Secret Bit Transmission Using a Random Deal of Cards on Hierarchical Structures

Reina Yoshikawa (吉川 玲奈) and Yoshihide Igarashi (五十嵐 善英)

Department of Computer Science, Gunma University, Kiryu, Japan 376-8515
E-mail:igarashi@comp.cs.gunma-u.ac.jp

Abstract

We propose a problem how we transmit an information-theoretically secure bit using a random deal of cards among players in hierarchical structured groups and a computationally unlimited eavesdropper. A player in the highest group wants to send players in lower groups a secret bit which is secure from the eavesdropper and some other players. We formalize this problem, and we design a protocol for constructing a secret key exchange spanning tree on two-level hierarchical groups of players. Then for the protocol we analyze the conditions that the secure bit transmission by the protocol is successful. We give a sufficient condition that the protocol successfully works on the sizes of hands of players and an eavesdropper.

key words: card games, hierarchical structured groups, information theoretically-secure, key exchange graph, secret bit transmission,

1 Introduction

Suppose that there are n players and a passive eavesdropper, Eve, whose computational power is unlimited. The n players are partitioned into hierarchical groups, $G_1, \ldots, G_h$, where $G_1 = \{P_{1,1}, \ldots, P_{1,k_1}\}, \ldots, G_h = \{P_{h,1}, \ldots, P_{h,1}, \ldots, P_{h,k_h}\}$ and $|G_i| \geq 1$ for each $1 \leq i \leq h$. For each pair of $i$ and $j$ ($i \neq j$), $G_i \cap G_j = \emptyset$, and $\bigcup_{i=1}^{h} G_i$ is the set of the n players (i.e., $n = \sum_{i=1}^{h} k_i$). We assume that the hierarchy of the groups $G_1, \ldots, G_h$ is in the suffix order. That is, $G_i$ is higher than $G_j$ in the hierarchy if $i < j$. Using a random deal of cards we construct a spanning tree with node set $\bigcup_{i=1}^{h} G_i$ satisfying the following conditions, where a node denotes a player:

1. A pair of nodes directly connected by an edge of the spanning tree has a secret key exchange.

2. For each $1 \leq j \leq h$, the subgraph of the spanning tree consisting of the nodes in $\bigcup_{i=1}^{j} G_i$ and their incident edges is a spanning tree of the nodes of $\bigcup_{i=1}^{j} G_i$.

3. If a pair of nodes are connected by an edge of the spanning tree, then both the nodes in the same group, or the one node is in $G_i$ and the other node is in $G_{i+1}$ for some $i$ between 1 and $h - 1$.

Once such a spanning tree is constructed, bit secret communication is possible between a pair of nodes directly connected by an edge of the spanning tree. In this paper we assume that communication from a node in a group to a node in any group higher than the group is inhibited.
even if the two nodes are connected by an edge of the spanning tree. The subtree rooted at a
node in group $G_i$ is a subtree rooted at the node of the spanning tree consisting of nodes not
in any group higher than $G_i$. A player chooses a secret bit, and using the subtree rooted at the
player can send the secret bit to a player in the subtree in the following fashion. If player $P_{i,j}$
wants to send a secret bit $r$ to player $P_{t',j'}$ along an edge $(P_{i,j}, P_{t',j'})$ of the subtree, $P_{i,j}$ computes
the exclusive-or $r \oplus r'$ and sends it to $P_{t',j'}$, where $r'$ is the secret exchange key between $P_{i,j}$
and $P_{t',j'}$. Then $P_{t',j'}$ obtains $r$ by computing $r \oplus r' \oplus r' = r$. Repeating this method a player
can send a secret bit to any node of the subtree rooted at the node of the player. This bit
transmission is information theoretically secure from not only Eve but also any node not in the
the path of the bit transmission. When the number of the hierarchical groups of the players is
just 1, this problem is the same as the secret key exchange using a random deal of cards studied
in [1][2][3][4]. Constructing a secret key exchange spanning tree on the hierarchical structured
players satisfying the three conditions listed above is therefore a more general problem.

2 Preliminary

Fischer and Wright proposed a protocol called the smallest feasible protocol (SFP for short) for
the one-bit secret key exchange [2]. Suppose that there are $n$ players and a passive eavesdropper
Eve. Let each player $P_i$ hold $c_i$ cards and Eve hold $e$ cards. Then $P_i$ is said to be feasible if
$c_i > 1$, or if $h_i = 1$, $e = 0$, and $h_j > 1$ for all $j \neq i$. We call $\xi = (c_1, \ldots, c_n; e)$ the signature of
the deal. The SFP is as follows [2]:

1. Let $P$ be the feasible player holding the smallest hand. (Ties are broken in favor of the
   lower-numbered player.)

2. $P$ chooses a random card $x$ contained in her hand and a random card not in her hand and
   propose $K = \{x, y\}$ as a key set by asking "Does any player hold a card in $K$ ?

3. If another player $Q$ holds $y$, she accepts $K$ by announcing that she holds a card in $K$. The
   cards $x$ and $y$ are discarded. Whichever $P$ and $Q$ holds fewer cards expose the remaining
   cards in her hand, which are discarded, and drops out of the protocol. The remaining
   players go back to step (1).

4. If none of the players hold $y$, then $K$ is rejected. In this case, $x$ and $y$ are discarded, and
   the players go back to step (1).

The execution of the protocol continues until either there are not enough cards left to complete
steps (1) and (2), or until only one player is left. The first case is the case where the
protocol fails, and the second case is the protocol is successful, i.e., a spanning tree of the players
is constructed, where each edge $(x, y)$ is the result by accepting set $K = \{x, y\}$ in step (3)
as an opaque set for Eve (i.e., it is equally likely for Eve that $P$ holds $x$ and $Q$ holds $y$ or that
$P$ holds $y$ and $Q$ holds $x$. Fischer and Write showed the following theorem [2].

**Theorem 1** [2] Let $\xi = (c_1, \ldots, c_n; e)$ be the signature of the deal. Let $c_i \geq 1$ for $1 \leq i \leq n$,
and $\max\{c_i|1 \leq i \leq n\} + \min\{c_i|1 \leq i \leq n\} \geq n + e$. Then the SFP performs successfully the
construction of a spanning tree with the $n$ nodes where each edge joining two nodes represents
the two nodes sharing a one-bit secret key.

The condition $\max\{c_i|1 \leq i \leq n\} + \min\{c_i|1 \leq i \leq n\} \geq n + e$ provides a sufficient condition
for the SFP to be successful on the signature. However, as shown in [3][6], it is not a necessary
condition. For example, the signature $\xi = (3, 3, 2, 1; 1)$ has $\max\{c_i | 1 \leq i \leq n\} + \min\{c_i | 1 \leq i \leq n\} = 4 < n + \epsilon = 5$, but the SFP succeeds on the signature. A necessary and sufficient condition for the SFP to be successful on a signature was recently given by Mizuki et al. [6]. However, the description of the necessary and sufficient condition is not simple, and the proof for the condition is a lengthy case analysis, where the necessary and sufficient condition is given in each of various cases [6]

3 Protocols for Constructing Key Exchange Spanning Trees

In the case where the number of the hierarchical groups of the players is 1, a secret one-bit key exchange spanning tree with the nodes of the players can be constructed by the SFP. In this section we give a protocol called 2-level protocol for constructing a key exchange spanning tree satisfying the conditions given in Section 1 in the case where the number of the hierarchical groups is 2 (i.e., the case where the $n$ players are divided into two hierarchical groups $G_1$ and $G_2$). The 2-level protocol partly uses a modified SFP. Let $\{P_{1,1}, \ldots, P_{1,k_1}\}$ be the set of the players in $G_1$ and $\{P_{2,1}, \ldots, P_{2,k_2}\}$ be the set of the players in $G_2$. The current size of $P_{i,j}$'s hand is denoted by $c_{i,j}$ for each pair of $i$ and $j$ $(1 \leq i \leq 2, 1 \leq j \leq k_j)$, and the current size of Eve's hand is denoted by $e$. Each player $P_{i,j}$ has a tag $T(i,j)$. For each pair of $i$ and $j$ $(1 \leq i \leq 2, 1 \leq j \leq k_j)$, $T(i,j)$ is initially set to $(i,j)$. A player $P_{i,j}$ is said to be feasible if (1) $c_{i,j} > 1$, or (2) $i = 1, c_{1,j} = 1, e = 0$, for every other player $P_{1,t}$ $(j \neq t)$ in $G_1$, $c_{1,t} \neq 1$, and for every player $P_{2,j}$ in $G_2$, $T(2,t) = (1,1)$, or (3) $i = 2, c_{2,j} = 1, e = 0$, for every player $P_{1,t}$ in $G_1$, $T(1,t) = (1,1)$, and for every other player $P_{2,t}$ $(j \neq t)$ in $G_2$, $c_{2,t} \neq 1$.

We use the lexicographical order of the indices of the players. That is, if $i < i'$, or $i = i'$ and $j' < j$, then $(i,j) < (i',j')$. The signature of the deal of the two hierarchical groups is denoted by $\xi = (c_{1,1}, \ldots, c_{1,k_1}; c_{2,1}, \ldots, c_{2,k_2}; e)$.

2-level protocol:

(1) If there is no player with a non-empty hand in $G_1$, and there is a player in $G_1$ or $G_2$ with its tag value not equal to $(1,1)$, then the protocol stops and fails. If $T(1,i) = (1,1)$ for all $1 \leq i \leq k_1$ then go to step (5). Let $P_{i,j}$ be the feasible player holding the smallest hand in $G_1$. (Ties are broken in favor of the lower ordered player.) If no player in $G_1$ is feasible, then the lowest ordered player holding an non-empty hand, say $P_{i,i}$, is chosen.

(2) For $P_{1,i}$ chosen in (1), $P_{1,i}$ chooses a random card $x$ contained in her hand and a random card $y$ not in her hand and proposes $K = \{x,y\}$ as a key set by asking, "Does any player with its tag value different from $T(1,i)$ hold a card in $K$? (If there are no cards not in $P_{1,i}$, $y$ can be a dummy card.)

(3) If another player in $G_1$, say $P_{1,j}$, with its tag value different from $T(1,i)$ holds $y$, then $P_{1,j}$ accepts $K$ by announcing that she holds a card in $K$. The cards, $x$ and $y$ are discarded, and for every $P_{1,t}$ such that $T(1,t) = T(1,i)$ or $T(1,t) = T(1,j)$, $T(1,t)$ is set to be $T(1,\min\{i,j\})$. A player holding fewer cards exposes the remaining cards in her hand (i.e., hereafter the player holds the empty hand). (Ties are broken by exposing the remaining cards in the hand of the player with the larger index.) If a player in $G_2$, say $P_{2,j}$, holds $y$, then $P_{2,j}$ accepts $K$ by announcing that she holds a card in $K$, then the cards $x$ and $y$ are discarded, and then $T(2,j)$ is set to be $(1,1)$, and then $P_{2,j}$ exposes the remaining cards in her hand (i.e., hereafter $P_{2,j}$ holds the empty hand). All the players go back to step (1) with the updated deal.
(4) If none of the players accept $K = \{x, y\}$, then $x$ and $y$ are discarded, and then all the players go back to step (1) with the updated deal.

(5) If for all $1 \leq i \leq k_2$, $T(2, i) = (1, 1)$, then the protocol successfully stops. If there is a player with its tag value not equal to $(1, 1)$ in $G_2$ holding the empty hand, then the protocol stops and fails. If there are no feasible players in $G_2$ but there is a player in $G_1$ holding a non-empty hand, then let $P_{1,i}$ be such a player and go to step step (9). Let $P_{2,i}$ be the feasible player holding the smallest hand in $G_2$. (Ties are broken in favor of the lower ordered player.)

(6) For $P_{2,i}$ chosen in (5), $P_{2,i}$ chooses a random card $x$ contained in her hand and a random card $y$ not in her hand and proposes $K = \{x, y\}$ as a key set by asking, "Does any player hold a card in $K$?"

(7) If a player in $G_1$ holds $y$, then the player accepts $K$ by announcing that she holds a card in $K$, then the cards $x$ and $y$ are discarded, and then for every player $P_{2,i}$ such that $T(2, t) = T(2, i), T(2, t)$ is set to be $(1, 1)$, and then $P_{2,i}$ expose the remaining cards in her hand (i.e., hereafter $P_{2,i}$ holds the empty hand). If another player, say $P_{2,j}$, in $G_2$ holds $y$, then $P_{2,j}$ accepts that she holds a card in $K$, then the cards $x$ and $y$ are discarded, then for every $P_{2,t}$ such that $T(2, t) = T(2, i)$ or $T(2, t) = T(2, j), T(2, t)$ is set to be $\min\{T(2, i), T(2, j)\}$, and then a player holding a smaller hand among the two players exposes the remaining cards (i.e., hereafter the player holds the empty hand.) (Ties are broken by exposing the remaining cards in the hand of the player with the larger index.) All the players go back to step (5) with the updated deal.

(8) If none of the players accept $K = \{x, y\}$, then $x$ and $y$ are discarded, and then all the players go back to step (5) with the updated deal.

(9) Let $P_{1,i}$ be the player defined in step (5) (i.e., the player in $G_1$ holding a non-empty hand). (Note that in this case every player other than $P_{1,i}$ holds the empty hand.) $P_{1,i}$ chooses a random card $x$ contained in her hand and a random card $y$ not in her hand and propose $K = \{x, y\}$ as a key set by asking, "Does any player hold a card in $K$?"

(10) If another player, say $P_{2,j}$, in $G_2$ holds $y$, then $P_{2,j}$ accepts that she holds a card in $K$, then the cards $x$ and $y$ are discarded, then for every $P_{2,t}$ such that $T(2, t) = T(2, j), T(2, t)$ is set to be $(1, 1)$, and then go back to step (5) with updated deal.

(11) If none of the players accept $K = \{x, y\}$, then $x$ and $y$ are discarded, and then all the players go back to step (5) with the updated deal.

**Example 1** Let $\xi = (4, 5, 6; 7, 8; 5)$ be the signature of a deal. We apply the 2-level protocol to the deal. The initial signature is shown in Figure 1 (a). The size of each hand is indicated by a number beside the corresponding node in Figure 1. Group $G_1$ consists of three players. Their initial tag values are $(1, 1), (1, 2)$ and $(1, 3)$. Group $G_2$ consists of two players. Their initial tag values are $(2, 1)$ and $(2, 2)$. The process of constructing a secret key exchange spanning tree by the 2-level protocol is shown in Figure 1. The construction of a secret key exchange spanning tree proceeds as shown in (a), (b), \ldots, (h) of Figure 1. Players with their tag value $(1, 1)$ are indicated by black circles. At each stage a player with the double circle proposes a key set of cards. A player who announces a card in the key set is indicated by an incoming arrow. At the end of process shown in (c), the tag values of all the players in $G_1$ are $(1, 1)$. The process from step (5) of the 2-level protocol is shown from (d) in Figure 1. At each proposal by the
player indicated by the double circle during the process in (e), Eve has a card in the key set, and eventually the stage shown in (f) reaches. At the stage shown in (f), the second player in $G_1$ has a card in the key set proposed by the player indicated by the double circle in $G_2$. This situation is shown in (g), and eventually we obtain a secret key exchange spanning tree. This spanning tree satisfies the three conditions listed in Section 1.

Figure 1: A process by the 2-level protocol on $\xi = (4, 5, 6; 7, 8; 5)$

**Theorem 2** Let $\xi = (c_{1,1}, \ldots, c_{1,k_1}; c_{2,1}, \ldots, c_{2,k_2}; e)$ be the signature of a deal on hierarchical groups, $G_1$ and $G_2$. If the following two inequalities hold, then the 2-level protocol performs successfully to construct a secret one-bit key exchange spanning tree satisfying the three conditions listed in Section 1.

1. $\max\{c_{1,i}|1 \leq i \leq k_1\} + \min\{c_{1,i}|1 \leq i \leq k_1\} \geq k_1 + k_2 + e$
2. $\min\{c_{2,i}|1 \leq i \leq k_2\} \geq e + k_2$

**Proof.** For the process before step (5) of the 2-level protocol, players in $G_1$ propose sets of cards. For each proposed(173,223),(824,745)
player in $G_2$ should be connected with a player in $G_1$ in a step after leaving step (4). For each loop starting step (5), the number of different tag values of players in $G_2$ is reduced by at least one, or a player in $G_2$ is directly connected with a player in $G_1$, or the size of Eve’s hand is reduced by one. Even if there are no chances such a player in $G_2$ is connected with a player in $G_1$ in step (7), there is such a chance in step (10). Note that step (9) and step (10) are prepared for this purpose. From this observation we can say that if the second condition holds then the all the players’ tag values eventually become $T(1,1)$ and a desired key exchange spanning tree with the set of players on the hierarchical structure is constructed. □

4 Concluding Remarks

The condition given in Theorem 2 is a sufficient condition but the converse does not hold in general. For example, the signature $\xi = (3,3,2,1;1;0)$ does not satisfies (1) in Theorem 2, but the $2$-level protocol works successfully on $\xi = (3,3,2,1;1;0)$ in any case. If we could use the necessary and sufficient condition given in [6] on the sizes of the hands of the players and Eve that the SFP works successfully, we might obtain a necessary and sufficient condition or a sufficient condition stronger than the condition given in Theorem 2. However, the necessary and sufficient condition given in [6] is complicated. We are asked to prepare an elegant necessary and sufficient condition on a signature in the case where the $2$-level protocol works successfully. We are also interested in designing an efficient protocol for constructing good shaped spanning tree satisfying the conditions given in Section 1 on a general hierarchical structures of the players. These problems would be worthy of further investigation.

References


