A Secure On-line Lottery Using Bank as a Notary

Wooseok Ham and Kwangjo Kim

International Research center for Information Security (IRIS), ICU, KOREA

Abstract

In this paper, we present a secure on-line lottery protocol which consists of three entities: the players, the lottery provider and the bank. We utilize blind signature and hash chain technique as basic building blocks. Our protocol faithfully satisfies the general security requirements to deal with electronic transactions in safe. The proposed protocol reduces the number of communications and all transactions are executed through the Internet(On-line). By using bank as a notary and bulletin board managed by the lottery provider, we can easily settle down potential disputes which frequently occur during commercial transactions.

I. Introduction

Since the lottery is one of the most interesting and attractive games, it has been used in the various purposes: to finance a certain project, to fund municipal capital, and to promote an event, *etc*. This inherent features currently result in a variety of nationwide or local lotteries in these days. Furthermore, as the Internet has remarkably affected human's activities concentrated into electronic ways, the lottery also has been changing from the typical paper- based system to an electronic one.

Electronic lottery must be really easy, effective and cheap so that it presents lots of advantages to players as well as the lottery provider with respect cost and time. Due to these, the lottery providers have been trying to adopt the Internet for their lottery more and more. However, as other e-commerce applications, the limited resources, the openness of the networks and anonymous transactions are traditional barriers in order to facilitate the Internet for e-commerce. We should prevent the lottery system from various potential attacks [1] which compromises the security of lottery systems. Even though a few lottery systems are available currently, most of them are too simple and weak to support necessary security without performance degradation.

Our target model of the lottery system is a multiple-choice-based lottery like a horse race or SportsTOTO [7]. So the result of lottery is announced in public as soon as the game terminates. Through this paper, we will suggest a secure lottery protocol to address security requirements. The proposed protocol also minimizes communicational overhead among entities and every communication is performed through the Internet.

This paper is organized as follows: In Section Ⅱ we define the basic requirements of the on-line lottery systems. Section Ⅲ describes previous works on the on-line lottery in the literature. Our proposed scheme is illustrated in Section Ⅳ in detail and its evaluation and comparison will be given in Section Ⅴ We will finish with our conclusion in Section Ⅵ

II. Requirements

Several requirements should be satisfied to make use of the Interent for the lottery system preserving security and efficiency.

○ Privacy: Identities of all players are kept in safe during whole transactions and even after the end of the lottery.

○ Fairness: No entity has disadvantages in transactions.

○ Publicly verifiability: Anybody can calculate and verify the result.

○ Reliability: Any lottery entity cannot do malicious activities without detection.

○ Unforgeability: The probability of tampering the lottery ticket is negligible.

○ Timeliness: A lottery should be terminated in the pre-defined time.

○ Accountability: All disputes can be traced and proved who committed a fault.

III. Previous Works

There have been a few proposals to resolve security and efficiency requirements, but most of them partially satisfy the requirements.

Goldschlag and Stubblebine [3] proposed a drawing-number-typed lottery based on delaying function. However, the verification of the winning number takes the same time as the total running time of delaying function. Kushilevitz and Rabin [5] improved computational complexity of [3] by applying intermediate result of delaying function. A problem of this scheme is that players' participations after closing the lottery are mandatory to decide the winner(s) and the winning pool, *i.e.*, this scheme doesn't have walk-away property. Zhou and Tan [8] presented a lottery protocol that includes the bank as an entity adopting CEMBS[2]. But its employment makes the scheme more complicated so a player should interact several times with the bank and the lottery provider to finish all procedures. However, most serious problem of these schemes [3,5,8] are that all are based on not multiple-choice but single-choice which doesn't match to our target model.

Kobayashi, Morita, Hakuta and Nakanowatari [4] suggested a scheme based on multiple-choice. They used bit commitment and one-way hash function as building blocks. We briefly introduce their scheme since we mainly compare our scheme to their scheme. Their protocol consists of 3 phases:

○ **Purchase**: A player sends both his target lottery pattern TLP and its hashing value $H1(=Hash(Hash(PID) \| TLP))$ with the payment to the shop. The shop returns its identity SID as a receipt to the player then transfers TLP and $H1$ to the lottery provider with SID. The lottery provider generates $H2(=Hash(SID \| H1))$ then posts TLP and $H2$ on its bulletin board.

○ **Inquiry**: Each player asks his ticket registration status by sending the partial bits of $H2$ to the lottery provider. The lottery provider retrieves all TLPs matching to the partial bits from the database and returns them to the player. If there is a fully matching value, the player convinces of the right registration of his ticket.

○ **Payment**: This phase is performed in both on-line and off-line. First, the winner shows $Hash(PID)$ to the bank in on-line for verification then presents his real identity PID in off-line when he receives the winning prize.

It seems to be practical but not secure. In their scheme, the final digital signature(= $Sig(\sum_{i=1}^{n} TLP_i \| H2_i)$ of the lottery provider is generated when closing the lottery. But, since the digital signature is the signed message of summation of all TLP and $H2$, a malicious lottery provider is able to easily alter his tickets by submitting multiple tickets of his own in advance. In addition, this protocol doesn't meet fairness as there is no signed receipt or any notary service so it cannot trace and judge who is faulty when a dispute occurs. Off-line transaction in Payment phase also feel the players inconvenience in some sense.

IV. The Proposed Scheme

1. Notations and Assumptions

We denotes a player by P, the lottery provider by LP and the bank by B. A player's ticket information which contains his betting is represented *TI*. *Hash*() and *HC*() indicates hash function and hash chain, respectively. $Dsig_E$ denotes digital signature generated by entity *E* using signature function *Sign*(). We don't restrict our digital signature scheme into a specific one. *Pay* is an electronic payment script which can be also one out of several micropayment candidates such as *PayWord* or *Micromint* [6]. This payment script is generated by *P* according to pre-defined rule. ∥ means the concatenation of two strings. Some other notations will be illustrated in the spot where they appear.

Our protocol makes use of RSA blind signature scheme to conceal betting information and payment information of each player. For RSA cryptosystem, we denote *B*'s public key by (e, n) and secret key by *d*. All exponent computation is performed under modulo *n*, otherwise stated. We assume that *B* is trustful and not collude as in real world. We also suppose every connection is built upon a secure channel such as SSL.

2. Our Proposed Scheme

Our scheme is composed of 3 phases: Preparation, Betting and Deposit phases.

1) Preparation Phase

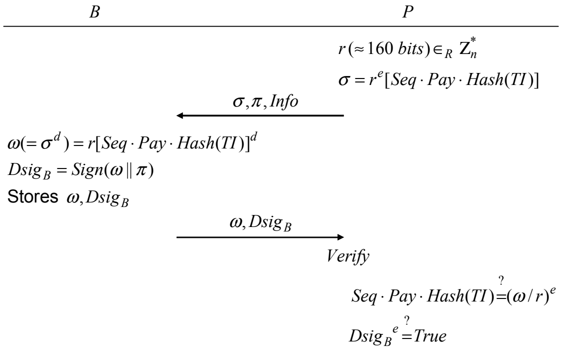
B
P
$r(\approx 160\ bits) \in_R Z_n^*$
$\sigma = r^e[Seq \cdot Pay \cdot Hash(TI)]$
$\sigma, \pi, Info$
$\omega(=\sigma^d) = r[Seq \cdot Pay \cdot Hash(TI)]^d$
$Dsig_B = Sign(\omega \parallel \pi)$
Stores $\omega, Dsig_B$
$\omega, Dsig_B$
Verify
$Seq \cdot Pay \cdot Hash(TI) \overset{?}{=} (\omega / r)^e$
$Dsig_B{}^e \overset{?}{=} True$

Fig. 1: Preparation protocol

In Fig. 1, π represents the amount of *Pay* and *Info* is additional information to identify *P* 's account. *Seq* denotes the serial number of the participating lottery. Using blind signature, *P* is able to receive the signature $Dsig_B$ on both payment information *Pay* and betting information *Hash*(*TI*) without disclosing these information. It enhances the player's privacy and *B* notarizes *Hash*(*TI*). Note that betting information is the hashed value not the information itself.

2) Betting Phase

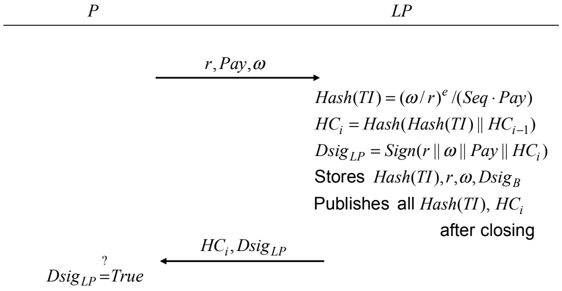
P
LP
r, Pay, ω
$Hash(TI) = (\omega / r)^e / (Seq \cdot Pay)$
$HC_i = Hash(Hash(TI) \parallel HC_{i-1})$
$Dsig_{LP} = Sign(r \parallel \omega \parallel Pay \parallel HC_i)$
Stores $Hash(TI), r, \omega, Dsig_B$
Publishes all $Hash(TI)$, HC_i
after closing
$HC_i, Dsig_{LP}$
$Dsig_{LP} \overset{?}{=} True$

Fig. 2: Betting Protocol

P transfers the signed betting information and blinding factor with the payment script. Then *LP* checks the correctness of received values and computes hash chain output using them. Since hash chain output implies the previous hash chain result, *LP* cannot do illegal activities such as modification of the hash output and insertion of other betting information without detection. *LP* returns HC_i and $Dsig_{LP}$ as a receipt. When the betting session ends, the lottery provider reveals all hashed bets and hash chain values to the bulletin board.

3) Deposit Phase

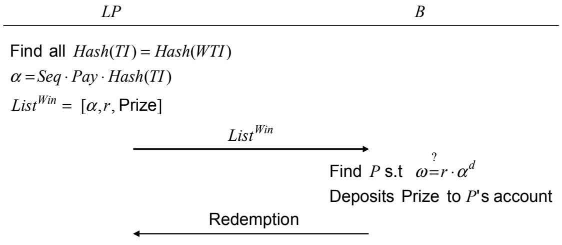
LP
B
Find all $Hash(TI) = Hash(WTI)$
$\alpha = Seq \cdot Pay \cdot Hash(TI)$
$List^{Win} =$ [α, r, Prize]
$List^{Win}$
Find P s.t $\omega \overset{?}{=} r \cdot \alpha^d$
Deposits Prize to P's account
Redemption

Fig. 3: Deposit Protocol

This phase is carried out after the game. Here *WTI* denotes the result of game. Winning information $List^{Win}$ could contain plural winners if exists. *LP* requests redemption to the bank after subtracting *Prize* from *ΣPay* which is the summation of bets of players. *B* deposits *Prize* to the winner's account after doing verification.

V. Evaluation and Comparison

We briefly evaluates our protocol in terms of requirements due to the space. Entire justifications will be appeared in our full paper.

Privacy is kept by blind signature, even *LP* doesn't know who has participated in the game as no player information is included in the messages from *P* in the betting phase. Every transaction is conducted in challenge-response way, in addition, digital signatures generated by *B* and *LP* consolidate fairness. Reliability and accountability also are preserved from the digital signatures and published values by *LP*. Publicly verifiability and Timeliness is straightforward.

Table 1 shows the comparison of our protocol to [4] with respect to security requirements.

Table 1. Security Comparison

	[4]	Our protocol
Privacy	O	O
Fairness	X	O
Publicly Verifiability	O	O
Reliability	X	O
Unforgeability	X	O
Timeliness	O	O
Accountability	X	O

Another advantages of our protocol compared to [4] are: our protocol is composed of only *three* entities, all communications including deposit phase are performed in *on-line*, total communication rounds(4 rounds) of a player is less then than of [4](7 rounds). Disadvantage to [4] comes from the volume of message-the biggest one is 256 bytes from *B* to *P* in our protocol-since modulo outputs and digital signature are transferred. However, we argue that such size(256 bytes) is not serious under the current high speed networks. In fact, [4] also should provide countermeasures like digital signature to address all security requirements then it will inevitably increase the message volume.

VI. Conclusion

We proposed a secure and efficient tripartite on-line lottery protocol including the bank as a notary. Our scheme utilizes blind signature to enhance player's privacy and also satisfies all security requirements. Furthermore, the message volume is so reasonable that it can be efficiently transmitted through the Internet. Any dispute during transactions among entities can be traced and resolved with the public information and digital signatures. Our protocol can be easily extended to the drawing number type lottery as well.

For further works, strict security proof of the proposed protocol and combining with suitable payment and signature scheme are required.

References

[1] R.Anderson, *How to cheat at the lottery*, Proc.of Computer Security Applications Conference, 1999.

[2] F.Bao,R.Deng and W.Mao, Efficient and Practical Fair Exchange Protoocls with Off-line TTP, IEEE Symposium on Security and Privacy, pp.77-85, 1998.

[3] D.M.Goldschlag and S.G.Stubblebine, *Publicly verifiable lotteries: Applications of delay functions*, FC '98, LNCS 1465, pp.214-226, 1998.

[4] K.Kobayashi, H.Morita, M.Hakuta and T.Nakanowatari, *An Electronic Soccer Lottery System that Uses Bit Commitment*, IEICE Transactions on Information and Systems '00, Vol.E83-D, pp.980-987, 2000.

[5] E.Kushelevits and T.Rabin, *Fair e-lotteries and e-casions*, CT-RSA '01, LNCS 20202, pp.100-109, 2001.

[6] R.Rivest and A.Shamir, *PayWord and Micromint: Two simple micropayment schemes*, International worksoph on Security protocols, LNCS 1189, pp.69-87, 1997.

[7] SportsTOTO, available at http://www.tigerpools.co.kr.

[8] J.Zhou and C.Tan, *Playing Lottery on the Internet*, ICICS 2001, LNCS 2229, pp.189-201, 2001.