A complete characterization of a family of key exchange protocols

Takaaki Mizuki1, Hiroki Shizuya2, Takao Nishizeki3

1 Information Synergy Center, Tohoku University, Aoba-yama, Aoba-ku, Sendai 980-8578, Japan; E-mail: mizuki@isc.tohoku.ac.jp, Fax: +81-22/217-6096
2 Information Synergy Center, Tohoku University, Kawauchi, Aoba-ku, Sendai 980-8576, Japan
3 Graduate School of Information Sciences, Tohoku University, Aoba-yama 05, Aoba-ku, Sendai 980-8579, Japan

Published online: 29 January 2002 – © Springer-Verlag 2002

Abstract. Using a random deal of cards to players and a computationally unlimited eavesdropper, all players wish to share a one-bit secret key which is information-theoretically secure from the eavesdropper. This can be done by a protocol to make several pairs of players share one-bit secret keys so that all these pairs form a tree over players. In this paper we obtain a necessary and sufficient condition on the number of cards for the existence of such a protocol.

Keywords: Card game – Information-theoretically secure – Key exchange graph – Key set protocol – Secret key exchange

1 Introduction

Using a random deal of cards, players can share a secret. Winkler [12] gives bidding conventions for the game of bridge whereby one player can send secret information to her partner. Fischer et al. [2] carry this idea further and develop some protocols for secret bit transmission between two players using a random deal of cards. Fischer and Wright give the “key set protocol” [3, 6] and the “transformation protocol” [4] as multiparty protocols. Furthermore, the properties of secret key exchange systems are explored in [5, 13].

The scenario is the same as that of the key set protocol [2, 3, 6]. Suppose that there are players $P_1, P_2, \ldots, P_k$, $k \geq 2$, and a passive eavesdropper, Eve, whose computational power is unlimited. All players wish to share a common one-bit secret key that is information-theoretically secure from Eve. Let $C$ be a set of $d$ distinct cards which are numbered from 1 to $d$. All cards in $C$ are randomly dealt to players $P_1, P_2, \ldots, P_k$ and Eve. We call a set of cards dealt to a player or Eve a hand. Let $C_i \subseteq C$ be $P_i$’s hand for each $1 \leq i \leq k$, and let $C_e \subseteq C$ be Eve’s hand. We denote this deal by $C = (C_1, C_2, \ldots, C_k, C_e)$. Clearly $\{C_1, C_2, \ldots, C_k, C_e\}$ is a partition of set $C$. We write $c_i = |C_i|$ for each $1 \leq i \leq k$ and $c_e = |C_e|$, where $|A|$ denotes the cardinality of a set $A$. Note that $c_1, c_2, \ldots, c_k$ and $c_e$ are the sizes of hands held by $P_1, P_2, \ldots, P_k$ and Eve, respectively, and that $d = \sum_{i=1}^{k} c_i + c_e$. We call $\gamma = (c_1, c_2, \ldots, c_k, c_e)$ the signature of deal $C$. In this paper we assume that $c_1 \geq c_2 \geq \cdots \geq c_k$; if necessary, we rename the players. The set $C$ and the signature $\gamma$ are public to all the players and even to Eve, but the cards in the hand of a player or Eve are private to herself, as is usual in card games.

We consider a graph called a key exchange graph, in which each vertex $i$ represents a player $P_i$ and each edge $(i, j)$ joining vertices $i$ and $j$ represents a pair of players $P_i$ and $P_j$ sharing a one-bit secret key $r_{ij} \in \{0, 1\}$ (Fig. 1). See [8] for the graph-theoretic terminology. If the key exchange graph is a tree as illustrated in Fig. 1e, then all the players can share a common one-bit secret key $r \in \{0, 1\}$ as follows: an arbitrary player chooses a one-bit secret key $r \in \{0, 1\}$ and sends it to the rest of the players along the tree; when player $P_i$ sends $r$ to player $P_j$ along an edge $(i, j)$ of the tree, $P_i$ computes the exclusive-or $r \oplus r_{ij}$ of $r$ and $r_{ij}$ and sends it to $P_j$, and $P_j$ obtains $r$ by computing $(r \oplus r_{ij}) \oplus r_{ij}$.

For the case $k = 2$, Fischer et al. [2] give a protocol using a random deal of cards to connect the two players with an edge, that is, to form a tree on the two players. Fischer and Wright [3, 6] extend this protocol to form a tree for any $k \geq 2$; they formalize a class of protocols called “key set protocols,” a formal definition of which will be given in the following section. Furthermore they give the so-called SFP (smallest feasible player) protocol as a key set protocol. We say that a key set protocol works...
for a signature $\gamma$ if the protocol always forms a tree as the key exchange graph for any deal $C$ having the signature $\gamma$ [2–6]. Let $\Gamma$ be the set of all signatures, where the number $k$ of players and the total number $d$ of dealt cards are taken over all values. Define a partition $\{W, L\}$ of set $\Gamma$ as follows:

$W = \{\gamma \in \Gamma | \text{there is a key set protocol that works for } \gamma\};$

and

$L = \{\gamma \in \Gamma | \text{there is no key set protocol that works for } \gamma\}.$

Fischer and Wright [3, 6] show that their SFP protocol is optimal in the sense that it works for all $\gamma \in W$. Furthermore they prove that a sufficient condition for $\gamma \in W$ is $c_k \geq 1$ and $c_1 + c_k \geq c_e + k$. They also show that it is a necessary and sufficient condition for the case $k = 2$ [3, 6]. However, a simple necessary and sufficient condition for the case $k \geq 3$ is not yet known [3, 6].

In this paper, for the case $k \geq 3$, we give a simple necessary and sufficient condition on a signature $\gamma$ for the existence of a key set protocol that works for $\gamma$. Given a signature $\gamma = (c_1, c_2, \ldots, c_k; c_e)$, one can easily determine in time $O(k)$ whether $\gamma$ satisfies our condition or not. Our condition appears to be similar to the condition that a given degree sequence be “graphical.” The proof for our condition is similarly sophisticated as those for a degree sequence [1, 7, 8, 11].

2 Preliminaries

In this section, we present the key set protocol, and related results, of Fischer and Wright [2, 3, 6].

We first define some terms. A key set $K = \{x, y\}$ consists of two cards $x$ and $y$, one in $C_i$, the other in $C_j$ with $i \neq j$, say $x \in C_i$ and $y \in C_j$. A key set $K = \{x, y\}$ is opaque if $1 \leq i, j \leq k$ and Eve cannot determine whether $x \in C_i$ or $x \in C_j$ with probability greater than 1/2. Note that both players $P_i$ and $P_j$ know that $x \in C_i$ and $y \in C_j$. If $K$ is an opaque key set, then $P_i$ and $P_j$ can share a one-bit secret key $r_{ij} \in \{0, 1\}$, using the following rule agreed on before starting the protocol: $r_{ij} = 0$ if $x > y$; $r_{ij} = 1$, otherwise. Since Eve cannot determine whether $r_{ij} = 0$ or $r_{ij} = 1$ with probability greater than 1/2, the secret key $r_{ij}$ is information-theoretically secure. We say that a card $x$ is discarded if all the players agree that $x$ has been removed from someone’s hand, that is, $x \not\in (\bigcup_{i=1}^{k} C_i) \cup C_e$.

We say that a player $P_s$ drops out of the protocol if she no longer participates in the protocol. We denote by $V$ the set of indices $i$ of all the players $P_i$ remaining in the protocol. Note that $V = \{1, 2, \ldots, k\}$ before starting a protocol.

The key set protocol has four steps as follows.

1. Choose a player $P_s$, $s \in V$, as a proposer by a certain procedure.

2. The proposer $P_s$ determines two cards in her mind, $x$ and $y$. The cards are randomly picked so that $x$ is in her hand and $y$ is not in her hand, i.e., $x \in R C_s$ and $y \in R (\bigcup_{i \in V - \{s\}} C_i) \cup C_e$. Then $P_s$ proposes $K = \{x, y\}$ as a key set to all the players. (The key set is proposed just as a set. Actually it is sorted in some canonical representation of a set. For example, the elements could always be sorted in ascending order, so that Eve learns nothing about which card belongs to $C_s$ unless Eve holds $y$.)

3. If there exists a player $P_t$ holding $y$, then $P_t$ accepts $K$. Since $K$ is an opaque key set, $P_s$ and $P_t$ can share a one-bit secret key $r_{st}$ that is information-theoretically secure from Eve. (In this case an edge $(s, t)$ is added to the key exchange graph.) Both cards $x$ and $y$ are discarded. Let $P_t$ be either $P_s$ or $P_t$ that holds a smaller hand; if $P_s$ and $P_t$ hold cards of the same size, let $P_t$ be the proposer of $P_s$. $P_t$ discards all her cards and drops out of the protocol. Set $V := V - \{i\}$. Return to step 1.

4. If there exists no player holding $y$—that is, Eve holds $y$—then both cards $x$ and $y$ are discarded. Return to step 1. (In this case no new edge is added to the key exchange graph.)

These steps 1–4 are repeated until either exactly one player remains in the protocol or there are not enough cards left to complete step 2 even if two or more players remain. In the first case the key exchange graph becomes a tree and therefore the protocol succeeds. In the second case the protocol fails to form a tree.

We now illustrate a sample execution of the key set protocol. Let $\gamma = (3, 2, 2, 2; 1)$ be the signature before starting the protocol. Thus there are four players $P_1, P_2, P_3, P_4$, and Eve; $P_1$ has a hand of size 3, players $P_2, P_3$, and $P_4$ have hands of size 2, and Eve has a hand of size 1. At the beginning of the protocol the key exchange graph