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.