Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

Design of electronic *t*-out-of-*n* lotteries on the Internet

Jung-San Lee [*], Chin-Chen Chang, Fellow, IEEE

Department of Information Engineering and Computer Science, Feng Chia University, Taichung, 40724, Taiwan, ROC

ARTICLE INFO

Article history:
Received 17 July 2007
Received in revised form 26 February 2008
Accepted 4 May 2008
Available online 17 May 2008

Keywords:
Electronic lottery
Digital coin
Anonymity
Blind signature

ABSTRACT

The explosive development of network technology makes playing lotteries on the Internet become a billion-dollar industry now. This article presents an electronic *t*-out-of-*n* lottery game based on Chinese Remainder Theorem on the Internet. It is proved that this new method can achieve the general requirements of common electronic lottery mechanisms. Specifically, it allows lottery players to simultaneously select *t* out of *n* numbers in a ticket without iterative selection. And, this functionality makes the new method possible to be applied in practice. The security of the novel scheme is based on the secure one-way hash function and the factorization problem in RSA cryptosystems.

1. Introduction

For certain charities or countries, conventional lotteries are often launched to raise funds. Different from gambling, a lottery game usually exists in a legitimate form which may bring people wishes and let them have a chance to make a large fortune. There are three main participants in most conventional lottery games: lottery agents, players, and a drawing center. Lottery agents sell lottery tickets to the public. Depending on the game rules, players bet small money on a set of numbers ranged within a pre-defined domain. After the deadline of the lottery game, the drawing center will follow a random procedure to draw a set of winning numbers and then announce it publicly. The drawing process, however, must be monitored by a trusted party, such as a lawyer, to persuade players of the fairness.

With explosive development of network technologies, the Internet has become one of the most important essentials in our daily lives. People then may wonder whether it is practical to purchase lotteries, generate winning numbers, and claim prizes on the Internet. The answer shall be positive. Since the Internet allows people to communicate with each other without direct contact, then how to ensure the fairness and security of lotteries over the Internet becomes more difficult than that of traditional lottery games. Moreover, there must be a bank which can provide digital coins. From another point of view, an electronic lottery mechanism can provide some advantages extra to conventional lottery methods can. Specifically, it permits players to purchase lottery tickets at any time and any place as long as they can connect to the Internet. Players need not queue up for a long time when buying tickets. Furthermore, the use of digital coins or e-cash can provide the anonymity of players when purchasing lottery or claiming prizes, which helps to enhance the security of lottery winners [2,7]. With above-mentioned merits, the fascination of lotteries has made it a billion-dollar industry [5,6,8,9,11]. Consequently, we aim to propose an electronic *t*-out-of-*n* lottery mechanism based on Chinese Remainder Theorem and the concept of blind signature [1,3,4].

The novel method must be able to achieve the following requirements so that it can be applied in practice.

(1) *Security*: No one can forge a winning ticket or counterfeit a lottery winner to claim their prizes.
(2) *Correctness*: Players must be able to purchase their lottery tickets of favorite numbers. Namely, no one can falsify players' choices.
(3) *Anonymity*: No one (including lottery agents) can link a lottery ticket to the identity of a player. Hence, the risks of those lottery winners being traced, robbed or stolen can be reduced.
(4) *Random generation*: No one shall bias the generation of winning result. That is, each number within the pre-defined domain shall be equally contributed to the result.
(5) *Public verification*: Players are able to monitor and verify the winning result. That is, lottery agents cannot cheat players into drawing the winning numbers, and players can verify if their lottery tickets are valid.
(6) *Privacy of lottery*: No one can learn of the choices of lottery players except themselves.

[*] Corresponding author. Department of Information Engineering and Computer Science, National Chung Cheng University, 100 Wenhwa Rd., Seatwen, Taichung 40724, Taiwan, ROC. Tel.: +886 4 24517250x3790; fax: +886 4 27066495.
E-mail addresses: ljs@cs.ccu.edu.tw (J.-S. Lee), ccc@cs.ccu.edu.tw (C.-C. Chang).

0920-5489/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.csi.2008.05.004

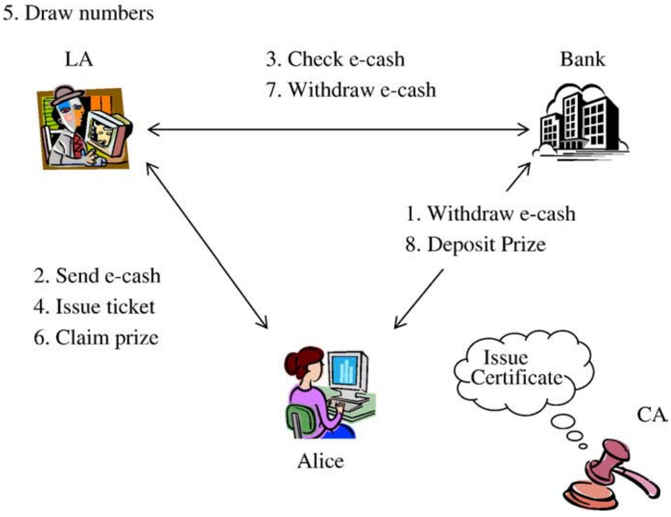


Fig. 1. The architecture of our scheme.

(7) *Fairness*: Before the deadline to run a lottery, no one can predict the winning numbers other than guessing.

(8) *Convenience*: Players shall be able to purchase lottery tickets when they can access to the Internet and possess enough digital coins.

(9) *Without online trusted third party*: An electronic lottery is said to be inflexible if the security of entire mechanism just depends on a trusted third party. Consequently, we insist that the novel scheme need not adopt an online trusted third party.

(10) *Without pre-registration*: Players need not register at any lottery agent or drawing center in advance. Pre-registration is not demanded in conventional lotteries. So this requirement should be confirmed in an electronic lottery to make it more realistic.

(11) *t-out-of-n choice*: Players can exactly select t out of n numbers from the pre-defined domain for each lottery ticket. That is, players are unable to select more than t numbers in each ticket to increase the winning possibility.

2. The novel electronic *t*-out-of-*n* lottery scheme

In this section, we describe a novel electronic t-out-of-n lottery scheme. The architecture of our scheme is illustrated in Fig. 1. The main participants in the lottery game include a Lottery Agent (LA), Players, a Certificate Authority (CA), and a Bank. LA launches the lottery game, sells tickets, maintains a bulletin board, draws a set of winning numbers of a lottery, and provides prizes. Players are those who buy tickets and can claim prizes if they win the game. CA must be responsible for arbitrating disputes and issuing digital certificates to participants, including public keys, expired dates, and verification information. The bank takes the responsibilities for generating digital coins for involved participants, and serves only when players purchase lottery tickets or claim prizes. Note that, each participant has to own an account before starting the game.

The novel mechanism consists of four phases: Initialization Phase, Purchase Phase, Draw Phase, and Claim Phase. Before describing the details of these phases, we first introduce notations used throughout our scheme.

Notations:

Alice the player

Prize the e-cash for the winner

$(e, N)/d$ the public/secret key of LA, N is the product of two large primes and $ed = 1 \bmod \phi(N)$

$PK_i/SK_i(\ )$ the encryption/decryption with participant i's public/secret key

$E_k/D_k(\ )$ symmetric encryption/decryption with secret key k

$H(\ )$ the secure one-way hash function

$a_1, a_2, \dots, a_n$ n lottery numbers, where a_i's are positive integers for $i = 1, 2$ to n

$d_1, d_2, \dots, d_n$ n positive integers that are pairwise relatively prime, where $d_i > a_i$ for $i = 1, 2$ to n

$\{b_1, b_2, \dots, b_t\}$: a set of t lottery numbers that Alice expected to buy, where b_j $\{a_1, a_2, \dots, a_n\}$

T_p the purchase deadline which is published on the bulletin board

T_c the claim prize deadline which is published on the bulletin board

E_cash_i a fixed number of digital coins of participant i, note that it will not reveal the identity of i

CW a set of lottery numbers determining the winner, $CW = \{cw_1, cw_2, \dots, cw_t\}$ and cw_i $\{1, 2, \dots, n\}$

Ran(w) a public random function with seed w, outputs of Ran(w) must be ranged from 1 to n without duplications.

2.1. Initialization phase

Step 1: At first, LA publishes n lottery numbers on a bulletin board, $a_1, a_2, \dots, a_n$, and then selects n relatively prime numbers, $d_1, d_2, \dots, d_n$, where $d_i > a_i$ for $i = 1, 2$ to n.

Step 2: LA subsequently computes

$$D = d_1 * d_2 * \dots * d_n,$$

and constructs congruence system as,

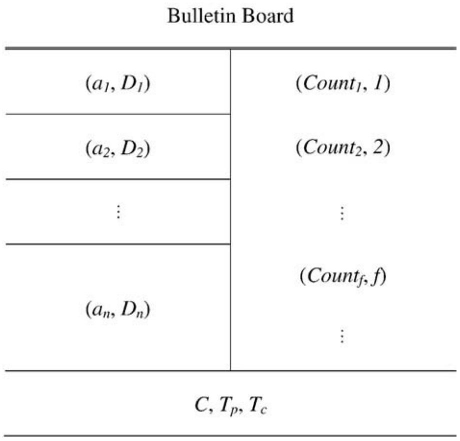
$$\begin{aligned} C &\equiv a_1 (\bmod d_1), \\ C &\equiv a_2 (\bmod d_2), \\ &\vdots \\ C &\equiv a_n (\bmod d_n). \end{aligned} \qquad (1)$$

Therefore, LA obtains $C = (D/d_1)y_1a_1 + (D/d_2)y_2a_2 + \dots + (D/d_n)y_na_n \bmod D$ by CRT, where $(D/d_i)y_i \equiv 1 \ (\bmod\ d_i)$, for $i = 1, 2$ to n.

Step 3: As illustrated in Fig. 2, LA finally computes and publishes on the bulletin board the followings.

$$\begin{aligned} D_1 &= d_1^e \bmod N, \\ D_2 &= d_2^e \bmod N, \\ &\vdots \\ D_n &= d_n^e \bmod N, \end{aligned} \qquad (2)$$

where (e, N) is the public key of LA.



Bulletin Board

(a_1, D_1)	$(Count_1, 1)$
(a_2, D_2)	$(Count_2, 2)$
$\vdots$	$\vdots$
(a_n, D_n)	$(Count_f, f)$ $\vdots$
C, T_p, T_c	

Fig. 2. The bulletin board.

2.2. Purchase phase

Supposing there is a player Alice. Alice then can purchase the lottery ticket through the following steps. And, the flowchart of Purchase Phase is depicted in Fig. 3.

Step 1: Alice chooses t pairs of (a'_j, D'_j)'s from the bulletin board, for $j=1, 2,\ldots, t$.

Step 2: For each (a'_j, D'_j), Alice generates a random number r_j and computes,

$$\begin{aligned} &\alpha_1 = r_1^e * D'_1 \bmod N, \\ &\alpha_2 = r_2^e * D'_2 \bmod N, \\ &\vdots \\ &\alpha_t = a_t^e * D'_t \bmod N. \end{aligned} \tag{3}$$

Alice subsequently computes and sends $PK_{\mathrm{LA}}(\alpha_1, \alpha_2,\ldots, \alpha_t, r_{A1}, r_{A2}, E\_cash)$ to LA, where r_{A1} and r_{A2} are two random numbers, and E_cash is a fixed number of Alice's digital coins.

Step 3: After receiving messages from Alice, LA computes $SK_{\mathrm{LA}}(PK_{\mathrm{LA}}(\alpha_1, \alpha_2,\ldots, \alpha_t, r_{A1}, r_{A2}, E\_cash))$ and checks if E_cash is valid. If it does not hold, LA terminates the connection; otherwise, LA employs its private key d to compute

$$\begin{aligned} &\beta_1 = \alpha_1^d \bmod N, \\ &\beta_2 = \alpha_2^d \bmod N, \\ &\vdots \\ &\beta_t = \alpha_t^d \bmod N, \end{aligned} \tag{4}$$

Step 4: LA then computes

$$\mathrm{Count}_f = \mathrm{Count}_{f-1} + r_{A1} \bmod f, \tag{5}$$

where f is the number of lottery tickets sold so far. Next, LA publishes (Count_f, f) on the public bulletin board and generates

$$k_f = H(r_{A2} || \mathrm{Count}_f || f).$$

Finally, it issues the lottery ticket $\mathrm{LT}_f=[\mathrm{Count}_f, f, E_{kf}(\mathrm{Count}_f, f, \beta_1, \beta_2,\ldots, \beta_t, T_c)]$ to Alice. Note that the tuple $(k_f, \mathrm{Count}_f, f)$ is stored in LA's databases, and k_f is used to ensure the following smooth communications between Alice and LA.

Step 5: Upon Alice receives the ticket sent by LA, she first computes

$$k'_f = H(r_{A2} || \mathrm{Count}_f || f) \text{ and } D_{k'_f}\left(E_{k_f}(\mathrm{Count}_f, f, \beta_1, \beta_2, \ldots, \beta_t, T_c)\right).$$

Then she compares the retrieved Count_f with the received one. If they are different, Alice informs LA to reconstruct the connection; otherwise, she keeps the ticket in its databases.

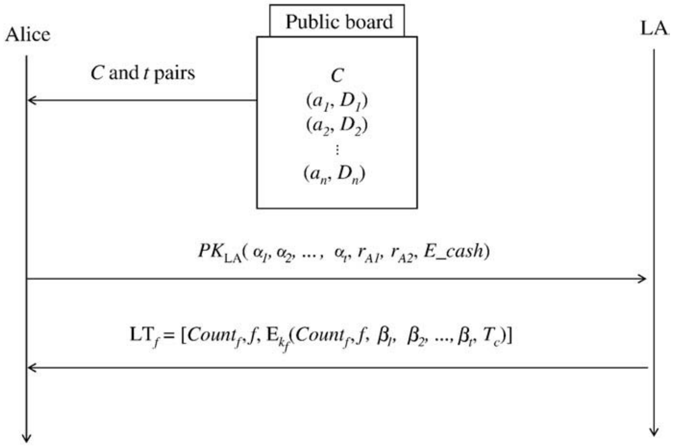

Alice
Public board
LA
C and t pairs
C
(a1, D1)
(a2, D2)
⋮
(an, Dn)
PKLA(α1, α2, …, αt, rA1, rA2, E_cash)
LTf = [Countf, f, Ekf(Countf, f, β1, β2, …, βt, Tc)]

Fig. 3. The flowchart of purchase phase.

2.3. Draw phase

Assume the final result to be $\mathrm{Count}_f=C_r$. After the deadline of lottery purchasing, LA performs the following procedure to generate a set of lottery numbers CW.

Step 1: It first computes $w=C_r \bmod n$, where n is the number of lottery numbers.

Step 2: LA then inputs seed w into the random function to generate CW,

$$\mathrm{Ran}(w) = CW = \{cw_1, cw_2, \ldots, cw_t\}.$$

Step 3: Next, LA announces the result of winning numbers

$$CW = \{cw_1, cw_2, \ldots, cw_t\}.$$

2.4. Claim phase

Assume that Alice wins the lottery, i.e., $CW=\{cw_1, cw_2,\ldots, cw_t\}=\{a'_1, a'_2,\ldots, a'_t\}$.

Step 1: Alice computes and sends $PK_{\mathrm{LA}}(\mathrm{Count}_f, f, \mathrm{LT}_f, (r_1^{-1}, r_2^{-1},\ldots, r_t^{-1}))$ to LA.

Step 2: When receiving messages from Alice, LA computes

$$SK_{LA}\left(PK_{LA}\left(\mathrm{Count}_f, f, LT_f, \left(r_1^{-1}, r_2^{-1}, \ldots, r_t^{-1}\right)\right)\right)$$

to obtain LT_f and $(r_1^{-1}, r_2^{-1},\ldots, r_t^{-1})$ and checks if LT_f has already been used to claim the Prize. If it is fresh, LA finds the secret key k_f according to (Count_f, f) to decrypt LT_f.

Step 3: LA subsequently uses the retrieved $\beta_1, \beta_2,\ldots, \beta_t$ to compute the following

$$\begin{aligned} &d'_1 = r_1^{-1} * \beta_1 \bmod N, \\ &d'_2 = r_2^{-1} * \beta_2 \bmod N, \\ &\vdots \\ &d'_t = r_t^{-1} * \beta_t \bmod N. \end{aligned} \tag{6}$$

Step 4: With above results and C, LA computes

$$\begin{aligned} &b_1 = C \bmod d'_1, \\ &b_2 = C \bmod d'_2, \\ &\vdots \\ &b_t = C \bmod d'_t. \end{aligned} \tag{7}$$

If $\{b_1, b_2, \ldots, b_t\}$ is the same as CW, LA is convinced of Alice's winning.

Step 5: After T_c, LA can compute and send E_{kf} (Prize) to Alice according to the retrieved Count_f. And, Alice is able to obtain the Prize without giving her identity.

3. Discussions

In the following, we are going to demonstrate that the novel scheme can achieve the requirements mentioned in Section 1 and then compare it with other related works in terms of confirming properties. The security of the novel mechanism is based on two well-known cryptographic assumptions: the secure one-way hash function and Factorization problem in RSA systems [10,12,13].

(1) Secure one-way hash function $H(\ )$: Given a message m, it is easy to compute $H(m)$, however, it is computationally infeasible to obtain m from $H(m)$. And, given $H(m)$, it is infeasible to find m' to let $H(m)=H(m')$.

(2) Factorization assumption: Let N be the product of two large primes, and (e, d) be a pair of two integers satisfying $ed=1$ mod $\phi(N)$. Then it is computationally infeasible to
- find d such that $m_1^d=m_2$ mod N, given two integers m_1 and m_2;
- find m_1 such that $m_1^d=m_2$ mod N, given an integer m_2.

3.1. Analyses of the novel electronic mechanism

Here, we construct several scenarios to analyze the way the novel electronic lottery mechanism achieve the requirements. To simplify the explanation, we assume that there exists an intruder Eve in the network system. And, Eve is aware of Alice's playing a lottery and is capable of eavesdropping communications between lottery agents and players.

3.1.1. Security

The novel mechanism claims that no one can forge a winning ticket or counterfeit a lottery winner to claim a prize.

Scenario 1. *If Eve wants to forge a winning ticket to get the prize, she must fail.*

Proof. A lottery ticket is in the form of $\mathrm{LT}_f=[\mathrm{Count}_f, f, E_{kf}(\mathrm{Count}_f, f, \beta_1, \beta_2,\ldots, \beta_t, T_c)]$. Though Eve may intercept the ticket, she can learn nothing but Count_f and f. Since r_{A2} is embedded in $PK_{\mathrm{LA}}(\alpha_1, \alpha_2,\ldots, \alpha_t, r_{A1}, r_{A2}, E\_cash)$, Eve cannot obtain it without the private key of LA. If she still persists in generating valid $k_f=H(r_{A2}\,||Count_f||f)$ to forge a fake winning ticket without knowing r_{A2}, this attempt must violate the assumption of secure one-way hash. As a result, Eve fails to forge a winning ticket. □

Scenario 2. *If Eve wants to counterfeit the winner Alice to get the prize, she must be unsuccessful.*

Proof. Assume that Eve is able to intercept PK_{LA} $(\mathrm{Count}_f, f, \mathrm{LT}_f, (r_1^{-1}, r_2^{-1},\ldots, r_t^{-1}))$ in Step 1 of Claim Phase somehow and to learn the fact that Alice has won the prize after the announcement of winning numbers. Eve has to pass the intercepted message to LA first. Hereafter LA will confirm the validity of this ticket and then return E_{kf}(Prize) to Alice in Step 4 of Claim Phase. Even though Eve is able to intercept this message again in some way, it is still computationally infeasible for her to construct a valid k_f to decrypt the message. Still, Eve is unable to obtain the prize without getting k_f under the assumption of secure one-way hash function. □

3.1.2. Correctness

The novel method claims that players can freely select lottery numbers and no one can falsify their choices.

Scenario 3. *If LA and Alice follow the initialization and purchase phases, then Alice is able to select her preferred numbers in a lottery ticket, and Eve can not falsify her choices.*

Proof. Since Alice select tuples (a_j', D_j')'s, for $j=1, 2,\ldots, t$, from the bulletin board, she can make her favorite choices without interference. Here, we prove that Alice's choices will not be altered by Eve. Before being transferred to LA, these choices have already been encrypted by the public key of LA. That is, if Eve wants to falsify Alice's choices in the form $(\alpha_1, \alpha_2,\ldots, \alpha_t)$, she has to solve the RSA public-key cryptosystem to obtain the public key. In fact, it is computationally infeasible under factorization assumption. On the other hand, after LA signs the blind signature for each tuple, it encrypts the results with the session key $k'_f=H(r_{A2}||Count_f||f)$. Namely, if Eve tries to alter Alice's choices in the form $(\beta_1, \beta_2,\ldots, \beta_t)$, she has to compute k'_f first. And, this violates the assumption of secure one-way hash function. □

Scenario 4. *If LA tries to alter the choice of Alice in Purchase Phase, Alice can detect this attempt and prove it to CA.*

Proof. Since Alice's choices are embedded into $\alpha_1, \alpha_2,\ldots,$ and α_t with blind signature, it is computationally infeasible for LA to tamper the choices under the factorization assumption. The only way for LA to falsify Alice's choice is replacing $\beta_1, \beta_2,\ldots,$ and β_t with t random numbers $\beta'_1, \beta'_2,\ldots,$ and β'_t. Nevertheless, we know that $(\alpha_1, \alpha_2,\ldots, \alpha_t)$ is the combination of r_j^e and D'_j, for $j=1, 2$ to t. And, this implies $(\beta_1, \beta_2,\ldots, \beta_t)$ is the combination of r_j and D'^d_j. Since Alice possesses the blind factors $r_1, r_2,\ldots,$ and r_t, only she can filter them out by Eq. (6). Hence, after Alice receives $\beta'_1, \beta'_2,\ldots,$ and β'_t from LA, it is she that can compute a set of $\{d''_1, d''_2,\ldots,d''_t\}$ as follows,

$$\begin{aligned} d''_1 &= r_1^{-1}{*}\beta'_1 \bmod N,\\ d''_2 &= r_2^{-1}{*}\beta'_2 \bmod N,\\ &\vdots\\ d''_t &= r_t^{-1}{*}\beta'_t \bmod N. \end{aligned}$$

Here, we have $\{d''_1, d''_2,\ldots, d''_t\}\not\subset\{d_1, d_2,\ldots, d_n\}$ since $\beta'_1, \beta'_2,\ldots,$ and β'_t are just random numbers. Then, given C and $\{d''_1, d''_2, \ldots, d''_t\}$, Alice is able to retrieve a set of $\{b'_1, b'_2,\ldots, b'_t\}$ by computing

$$\begin{aligned} b'_1 &= C \bmod d''_1,\\ b'_2 &= C \bmod d''_2,\\ &\vdots\\ b'_t &= C \bmod d''_t, \end{aligned}$$

Since C is constructed with tuples (a_i, d_i)'s by Eq. (1), according to Chinese Remainder Theorem and $\{d''_1, d''_2,\ldots, d''_t\}\not\subset\{d_1, d_2,\ldots, d_n\}$, $b'_1, b'_2, \ldots,$ and b'_t must be different from Alice's choices $a'_1, a'_2,\ldots,$ and a'_t. Hence, Alice can prove the falsification to CA. □

3.1.3. Anonymity

No one, including LA, can link a lottery ticket to the identity of player.

Scenario 5. *If LA wants to link Alice's identity to her lottery ticket, LA must fail.*

Proof. Since the novel method adopts the concept of digital coins, Alice can use *E-cash* issued by a legal bank to purchase lottery without giving her identity. LA needs to check the validity of *E-cash* in Purchase Phase. Again, since *E-cash* applies the mechanism of blind signature to achieve the anonymity property, anyone who possesses *E-cash* can use it. According to the definition of blind signature, we learn that the security of blind signature is based on the factorization problem in RSA cryptosystems. That is, if LA wants to connect the owner with *E-cash*, it violates the factorization assumption. □

Scenario 6. *If Eve wants to link Alice's identity to her lottery ticket, she must fail.*

Proof. Since the identity of Alice is not revealed in Purchase Phase and Claim Phase, it is impossible for Eve to link Alice's personal information to a lottery ticket. □

3.1.4. Random generation

No one can bias the generation of winning result.

Scenario 7. *No one, including LA, can bias the winning result.*

Proof. The randomness of winning lottery is guaranteed by Eq. (5). Furthermore, each purchase is random and occasional, and thus LA is unable to make sure which set of lottery numbers will finally be the winning one. □

3.1.5. Public verification

Players are able to monitor and verify the winning result.

Scenario 8. *After Alice purchases a lottery, she can check if its contribution to the generation of winning numbers is counted and can publicly verify the final result.*

Proof. After LA confirms the validity of e-*cash* and issues LT_f to Alice, it publishes (Count_f, f) on the public board. Then Alice checks if r_{A1} is counted by Eq. (5). Step by step, Alice also can verify the result by computing $w = C_r \bmod n$, as illustrated in Step 1 of Drawing Phase, where w is the final result of Count_f. Finally, Alice can input w into the random function Ran( ) to construct a set of winning numbers and compare it with the announced one. □

3.1.6. Privacy of lottery

No one can learn the choices of lottery players but only themselves.

Scenario 9. *No one, including LA, can learn the choices of players but themselves.*

Proof. After Alice makes her choices from the public board, she generates a random number for each selection. Subsequently, Alice combines selected items with random numbers by Eq. (3). That is, Alice adopts the mechanism of blind signature to make her choices concealed. When receiving $\{\alpha_1, \alpha_2, \ldots, \alpha_t\}$ from Alice, LA has to solve the factorization problem in RSA cryptosystems if LA tries to learn the choices of Alice. And it is computationally infeasible under the assumption.

On the other hand, an intruder Eve may select a set of $\{a''_1, a''_2, \ldots, a''_t\}$ to guess what happened to Alice. The probability of guessing the right choices of Alice is computed as:

$$\Pr\left(a''_j = a'_j \middle| j = 1, 2 \text{ to } t\right) = 1/C^n_t = \frac{\frac{1}{n!}}{t!(n-t)!} = \frac{t!(n-t)!}{n!}.$$

This is the same as that of hitting a set of winning numbers. Hence, it conforms to the game rule. □

3.1.7. Fairness

Before the deadline to run a lottery, no one can predict the winning numbers but only guessing.

Scenario 10. *If LA and Alice follow the protocol, no one can indicate the winning lottery before T_p.*

Proof. Since each purchase of lottery is random and occasional, the random seed w contributed by all tickets will change often according to the submissions. Hence, even LA is incapable of learning the final result before T_p. □

3.1.8. Convenience

Players shall be able to purchase lottery tickets if they can access to the Internet and possess enough digital coins. Obviously, the novel electronic lottery mechanism can fulfill this requirement as indicated in Purchase Phase.

3.1.9. No online trusted third party

The novel scheme needs not adopt an online trusted third party. Throughout the mechanism, we find no online trusted third party used to monitor purchasing or drawing processes other than CA. And, CA is only involved in the procedure when disputes occur. Consequently, this requirement is reached in the new method.

3.1.10. No pre-registration required

Players need not register at any lottery agent or drawing center in advance. As described in Initialization Phase, Alice does not need to register at any lottery agents except a legal bank. And, the registration to a bank is necessary if Alice wants to join an electronic commerce model.

3.1.11. t-out-of-n choice

Players can exactly select t numbers from the pre-defined domain for each lottery ticket.

Scenario 11. *If Alice chooses more than t numbers to increase the winning probability, LA will detect this attempt and terminate the transaction.*

Table 1
Comparisons between related works and ours

	[8]	[5]	[6]	[9]	[11]	Ours
CON	Yes	Yes	Yes	Yes	Yes	Yes
RG	Yes	Yes	Yes	Yes	Yes	Yes
PV	Yes	No	No	No	Yes	Yes
PL	No	Yes	Yes	No	Yes	Yes
AN	Yes	No	No	No	Yes	Yes
NPR	Yes	No	Yes	Yes	Yes	Yes
NOP	Yes	Yes	Yes	No	Yes	Yes
FA	Yes	No	No	No	Yes	Yes
SEC	Yes	No	Yes	Yes	Yes	Yes
TN	No	No	No	No	No	Yes

Proof. As illustrated in Step 3 of Purchase Phase, LA employs its private key to blindly sign Alice's choices. By Eq. (4), we know that only t selections are signed by LA for each lottery ticket. Hence, this requirement is ensured in the novel method. □

3.2. More discussions

In this subsection, we are going to compare several related works with ours in terms of achieving properties. First, we define notations used in Table 1. “Yes” denotes that the method can achieve the requirement while “No” represents negative situation. “CON” means the requirement of convenience. “RG” denotes the requirement of random generation of winning lottery. “PV” denotes the requirement of public verification. “PL” denotes the requirement of privacy of lottery numbers. “AN” means the requirement of anonymity. “NPR” means no pre-registration required. “NOP” means no online trusted third party required. “FA” denotes the requirement of fairness. “SEC” means the requirement of security. “TN” means that players can simultaneously select t numbers without iterative selection.

Requirements listed in Table 1 are the essentials of general e-lottery mechanisms. In [8,9], the privacy of players' lottery numbers can not be preserved. This is harmful to prizewinners after the declaration of winning numbers. Furthermore, the requirement of anonymity can not be confirmed in [5,6,9]. This may subject prizewinners to the threat of being robbed or stolen. Even the fairness requirement is not introduced in [5,6,9]. That is, the fairness of winner generation is under suspicion. Besides, the security of e-lottery system must rely on an online trusted third party in [9]. In such mechanism, we have to assume that the online trusted third party must be very powerful and stable. More precisely, any crash of the online server is intolerable since each transaction may involve with a large amount of money. But, this assumption is hard to achieve in nowadays network environments.

As illustrated in Table 1, the novel method is able to achieve the requirements of general electronic lottery mechanisms. In particular, only the new scheme allows players to simultaneously select t lottery numbers in a ticket without iterative selection. This functionality makes the novel scheme more similar to conventional lottery games. Hence, it has higher probability to be applied over the Internet than other related works.

4. Conclusions and future works

Undoubtedly, playing lotteries over the Internet is now a billion-dollar industry. In this article, we presented a novel electronic lotteries on the Internet based on Chinese Remainder Theorem. Having been proved, the new mechanism can achieve the requirements of general electronic lotteries. Specifically, it allows players to simultaneously select t numbers in a ticket without iterative selection. And, this functionality increases the possibility of the new method to be applied in practice. In the future, we are going to lower down the computation overheads of players in purchasing lotteries. This attempt may attract players who access to the Internet with mobile or wireless devices into electronic lottery games.

References

[1] C.W. Chan, C.C. Chang, A scheme for threshold multi-secret sharing, Applied Mathematics and Computation 166 (1) (July 2005) 1–14.

[2] C.C. Chang, J.S. Lee, An anonymous voting mechanism based on the key exchange protocol, Computers and Security 25 (4) (2006) 307–314.

[3] D. Chaum, Untraceable electronic mail, return addresses and digital pseudonyms, Communications of the ACM 24 (2) (1981) 84–88.

[4] D. Chaum, Blinding for unanticipated signatures, Proceedings of Advances in EUROCRYPT'87, Berlin, 1987, pp. 227–233.

[5] D.M. Goldschlag, S.G. Stubblebine, Publicly verifiable lotteries: applications of delaying functions, Proceedings of the Second International Conference on Financial Cryptography (FC' 98), Anguilla, British West Indies, February 1998, pp. 214–226.

[6] E. Kushilevitz, T. Rabin, Fair e-lotteries and e-casinos, Proceedings of The Cryptographer's Track at RSA Conference 2001, San Francisco, CA, USA, April 2001, pp. 100–109.

[7] H.F. Hwang, C.C. Chang, An untraceable electronic cash system using fair blind signatures, Proceedings of 2006 IEEE International Conference on e-Business Engineering (ICEBE 2006), Shanghai, China, October 2006, pp. 39–46.

[8] J. Zhou, C. Tan, Playing lottery on the Internet, Proceedings of the Third International Conference on Information and Communications Security (ICICS 2001), Xian, China, November 2001, pp. 189–201.

[9] K. Sako, Implementation of a digital lottery server on WWW, Proceedings of the International Exhibition and Congress on Secure Networking, Germany, 1999, pp. 101–108.

[10] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM 21 (2) (1977) 120–126.

[11] S.S.M. Chow, L.C.K. Hui, S.M. Yiu, K.P. Chow, Practical electronic lotteries with offline TTP, Computer Communications 29 (2006) 2830–2840.

[12] R. Gramer, V. Shoup, Signature schemes based on the strong RSA assumption, Proceedings of the 6th ACM Conference on Computer and Communications Security, Singapore, 1999, pp. 46–51.

[13] T. ElGamal, A public-key cryptosystem and a signature protocol based on discrete logarithms, IEEE Transactions on Information Theory 31 (4) (1985) 469–472.

Jung-San Lee received the BS degree in Computer Science and Information Engineering in 2002 and his Ph.D in Computer Science and Information Engineering in 2008, both from the National Chung Cheng University, Chiayi, Taiwan. His current research interests include electronic commerce, information security, cryptography, and mobile communications.

Chin-Chen Chang received his BS degree in Applied Mathematics in 1977 and his MS degree in Computer and Decision Sciences in 1979, both from the National Tsing Hua University, Hsinchu, Taiwan. He received his Ph.D in Computer Engineering in 1982 from the National Chiao Tung University, Hsinchu, Taiwan. During the academic years of 1980–1983, he was on the faculty of the Department of Computer Engineering at the National Chiao Tung University. From 1983–1989, he was on the faculty of the Institute of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan. From 1989 to 2004, he has worked as a professor in the Institute of Computer Science and Information Engineering at the National Chung Cheng University, Chiayi, Taiwan. Since 2005, he has worked as a professor in the Department of Information Engineering and Computer Science at Feng Chia University, Taichung, Taiwan. Dr. Chang is a Fellow of IEEE, and a member of the Chinese Language Computer Society, the Chinese Institute of Engineers of the Republic of China, and the Phi Tau Phi Society of the Republic of China. His research interests include computer cryptography, data engineering, and image compression.