Robust t-out-of-n Internet Lottery Games with Player Anonymity

Jung-San Lee, Kuo-Jui Wei, and Wei-Chiang Kao

Abstract—No matter where you stay, you must often notice a scenario that people stand in a queue in front of lottery vendors. This phenomenon has lasted out for centuries. Different from gambling, a lottery game is usually launched by the Government or a legitimate organization for gathering funds or raising charity finance. To enhance the convenience and popularity of lottery, Lee and Chang have developed an electronic lottery system which allows players to purchase lotteries over the Internet recently. Unfortunately, it has been demonstrated that the system cannot ensure the robustness requirement. That is, a player can forge a winning ticket to earn the price. We therefore propose an improvement on their system to fix the weakness. Aside from that, we design a brand-new method which can preserve essentials of e-lottery game system.

Keywords—Digital coin; Privacy; Anonymity; Robustness

I. Introduction

Lottery games are designed to raise funds by selling tickets; it is often launched by the Government or a legitimate organization. Lottery surpluses are contributed to charitable institutions, while the main prize of the lottery gives players the chance to win a large fortune. This enticement is the reason why lottery games have become so popular over the whole world and lasted for centuries. A lottery game ordinarily consists of three parties: players, sellers, and a drawer. According to the pre-defined game rules, players pick and bet some money on a set of their favorite numbers to purchase a lottery ticket from lottery sellers. Once the deadline of lottery game comes, the drawer will publicly choose a set of random numbers and announce it to determine the winner of the lottery game [10, 11].

With fast development and progress of network technologies, the Internet and our daily lives has become inseparable. This fact reveals that it is time to perform lottery games over the Internet. In 2009, Lee and Chang proposed an innovative idea to carry out the electronic lottery game [11]. They have defined the following essential for designing a secure e-lottery game.

(1) *Robustness*: No one can forge a winning ticket to claim the prizes [12].
(2) *Correctness*: Players are allowed to purchase lottery ticket with a set of favorite numbers.
(3) *Anonymity*: No one can link the lottery to the player's identity.
(4) *Random generation*: Each number within the predefined domain must contribute to the result equally.
(5) *Public verification*: Players must be able to monitor and check the winning result.
(6) *Privacy of lottery*: No one can learn of the choice of the player from the ticket except themselves.
(7) *Fairness*: No one can foresee the winning set except for guessing.
(8) *Convenience*: Everyone can be a player to purchase lottery whenever they can link to the Internet and possess sufficient e-cash [11].
(9) *Without online trusted third party (TTP)*: The security of electronic lottery mechanism shall not depend on a trusted third party since it is hard to guarantee that TTP can be accessed all the time.
(10) *Without pre-registration*: While purchasing lottery, players need not to register at any lottery seller or drawer.
(11) *t-out-of-n choice*: Players can non-iteratively pick *t* numbers from the pre-defined domain for each lottery ticket[4].

In [11], Lee and Chang have claimed that their e-lottery system is able to confirm all the essentials. Particularly, they have introduced the digital cash in [1, 3] to help achieve the essential of anonymity. This implies that no one can link the digital cash to the user. Unfortunately, it has been found that a player who has bought several tickets to collect all the numbers of the predefined domain is able to forge a winning ticket to gain the price. We therefore propose an improvement on their system to fix the weakness. Furthermore, we design a brand-new method which can preserve essentials of e-lottery game system.

The rest of this article is organized as follows. In Section II, we propose a new and robust e-lottery scheme. The security analysis of the new method is demonstrated in Section III. Finally, we make conclusions in Section IV.

This work was supported by MOST104-2221-E-035-036-
J.S. Lee is with Department of Information Engineering and Computer Science, Feng-Chai University, Taichung 407, Taiwan.
(Corresponding author phone: 8864-24517250 ext. 3767; fax: 8864-27066495; e-mail: leejs@fcu.edu.tw)
K.J. Wei is with Department of Information Engineering and Computer Science, Feng-Chai University, Taichung 407, Taiwan.
W.C. Kao is with Department of Information Engineering and Computer Science, Feng-Chai University, Taichung 407, Taiwan.

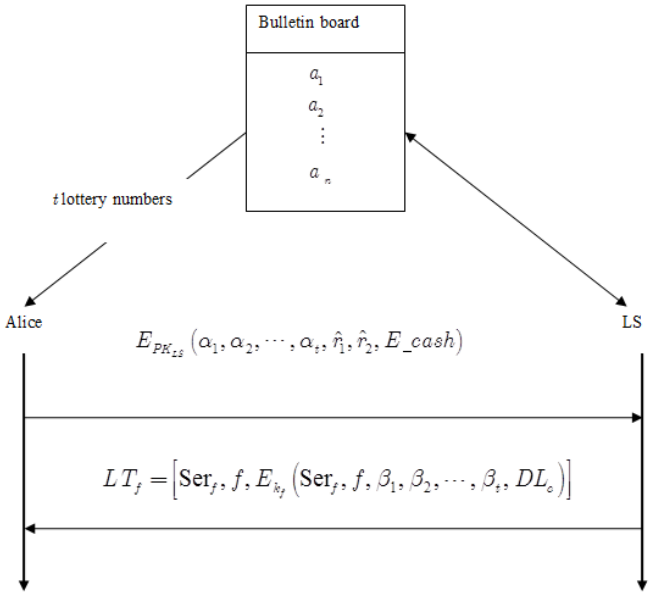


Fig. 1. The flowchart of purchase-issue phase

II. Proposed Method

In the new method, characteristics of the lottery ticket are embedded into the signature signed by LS to prevent an attacker from forging a winning ticket. The new mechanism contains four phases, and details are given below.

A. Setting Phase

In this phase, LS has to define the domain of lottery numbers and publish them on the bulletin board along with DL_p and DL_c.

B. Purchase-Issue Phase (Fig. 1)

Step 1: Alice selects t lottery numbers a'_j from the bulletin board and chooses t random numbers $r_1, r_2, \ldots, r_t$ in $\mathbb{Z}_N^*$ to blind them as follows,

$$\alpha_j = r_j^e \cdot a'_j \bmod N. \quad (2.1)$$

Step 2: Alice subsequently generates two random numbers ($\hat{r}_1$, $\hat{r}_2$) and sends the purchase request $E_{PK_{LS}}(\alpha_1, \alpha_2, \ldots, \alpha_t, \hat{r}_1, \hat{r}_2, E\_cash)$ to LS, where E_cash is a fixed number of digital coins of Alice.

Step 3: LS decrypts and verifies if *E_cash* is valid after receiving the request from Alice. If it is invalid, LS terminates the connection; otherwise, LS employs the following recursive formula to compute the serial number of Alice's ticket,

$$\mathrm{Ser}_f = \mathrm{Ser}_{f-1} + \hat{r}_1 \bmod f, \quad (2.2)$$

where f is the amount of lottery tickets sold so far.

Subsequently, LS computes the characteristic of the ticket $\tau = H(f \| \mathrm{Ser}_f)$ and uses *d* to sign the signature of $\tau \cdot \alpha_j$ as

$$\beta_j = (\tau \cdot \alpha_j)^d \bmod N. \quad (2.3)$$

Step 4: LS utilizes Ser_f and f to generate a session key k_f shared between LS and Alice,

$k_f = H(\hat{r}_2 \| \mathrm{Ser}_f \| f)$.

Afterward, LS keeps the tuple (f, Ser_f, k_f) in its databases.

Finally, LS issues a lottery ticket

$LT_f = [\mathrm{Ser}_f, f, E_{k_f}(\mathrm{Ser}_f, f, \beta_1, \beta_2, \ldots, \beta_t, DL_c)]$ to Alice and publishes (f, Ser_f) on the bulletin board.

Step 5: When Alice receives her ticket, she computes

$k'_f = H(\hat{r}_2 \| \mathrm{Ser}_f \| f)$ and

$D_{k'_f}(E_{k_f}(\mathrm{Ser}_f, f, \beta_1, \beta_2, \ldots, \beta_t, DL_c))$.

Then she can verify the validity of this ticket by comparing the retrieved Ser_f with the one on the bulletin board. If these two values are the same, Alice stores this ticket in her databases; otherwise, she informs LS to transmit the ticket again.

C. Draw Phase

Assume that the last serial number on the ticket is Ser_F. After the deadline of lottery purchasing, LS generates a set of winning numbers according to the following procedure.

Step 1: LS inputs Ser_F as the seed into the pseudo-random number generator to construct a set of t numbers,

$\mathrm{PRNG}(\mathrm{Ser}_F) = \{a_1^*, a_2^*, \ldots, a_t^*\}$.

Step 2: LS announces that these *t* numbers are the winning numbers *WN*,

$WN = \{a_1^*, a_2^*, \ldots, a_t^*\}$.

D. Claim Phase

Assume that Alice wins the lottery, that is $WN = \{a_1^*, a_2^*, \ldots, a_t^*\} = \{a'_1, a'_2, \ldots, a'_t\}$.

Step 1: Alice computes and sends $E_{PK_{LS}}(\mathrm{Ser}_f, f, LT_f, (r_1, r_2, \ldots, r_t))$ to LS.

Step 2: When receiving the message from Alice, LS computes $D_{SK_{LS}}(E_{PK_{LS}}(\mathrm{Ser}_f, f, LT_f, (r_1, r_2, \ldots, r_t)))$, and checks if LT_f has been used to claim the prize. If LT_f is fresh, LS gets (f, Ser_f, k_f) from its database according to f. LS utilizes f and Ser_f to compute $\tau' = H(f \| \mathrm{Ser}_f)$ and uses k_f to decrypt LT_f.

Step 3: LS subsequently uses the retrieved β_j and r_j to calculate

$$b_j = r_j^{-1} \cdot \beta_j \bmod N \quad (2.4)$$

For each b_j, LS computes,

$$\tilde{b}_j = (\tau')^{-1} \cdot b_j^e \bmod N \quad (2.5)$$

If $\{\tilde{b}_1, \tilde{b}_2, \cdots, \tilde{b}_t\}$ is the same as *WN*, then LS is convinced of that Alice is the winner.

Step 4: LS computes and sends $E_{k_f}(\text{Prize})$ to Alice according to the retrieved Ser_f after DL_c. Note that Alice needs not to show her identity to acquire the prize.

III. Analysis

In this section, we are going to demonstrate that the proposed scheme can withstand the forgery attack and satisfy the essential defined by Lee and Chang [11]. Moreover, we compare related works with ours in Subsection III.B. The security of new lottery mechanism is based on two cryptographic assumptions: Factorization problem in RSA cryptosystem and the secure one-way hash function [2, 7].

(1) Factorization problem assumption: Let *N* be the product of two large primes, and *e*, *d* are two integers satisfying $ed \equiv 1 \pmod{\phi(N)}$. It is computationally infeasible to achieve the following.

Given two integers m_1 and m_2, find an integer d such that $m_1^d = m_2 \bmod N$.

Given an integer m_2, find an integer m_1 such that $m_1^d = m_2 \bmod N$.

(2) Secure one-way hash function $H(\cdot)$: For an integer m, it is easy to compute $H(m)$ but computationally infeasible to achieve the following.

(Preimage resistance) Given an integer m', find m such that $H(m) = m'$.

(2nd-preimage resistance) Given $H(m)$, find an integer m' such that $m' \neq m$ and $H(m') = H(m)$.

A. Requirement Analysis

Now, we draw up several propositions to show how the robust lottery mechanism can confirm all the essentials mentioned in Section I. In these scenarios, we assume that there exists an attacker Oscar on the Internet.

A.1 Robustness

No one can forge a winning ticket to claim the prize.

Proposition 1. *If Oscar wants to forge a winning ticket to get the prize by intercepting the information communicated between Alice and LS, then he must fail.*

Proof. LS transmits the lottery ticket to Alice in the form $LT_f = [\text{Ser}_f, f, E_{k_f}(\text{Ser}_f, f, \beta_1, \beta_2, \ldots, \beta_t, DL_c)]$. Even Oscar can intercepts this message, he learn nothing but f and Ser_f. If Oscar wants to decrypt the message embedded in the ticket, he must construct k_f first. Under the second assumption, Oscar cannot generate $k_f = H(\hat{r}_2 \| \text{Ser}_f \| f)$ without $\hat{r}_2$. Furthermore, since $\hat{r}_2$ is embedded in $E_{PK_{LS}}(\alpha_1, \alpha_2, \ldots, \alpha_t, \hat{r}_1, \hat{r}_2, E\_cash)$, Oscar cannot retrieve it unless he knows the private key of LS. Consequently, Oscar fails to forge a winning ticket.

Proposition 2. *If Oscar tries to falsify the lottery numbers from a valid ticket to forge a winning ticket, he must be unsuccessful.*

Proof. Assume that Oscar has changed the number of a valid ticket, i.e. replace β_j with β_j'. To succeed in forging a valid ticket, β_j' must be able to pass the verification procedure in Step 3 of Claim phase. According to Eq. (3.4) and (3.5), we know that β_j' ought to satisfy the equation as follows,

$$\left(r_j^{-1}\beta_j'\right)^e = \tau \cdot a_j^* \bmod N,$$

Although Oscar can obtain $\tau = H(f \| \text{Ser}_f)$ and a_j^* to compute $\tau \cdot a_j^*$ after the draw phase, he still cannot generate β_j' such that it can satisfy the above equation unless he can solve the Factorization problem in RSA cryptosystem to obtain *d*. As a result, Oscar fails to forge a winning ticket under the first assumption.

Proposition 3. *If Oscar wants to counterfeit the lottery winner Alice to get the prize, he must fail.*

Proof. Suppose that Oscar has learned that Alice wins the prize by intercepting $E_{PK_{LS}}(\text{Ser}_f, f, LT_f, (r_1, r_2, \ldots, r_t))$ in Step 1 of the claim phase. Even though Oscar can pass the intercepted message to LS to claim the prize, LS can prevent this attack. First LS must confirm the validity of this ticket and then send $E_{k_f}(\text{Prize})$ to Alice according to Ser_f on the ticket in Step 4 of the claim phase. Granted that Oscar is able to intercept this message again, it is still computationally infeasible for him to generate a valid k_f to decrypt the message. As a result, Oscar is unable to obtain the prize under the assumption of secure one-way hash function.

A.2. Correctness

Players are allowed to purchase lottery ticket with a set of favorite numbers.

Proposition 4. *According to the procedure of purchase-issue phase, Alice is able to select numbers she wants in her lottery ticket, and Oscar can not alter her choices.*

Proof. As described in Step 1 of purchase-issue phase, Alice can select any number she likes from the bulletin board. Now, if Oscar wants to alter Alice's choices by falsifying $(\alpha_1, \alpha_2, \ldots, \alpha_t)$ in the purchase request $E_{PK_{LS}}(\alpha_1, \alpha_2, \ldots, \alpha_t, \hat{\hat{r}}_1, r_2, E\_cash)$, he has to solve the RSA public-key cryptosystem. This is computationally infeasible under the factorization assumption. In addition, assume that Oscar can alter Alice's choices of the ticket LT_f when LS sends it to Alice, he must be able to generate the shared key $k_f' = H(\hat{r}_2 \| \text{Ser}_f \| f)$ so that he can decrypt the message $E_{k_f}(\text{Ser}_f, f, \beta_1, \beta_2, \ldots, \beta_t, DL_c)$ on LT_f. But, this has violated the assumption of secure one-way hash function.

Proposition 5. *If LS falsifies the choice of Alice in purchase-issue phase, Alice can detect this intention and prove it to CA.*

Proof. It is clear that Alice's choices are blinded into $\alpha_1, \alpha_2, \ldots,$ and α_t with random numbers $r_1, r_2, \ldots,$ and r_t. Hence it is computationally infeasible for LS to know the chosen numbers a_j. The only method for LS to falsify Alice's choice is to replace ($\alpha_1, \alpha_2, \ldots, \alpha_t$) with another set of ($\alpha_1', \alpha_2', \ldots, \alpha_t'$), sign them as $\beta_1', \beta_2', \ldots, \beta_t'$ and then issue the ticket with β_j' to Alice. Since Eq. (2.3) implies that $\beta_j = r_j \left(\tau a_{i_j}\right)^d \bmod N$, when Alice receives $\beta_1', \beta_2', \ldots,$ and β_t', she can remove the blind factor $r_1, r_2, \ldots,$ and r_t by Eq. (2.4). Alice can also use f and Ser_f of the ticket to generate $\tau = H\left(f \,||\, \mathrm{Ser}_f\right)$ and further calculate a set of $\left\{b_1'', b_2'', \ldots, b_t''\right\}$ as follows,

$$b_1'' = \tau^{-1} \cdot \left(b_1'\right)^e \bmod N,$$

$$b_2'' = \tau^{-1} \cdot \left(b_2'\right)^e \bmod N,$$

$$\vdots$$

$$b_t'' = \tau^{-1} \cdot \left(b_t'\right)^e \bmod N,$$

where $b_j' = r_j^{-1} \cdot \beta_j' \bmod N$.

Note that $\left\{b_1'', b_2'', \ldots, b_t''\right\} \neq \left\{a_{i_1}, a_{i_2}, \ldots, a_{i_t}\right\}$ since α_1', $\alpha_2', \ldots,$ and α_t' are generated by LS using the numbers different from Alice's choices. Consequently, Alice can prove the falsification to CA.

A.3. Anonymity

No one can link the lottery to the player's identity. Since the winner of the lottery usually earns a big fortune, the true identity of the player must be concealed to prevent the winners from potential risks.

Proposition 6. *If Oscar or LS try to link to Alice's identity from her lottery ticker, he must fail.*

Proof. Since the lottery is in the form of $LT_f = \left[\mathrm{Ser}_f, f, E_{k_f}\left(\mathrm{Ser}_f, f, \beta_1, \beta_2, \ldots, \beta_t, DL_c\right)\right]$, Oscar can learn nothing but Ser_f and *f*. As we know that $\mathrm{Ser}_f = \mathrm{Ser}_{f-1} + \hat{r}_1 \bmod f$ and f is the amount of lottery tickets sold so far, no information related to Alice can be revealed.

On the other hand, the new mechanism adopts the concept of e-cash which can preserve the anonymity of the user. This helps that Alice is able to use *E_cash* to purchase lottery without revealing her identity. The main technique used to design anonymous digital cash is blind signature. That is, if LS tries to connect the *E_cash* to find the identity of Alice, LS must face the problem of solving factorization. Hence the new method can effectively guarantee the anonymity essential.

A.4. Random Generation

Each number within the predefined domain must contribute to the result equally.

Proposition 7. *No one can bias the generation of winning result.*

Proof. According to Eq. (2.2) and $\mathrm{PRNG}(\mathrm{Ser}_F) = \left\{a_1^*, a_2^*, \ldots, a_t^*\right\}$, the winning number set depends on the final result of Ser_F. Since each purchase comes from the Internet randomly, no one, including LS, can predict or bias the final result.

A.5. Public Verification

Players shall be able to monitor and check the winning result.

Proposition 8. *After purchasing a lottery ticket, Alice can check if her ticket has contributed to the winning numbers and verify the winning result.*

Proof. After LS sends lottery ticket LT_f to Alice, it publishes $\left(f, \mathrm{Ser}_f\right)$ on the public board immediately. Alice then can use Eq. (2.2) to check if $\hat{r}_1$ is counted in this play. Similarly, Alice also can get Ser_F from the public board and input it into PRNG( ) to generate the winning set. Then she can make sure if the result is correct or not by comparing the winning set she calculated with the announced one.

A.6. Privacy of Lottery

No one can learn of the choice of the player from the ticket except themselves.

Proposition 9. *No one, including LS, can know the choices of players except themselves.*

Proof. According to Eq. (2.1), we know that the new method utilizes the concept of blind signature to conceal choices of player. When receiving Alice's choices, LS learns nothing about the choices of Alice unless it can retrieve a' from $\alpha_j = r_j^e \cdot a_j' \bmod N$. To achieve this, LS must be able to solve the factorization problem in RSA cryptosystems. This has violated the first assumption. On the other hand, Oscar may intercept $E_{PK_{LS}}\left(\alpha_1, \alpha_2, \ldots, \alpha_t, \hat{\hat{r}}_1, r_2, E\_cash\right)$ or LT_f. Since these information are encrypted by the public key of LS and k_f, respectively, Oscar figures out nothing about Alice's choices under the assumption of Factorization problem and secure one-way hash function.

A.7. Fairness

No one can foresee the winning set except for guessing.

Proposition 10. *No one can predict the winning numbers before* DL_p.

Proof. According to Proposition 7, the input seed of PRNG( ) is contributed by all tickets, and each purchase of lottery is unpredictable and occasional. This implies that no one, including LS, can know what the result is before DL_p.

A.8. Convenience

As described in purchase-issue phase, it is clear that a player who possesses enough digital cash and can access to the Internet is able to purchase lottery tickets. This implies that the new method can guarantee this essential to enhance the practicability.

A.9. Without Online TTP

The security of electronic lottery mechanism shall not depend on a trusted third party since it is hard to guarantee that TTP can be accessed all the time. Furthermore, the performance of TTP must be the bottleneck of the whole system. Hence, the new method is claimed to remove this component. As described in Section II, the new method introduces an offline CA instead of TTP. And CA is just involved in the judgment while disputes occur. Consequently, this requirement can be achieved in our scheme.

A.10. Without Pre-registration

For a player to purchase a ticket in conventional lottery games, it is unnecessary for him/her to register at any seller or drawer in advance. This essential must be preserved to make the e-lottery games more realistic. The only request is that all players must possess an account at a legal bank which can issue *E_cash* [9, 10, 11]. In fact, whenever someone wants to join an e-commerce model, this request is normal and acceptable.

A.11. t-out-of-n choice

For each lottery ticket, players can exactly pick *t* numbers from the pre-defined domain non-iteratively. This can significantly enhance the efficiency of number selection and prevent players from choosing more numbers in a ticket to increase the winning probability.

Proposition 11. *If Alice chooses more than t numbers to increase her winning probability, LS will detect this intention and terminate the transaction.*

Proof. In Step 3 of purchase-issue phase, LS uses its private key to sign exactly *t* numbers. If Alice chooses and sends more than *t* numbers, LS must be able to detect this attempt immediately by Eq. (2.3). Consequently, Alice can choose exactly *t* numbers for each ticket.

Table 1. Comparisons with related works

Essentials	Methods					
	[9]	[5]	[6]	[8]	[11]	[Ours]
Robustness	Yes	No	Yes	Yes	No	Yes
Convenience	Yes	Yes	Yes	Yes	Yes	Yes
Correctness	Yes	Yes	Yes	Yes	Yes	Yes
Fairness	Yes	No	No	No	Yes	Yes
Privacy of lottery	No	Yes	Yes	No	Yes	Yes
Anonymity	Yes	No	No	No	Yes	Yes
On-line TTP	No	No	No	Yes	No	No
Pre-registration	No	Yes	No	No	No	No
Public verification	Yes	No	No	No	Yes	Yes
t-out-of-n choice	No	No	No	No	Yes	Yes

B. More Discussions

In the following, we compare several related works with our method to show the practicability. As illustrated in Table 1, the new method is able to achieve the essentials of general electronic lottery mechanisms. Especially, the new method can withstand the forgery attack which Lee and Chang mechanism suffered from. Aside from that, it adopts the concept of blind signature and digital cash to confirm the anonymity of players. This can lower the potential risk that a winner may be robbed. And, it conceals the choices of players. Even lottery sellers cannot learn the numbers the players have chosen. Without loss of generality, players must share the same prize while their tickets hit the same numbers. Hence, the proposition of lottery privacy is very important for guaranteeing the profit of players. Furthermore, the procedure of pre-registration is eliminated from the new mechanism. This makes e-lottery games easier to attract more participation. As to the essential of t-out-of-n choice, only [11] and our method can preserve this requirement. This functionality can effectively reduce the bandwidth consumption of the communication between players and LS.

Table 2. Computation overhead

Stage	Improved version of [11]		Ours	
	Player	Lottery Seller	Player	Lottery Seller
1st phase	None	$n\cdot\mathrm{I}+n\cdot\mathrm{E}$	None	None
2nd phase	$t\cdot\mathrm{E}+1\cdot\mathrm{H}+1\cdot\mathrm{S}+1\cdot\mathrm{A}$	$t\cdot\mathrm{E}+2\cdot\mathrm{H}+1\cdot\mathrm{S}+1\cdot\mathrm{A}$	$t\cdot\mathrm{E}+1\cdot\mathrm{H}+1\cdot\mathrm{S}+1\cdot\mathrm{A}$	$t\cdot\mathrm{E}+2\cdot\mathrm{H}+1\cdot\mathrm{S}+1\cdot\mathrm{A}$
3rd phase	None	None	None	None
4th phase	$t\cdot\mathrm{I}+1\cdot\mathrm{S}+1\cdot\mathrm{A}$	$1\cdot\mathrm{H}+2\cdot\mathrm{S}+1\cdot\mathrm{A}$	$1\cdot\mathrm{S}+1\cdot\mathrm{A}$	$t\cdot\mathrm{E}+(t+1)\cdot\mathrm{I}+1\cdot\mathrm{H}+2\cdot\mathrm{S}+1\cdot\mathrm{A}$

I: multiplicative inverse operation E: modular exponentiation H: hash function
S: symmetric encryption/decryption A: asymmetric encryption/decryption

To highlight the advantage of the new method, we further compare the improved version of [11] with our scheme in terms of computation overheads. The result is shown in Table 2. Main operations considered in Table 2 include the modular inverse, modular exponentiation, one-way hash function, and symmetric/asymmetric encryption/decryption.

In the first phase of Lee and Chang scheme, players need not to do anything, but LS has to compute $C=\sum_{i=1}^{n}(M/m_i)y_i a_i$ and $M_i=m_i^e \bmod N$, which needs n modular inverse operations and *n* modular exponentiation operations. Under the same situation, players and LS need to do nothing in our new method. This can effectively diminish the burden of LS.

In the claim phase (the 4th phase), the winner in [11] must perform t modular inverse operations, one symmetric decryption, and one asymmetric encryption for r_j^{-1}, $E_{k_j}(\text{Prize})$, and $E_{PK_{LS}}\left(\text{Ser}_f, f, LT_f, \left(r_1^{-1}, r_2^{-1}, \ldots, r_t^{-1}\right)\right)$. Under the same achievement, the new method outperforms [11] since the winner just has to perform one symmetric decryption and one asymmetric encryption. Undoubtedly, the lower computation overhead the client needs to spend, the higher population of player we can have. In particular, the explosive development of mobile communications has brought another revolution in e-commerce. More and more people prefer to access to the internet via mobile devices since they do not want to be bound to a fixed place. If the computation overhead from the e-lottery game is light, i.e. the mobile device can afford to support, players who surf on the Internet via mobile device may be interested in joining the games. For instance, they may enjoy this game to kill the time while they are traveling or waiting for something.

Nevertheless, in the case of the claim phase, the new method can not outperform the improved version of [11] in LS. The new method needs to perform additional $t \cdot \mathrm{E} + (t+1) \cdot \mathrm{I}$ to preserve the robustness in comparison with [11]. Generally speaking, only a few players can be the winners. That is, LS just needs to execute these additional operations for some specific players instead of for all players. This fact indicates that the increase of computation overhead in the new method is limited and acceptable. Further, while we consider one complete play of e-lottery game, the amount of overhead LS needs to perform is $n \cdot \mathrm{I} + (n+t) \cdot \mathrm{E}+3\mathrm{H}+3\mathrm{S}+2\mathrm{A}$ in [11] and $(t+1) \cdot \mathrm{I} + 2t \cdot \mathrm{E}+3\mathrm{H}+3\mathrm{S}+2\mathrm{A}$ in the new mechanism. Without loss of generality, we have known $t<<n$. Hence, we can conclude that our method outperforms [11] in the computation overheads of players and LS.

IV. Conclusions

As reported in [10, 11], e-lottery games will gather more and more attention and become a billion-dollar industry in the future. Hence, it is urgent and important for researchers to design a robust and efficient mechanism. In this article, we have pointed out the weakness of Lee and Chang method and provided improvements to fix it. Moreover, we have designed a brand-new e-lottery game mechanism which can preserve all the essentials. Particularly, the new method can resist the attack [11] suffered from and possess better performance than [11] does.

Acknowledgment

This work is supported by MOST104-2221-E-035-036-

References

[1] C.C. Chang and Y.P. Lai, "A flexible date attachment scheme on e-cash," *Computers and Security*, vol. 22, no. 2, pp. 160-166, 2003.

[2] T. ElGamal, "A public-key cryptosystem and a signature protocol based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469-472, 1985.

[3] H.F. Hwang and 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, pp. 39-46, October, 2006.

[4] C.C. Chang and J.S. Lee, "Robust t-out-of-n Oblivious Transfer Mechanism Based on CRT," *Journal of Network and Computer Applications*, vol. 32, pp. 226-235, 2009.

[5] D.M. Goldschlag and 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, pp. 214-226, February, 1998.

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

[7] 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, 1977.

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

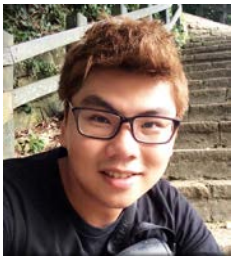
[9] J. Zhou and C. Tan, "Playing lottery on the Internet," *Proceedings of the Third International Conference on Information and Communications Security (ICICS 2001)*, China, pp.189-201, 2001.

[10] 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.

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

[12] N. Hoque, Monowar H. Bhuyan, R.C. Baishya, D.K. Bhattacharyya, J.K. Kalita, "Network attacks: Taxonomy, tools and systems" *Journal of Network and Computer Applications*, vol. 40, pp. 307-324, 2014.

Jung-San Lee received the BS degree in computer science and information engineering from National Chung Cheng University, Chiayi, Taiwan in 2002. He received his Ph.D. degree in computer science and information engineering in 2008 from National Chung Cheng University, Chiayi, Taiwan. Since 2012, he has worked as an associate professor in the Department of Information Engineering and Computer Science at Feng Chia University, Taichung, Taiwan. His current research interests include image processing, information security, and mobile communications.



Kuo-Jui Wei received MS degree in information engineering and computer science in Feng Chia University, Taichung, Taiwan in 2010. His current research interests include network security and cryptography.

Wei-Chiang Kao received MS degree in information engineering and computer science in Feng Chia University, Taichung, Taiwan in 2010. His current research interests include e-commerce and network security.