INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS
Int. J. Commun. Syst. 2014; **27**:3223–3231
Published online 1 April 2013 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/dac.2536

An improved *t*-out-of-*n* e-lottery protocol

Y. Liu[1], D. Lin[1], C. Cheng[2,3,*,†], H. Chen[4] and T. Jiang[5]

[1]*School of Mathematics and Computing Science, Guilin University of Electronic Technology, Guilin 541004, China*
[2]*School of Science, Hubei University of Technology, Wuhan 430068, China*
[3]*Hubei Key Laboratory of Intelligent Wireless Communications, South-Central University for Nationalities, Wuhan 430074, China*
[4]*School of Information and Communication, Guilin University of Electronic Technology, Guilin 541004, China*
[5]*Department of Electronics and Information Engineering, Huazhong University of Science and Technology, Wuhan 430074, China*

SUMMARY

In 2009, Lee and Chang proposed an electronic *t*-out-of-*n* lottery protocol over the Internet based on the Chinese remainder theorem and blind signature. However, a security flaw exists in Lee–Chang's protocol that the lottery agent and the malicious purchaser can collude to control the winning result, which is unfair for the honest participants. On the basis of a verifiable random number generated by using the Lagrange interpolation formula over a finite field, an improved *t*-out-of-*n* e-lottery protocol is proposed, which guarantees that each participant can generate the winning result equally. The improved protocol achieves public verifiability and fairness without a trusted third party and a delaying function, which makes it more robust and more efficient. Copyright © 2013 John Wiley & Sons, Ltd.

Received 25 October 2012; Revised 11 January 2013; Accepted 21 February 2013

KEY WORDS: electronic lottery; verifiable random number; Lagrange interpolation formula; without a trusted third party

1. INTRODUCTION

Electronic lottery is an important way to raise fund for charities [1–4]. Goldschlag and Stubblebine claimed that an e-lottery protocol should at least satisfy three properties [5]. First, the protocol should be fair, that is, each ticket should have the same probability of winning. Second, it should be publicly verifiable, that is, anyone can calculate the winning numbers (after the lottery has been closed) and verify the integrity of the lottery. Third, it should be closed, that is, the calculation of the winning numbers should depend only on the purchased tickets and not on the information supplied by a trusted third party (TTP). Goldschlag and Stubblebine designed an e-lottery protocol with these properties by using delaying functions.

A practical e-lottery protocol usually possesses the following requirements:

1. Security: No one can forge a winning ticket or control the implementation of the lottery protocol.
2. Correctness: Nobody can falsify players' choices.
3. Anonymity: No identification information is attached to the lottery tickets.
4. Randomness: The result should be random within the pre-defined domain, that is, nobody can deviate the generation of the winning result.
5. Verifiability: Any participant or observer can verify the process of generating the winning result.

*Correspondence to: C. Cheng, School of Science, Hubei University of Technology, Wuhan 430068, China.
†E-mail: chengchizz@gmail.com

6. Fairness: Before the deadline to draw a lottery, no one can predict the winning numbers other than guessing.
7. Without a TTP: The lottery protocol without a TTP is more flexible and more robust since the bottleneck of the trust and security is eliminated.
8. Without a delaying function: The protocol without a delaying function is more practical because the adversary's computation resources cannot be predicted accurately in practice.

Recently, Lee and Chang proposed a t-out-of-n e-lottery protocol [6] by using the Chinese remainder theorem and blind signature. They claimed that their protocol achieves the aforementioned requirements. However, it turns out that their claim is not true. The reason is that the lottery agent (LA) and the last purchaser maybe colluded to control the winning result, which destroys the fairness of lottery.

In this paper, a publicly verifiable t-out-of-n e-lottery protocol is proposed. First, a verifiable random number (VRN) is constructed by using the Lagrange interpolation formula over a finite field, similar to that in Shamir's secret sharing [7]. Next, the VRN is used to create the winning result of the lottery protocol, which guarantees that each participant or any observer can verify the result without help. The improved e-lottery protocol is fair because each participant is equally involved in the generation of the winning result, which prevents the malicious participant from colluding. Furthermore, the improved protocol inherits all merits of Lee–Chang's protocol, efficiency, anonymity, and convenience, which are the basic requirements in most protocol such as [8].

The rest of this paper is organized as follows. In Section 2, the Lee–Chang's e-lottery protocol is outlined, and its security flaw is analyzed. The method of generating the VRN by using the Lagrange interpolation formula is introduced in Section 3. In Section 4, the improved t-ouf-of-n e-lottery protocol is described. Security analysis of the proposed e-lottery protocol is presented in Section 5. Finally, some concluding remarks are drawn in Section 6.

2. REVIEW OF LEE-CHANG'S PROTOCOL

2.1. Lee–Chang's e-lottery protocol

On the basis of the Chinese remainder theorem [9, 10] and blind signature [11–13], Lee–Chang's e-lottery protocol consists of four phases: *initialization phase*, *purchase phase*, *draw phase*, and *claim phase*. The main participants includes LA, players (purchaser), a certificate authority (CA), and a bank.

1. Initialization phase
   LA executes the following steps:
   i. LA selects n pairs of (a_i, d_i), $d_i > a_i$, $i \in \{1, \ldots, n\}$, where $d_i, d_j (i \neq j)$ are co-prime;
   ii. LA computes $D_i = d_i^e (\text{mod } N)$, $(1 \leqslant i \leqslant n)$, where (e, N) is the RSA public key of LA;
   iii. LA computes $D = d_1 \times \cdots \times d_n$, and computes the solution C of the congruence system

$$\begin{cases} C = a_1 (\text{mod } d_1) \\ \vdots \quad \vdots \\ C = a_n (\text{mod } d_n) \end{cases},$$

   which equals to $C = \sum_{i=1}^{n} (D/d_i) y_i a_i \bmod D$, where $(D/d_i) y_i = 1 \bmod d_i, (i = 1, \ldots, n)$.
   iv. LA publishes $(a_1, D_1), \ldots, (a_n, D_n)$, and C on the bulletin board.
2. Purchase Phase
   Alice purchases a ticket from LA by executing the following steps:
   i. Alice chooses t pairs of (a'_j, D'_j), $(j = 1, \cdots, t)$ from $(a_1, D_1), \ldots, (a_n, D_n)$ published on the bulletin board.
   ii. Alice computes $\alpha_j = r_j^e D'_j \bmod N$ by choosing blind factors $r_j, (j = 1, \cdots, t)$, then sends $\alpha_1, \cdots, \alpha_t, r_{A1}, r_{A2}$ to LA in a secure manner, where r_{A1}, r_{A2} are random numbers.

DOI: 10.1002/dac

iii. LA signs on the messages $\alpha_1, \cdots, \alpha_t$, then sends $\beta_j = \alpha_j^d \bmod N$, $(1 \leqslant j \leqslant t)$ to Alice, where (d, N) denotes LA's private key.
iv. Assuming that this is the fth ticket sell. LA computes $Count_f = Count_{f-1} + r_{A1} \bmod f$ and publishes $(Count_f, f)$, then computes a symmetric key $k_f = H(r_{A2}||Count_f||f)$ between Alice and LA, where $H(\cdot)$ is a secure hash function.
v. The fth ticket $LT_f = Count_f, f, E_{k_f}(Count_f, f, \beta_1 \cdots, \beta_t)$ is issued to Alice by LA where $E_{k_f}(\cdot)$ denotes a symmetric encryption with a key k_f.

3. Draw phase
   In this phase, the winning result is created and published.
   First, LA computes $w = Count_n \bmod n$ where n is the amount of lotteries sold in the previous phase. Then, the seed w is fed into a pre-announced random number generator $Ran(\cdot)$ to get $Ran(w) = \{cw_1, \cdots, cw_t\}$ that is published as the winning number.
4. Claim phase
   If $\{a'_1, \cdots, a'_t\} = \{cw_1, \cdots, cw_t\}$, Alice sends $\{r_1, \cdots, r_t\}$ to LA to prove that she holds the winning ticket.
   LA computes $d'_i = \beta_i / r_i$, $(i = 1, \ldots, t)$, and $b_j = C \bmod d'_j$, $(1 \leqslant j \leqslant t)$, where $C = \sum_{i=1}^{n} (D/d_i) y_i a_i \bmod D$.
   LA is convinced of Alice's winning if $\{b_1, \cdots, b_t\} = \{cw_1, \cdots, cw_t\}$, since nobody knows the blind factors $r_1, \cdots, r_t$ except Alice.

2.2. *Security flaw of Lee–Chang's protocol*

Lee–Chang's protocol chains Alice's ticket by using $Count_f = Count_{f-1} + r_{A1} \bmod f$. For two adjacent purchasers, the latter can easily eliminate the former's contribution. As for all purchasers, the last purchaser can make others' contribution useless. Suppose that Alice is the last purchaser in the purchase phase, Alice and LA can control the seed of the random number generator to guarantee that Alice always wins. Moreover, nobody has evidence to reveal their conspiracy. The detailed attack is described as follows:

1. LA chooses a seed w, computes $Ran(w) = \{cw_1, \cdots, cw_t\}$, and sets $\{cw_1, \cdots, cw_t\}$ as the winning number in advance. LA sends w and $\{cw_1, \cdots, cw_t\}$ to Alice.
2. Alice purchases the last ticket by computing $r_{A1} = w - Count_{f-1} \bmod f$, and selects $\{a'_1, \cdots, a'_t\}$ as well as the corresponding $\{D'_1, \cdots, D'_t\}$ from the bulletin board such that $\{a'_1, \cdots, a'_t\} = \{cw_1, \cdots, cw_t\}$.
3. Alice sends the blind factors $\{r_1, \cdots, r_t\}$ to support her winning claim. Nobody can detect the collusion between Alice and LA.

Lee and Chang claimed that their protocol provides public verifiability, that is, Alice checks the equation $Count_f = Count_f + r_{A1} \bmod f$ to verify if her participation is really counted in the final result. But a purchaser cannot verify whether his contribution is really involved in generating the winning number from the aforementioned analysis. On the contrary, he can only check if he is involved in generating the next lottery ticket. In fact, every participant's influence is not equal. The latter can eliminate the former's influence by adjusting his r_{A1}. If the last purchaser colludes with LA, others' verification is useless.

To overcome the security flaw, an improved t-out-of-n e-lottery protocol is proposed by using VRN instead of the aforementioned ticket chain. With the VRN, each purchaser's contribution is equally involved in the generation of the winning number, which ensures that nobody can get more than others. Any collusion between LA and the malicious purchaser can be avoided.

3. VRN BASED ON LAGRANGE INTERPOLATION FORMULA

Lagrange interpolation formula over the finite field is an important tool for designing security protocols, such as Shamir's secret sharing scheme [7, 14, 15] and the key transfer protocol [16, 17].

Shamir's secret sharing scheme based on the Lagrange interpolation formula is denoted as (t, n)-SS, which consists of n shareholders $U_1, \ldots, U_n$ and a mutually trusted dealer. A secret s is

DOI: 10.1002/dac

divided into n shares and shared among n shareholders. It is easy to recover s with t or more than t shares, whereas fewer than t shares reveals nothing about s. The scheme includes *share generation algorithm* and *secret reconstruction algorithm*, which is information-theoretically secure.

1. Share generation algorithm
   The dealer randomly picks a polynomial of degree $t-1$, that is, $f(x) = s + a_1 x + \ldots + a_{t-1}x^{t-1} \in F_p[x]$. Then, the dealer computes $s_i = f(i)$, $(i = 1, \ldots, n)$ and distributes s_i to U_i securely.
2. Secret reconstruction algorithm
   With any t shares $(s_{i_1}, s_{i_2}, \ldots, s_{i_t})$, s can be recovered by using the formula

$$f(x) = \sum_{i \in A} s_i \left(\prod_{j \in A \setminus \{i\}} \frac{x_j - x}{x_j - x_i} \right) \pmod{p}, s = f(0) \tag{1}$$

where $A = \{i_1, \ldots, i_t\} \subset \{1, \ldots, n\}$.

Next, a method is proposed to generate the VRN that is inspired by Shamir's secret sharing. Suppose that there are n participants $U_1, \ldots, U_n$ who collaborate to generate a VRN by contributing the corresponding (x_i, y_i). To guarantee the existence of the VRN, the condition $x_i \neq x_j$ is required if $i \neq j$; moreover, all computations are performed over a finite field F_p, which is vital for the implementation of the protocol [18, 19].

1. U_i randomly chooses $(x_i, y_i) \in F_p$, $(i = 1, \ldots, n)$ and send it to LA;
2. LA computes the interpolation polynomial $f(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$ passing through $(x_1, y_1), \ldots, (x_n, y_n)$;
3. $H(a_0 || \ldots || a_{n-1})$ is defined as the VRN where $H(\cdot)$ is a secure hash function.

Remark 1
The VRN is random and verifiable for U_i if (x_i, y_i) is random.

First, the polynomial $f(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$ of degree $n-1$ is generated with n pairs, whereas $n-1$ pairs leaves completely unknown about $f(x)$. Nobody can predict $f(x)$ even if $n-1$ participants collude, that is to say, the coefficients of $f(x)$ is random over F_p even if only one pair in $(x_1, y_1), \ldots, (x_n, y_n)$ is random. Furthermore, $H(a_0 || \ldots || a_{n-1})$ is also random.

Next, U_i can verify if his (x_i, y_i) is really involved in generating $f(x)$ by checking the equation $y_i = f(x_i)$. If $f(x)$ is generated without involving (x_i, y_i), the probability that the equation $y_i = f(x_i)$ holds is $1/p$. Considering that p is a secure prime, this collusion can be detected with the probability almost equal to 1.

4. IMPROVED t-OUT-OF-n E-LOTTERY PROTOCOL

The improved electronic t-out-of-n e-lottery protocol consists of five phases: initialization phase, purchase phase, draw phase, claim phase, and *verification phase*.

- Initialization phase

  1. LA publishes a secure prime p, and selects $a_i, d_i, d_i > a_i, (i = 1, \ldots, n)$ where $d_i, d_j (i \neq j)$ are relatively prime.
  2. LA computes $D_i = d_i^e \bmod N, (i = 1, \ldots, n)$ where (e, N) is LA's public key, $D = \prod_{i=1}^{n} d_i$.
  3. LA computes the solution C of the following congruence system with the Chinese remainder theorem, that is,

$$\begin{cases} C = a_1 (\bmod\, d_1) \\ \vdots \quad \vdots \\ C = a_n (\bmod\, d_n) \end{cases}$$

DOI: 10.1002/dac

which is equivalent to $C = \sum_{i=1}^{n}(D/d_i)y_i a_i \bmod D$, where $(D/d_i)y_i = 1 \bmod d_i$, $(i = 1, \ldots, n)$.

4. LA publishes $(a_i, D_i), (i = 1, \ldots, n), C$ on the bulletin board.

- Purchase phase

  Alice purchases the fth ticket issued by LA as follows:

  1. Alice chooses her favorite t pairs of $(a'_j, D'_j), (j = 1, \ldots, t)$ from $(a_i, D_i), (i = 1, \ldots, n)$, and computes

$$\begin{cases} \alpha_1 = r_1^e D'_1 \bmod N \\ \vdots \quad \vdots \\ \alpha_t = r_t^e D'_t \bmod N \end{cases}$$

     where $r_1, \ldots, r_t$ are randomly chosen by Alice. Then Alice encrypts the message $(\alpha_1, \ldots, \alpha_t, r_{A1}, r_{A2})$ by using LA's public key, and sends the cipher to LA, where r_{A1}, r_{A2} are random numbers.
  2. LA first decrypts the received cipher, then signs on $(\alpha_1, \ldots, \alpha_t)$ by using the secret key (d, N) to obtain

$$\begin{cases} \beta_1 = \alpha_1^d \bmod N \\ \vdots \quad \vdots \\ \beta_t = \alpha_t^d \bmod N \end{cases}$$

  3. LA computes $Count_f = Count_{f-1} + r_{A1} \bmod f$, issues the ticket $LT_f = \{Count_f, f, E_{k_f}(Count_f, f, \beta_1 \cdots, \beta_t)\}$ to Alice, where $E_{k_f}(\cdot)$ denotes a symmetric encryption with a key k_f, $k_f = H(r_{A2}||Count_f||f)$. Then, LA publishes $(f, Count_f)$.
  4. Alice decrypts and authenticates the ticket.

- Draw phase

  The sell system of lottery has been closed in this phase, and no one can buy a ticket. The improved electronic lottery protocol generates a VRN, which is used as the seed of the pre-announced random number generator $Ran(\cdot)$. The steps are listed as follows:

  1. Alice computes and publishes $x_f = H(r_1|| \ldots ||r_t)$.
  2. Suppose that there are n tickets sold so far in the previous phase. LA computes the interpolation polynomial $f(x)$ and the corresponding VRN with $(x_i, Count_i), (i = 1, \ldots, n)$. In fact, any participant or observer can compute and verify it with the published information. Then, VRN is used as a seed w, and $Ran(w) = \{cw_1, cw_2, \ldots, cw_t\}$.
  3. LA publishes the results $\{cw_1, cw_2, \ldots, cw_t\}$, and $f(x), w$ for public verification.

- Claim phase

  If $\{a'_1, a'_2, \ldots, a'_t\} = \{cw_1, cw_2, \ldots, cw_t\}$, Alice claims that she is a winner as follows:

  1. Alice sends her ticket and blind factors $LT_f, (r_1, \ldots, r_t)$ to LA;
  2. LA authenticates and decrypts LT_f, and computes

$$\begin{cases} d'_1 = \beta_1 / r_1 \bmod N \\ \vdots \quad \vdots \\ d'_t = \beta_t / r_t \bmod N \end{cases}$$

     where $\beta_1, \ldots, \beta_t$ are blind signatures generated by LA in the purchase phase.
  3. LA computes

$$\begin{cases} b_1 = C \bmod d'_1 \\ \vdots \quad \vdots \\ b_t = C \bmod d'_t \end{cases}$$

DOI: 10.1002/dac

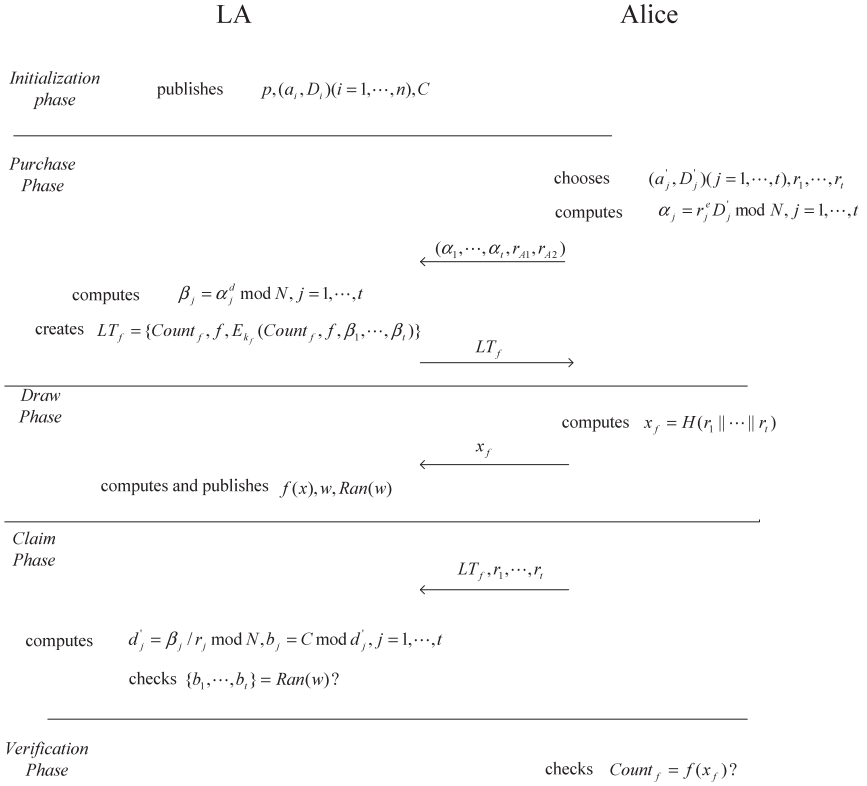

Figure 1. Flowchart of the improved t-out-of-n e-lottery protocol.

If $\{b_1, b_2, \ldots, b_t\} = \{cw_1, cw_2, \ldots, cw_t\}$, LA ensures that Alice is the winner.

- Verification phase

  If Alice doubts the fairness of the result, she checks whether the equation $Count_f = f(x_f)$ holds or not. If yes, Alice ensures that her participation has been involved in the generation of the result, and the result is fair.

The procedure of the improved t-out-of-n e-lottery protocol is illustrated in Figure 1.

5. SECURITY ANALYSIS

The proposed t-out-of-n e-lottery protocol achieves a series of properties, including security, correctness, anonymity, privacy, and convenience, which stem from the cryptographic techniques such as Chinese remainder theorem, blind signature, and verifiable random number. In this section, it will be shown that the proposed protocol is publicly verifiable, fair, and does not need a trusted third party as well as a delaying function.

- Verifiability

  The winning number is determined by the interpolation polynomial passing through all pairs $(x_1, Count_1), \ldots, (x_f, Count_f), \ldots, (x_n, Count_n)$. Because each ticket is equally involved in the generation of the polynomial, nobody can control the result even if only one ticket is randomly chosen. Unless all participants collude, the polynomial is unpredictable for all, and the winning result is random for all.

  As for the verifiability, Alice verifies the result by checking the equation $Count_f = f(x_f)$. Because x_f is the hash value of the blind factors that is randomly chosen by Alice, the probability of a forgery polynomial $g(x)$ that satisfies $Count_f = g(x_f)$ is $1/p$. Considering that p is a secure prime, Alice can detect the forgery with the probability almost equal to 1.

DOI: 10.1002/dac

Any observer can verify the generation of the interpolation and the winning result because $(x_i, Count_i), i = 1, \ldots, n$ are published. If no verification holds, the observer reports it to the certificate authority.

- Fairness

  Fairness is closely related to randomness. If the winning number $Ran(w) = \{cw_1, cw_2, \ldots, cw_t\}$ is random, nobody contributes more than the others, which assures that the protocol is fair for all participants.
- No trusted third party

  In the proposed protocol, $Count_1, \ldots, Count_n$ are published at the end of the purchase phase, $x_1, \ldots, x_n$ are published in the draw phase after the sell system has been closed. Unless all purchaser collude to control the result, nobody can preset the seed w to obtain extra advantage even if LA is corrupted. In the proposed protocol, LA is not a trusted third party, it only serves as a computing resources. In fact, every volunteer can also bear this work. Therefore, the proposed lottery protocol need no trusted third party.
- No delaying function

  In [5], delaying function is a function, which is moderately hard to compute, as opposed to easy or cryptographically hard. The computation time may take several hours when using the known fastest implementation, depending on the lottery requirements. Delaying function is used to prevent from cheating of adversaries who is computationally bound. For example, a sell system can still sell lottery tickets after the winning number has been generated, because the time of the sell system is a little later than that of the LA, which is unfair for others. It is possible for an adversary to forge the winning ticket by using the tiny asynchrony between LA and the sell system. With a delaying function, this drawback can be eliminated. But how to design a good delaying function and how to control its calculation are still difficult problems.

  In the improved t-out-of-n e-lottery protocol, after the sell system has been shut down in the draw phase, $x_1, \ldots, x_m$ are published. Then, the winning result is generated. Any adversary cannot forge the winning ticket even if there is asynchrony between LA and the sell system. The delaying function is not necessary for the improved protocol.
- Efficiency

  The proposed lottery protocol uses the verifiable random number to prevent the collusion, it is efficient compared with the protocol with delaying function that need a moderate long time to execute.

Remark 2

The improved scheme inherits the structure of Lee–Chang's protocol, in which the assumption of $D < N$ is necessary. For a practical lottery protocol, n should not be a large number. For example, let $n = 100, t = 6$, the winning probability $1/1192052400$ is so tiny that the protocol is unacceptable in practice. Therefore, the assumption of $D < N$ is reasonable considering that D is the product of n non-cryptographic large numbers, and N is a product of two cryptographic large primes.

6. CONCLUSION

In this paper, an improved t-out-of-n e-lottery protocol has been proposed, which is built on a verifiable random number generated by using the Lagrange interpolation formula over a finite field. The proposed protocol satisfies the requirements of general lotteries without the help of a trusted third party and a delaying function.

ACKNOWLEDGEMENTS

This work was supported by Foundation of Guangxi Key Laboratory of Trusted Software (Guilin University of Electronic Technology) under grant no. KX201215 and Foundation of Hubei Key Laboratory of Intelligent Wireless Communications under grant no. IWC2012006.

DOI: 10.1002/dac

REFERENCES

1. Zhou J, Tan C. Playing lottery on the Internet. *Proc. 3rd International Conference on Information and Communications Security*, Xi'an, China, 2001; 189–201.
2. Chow SSM, Hui LCK, Yiu SM, Chow KP. Practical electronic lotteries with offline TTP. *Computer Communications* 2006; **29**(15):2830–2840.
3. Chen YY, Jan JK, Chen CL. Design of a fair proxy raffle protocol on the Internet. *Computer Standards & Interfaces* 2005; **27**(4):415–422.
4. Liu Y, Hu L. Using an efficient hash chain and delaying function to improve an e-lottery scheme. *International Journal of Computer Mathematics* 2007; **87**(7):967–970.
5. Goldschlag DM, Stubblebine SG. Publicly verifiable lotteries: application of delaying functions. *Financial Cryptography, Lectures in Computer Science* 1998; **1465**:214–226.
6. Lee JS, Chang CC. Design of electronic t-out-of-n lotteries on the Internet. *Computer Standard & Interfaces* 2009; **31**(2):395–400.
7. Shamir A. How to share a secret. *Communications of the ACM* 1979; **22**(11):612–613.
8. Chen C, He D, Chan S, Bu J, Gao Y, Fan R. Lightweight and provably secure user authentication with anonymity for the global mobility network. *International Journal of Communication Systems* 2011; **24**(3):347–362.
9. Ding C, Pei D, Salomaa A. *Chinese Remainder Theorem*. Word Scientific: Singapore, 1996.
10. Baker KA, Pixley AF. Polynomial interpolation and the Chinese remainder theorem. *Mathematics and Statistics* 1975; **143**(2):165–174.
11. Chaum D. Blind signatures for untraceable payments. *Crypto'82*, Santa Barbara, California, USA, August 23–25, 1982; 199–203.
12. Chaum D. The dining cryptographers problem: unconditional sender and pecipient untraceability. *Journal of Cryptology* 1988; **1**(1):65–75.
13. Camenisch JL, Piveteau J, Stadler MA. Blind signatures based on the discrete logarithm problem. *Advances in Cryptology, Lecture Notes in Computer Science* 1994; **950**:428–432.
14. Pedersen T. A threshold cryptosystem without a trusted party. *Advances in Cryptology, Lecture Notes in Computer Science* 1991; **547**:522–526.
15. Zhao JJ, Zhang JZ, Zhao R. A practical verifiable multi-secret sharing scheme. *Computer Standards & Interfaces* 2007; **29**(1):138–141.
16. Harn L, Lin C. Authenticated group key transfer protocol based on secret sharing. *IEEE Transaction on Computers* 2010; **59**(6):842–846.
17. Liu YN, Cheng C, Cao JY, Jiang T. An improved authenticated group key transfer protocol based on secret sharing. *IEEE Transaction on Computers*. DOI: 10.1109/TC.2012.216.
18. Chuang YH, Tseng YM. Towards generalized ID-based user authentication for mobile multi-server environment. *International Journal of Communication Systems* 2012; **25**(4):447–460.
19. Xie Q. A new authenticated key agreement for session initiation protocol. *International Journal of Communication Systems* 2012; **25**(1):47–54.

AUTHORS' BIOGRAPHIES

Yining Liu is currently an associate professor in Guilin University of Electronic Technology, Guilin, China. He is also a researcher in Guangxi Key Lab of Trusted Software. He received his BS degree in Applied Mathematics from Information Engineering University, Zhengzhou, China, in 1995; MS in Computer Software and Theory from Huazhong University of Science and Technology, Wuhan, China, in 2003; and PhD degree in Mathematics from Hubei University, Wuhan, China, in 2007. His research interests focus on the analysis of security protocols and secure e-voting.

Danzhu Lin is now an MS candidate in the School of Mathematics and Computational Science, Guilin University of Electronic Technology, Guilin, China. She received her BS degree in Information and Computational Science from Xiangtan University, Xiangtan, China, in 2012. Her research interests focus on the analysis of electronic commerce protocol.

Chi Cheng is a Lecturer in the School of Science, Hubei University of Technology, Wuhan, China. He received his BS and MS degrees in Mathematics from Hubei University, Wuhan, China, in 2003 and 2006, respectively. His research interests include the security problems in network coding, key distribution, and e-voting.

Hongbin Chen is an associate professor in the School of Information and Communication, Guilin University of Electronic Technology, China. He received his BE degree in Electronic and Information Engineering from Nanjing University of Posts and Telecommunications, China, in 2004, and PhD degree in Circuits and Systems from South China University of Technology, China, in 2009. His research interests lie in cooperative, cognitive, and green communications. He is serving as an Editor for *IET Wireless Sensor Systems* from October 2010 to September 2013.

Tao Jiang is currently a full Professor in Wuhan National Laboratory for Optoelectronics, Department of Electronics and Information Engineering, Huazhong University of Science and Technology, Wuhan, China. He received his BS and MS degrees in Applied Geophysics from China University of Geosciences, Wuhan, China, in 1997 and 2000, respectively, and PhD degree in Information and Communication Engineering from Huazhong University of Science and Technology, Wuhan, China, in April 2004. From Aug. 2004 to Dec. 2007, he worked in some universities, such as Brunel University and University of Michigan in UK and USA, respectively. He has authored or co-authored over 100 technical papers in major journals and conferences, and five books/chapters in the areas of communications. His current research interests include the areas of wireless communications and corresponding signal processing, especially for cognitive wireless access, vehicular technology, OFDM, UWB and MIMO, cooperative networks, smart grid, and wireless sensor networks. He served or is serving as symposium technical program committee membership of many major IEEE conferences, including INFOCOM, ICC, GLOBECOM, and so on. He has been invited to serve as TPC Symposium Chair for the IEEE GLOBECOM 2013 and IEEEE WCNC 2013, and as a general co-chair for the workshop of M2M Communications and Networking in conjunction with IEEE INFOCOM 2011. He served or is serving as associate editor of some technical journals in communications, including in *IEEE Communications Surveys and Tutorials, IEEE Transactions on Vehicular Technology*, and so on. He is a recipient of the Best Paper Awards in IEEE CHINACOM09 and WCSP09. He is a Senior Member of IEEE, and a member of IEEE Communication Society, IEEE Vehicular Technology Society, IEEE Broadcasting Society, and IEEE Signal Processing Society.

DOI: 10.1002/dac