Computers and Electrical Engineering 49 (2016) 146–160

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

A novel lottery protocol for mobile environments ☆

Chin-Ling Chen [a,*], Mao-Lun Chiang [b], Wei-Chech Lin [a], De-Kui Li [c]

[a] Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung 41349, Taiwan, ROC
[b] Department of Information and Communication Engineering, Chaoyang University of Technology, Taichung 41349, Taiwan, ROC
[c] Department of Information Management, Liaocheng University, Liaocheng, Shandong, China

ARTICLE INFO

Article history:
Received 25 August 2014
Received in revised form 16 July 2015
Accepted 17 July 2015
Available online 8 August 2015

Keywords:
E-lottery
Fairness
Elliptic curve
Attack
Mutual authentication

ABSTRACT

In general, in order for individuals to take part in a lottery, they must purchase physical lottery tickets from a store. However, due to the popularity and portability of smart phones, this paper proposes a lottery entry purchase protocol for joint multi-participants in a mobile environment. This method integrates cryptology, including elliptic curve cryptography and public key infrastructure, enabling users to safely and fairly join a lottery via a mobile device. The lottery organization involves an untraceable tamperproof decryptor to generate the winning numbers, and the generation of those winning numbers is fair and publicly verifiable. All participants share an equal probability of winning the prize. Subsequently, a comparison table shows that the proposed protocol can withstand attacks and efficiently satisfy the known requirements in a mobile environment. In addition, this study also ensures public verification and mutual authentication.

1. Introduction

Lottery gambling is non-predictable [1–3] and its prizes vary in size. While all participants stand a chance of winning, it is impossible to know which participant will win each lottery. The actual value of the prize will vary, depending on how many people take part in each lottery, and how many winners there are for each draw. This form of gambling thus remains fascinating and exciting for many people. Participants must select several numbers when they purchase each lottery ticket, and the lottery organization (LO) randomly generates the winning number. If the numbers selected by a participant match the randomly selected winning numbers, then they will have won the lottery. Sometimes, however, different participants select the same winning numbers, and in this case the prize money will be shared between them. If the prize is not claimed, the prize will be added to the prize money generated for the next draw, often called "roll-over". This is an extremely powerful method to entice participant to purchase lottery tickets.

With the rapid growth and development of portable devices (such as the cell phone or PDA) [4–7], mobile commerce has becomes a focal issue. At present, a method for implementing a fair and secure joint purchase e-lottery protocol via a mobile environment has still not been proposed. This study thus reviewed some lottery schemes to propose just such a solution. In 2005, Chow et al. [8] proposed an e-lottery scheme using a verifiable random function. Lee and Chang [9] proposed an

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. W-H-Hsieh.

* Corresponding author.
E-mail addresses: clc@mail.cyut.edu.tw (C.-L. Chen), mlchiang@cyut.edu.tw (M.-L. Chiang), weichech@gmail.com (W.-C. Lin), jerryinkorea@gmail.com (D.-K. Li).

http://dx.doi.org/10.1016/j.compeleceng.2015.07.016
0045-7906/

electronic t-out-of-n lottery on the Internet in 2009. Even though the winning prize probability is very low [10], the participants can adopt the following two methods to enhance their probability of winning.

- The coordinator can join other participants to purchase one lottery ticket if the coordinator and participant just want to spend a small amount of money.
- If the coordinator wants to purchase sequential numbers of lottery tickets, the coordinator can invite other participants in order to collect more money.

The previous schemes [9–11] offered a participant lottery purchases on the Internet, but could not support an efficient joint purchase protocol in a mobile environment.

So, the participants had to collect funds and commit a coordinator to purchase many lottery tickets in order to increase the probability of winning the lottery. A fair and joint e-lottery protocol cannot depend on the presupposition that the coordinator can be trusted. The chances for any participant to win the prize must be equal, and that participant must be able to claim his/her own prize. However the important issue is that the participant can be awarded the prize individually, even when the coordinator denies the committed activity. Moreover, this study noted that the elliptic curve is suitable for mobile environments [12,13]. Elliptic curve cryptography (ECC) can use a small key size to achieve the same security level of a discrete logarithm problem (DLP). For example, 160-bit ECC and 1024-bit RSA have the same security level [14]. In 2004, Liaw [15] proposed an untraceable decryptor which can randomly input a selector with memory, and store the input data in a buffer. Furthermore, it can be designed to output data when receiving n records, or at a specific pre-set time. If it receives an enabling signal, the public key decryptor will select a pair of parameters for itself automatically, and the private key cannot be modified because it is stored in the PROM.

In a lottery protocol, one of the fundamental characteristics is that no one can predict or control the outcome. When a lottery is run, participants must believe that the lottery was fair and secure. In addition, a fair and secure joint purchase e-lottery protocol in a mobile environment is also necessary. Therefore, this study proposes the following requirements for a good joint purchase lottery protocol for a mobile environment:

- Defend against attacks: The proposed protocol must be secure against known attacks (such as replay attack, man-in-the-middle attack, and impersonation attack).
- Anonymity: The coordinator should be anonymous to ensure a fair transaction during the ticket purchase.
- Verifiability: All legal lotteries and the generation of the winning numbers must be publicly verifiable.
- Fairness: The probability of each participant winning must be the same.
- Accuracy: The prize should be rewarded to the real winner/s and genuine proportional prizes allotted.

The remainder of this paper is arranged as follows. Section 2 presents the preliminaries of bilinear pairings and related mathematical assumptions. Section 3 describes the proposed efficient joint purchase protocol. Security analyses of this protocol are presented in Section 4. Section 5 offers discussion of the performance analysis. Conclusions are presented in Section 6.

2. Preliminary

This section will introduce bilinear pairings and related methodologies. Bilinear pairings are defined on elliptic curves for efficient ID-based cryptosystems [16–20].

2.1. Bilinear pairing

G_1 is an additive cyclic group with a large prime order q, and G_2 is a multiplicative cyclic group with the same order q. G_1 is a subgroup of the additive group of points on an elliptic curve over a finite field $E(F_p)$, and G_2 is a subgroup of the multiplicative group over a finite field. P is a generator of G_1. The detailed descriptions of groups, maps and other parameters are given in [16–20]. A bilinear pairing is a map $e : G_1 \times G_1 \rightarrow G_2$, and satisfies the following properties:

(1) Bilinear: $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in G_1$, and $a, b \in Z_q^*$.
(2) Non-degenerate: there exists $P, Q \in G_1$ such that $e(P, Q) \neq 1$.
(3) Computability: For all $P, Q \in G_1$, there is an efficient algorithm to compute $e(P, Q)$.

A bilinear map which satisfies the above three properties is called an admissible bilinear map.

2.2. Related mathematical assumptions

Bilinear pairings have the following problems and assumptions defined on elliptic curves.

(1) Decision Diffie-Hellman (DDH) problem: Given $xP, yP, zP \in G_1$ for some $x, y, z \in Z_q^*$, let $e(xP, yP)$ and $e(P, zP)$. Hence, the DDH problem is easily addressed in G_1.
(2) Computational Diffie-Hellman (CDH) problem: Given $P, xP, yP \in G_1$, it is difficult to compute $xyP \in G_1$; hence, the CDH problem is difficult to address in G_1.
(3) Bilinear Diffie-Hellman (BDH) assumption: Let (P, xP, yP, zP) for some $x, y, z \in Z_q^*$; computing $e(P, P)^{xyz} \in G_2$ is difficult.

3. The proposed scheme

This section will describe an efficient joint purchase protocol based on an elliptic curve for mobile environments. The method consists of five phases: the initial phase, the joint participant phase, the ticket purchase phase, the winning number generation phase and the lottery prize claim phase. There are five parties in the proposed protocol:

- Coordinator (C): The coordinator collects participants' information and commits to buying lottery tickets.
- Participant (P): One of the participants using a mobile device to participate in the lottery.
- Participant Group (PG): All of the participants (including the coordinator).
- Lottery Proxy Center (LPC): A trustee web site that is committed to coordinating the lottery.
- Lottery Originator (LO): An organization deploying an LPC provides the lottery prizes and holds the lottery; The LO also sets up an untraceable and tamperproof decryptor [14] to generate winning numbers for each lottery draw.

In order to hold a fair and verifiable lottery, the LO is involved in the proposed protocol, generating the winning number, for public verification. Cryptology, such as symmetrical encryption and hash chain, is applied in the proposed protocol. The Internet Secure Socket Layer (SSL) protocol is applied to protect the end-to-end communications for lottery issuing and casting. A scenario involving the proposed protocol is shown in Fig. 1.

(1) LO ⟷ P: The participant uses his/her identity to register to the LO. The LO sends back a permit ticket.
(2) C ⟷ P: The coordinator sends a request message for ticket purchases to other participants. The participants then respond to a hidden identity message.
(3) C ⟶ LPC: The coordinator proposes a purchase request including a participant's information, to purchase lottery tickets with participants' information.
(4) LPC ⟶ PG: The LPC sends shadows to the participants' group, respectively.
(5) LPC ⟶ LO: The LPC sends shadows to the participants' group, respectively.
(6) LO ⟶ P: The LO generates winning numbers by untraceable decryptor, and then publishes the winning numbers.
(7) P ⟷ LO: The winning participant uses his/her shadow to claim the winning prize. Finally, the LO returns an invoice to the participant.

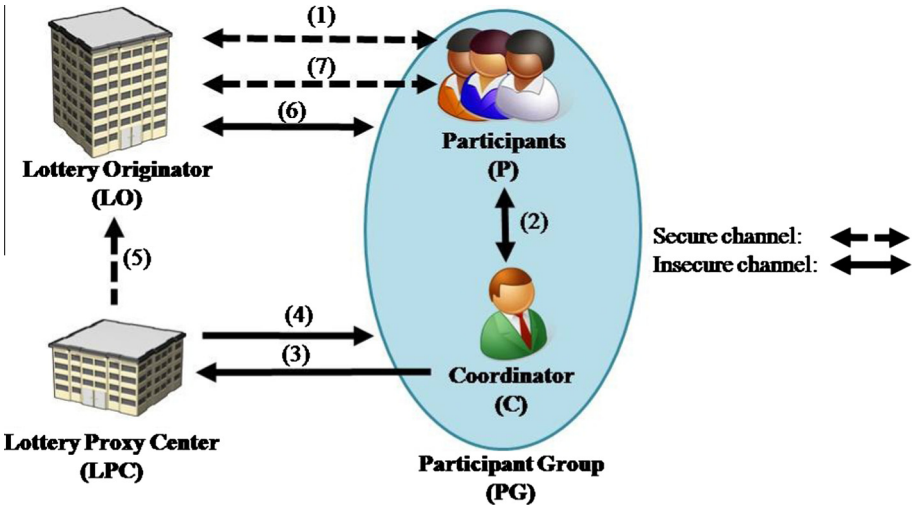

Fig. 1. Structure of our protocol.

The following notations are used in the proposed protocol:

r_x	the random number generated by X, $r_X \in Z_q^*$
n	a large number where $n = p \cdot q$, $\varphi(n)$ is a Euler Totient function and $\varphi(n) = (p-1)(q-1)$. The (p, q) is a pair of large prime numbers
$h_1(\cdot)$	a one way hash function, $h_1 : \{0,1\}^* \times G_1 \rightarrow \{0,1\}^k$, where k is the fixed output length [21]
$h_2(\cdot)$	the map-to-point function, $h_2 : \{0,1\}^* \rightarrow G_1$
$R(\cdot)$	the real random number function [22]
$PRG(\cdot)$	the pseudo-random number generation function
ID_i	the identity of user i
H_{IDi}	the hash value of the user i identity, where $H_{IDi} = h_2(ID_i)$
s	the LO and LPC's secret key, $s \in Z_q^*$
d_{ID}	the private identity of user i
$CK_{c,i}$	the session key between coordinator and user i
$E_k(M)/Dk(M)$	use symmetrical key k to encrypt or decrypt message M
$S_{SKX}(M)$	use X's private key SK_X to sign message M
$V_{PKX}(M)$	use X's public key PK_X to verify message M
Sig_i	the ith signature
TK_i	the permit ticket of the ith purchase
SHK_X	X's shadow
SHK_{XY}	the shadow key between X and Y
$f(x)$	a polynomial function generated for embedding the LO's private key SK_{LO}, where $f(x) = c \cdot x + SK_{LO} \bmod \varphi(n), c \in [1, \varphi(n)]$
Q	the point of group G_1
N_X	the nonce generated by X, and the $N_X \in Z_q^*$
Num	the lottery number selected by coordinator, where $Num = (no_1, no_2, \ldots, no_j)$
ta, tp, tc	the time of winner announcement; deadline of prize claim request; deadline for collecting information between coordinator and participants
$timestampX$	X's timestamp
$x[R]$	the x coordinate of the R point on the elliptic curve [23]
Inv_X	X's invoice
m	the number of participants
$\|\|$	the concatenation operation
$\oplus$	the exclusive OR operation
$A \stackrel{?}{=} B$	comparing whether or not A is equal to B
- - - →	the secure channel (for example: SSL channel)
⟶	the insecure channel

3.1. Construct session key model

In the initial phase, the participant i should register to be a legal user. The LO then issues a purchasing permit, public identity and private identity for participant i. The scenario of the initial phase is shown in Fig. 2.

Step 1: The LO generates a secret key s and sends it to LPC; the LO also selects a finite field F_q over a large odd prime $q > 2^{160}$, and then an elliptic curve function is used: $EC_q(a,b) : y^2 \equiv x^3 + ax + b (\bmod\ q)$ with the order q over F_q, where $a, b \in F_q$, and $4a^3 + 27b^2 \neq 0 \bmod q$ [16], with the public point Q with the order n over $EC_q(a,b)$. The LO computes $Q_{pub} = s \cdot Q$. The $E_k(\cdot)$ and $D_k(\cdot)$ are the symmetric encryption and decryption algorithms [16], respectively. Then it publishes: $EC_q(a,b), Q, Q_{pub}, E_k(\cdot), \text{and}, D_k(\cdot)$.

Step 2: The participant i sends his/her real identity ID_i to the LO for registration.

Step 3: First, the LO checks the real identity, and then generates the public identity H_{ID_i}, private identity d_{ID_i}, and purchases permit ticket TK_i.

$$H_{ID_i} = h_2(ID_i) \tag{1}$$
$$d_{ID_i} = s \cdot H_{ID_i} \tag{2}$$
$$C_{TK_i} = E_{SK_{LO}}(d_{ID_i}) \tag{3}$$
$$SG_i = S_{SK_{LO}}(C_{TK_i}) \tag{4}$$
$$TK_i = (C_{TK_i}, SG_i) \tag{5}$$

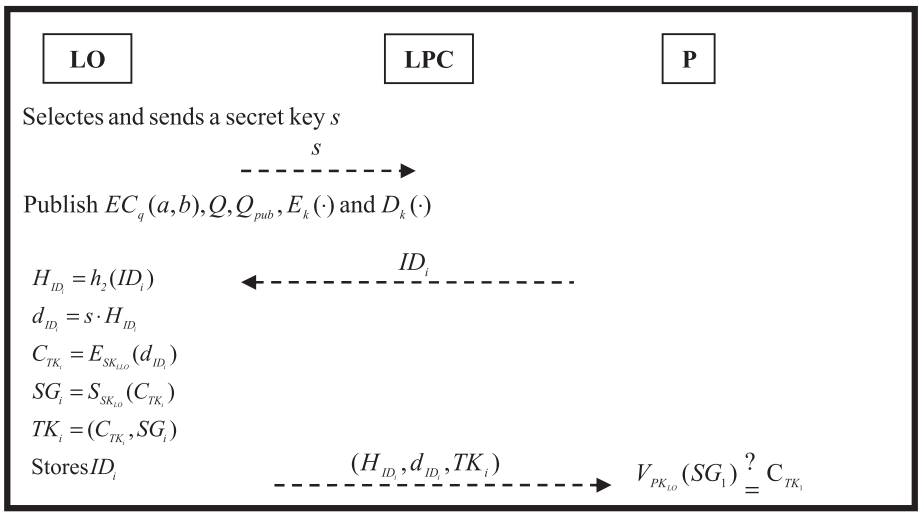

Fig. 2. Overview of the initial phase.

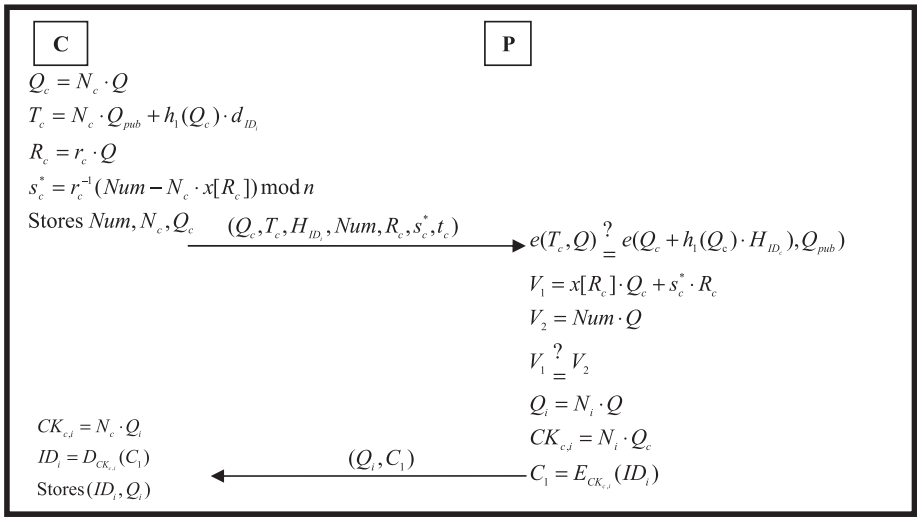

Fig. 3. Overview of the joint participant phase.

The LO stores ID_i, and then sends the initial messages $(H_{ID_i}, d_{ID_i}, TK_i)$ to participant i.

Step 4: Upon receiving the initial message, participant i verifies ticket TK_i

$$V_{PK_{LO}}(SG_1) \stackrel{?}{=} C_{TK_1} \tag{6}$$

If the equality holds, then participant i uses TK_i to purchase a lottery entry. Afterward, the LO and LPC can verify the participant's identity via ticket TK_i.

3.2. Joint participant phase

In the joint participant phase, coordinator C broadcasts a request message to other participants. If the other participators agree to the coordinator's request, they will respond with a message to the coordinator. The scenario of the joint participant phase is shown in Fig. 3.

Step 1: The Coordinator C chooses a nonce N_c and a point Q of the group G_1. The coordinator then computes Q_c and T_c:

$$Q_c = N_c \cdot Q \tag{7}$$

$$T_c = N_c \cdot Q_{pub} + h_1(Q_c) \cdot d_{ID_c} \tag{8}$$

The coordinator selects a random number r_c and a number *Num* of the lottery to generate a signature s_c^*:

$$R_c = r_c \cdot Q \tag{9}$$

$$s_c^* = r_c^{-1}(Num - N_c \cdot x[R_c]) \bmod n \tag{10}$$

The coordinator repeatedly stores *Num*, N_c and Q_c in the database and broadcasts request messages $(Q_c, T_c, H_{ID_c}, Num, R_c, s_c^*, t_c)$ to other participants.

Step 2: Upon receiving the request message, participant *i* checks if the request has been made before the collect deadline time t_c. Next, the participant checks the coordinator's legality:

$$e(T_c, Q) \stackrel{?}{=} e(Q_c + h_1(Q_c) \cdot H_{ID_c}), Q_{pub}) \tag{11}$$

If the equality holds, then participant *i* checks the lottery number *Num*:

$$V_1 = x[R_c] \cdot Q_c + s_c^* \cdot R_c \tag{12}$$

$$V_2 = Num \cdot Q \tag{13}$$

$$V_1 \stackrel{?}{=} V_2 \tag{14}$$

Participant *i* chooses a nonce N_i and computes Q_i:

$$Q_i = N_i \cdot Q \tag{15}$$

Participant *i* generates the session key $CK_{c,i}$ between coordinator C and participant *i* for encrypting the participant's information:

$$CK_{c,i} = N_i \cdot Q_c \tag{16}$$

$$C_1 = E_{CK_{c,i}}(ID_i) \tag{17}$$

Finally, participant *i* sends the response message (Q_i, C_1) to the coordinator *C*.

Step 3: Upon receiving the response message, coordinator *C* computes the session key $CK_{c,i}$ and decrypts C_1:

$$CK_{c,i} = N_c \cdot Q_i \tag{18}$$

$$ID_i = D_{CK_{c,i}}(C_1) \tag{19}$$

The coordinator stores (ID_i, Q_i) in the database.

3.3. Lottery ticket purchase phase

3.3.1. The lottery ticket purchase procedure

In this procedure, the coordinator integrates the participants' information into the purchase request for the LPC. The scenario is shown in Fig. 4.

Step 1: After the t_c, coordinator *C* generates the purchase message M_{buy} with participants' information:

$$M_{buy} = (ID_1 \| ID_2 \| \ldots \| ID_m \| Q_1 \| Q_2 \| \ldots \| Q_m) \tag{20}$$

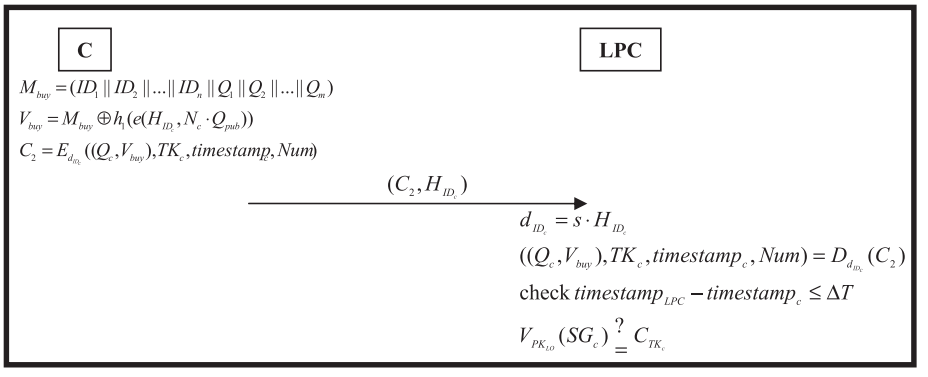

Fig. 4. Overview of the lottery purchase procedure.

$$V_{buy} = M_{buy} \oplus h_1(e(H_{ID_c}, N_c \cdot Q_{pub})) \tag{21}$$

Coordinator C uses his/her private identity to encrypt the purchase information $((Q_c, V_{buy}), TK_c, timestamp_c, Num)$, where $TK_c = (C_{TK_c}, SG_c)$ issued by LO:

$$C_2 = E_{d_{ID_c}}((Q_c, V_{buy}), TK_c, timestamp_c, Num) \tag{22}$$

Coordinator C sends purchase message (C_2, H_{ID_c}) to the LPC for lottery ticket purchase.

Step 2: The LPC uses secret key s and H_{IDc} to decrypt C_2:

$$d_{ID_c} = s \cdot H_{ID_c} \tag{23}$$

$$((Q_c, V_{buy}), TK_c, timestamp_c, Num) = D_{d_{ID_c}}(C_2) \tag{24}$$

The LPC checks if $timestamp_{LPC} - timestamp_c \leqslant \Delta T$.
Upon receiving SG_c and C_{TKc} from TK_c, the LPC then verifies:

$$V_{PK_{LO}}(SG_c) \stackrel{?}{=} C_{TK_c}. \tag{25}$$

3.3.2. The lottery ticket purchase procedure

Upon receiving the purchase message, the LPC verifies the coordinator's identity, generates the lottery for the participant group, and then sends the lottery numbers to participants, respectively. The scenario is shown in Fig. 5.

Step 1: The LPC extracts the participants' information M_{buy} from V_{buy}:

$$M_{buy} = V_{buy} \oplus h_1(e(d_{ID_c}, Q_c)) = (ID_1 \| ID_2 \| \ldots \| ID_m \| Q_1 \| Q_2 \| \ldots \| Q_m) \tag{26}$$

$H_{ID_1} = h_2(ID_1)$, for $i = 1$ to m, where m is the number of participants.
The LPC then selects a nonce N_{RPC} and generates K_i as participants' shadows SHK_i for claiming the prize:

$$SH_i = f(H_{ID_i})(-H_{LO}/(H_{ID_i} - H_{LO})) \bmod \phi(n), \text{for } i = 1 \text{ to } m$$

$$K_i = (N_{LPC} \oplus H_{ID_i})^{PK_{LO}} \bmod n, \text{ for } i = 1 \text{ to } m \tag{27}$$

$$SHK_i = K_i^{SH_i} \bmod n, \text{ for } i = 1 \text{ to } m \tag{28}$$

The LPC generates the RQ_{LPC} and ST_j in order for participants to verify the LPC's identity:

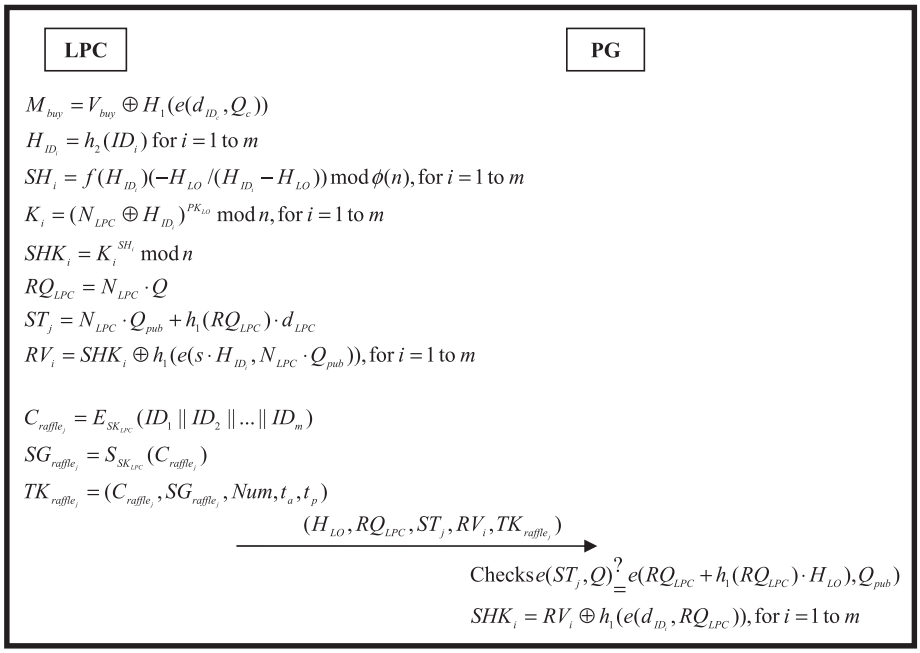

Fig. 5. Overview of the LPC lottery issues procedure.

$$RQ_{LPC} = N_{LPC} \cdot Q \tag{29}$$

$$ST_j = N_{LPC} \cdot Q_{pub} + h_1(RQ_{LPC}) \cdot d_{LPC} \tag{30}$$

To ensure that the shadow is mapped to the true participant, the LPC hides the lottery SHK_i in RV_i by the participant's public identity H_{ID_i} and public point Q_{pub}. The participant extracts his/her own shadow SHK_i by using the secret key s and public identity H_{ID_i}:

$$RV_i = SHK_i \oplus h_1(e(s \cdot H_{ID_i}, N_{LPC} \cdot Q_{pub})), \text{ for } i = 1 \text{ to } m \tag{31}$$

At last, the LPC generates the tickets of lottery TK_{raffle_j} as proof that the participants possess their lottery tickets:

$$C_{raffle_j} = E_{SK_{LPC}}(ID_1 \| ID_2 \| \ldots \| ID_m) \tag{32}$$

$$SG_{raffle_j} = S_{SK_{LPC}}(C_{raffle_j}, Num, t_a, t_p) \tag{33}$$

$$TK_{raffle_j} = (C_{raffle_j}, SG_{raffle_j}, Num, t_a, t_p) \tag{34}$$

The LPC sends lottery message $(H_{LO}, RQ_{LPC}, ST_j, RV_i, TK_{raffle_j})$ to the participant group.

Step 2: Upon receiving the lottery message, the participants check if the message is round or not:

$$\text{Check } e(ST_j, Q) \stackrel{?}{=} e(RQ_{LPC} + h_1(RQ_{LPC}) \cdot H_{RO}), Q_{pub}) \tag{35}$$

If the equality holds, the participants get their shadows SHK_i with the private identity d_{IDi}:

$$SHK_i = RV_i \oplus h_1(e(d_{ID_i}, RQ_{LPC})), \text{ for } i = 1 \text{ to } m \tag{36}$$

3.3.3. Storage of purchase information by LO procedure

The LPC sends participants' information to the LO. The LO generates the shadow key by the participant information and stores it in the database. Fig. 6 shows the scenario of storing purchase information.

Step 1: The LPC generates shadow key $SH_{i,LO}$:

$$SH_{i,LO} = f(H_{LO})(-H_{ID_i}/(H_{LO} - H_{ID_i})) \bmod \phi(n), \text{for } i = 1 \text{ to } m \tag{37}$$

and integrates K_i into K and $SH_{i,LO}$ into SH:

$$K = (K_1 \| K_2 \| \ldots \| K_m), \text{for } i = 1 \text{ to } m \tag{38}$$

$$SH = (SH_{1,LO} \| SH_{2,LO} \| \ldots \| SH_{m,LO}), \text{for } i = 1 \text{ to } m \tag{39}$$

The LPC sends $(Num, N_{LPC}, M_{buy}, K, SH)$ to the LO via secure channel.

Step 2: Upon receiving the message, the LO uses $SH_{i,LO}$ and K_i to compute $T_{i,LO}$:

$$T_{i,LO} = K_i^{SH_{i,LO}}, \text{for } i = 1 \text{ to } m \tag{40}$$

The LO stores $(Num \| N_{LPC} \| M_{buy} \| K \| T_{1,LO} \| T_{2,LO} \| \ldots \| T_{m,LO})$ in the database.

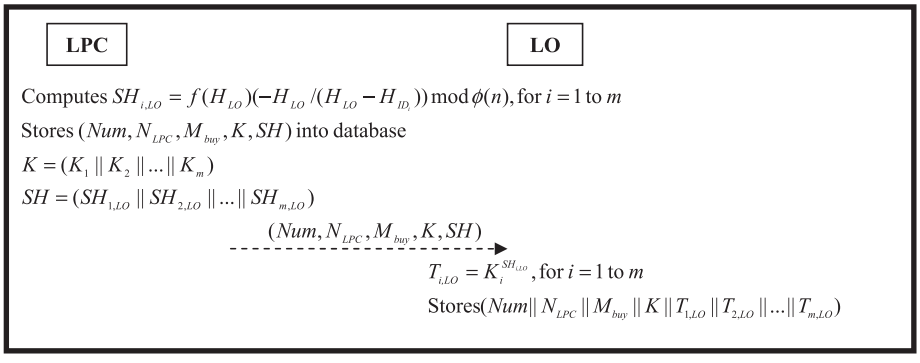

Fig. 6. Overview of the LO stores purchase information procedure.

3.4. Winning number generation phase

After the winner announcement deadline, the LO sends k numbers (i.e. 1, 2, ..., 59) [1] to the decryptor for the generation of the winning numbers. The scenario of the decryptor generating the winning numbers is shown in Fig. 7.

Step 1: Upon receiving the 59 numbers from the LO, the decryptor generates a new public/private key $(e_p, n_p)/d_p$ [23], and then selects a random number t_i by real random function [22], for $i = 1$ to k.

Step 2: The decryptor uses t_i and the public key (e_p, n_p) to generate M_i:

$$M_i = t_i^{e_p}(no_i) \bmod n_p, \quad \text{for } i = 1 \text{ to } k \tag{41}$$

$$M = (M_1 \| M_2 \| \dots \| M_k) \tag{42}$$

It then selects 6 winning numbers $V_1, V_2, \dots, V_6$ by pseudo-random number generating function $PRG()$:

$$V_j = PRG(M), \quad \text{for } j = 1 \text{ to } 6 \tag{43}$$

The decryptor uses private key d_p to sign V_j:

$$V'_j = (V_j)^{d_p} \cdot t_j^{-1} = (no_j)^{d_p} \bmod n_p, \ \text{for } j = 1 \text{ to } 6 \tag{44}$$

The decryptor then publishes $(V'_1 \| V'_2 \| \dots \| V'_6 \| M \| e_p \| d_p \| n_p)$ for public verification. Moreover, the decryptor sends $(V'_1 \| V'_2 \| \dots \| V'_6 \| e_p \| n_p)$ to the LO.

Step 3: The LO uses the public key (e_p, n_p) to decrypt:

$$wno_j = (V_j)^{e_p} \bmod n_p = no_i, \text{for } j = 1 \text{ to } 6 \tag{45}$$

and then publishes the winning numbers $(wno_1, wno_2, \dots, wno_6)$.

3.5. Lottery prize claim phase

In this phase, the winning participant claims the prize if his/her number matches the winning number. The LO uses the relative shadow to check the participant's identity, which is already in the database; if it matches, the LO grants the claim into his/her credit and generates an invoice for the winning participant. In Fig. 8, the participant claims the prize from LO by his/her shadow and ticket.

Step 1: Before the claim deadline t_p, participant i must generate the claim message with his/her shadow SHK_i, private ID_i and TK_{raffle_j} to claim the prize:

$$U_{i,WIN} = SHK_i \oplus h_1(e(H_{ID_i}, N_i \cdot Q_{pub})) \tag{46}$$

$$C_3 = E_{d_{ID_i}}((Q_i, U_{i,WIN}), TK_{raffle_j}, timestamp_{i,WIN}) \tag{47}$$

To prove the participant has claimed the prize, the participant must generate the signature by his/her shadow SHK_i:

$$R_i = r_i \cdot Q \tag{48}$$

$$s_i^* = r_i - 1(SHK_i - N_i \cdot x[R_i]) \bmod n \tag{49}$$

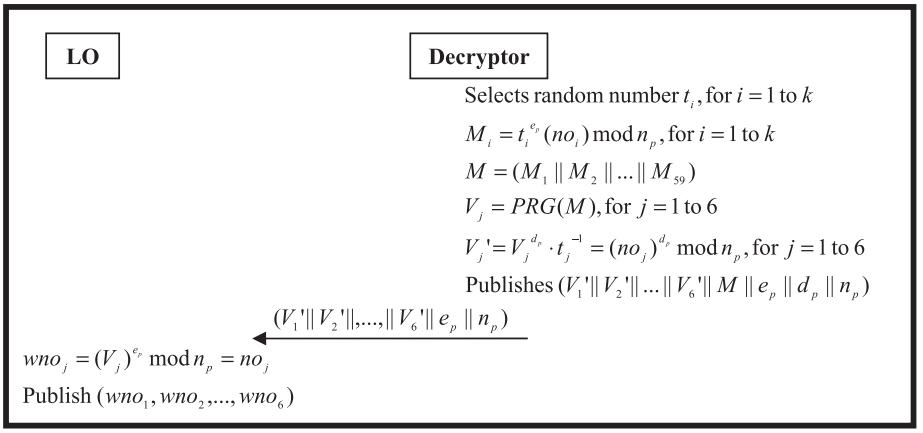

Fig. 7. Overview of the decryptor winning numbers generating phase.

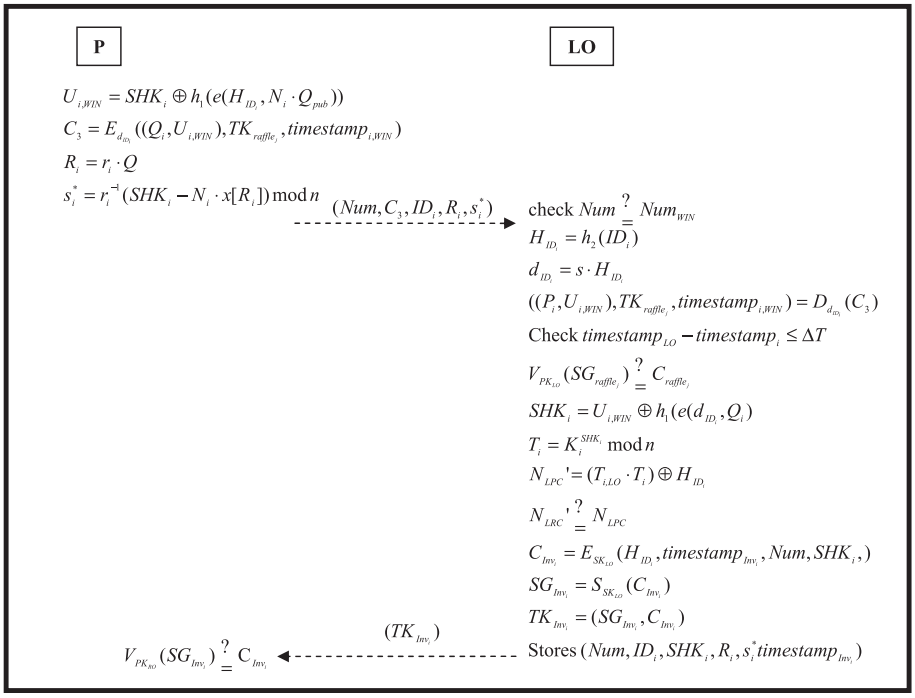

Fig. 8. Overview of the lottery prize claim phase.

The LPC then sends $(Num, C_3, ID_i, R_i, s_i^*)$ to the LO via secure channel.

Step 2: The LO first checks if the *Num* and ID_i exist in the database. If they do not, it rejects the request. Next, the LO uses *Num* to find if the consistent lottery information exists in the database and then checks the participant's identity and number:

$$Num \stackrel{?}{=} Num_{WIN} \tag{50}$$

The LO recovers the private identity d_{IDi} from the database by the identity ID_i:

$$H_{ID_i} = h_2(ID_i) \tag{51}$$
$$d_{ID_i} = s \cdot H_{ID_i} \tag{52}$$
$$((P_i, U_{i,WIN}), TK_{raffle_j}, timestamp_{i,WIN}) = D_{d_{ID_i}}(C_3) \tag{53}$$
$$\text{Check } timestamp_{LO} - timestamp_i \leqslant \Delta T \tag{54}$$
$$V_{PK_{LO}}(SG_{raffle_j}) \stackrel{?}{=} C_{raffle_j} \tag{55}$$
$$SHK_i = U_{i,WIN} \oplus h_1(e(d_{ID_1}, Q_i) \tag{56}$$
$$T_i = K_i^{SHK_i} \bmod n \tag{57}$$
$$N'_{LPC} = (T_{i,LO} \cdot T_i) \oplus H_{ID_i} \tag{58}$$
$$\text{Check } N'_{LRC} \stackrel{?}{=} N_{LPC} \tag{59}$$

If the above verifications hold, the LO dispatches the prize to the winner's credit, and computes invoice C_{Inv_i}:

$$C_{Inv_i} = E_{SK_{LO}}(H_{ID_i}, timestamp_{Inv_i}, Num, SHK_i) \tag{60}$$
$$SG_{Inv_i} = S_{SK_{LO}}(C_{Inv_i}) \tag{61}$$
$$TK_{Inv_i} = (SG_{Inv_i}, C_{Inv_i}) \tag{62}$$

Finally, the LO stores the draw information $(Num, ID_i, SHK_i, R_i, s_i^* timestamp_{Inv_i})$ in the database. In this way, if the winning participant denies having claimed the prize, the LO can use $(Num, ID_i, SHK_i, R_i, s_i^* timestamp_{Inv_i})$ to prove that the prize was issued, and then send the invoice message TK_{Inv_i} to the winning participant.

Step 3: Participant *i* verifies the invoice message:

$$V_{PK_{LO}}(SG_{Inv_i}) \stackrel{?}{=} C_{Inv_i} \tag{63}$$

If the equality holds, the participant checks if the prize has been transferred to his/her credit.

4. Security analysis

This section will discuss known attacks and criteria for the proposed protocol.

4.1. Replay attack

In the lottery ticket purchase phase, coordinator C sends purchase messages (C_2, H_{ID_i}) to the LPC. If a malicious attacker intercepts or wiretaps the messages, the attacker can use the message to request a lottery ticket as the message comprises the coordinator's public identity H_{IDi}. Even if the LPC receives and agrees to the replay message; the attacker will still not be able to claim the prize because the LPC sends back the lottery tickets with the identity from $M_{buy} = (ID_1 \| ID_2 \| \ldots \| ID_m \| Q_1 \| Q_2 \| \ldots \| Q_m)$ and only the receiver should use the correct private identity d_{IDi} to retrieve the shadow SHK_i to claim the prize as follows:

$$SHK_i = RV_i \oplus h_1(e(d_{ID_i}, RQ_{LPC}))$$

Therefore, an attacker cannot claim the prize by replay attack.

4.2. Man-in-the-middle attack

Assume an attacker intercepts messages $(Q_c, T_c, H_{ID_c}, Num, R_c, s_c^*, t_c)$ between the coordinator and participant. They can modify the coordinator's identity H_{ID_c} to H_{ID_A} and the number Num to Num_A. The participant will thus receive the fake messages $(Q_c, T_c, H_{ID_A}, Num_A, R_c, s_c^* \cdot t_c)$.

First, the participant checks the legality by:

$$e(T_c, Q) \stackrel{?}{=} e(Q_c + h_1(Q_c) \cdot H_{ID_A}), Q_{pub})$$

$$\begin{aligned} e((Q_c + h_1(Q_c) \cdot H_{ID_A})Q_{pub}) = \; & e((N_c \cdot Q + h_1(Q_c) \cdot H_{ID_A}), s \cdot Q) \\ = \; & e((N_c \cdot Q + h_1(Q_c) \cdot H_{ID_A}), Q)^s \\ = \; & e((N_c \cdot s \cdot Q + h_1(Q_c) \cdot s \cdot H_{ID_A}), Q) \\ = \; & e((N_c \cdot Q_{pub} + h_1(Q_c) \cdot d_{ID_A}), Q) \\ \neq \; & e(T_c, P) = e((N_c \cdot Q_{pub} + h_1(Q_c) \cdot d_{ID_c}), Q) \end{aligned}$$

Therefore, the attacker should have the secret key s to make the private identity d_{ID_c} for forging the legal identity. But the secret key s is kept secret by the LO and LPC.

Second, the selected lottery number Num_A should be checked as follows:

$$\begin{aligned} V_1 = \; & x[R] \cdot Q_c + (s^*) \cdot R_c \\ = \; & (x[R]) \cdot N_c \cdot Q + (r_c^{-1}(Num - N_c \cdot x[R])(r_c \cdot Q) \\ = \; & (x[R]) \cdot N_c \cdot Q + (Num - N_c \cdot x[R])Q \\ = \; & (Num)Q \\ \neq \; & (Num_A)Q = V_2 \end{aligned}$$

Thus, it cannot pass the verification, unless the attacker knows the nonce N_c. But nonce N_c was generated by the coordinator and can never be disclosed.

4.3. Impersonation attack

Due to repeated forgery attempts (such as double claiming, without sharing with anyone else) taking place in lotteries, it is important to be able to verify a participant's identity. This study discusses three cases of attempted forgery that are addressed by the proposed protocol.

Case 1: The attacker impersonates a legal coordinator.
The attacker uses the request message $(Q_c, T_c, H_{ID_c}, Num, R_c, s_c^*, t_c)$ to request a participant's information. He/she can get the replay message (Q_i, C_1) and use the nonce n_c to generate the session key $CK_{c,i} = N_c \cdot Q_i$. However, an attack that extracts nonce N_c is difficult to achieve because of the Elliptic Curve Discrete Log Problem (ECDLP) from Q_c. Therefore, the attacker cannot obtain the participant's real identity ID_i.

Case 2: The attacker impersonates a legal participant.
If the LPC agrees to the purchase, it will generate shadow SHK_i for every participant from M_{buy} and send them to participants, respectively. Even if the attacker gets the messages (RQ_{LPC}, ST_j, RV_i); he/she must have a private identity d_{ID_c} to receive the shadow as follows:

$$\begin{aligned} RV_i \oplus h_1(e(s \cdot H_{ID_i}, RQ_i)) &= RV_i \oplus h_1(e(H_{ID_i}, N_{LPC} \cdot Q)^s) \\ &= RV_i \oplus h_1(e(H_{ID_i}, Q)^{s \cdot N_{LPC}}) \\ &= SHK_i \oplus h_1(e(H_{ID_i}, Q_{pub})^{N_{LPC}}) \oplus h_1(e(H_{ID_i}, s \cdot Q)^{N_{LPC}}) \\ &= SHK_i \end{aligned}$$

However, the private identity d_{ID_c} and secret key s can never be leaked, so it is impossible for an attacker to obtain the shadow SHK_i.

Case 3: The attacker impersonates a legal winning participant.

When a participant presents SHK_i and Num to claim a prize, the LO will index by Num to find the corresponding K_i and $T_{i,LO}$ in the database. The LO then checks the legality as follows:

$$\begin{aligned} (T_{i,LO} \cdot T_i) \oplus H_{ID_i} &= (K_i^{SH_{i,LO}} \cdot K_i^{SHK_i}) \oplus H_{ID_i} \\ &= \left(K_i^{f(H_{LO})(-H_{ID_i}/(H_{LO}-H_{ID_i}))} \cdot K_i^{f(H_{ID_i})(-H_{LO}/(H_{ID_i}-H_{LO}))}\right) \oplus H_{ID_i} \\ &= \left(K_i^{(c \cdot H_{LO}+SK_{LO})(-H_{ID_i}/(H_{LO}-H_{ID_i}))} \cdot K_i^{(c \cdot H_{ID_i}+SK_{LO})(-H_{LO}/(H_{ID_i}-H_{LO}))}\right) \oplus H_{ID_i} \\ &= \left(K_i^{(-c \cdot H_{LO} \cdot H_{ID_i}+c \cdot H_{ID_i} \cdot H_{LO}+SK_{LO}(-H_{ID_i}+H_{LO})/(H_{LO}-H_{ID_i}))}\right) \oplus H_{ID_i} \\ &= \left((N_{LPC} \oplus H_{ID_i})^{PK_{LO}}\right)^{SK_{LO}} \oplus H_{ID_i} \\ &= N_{LRC} = N'_{LRC} \end{aligned}$$

If the participant is not a real winner, his/her identity will not be present in the database.

4.4. Anonymity issue

A participant's ticket TK_c is very important, so the proposed method encrypts this information into C_2 with his/her private identity d_{ID_c} and then blends it into the lottery ticket purchase phase as follows:

$$C_2 = E_{d_{ID_c}}((Q_c, V_{buy}), TK_c, timestamp_c, Num)$$

In particular, the participant's information (ID_i, Q_i) is blended into V_{buy} as follows:

$$M_{buy} = (ID_1 \| ID_2 \| \ldots \| ID_n \| Q_1 \| Q_2 \| \ldots \| Q_m)$$
$$V_{buy} = M_{buy} \oplus h_1(e(H_{ID_c}, Q_{pub})^{N_c})$$

Only the LO and LPC have the secret key s to make the private identity d_{IDi}, as follows:

$$d_{ID_i} = s \cdot H_{ID_i}$$

Thus participants' identities are secret during the transactions.

4.5. Verifiability issue

In the winning number generation phase, the decryptor selects and publishes the winning number message $(V'_1 \| V'_2 \| \ldots \| V'_6 \| M \| e_p \| d_p \| n_p)$. The participants can use the published parameters $(M \| e_p \| d_p \| n_p)$ to verify the published winning numbers $(wno_1, wno_2, \ldots, wno_6)$ as follows:

$$\text{check } t_i^{e_p} \cdot (no_i) \bmod n_p \stackrel{?}{=} M_i, \text{for } i = 1 \text{ to } k$$
$$\text{check } (M_j)^{d_p} \cdot t_j^{-1} \stackrel{?}{=} V'_j, \text{for } j = 1 \text{ to } 6$$
$$\text{check } (V'_j)^{e_p} \bmod n_p \stackrel{?}{=} wno_u, \text{for } j = 1 \text{ to } 6$$

If anyone challenges the result of the winning numbers $(wno_1, wno_2, \ldots, wno_6)$, they can use the pseudo-random number generation function $PRG(\cdot)$ with M to generate the winning numbers again.

4.6. Fairness issue

The lottery protocol should ensure an equal probability of winning the prize for every participant. The decryptor's winning number generating function cannot be controlled or influenced by the LO or any participants. In the proposed protocol, the untraceable and tamperproof decryptor is independent, despite being set up by the LO. When the LO sends the selected numbers no_i to the decryptor, the decryptor automatically generates a pair of parameters e/d for itself. Even if the decryptor publishes the parameters after generating the winning numbers, the LO or participants will not be able to guess the parameters for the next generation. Because the decryptor uses the real random number function to generate parameters, the real

number has a corresponding random number t_i. For this reason, the real random numbers have a new fake number M' for every iteration by new parameters (t_i, e_p, d_p, n_p). The queue is also different every time in the decryptor. Since no one can predict the outcome, the winning number generation is fair.

4.7. Accuracy issue

If the LO distributes the winning prize, he/she should accurately know how many participants are engaged in the lottery. In the purchase phase, the coordinator integrates participants' information into purchase message M_{buy}; the LPC then follows the message to generate shadows and the LO stores the purchase message in the database. When a participant claims a prize, the LO will generate correlated shadow keys by the purchase message. If the participant is a legal winner, the LO checks:

$$N'_{LRC} \stackrel{?}{=} N_{LPC}$$

Moreover, the purchase message includes participants' information. The LO can count the number of the purchase in order to determining which prize/s should be allocated to each winning participant.

5. Performance analysis

This section compares the performance of the proposed method in terms of security and computation costs, and compares this performance with those of other methods to show the contribution of this paper. First, the security and function analysis of the proposed protocol is compared with previous protocols in Table 1. From this it is clear that the proposed protocol can withstand attacks and satisfy the known requirements, while other protocols cannot. Chow et al. and Lee and Chang's protocol only use the pseudo-random function to generate winning numbers. These other protocols cannot, therefore, defend against known attacks. Moreover, they do not satisfy the fairness, accuracy and public verification request requirements in a mobile environment. Therefore, a participant in the proposed protocol can use his/her cell phone or mobile device to simply and safely purchase lottery numbers by him/herself or jointly with other participants.

Subsequently, Table 2 summarizes the performance of the proposed protocol in terms of joint purchase, lottery ticket purchase, and prize claiming. This study defines some notations for the proposed protocol as follows:

T_e: the time taken to execute a bilinear map operation $e : G_1 \times G_1 \rightarrow G_2$.
T_{mul}: the time taken to execute a multiplication operation of point.
T_{H1}: the time taken to execute a one-way hash function $h_1(\cdot)$.
T_{H2}: the time taken to execute a map-to-point hash function $h_2(\cdot)$.
T_{add}: the time taken to execute an addition operation of points.
T_{exp}: the time taken to execute a modular exponentiation operation.
T_{sym}: the time taken to execute a symmetrical encryption/decryption operation.
T_{XOR}: the time taken to execute an XOR operation.
T_{sign}: the time taken to sign a signature.
m: the number of participants.

The time taken to execute a bilinear map operation T_e is longer than other operations, with the exclusion of the time taken to execute a symmetrical encryption/decryption operation T_{sym}. Some lightweight operations of the simulation results demonstrate that T_{add} and T_{H1} are trivial in comparison with T_e, T_{mul} and T_{H2}. The operation of the participant's mobile device is lightweight while the lottery proxy center and lottery originator are regarded as powerful devices.

Table 1
The security comparison of our protocol and related protocols.

	Our protocol	Chow et al.'s protocol [8]	Lee and Chang protocol [9]
Against replay attack	Y	Y	Y
Against man-in-the middle attack	Y	N	Y
Against impersonation attack	Y	N	Y
Against insider attack	Y	N	N
On-line system	Y	Y	Y
Anonymity	Y	Y	Y
Mutual authentication	Y	N	Y
Fairness	Y	N	N
Public verification	Y	N	N
Accuracy	Y	Y	N
Based on mobile environment	Y	N	N
Joint purchase	Y	N	N

Table 2
The computation cost of the joint purchase and claim prize.

	Participant	Coordinator	LPC	LO	Decryptor
Joint purchase	$2T_e + 6T_{mul} + 1T_{H1} + 2T_{add} + 1T_{sym}$	$7T_{mul} + 1T_{H1} + 2T_{add} + 1T_{sym}$			
Purchase lottery	$3T_e + 1T_{mul} + 2T_{H1} + 1T_{add} + 1T_{XOR}$	$1T_e + 1T_{mul} + 1T_{H1} + 1T_{add} + 1T_{sym} + 1T_{XOR}$	$(1+m)T_e + (4+5m)T_{mul} + (2+m)T_{H1} + (m)T_{H2} + (1+2m)T_{add} + (2m)T_{exp} + 1T_{sym} + (1+2m)T_{XOR}$	mT_{exp}	
Generate winning number				$6T_{exp}$	$(k+6)T_{exp} + 6T_{mul}$
Claim prize	$1T_e + 4T_{mul} + 1T_{add} + 1T_{H1} + 1T_{sym} + 1T_{XOR}$			$1T_e + 2T_{mul} + 1T_{H1} + 1T_{H2} + 1T_{add} + 1T_{exp} + 1T_{sym} + 2T_{XOR} + 1T_{sign}$	

In Table 2, it is seen that the participant plays a part in every phase, but his/her computation cost is not heavy. The coordinator joins other participant information and purchase lottery. However, his/her computation is similar to that of other participants. The LO should maintain low computation to keep the system stable, even if the LO is a powerful server. Obviously, the LPC has high computation cost; it must verify the coordinator's identity, generate lottery numbers for every participant and send participant information to the LO. This is necessary so that the proposed scheme can prevent the attacks discussed above, and so that participants can claim their prizes. Based on the description above, the ticket purchase process can be guaranteed by the proposed lottery ticket purchase protocol with low computation cost.

6. Conclusions

In general, lottery participants must purchase physical lottery tickets in stores. However, smart phones and mobile devices have become very popular and powerful, and are capable of supporting secure mobile environments. This study therefore proposes a fair and secure protocol allowing users to safely and fairly purchase lottery tickets by smart phone.

Since ECC is easily implemented in mobile devices, a joint e-lottery scheme is proposed. The proposed scheme can achieve security and particular requests as follows:

- Support e-lottery activity.
- Public verification.
- Fairness.
- Defend against known attacks.
- Mutual authentication.

In the proposed scheme, even if the coordinator wishes to pocket prizes without sharing with anyone else, they will fail. This is because winning participants can claim prizes independently, even if the coordinator misappropriates the prize. Furthermore, the fairness of the winning number is ensured by the use of an untraceable and tamperproof decryptor with a real random number generation function. It can also provide public verification by a pseudo-random number generation function.

Based on the performance analysis, the proposed lottery protocol can satisfy the fairness, accuracy, and public verification requests in a mobile environment requirements. As a result, each mobile user can easily purchase lottery numbers using their smart device. In addition, the proposed protocol can prevent the various malicious attacks discussed above with low computation costs. Future research will investigate participant commissions join other brokers to claim prizes in a mobile environment.

Acknowledgements

This research was supported by the Ministry of Science and Technology, Taiwan, ROC, under contract number MOST 103-2221-E-324 -023, MOST 103-2622-E-212-009 -CC2, MOST103-2632-E-324-001-MY3 and MOT 104-2221-E-324-012.

References

[1] California State Lottery Home Page. <http://www.calottery.com/default.htm> [access available on 07.05.15].
[2] Mega millions Official Home. <http://www.megamillions.com/> [access available on 07.05.15].
[3] Powerball-Home page. <http:/www.powerball.com/> [access available on 07.05.15].
[4] Mahmood Anzar, Javaid Nadeem, Razzaq Sohail. A review of wireless communications for smart grid. Renew Sustain Energy Rev 2015(41):248–60.
[5] Daghighi Babak, Kiah Miss Laiha Mat, Shamshirband Shahaboddin, Rehman Muhammad Habib Ur. Toward secure group communication in wireless mobile environments: issues, solutions, and challenges. J Network Comput Appl 2015(50):1–14.

[6] Chen Y-L, Cheng C-M. Combining a chaos system with an Arnold cat map for a secure authentication scheme in wireless communication networks. Eng Comput 2014(31):317–30.
[7] Pietro R-D, Guarino S, Verde N-V, Domingo-Ferrer J. Security in wireless ad-hoc networks–a survey. Comput Commun 2014(51):1–20.
[8] Chow S-S-M, Hui L-C-K, Yiu S-M, Chow K-P. An e-lottery scheme using verifiable random function. Lect Notes Comput Sci 2005;3428:651–60.
[9] Lee J-S, Chang C-C. Design of electronic *t*-out-of-*n* lotteries on the Internet. Comput Stand Inter 2009;31(2):395–400.
[10] Wu H-H. Testing of the randomness of the lottery winning numbers and the signed lottery. Institute of Statistics National University of Kaohsiung, Master thesis; July 2005.
[11] Chen C-L, Liao Y-H, Tsaur W-J. A secure and fair joint e-lottery protocol. Sci World J 2014;2014:14. http://dx.doi.org/10.1155/2014/139435. Article ID 139435, <http://www.hindawi.com/journals/tswj/2014/139435/>.
[12] Wu T-Y, Tseng Y-M. An efficient user authentication and key exchange protocol for mobile client–server environment. Comput Netw 2010;54(9):1520–30.
[13] Yang J-H, Chang C-C. An efficient three-party authenticated key exchange protocol using elliptic curve cryptography for mobile-commerce environments. J Syst Softw 2009;82(9):1497–502.
[14] Buchmann J-A. Introduction to cryptography, second ed.; 2003.
[15] Liaw H-T. A secure electronic voting protocol for general elections. Comput Secur 2004;23(2):107–19.
[16] Boneh D, Franklin M. Identity-based encryption from the Weil pairing. Adv Cryptology 2001;2139:213–29.
[17] Koblitz N. Elliptic curve cryptosystem. Math Comput 1987;48:203–9.
[18] Okamoto E, Okamoto T. Cryptosystems based on pairing over elliptic curve pairing. Lect Notes Comput Sci 2005;3558:1–4.
[19] Sakai R, Kasahara M. ID-based cryptosystems with pairing on elliptic curve, Cryptology ePrint Archive (2003), Report 2003/54. <http:/eprint.iacr.org/2003/054.pdf> [access available on 25.0814].
[20] Sakai R, Ohgishi K, Kasahara M. Cryptosystems based on pairing. In: Proceedings of the 2000 symposium on cryptography and information security. Okinawa 2000-C20; 2000.
[21] Sarkar P. Domain extender for collision resistant hash functions: improving upon Merkle–Damgard iteration. Discrete Appl Math 2009;157:1086–97.
[22] Quantum Random Bit Generator Service. <http://random.irb.hr/> [access available on 25.08.14].
[23] RSA-Home. <http://www.thersa.org/> [access available on 07.05.15].

Chin-Ling Chen was born in Taiwan in 1961. He received his B.Sc. degree in Computer Science and Engineering from Feng Cha University in 1991, and his M.Sc. and Ph.D. degrees in Applied Mathematics at National Chung Hsing University, Taichung, Taiwan, in 1999 and 2005, respectively. He is a member of the Chinese Association for Information Security. From 1979 to 2005, he was a senior engineer at Chunghwa Telecom Co., Ltd. He is currently a professor in the Department of Computer Science and Information Engineering at Chaoyang University of Technology, Taiwan. His research interests include cryptography, network security and electronic commerce. Dr. Chen has published over 60 articles on the above research fields in SCI/SSCI international journals.

Mao-Lun Chiang received his M.S. degree in Information Management from Chaoyang University of Technology, and his Ph.D. degree from the Department of Computer Science of National Chung-Hsing University, Taiwan. He is an assistant professor in the Department of Information and Communication Engineering at the Chaoyang University of Technology, Taiwan. His current research interests include Ad Hoc network, mobile computing, distributed data processing, fault tolerant computing, and cloud computing.

Wei-Chech Lin was born in Taiwan in 1985. He received his B.S. degree in Computer Science and Information Engineering from DAYEH University, Changhuam, Taiwan. He received his M.S. degree from the Department of Computer Science and Information, Chaoyang University of Technology in 2010. His research interests include cryptography and electronic commerce.

De-Kui Li was born in 1979. He received his M.S., and Ph.D. degrees in Management Information Systems from Kwangwoon University, Seoul, South Korea, in 2012. His research interests include business intelligence and data mining.