



An Efficient Internet Bingo Scheme

Sattar J. Aboud*, Mohammad A. AL-Fayoumi

Faculty of Information Technology

Al-Isra University, Jordan-Amman

Abstract— in this paper, we propose a secure virtual casino for large number of players; the multicast network is credible to be used for one-to-many communication. So, we introduced the scheme for Internet bingo by which prevents the failure in many-to-one transmission between the players and a bingo hall. The scheme combines bits employing the probabilistic public-key encryption and promises a security of communication.

Keywords— Internet bingo, multicast network, many-to-one communications, one-to-one communications

I. INTRODUCTION

With an extensive utilization of Internet, lots of virtual casinos use e-versions of some like bingo [1, 2]. With constructing a secure Internet version for bingo to many players, the multicast network is possible to be employed for one-to-many transmission [3]. The multicast transmission includes one source passing the one stream of bits to the set of multicast routers. The stream bits overflow a multicast tree so that efficiently reach each client started with a present session. Before the multicast communication starts, a session is publicized to possible clients [4]. Responses are generated by Internet Group Management Protocol. Figure 1 shows the mechanism of the protocol. This protocol gives a source with bits regarding who is interested in next session. By this communication, the best multicast tree is constructed. Employing multicast communication for one-to-many transmission results in a considerable saving in bandwidth and memory employed in transitional routers [5].

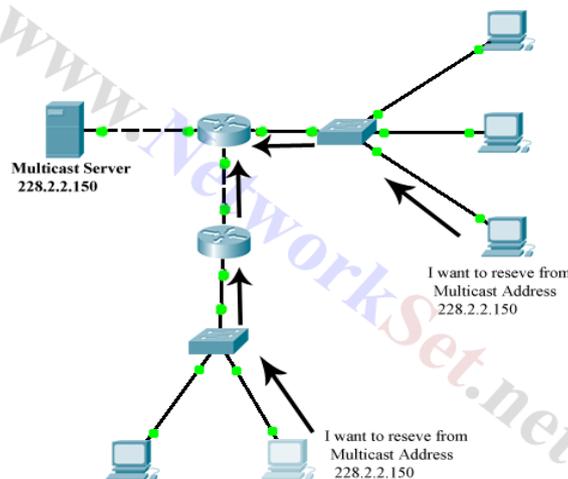


Figure 1: Shows the protocol

For many players, reverse many-to-one transmission can possibly failure the source. So, we need the solutions to prevent this failure. Going a bingo game from physical casinos to virtual game needs many-to-one transmission between players and virtual hall. When a game is played on virtual, special care should be taken to prevent failure of transmissions on a part of virtual hall [6]. In this paper, we introduced a scheme of bingo that prevents failure in many-to-one transmission between players and the hall. The resulting scheme combines bits employing a probabilistic public-key to promises security of transmissions.

This paper is organized as follows. Section 2 illustrates scheme passes information from many players to a source. The secure virtual bingo is illustrated in Section 3. In Section 4 a security of a scheme is discussed.

II. MULTICAST COMMUNICATION

In this section, we illustrate the scheme that passes information from many players to a source by a multicast connection. In the multicast protocol there are three players, these are as follows:

1. The source multicasts several bits to each player in a session.
2. The transitional routers combine bits and pass them to the father router.
3. The player obtain the bits by multicast then pass them to a source,

However, the scheme contains two protocols which are as follows:

Protocol 1: Set-up

The steps of the protocol are as follows:

1. The source should do the following:
 - Select an exponent key x
 - Select an integer p represent player.
2. The source creates $2p$ as follows:
 - Compute $y_1 = (1, 2^x - 1)$
 - Compute $y_j = y_j^{\min}, y_j^{\max}$

$$= ((2^j - 2)(2^x - 1) + 2^{j-1} - 1, (2^j - 1)(2^x - 1) + (2^{j-1} - 1))$$
 - for $j = 2$ to $2p$ do
3. A source creates keys r_i using block cipher for $i = 1$ to p do
4. A source creates the key pair for the probabilistic public-key so that its message space is $g = (0, 1, 2, \dots, w-1)$ such as w must be greater than $2y_{2p}^{\max} + 1$. After certain operation, it can be shown that a lower bound of w is

$$w > (2p-1)(2^{x+1} - 1) \quad (1)$$
5. The source multicasts a public key and $y_{2i-1}^{\min}, y_{2i-1}^{\max}, y_{2i}^{\min}, y_{2i}^{\max}$ for $i = 1$ to p do
6. The source privately passes r_i to every player p_i , who must keep this key private in a smart card.

Following the set-up, a usual process of a scheme comprises many-to-one communications of binary bits. To gather the binary bits from every player, the following four-step protocol is employed:

Protocol 2: Many-to-one Communication

1. Transmission request. The challenge message is multicast by a source to each player. This challenge message includes the arbitrary value f .
2. Message generation.
 - If the player p_i obtains a challenge message, he finds

$$s_{2i-1} = y_{2i-1}^{\min} + h(f + r_i)$$

$$s_{2i} = y_{2i-1}^{\min} + h(f + 1 + r_i) \quad (2)$$
 Such as h is a secure hash function giving x -bit hash value. This result of h guarantees that $s_{2i-1} \in y_{2i-1}$, and $s_{2i} \in y_{2i}$. Also, the value of h guarantees that g no overflow in g can happen in a cipher-text space.
 - Then, every player p_i creates his message as follows:
 - When he needs to transfer 0 bit value, he creates a message $m_i = e(s_{2i-1})$ such as e is a public-key of a probabilistic scheme employed.
 - When he needs to transfer 1 bit value, he creates a message $m_i = e(s_{2i})$
 - In case of sending three bits, the third bit other than 0 and 1, can be transferred if p_i pass $m_i = e(s_{2i-1} + s_{2i})$
 - Finally p_i passes m_i to his parent router.
3. Message combination. Middle routers accept messages from their child routers and do the following:
 - When all predictable messages m_i have been obtained, a router combines them as $m = \sum_i^- m_i$ such as \sum^- indicate an encrypted message process of a probabilistic scheme according to clear-text addition.
 - The router passes m to its parent router.
4. Bit extraction. If a previous operation finishes, a source obtains a combined message m , from which a transferred bit is extracted as follows:
 - The source builds a super-increasing sequence $s = (s_j)$ for $j = 1$ to $2p$ do for every player p_i , applying formula (2).
 - The source decrypts m employing its private key to retrieve the value T which is used to solve a super-increasing knapsack problem [7] and find a sequence $s' = (s_1, s_2, \dots, s_j)$ that gives the bit value passed by a player. There are four cases for every player p_i
 1. If $s_{2i-1} \notin s'$, and $s_{2i} \notin s'$, then p_i passed nothing.
 2. If $s_{2i-1} \in s'$, and $s_{2i} \notin s'$, then p_i passed the bit value 0.
 3. If $s_{2i-1} \notin s'$, and $s_{2i} \in s'$, then p_i passed the bit value 1.

4. If $s_{2i-1} \in s'$ and $s_{2i} \in s'$ then this is inaccuracy in the binary transmission.

III. SECURE BINGO SCHEME

First we will describe the physical bingo game which is as follows:

A. Description of Physical Bingo

Physical bingo is played in the hall. Players encounter at a hall and a game starts. The following explanation relate to European scheme. The bingo game starts as follows:

1. There are 99 probable bingo numbers $B = (1..99)$. Every number is denoted by the ball in the big rotating box. Every ball has its unique bingo number.
2. Each player has bingo card with 15 mix numbers. The numbers are dispersed in three rows, but every row has five numbers.
3. A presenter spins a box then picks the ball or let the computer arbitrarily chooses the number. The number is proclaimed to the spectators.
4. Then every player checks its card to notice if a proclaimed number looks on it.
5. This operation is repeated till the bingo or the line is exclaimed. This means that there are two winning patterns:

Line: When numbers in the row have been chosen, its owner exclaims line. A game pauses whereas a card is checked. When the line has been fulfilled, a player obtains about 8% of a total gamble. Afterward, a game continues, but no one else can exclaim the line.

Bingo: If all numbers on the card have seemed, its holder should exclaim bingo. A game pauses whereas a card is checked. When an entire card has been finished, a game completes. Note that a game should finishes, since somebody will fulfil the card sooner or later.

B. Secure Bingo Scheme

Now, the e-version of an above bingo rules is illustrated.

Registration

A source proclaims the registration period to let new players to connect. If the player is like to joining the Internet bingo hall, he enrolls to a source using the unicast communication. The keys employed in Protocols 1 and 2 are provided by a source. This needs to send new keys to players in a system.

Game Opening

In physical bingo, card is created and provided by a source. In e-bingo, every player arbitrarily generates his bingo card as follows:

1. Each player p arbitrarily selects 15 different numbers to load his bingo card c_p . The numbers are classified in ascending order and distribute in three rows, each row has five numbers.

$$\delta_x^p = (b_{x,1}, b_{x,2}, b_{x,3}, b_{x,4}, b_{x,5})$$

for $x = 1..3$ do

$$c_p = (\delta_1^p, \delta_2^p, \delta_3^p)$$

2. A player finds the secure hash value of every line x , as follows:

$$h_x^p = (b_{x,1}, b_{x,2}, b_{x,3}, b_{x,4}, b_{x,5}, d_x)$$

Such as d_x is arbitrary number, and pass a hash value to a source. Thus, a player devotes to a chosen hash result. The hash value is passed to a source one bit each time by Protocol 2. Such process prevents bits failure at a source.

3. A Protocol 2 promises that a source realizes an identity of new game players, as illustrated below.
4. Throughout this step, players can do e-payment that lets them to play. Else, the subscription type can be applied for payment.

Game Process

After a game started, bingo numbers are arbitrarily selected by a source and verified by players.

1. The bingo number b is arbitrarily selected. This number cannot see again in an existing bingo game because of bingo rules. The b multicast to each player.
2. Each player verifies if b is in his bingo card. If yes, b is marked.
3. The communication request is multicast by a source to each player. The player p_i creates the message m_i consistent with the following message-to-bit mapping:
 - a. s_{2i-1} = Player has obtained a number, but has not finished the line or bingo.
 - b. s_{2i} = The five numbers of $\delta_0^{p_i}, \delta_1^{p_i}$, or $\delta_2^{p_i}$ have done line.
 - c. $s_{2i-1} + s_{2i}$ = The numbers of c_{p_i} have done bingo

Messages are passed and combined following steps 3a and 3b of protocol 2.

4. The source finally obtains a combined message m , from which the transferred bits are extracted.
 - When the player p_i has passed the line message, the uncast joining is set up between a source and p_i . The latter passes the message to a source having bingo numbers of a winning line, and d_x value used for that line. A source then verifies a hash p_i devoted to a start of a game according to send line. After all messages from line-winning players have been verified, no more line messages will be received because of bingo rules.
 - When the user p_i has passed the bingo message, p_i passes to a source the three lines of c_{p_i} and corresponding d_x values for verifying.

IV. SECURITY DISCUSSIONS

Now, we describe the security characteristics of the proposed scheme, which are as follows.

1. Confidentiality: When the secure probabilistic public-key scheme is used in which the slight probability of finding a same encrypted message as the result of two independent encryptions of the same message, then an impostor cannot fix a bit transmitted by the user in Protocol 2.

Proof of Confidentiality: Suppose an impostor obtains the message m transmitted by p_i through Protocol 2. The message m is either $e(s_{2i-1})$, $e(s_{2i})$ or $e(s_{2i-1} + s_{2i})$. Decryption of message m is impossible since an impostor is not having access to a secret key. Sequentially search for a message is another attack approach to be studied. Since search for a sequence values s_{2i-1} or s_{2i} by encrypting messages and comparing a value to message m is not possible as a scheme is probabilistic and there is a small prospect with two separate encryptions of a same message produce a same message. Thus, a comparison and a sequentially search will not succeed with irresistible probability.

2. Authentication: When the secure probabilistic public key scheme and the secure one-way hash function with x -bit yield are used, the following holds:

1. The probability of successful impersonating if sending bit value to a source is 2^{-x}
2. Replacing false message m' over real message m across transmission is hard as impersonation
3. Replacing message m' over real message m in upcoming transmissions from existing transmission is impossible.

Proof of Authentication: The impostor who needs to impersonate player p_i goes to create a message $e(s_{2i-1})$, $e(s_{2i})$ or $e(s_{2i-1} + s_{2i})$. Then, an impostor wants to find s_{2i-1} or s_{2i} . Every round s_j of a super-increasing sequence s is arbitrarily selected within range y_j having 2^x values. The select is made by a hash value of a challenge and a private key r_i unknown to an impostor, as shown in formula (2). So, a probability of an impostor arbitrarily defeat s_j is 2^{-x} . The sequentially search is not possible, because there is no way of verifying if a right s_j is hit. A substitution attack can be framed in an existing transmission:

1. In an existing transmission, suppose an impostor needs to replace a false message m' instead of a real message m sent by p_i with. However, assume $m = e(s_{2i})$; an impostor needs to transform m in $m' = e(s_{2i-1} - s_{2i})$ or $m' = e(s_{2i-1})$. This needs the following steps:
 1. Retrieve s_{2i} from m
 2. Find s_{2i-1} with knowledge of s_{2i}
 3. Find m' . Thus, even if recovering m at step 1 was easy which does not; resolving step 2 is as hard as increasing the successful impersonation attack.
2. The second option for an impostor is to use bits resulting from existing transmission of a message by p_i to modify upcoming messages sent by p_i . But this is impossible, since in the executions of Protocol 2, the super-increasing sequence is used to encrypt a message which is not relied on an existing super-increasing sequence.

V. CONCLUSIONS

Changing a bingo game from physical version to a virtual version needs efficient and secure many-to-one transmission between players and a source. This paper has proposed a scheme for virtual bingo which prevents failure in many-to-one transmission. The resulting scheme combines bits using the probabilistic public-key scheme and promises a security of communications.

ACKNOWLEDGMENT

Causal Productions wishes to acknowledge Michael Shell and other contributors for developing and maintaining the IEEE LaTeX style files which have been used in the preparation of this template. To see the list of contributors, please refer to the top of file IEEETran.cls in the IEEE LaTeX distribution.

REFERENCES

- [1] National Indian Commission, Technical Standards for “Electronic Computer or Other Technologic Aids” Used in the Play of Class II Games, Proposed Rules, Vol. 71, No. 155 / Friday, August 11, 2006, pp. 46336-46361
- [2] Antoni Martí nez-Ballest e, Francesc Seb e and Josep Domingo-Ferrer, “Secure Large-Scale Bingo”, Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC’04) 2004, pp. 758-762, IEEE
- [3] Jordi Castella-Roca, Josep Domingo-Ferrer, Andreu Riera, and Joan Borrell, “Practical Mental Poker without a TTP Based on Homomorphic Encryption”, INDOCRYPT 2003, LNCS 2904, pp. 280–294, 2003, Springer-Verlag, Berlin Heidelberg 2003
- [4] Gambling Commission report, Bingo and Casino Equipment Technical Requirements, July 2008
- [5] Christian Henrich, Improving and Analyzing Bingo Voting, PhD Dissertation, Karlsruher Institutes of Technology (KIT), 2012.
- [6] John L. McMullan & Aunshul Rege, “Online crime and internet gambling”, Journal of Gambling Issues: Issue 24, July 2010, pp. 54-85.
- [7] R. C. Merkle and M. Hellman, “Hiding information and signatures in trapdoor knapsacks”, IEEE Transactions on Information Theory, vol. 24, no. 5, pp. 525-530, 1978.