Journal of Information & Computational Science 7: 11 (2010) 2312–2317
Available at http://www.joics.com

A Fair E-Lottery Scheme Based on Interpolated Polynomial over Fp ⋆

Yining Liu [a,*], Jianyu Cao [a], Chi Cheng [b,c]

[a] *School of Mathematical and Computational Sciences, Guilin University of Electronic Technology Guilin 541004, China*

[b] *School of Science, Hubei University of Technology, Wuhan 430068, China*

[c] *Hubei key Laboratory of Applied Mathematics, Hubei University, Wuhan 430062, China*

Abstract

Fairness is important in electronic lottery scheme. Based on the interpolated polynomial theory, Verifiable Random Number is proposed over finite field Fp, which assures the generated result is fair for all entities. A fair e-lottery scheme is given with verifiable random number. When the number of participants is large, a structure of multi-level polynomial is constructed which makes computational time increases lineally even if the number rises exponentially. The improved lottery scheme is secure, fair and efficient, which is suitable for mobile user.

Keywords: Verifiable Random Number; Interpolated Polynomial; Finite Field; Multi-level Polynomial Structure; Electronic Lottery

1 Introduction

Lottery scheme is not only important for charity fund raising, it can be used to design a probabilistic micropayment in the past [1], there are other applications in other social cases. With the experience of lottery scheme, some criteria are proposed:

1. Requirement to generate a wining number;
2. Requirement that lottery players involved the generation of the wining number off-line;
3. Each participant can verify the winning number ;
4. Everyone can not forge the winning number ;

The scheme satisfies all the above requirements [2], but it uses a linear hash chain to link all tickets involved in the generation of the winning result which makes the efficiency of verification phase is low. The drawback is improved in [3] with a multi-level hash chain and delaying function,

⋆Project supported by the Foundation of Guilin University of Electronic Technology under Grant No. UF08014Y and partly supported by Hubei Key Laboratory of Applied Mathematics (Hubei University).

*Corresponding author.
Email address: ynliu@guet.edu.cn (Yining Liu).

November 2010

the complexity of verification is reduced from $O(j)$ to $O(\lceil \log_T j \rceil)$, which is more efficient. But all hash values in each level need to be published in the phase of generating winning number. If a participant wants to verify whether the result is fair, he need calculates hash value of the corresponding block, the input of hash must be strictly correspond to the previous generating process, which is troublesome for participants. In order to simplify the computational burden and consumption of time for user, a new lottery scheme based on verifiable random number (VRN) is proposed, in which VRN is constructed based on interpolated polynomial over F_p. The remainder of the paper is organized as follows. Section 2 presents how to generate verifiable random number, and the improved e-lottery scheme is proposed in section 3. We analyze the security and fairness of the improved scheme in section4. Section5 concludes the paper.

2 Verifiable Random Number

2.1 Interpolated Polynomial

The method of interpolating is used to approximate calculation $y = f(x)$, which constructs a polynomial $A(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ through $(x_i, y_i), (i = 0, ...n)$. Interpolated polynomial over F_p satisfies the property of existence and uniqueness.

Interpolated polynomial is widely used for group key management in [4, 5, 6, 7, 8, 9, 10].

Random is important for e-commerce protocol, winning number should be random or unpredicted to ensure the fairness in electronic lottery scheme. Simultaneously, verifiability is also necessary. Most random generation algorithm cannot be verified without seed or key. So in many scheme, the Trusted Third Party (TTP) is indispensable. If the TTP colludes with others, nobody can judge whether the random number is genuine.

Verifiable Random Number is put forward and used in the e-lottery scheme to improve the flaws of the above scheme.

2.2 VRN Based on Interpolated Polynomial

For instance, a random number is used as key to encrypt the content among $U_1, U_2, \cdots, U_n$ to assure confidentiality in teleconference [9]. Usually the key is selected randomly by chairperson, which makes it secure bottleneck. A fair key management should be one that the key contains some contribution from each participant, so that nobody has unfair advantage in controlling the key. The good method not only requires its generation involving everyone's contribution, but also its randomness should be verified by all. We abbreviate the verifiable random number VRN. Based on interpolated polynomial, a method of constructing verifiable random number is proposed. The step of generating verifiable random number is as follows:

1. U_i selects a pair of number $r_i = (x_i, y_i)$ randomly, and sends it to Computing Center (CC).

2. CC selects a pair of number $r_0 = (x_0, y_0)$ randomly;

3. CC constructs a polynomial $A(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ using $n + 1$ points $(x_0, y_0), (x_1, y_1), \cdots, (x_n, y_n)$ by adopting Lagrange polynomial Interpolation as in [9]. We assume CC's computing capacity is powerful. When the number of points is not large enough, it is easy to calculate the corresponding coefficients $(a_0, a_1, \cdots, a_n)$ of interpolated polynomial which satisfies

the equation $y_i = A(x_i)(0 \leq i \leq n)$.

$r = a_0||a_1||\cdots||a_n$ (|| denotes concatenation) is called interpolated polynomial coefficient random. Let $hash(.)$ is a secure hash function such as SHA-256, $R = hash(r)$. CC publishes r and R, and R is used as VRN.

If U_i doubts the authenticity of R, U_i can verify whether he is involved in generating R. The step of verifying the VRN is as follows:

1. U_i recovers $A(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ [2] from $r = a_0||a_1||\cdots||a_n$;

2. U_i verifies whether the equation $y_i = A(x_i)$ is true or false. If it is true, $r_i = (x_i, y_i)$ is involved the process of creating r.

3. U_i verifies whether $R = hash(r)$ is true.

If they are all hold, R is a trusted VRN.

We give a example for illustrating the interpolated polynomial over F_p.

Let $p = 7$, if there are three points $(x_0, y_0) = (1, 2), (x_1, y_1) = (2, 6), (x_2, y_2) = (4, 5)$, the corresponding Interpolating polynomial is $A(x) = 2 + 5x + 2x^2 \in F_7(x)$. r is $2||5||2$, and the verification random number $R = hash(2||5||2)$.

The provider of (x_i, y_i) can verify whether $A(x_i) = y_i$ is true and judges the authenticity of r and R easily.

2.3 Multi-level Polynomial Structure

When n is too large for CC, it may be difficult for calculating interpolated polynomial $A(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ quickly. An improved scheme is proposed. The step is as follows:

1. We array according the formula of $s - by - t$ matrix $M = \begin{pmatrix} m_{11} & m_{12} & \dots & m_{1t} \\ m_{21} & m_{22} & \dots & m_{2t} \\ \vdots & \vdots & \vdots & \vdots \\ m_{s1} & m_{s2} & \dots & m_{st} \end{pmatrix}$, (x_i, y_i) is in the $\lfloor (i/t) + 1 \rfloor^{th}$ row, in $(i\%p + 1)^{th}$ column, if $(n + 1) < s \cdot t$, CC pads the blanks randomly.

2. With the first row $(m_{11}, m_{12}, \cdots, m_{1t})$, $A_1(x)$ is constructed; $\cdots$, with the last row $(m_{s1}, m_{s2}, \cdots, m_{st})$, $A_s(x)$ is constructed.

3. We construct another $s-by-t$ matrix $\begin{pmatrix} m'_{11} & m'_{12} & \dots & m'_{1t} \\ m'_{21} & m'_{22} & \dots & m'_{2t} \\ \vdots & \vdots & \vdots & \vdots \\ m'_{s1} & m'_{s2} & \dots & m'_{st} \end{pmatrix}$ with M, and set $m'_{ij} = (y, x)$ provided with $m_{ij} = (x, y)$;

4. By analogy with step 2, a series of interpolating polynomials is constructed, which is denoted $A'_1(x), \cdots, A'_s(x)$;

5. The coefficients of $A_1(x)$ is $a_{10}, a_{11}, \cdots, a_{1(t-1)}$, we denote the concatenation $a_{10}||a_{11}||\cdots||a_{1(t-1)}$ of $A_1(x)$ as k_1;

$\cdots$.

the coefficient concatenation $a_{s0}||a_{s1}||\cdots||a_{s(t-1)}$ of $A_s(x)$ as k_s

the coefficient concatenation $a'_{10}||a'_{11}||\cdots||a'_{1(t-1)}$ of $A'_1(x)$ as k'_1

$\cdots$.

the coefficient concatenation $a'_{s0}||a'_{s1}||\cdots||a'_{s(t-1)}$ of $A'_s(x)$ as k'_s

6. With $(k_1, k'_1), (k_2, k'_2), \cdots, (k_s, k'_s)$ the interpolating polynomial $B(x)$ is constructed, the coefficient concatenation $r = b_0||b_1||\cdots||b_{s-1}$ of the interpolating polynomial and $R = hash(r)$ are all published with intermediate values $(k_1, k'_1), (k_2, k'_2), \cdots, (k_s, k'_s)$.

If U_{ij} who is in the i^{th} row and j^{th} column wants to verify the generation of r, the verification procedure is as follows:

1. U_{ij} picks its $m_{ij} = (x, y)$, and verify the equation $A_i(x) = y$, $A'_i(y) = x$. If they are true, (k_i, k'_i) is trusted.

2. U_{ij} verifies the equation $k'_i = B(k_i)$. If it is true, $m_{ij} = (x, y)$ is involved in generating $r = b_0||b_1||\cdots||b_{s-1}$.

3. After $r = b_0||b_1||\cdots||b_{s-1}$ is verified by U_{ij}, the only work is to verify the equation $R = hash(r)$.

3 A Fair E-lottery Scheme Based on Verifiable Random Number

In this section, we propose a fair e-lottery scheme in which two parties are lottery purchasers and dealer (or computing center), the TTP is not required. The scheme consists of four phases: "Setup", "Ticket Purchasing", "Winning Result generation", and "Verification". We mainly focus on the fairness of the scheme, omit other details.

—Setup

Dealer chooses proper prime p according the expected sale volume and publishes it. Dealer publishes secure hash function $hash(.)$ which is used as random oracle. Dealer publishes digital signature algorithm $sig_x(y)$ which denote the data y is signed by x.

—Ticket Purchasing

E-lottery purchaser sends a request to Dealer and gets a serial number SN from dealer, then chooses a favorite number y_{SN} in F_p and sends it to dealer. Dealer sends the SN^{th} lottery ticket $ticket_{SN} = sig_{dealer}(SN||y_{SN})$ to purchaser. Every ticket's SN is different.

—Winning Result Generation

Serial number of dealer is denoted by max_SN, Dealer constructs the interpolated polynomial in F_p with all (SN, y_{SN}) and (max_SN, y_{max_SN}).Dealer generates r and $R = hash(r)modp$ using the method of section 2.

Dealer publishes R, r and $(k_1, k'_1), (k_2, k'_2), \ldots, (k_s, k'_s)$ for verification.

The purchaser whose serial number is same as R can claim to be lucky in the scheme and apply to get prize.

—Verification

If a participant wants to verify whether R and r is authentic, he verifies whether his SN, y is involved in the procedure of generating r. If the verification is hold, the winning number r is not colluded by others.

4 Analysis

In our improved scheme, the generation of the winning number involves all the participants. Every participant provides his favorite number to involve the process of generating result. Comparing with the previous scheme, the improved scheme is more efficient and fair for all entities, which prevent dishonest from colluding.

1. The process of generating VRN is efficient. For simple analysis, supposing that it is easy for CC to calculate a polynomial constructed by 100 points, we denote the computation time for generating polynomial is t. The two-level structure can contain 100^2, three-level structure accommodates 100^3 participants. But in our scheme, the computation time of constructing interpolating polynomial is only from t to $3t$ when the number of participant increasing from 100 to 100^3. In a word, the computational time increases lineally when the number of participants rises exponentially.

2. The verification is light. For example, there are 100^3 participants whose ticket data are distributed in 100 matrix, $M_1, M_2, \ldots, M_{100}$. Three-level structure is as shown in Fig. 1. $A(x)$ is the first level, $B(x)$ is the second level, and $C(x)$ is the third level.

$$
\begin{array}{l}
M_1 \rightarrow \begin{matrix} (A_1(x), A_1^{'}(x)) \\ \vdots \\ (A_{100}, A_{100}^{'}) \end{matrix} \rightarrow \begin{matrix} (k_1, k_1^{'}) \\ \vdots \\ (k_{100}, k_{100}^{'}) \end{matrix} \rightarrow (B_1(x), B_1^{'}(x)) \rightarrow (s_1, s_1^{'}) \\
\cdots\cdots\cdots\cdots \\
M_{100} \rightarrow \begin{matrix} (A_{9901}(x), A_{9901}^{'}(x)) \\ \vdots \\ (A_{10000}(x), A_{10000}^{'}(x)) \end{matrix} \rightarrow \begin{matrix} (k_{9901}, k_{9901}^{'}) \\ \vdots \\ (k_{10000}, k_{10000}^{'}) \end{matrix} \rightarrow (B_{100}(x), B_{100}^{'}(x)) \rightarrow (s_{100}, s_{100}^{'})
\end{array}
\Bigg\} \rightarrow C(x) \rightarrow r
$$

$\underbrace{\qquad\qquad}_{first-level}$ $\underbrace{\qquad\qquad}_{second-level}$ $\underbrace{\qquad}_{third\text{-}level}$

Fig. 1: 3-levels Interpolated polynomial structure

When the 100000^{th} purchaser wants to verify, he knows his position is in the M_{10}, he only need to verify $A_{1000}(x_{100000}) = y_{100000}$, $A_{1000}^{'}(y_{100000}) = x_{100000}$, $B_{10}(k_{1000}) = k_{1000}^{'}$, $B_{10}^{'}(k_{1000}^{'}) = k_{1000}$ and $C(s_{10}) = s_{10}^{'}$, their computation cost is low, which makes it more suitable for portable terminal whose condition is restricted.

3. The proposed structure can be extend to multi-level easily. If the number of participants is enormous, the matrix M may be extend from $100 - by - 100$ to $150 - by - 150$, or the levels may be extend from 3-level to 4-level, or more, they are implemented conveniently.

The proposed e-lottery based on verifiable random number is fair for all entities. Every ticket is involved in generating the winning number. Even if single ticket is not controlled by others, the final result is unpredicted and random, which is fair for all.

5 Conclusions

There are many applications for lottery, which is used to design electronic commerce protocol to ensure fairness. With Interpolated polynomial over F_p, a verifiable random number is given. Based on VRN, a fair e-lottery scheme is proposed, which is fair, efficient and secure, suitable for wireless mobile environment.

References

[1] Silvio Micali, Ronald L. Rivest. Micropayments Revisited. In CT-RSA'2002. LNCS 2271, pp. 149-163, Springer

[2] Sherman S. M. Chow, Lucas C. K. hui, S. M. Yiu, and K. P. Chow. An e-lottery scheme using Verifiable Random Function. In ICCSA'2005, LNCS3482, pp. 651-660, 2005, Springer

[3] Yining Liu, Lei Hu. Using an efficient hash chain and delaying function to improve an e-lottery scheme. International journal of computer mathematics. Vol. 87, No. 7, July 2007, pp. 967-970

[4] Anzai J, Matsuzaki N, Matsumoto T. A quick group key distribution scheme with entity revocation. ASIACRYPT' 99, LNCS 1716, 1999: 333-347

[5] Kurnio H, Safavi Naini R, Wang Huaxiong. A group key distribution scheme with centralized user Join, LNCS 2576: 146-163 2003

[6] V. Shen and T. Chen, A Novel Key Management Scheme based on Discrete Logarithms and Polynomial Interpolations, Comput. & Security, 21(2), 164-171, 2002

[7] W. G. Tzeng, A secure fault-tolerant conference key agreement protocol, IEEE Transactions on Computers, Vol. 51 (4) (2002), pp. 373-379

[8] M. L. Das, A. Saxena, V. P. Gulati and D. B. Phatak, Hierarchical key management scheme using polynomial interpolation, SIGOPS Operational Systematic Review 39 (1) (2005), pp. 40-47

[9] W. H. Kim, E. K. Ryu, J. Y. Im and K. Y. Yoo, New conference key agreement protocol with user anonymity, Computer Standards, &Interfaces 27 (2005), pp. 185-190

[10] Lein Harn, Changlu Lin. Authenticated group key transferr protocol based on secret sharing. IEEE Transaction on Computer, 59(6), 842-846, 2010