An Improved Non-Iterative Privacy Preservation Lotteries

Juan Huang†, Jihong Yan†, Yining Liu†

Guilin University of Electronic Technology, School of Mathematics and Computational Science, Guilin, China

Summary
In 2009, a non-iterative privacy preservation for online lotteries is proposed in IET Information Security. In this paper, we analyze the security flaw of Lee-Chan-Chang's scheme that can not provide the public verification. With Lagrange interpolating formula over F_p, the method of verifiable random number is introduced, which makes each purchaser involved equally in the generation of winning result. Trusted third party is no longer necessary, which eliminate the fairness bottleneck..

Key words:
Electronic lottery, public verification, trusted third party, Lagrange interpolating formula, verifiable random number

1. Introduction

In 2009, a non-iterative privacy preservation for online lotteries is proposed in IET Information Security by J.S lee, C.S Chan and C.C Chang [1], who claim their scheme achieve the following properties:

- Privacy. No one can learn the choices made by lottery players except the players themselves.
- Security. No one can counterfeit a winner or forge a winning lottery ticket to claim the prize.
- Accuracy. Players can obtain their lottery ticket with preferred numbers.
- Anonymity. The lottery ticket can not be linked to the identity of player.
- Fairness. Each ticket shall be equally contributed to the winning set.
- Convenience. Players need not sophisticated techniques or additional devices.
- Public verification. the player shall be able to observe the winning result and verify his lottery ticket.
- No online trusted third party needed.
- Non-iterative t-out-of-n choice.

In Lee-Chan-Chang's scheme, the main participants include a lottery issuer(LI), a player Alice, an off-line trusted third party(TTP) and a bank(B).

Lee-Chan-Chang's scheme constructs t-out-of-n lottery ticket using the method of robust non-interactive oblivious transfer protocol designed by Yi Mu et al. in 2003[2]. t-out-of-n oblivious transfer is defined as follows. Alice knows n messages and wants to send t of them to Bob, Bob gets t of them and knows which ones he has got, but Alice has no idea about which t messages Bob has received.

In Lee-Chan-Chang's scheme, LI knows and publishes n numbers and player Alice gets or selects t of n as his preferred number, then obtains corresponding ticket generated from these t number, LI knows nothing which t number has been chosen.

In 2009, some weakness of Mu et al.'s method is analyzed by Chin-Chen Chang and Jung-san Lee [3]. In [3], adversary Bob maybe obtain more than t number through selecting proper public keys (x_1, y_1) , (x_2, y_2), $\cdots, (x_n, y_n)$ determined with particular polynomial $y = f(x) = c_1 x + \cdots + c_t x^t \bmod p$ where $x_i = g^{r_i}$ $(1 \le i \le n)$, $c_1 = g^{r_0}$, $c_2 = 0$, $\cdots, c_t = 0$, and $r_0, r_1, \cdots, r_n$ are randomly selected by Bob. With n pairs of $(x_i, y_i) = (g^{r_i}, g^{r_0 + r_i}), (1 \le i \le n)$, Bob can easily obtain $a_1, a_2, \cdots, a_n$ possessed by Alice, and Alice cannot find such dishonest behavior, which destroys the fairness of the lottery protocol.

The above weakness has been easily improved in Lee-Chan-Chang's lottery scheme though Lee-Chan-Chang's lottery scheme is still based on Mu et al.'s oblivious transfer protocol. In [1], the $x-$coordinate of (x_1, y_1), (x_2, y_2), $\cdots, (x_n, y_n)$ are selected by LI in Initialization Phase, $y-$coordinate are selected by Alice in Purchase Phase, which make it impossible for constructing particular equation $y = f(x) = c_1 x + \cdots + c_t x^t \bmod p$ such that $(x_i, y_i) = (g^{r_i}, g^{r_0 + r_i}), (1 \le i \le n)$ unless LI and Alice collude.

But there still exist flaws of Lee-Chan-Chang's lottery scheme, listed as follows:

1. the protocol can not achieve real public verification
2. TTP is perhaps not necessary.

Manuscript received May 5, 2013
Manuscript revised May 20, 2013

The rest of this paper is organized as follows. In Section 2, we brief review Lee-Chan-Chang's non-iterative privacy preservation lotteries scheme, and give its flaws. The improved lottery without TTP is described in Section 3, which achieve real public verification. The discussion of the improved mechanism is given in Section 4, and conclusion is given in Section5.

2. Review of Lee-Chan-Chang' lottery scheme and security analysis

2.1 Review of Lee-Chan-Chang' lottery scheme

All notations in Lee-Chang's scheme are inherited throughout this paper.

Table 1 Notations:

Alice	The player
Prize	The first prize P_1 for the full-matching winner
p	a large prime number
g	a primitive element in F_p with order $q = p-1$
$PK_i / SK_i(.)$	RSA-based encryption/decryption with public/secret key of lottery issuer
$E_k / D_k(.)$	Symmetric encryption/decryption with secret key k
$H(x)$	The secure one-way hash function
SN_f	The serial number of lottery ticket f, where f is the number of tickets sold so far
$a_1, a_2, \cdots, a_t$	A set of t lottery numbers that player is expected to buy
E_cash	A fixed number of digital coins belonging to Alice
$W = \{win_1, \cdots, w$	A set of lottery number that determines the winner
T_p / T_c	Purchase deadline/Claim prize deadline

Lee-Chang's lottery scheme consists of three phases: purchase, drawing, and claim. LI sells ticket to player in the purchase phase, TTP draws a set of winning number in the drawing phase, and the winner claims the prize in the claim phase.

- *Initialization Set-UP*

TTP constructs a one-time secret number S and shares it with LI. LI selects n distinct random numbers $x_1, x_2, \cdots, x_n \in F_p$, and publishes n pairs of $(i, x_i), (i = 1,2,\cdots,n)$ on the bulletin board.

- *Purchase Phase*

Alice purchases a lottery ticket through the followings steps:

Step 1.1 Alice chooses t pairs of (a_i, x_i) from the bulletin board for $i = 1,2,\cdots,t$.

Step 1.2 For each (a_i, x_i), Alice generates a random number s_i and computes $y_i = g^{s_i} \bmod p$, $(i = 1,2,\cdots,t)$.

Step 1.3 Alice uses t pairs of (a_i, x_i) to construct a polynomial $f(x)$ by Lagrange interpolating polynomial.

$f(x) = b_1 x + b_2 x^2 + \cdots + b_t x^t \bmod p$.

Step 1.4 Alice substitutes other x_i into $f(x)$, corresponding y_i is obtained by computing $y_i = f(x_i) = b_1 x_i + b_2 x_i^2 + \cdots + b_t x_i^t \bmod p$, $(t+1 \le i \le n)$.

Step 1.5 Alice computes and sends $PK_{LI}((x_1, y_1), \cdots, (x_n, y_n), r, E\_cash)$ to LI, where r is a random number.

Step 2.1 Upon receiving the message sent by Alice, LI decrypts it and checks the validity of E_cash. If it is valid, he randomly selects t pairs of public keys from $\{(x_i, y_i)\}_{i=1}^n$, computes corresponding polynomial $\hat{f}(x) = \hat{b}_1 x + \cdots + \hat{b}_t x^t \bmod p$, LI can verify whether $\{(x_i, y_i)\}_{i=1}^n$ is genuine through substituting other $n-t$ public keys into $\hat{f}(x) = \hat{b}_1 x + \cdots + \hat{b}_t x^t \bmod p$, if the other $n-t$ equations hold, LI is convinced of $\{(x_i, y_i)\}_{i=1}^n$ from Alice.

Step 2.2 LI generates random numbers $r_1, r_2, \cdots, r_n$, computes $\alpha_i = g^{r_i} \bmod p$, $(i = 1,2,\cdots,n)$, and $M_i = i \,||\, H(i \,||\, SN_f \,||\, S)$.

Step 2.3 LI computes $w_i = M_i y_i^{r_i} \bmod p, (1 \le i \le n)$, constructs the session key $K_f = H(SN_f \,||\, r)$, and generates the f^{th} lottery ticket as

$LT_f = SN_f \| E_{K_f}[SN_f \| (\alpha_1, w_1) \| \cdots \| (\alpha_n, w_n)]$.

Step 2.4 LI connects LT_f to the one-way hash chain $C_f = H(LT_f \| C_{f-1})$, where $C_1 = H(LT_1 \| S)$. LI publishes (SN_f, C_f) on the bulletin board and sends LT_f back to Alice.

Step 3.1 After receiving the ticket, Alice generates $K_f = H(SN_f \| r)$ and decrypts ticket to get $(\alpha_1, w_1), \cdots, (\alpha_n, w_n)$, then she can obtain the receipt by computing $M_i = \frac{w_i}{\alpha_i^{s_i}} \bmod p$ for $i = 1,2,\cdots,t.$ and keeps $M_1, M_2, \cdots, M_t$ and LT_f in her databases.

- *Drawing Phase*

Assuming that the final $C_f = C$, after T_p , TTP performs the following procedure to generate a set of lottery numbers W :

Step 1: TTP first computes the random seed $d = C \bmod n$;

Step 2: TTP inputs d into the random function to generate W , $W = RF(d) = \{win_1, win_2, \cdots, win_t\}$;

Step 3: TTP publishes the result on the public board.

- *Claim Phase*

Assuming that Alice is the full-matching winner, i.e., $\{a_1, a_2, \cdots, a_t\} = W$, she claims the first prize as follows:

Step 1: Alice generates a random number r_1 and sends $PK_{LI}(SN_f, (a_1, M_1), \cdots, (a_t, M_t), r_1)$ to LI.

Step 2: when receiving the message from Alice, LI decrypts it, checks its validity, then computes $M_i^{'} = a_i \| H(a_i \| SN_f \| S)$, and compares it with the received $M_i, i = 1,2,\cdots,t$. If they are all valid, LI is convinced that Alice is the winner. LI constructs the secret key $K_f^{'} = H(SN_f \| r_1)$, and sends $E_{k_f^{'}}[\mathrm{Pr}\,ize]$ to Alice.

Step 3: Alice generates $K_f^{'} = H(SN_f \| r_1)$ to obtain the prize by decrypting $E_{k_f^{'}}[\mathrm{Pr}\,ize]$ without disclosing her identity.

2.2 Security analysis of Lee-Chan-Chang's lottery scheme

From the above description, we know there are two flaws in Lee-Chan-Chang's lottery scheme.

1) Lee-Chan-Chang's lottery scheme can not achieve public verification that they claim it. In order to realize the public verification, Lee-Chan-Chang's lottery scheme uses hash chain $C_f = H(LT_f \| C_{f-1})$ to involve all tickets, which has been introduced in [4,5]. In [6], the similar flaw has been discussed, but the improvement is still imperfect.

When Alice wants to verify if her contribution is involved to generate the winning result, she computes $C_f^{'} = H(LT_f \| C_{f-1})$ and compares it with C_f . Although it is computationally infeasible for LI to publish a fake hash value that equals to $C_f^{'}$, hash chain only ensures Alice's contribution is involved in generating C_f , which can not assure that LT_f is involved in generating the random seed d . Supposing the owner of $(f+1)^{th}$ lottery ticket colludes with LI to destroy the fairness, Alice has no idea to verify the seed is genuine or not.

If Alice want to verify whether her contribution C_f is counted in the process of generating d , she need collaborate with the owners of $LT_{f+1}, LT_{f+2}, \cdots, LT_{SN_f}$. If Alice holds the first ticket, in order for verification, she needs all players' collaboration. If LI and the last purchaser collude to destroy the fairness, other players cannot find this attack.

On the other side, there are numerous players in the lottery protocol. They are everywhere, it is impossible for all players to collaborate to verify the seed. So the public verify should make Alice independently verify whether its contribution is used to generate the random seed, even if all others refuse to cooperate with her.

2) The fairness of Lee-Chan-Chang's lottery scheme relies on TTP, which maybe the bottleneck of the protocol's security. In Drawing Phase, the random seed d is input into the trusted random function to generate the winning number. If TTP is corrupted or attacked by adversary, the whole security and fairness would collapse. The solution is to adopt the verifiable random number to burden the deputy of TTP, which ensure each participant to verify the random number generation without other's help. If Alice can verify his contribution is counted the

procedure of winning number generation, she is convinced that the result is fair. Otherwise, Alice reports her doubt to the authority organization.

3. Improved lottery scheme

3.1 Introduction of Verifiable Random Number

We assume there are n participants to work together to generate a random number which is fair for all. Each participant U_i chooses his (x_i, y_i) as his contribution to generate a verifiable random number. In order to ensure the existence of verifiable random number, the condition of $x_i \neq x_j, (i \neq j)$ is necessary.

With n pairs of (x_i, y_i) $(i = 1,2,\cdots,n)$, $P(x) = \sum_{i=1}^{n} y_i \prod_{j=1, j\neq i}^{n} \frac{x - x_j}{x_i - x_j} (\mathrm{mod}\ p)$ is generated with Lagrange interpolating formula, $P(x) = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ is determined by all participant. The influence of (x_i, y_i) is equal weighted, even if all participants collude but for U_i, the polynomial is still unpredictable for all, which ensures the fairness of scheme.

Then we input the coefficient concatenation of $P(x)$ into a secure hash function, i.e. $R = hash(a_{n-1} \| a_{n-2} \| \cdots \| a_0)$, we see secure hash function as a random oracle, the output is random. $P(x)$ and R should be published for verification.

In the process of generating verifiable random number, some participants maybe collude to get extra advantage. If U_i doubts if the result is fair, he can verify whether $y_i = P(x_i)$ and $R = hash(a_{n-1} \| a_{n-2} \| \cdots \| a_0)$ hold or not. The equation $y_i = P(x_i)$ ensures that (x_i, y_i) provided by U_i is involved in generating $P(x)$. Even if only U_i is honest, the result continues to be fair. From the viewpoint of information theory, each (x_i, y_i) has the same entropy as $a_{n-1} \| a_{n-2} \| \cdots \| a_0$, each participant has same weighting factor. As long as one participant is honest, $P(x)$ is unpredictable for all. And we assume hash function is Random Oracle, the result R is verifiable and random.

3.2 The improvement of Lee-Chan-Chang's Scheme

With the method of verifiable random number, the improvement of Lee-Chan-Chang's scheme is proposed, which consists of four phases: purchase, drawing, claim and verification. The improved scheme inherits the most of properties of Lee-Chan-Chang's scheme and does not rely on TTP to provide trusted computing, which eliminates the security bottleneck.

- *Initialization Phase*

LI selects a secret number S, and publishes n distinct random numbers $x_1, x_2, \cdots, x_n \in F_p$ on the bulletin board.

- *Purchase Phase*

Alice buys her lottery ticket as follows:

Step 1 : Alice selects t random number $s_1, s_2, \cdots, s_t$, computes $y_i = g^{s_i} \bmod p$, for $i = 1,2,\cdots,t$. Alice chooses her t favorite numbers from $x_1, x_2, \cdots, x_n$ as $x-$ coordinate, which are used to construct Lagrange interpolating polynomial

$$P(x) = \sum_{i=1}^{t} y_i \prod_{j=1, j\neq i}^{t} \frac{x - x_j}{x_i - x_j} = b_0 + b_1 x + \cdots + b_{t-1} x^{t-1} \bmod p$$

with $y_1, y_2, \cdots, y_t$ that are $y-$coordinate.

Alice computes $y_j = P(x_j) \bmod p$, where x_j are not used in constructing $P(x)$, then she sends $PK_{LI}((x_1, y_1),(x_2, y_2),\cdots,(x_n, y_n), r, E\_cash)$ to LI, where r is a random number.

Step 2: Upon receiving the message sent by Alice, LI decrypts it. If E_cash is valid, LI randomly selects t pairs from $\{x_i, y_i\}_{i=1}^{n}$ to retrieve a polynomial $\hat{P}(x)$, LI can verify $y_i = \hat{P}(x_i)$ with the others $n-t$ pairs of (x_i, y_i). If $n-t$ equations all hold, LI generates n random numbers, $r_1, r_2, \cdots, r_n$, computes $\alpha_i = g^{s_i} \bmod p$, $M_i = i \| H(i \| SN_f \| S)$, $w_i = M_i y_i^{r_i} \bmod p$, for $i = 1,2,\cdots,n$. Then LI constructs the session key $K_f = H(SN_f \| r)$, the f^{th} lottery ticket as $LT_f = SN_f \| E_{K_f}[SN_f \| (\alpha_1, w_1) \| \cdots \| (\alpha_n, w_n)]$.

LI publishes (SN_f, C_f) on the public board and sends LT_f back to Alice.

Step 3: After receiving the ticket, Alice generates K_f and decrypts the ticket with it. If the ticket is valid, she obtain the receipt by computing $M_i = \frac{w_i}{\alpha_i^{s_i}} \bmod p$, for $i = 1,2,\cdots,t$. Alice stores $M_1, M_2, \cdots, M_t$, and LT_f.

- *Drawing Phase*

In Drawing Phase, the purchase system is shut down to prevent dishonest player from forging the winning ticket, we suppose the number of tickets sold so far is m.

Step1: Alice sends $h_f = H(s_1, s_2, \cdots, s_t)$ to the bulletin board, where $s_1, s_2, \cdots, s_t$ are randomly chosen by herself in Purchase Phase.

Step2: With $(h_1, C_1), \cdots, (h_f, C_f), \cdots, (h_m, C_m)$, LI computes and publishes $R(x) = \sum_{i=1}^{m} C_i \prod_{j=1, j\neq i}^{m} \frac{x - h_j}{h_i - h_j} = a_0 + a_1 x + \cdots + a_{m-1} x^{m-1} \bmod p$, then the coefficients is input a random oracle to ensure the randomness, we use a secure hash function $H(x)$ as a random oracle to obtain the verifiable random number $VR = H(a_0 \| \cdots \| a_{m-1}) = \{win_1, win_2, \cdots, win_t\}$, which is published.

In fact, every volunteer can compute and verify the above procedure.

- *Verification Phase*

Alice substitutes his h_f into $R(x)$, and checks whether $R(h_f) = C_f$ holds or not, if she doubts the fairness of result generation.

If $R(h_f) = C_f$ and $VR = H(a_0 \| \cdots \| a_{m-1})$ all hold, Alice is convinced of his contribution (h_f, C_f) really involved in generating the winning result $\{win_1, win_2, \cdots, win_t\}$, which ensures the result is fair.

4. Discussion

The frame of improved scheme adopts Lee-Chan-Chang's design, previous excellent properties are inherited. In this subsection, we will only demonstrate verifiable randomness, public verification, fairness, no trusted third party, are achieved in the improved scheme.

1. randomness

The winning number is determined by the coefficients of $R(x)$, $R(x)$ is constructed by all ticket's $(h_1, C_1), \cdots, (h_f, C_f), \cdots, (h_m, C_m)$.

Since interpolating formula is information-theoretically secure, even if all purchasers collude but Alice, they have no idea to influence the generation of $R(x)$, i.e. the coefficients of $R(x)$ is still unpredictable for all. The output of $H(a_0 \| \cdots \| a_{m-1})$ is really random assuming secure hash function as random oracle.

2. public verification

C_f is published on the bulletin board in Purchase Phase, h_f is published in Draw Phase. Every one can check if the contribution of each ticket is involved in generating winning number. If any verification does not hold, any one can report it to the authority.

3. fairness

Fairness is closely related to randomness. If the winning number is unpredictable or random, the result is fair for all participants.

4. no trusted third party

Lee-Chan-Chang's scheme computes the seed of random function using hash chain, which make it impossible for Alice to verify his LT_f involved in the generation of the seed without other players' cooperation.

In the improved scheme, the $y-$coordinate of $R(x)$ is published at the end of purchase phase, $x-$coordinate of $R(x)$ is published in Draw Phase when the selling system has been closed. Unless all purchaser collude to control the result, nobody can predict $R(x)$ to obtain unfair advantage even if LI is corrupted. LI only provides computing capacity, is no longer a trusted third party. In fact, every volunteer can also burden this work. So the improved scheme need not trusted third party any more.

5. Conclusion

In this article, we propose an improved lotteries scheme, which achieves fairness, public verification, privacy, accuracy, security with verifiable random number based on Lagrange interpolating formula. The improvement does not rely on trusted third party to ensure the fairness, eliminate the security bottleneck.

References

[1] J.S. Lee, C.S Chan, C.C Chang. Non-iterative privacy preservation for online lotteries. IET Information Security, Vol.3(4): 139-147, 2009.

[2] Y. Mu, J. Zhang, V. Varadharajan, and Y.X. Lin, "Robust Non-interactive Oblivious Transfer," IEEE Communications

Letters, Vol. 7, No. 4, pp. 153-156, April 2003.
[3] Chin-Chen Chang, Jung-San Lee. Robust t-out-of-n oblivious transfer mechanism based on CRT. Journal of network and computer applications. Vol.32(2009): 226-235, 2009.
[4] S.S.M. Chow, L.C.K. Hui, S.M. Yiu and K.P. Chow, Practical electronic lotteries with offline TTP. *Computer Communications*, **29** (2006), pp. 2830–2840
[5] Chow, S.S.M., Hui, L.C.K., Yiu, S.M., Chow, K.P. An e-Lottery Scheme Using Verifiable Random Function. In ICCSA 2005. LNCS, vol. 3482, pp. 651–660. Springer, Heidelberg (2005)
[6] Yining Liu , Lei Hu , Heguo Liu, Using an efficient hash chain and delaying function to improve an e-lottery scheme, International Journal of Computer Mathematics, v.84 n.7, p.967-970, July 2007

Juan Huang received the M.S. degrees in Software Engineering from University of Electronic Science and Technology of China in 2012.