message, anyone can distinguish whether or not the signature is a proxy signature. (3) Identifiability: from the signature information, anyone can determine the identity of the signer. (4) Verifiability: once they receive the signature information, anyone can test the signature's validity. (5) Ambiguity: when the recipient requests the signature, the signer is unable to determine the content of the signed plaintext, thus ensuring the recipient's privacy. (6) Nonrepudiation: once the proxy signer signs the plaintext authorization specification, it becomes valid and the original signer is unable to repudiate the proxy signer's authorization, while the proxy signer is unable to repudiate that he/she signed the document. (7) Unforgeability: aside from the proxy signer specifically authorized by the original signer, no one can produce a verifiable signature, including the original signer him or herself. (8) Prevention of misuse: once the proxy signer secures the original signers proxy authorization, the proxy authority cannot be used outside the specified use, and misuse of authorization should be clearly demonstrable.

3.3. Proposed Protocol. The proposed *t*-out-of-*n* proxy blind signature protocol is based on RSA-FDH, RSA-based blind signatures, and certificate chains that follow the hash-and-sign paradigm. It includes four roles (original signer O, proxy signer P, recipient R, and verifier V) and is divided into four phases (initialization, proxy, signing, and verification) (Figures 1–3).

(1) *Initialization Phase*. O and P generate RSA cryptosystem public keys (e_O, N_O) and (e_P, N_P) and private keys (d_O, N_O) and (d_P, N_P) and then produce the warrant of delegation m_{wr} to demonstrate the proxy signer's signing authorization.
(2) *Proxy Phase*. As shown in Figure 1, O transfers signing authority to P as follows:

(1) O calculates $s_O \equiv H(m_{wr} \| e_P)^{d_O} \bmod N_O$ and transfers s_O and m_{wr} to P.
(2) P verifies whether $s_O^{e_O ?} \equiv H(m_{wr} \| e_P) \bmod N_O$ is held. If it does, it is believed O's authorization is obtained.

(3) *Signing Phase*. As shown in Figure 2, P transmits n plaintext documents $m_i (i = 1, 2, \ldots, n)$ allowing recipient R to determine t "selections" $(t < n)$. Then, R blinds the "selections" before transmitting them to P for signing. Finally, R resolves P's valid signature as follows:

(1) P selects a random number $SN \in Z_{N_P}$ as a protocol identifier and then calculates $s_{m_i} \equiv H(m_i \| m_{wr} \| SN)^{d_P} \bmod N_P$ before transmitting SN, $\{m_i, s_{mi}\}$, s_O, and m_{wr} to R.
(2) R verifies whether $s_O^{e_O ?} \equiv H(m_{wr} \| e_P) \bmod N_O$ and $s_{m_i}^{e_P ?} \equiv H(m_i \| m_{wr} \| SN) \bmod N_P$. If both the equations hold, it is believed that m_i is a legitimate option. R selects t options $M_j = m_i$ $(j = 1, 2, \ldots, t)$, selecting a random number $b_j \in Z_{N_P}^*$ as a blinding factor, then calculates $\beta_j \equiv b_j^{e_P} \times M_j \bmod N_P$, and transmits $\{\beta_j\}$ to P.
(3) P selects a random number $r_j \in Z_{N_P}$, calculates $s_j \equiv (H(r_j \| SN) \times \beta_j)^{d_P} \bmod N_P$, and transmits s_j and r_j to R.
(4) R calculates $s_{c_j} \equiv b_j^{-1} s_j s_{M_j} \bmod N_P$ to obtain a valid signature for M_j: $\mathrm{Sig}(M_j) = \{s_{c_j}, r_j, SN, s_O, m_{wr}, e_O, e_P\}$.

(4) *Verification Phase*. As shown in Figure 3, R sends the M_j signature value to the verifier V for verification. V thus believes the plaintext has in fact been selected

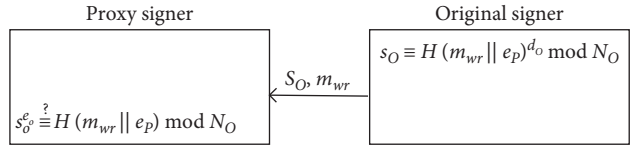


Figure 1: Proxy phase.

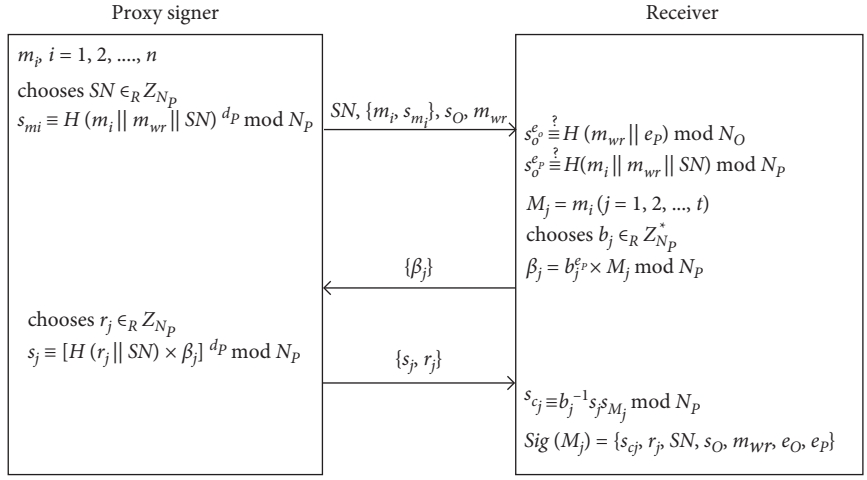


Figure 2: Signing phase.

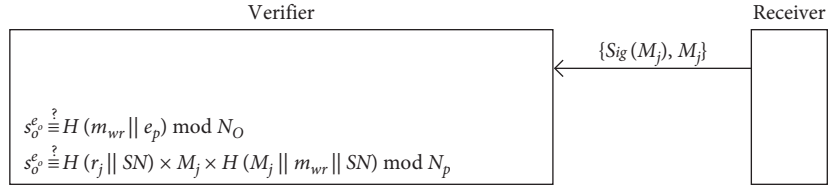


Figure 3: Verification phase.

by a legitimate signer, and this plaintext was in fact selected by R, as follows:

(1) R sends $\mathrm{Sig}(M_j)$ and M_j to V.

(2) V verifies $s_O^{e_O ?} \equiv H(m_{wr} \| e_P) \bmod N_O$ and $s_{c_j}^{e_P ?} \equiv H(r_j \| SN) \times M_j \times H(M_j \| m_{wr} \| SN) \bmod N_P$. If both the equations hold, the signature is valid.

4. Proposed Fair Lottery System

4.1. Security and System Requirements of the Proposed E-Lottery System. The proposed lottery system satisfies the game fairness principle, and its security and security requirements are described as Definitions 2 and 3.

Definition 2 (security requirement of fair e-lottery system). Assume owner, banker, and player interact in the fair e-lottery system. The system is secure if it achieves the following conditions. (1) Verifiability: After the lottery, player can verify the prize content announced by banker, thus protecting his own interests. Once the winning card is redeemed, anyone can verify its validity. (2) Privacy: Player's identifying information is never made available in the public lottery information, thus ensuring player's privacy. In the lottery process, player's selection must be kept secret to protect the privacy of the winning content. (3) Undeniability: After the lottery, banker is unable to repudiate the prize content or player's claim. (4) Unforgeability: Valid winning card information can only be produced through the valid protocol and cannot be forged. (5) Fairness for all players: In the lottery, no player (including owner and banker) should have an unfair advantage over other players.

Definition 3 (system requirement of our lottery system). Our lottery system is correct if it conforms the following characteristics: (1) no need for a trusted third party, (2) owner may not repudiate a legitimate lottery card, (3) the privacy of the player's selection content is protected, (4) the player is anonymous, (5) fairness for all players, and (6) multiple choices with multiple prizes.

4.2. Proposed System. The proposed lottery system design is an electronic adaptation of popular "scratch card" type lotteries. In the system, all messages are presented digitally. Hereinafter, the proposed e-lottery system is referred to as "the game" and traditional scratch cards are referred to as "(digital) lottery."

Each game session includes one lottery card and three roles: owner O, banker B, and player. O holds the money for the game and bears responsibility for profits and losses. Under the owner, there can be multiple bankers who are primarily responsible for verifying game wins or losses. B is the agent for O and serves as the host of the game, providing a link between player and O. B is responsible for issuing a lottery card with a valid signature and for signing player's selection. Player is in competition with O and makes a request to participate in the game.

B provides a lottery card containing a total of n blind prizes. Player can select t prizes. Once his selection is confirmed, player can know the content of his own selection. He can then present his card to O as proof to receive his prize. Each game session includes four phases (initialization, lottery card production, player drawing, and prize redemption) (Figures 4–7).

(1) *Initialization Phase.* As shown in Figure 4, owner O authorizes the agent to create banker B's game as follows:

(1) O calculates $s_O \equiv H(m_{wr} \| e_B)^{d_O} \bmod N_O$ and sends s_O and m_{wr} to B.

(2) B verifies $s_O^{e_O ?} \equiv H(m_{wr} \| e_B) \bmod N_O$ to check O's authorization.

(2) *Lottery Card Production Phase.* As shown in Figure 5, player requests a game from B, triggering the lottery production process as follows:

(1) B receives player's request and applies to O for a lottery card.

(2) O selects a random number $r_O \in Z_{N_O}^*$, calculates $h_k = \quad h_k = H(k \| m_k \| r_O \| e_B)$ to blind prize m_k $(k = 1, 2, \ldots, n)$, and calculates $SN \equiv r_O^{e_O} \bmod N_O$ and $s_{SN} \equiv H(SN \| h_1 \| \ldots \| h_n)^{d_O} \bmod N_O$. O then transmits the lottery card information $\{h_k\}$, SN and s_{SN} to B, and stores (r_O, h_k, k, m_k) in the database.

(3) Once B has received the lottery card, he/she verifies $s_{SN}^{e_O ?} \equiv H(SN \| h_1 \| \ldots \| h_n) \bmod N_O$ to establish the card as accepted. B then selects a random number $r_B \in Z_{N_B}$, extracts current time t_B, and calculates $\{p_i\} = \{H(h_k \| r_B \| t_B)\}$ and $s_{p_i} \equiv H(p_i \| m_{wr} \| \ SN)^{d_B} \bmod N_B$.

(3) *Player Drawing Phase.* As shown in Figure 6, player selects t p_i unseen by B and obtains B's valid signature for p_i as follows:

(1) B transmits SN, $\{p_i, s_{pi}\}$, s_O, and m_{wr} to player.

(2) Player verifies $s_O^{e_O ?} \equiv H(m_{wr} \| e_B) \bmod N_O$ and $s_{p_i}^{e_B ?} \equiv H(p_i \| m_{wr} \| SN) \bmod N_B$ to check whether p_i is a valid selection. Player selects t options $M_j = p_i$ and $j = 1, 2, \ldots, t$, selects a random number $b_j \in Z_{N_B}^*$ as the blinding factor, calculates $\beta_j \equiv b_j^{e_B} \times M_j \bmod N_B$, and sends β_j to B.

(3) B selects a random number $r_j \in Z_{N_B}$, calculates $s_j \equiv [H(r_j \| SN) \times \beta_j]^{d_B} \bmod N_B$, and sends $\{s_j, r_j\}$, r_B, t_B to player.

(4) Player calculates $s_{c_j} \equiv b_j^{-1} s_j s_{M_j} \bmod N_B$ and obtains the valid signature value for M_j: $\mathrm{Sig}(M_j) = \{s_{c_j}, r_j, SN, s_O, m_{wr}, e_O, e_B\}$.

(4) *Prize Redemption Phase.* As shown in Figure 7, player sends the signed content to O for verification, unlocking the prize content and obtaining the game prize as follows:

(1) Player sends $\{\mathrm{Sig}(M_j), M_j\}, r_B, t_B$ to O.

(2) O verifies $s_O^{e_O ?} \equiv H(m_{wr} \| e_B) \bmod N_O$ and $s_{c_j}^{e_B ?} \equiv H(r_j \| SN) \times M_j \times H(M_j \| m_{wr} \| SN) \bmod N_B$ to check whether the lottery card is valid. O calculates $r_O \equiv SN^{d_O} \bmod N_O$ and checks whether the value r_O exists in the database. If it does, (r_O, M_j, r_B, t_B) is used to find h_k from $M_j = p_j = H(h_k \| r_B \| t_B)$ and resolve k_j and m_{k_j} and then M_j data k_j, m_{k_j}, r_O are announced to player. Finally, the item about (r_O, h_k, k_j, m_{k_j}) is marked as "completed" in the database.

(3) Player verifies $M_j \stackrel{?}{=} H(H(k_j \| m_{k_j} \| r_O \| e_B) \| r_B \| t_B)$ to confirm and collect the prize content m_{k_j}.

5. Comparison and Security Analysis

5.1. Performance Comparison of the Proposed Signature Protocol. This section provides a comparison between the proposed signature protocol and the methods proposed by Yang et al. [19], Chen [8], Tso et al. [9], Chiou et al. [38], and Chiou and Chen [39], where Yang et al.'s [19] scheme is a blind signature scheme, Chiou and Chen's [39] scheme is a t-n (t-out-of-n) OT scheme, and the others are 1-n (one-out-of-n) OT schemes.

In Table 1, T_{ex} indicates modular exponentiation operation time unit, which is the most significant computational operation while the other operations in the schemes are ignored. The results in Table 1 show that the proposed method outperforms other protocol in terms of computational analysis.

Table 2 shows that the proposed method provides improvement or similar performance in terms of communication cost, where $q|p-1$ and $(l_N, l_p, l_q, l_m, l_H)$ indicates the length of N, p, q, a message, and a hash function.

Table 3 shows that the proposed method provides more features than other protocols. Therefore, compared with other related schemes, our scheme provides the most abilities with low computation cost. Furthermore, the communication cost is no higher than that of other oblivious signature schemes.

5.2. Functional Comparison of Lottery System. This section compares the proposed online lottery system with systems proposed by Zhao [32], Kushilevitz [33], and Blundo [34] in terms of the system requirements in Definition 2, and the results are summarized in Table 4. From Table 4, only our proposed lottery scheme provides "fairness for all players"

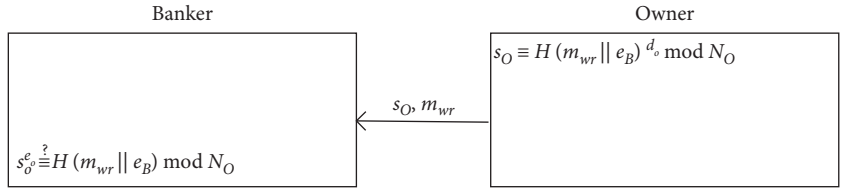


Figure 4: System initialization phase.

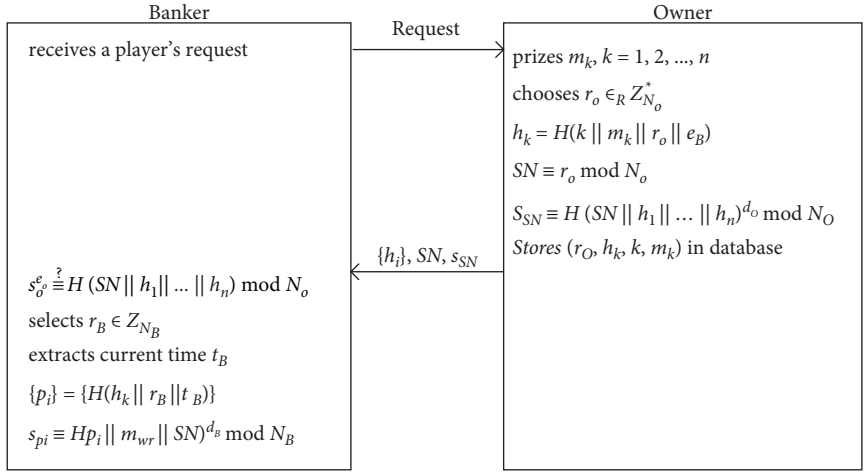


Figure 5: Lottery card production phase.

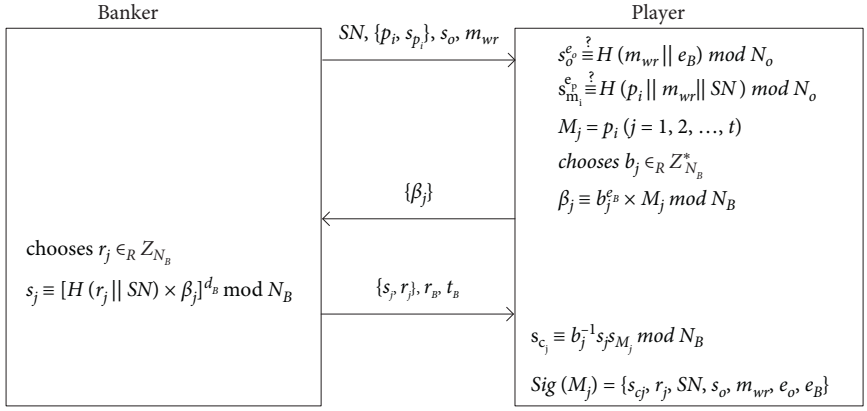


Figure 6: Player drawing phase.

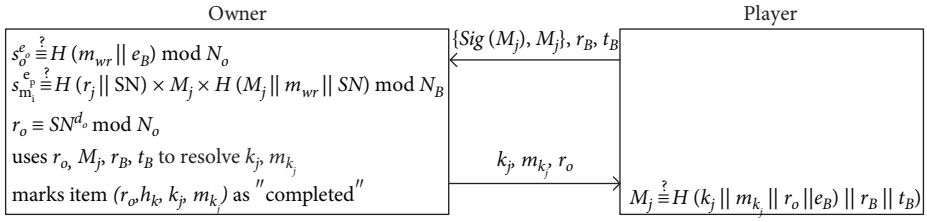


Figure 7: Prize redemption phase.

Table 1: Computation cost comparison.

Scheme	Original signer	(Proxy) signer	Receiver	Verifier
Yang (blind) [19]	T_{ex}	$4T_{ex}$	$2T_{ex}$	$3T_{ex}$
Chen (1-n) [8]	—	$3nT_{ex}$	$(2n+10)T_{ex}$	$8T_{ex}$
Tso (1-n) [9]	—	$2nT_{ex}$	$(2n+2)T_{ex}$	$2T_{ex}$
Chiou (1-n) [38]	$2T_{ex}$	$(n+2)T_{ex}$	$(2n+2)T_{ex}$	$2T_{ex}$
Chiou (1-n) [39]	—	$(n+1)T_{ex}$	$2nT_{ex}$	$2T_{ex}$
Chiou (t-n) [39]	—	$(n+t)T_{ex}$	$2nT_{ex}$	$2tT_{ex}$
Proposed (1-n)	T_{ex}	$(n+2)T_{ex}$	$(n+2)T_{ex}$	$2T_{ex}$
Proposed (t-n)	T_{ex}	$(n+t+1)T_{ex}$	$(n+t+1)T_{ex}$	$(t+1)T_{ex}$

Table 2: Communication cost comparison.

Scheme	OS $\longrightarrow$ PS	PS $\longrightarrow$ R	$R \longrightarrow$ PS	$R \longrightarrow V$
Yang (blind) [19]	$l_q + l_H$	$l_p + l_q + l_H$	l_q	$l_q + 2l_H$
Chen (1-n) [8]	—	$3nl_p + nl_q$	l_q	$7l_p + l_q + l_H$
Tso (1-n) [9]	—	$n(l_q + l_H)$	l_p	$l_q + l_H$
Chiou (1-n) [38]	$l_p + l_q$	$n(l_q + l_H)$	l_p	$l_q + l_H$
Chiou (1-n) [39]	—	$(2n+1)l_N + nl_m$	l_N	$l\,l_N + l_m + l_H$
Chiou (t-n) [39]	—	$(2n+t)l_N + nl_m$	tl_N	$t(l_N + l_m + l_H)$
Proposed (1-n)	$l_N + l_m$	$(n+4)l_N + (n+1)l_m$	l_N	$4l_N + 2l_m + 2l_q$
Proposed (t-n)	$l_N + l_m$	$(n+2t+2)l_N + (n+1)l_m$	tl_N	$4tl_N + 2tl_m + 2tl_q$

Table 3: Ability comparison.

Scheme	Blindness	Ambiguity	Multichoice	Proxy ability
Chen [8]	✓	✓		
Mambo [13]				✓
Tso [9]	✓	✓		
Yang [19]	✓			✓
Chiou [38]	✓	✓		✓
Chiou [39]	✓	✓	✓	
Proposed	✓	✓	✓	✓

Table 4: System feature comparison.

Scheme	[A]	[B]	[C]	[D]	[E]	[F]
Zhao [32]		✓	✓	✓		
Kushilevitz [33]	✓	✓	✓			
Blundo [34]	✓	✓	✓	✓		
Proposed	✓	✓	✓	✓	✓	✓

[A]: no need for a trusted third party (TTP); [B]: owner may not repudiate a legitimate lottery card; [C]: the privacy of the player's selection content is protected; [D]:the player is anonymous; [E]: fairness for all players; [F]: multiple choices with multiple prizes.

and "multiple choices with multiple prizes." Zhao et al.'s method [32] requires a TTP to achieve fair online gambling, and Kushilevitz and Rabin's e-lottery and e-casino schemes [33] do not provide an anonymous-player function.

5.3. Security Analysis of the Proposed Signature Protocol. This proposed signature protocol provides eight security requirements defined in Definition 1.

(1) *Completeness*. From the signature initialization phase to the final verification phase, R can finally use the verification formula $s_O^{e_O?} \equiv H(m_{wr} \| e_P) \bmod N_O$ and $s_{c_j}^{e_P?} \equiv H(r_j \| SN) \times M_j \times H(M_j \| m_{wr} \| SN) \bmod N_P$ to determine whether P and O are valid signers in the protocol and can also use the verification formula to validate the signatures, thus ensuring the protocol's integrity. Theorems 1 and 2 prove the property of completeness from Definitions 4 and 5.

(2) *Distinguishability*. It is provided from $\mathrm{Sig}(M_j) = \{s_{c_j}, r_j, SN, s_O, m_{wr}, e_O, e_P\}$, where the authorization validation m_{wr} shows the proxy relationship between O and P, thus anyone can determine that the signature on this message is a proxy signature. Theorem 3 proves the property of distinguishability from Definition 6.

(3) *Identifiability*. The verification equations in the verification phase $s_O^{e_O?} \equiv H(m_{wr} \| e_P) \bmod N_O$ and $s_{c_j}^{e_P?} \equiv H(r_j \| SN) \times M_j \times H(M_j \| m_{wr} \| SN) \bmod N_P$ require the use of a valid signer's public key to conduct the necessary calculations for a successful verification, thus V can use the verification public keys e_P and e_O to determine the identity of the document signer. Theorem 4 proves the property of identifiability from Definition 7.

(4) *Verifiability*. Using public keys (e_P, N_P) and (e_O, N_O) can verify $s_O^{e_O?} \equiv H(m_{wr} \| e_P) \bmod N_O$ and $s_{c_j}^{e_P?} \equiv H(r_j \| SN) \times M_j \times H(M_j \| m_{wr} \| SN) \bmod N_P$ via the signature $\mathrm{Sig}(M_j) = \{s_{c_j}, r_j, SN, s_O, m_{wr}, e_O, e_P\}$. Moreover, the ownership of public keys can be verified using the public key of root CA from a PKI system. Theorem 5 proves the property of verifiability.

(5) *Ambiguity*. In the signing phase, R selects t blind factors b_j and calculates $\beta_j \equiv b_j^{e_P} \times M_j \bmod N_P$, thus

P is unable to determine the content of the signed message. Then, R sends s_j back to P, and P calculates $b_j^{-1}s_j s_{M_j}$ to obtain the valid signature for M_j, thus ensuring the privacy of R. This method implies another security feature in which each of the t signatures M_j can be independently verified. This means that, according to the requirements of the situation, R only wants to provide a proof of signature and does not require open verification of t signatures, thus the privacy of R's other selections. Theorem 6 proves the property of ambiguity from Definition 8.

(6) *Nonrepudiation*. During signing, this protocol requires the use of P and O's private keys along with a hash function. Given that others do not have access to these private keys, they are unable to create a signature which would pass verification. Likewise, a verifiable signature must have the public key's master signature at the time of verification, which the signer is unable to repudiate. Theorem 7 proves the property of nonrepudiation.

(7) *Unforgeability*. We analyze warrant and message unforgeability, and Theorem 8 proves the property of unforgeability.

(8) *Prevention of Misuse*. The signature of m_{wr} is verified, and m_{wr} is used to verify the authentication to clearly document the proxy signer's signing capability, time, and usage conditions. The authorization certificate cannot be forged, thus the proxy signer is unable to use its proxy signature for unauthorized purposes, thus preventing misuse of the proposed protocol. Theorem 9 proves the property of prevention of misuse.

5.4. Security Analysis of Proposed Lottery System. In practice, each banker hosts one or multiple servers. Assuming that multiple bankers represent a single owner, then multiple servers jointly use a single private key. For the overall system, this is equivalent to putting all of one's eggs in a single basket, and thus the security of the overall system relies on a single key. On the other hand, using a proxy system can significantly reduce the potential risk to system security even if the banker's key or even the owner's key is stolen. This additional layer of protection greatly increases overall system security.

If the prize redemption involves actual money, it could be realized through anonymous and secure mechanisms which are commonly applied in online transactions [57–60]. A user can register with a third party middleman (such as Paypal, Google Checkout, or Amazon Payment), providing required information, such as bank accounts and redemption certificates. The middleman presents the owner with a cash request based on these redemption certificates. Once the middleman receives the required payout and delivers a corresponding receipt to the owner, the middleman then transfers the money to the player's bank account. Thus, the identity of the prize winner is not revealed to the owner (thus achieving privacy). Moreover, this approach eliminates the possibility of the owner refusing to deliver the claimed prize.

To meet the game's fairness principle, this system satisfies the five security requirements as defined in Section 5.1: verifiability, privacy, undeniability, unforgeability, and fairness for all players.

(1) *Verifiability*. In the prize redemption phase, player uses the verification equation $M_j \stackrel{?}{=} H[H(k_j \| m_{k_j} \| r_O \| e_B) \| r_B \| t_B]$ to inspect the prize content. When redeeming prizes, anyone can substitute O and B's public key into the verification equations $s_O^{e_O ?} \equiv H(m_{wr} \| e_B) \bmod N_O$ and $s_{c_j}^{e_B ?} \equiv H(r_j \| SN) \times M_j \times H(M_j \| m_{wr} \| SN) \bmod N_B$ to inspect the card validity. Theorem 10 proves the property of verifiability.

(2) *Privacy*. Each lottery session does not require the use of player's identifying information, thus the public lottery card information will not leak the player's identity. In the lottery process, player's selection uses the random number b_j plus blinding and thus B is unaware of the selection, ensuring the privacy of the prize content. Theorem 11 proves the property of privacy.

(3) *Undeniability*. Prizes are awarded through a one-way hash function algorithm. When the prizes are awarded, O is unable to change the prize content or otherwise deceives player. Player's selection is verified using O and B's public key, and thus O is unable to repudiate the lottery card's validity. Theorem 12 proves the property of undeniability.

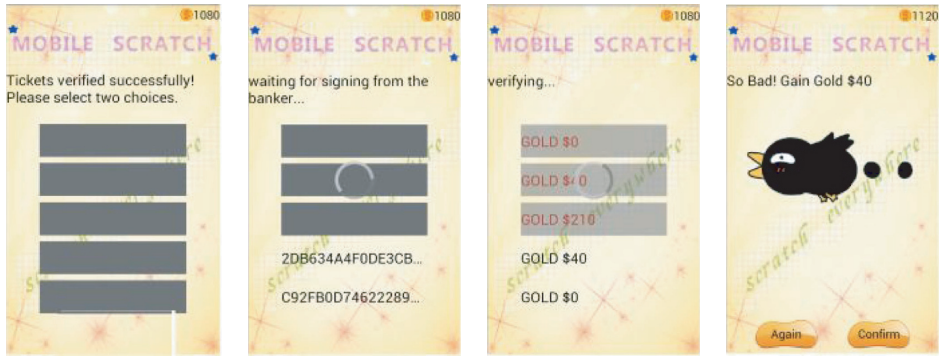
(4) *Unforgeability*. Player's prize must be legitimately signed using B's private key. Following the signing phase, it will be impossible to forge another valid winning lottery card. Theorem 13 proves the property of unforgeability.

(5) *Fairness for All Players*. At the outset, O uses a one-way hash function to blind the selected prize. Aside from O, no other parties know the prize content. Then, B double blinds the prize item, at which time no one including O and B is able to determine which card has the prize. Theorem 14 proves the property of fairness for all players.

6. Implementation

This section presents an implementation of the proposed e-lottery system on an Android platform, allowing the user to interact with the system through a mobile device to achieve a scratch game e-lottery. The implementation results are presented in two parts. First, we introduce the program flow chart and then show the user experience through the interface.

The program's related user interface is illustrated in Figure 8. The owner and banker roles operate on the server end, while the player role operates on the client-end mobile device, as shown in Figure 9. (please refer to http://youtu.be/9je3gtThnTY for the full demonstration.).



(a) (b) (c) (d)

Figure 8: (a) Player receives the successful lottery card verification from cloud banker; (b) after choosing an option, player waits for banker's signature; (c) player verifies the prize; (d) following the successful verification, the game is concluded.

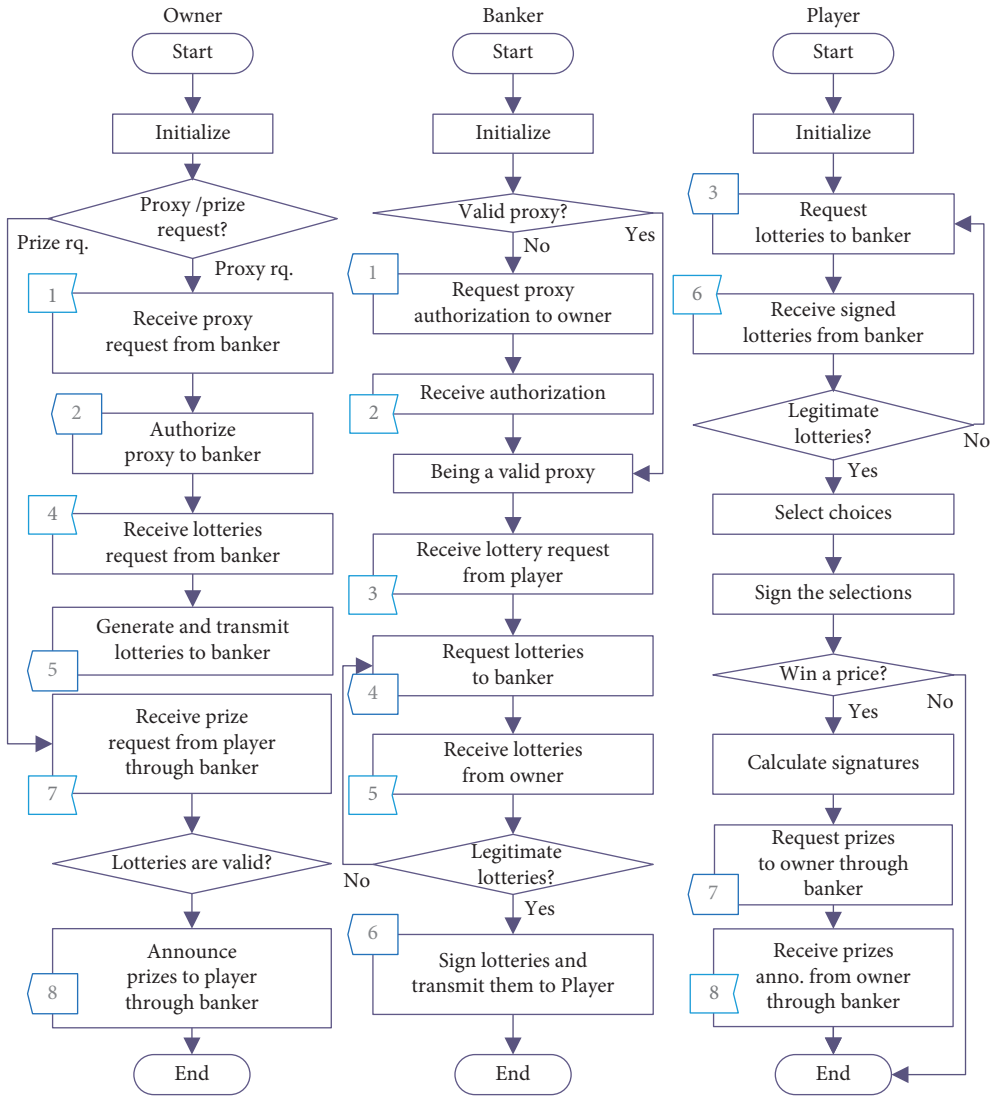


Figure 9: Application flow chart.

Table 5: Implementation time.

Phases	Banker	Owner	Player	Trans.	Time
Lottery card prod. phase	79.85	79.85	—	38.65	198.35
Player drawing phase	39.35	—	97.6	401.6	538.55
Prize redemption phase	—	39.6	21.15	261.55	322.3

Time unit: millisecond (ms).

Table 6: Ranking of user studies.

Item	Trust before expl.	Convenience	Willing to play	Trust after expl.
Average	5.67	7.79	5.36	6.83
Variable	5.47	3.70	6.13	5.17
≥5	73.74%	94.95%	70.71%	85.86%
≥6	54.55%	84.85%	52.53%	79.80%

We use one personal computer and one android phones to implement two servers (banker and owner) and a player, where the player communicates to each other through WiFi wireless networks and the owner and the banker communicate to each other through wired networks. The personal computer implementation used Windows 10 with an Intel (R) Xeon (R) CPU E3-1230 v3 @ 3.30 GHz (8 CPUs) and 8G RAM. Android phone implementation used HTC Desire 816 based on Android 5.0 and Qualcomm S400 1.6 G Hz.

The owner and banker (server) programs are written in JAVA and run under Windows 10. The RSA system parameters are generated through an official method with a module length of 1024 bits. The hash function used is SHA-256 [61]. In this scenario, we set $t = 2$ and $n = 5$. Each time the program needs only 1~3 seconds to finish all the processes (from initialization to prize redemption) excluding the user's operating time. Table 5 shows the average implementation time in each phase.

Table 6 shows the ranking result of user studies for 99 college students. The ranking score is from 1 (the lowest) to 10 (the highest), the ranking items include (1) trust before explanation, (2) convenience, (3) willing to play, and (4) trust after explanation, and the statistical information includes (1) average, (2) variable, (3) "≥5" (scores equal to or great than 5), and (4) "≥6."

In the first phase, we let users play the mobile lottery and rank the scores of the first three items (i.e., trust before explanation, convenience, and willing to play). In the second phase, we let users rank the final item (i.e., trust after explanation) after the one-minute explanation of the security design on our mobile lottery scheme. Normally, a "sense of security" is remarkably increased after a slight explanation. Most users think the mobile lottery is convenient, and more than half persons are willing to play the game again.

7. Conclusion

This paper proposes a generalized t-out-of-n oblivious signature scheme with proxy function. A new mobile lottery system is then proposed based on the proposed signature protocol with the aim of providing a more complete fairness and more convenient security. Compared with other schemes, only our system provides the system property: fairness for all players and multiple choices with multiple prizes. Moreover, most signature schemes do not supply both multichoice and proxy ability while preserving the security properties (along with security proves via a formal security proving model), including blindness and ambiguity. The proposed system is implemented on in Android smart phone, providing greater convenience for the user as compared with traditional game counter mechanisms. Based on the above analysis, the proposed signature protocol can also be used in applications outside lottery systems. Our future work will focus in this area, along with making further improvements to increase efficiency and security.

Appendix

The appendix provides 14 theorems along with definitions and proofs security analysis of the proposed signature protocol and e-lottery system using a formal proof method [40].

A. Security Proofs of the Proposed Signature Protocol

A.1. Completeness

Definition 4 (1st modified RSA signature forgery problem). Let (e, N) be the public key of a RSA cryptosystem, $a, b, b' \in Z, s^e = H(b \| a) \bmod N$, and $s'^e = H(b' \| a) \bmod N$. If (s', b') can be evaluated from given (a, s, b), then we say the 1st modified RSA signature forgery problem is solved (the probability of solving this problem is denoted as $\Pr(s', b' | a, s, b) = \varepsilon_1$).

Theorem 1 (warrant completeness). *In our scheme, if an adversary can modify (s_O, m_{wr}) to a valid (s'_O, m'_{wr}), then the 1st modified RSA signature forgery problem can be solved.*

Proof. In our scheme, assume an adversary tries to calculate (s'_O, m'_{wr}) from eavesdropped (s_O, m_{wr}, e_p), where $s_O^{e_O} = H(m_{wr} \| e_p) \bmod N_O$ and $s'^{e_O}_O = H(m'_{wr} \| e_p) \bmod N_O$. Let RO_1 be a random oracle: input s_O, m_{wr}, and e_p to output

s'_O and $m_{wr}{}'$ (i.e., $RO_1(m_{wr}, e_p, s_O) \longrightarrow (s'_O, m_{wr}{}')$). In Definition 4, let $e_p \leftarrow a$, $m_{wr} \leftarrow b$, and $s_O \leftarrow s$ be input parameters of RO_1 and obtain output s'_O and m'_{wr}. Let $s' \leftarrow s'_O$ and $b' \leftarrow m'_{wr}$, then (s', b') are evaluated. Therefore, $\Pr(s'_O, m'_{wr} | e_p, s_O, m_{wr}) \leq \Pr(s', b' | a, s, b) = \varepsilon_1$, which means the 1st modified RSA signature forgery problem can be solved if RO_1 exists.

Definition 5 (2nd modified RSA signature forgery problem). Let (e, N) be the public key of a RSA cryptosystem, $a, b, b' \in Z$, $a, b, b' \in Z$, $s^e \equiv H(r_1 \| r_2) \cdot m_1 \cdot H(m_1 \| m_2 \| r_2) \bmod N$, and $s'^e \equiv H(r'_1 \| r'_2) \cdot m'_1 \cdot H(m'_1 \| m_2 \| r'_2) \bmod N$. If (s', m'_1, r'_1, r'_2) can be evaluated from given (s, m_1, r_1, r_2, m_2), then we say the 2nd modified RSA signature forgery problem is solved (the probability of solving this problem is denoted as $\Pr(s', m'_1, r'_1, r'_2 | s, m_1, r_1, r_2, m_2) = \varepsilon_2$).

Theorem 2 (message completeness). *In our scheme, if an adversary can modify (s_c, M_j, r_j, SN) to valid (s'_c, M'_j, r'_j, SN') from given m_{wr}, then the 2nd modified RSA signature forgery problem can be solved.*

Proof. In our scheme, assume an adversary tries to calculate (s'_c, M'_j, r'_j, SN') from $(s_c, M_j, r_j, SN, m_{wr})$, such that $s_c^{'e_P} \equiv H(r'_j \| SN') \times M'_j \times H(M'_j \| m_{wr} \| SN') \bmod N_P$. Let RO_2 be a random oracle: input $(s_c, M_j, r_j, SN, m_{wr})$ to output (s'_c, M'_j, r'_j, SN'). In Definition 5, let $(s, m_1, r_1, r_2, m_2) \leftarrow (s_c, M_j, r_j, SN, m_{wr})$ be input parameters of RO_2 and obtain output (s', m'_1, r'_1, r'). Let $(s'_c, M'_j, r'_j, SN') \leftarrow (s', m'_1, r'_1, r')$, then (s'_c, M'_j, r'_j, SN') are evaluated. Therefore, $\Pr(s'_c, M'_j, r'_j, SN' | s_c, M_j, r_j, SN, m_{wr}) \leq \Pr(s', |m'_1, r'_1, r'_2 | s, m_1, r_1, r_2, m_2) = \varepsilon_2$, which means the 2nd modified RSA signature forgery problem can be solved if RO_2 exists.

A.2. Distinguishability

Definition 6 (RSA signature forgery problem). Let (e, N) be the public key of a RSA cryptosystem, $a, b, a', b' \in Z$, $s^e = H(b \| a) \bmod N$, and $s'^e = H(b' \| a') \bmod N$. If (s', b', a') can be evaluated from given (s, b, a, e, N), then we say the RSA signature forgery problem is solved (the probability of solving this problem is denoted as $\Pr(s', b', a' | s, b, a) = \varepsilon_3$).

Theorem 3 (Distinguishability). *In our scheme, if an adversary can counterfeit a valid (s'_O, m'_{wr}, e'_P) from $(s_O, m_{wr}, e_P, e_O, N_O)$, then the RSA signature forgery problem can be solved.*

Proof. In our scheme, assume an adversary tries to calculate (s'_O, m'_{wr}, e'_P) from $(s_O, m_{wr}, e_P, e_O, N_O)$, where $s_O^{e_O} = H(m_{wr} \| e_p) \bmod N_O$ and $s_O^{'e_O} = H(m'_{wr} \| e'_P) \bmod N_O$. Let RO_3 be a random oracle: input $(s_O, m_{wr}, e_P, e_O, N_O)$ to output (s'_O, m'_{wr}, e'_P). In Definition 6, let $(s_O, m_{wr}, e_P, e_O, N_O) \leftarrow (s, b, a, e, N)$ be input parameters of RO_3 and obtain output (s'_O, m'_{wr}, e'_P). Let $(s', b', a') \leftarrow (s'_O, m'_{wr}, e'_P)$, then (s', b', a') are evaluated. Therefore, $\Pr(s'_O, m'_{wr}, e'_P | s_O, m_{wr}, e_P, e_O, N_O) \leq \Pr(s', b', a' | s, b, a) = \varepsilon_3$, which means the RSA signature forgery problem can be solved if RO_3 exists. □

A.3. Identifiability

Definition 7 (2nd RSA signature forgery problem). Let (e, N) be the public key of a RSA cryptosystem, $m, m' \in Z$, $s^e = H(m) \bmod N$, and $s'^e = H(m') \bmod N$. If (s', m') can be evaluated from given (s, m, e, N), then we say the 2nd RSA signature forgery problem is solved (the probability of solving this problem is denoted as $\Pr(s', m' | s, m, e, N) = \varepsilon_4$).

Theorem 4 (identifiability). *Given (e_{Root}, N_{Root}). In our scheme, if an adversary can counterfeit valid (s'_{e_O}, e'_O) from (s_{e_O}, e_O) or counterfeit valid (s'_{e_p}, e'_P) from (s_{e_p}, e_P), such that $s_i^e = H(e_i) \bmod N$, where $(s_i, e_i) = (s_{e_O}, e_O)$, (s_{e_p}, e_P), (s'_{e_O}, e'_O), or (s'_{e_p}, e'_P), then the 2nd RSA signature forgery problem can be solved.*

Proof. In a PKI system, a signature s_i on a public key e_i is signed by root such that $s_i^{e_{\text{root}}} = H(e_i) \bmod N_{\text{root}}$, where $(e_{\text{Root}}, N_{\text{Root}})$ are root public keys. Assume an adversary tries to counterfeit (s'_{e_O}, e'_O) from (s_{e_O}, e_O) or counterfeit (s'_{e_p}, e'_P) from (s_{e_p}, e_P). Let RO_4 be a random oracle: input (s_{e_O}, e_O) to output (s'_{e_O}, e'_O). In Definition 7, let $(s, m, e, N) \leftarrow (s_{e_O}, e_O, e_{\text{Root}}, N_{\text{Root}})$ be input parameters of RO_4 and obtain output (s', m'). Let $(s'_{e_O}, e'_O) \leftarrow (s', m')$, then (s'_{e_O}, e'_O) are evaluated. Therefore, $\Pr(s'_{e_O}, e'_O | s_{e_O}, e_O, e_{\text{Root}}, N_{\text{Root}}) \leq \Pr(s', m' | s, m, e, N) = \varepsilon_4$, which means the 2nd RSA signature forgery problem can be solved if RO_4 exists. □

A.4. Verifiability

Theorem 5 (verifiability). *In our scheme, if an adversary can forge valid signatures $(s'_O, m_{wr}{}')$ and (s'_c, M'_j, r'_j, SN') from (s_O, m_{wr}) and $(s_c, M_j, r_j, SN, m_{wr})$ and pass the verification equations using public keys (e_P, N_P, e_O, N_O), then both the 1st and 2nd modified RSA signature forgery problems can be solved.*

Proof. The proofs are the same as the content of the proof of Theorem 1 plus the proof of Theorem 2.

A.5. Ambiguity

Definition 8 (entropy problem). Let (e, N) be the public key of a RSA cryptosystem, $a, b \in Z$, and $\alpha = b^e \times m \bmod N$. If m can be evaluated from given (α, e, N) without given b, then we say the entropy problem is solved. The probability of solving this problem is denoted as $\Pr(m | \alpha, e, N) = \varepsilon_5$.

Theorem 6 (ambiguity). *In our scheme, if the proxy signer or an adversary can calculate M_j from (β_j, e_P, N_P), then the entropy problem can be solved.*

Proof. In our scheme, assume the proxy signer or an adversary tries to calculate M_j from (β_j, e_P, N_P) where $\beta_j = b^{e_P} \times M_j \bmod N_P$. Let RO_5 be a random oracle: input (β_j, e_P, N_P) to output M_j. In Definition 8, let (β_j, e_P, N_P), $\leftarrow$, (α, e, N) be input parameters of RO_5 and obtain output M_j. Let m, $\leftarrow$, M_j, then m is evaluated. Therefore, $\Pr(M_j|\beta_j, e_P, N_P) \le \Pr(m|\alpha, e, N) = \varepsilon_5$, which means the entropy problem can be solved if RO_5 exists.

A.6. Nonrepudiation

Theorem 7 (nonrepudiation). *In our scheme, if an adversary can calculate a valid signature (s'_O, m'_{wr}) from $(s_O, m_{wr}, e_O, e_P, N_O)$ without given d_O, then the 1st modified RSA signature forgery problem can be solved. If an adversary can calculate a valid signature (s'_c, M'_j, r'_j, SN') from $(s_c, M_j, r_j, SN, e_P, N_P)$ without given d_P, then the 2nd modified RSA signature forgery problem can be solved.*

Proof. The proof is the same as the content of the proof of Theorem 1 plus the proof of Theorem 2.

A.7. Unforgeability

Theorem 8 (unforgeability). *In our scheme, if an adversary can evaluate a forged warrant signature (s'_O, m'_{wr}) from $(s_O, m_{wr}, e_O, e_P, N_O)$, then the 1st modified RSA signature forgery problem can be solved. If an adversary can evaluate a forged message signature (s'_c, M'_j, r'_j, SN') from $(s_c, M_j, r_j, SN, e_P, N_P)$, then the 2nd modified RSA signature forgery problem can be solved.*

Proof. The proof is the same as the content of the proof of Theorem 1 plus the proof of Theorem 2.

A.8. Prevention of Misuse

Theorem 9 (prevention of misuse). *In our scheme, if an adversary can calculate valid signature (s'_O, m'_{wr}) from $(s_O, m_{wr}, e_O, e_P, N_O)$ without given d_O, then the 1st modified RSA signature forgery problem can be solved. If an adversary can calculate valid signature (s'_c, M_j, r'_j, SN') from $(s_c, M_j, r_j, SN, e_P, N_P)$ without given d_P, then the 2nd modified RSA signature forgery problem can be solved.*

Proof. The proof is the same as the content of the proof of Theorem 2.

B. Security Proofs of the Proposed Lottery System

B.1. Verifiability

Theorem 10 (verifiability). *In our scheme, if an adversary can forge valid (s'_O, m'_{wr}) and (s'_c, M'_j, r'_j, SN') from (s'_O, m'_{wr}) and (s_{c_j}, M_j, r_j, SN), then both the 1st and 2nd modified RSA signature forgery problems can be solved. If an adversary can counterfeit valid $(k'_j, m_{k_j}{}', r'_O, e'_B, t'_B, r'_B)$ from $(k_j, m_{k_j}, r_O, e_B, t_B, r_B)$, then both the 2nd RSA signature forgery problem and the hash problems can be solved.*

Proof. (1) The proofs about (s'_O, m'_{wr}) and (s'_c, M'_j, r'_j, SN') forgery are the same as the content of the proof of Theorem 1 plus the proof of Theorem 2. (2) About $(k'_j, m'_{k_j}, r'_O, e'_B, t'_B, r'_B)$ counterfeit, the proof for uncounterfeiting e'_O is the same as the content of the proof of Theorem 4. (3) The value t'_B is the banker's current time and cannot be forged because it can be verified by the play's current time. (4) The value r'_O cannot be forged because it can be verified via $SN^? \equiv r_O'^{e_O} \bmod N_O$ and counterfeiting a r'_O faces to a RSA signature forgery problem. (4) Forging (k'_j, m'_{k_j}) directly faces hash problem because player verifies $M_j \stackrel{?}{=} H(H(k_j \| m_{k_j} \| r_O \| e_B) \| r_B \| t_B)$ to confirm (k'_j, m'_{k_j}).

B.2. Privacy

Theorem 11 (privacy). *In our scheme, if the banker or an adversary can calculate M_j from (β_j, e_B, N_B), then the entropy problem can be solved.*

Proof. The proof is similar to the content of the proof of Theorem 6.

B.3. Undeniability

Theorem 12 (undeniability). *In our scheme, if an adversary can calculate a valid signature (s'_O, m'_{wr}) from $(s_O, m_{wr}, e_O, e_B, N_O)$ without given d_O, then the 1st modified RSA signature forgery problem can be solved. If an adversary can calculate a valid signature (s'_c, M'_j, r'_j, SN') from $(s_{c_j}, M_j, r_j, SN, e_B, N_B)$ without given d_B, then the 2nd modified RSA signature forgery problem can be solved.*

Proof. The proof is similar to the content of the proof of Theorem 7.

B.4. Unforgeability

Theorem 13 (unforgeability). *In our scheme, if an adversary can evaluate a forged warrant signature (s'_O, m'_{wr}) from $(s_O, m_{wr}, e_O, e_B, N_O)$, then the 1st modified RSA signature forgery problem can be solved. If an adversary can evaluate a forged message signature (s'_c, M'_j, r'_j, SN') from $(s_{c_j}, M_j, r_j, SN, e_B, N_B)$, then the 2nd modified RSA signature forgery problem can be solved.*

Proof. The proof is similar to the content of the proof of Theorem 8.

B.5. Fairness for All Players

Theorem 14 (fairness for all players). *In our scheme, if any of players, bankers, or the owner can calculate m_k in player drawing phase, then the RSA decryption problem or entropy problem can be solved.*

Proof. In our scheme, assume a banker tries to calculate m_k from (h_k, e_B, SN, e_O, N_O), where $h_k = H(k \| m_k \| r_O \| e_B)$ and $SN \equiv r_O^{e_O} \bmod N_O$. It faces RSA decryption problem. If the owner tries to get the connection between h_k and p_i from $\{p_i\}$ and $\{h_k\}$ without known (r_B, t_B), where $p_i \equiv H(h_k || r_B || t_B)$, it faces entropy problem. If a player tries to calculate m_k from p_i without known (r_B, t_B), it also faces entropy problem.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was partially supported by the Ministry of Science and Technology under grant MOST 109-2221-E-182-020 and by the CGMH project under grant BMRPB46.

References

[1] M. Shuai, B. Liu, N. Yu, L. Xiong, and C. Wang, "Efficient and privacy-preserving authentication scheme for wireless body area networks," *Journal of Information Security and Applications*, vol. 52, Article ID 102499, 2020.

[2] M. Kaur and D. Singh, "Multiobjective evolutionary optimization techniques based hyperchaotic map and their applications in image encryption," *Multidimensional Systems and Signal Processing*, vol. 32, no. 1, pp. 281–301, 2021.

[3] M. Kaur, D. Singh, and V. Kumar, "Color image encryption using minimax differential evolution-based 7D hyper-chaotic map," *Applied Physics B*, vol. 126, no. 147, pp. 1–19, 2020.

[4] R. Rabaninejad, M. A. Attari, M. R. Asaar, and M. R. Aref, "A lightweight identity-based provable data possession supporting users' identity privacy and traceability," *Journal of Information Security and Applications*, vol. 51, Article ID 102454, 2020.

[5] D. Chaum, "Blind signatures for untraceable payments," *Advances in Cryptology*, vol. 82, pp. 199–203, 1982.

[6] S. K. Nayak, B. Majhi, and S. Mohanty, "An ECDLP based untraceable blind signature scheme," in *Proceedings of the 2013 International Conference on Circuits, Power and Computing Technologies (ICCPCT)*, Kumaracoil, Nagercoil, India, March 2013.

[7] M. O. Rabin, "How to exchange secrets by oblivious transfer," Technical Report TR-81, Aiken Computation Laboratory, Harvard University, Cambridge, MA, USA, 1981.

[8] L. Chen, "Oblivious signatures," in *Proceedings of the Computer Security-ESORICS 94*, pp. 161–172, Brighton, UK, November 1994.

[9] R. Tso, T. Okamoto, and E. Okamoto, "1-out-of-*n* oblivious signatures," *Proceedings of ISPEC2008, Lectures Notes in Computer Science*, vol. 4991, pp. 45–55, 2008.

[10] J. S. Chou, "A novel *k*-out-of-*n* oblivious transfer protocol from bilinear pairing," *Advances in Multimedia*, vol. 2012, Article ID 630610, 3 pages, 2012.

[11] P. Zhang, H. Jiang, Z. Zheng, P. Hu, and Q. Xu, "A new post-quantum blind signature from lattice assumptions," *IEEE Access*, vol. 6, pp. 27251–27258, 2018.

[12] L. Wang, Y. Tian, Y. Pan, and Y. Yang, "New construction of blind signatures from braid groups," *IEEE Access*, vol. 7, pp. 36549–36557, 2019.

[13] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures: delegation of the power to sign messages," *IEICE Transaction on Fundamentals*, vol. E79-A, no. 9, pp. 1338–1354, 1996.

[14] B. T. Lau, "Proxy signature schemes," in *Proceedings of the 2006 1ST IEEE Conference on Industrial Electronics and Applications*, Singapore, March 2006.

[15] H. Wang and R. Yan, "A code-based multiple grade proxy signature scheme," in *Proceedings of the 2013 Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)*, Compiegne, France, October 2013.

[16] W. D. Lin and J. K. Jan, "A security personal learning tools using a proxy blind signature scheme," in *Proceedings of the International Conference on Chinese Language Computing*, pp. 273–277, Chicago, IL, USA, November 2000.

[17] A. Z. Tan, Z. Liu, and C. Tang, "Digital proxy blind signature schemes based on DLP and ECDLP," *MM Research Preprints*, vol. 21, no. 7, pp. 212–217, 2002.

[18] S. Lal and A. K. Awasthi, "Proxy blind signature scheme," *Journal of Information Science and Engineering*, vol. 72, 2003.

[19] F.-Y. Yang and L.-R. Liang, "A proxy partially blind signature scheme with proxy revocation," *Journal of Ambient Intelligence and Humanized Computing*, vol. 4, no. 2, pp. 255–263, 2013.

[20] S. Y. Chiou, T. J. Wang, and J. M. Chen, "Design and implementation of a mobile voting system using a novel oblivious and proxy signature," *Security and Communication Networks*, vol. 2017, Article ID 3075210, , 2017.

[21] Q. Lin, J. Li, Z. Huang, W. Chen, and J. Shen, "A short linearly homomorphic proxy signature scheme," *IEEE Access*, vol. 6, pp. 12966–12972, 2018.

[22] H. Li, Z. Han, L. Wang, and L. Pang, "Blind proxy re-signature scheme based on isomorphisms of polynomials," *IEEE Access*, vol. 6, pp. 53869–53881, 2018.

[23] R. Tso, "Two-in-one oblivious signatures," *Future Generation Computer Systems*, vol. 101, pp. 467–475, 2019.

[24] I. Ray and N. Narasimhamurthi, "An anonymous electronic voting protocol for voting over the internet," in *Proceedings of the Third International Workshop on IEEE Advanced Issues of E-Commerce and Web-Based Information Systems*, San Juan Capistrano, CA, USA, June 2001.

[25] H. Pan, E. Hou, and N. Ansari, "RE-NOTE: an e-voting scheme based on ring signature and clash attack protection," in *Proceedings of the Global Communications Conference (GLOBECOM)*, Atlanta, GA, USA, December 2013.

[26] B. Zwattendorfer, C. Hillebold, and P. Teufl, "Secure and privacy-preserving proxy voting system," in *Proceedings of the 2013 IEEE 10th International Conference on e-Business Engineering (ICEBE)*, pp. 472–477, Coventry, UK, September 2013.

[27] S. Kardaş, M. S. Kiraz, M. A. Bingöl, and F. Birinci, "Norwegian internet voting protocol revisited: ballot box and receipt generator are allowed to collude," *Security and Communication Network*, vol. 9, no. 18, pp. 5051–5063, 2016.

[28] O. Kulyk, S. Neumann, K. Marky, J. Budurushi, and M. Volkamer, "Coercion-resistant proxy voting," in

Proceedings of the 31st International Conference on ICT Systems Security and Privacy Protection (IFIP SEC 2016), pp. 3–16, Ghent, Belgium, June 2016.

[29] O. Kulyk, K. Marky, S. Neumann, and M. Volkamer, "Introducing Proxy Voting to Helios," in *Proceedings of the 2016 11th International Conference on Availability, Reliability and Security (ARES)*, pp. 98–106, Salzburg, Austria, September 2016.

[30] B. Adida, "Helios: web-based open-audit voting," *USENIX Security Symposium*, vol. 17, pp. 335–348, 2008.

[31] G. Cohensius, S. Mannor, R. Meir, E. Meirom, and A. Orda, "Voting for better outcomes," in *Proceedings of the 16th Conference on Autonomous Agents and MultiAgent Systems*, pp. 858–866, Sao Paulo, Brazil, May 2017.

[32] W. Zhao, V. Varadharajan, and Y. Mu, "Fair on-line gambling," in *Proceedings of the 16th Annual Conference Computer Security Applications, 2000, ACSAC'00*, Washington, DC, USA, December 2000.

[33] E. Kushilevitz and T. Rabin, "Fair e-lotteries and e-casinos," *Topics in Cryptology—CT-RSA 2001*, Springer, Berlin, Heidelberg, Germany, 2001.

[34] C. Blundo and S. Cimato, "A platform for secure e-gambling," in *Proceedings of the ITCC 2004, International Conference on Information Technology: Coding and Computing*, Las Vegas, NV, USA, April 2004.

[35] Y. Han and T. Okamoto, "Information and communications security," in *Proceedings of theInternational Conference on Information and Communications Security*, pp. 223-224, Beijing, China, November 1997.

[36] B. Lee, H. Kim, and K. Kim, "Strong proxy signer and its applications," in *Proceedings of the 2001 Symposium on Cryptography and Information Security (SCIS' 01)*, pp. 603–608, Oiso, Japan, January 2001.

[37] H. Gao, Z. Ma, S. Luo, and Z. Wang, "BFR-MPC: a blockchain-based fair and robust multi-party computation scheme," *IEEE Access*, vol. 7, pp. 110439–110450, 2019.

[38] S. Y. Chiou, T. J. Wang, and J. M. Chen, "Design and implementation of a mobile proxy voting system using a novel oblivious and proxy signature," *Security and Communication Networks*, vol. 2017, Article ID 3075210, 16 pages, 2017.

[39] S. Y. Chiou and J. M. Chen, "Design and implementation of a multiple-choice e-voting scheme on mobile system using novel *t*-out-of-*n* oblivious signature," *Journal of Information Science and Engineering*, vol. 34, no. 1, pp. 135–154, 2018.

[40] M. Bellare and P. Rogaway, "Random oracles are practical: a paradigm for designing efficient protocols," in *Proceedings of the 1st ACM Conference on Computer and Communications Security*, pp. 62–73, Fairfax, VA, USA, November 1993.

[41] H. Wang, "Identity-based distributed provable data possession in multicloud storage," *IEEE Transactions on Services Computing*, vol. 8, no. 2, pp. 328–340, 2015.

[42] V. Chang and M. Ramachandran, "Towards achieving data security with the cloud computing adoption framework," *IEEE Transactions on Services Computing*, vol. 9, no. 1, pp. 138–151, 2016.

[43] Y. A. Ridhawi and A. Karmouch, "Decentralized plan-free semantic-based service composition in mobile networks," *IEEE Transactions on Services Computing*, vol. 8, no. 1, pp. 17–31, 2015.

[44] B. Dong, R. Liu, and H. W. Wang, "Trust-but-verify: verifying result correctness of outsourced frequent itemset mining in data-mining-as-a-service paradigm," *IEEE Transactions on Services Computing*, vol. 9, no. 1, pp. 18–32, 2016.

[45] N. Basilico, N. Gatti, M. Monga, and S. Sicari, "Security games for node localization through verifiable multilateration," *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 1, pp. 72–85, 2014.

[46] J. Vaidya, B. Shafiq, W. Fan, D. Mehmood, and D. Lorenzi, "A random decision tree framework for privacy-preserving data mining," *IEEE Transactions on on Dependable and Secure Computing*, vol. 11, no. 5, pp. 399–411, 2014.

[47] X. Chen, I. Diakonikolas, A. Orfanou, D. Paparas, X. Sun, and M. Yannakakis, "On the complexity of optimal lottery pricing and randomized mechanisms," in *Proceedings of the 2015 IEEE 56th Annual Symposium on Foundations of Computer Science (FOCS)*, pp. 1464–1479, Berkeley, CA, USA, October 2015.

[48] J. Pak and L. Zhou, "Temporal patterns of structural deception behavior in a massively multiplayer online game," in *Proceedings of the 48th Hawaii International Conference on System Sciences (HICSS)*, pp. 131–140, Kauai, HI, USA, January 2015.

[49] E. Arslan, M. Yuksel, and M. H. Gunes, "Training network administrators in a game-like environment," *Journal of Network and Computer Applications*, vol. 53, pp. 14–23, 2015.

[50] W. Y. Liu, F. Tong, B. W. Wang, and Y. D. Wang, "A new proxy blind signature scheme with proxy revocation," *Journal of Electornics and Information Technology*, vol. 30, no. 10, pp. 2468–2471, 2008.

[51] C. P. Schnorr, "Efficient signature generation by smart cards," *Journal of Cryptology*, vol. 4, no. 3, pp. 161–174, 1991.

[52] F. Y. Yang and J. K. Jan, "A secure scheme for restrictive partially blind signatures," in *Proceedings of the Sixth International Conference on Information Integration and Web-Based Applications & Services (IIWAS 2004)*, pp. 541–548, Jakarta, Indonesia, September 2004.

[53] C. C. Lee, M. S. Hwang, and W. P. Yang, "A new blind signature based on the discrete logarithm problem for untraceability," *Applied Mathematics and Computation*, vol. 164, no. 3, pp. 837–842, 2005.

[54] S. Y. Chiou, Z. Ying, and J. Liu, "Improvement of a privacy authentication scheme based on cloud for medical environment," *Journal of Medical Systems*, vol. 40, no. 4, pp. 1–15, 2016.

[55] S. Y. Chiou, "Common friends discovery for multiple parties with friendship ownership and replay-attack resistance in mobile social networks," *Wireless Networks*, vol. 24, no. 3, pp. 1–15, 2018.

[56] B. Lee, H. Kim, and K. Kim, "Secure mobile agent using strongnon-designated proxy signature," in *Information Security and Privacy*, ACISP 2001, Lecture Notes in Computer Science, V. Varadharajan and Y. Mu (Eds.), vol. 2119, pp. 474–486, Springer, Berlin, Germany, 2001.

[57] W. Qian and C. Li, "The model of anonymous fair e-cash transactions protocol with off-line TTP," in *Proceedings of the Second International Conference on Innovative Computing, Information and Control (ICICIC'C7)*, Kumamoto, Japan, September 2007.

[58] V. V. Das, "Protocol for anonymous and secure e-cash transaction," in *Proceedings of the International Conference on Advances in Computing, Control, & Telecommunication Technologies (ACT'09)*, Bangalore, India, December 2009.

[59] D. Slamanig and S. Rass, "Anonymous but authorized transactions supporting selective traceability," in *Proceedings of the 2010 International Conference on Security and Cryptography (SECRYPT)*, Athens, Greece, July 2010.

[60] M. Zhang, "The online game secure transaction platform based on cooperation model," in *Proceedings of the 2010 International Conference on E-Product E-Service and E-Entertainment (ICEEE)*, Henan, China, November 2010.

[61] Elar: Java JS SHA-256, https://www.cnblogs.com/elaron/archive/2013/04/09/3010375.html.