Hindawi Publishing Corporation
The Scientific World Journal
Volume 2014, Article ID 139435, 14 pages
http://dx.doi.org/10.1155/2014/139435

Research Article

A Secure and Fair Joint E-Lottery Protocol

Chin-Ling Chen,[1] Yuan-Hao Liao,[1] and Woei-Jiunn Tsaur[2]

[1] *Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung 41349, Taiwan*
[2] *Department of Information Management, Da-Yeh University, Changhua 51591, Taiwan*

Correspondence should be addressed to Woei-Jiunn Tsaur; wjtsaur@mail.dyu.edu.tw

Received 23 January 2014; Accepted 3 March 2014; Published 4 May 2014

Academic Editors: M. Ivanovic and F. Yu

The attractive huge prize causes people to adore lotteries. Due to the very small probability of winning prizes, the players can enhance their probability of winning by using the method of joint purchase. In spite of many lottery schemes having been proposed, most e-lottery schemes focus on the players' privacy or computation overhead rather than support a joint purchase protocol on the Internet. In this paper, we use the multisignature and verifiable random function to construct a secure and fair joint e-lottery scheme. The players can check the lottery integrity, and the winning numbers can be verified publicly.

1. Introduction

Gambling has the property of nonpredictability and attractive prizes. Players have the chance to obtain a huge prize but of course they cannot predict who the winner will be. Hence, gambling is very fascinating for many people, and the lottery is one kind of popular gambling [1–3]. The players must select their favorite numbers and pay money to purchase lottery tickets. After the deadline of the purchasing phase, the lottery organization (LO) randomly generates the winning numbers. If no one wins the lottery, the prize money will accumulate for the next round. The attractive huge prizes are an extremely powerful factor causing people to purchase lottery tickets and the main reason remains popular among players.

In past years, many lottery schemes were proposed. In 2006, Chow et al. [4] proposed practical electronic lotteries with an offline trusted third party (TTP); their scheme can satisfy all of the identified requirements without the presence of TTP for generating the winning numbers; the result of this generation is publicly verifiable.

Next, Lee and Chang [5] proposed an electronic t-out-of-n lottery on the Internet in 2009. The scheme is based on the Chinese Remainder Theorem that allows lottery players to simultaneously select t out of n numbers in a ticket without iterative selection. The drawback of this scheme is that the computation overhead of players in purchasing lotteries is too heavy.

In the same year, Lee et al. [6] proposed noniterative privacy preservation for online lotteries. This scheme not only allows players to choose t-out-of-n numbers in lotteries without iterative selection but also preserves the privacy of players' choices. Nevertheless, the computation overhead in purchasing lotteries is still heavy for the player who accesses the Internet with mobile or wireless devices.

In an overview of the above schemes, we find that the majority of the schemes focus on the players' privacy or computation overhead but cannot support a joint purchase protocol on the Internet.

Due to the probability of winning prize being very small [7], the players can employ two strategies of purchase to enhance the probability of winning prizes as follows.

(i) The player invites other players to collect more cash, and then the player purchases the sequential numbers to increase the probability of obtaining a prize.

(ii) The player pays a small amount of money to purchase the lotteries in cooperation with other players.

To the best of our knowledge, there exist only two websites, called "e-Lottery Syndicates" [8] and "Myleto" [9], which provide a trading platform (TP) for purchases and a proxy purchase service. The difference between the above websites is that the former provides individual purchases while the latter provides joint purchases. Since our scheme

focuses on joint purchases, we chose "Myleto" to discuss joint purchases.

The process for joint purchase in "Myleto" enables the players to bet their favorite numbers by using the "Myleto," and then "Myleto" counts the preferred numbers of players to generate the popular numbers after the deadline of purchase phase. Then, "Myleto" takes the popular numbers to purchase the lottery for the trusted lottery organization (LO). Finally, LO generates the winning numbers and publishes them on the bulletin board. Then "Myleto" distributes the different prizes to the winning players according to the numbers they bet.

Even if the solution for the joint purchase lottery exists, according to our observations some drawbacks remain.

(1) From the user's viewpoint, the risks are as follows:

  (i) if the joint purchase players win the first prize, the person receiving the award has a chance to abscond with the funds;

  (ii) the player's lottery purchase evidence depends on the picture at the time of purchase and the credit card transaction receipt. However, the former lacks credibility because it is easy to fake, and the latter lacks immediacy since the credit card transaction receipt adopts a monthly settlement;

  (iii) if the player's purchase information is lost or the TP refuses to give out the prize, the player cannot proffer strong evidence to prove the winner is himself/herself.

(2) From the TP's viewpoint, the risk is as follows:

  (i) if a malicious player forges a picture and a credit card transaction receipt to claim the prize, the TP will find it hard to recognize whether the prize claim evidence is true or false.

At present, we have seen that the current TP of joint purchase exhibits some drawbacks, so determining how to implement a fair and secure joint purchase e-lottery protocol is still an open issue.

Hence, we propose a fair and secure joint e-lottery protocol to guarantee the rights and interests of the players and TP. Simultaneously, our proposed protocol also supports individual purchases.

The proposed scheme must be able to achieve the following requirements [4–6] such that the proposed scheme can be applied in actual practice.

(1) *Public Verification*. All the valid lottery tickets and the winning numbers must be verified via a verifiable random function.

(2) *Fairness*. No one can predict the winning result before the winning numbers are published.

(3) *Security*. No one can forge a winning lottery or impersonate a lottery winner to claim the prize.

(4) *Correctness*. The players can verify the public information of the bulletin board by themselves.

(5) *Anonymity*. Including lottery agents, no one can identify the participants by the lottery ticket.

(6) *Convenience*. The legitimate players should be able to purchase lottery via Internet.

(7) *Without Preregistration*. Players need not register at any lottery agent or drawing center in advance, as registration in advance is unnecessary; this requirement should conform to an electronic lottery to make it more realistic.

(8) *No Online Trusted Third Party (TTP)*. An electronic lottery is said to be impractical if the security of the entire mechanism depends on an online trusted third party.

(9) *Participants' Legality*. The scenario of the joint e-lottery scheme should ensure the participants' legality via a multisignature.

(10) *Support Joint and Individual E-Lottery Service*. The protocol must support joint and individual e-lottery service, respectively.

The remainder of this paper is organized to describe and analyze our joint e-lottery scheme as follows. Section 2 introduces related cryptographic techniques used in our scheme. Section 3 presents our proposed protocol, and the security requirements are analyzed in Section 4. Our conclusions are presented in the final section.

2. Preliminaries

In this section, we introduce three cryptographic techniques used in our scheme: a verifiable random function, an identity-based signature scheme, and an efficient identity-based RSA multisignature scheme.

2.1. Verifiable Random Function. A verifiable random function (VRF) was first proposed by Micali et al. [10]. Essentially, it is a pseudorandom function [11] providing noninteractively verifiable proof of the output's correctness. Therefore, the above properties of VRF are suitable for our scheme.

On the basis of the notation in [12], a set of functions $F_{(\cdot)}(\cdot) : \{0,1\}^k \rightarrow \{0,1\}^{l(k)}$ is a verifiable function; suppose there exist polynomial-time algorithms Gen $(\cdot)$, Eval $(\cdot,\cdot)$, Prove $(\cdots)$, Verify $(\cdot,\cdot,\cdot,\cdot)$ such that

(1) Gen(k) is a probabilistic algorithm to generate a secret key SK that is generated by a random function and the corresponding public key PK that enables public verification;

(2) Eval(SK, x) is an algorithm that computes the VRF's output $y = F_{\mathrm{SK}}(x)$;

(3) Prove(SK, x) is an algorithm that computes the proof π that $y = F_{SK}(x)$;

(4) Verify(PK, x, y, π) is an algorithm that verifies $y = F_{SK}(x)$;

(5) the VRF should satisfy the following properties.

(6) uniqueness:

$$\text{Verify}(\text{PK}, x, y_1, \pi_1) = \text{Verify}(\text{PK}, x, y_2, \pi_2), \quad (1)$$

where $y_1 = y_2$;

(7) computability: Eval(SK, x) $= F_{SK}(x)$ is efficiently computable;

(8) provability: (y, π) = (Eval(SK, x), Prove (SK, x)) and Verify(PK, x, y, π);

(9) pseudorandomness: the probability that an attacker can input any bit of $F_{SK}(x)$ for x his/her choice is negligible even if she/he has seen the values of many $F_{SK}(x')$ given $x' \neq x$.

2.2. Review of Shamir's Identity-Based Signature Scheme. In 1985, in order to simplify the public key authentication problem, Shamir [13] first offered the concept of an identity-based (ID-based) cryptosystem. In this system, each signer needs to register with a private key generator (PKG) and identify himself/herself before accessing the network resource. Once the registration is completed, the PKG will use the signer's identity to generate the secret key. The signer's identity may include the signer's name, email, and address. The advantage of this scheme is that there is no need for a public key directory in the system. The communicating parties only need to know the "identity" of his/her communication partner and the public key of the PKG is able to verify the signature or send an encrypted message.

We first introduce the notations used to explain how Shamir's scheme was constructed:

(p_X, q_X): a pair of large prime numbers;

N_X: a large number, where $N_X = p_X \cdot q_X$, $\varphi(N_X) = (p_X - 1)(q_X - 1)$, and $\varphi(\cdot)$ is Euler's totient function;

(e_X, d_X): X's public and private key, respectively, where $e_X d_X = 1 \bmod \varphi(N_X)$;

$H(\cdot)$: a one way hash function;

m: a message;

$A \stackrel{?}{=} B$: comparing whether or not A is equal to B.

2.2.1. Private Key Generator (PKG) Keys. The private key generator (PKG) chooses its public and private key pair as follows.

Step 1. Run the probabilistic polynomial algorithm K_{RSA} to generate two random large primes, p_{PKG} and q_{PKG}.

Step 2. Choose a random public key e_{PKG} such that $gcd(e_{PKG}, \phi(N_{PKG})) = 1$ and compute the private key $d_{PKG} = e_{PKG}^{-1} \bmod \phi(N_{PKG})$.

2.2.2. Signer Secret Key Generation. In this algorithm, the signer gets a copy of his/her secret key from the PKG through a two-step process.

Step 1. A signer submits his/her identity to the PKG.

Step 2. The PKG uses its private key d_{PKG} to sign the signer's identity i by generating the secret key g such that $g = i^{d_{PKG}} \bmod N_{PKG}$.

2.2.3. Message Signing. To sign a message m, the signer with the secret key g and the corresponding public key e_{PKG} of the PKG signs a message m by generating a signature pair $\sigma = (T, S)$ as follows.

Step 1. Select a random number r and compute

$$T = r^{e_{PKG}} \bmod N_{PKG}. \quad (2)$$

Step 2. For the same random number r, compute

$$S = g \cdot r^{H(T,m)} \bmod N_{PKG}. \quad (3)$$

$\sigma = (T, S)$ is the complete signature of the message m.

2.2.4. Message Verification. The identity-based signature $\sigma = (T, S)$ of a signer with identity i is valid if and only if the following equality holds:

$$S^e = i \cdot T^{H(T,m)} \bmod N_{PKG}. \quad (4)$$

2.3. Review of Harn's Efficient Identity-Based RSA Multisignatures Scheme. In the 2008, Harn and Ren [14] first proposed a digital signature of a message generated by multiple signers with multiple private keys based on Shamir's identity-based signature (IBS) scheme. This was a first efficient identity-based RSA multisignatures scheme with both fixed length and verification time. Harn and Ren's scheme is secure against forgeries under chosen-message attack, against multisigner collusion attack, and adaptive chosen-identity attack.

2.3.1. Private Key Generator (PKG) Keys. The PKG chooses its public and private key pairs as follows.

Step 1. Runs the probabilistic polynomial algorithm K_{RSA} to generate two random large primes, p_{PKG} and q_{PKG}.

Step 2. Choose a random public key e_{PKG} such that $gcd(e_{PKG}, \phi(N_{PKG})) = 1$ and compute the private key $d_{PKG} = e_{PKG}^{-1} \bmod \phi(N_{PKG})$.

2.3.2. Signer Secret Key Generation. In this algorithm, the signer gets a copy of his/her secret key from the PKG through a two-step process.

Step 1. A signer submits his/her identity to the PKG.

Step 2. The PKG uses its private key d_{PKG} to sign the message digest of the identity to generate the secret key g_j, such that

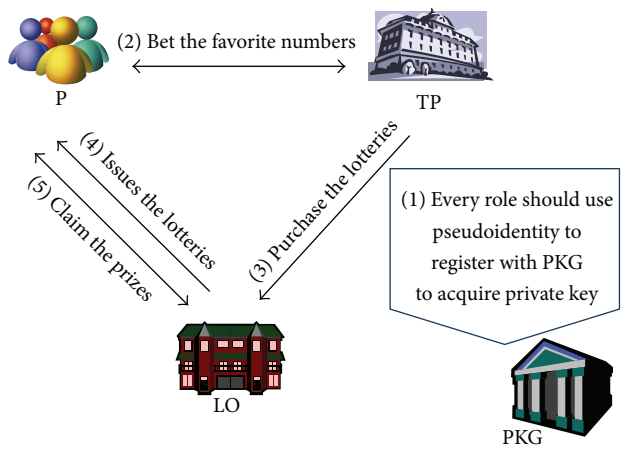

Figure 1: The structure of our scheme.

$g_j = i_j^{d_{\mathrm{PKG}}} \bmod N_{\mathrm{PKG}}$. No one will be able to distinguish between the identity and its message digest i_j.

2.3.3. Message Signing. To generate an identity-based multisignature, each signer carries out the followings steps.

Step 1. Choose a random integer r_j and compute $t_j = r_j^{e_{\mathrm{PKG}}} \bmod N_{\mathrm{PKG}}$.

Step 2. Broadcast t_j to other signers.

Step 3. Upon receiving of $t_j, j = 1, 2, \ldots, l$. each signer computes

$$T = \prod_{j=1}^{l} t_j \bmod N_{\mathrm{PKG}}$$
$$s_j = g_j \cdot r_j^{H(T,m)} \bmod N_{\mathrm{PKG}}. \quad (5)$$

Step 4. Broadcast s_j to all signers.

Step 5. After receiving of $t_j, j = 1, 2, \ldots, l$. the multisignatures component S can be computed as

$$S = \prod_{j=1}^{l} s_j \bmod N_{\mathrm{PKG}}. \quad (6)$$

The multisignature for message m is $\sigma = (T, S)$.

2.3.4. Multisignature Verification. To verify a multisignature $\sigma = (T, S)$ of a message m of signers whose identities are $i_1, i_2, \ldots, i_l$, anyone can verify the correctness as follows:

$$S^{e_{\mathrm{PKG}}} \stackrel{?}{=} (i_1, i_2, \ldots, i_l) \cdot T^{H(T,m)} \bmod N_{\mathrm{PKG}}. \quad (7)$$

3. The Proposed Joint E-Lottery Protocol

The structure of our scheme is illustrated in Figure 1.

There are four participants involved in the proposed e-lottery scheme.

(1) *Private Key Generator (PKG).* The off-line trusted third party which generates private keys to all participants.

(2) *Player (P).* The player is a participator in the lottery gamble.

(3) Trading *Platform (TP).* The trading platform is a website to provide players for joining the e-lottery game.

(4) *Lottery Originator (LO).* The LO issues the lotteries, generates the winning numbers to sell lotteries to gain revenue, and gives out the prizes.

Step 1. P, TP, LO ↔ PKG: all participants must register to PKG to acquire their private key with his/her pseudoidentity.

Step 2. P ↔ TP: the players bet their favorite numbers to the TP.

Step 3. TP → LO: the TP gathers the statistics on the betting numbers to generate the majority of popular numbers and then purchases the popular numbers with the LO.

Step 4. LO → P: the LO issues lotteries to the players.

Step 5. P ↔ LO: after the winning numbers are announced, the winning players use their winning lotteries and private keys to claim the prizes won.

The following notations are used in our protocol:

number$_j$: the favorite numbers of the jth player;

chain$_j$: the published hash chain set of the valid random seed β_j generated by player, which is involved in generating the winning number, where chain$_0$ is the initial vector; the chain$_0$ = 0, chain$_1$ = H(chain$_0$, β_1), chain$_2$ = H(chain$_1$, β_2), and chain$_j$ = H(chain$_{j-1}$, β_j);

C_i: the ith ciphertext;

σ_m: the identity-based signature of message m;

m_{req}: the request message;

i_j: the message digest of the jth player's identity;

PL: the purchased list, where PL = (i_j, β_j);

$H(\cdot)$: one way hash function [15];

r_X: the random number is selected by X;

β_j: the hash value, where $\beta_j = H(r_X)$;

$K_{X\text{-}Y}$: the session key between the X and Y which is constructed by IETF [16, 17];

$E(K_{X\text{-}Y}, (m))$: an encryption function which uses the session key $K_{X\text{-}Y}$ to encrypt the message m;

$D(K_{X\text{-}Y}, (C))$: a decryption function which uses the session key $K_{X\text{-}Y}$ to decrypt the ciphertext C.

3.1. Constructing the Session Key Model. Diffie and Hellman proposed a key agreement protocol [18] in 1978. The RFC 2631 was drawn up for the key agreement protocol in 1999 by the IETF. Therefore, we use the RFC 2631 protocol to construct the session keys. The session keys are used in our protocol with three situations. First, when the purchase is individual, the player must share the session key to protect his/her favorite numbers. Second, the TP and LO are jointed to sign the multisignature; they must share a common secret key to encrypt the signature. Third, the LO issues the lotteries to players, and the winning players send the claim prize message to the LO; they must also share a session key to encrypt or decrypt the messages.

3.2. The Initialization Phase. In this phase, the PKG performs the keys generating function to generate the public and private keys. On the other hand, the LO performs the VRF to generate the related functions and then publishes it.

Step 1. The PKG selects a random number k and then performs $\mathrm{Gen}(k)$ to generate the public e_{PKG} and private d_{PKG}.

Step 2. The LO performs the VRF to generate the related functions that include $\mathrm{Eval}(\cdot,\cdot)$, $\mathrm{Prove}(\cdot,\cdot)$, and $\mathrm{Verify}(\cdot,\cdot,\cdot)$.

3.3. The Registration Phase. In this phase, all of the roles submit their identities to the PKG to become legal participants. Notably, the players must submit their identities (including the players' name, email, and addresses) and a random number to PKG and then PKG signs the message digest of the identity by its d_{PKG} and d_{PKG}.

The PKG computes the participants' private keys with its d_{PKG} as in the following equations:

$$\begin{aligned} d_j &= i_j^{d_{\mathrm{PKG}}} \bmod N_{\mathrm{PKG}} \quad \text{for } j = 1, 2, \ldots, n. \\ d_{\mathrm{TP}} &= \mathrm{ID}_{\mathrm{TP}}^{d_{\mathrm{PKG}}} \bmod N_{\mathrm{PKG}}, \\ d_{\mathrm{LO}} &= \mathrm{ID}_{\mathrm{LO}}^{d_{\mathrm{PKG}}} \bmod N_{\mathrm{PKG}}. \end{aligned} \tag{8}$$

After that, the PKG publishes $\mathrm{ID}_{\mathrm{TP}}$ and $\mathrm{ID}_{\mathrm{LO}}$ on the bulletin board.

3.4. The Players Bet for Lottery Numbers Phase. In this phase, the players can bet their favorite numbers via the TP and then the TP publishes the purchase information on the bulletin board. When this phase is finished, the TP will send bulletin board information to the LO. According to the received information, the LO publishes the winning numbers. Moreover, players, TP, and LO can use the published bulletin board information to check whether or not the following three information items are correct.

(1) The players' purchased lotteries are included in the hash chain.

(2) The players' bet numbers are valid or not.

(3) The players are legal or not.

Table 1: The information of bulletin board.

Initial condition			
$\mathrm{chain}_0 = 0$			
$\mathrm{chain}_1 = H(\mathrm{chain}_0, \beta_1)$			
$\mathrm{chain}_2 = H(\mathrm{chain}_1, \beta_2)$			
$\vdots$			
$\mathrm{chain}_j = H(\mathrm{chain}_{j-1}, \beta_j)$			
Identity information	Hash chain value	Hash value of the random number r_{P_j}	Selected favorite number
(i_1, σ_{i_1})	chain_1	β_1	number_1
(i_2, σ_{i_2})	chain_2	β_2	number_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$
(i_j, σ_{i_j})	chain_j	β_j	number_j

The individual purchase is also included in the hash chain and the purchased information (including identity information, hash chain value, and hash value of the random number) is also published on the bulletin board, except for the selected favorite numbers.

The players bet for lottery numbers phase is illustrated in Figure 2, and the bulletin board information is illustrated in Table 1.

If anyone questions the players' legality then they can use the signature of the players' identity of the bulletin board to verify the legality of the players by

$$s_{P_j}^{e_{\mathrm{PKG}}} \stackrel{?}{=} i_j \cdot t_{P_j}^{H(t_{P_j}, i_j)} \bmod N_{\mathrm{PKG}}. \tag{9}$$

Step 1. If the purchase is individual then the player must compute session key $K_{P_j\text{-TP}}$ (refer to Section 3.1), using it to protect the individual's favorite number number_j as follows:

$$C_1 = E\left(K_{P_j\text{-TP}}, \left(\mathrm{number}_j\right)\right). \tag{10}$$

The individual and joint purchases are both required to process (11)–(15).

Then, the jth player selects a random number r_{P_j} to compute

$$\begin{aligned} \beta_j &= H\left(r_{P_j}\right), \\ t_{P_j} &= r_{P_j}^{e_{\mathrm{PKG}}} \bmod N_{\mathrm{PKG}}. \end{aligned} \tag{11}$$

The P_j uses his/her private key d_j to compute

$$s_{P_j} = d_j \cdot r_{P_j}^{H(t_{P_j}, i_j, \mathrm{number}_j, \beta_j)} \bmod N_{\mathrm{PKG}}. \tag{12}$$

Here, we denote the signature as follows:

$$\sigma_{i_j, \mathrm{number}_j, \beta_j} = \left(s_{P_j}, t_{P_j}\right). \tag{13}$$

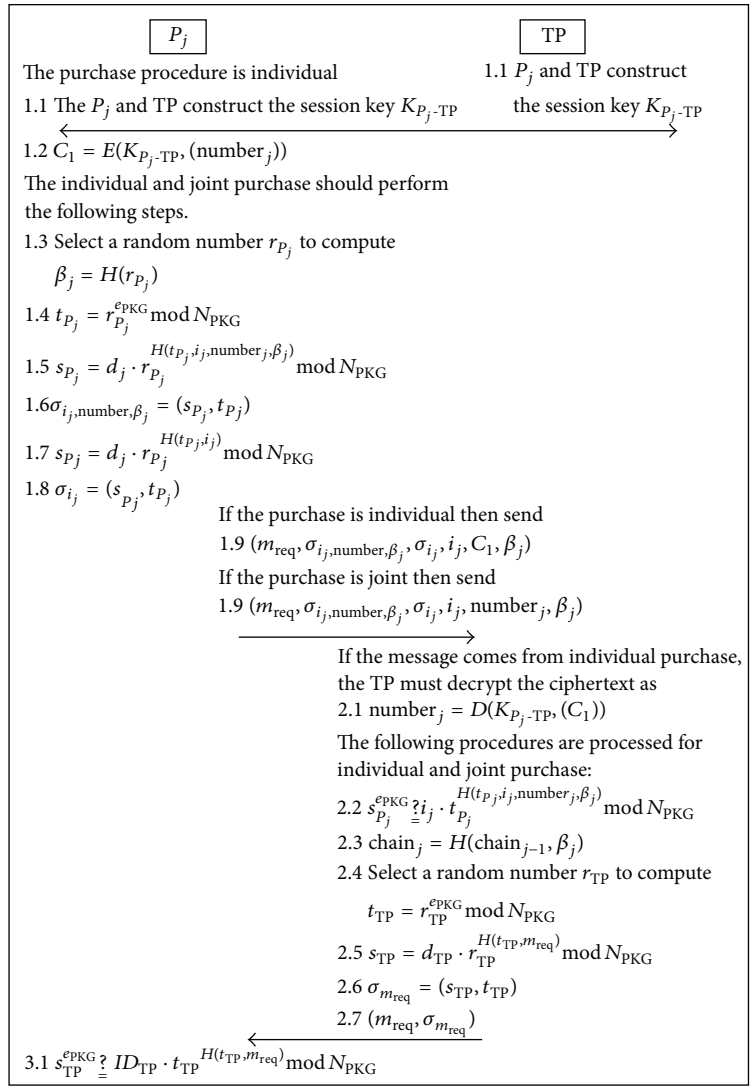

Figure 2: Overview of the players bet for lottery number phase.

Finally, the P_j uses his/her private key d_j to sign his/her identity i_j as follows:

$$s_{P_j} = d_j \cdot r_{P_j}^{H(t_{P_j}, i_j)} \bmod N_{\text{PKG}}. \tag{14}$$

We denote the signature as follows:

$$\sigma_{i_j} = \left(s_{P_j}, t_{P_j}\right). \tag{15}$$

The difference between the multisignature σ_{i_j} and $\sigma_{i_j,\text{number}_j,\beta_j}$ is that the former is published on the bulletin board and all participants can use it to verify the player's legality, while the latter is used to achieve the message nonrepudiation for the TP.

Afterward, if the purchase is individual then the request message m_{req}, signature $\sigma_{i_j,\text{number}_j,\beta_j}$, and related parameters (i_j, C_1, β_j) are sent to the TP.

If the purchase is joint, the request message m_{req}, signature $\sigma_{i_j,\text{number}_j,\beta_j}$, and related parameters $(i_j, \text{number}_j, \beta_j)$ are sent to the TP.

Step 2. After receiving the message, if it comes from individual purchase then the TP must decrypt the ciphertext C_1 to obtain number_j and then the following procedures are processed for individual and joint purchases.

First, the TP checks the validity of signature as follows:

$$s_{P_j}^{e_{\text{PKG}}} \stackrel{?}{=} i_j \cdot t_{P_j}^{H(t_{P_j}, i_j, \text{number}_j, \beta_j)} \bmod N_{\text{PKG}}. \tag{16}$$

The TP links β_j into the hash chain as follows:

$$\text{chain}_j = H\left(\text{chain}_{j-1}, \beta_j\right). \tag{17}$$

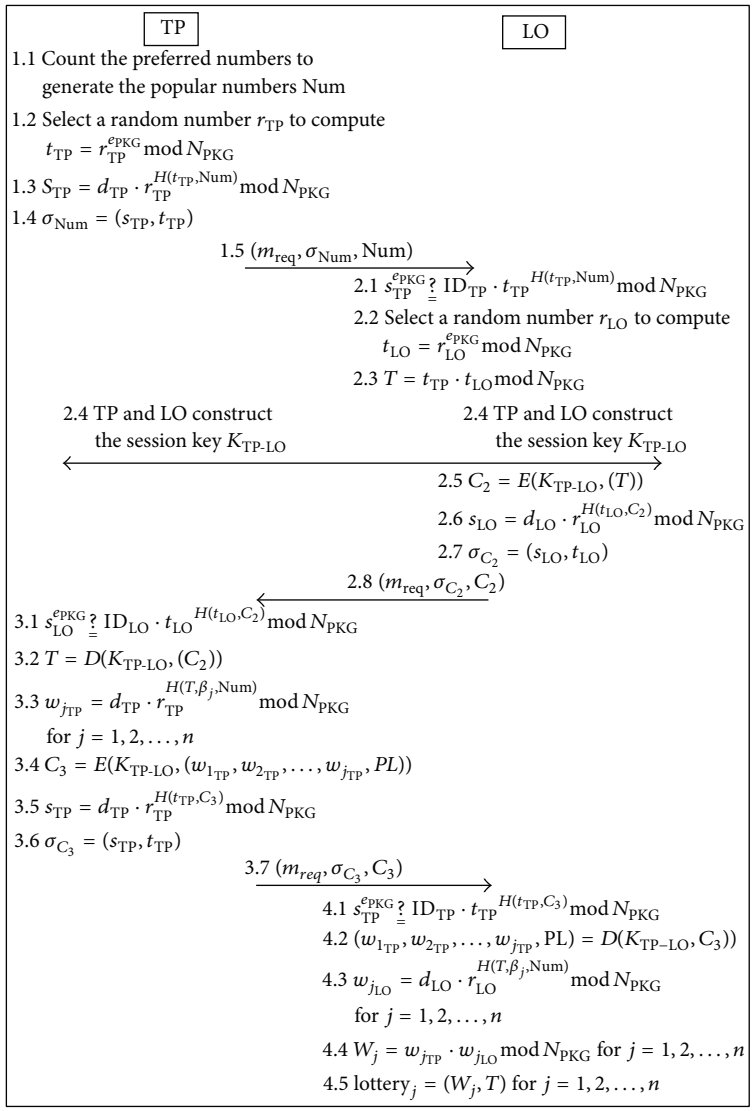

Figure 3: Overview of the purchase phase.

Next, the TP selects a random number r_{TP} to compute

$$t_{TP} = r_{TP}^{e_{PKG}} \bmod N_{PKG}$$
$$s_{TP} = d_{TP} \cdot r_{TP}^{H(t_{TP},m_{req})} \bmod N_{PKG}. \quad (18)$$

Here, we denote the signature of m_{req} as follows:

$$\sigma_{m_{req}} = (s_{TP}, t_{TP}). \quad (19)$$

Finally, TP sends signature $(\sigma_{m_{req}}, m_{req})$ to the P_j.

Step 3. After receiving $(\sigma_{m_{req}}, m_{req})$, P_j checks the validity of signature as follows:

$$s_{TP}^{e_{PKG}} \stackrel{?}{=} ID_{TP} \cdot t_{TP}^{H(t_{TP},m_{req})} \bmod N_{PKG}. \quad (20)$$

If the signature is invalid, then the P_j terminates the transaction.

3.5. The Purchase Phase. After the purchase deadline, the TP gathers the statistics on numbers to generate the popular numbers. Subsequently, the TP sends the purchase message that includes purchase list and the partial signature to the LO. Note that the lottery's numbers of individual purchase are determined by individual buyers rather than through counting by TP; individual purchase is the same as joint purchase.

(1) The individual purchase is included in the purchase list.

(2) The TP also computes the partial signature for individual purchase.

The overview of the purchase phase is illustrated in Figure 3.

Step 1. After the purchase deadline, the TP counts the preferred numbers of all of the players to generate the popular

numbers Num; then the TP selects a random number r_{TP} to compute the partial signature t_{TP} and s_{TP} as follows:

$$\begin{aligned} t_{\mathrm{TP}} &= r_{\mathrm{TP}}^{e_{\mathrm{PKG}}} \bmod N_{\mathrm{PKG}} \\ s_{\mathrm{TP}} &= d_{\mathrm{TP}} \cdot r_{\mathrm{TP}}^{H(t_{\mathrm{TP}},\mathrm{Num})} \bmod N_{\mathrm{PKG}}. \end{aligned} \tag{21}$$

Here, we denote the signature of Num as follows:

$$\sigma_{\mathrm{Num}} = \left(s_{\mathrm{TP}}, t_{\mathrm{TP}}\right). \tag{22}$$

Finally, the TP sends the request message m_{req}, signature σ_{Num}, and the popular numbers Num to the LO.

Step 2. Before receiving the message $(m_{\mathrm{req}}, \sigma_{\mathrm{Num}}, \mathrm{Num})$, the LO checks the signature validity as follows:

$$s_{\mathrm{TP}}^{e_{\mathrm{PKG}}} \stackrel{?}{=} \mathrm{ID}_{\mathrm{TP}} \cdot t_{\mathrm{TP}}^{H(t_{\mathrm{TP}},\mathrm{Num})} \bmod N_{\mathrm{PKG}}. \tag{23}$$

Subsequently, the LO selects random number r_{LO} to compute

$$t_{\mathrm{LO}} = r_{\mathrm{LO}}^{e_{\mathrm{PKG}}} \bmod N_{\mathrm{PKG}}. \tag{24}$$

LO uses the partial signature of the TP and LO to compute T as follows:

$$T = t_{\mathrm{TP}} \cdot t_{\mathrm{LO}} \bmod N_{\mathrm{PKG}}. \tag{25}$$

The TP and LO construct the session key $K_{\text{TP-LO}}$ and then encrypt the partial signature as follows:

$$C_2 = E\left(K_{\text{TP-LO}}, (T)\right). \tag{26}$$

The LO uses the private key d_{LO} to compute the partial signature of C_2 as follows:

$$s_{\mathrm{LO}} = d_{\mathrm{LO}} \cdot r_{\mathrm{LO}}^{H(t_{\mathrm{LO}},C_2)} \bmod N_{\mathrm{PKG}}. \tag{27}$$

Here, we denote the signature of C_2 as

$$\sigma_{C_2} = \left(s_{\mathrm{LO}}, t_{\mathrm{LO}}\right). \tag{28}$$

Finally, the LO sends $(m_{\mathrm{req}}, \sigma_{C_2}, C_2)$ to TP.

Step 3. After receiving $(\sigma_{C_3}, m_{\mathrm{req}})$, the TP checks the validity of signature as follows:

$$s_{\mathrm{LO}}^{e_{\mathrm{PKG}}} \stackrel{?}{=} \mathrm{ID}_{\mathrm{LO}} \cdot t_{\mathrm{LO}}^{H(t_{\mathrm{LO}},C_2)} \bmod N_{\mathrm{PKG}}. \tag{29}$$

The TP uses the session key $K_{\text{TP-LO}}$ to decrypt the cipher text as follows:

$$T = D\left(K_{\text{TP-LO}}, (C_2)\right). \tag{30}$$

According to the purchased list PL, the TP uses its private key d_{TP} to compute the partial multisignatures $w_{j_{\mathrm{TP}}}$ of the player's lottery as in (31) as follows:

$$w_{j_{\mathrm{TP}}} = d_{\mathrm{TP}} \cdot r_{\mathrm{TP}}^{H(T,\beta_j,\mathrm{Num})} \bmod N_{\mathrm{PKG}}, \quad \text{for } j = 1, 2, \ldots, n. \tag{31}$$

To protect the message, the TP uses the session key $K_{\text{TP-LO}}$ to encrypt parameters $(w_{1_{\mathrm{TP}}}, w_{2_{\mathrm{TP}}}, \ldots, w_{j_{\mathrm{TP}}}, \mathrm{PL})$ as follows:

$$C_3 = E\left(K_{\text{TP-LO}}, \left(w_{1_{\mathrm{TP}}}, w_{2_{\mathrm{TP}}}, \ldots, w_{j_{\mathrm{TP}}}, \mathrm{PL}\right)\right). \tag{32}$$

The TP uses its private key d_{TP} to compute the partial signature of C_3 as

$$s_{\mathrm{TP}} = d_{\mathrm{TP}} \cdot r_{\mathrm{TP}}^{H(t_{\mathrm{TP}},C_3)} \bmod N_{\mathrm{PKG}}. \tag{33}$$

Here, we denote the signature of C_3 as follows:

$$\sigma_{C_3} = \left(s_{\mathrm{TP}}, t_{\mathrm{TP}}\right). \tag{34}$$

Afterward, the TP sends the request message m_{req}, signature σ_{C_3}, and cipher message C_3 to the LO.

Step 4. Once receiving the message $(m_{\mathrm{req}}, \sigma_3, C_3)$, the LO checks the signature validity as follows:

$$s_{\mathrm{TP}}^{e_{\mathrm{PKG}}} \stackrel{?}{=} \mathrm{ID}_{\mathrm{TP}} \cdot t_{\mathrm{TP}}^{H(t_{\mathrm{TP}},C_3)} \bmod N_{\mathrm{PKG}}. \tag{35}$$

The LO uses its private key d_{LO} to decrypt the cipher text as follows:

$$\left(w_{1_{\mathrm{TP}}}, w_{2_{\mathrm{TP}}}, \ldots, w_{j_{\mathrm{TP}}}, \mathrm{PL}\right) = D\left(K_{\text{TP-LO}}, (C_3)\right). \tag{36}$$

According to the purchase list PL, the LO uses its private key d_{LO} to compute the partial multisignatures $w_{j_{\mathrm{LO}}}$ of all players as follows:

$$w_{j_{\mathrm{LO}}} = d_{\mathrm{LO}} \cdot r_{\mathrm{LO}}^{H(T,\beta_j,\mathrm{Num})} \bmod N_{\mathrm{PKG}}, \quad \text{for } j = 1, 2, \ldots, n \tag{37}$$

and then LO uses the partial multisignatures of $w_{j_{\mathrm{TP}}}$ and $w_{j_{\mathrm{LO}}}$ to compute

$$W_j = w_{j_{\mathrm{TP}}} \cdot w_{j_{\mathrm{LO}}} \bmod N_{\mathrm{PKG}}, \quad \text{for } j = 1, 2, \ldots, n. \tag{38}$$

We denote the lottery $\mathrm{lottery}_j$ as

$$\mathrm{lottery}_j = \left(W_j, T\right), \quad \text{for } j = 1, 2, \ldots, n. \tag{39}$$

3.6. The Lottery Issue Phase. Upon receiving the purchase message, the LO issues the lotteries to all players (including the joint purchase and individual purchase) and then the players can apply the multisignature to verify the validity of the lottery. The lottery issue phase is illustrated in Figure 4.

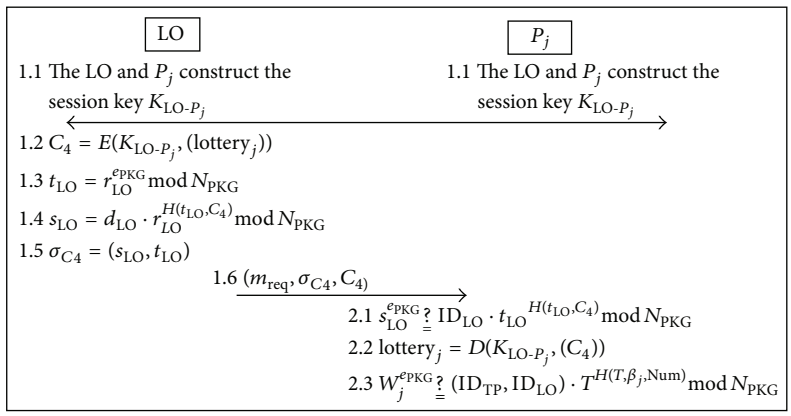

Figure 4: Overview of the lottery issue phase.

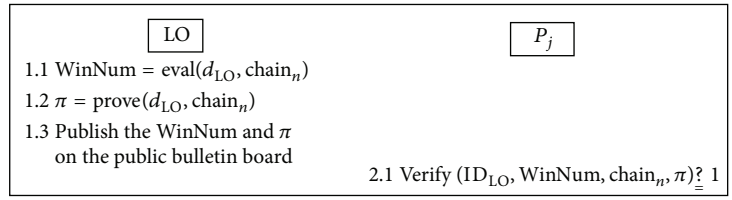

Figure 5: Overview of the winning numbers generation and verification phase.

Step 1. The LO and P_j construct the session key $K_{\text{LO-}P_j}$ and then encrypt the lottery_j as follows:

$$C_4 = E\left(K_{\text{LO-}P_j}, \left(\text{lottery}_j\right)\right). \tag{40}$$

Next, the LO selects random number r_{LO} to compute

$$t_{\text{LO}} = r_{\text{LO}}^{e_{\text{PKG}}} \bmod N_{\text{PKG}} \tag{41}$$

and uses its private key d_{LO} to compute the partial signature as follows:

$$s_{\text{LO}} = d_{\text{LO}} \cdot r_{\text{LO}}^{H(t_{\text{LO}}, C_4)} \bmod N_{\text{PKG}}. \tag{42}$$

Here, we denote the signature of C_4 as follows:

$$\sigma_{C_4} = \left(s_{\text{LO}}, t_{\text{LO}}\right). \tag{43}$$

Afterward, the LO sends the request message m_{req}, signature σ_{C_4}, and ciphertext C_4 to P_j.

Step 2. When receiving the message $(m_{\text{req}}, \sigma_4, C_4)$, P_j checks the validity of signature as follows:

$$s_{\text{LO}}^{e_{\text{PKG}}} \stackrel{?}{=} \text{ID}_{\text{LO}} \cdot t_{\text{LO}}^{H(t_{\text{LO}}, C_4)} \bmod N_{\text{PKG}} \tag{44}$$

and then uses the session key $K_{\text{LO-}P_j}$ to decrypt ciphertext C_4 as follows:

$$\text{lottery}_j = D\left(K_{\text{LO-}P_j}, \left(C_4\right)\right). \tag{45}$$

Finally, P_j checks the validity of signature as follows:

$$W_j^{e_{\text{PKG}}} \stackrel{?}{=} \left(\text{ID}_{\text{TP}}, \text{ID}_{\text{LO}}\right) \cdot T^{H(T, \beta_j, \text{Num})} \bmod N_{\text{PKG}}. \tag{46}$$

3.7. The Winning Numbers Generation and Verification Phase. After the lottery purchase deadline, the LO uses the function of winning numbers generation with the value of final hash chain to generate the winning numbers and then publishes it on the bulletin board. The overview of the winning numbers generation and verification phase is illustrated in Figure 5.

Simultaneously, if the players question whether or not the LO is honest, they can use the public verification function to verify the correctness of the winning numbers.

Step 1. The LO uses its private key d_{LO} and the value of final hash chain chain_n to calculate

$$\begin{aligned} \text{WinNum} &= \text{Eval}\left(d_{\text{LO}}, \text{chain}_n\right) \\ \pi &= \text{Prove}\left(d_{\text{LO}}, \text{chain}_n\right). \end{aligned} \tag{47}$$

Finally, the LO publishes the WinNum and π on the bulletin board.

Step 2. After the winning numbers are published, any player can checkthecorrectness of the winning numbers via the public verification function as follows:

$$\text{Verify}\left(\text{ID}_{\text{LO}}, \text{WinNum}, \text{chain}_n, \pi\right) \stackrel{?}{=} 1. \tag{48}$$

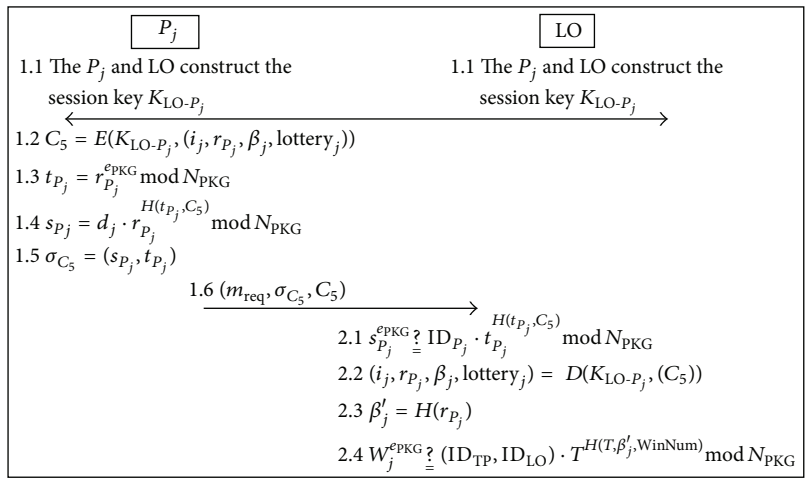

Figure 6: Overview of the claim prize phase.

3.8. The Claim Prize Phase. After the winning numbers are published, the winner of jth player can submit his/her winning lottery and the random number to claim the prize. Simultaneously, the LO publishes the winning lotteries, random number of winning player selected, and identity digest of winners on the bulletin board. If the other players suspect the legality of winning lottery, they can use the public verification function to verify it. The overview of the claim prize phase is illustrated in Figure 6.

Step 1. The P_j and LO construct the session key $K_{\text{LO-}P_j}$. In order to claim the prize, the winning player presents the important evidences $(i_j, r_{P_j}, \beta_j, \text{lottery}_j)$ to prove his/her identity and then uses the session key $K_{\text{LO-}P_j}$ to encrypt that evidence as follows:

$$C_5 = E\left(K_{\text{LO-}P_j}, \left(i_j, r_{P_j}, \beta_j, \text{lottery}_j\right)\right). \tag{49}$$

Next, the P_j computes as

$$t_{P_j} = r_{P_j}^{e_{\text{PKG}}} \bmod N_{\text{PKG}} \tag{50}$$

and uses its private key d_j to compute the partial signature as follows:

$$s_{P_j} = d_j \cdot r_{P_j}^{H(t_{P_j}, C_5)} \bmod N_{\text{PKG}}. \tag{51}$$

Here, we denote the signature of C_5 as follows:

$$\sigma_{C_5} = \left(s_{P_j}, t_{P_j}\right). \tag{52}$$

Afterward, P_j sends the request message m_{req}, signature σ_{C_5}, and ciphertext C_5 to LO.

Step 2. Once receiving message $(m_{\text{req}}, \sigma_5, C_5)$, the LO checks the signature validity as follows:

$$s_{P_j}^{e_{\text{PKG}}} \stackrel{?}{=} \text{ID}_{P_j} \cdot t_{P_j}^{H(t_{P_j}, C_5)} \bmod N_{\text{PKG}} \tag{53}$$

and then uses the session key $K_{\text{LO-}P_j}$ to decrypt the cipher message C_5 as follows:

$$\left(i_j, r_{P_j}, \beta_j, \text{lottery}_j\right) = D\left(K_{\text{LO-}P_j}, (C_5)\right). \tag{54}$$

If (53) holds, and then computes β'_j as follows

$$\beta'_j = H\left(r_{P_j}\right). \tag{55}$$

Finally, the LO uses the multisignature to verify the correctness of winning lottery as

$$W_j^{e_{\text{PKG}}} \stackrel{?}{=} (\text{ID}_{\text{TP}}, \text{ID}_{\text{LO}}) \cdot T^{H(T, \beta'_j, \text{WinNum})} \bmod N_{\text{PKG}}. \tag{56}$$

4. Analysis

Here, we use many kinds of scenarios to analyze the proposed joint electronic lottery scheme and to verify whether or not it achieves the requirements. In order to simplify the explanation, suppose there exists an intruder *Eve* in the network system and she is capable of eavesdropping communications between the TP, LO, and players.

4.1. Public Verification. All the valid lotteries and the winning numbers must be verified via a verifiable random function.

Scenario 1. Suppose that any player suspects the correctness of winning numbers.

Proof. The one suspecting can use (48) to verify the correctness of the winning numbers by (48). □

Scenario 2. Suppose that any player suspects the correctness of winning lotteries.

Proof. The one suspecting can use the related parameters (including random number of the winning player selected r_{P_j}, the winning numbers WinNum, and the winning lottery (W_j, T)) and (56) to verify the correctness of winning lotteries. The verification equation is as in (56), where $\beta'_j = H(r_{P_j})$.

The derivation of the verification is shown as follows:

$$\begin{aligned}
&\left(\mathrm{ID}_{\mathrm{TP}} \cdot \mathrm{ID}_{\mathrm{LO}}\right) \cdot T^{H(T,\beta'_j,\mathrm{WinNum})} \bmod N_{\mathrm{PKG}} \\
&= \left(d_{\mathrm{TP}}^{e_{\mathrm{PKG}}} \cdot d_{\mathrm{LO}}^{e_{\mathrm{PKG}}}\right) \cdot \left(t_{\mathrm{TP}} \cdot t_{\mathrm{LO}}\right)^{H(T,\beta'_j,\mathrm{WinNum})} \bmod N_{\mathrm{PKG}} \\
&= \left(d_{\mathrm{TP}}^{e_{\mathrm{PKG}}} \cdot d_{\mathrm{LO}}^{e_{\mathrm{PKG}}}\right) \cdot \left(r_{\mathrm{TP}}^{e_{\mathrm{PKG}}} \cdot r_{\mathrm{LO}}^{e_{\mathrm{PKG}}}\right)^{H(T,\beta'_j,\mathrm{WinNum})} \bmod N_{\mathrm{PKG}} \\
&= \left(d_{\mathrm{TP}}^{e_{\mathrm{PKG}}} \cdot d_{\mathrm{LO}}^{e_{\mathrm{PKG}}}\right) \cdot \left(r_{\mathrm{TP}}^{e_{\mathrm{PKG}} \cdot H(T,\beta'_j,\mathrm{WinNum})} \cdot r_{\mathrm{LO}}^{e_{\mathrm{PKG}} \cdot H(T,\beta'_j,\mathrm{WinNum})}\right) \bmod N_{\mathrm{PKG}} \\
&= \left(\left(d_{\mathrm{TP}} \cdot d_{\mathrm{LO}}\right) \cdot \left(r_{\mathrm{TP}}^{H(T,\beta'_j,\mathrm{WinNum})} \cdot r_{\mathrm{LO}}^{H(T,\beta'_j,\mathrm{WinNum})}\right)\right)^{e_{\mathrm{PKG}}} \bmod N_{\mathrm{PKG}} \\
&= \left(\left(d_{\mathrm{TP}} \cdot r_{\mathrm{TP}}^{H(T,\beta'_j,\mathrm{WinNum})}\right) \cdot \left(d_{\mathrm{LO}} \cdot r_{\mathrm{LO}}^{H(T,\beta'_j,\mathrm{WinNum})}\right)\right)^{e_{\mathrm{PKG}}} \bmod N_{\mathrm{PKG}} \\
&= \left(w_{j_{\mathrm{TP}}} \cdot w_{j_{\mathrm{LO}}}\right)^{e_{\mathrm{PKG}}} \bmod N_{\mathrm{PKG}} \\
&= W_j^{e_{\mathrm{PKG}}} \bmod N_{\mathrm{PKG}}.
\end{aligned} \tag{57}$$

Because the multisignature of the winning numbers is valid, the winning lottery is correct. □

4.2. Fairness. No one can predict the winning result before the LO publishes the winning numbers.

Scenario 3. If a player wants to predict or bias the winning result, he or she will fail.

Proof. Since each purchasing behavior is random and occasional, the final value of hash chain chain_n is contributed by all of the lotteries. Hence, no one can learn the final value of the hash chain chain_n. □

4.3. Security. No one can forge winning lotteries or impersonate lottery winners to claim their prize.

Scenario 4. If *Eve* tries to forge a winning lottery to claim the prize, she will fail.

Proof. In reviewing the purchase phase, the TP and LO used their private keys d_{TP} and d_{LO} to sign the lotteries. On the other hand, if *Eve* wants to fake the winning lottery, she must forge their private keys, respectively. In fact, she must solve the factorization problem in RSA cryptosystems [19]. □

Scenario 5. If *Eve* tries to forge a winning player, she will fail.

Proof. In the prize claim phase, the lottery winner must submit his/her digest i_j, random number r_{P_j} and β_j (where $\beta_j = H(r_{P_j})$) to proof his/her identity. If *Eve* uses the fake random number r'_{P_j} to claim the prize, then LO can perceive the attempt via the following equation:

$$\beta_j \stackrel{?}{=} H\left(r'_{P_j}\right). \tag{58}$$

□

On the other hand, if *Eve* wants to impersonate a winning player, she must find the r_{P_j}. In fact, based on the secure one way hash function, it is computationally infeasible to obtain r_{P_j} from β_j.

4.4. Correctness. The players can verify the public information via the bulletin board by themselves.

Scenario 6. The one suspecting questions

(1) the correctness of the player who bet numbers number_j,

(2) the correctness of the value of final hash chain chain_n,

(3) the correctness of popular numbers Num.

Proof. The one suspecting can use the published bulletin board information to verify the number_j, Num, and chain_n as

(1) the players can check whether the bet numbers are equal to the public information number_j;

(2) they can recalculate all bet numbers of players to determine whether the popular numbers Num is equal to the recalculated value;

(3) finally, the players can verify the validity of the value of final hash chain chain_n by using the public function hash chain as follows:

$$\begin{aligned}
&\text{Initial condition } \mathrm{chain}_0 = 0 \\
&\mathrm{chain}_1 = H\left(\mathrm{chain}_0, \beta_1\right) \\
&\mathrm{chain}_2 = H\left(\mathrm{chain}_1, \beta_2\right) \\
&\quad\vdots \\
&\mathrm{chain}_n = H\left(\mathrm{chain}_{n-1}, \beta_n\right),
\end{aligned} \tag{59}$$

where n is the number of the sold lottery tickets so far. □

4.5. Anonymity. Including the TP and LO, no one can identify the player from the lottery.

Scenario 7. If *Eve* tries to distinguish between messages digest i_j and real identity of player, she will fail.

Proof. In the registration phase, the players submit their personal information to the PKG and then PKG generates a message digest with personal information as $i_j = H$ (players' personal information).

The message digest is a well-known cryptographic assumption: the secure one way hash function has properties such that given a message m, it is easy to compute $H(m)$. On the other hand, it is computationally infeasible to obtain m from $H(m)$. And given $H(m)$, it is infeasible to find m' to let $H(m) = H(m')$. Hence *Eve* cannot find the real identity of the player from i_j. □

4.6. Convenience. Players are able to purchase lottery tickets if they can access the Internet. Clearly, the proposed joint e-lottery mechanism can achieve this requirement as indicated in the players betting for lottery numbers phase.

4.7. Without Preregistration. Players need not register at any lottery organizations in advance. In our scheme, the players need not register at any lottery organizations except for the PKG. In fact, if the players want to join other ID-based applications, the players still need to register to PKG for any PKI applications.

4.8. No Online Trusted Third Party. The proposed joint e-lottery mechanism does not require an online TTP.

In our scheme, no online TTP is used to participate in all of the transaction scenarios. Therefore, this requirement is completed in our scheme.

4.9. Participants' Legality. The scenario of the proposed joint e-lottery mechanism should ensure participants' legality.

Scenario 8. Suppose that players suspect the legality of the TP and LO.

Proof. In the lottery issuing phase, upon the players receiving lotteries from the LO, players can use the multisignature of lotteries to confirm the legality of TP and LO by (46).

If the equation holds, the participants' legality can be authenticated.

That is, only the legitimate private key is able to sign the valid signature. From another viewpoint, the PKG uses its private key d_{PKG} to generate d_{LO} in the registration phase; if anyone attempts to forge d_{LO} he/she must solve the RSA public-key cryptosystem to acquire the private keyd_{PKG}. In fact, it is an integer factorization problem [19]. □

Scenario 9. Suppose that the players, TP, or LO suspect the legality of player.

Proof. Anyonesuspecting can authenticate the player's legality by verifying the signature $\sigma_{i_j} = (s_{P_j}, t_{P_j})$ by (9).

If the equation holds, the jth player's legality can be authenticated; the derivation of the verification is shown as follows:

$$\begin{aligned} & i_j \cdot t_{P_j}^{H(t_{P_j}, i_j)} \bmod N_{\mathrm{PKG}} \\ &= d_j^{e_{\mathrm{PKG}}} \cdot t_{P_j}^{H(t_{P_j}, i_j)} \bmod N_{\mathrm{PKG}} \\ &= d_j^{e_{\mathrm{PKG}}} \cdot \left(r_{P_j}^{e_{\mathrm{PKG}}}\right)^{H(t_{P_j}, i_j)} \bmod N_{\mathrm{PKG}} \\ &= \left(d_j \cdot r_{P_j}\right)^{e_{\mathrm{PKG}} \cdot H(t_{P_j}, i_j)} \bmod N_{\mathrm{PKG}} \\ &= s_{P_j}^{e_{\mathrm{PKG}}} \bmod N_{\mathrm{PKG}}. \end{aligned} \tag{60}$$

□

From the above derivation of the verification, only the legitimate private key d_j is able to sign the valid signature. On the other hand, the player is only able to sign the valid signature if he/she registers with the PKG as a legal participant and acquires the private key d_j.

4.10. Support Joint and Individual E-Lottery Service. The protocol can support joint and individual e-lottery service, respectively. In our proposed scheme, we propose two purchase models to satisfy the requirements. Hence, two purchase models have the same rights and protections making our proposed scheme more practical and attractive.

4.11. Discussions. Our scheme focuses on proposing a secure and fair joint e-lottery, despite requiring more communication, more data transfer, and a higher computational complexity. We compare the functional properties between related works and ours in Table 2.

Table 2 shows that our scheme achieves the two new functional properties in comparison with related works [4–6]: participant's legality and supporting joint and individual e-lottery service.

In addition, we compare mechanisms with the existed lottery websites [8, 9] and ours in Table 3. Basically, [8, 9] only support a lottery agent. So, the player should register with the TP; this differs from ours.

Table 3 shows that our scheme adopted the ID-based multisignature to verify the legality of all participants while existing lottery websites lack effective mechanisms to achieve this requirement. On the other hand, the existing websites do not have remedial measures to prevent malicious behaviors by the lottery agent or players; for instance, the lottery agent refuses to give out the prize, a malicious player forges a picture to claim a prize, or the purchased lottery of a player is lost when the lottery agent's database crashes. Our scheme uses the ID-based multisignature to provide nonrepudiation evidence to prevent the above situations.

5. Conclusions

In this paper, we present a novel joint e-lottery protocol using the multisignature and verifiable random function. Having

Table 2: Comparisons between related works and ours.

	Chow et al.'s [4]	Lee and Chang's [5]	Lee et al.'s [6]	Ours
Security	Yes	Yes	Yes	Yes
Correctness	Yes	Yes	Yes	Yes
Anonymity	Yes	Yes	Yes	Yes
Random generation	Yes	Yes	Yes	Yes
Public verification	Yes	Yes	Yes	Yes
Fairness	Yes	Yes	Yes	Yes
Convenience	Yes	Yes	Yes	Yes
No online trusted third party	Yes	Yes	Yes	Yes
No pre-registration required	Yes	Yes	Yes	Yes
Participants legality	No	No	No	Yes
Support joint and individual e-lottery service	Support individual only	Support individual only	Support individual only	Yes

Table 3: Comparisons with the existing e-lottery websites.

	E-Lottery Syndicates [8]	Myleto [9]	Ours
Support joint and individual e-lottery service	Support individual only	Support joint only	Support joint and individual
Player should register with the TP	Yes	Yes	No
Allows players to verify legality of lottery agent	Absence of verification mechanisms	Absence of verification mechanisms	Adopts ID-based multi-signature
Allows players and lottery agent to verify the legality of other players	Absence of verification mechanisms	Absence of verification mechanisms	Adopts ID-based signature
The lottery agent refuses to give out the prize	No remedial measures	No remedial measures	Players hold the TP's signature to arbitral request
If a malicious player forges a picture to claim prize	Not easy to identify the legal lottery	Not easy to identify the legal lottery	Prompt identification by digital signature
Non-repudiation evidence	Depend on the scanned copy of the lottery shown on the screen	Depend on the scanned copy of the lottery shown on the screen	PKI digital signature

been proved, the new mechanism can achieve the requirements of general electronic lotteries. The players can increase the probability of winning prizes by using the proposed secure and fair joint e-lottery scheme. Notably, anyone can verify the correctness of winning lotteries and participants' legality simultaneously by verifying the multisignature; this functionality increases the convenience and security when a new participant joins the system. In the future, we are going to integrate the cash flow concept into our system.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This research was supported by the National Science Council, Taiwan, under contract nos. NSC 101-2221-E-324-005-MY2, 101-2221-E-212-006-MY3, and 102-2219-E-212-001.

References

[1] Mega millions, http://www.megamillions.com/.

[2] 649Lotter, http://www.649lotter.com/.

[3] California State Lottery, http://www.calottery.com/default.htm.

[4] S. S. M. Chow, L. C. K. Hui, S. M. Yiu, and K. P. Chow, "Practical electronic lotteries with offline TTP," *Computer Communications*, vol. 29, no. 15, pp. 2830–2840, 2006.

[5] J.-S. Lee and C.-C. Chang, "Design of electronic t-out-of-n lotteries on the Internet," *Computer Standards and Interfaces*, vol. 31, no. 2, pp. 395–400, 2009.

[6] J.-S. Lee, C.-S. Chan, and C.-C. Chang, "Non-iterative privacy preservation for online lotteries," *IET Information Security*, vol. 3, no. 4, pp. 139–147, 2009.

[7] J. Haigh, "The statistics of lotteries," in *Handbook of Sports and Lottery Markets*, pp. 481–502, 2008.

[8] e-Lottery Syndicates, http://www.e-lottery-syndicates.com/.

[9] Myleto, http://www.myleto.cc/.

[10] S. Micali, M. Rabin, and S. Vadhan, "Verifiable random functions," in *Proceedings of the IEEE 40th Annual Conference on Foundations of Computer Science*, pp. 120–130, October 1999.

[11] O. Goldreich, S. Goldwasser, and S. Micali, "How to construct random functions (extended abstract)," in *Proceedings of the IEEE Annual Symposium on Foundations of Computer Science*, pp. 464–479, 1984.

[12] A. Lysyanskaya, "Unique signatures and verifiable random functions from the DH-DDH separation," in *Proceedings of the Advances in Cryptology (CRYPTO '02)*, vol. 2442 of *Lecture Notes in Computer Science*, pp. 597–612, 2002.

[13] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proceedings of the Advances in Cryptology (CRYPTO '85)*, vol. 196 of *Lecture Notes in Computer Science*, pp. 47–53, 1985.

[14] L. Harn and J. Ren, "Efficient identity-based RSA multisignatures," *Computers and Security*, vol. 27, no. 1-2, pp. 12–15, 2008.

[15] P. Sarkar, "Domain extender for collision resistant hash functions: improving upon Merkle-Damgård iteration," *Discrete Applied Mathematics*, vol. 157, no. 5, pp. 1086–1097, 2009.

[16] C.-L. Chen and M.-H. Liu, "A traceable E-cash transfer system against blackmail via subliminal channel," *Electronic Commerce Research and Applications*, vol. 8, no. 6, pp. 327–333, 2009.

[17] Internet Engineering Task Force (IETF) Working Group, "RFC 2631 Diffie-Hellman Key Agreement Method," June 1999.

[18] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[19] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.