Characterization of Optimal Key Set Protocols
(Extended Abstract)

Takaaki Mizuki[1], Hiroki Shizuya[2], and Takao Nishizeki[1]

[1] Graduate School of Information Sciences, Tohoku University,
Aoba-yama 05, Aoba-ku, Sendai 980-8579, Japan
{mizuki,nishi}@ecei.tohoku.ac.jp
[2] Education Center for Information Processing, Tohoku University,
Kawauchi, Aoba-ku, Sendai 980-8576, Japan
shizuya@ecip.tohoku.ac.jp

Abstract. Using a random deal of cards to players and a computationally unlimited eavesdropper, all players wish to share a common one-bit secret key which is information-theoretically secure from the eavesdropper. This can be done by the so-called key set protocol. In this paper we give a necessary and sufficient condition for a key set protocol to be "optimal," that is, to succeed always in sharing a one-bit secret key.

1 Introduction

Suppose that there are k (≥ 2) players $P_1, P_2, \cdots, P_k$ 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 $P_1, P_2, \cdots, P_k$ 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, and let $C_e \subseteq C$ be Eve's hand. We denote this *deal* by $\mathcal{C} = (C_1, C_2, \cdots, C_k; C_e)$. Clearly $\{C_1, C_2, \cdots, C_k, C_e\}$ 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 $c_1, c_2, \cdots, c_k$ and c_e are the sizes of hands held by $P_1, P_2, \cdots, P_k$ and Eve respectively, and that $d = \sum_{i=1}^{k} c_i + c_e$. We call $\gamma = (c_1, c_2, \cdots, c_k; c_e)$ the *signature* of deal $\mathcal{C}$. 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 γ 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 in the case of usual card games. This paper addresses protocols which make all the players share a common one-bit secret key information-theoretically securely using such a random deal of cards [2,3,4,5,6,10]. A reasonable situation in which such protocols are practically required is discussed in [4,6], and also the reason why we deal cards even to Eve is found there.

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 $r_{ij} \in \{0, 1\}$. Refer to

J. van Leeuwen et al. (Eds.): IFIP TCS 2000, LNCS 1872, pp. 273–285, 2000.

[8] for the graph-theoretic terminology. A connected graph having no cycle is called a tree. If the key exchange graph is a tree, 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 $k = 2$, Fischer, Paterson and Rackoff give a protocol to form a tree, i.e. a graph having exactly one edge, as the key exchange graph by using a random deal of cards [2]. Fischer and Wright extend this protocol for any $k \geq 2$, and formalize a class of protocols called "key set protocols," a formal definition of which will be given in the succeeding section [3, 6]. We say that a "key set protocol" *works for a signature* γ if the protocol always forms a tree as the key exchange graph for any deal $\mathcal{C}$ having the signature γ.

Let $\mathit{\Gamma}_k$ be the set of all signatures of deals for k players, where the total number d of dealt cards is not fixed but takes any value. Furthermore, let $\mathit{\Gamma}$ be the set of all signatures where the number k of players is taken over all values, that is,

$$\mathit{\Gamma} = \bigcup_{k=2}^{\infty} \mathit{\Gamma}_k.$$

Define sets W and L as follows:

$$W = \{\gamma \in \mathit{\Gamma} \mid \text{there is a key set protocol working for } \gamma\}; \text{ and}$$

$$L = \{\gamma \in \mathit{\Gamma} \mid \text{there is no key set protocol working for } \gamma\}.$$

Thus $\{W, L\}$ is a partition of set $\mathit{\Gamma}$. For $k = 2$, i.e. $\gamma \in \mathit{\Gamma}_2$, Fischer and Wright give a simple necessary and sufficient condition for $\gamma \in W$ [3]. For $k \geq 3$, the authors give a simple necessary and sufficient condition for $\gamma \in W$ [10]. (These necessary and sufficient conditions will be described in Section 2.5.)

One wishes to design a key set protocol which works for all signatures $\gamma \in W$, that is, always forms a tree as the key exchange graph for all deals $\mathcal{C}$ having any signature $\gamma \in W$. Such a protocol is said to be *optimal* for the class of key set protocols [3,6]. There exists an optimal key set protocol indeed: the "SFP protocol" given by Fischer and Wright is an example of an optimal key set protocol [3,6]. However, neither an optimal key set protocol other than the SFP protocol nor a characterization of optimal key set protocols has been known so far.

In this paper, using the condition for $\gamma \in W$ in [10], we give a complete characterization of optimal key set protocols, that is, we give a necessary and sufficient condition for a key set protocol to be optimal. Using the characterization, we can design many optimal key set protocols. Thus we show that not only the SFP protocol but also many others are optimal. Using these optimal protocols, one can produce trees of various shapes as a key exchange graph; some of them would be appropriate for efficient broadcast of a secret message. For example, one can produce a tree of a small radius, as we will show later in Section 4.

2 Preliminaries

In this section we explain the "key set protocol" formalized by Fischer and Wright, and present some of the known results on this protocol [2,3,6,10].

2.1 Key Set Protocol

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 $y \in C_j$. We say that 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 a 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, $x \notin (\bigcup_{i=1}^{k} C_i) \cup C_e$. We say that a player P_i *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 $V = \{1, 2, \cdots, k\}$ 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 in mind two cards x, y. The cards are randomly picked so that x is in her hand and y is not in her hand, i.e. $x \in C_s$ and $y \in (\bigcup_{i \in V - \{s\}} C_i) \cup C_e$. 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 order, for example in ascending order, so 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_i be either P_s or P_t that holds the smaller hand; if P_s and P_t hold hands of the same size, let P_i be the proposer P_s. P_i 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.

In the second case the key exchange graph does not become a connected graph and hence does not become a tree.

Considering various procedures for choosing the proposer P_s in step 1, we obtain the class of *key set protocols*, where all the procedures are functions $\Gamma_k \rightarrow V$.

2.2 Malicious Adversary

If a key set protocol works for a signature γ, then the key exchange graph must become a tree for any deal $\mathcal{C}$ having the signature γ. Hence, whoever has the card y contained in the proposed key set $K = \{x, y\}$, the key exchange graph should become a tree. The *malicious adversary* determines who holds the card y. We use a function $\mathcal{A} : \Gamma_k \times V \rightarrow V \cup \{e\}$ to represent a malicious adversary, where e is Eve's index. The inputs to the function $\mathcal{A}(\gamma, s)$ are the current signature $\gamma \in \Gamma_k$ and the index $s \in V$ of a proposer P_s chosen by the protocol. Its output is either the index t of a player P_t remaining in the protocol or the index e of Eve; $\mathcal{A}(\gamma, s) = t \neq e$ means that player P_t holds card y; and $\mathcal{A}(\gamma, s) = e$ means that Eve holds card y.

From now on, we denote by $\gamma = (c_1, c_2, \cdots, c_k; c_e)$ the current signature, and denote by $\gamma'_{(s,\mathcal{A})} = (c'_1, c'_2, \cdots, c'_{k'}; c'_e)$ the resulting signature after executing steps 1–4 under the assumption that P_s proposes a key set $K = \{x, y\}$ and $y \in C_{\mathcal{A}(\gamma,s)}$. We sometimes write γ' instead of $\gamma'_{(s,\mathcal{A})}$ if it is clear from context.

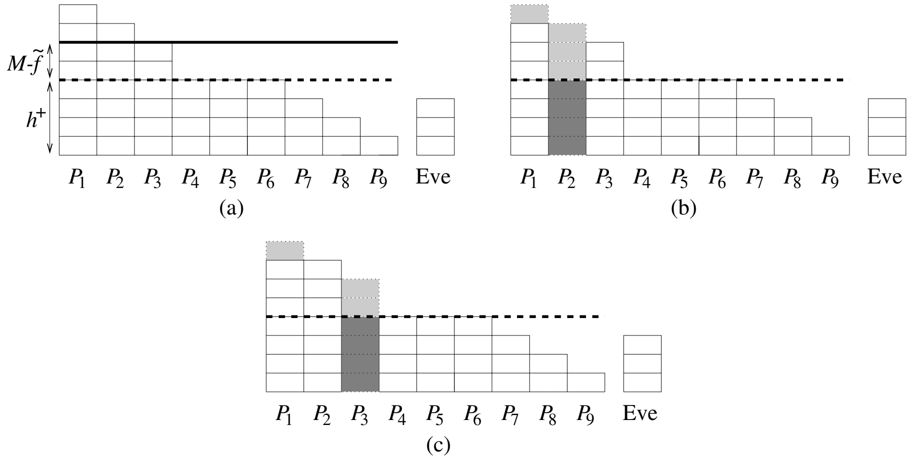
Consider a signature $\gamma = (8, 7, 6, 4, 4, 4, 3, 2, 1; 3)$ as an example. Then, as illustrated in Fig. 1(a), the size of the hand of each player or Eve can be represented by white rectangles. For example, if the malicious adversary $\mathcal{A}$ satisfies $\mathcal{A}(\gamma, 2) = \mathcal{A}(\gamma, 3) = 1$, then $\gamma'_{(2,\mathcal{A})} = (7, 6, 4, 4, 4, 3, 2, 1; 3)$ as in Fig. 1(b), and $\gamma'_{(3,\mathcal{A})} = (7, 7, 4, 4, 4, 3, 2, 1; 3)$ as in Fig. 1(c). In Figs. 1(b) and (c), the shaded rectangles correspond to the discarded cards.

If an optimal key set protocol chooses a proposer P_s for $\gamma \in W$, then $\gamma'_{(s,\mathcal{A})} \in W$ for any malicious adversary $\mathcal{A}$; for convenience sake any signature $\gamma = (c_1; c_e)$ with $k = 1$ is assumed to be in W.

It follows from the definition of a key set protocol that if two players P_i and P_j hold hands of the same size, that is, $c_i = c_j$, then

$$\forall \mathcal{A} \ \ \gamma'_{(i,\mathcal{A})} \in W \Longleftrightarrow \forall \mathcal{A} \ \ \gamma'_{(j,\mathcal{A})} \in W.$$

Hence, if there exist two or more players P_i with $c_i = c_s$ (including the proposer P_s), then one may assume without loss of generality that P_s has the largest index among all these players. We call it *Assumption 1 for convenience sake.* Similarly, if $\mathcal{A}(\gamma, s) = t \neq e$ and there exist two or more players P_i with $c_i = c_t$ and $i \neq s$ (including P_t), then one may assume without loss of generality that P_t has the largest index among all these players. We call it *Assumption 2 for convenience sake.* Under the two assumptions above, $\gamma'_{(s,\mathcal{A})} = (c'_1, c'_2, \cdots, c'_{k'}; c'_e)$ satisfies $c'_1 \geq c'_2 \geq \cdots \geq c'_{k'}$ since γ satisfies $c_1 \geq c_2 \geq \cdots \geq c_k$.


M-$\tilde{f}$
h^+
P_1 P_2 P_3 P_4 P_5 P_6 P_7 P_8 P_9 Eve
P_1 P_2 P_3 P_4 P_5 P_6 P_7 P_8 P_9 Eve
P_1 P_2 P_3 P_4 P_5 P_6 P_7 P_8 P_9 Eve

(a)

(b)

(c)

Fig. 1. The alteration of a signature.

2.3 Feasible Players

Fischer and Wright define a "feasible" player for a proposer as follows [3,6]. Let $k \geq 3$. If $c_e \geq 1$, P_i with $c_i = 1$ were chosen as a proposer, and $\mathcal{A}(\gamma, i) = e$, then P_i's hand would become empty although she remains in the protocol, and hence the key exchange graph would not become a tree. On the other hand, if $c_e = 0$, then $\mathcal{A}(\gamma, i) \neq e$ and hence the protocol appears to be able to choose P_i with $c_i = 1$ as a proposer; however, if $\mathcal{A}(\gamma, i) = j$ and $c_j = 1$, then P_j's hand would become empty and hence the key exchange graph would not become a tree. Thus the protocol can choose P_i with $c_i = 1$ as a proposer only if $c_e = 0$ and $c_j \geq 2$ for every j such that $1 \leq j \leq k$ and $j \neq i$, that is, only if $c_e = 0$, $i = k$ and $c_{k-1} \geq 2$. Remember that $c_1 \geq c_2 \geq \cdots \geq c_k$ is assumed. Hence, we say that a player P_i is *feasible* if the following condition (1) or (2) holds.

(1) $c_i \geq 2$.
(2) $c_e = 0$, $c_i = 1$ with $i = k$, and $c_{k-1} \geq 2$.

Thus, if the hands of all the players remaining in a protocol are not empty, i.e. $c_k \geq 1$, and the proposer P_s is feasible, then the hands of all the players remaining in the protocol will not be empty at the beginning of the succeeding execution of steps 1–4, i.e. $c'_{k'} \geq 1$. Note that there will not always exist a feasible player at the beginning of the succeeding execution of steps 1–4 even if the proposer P_s is feasible.

We define a mapping f from Γ_k to $\{0, 1, 2, \cdots, k\}$, as follows: $f(\gamma) = i$ if P_i is the feasible player with the smallest hand (ties are broken by selecting the player having the largest index); and $f(\gamma) = 0$ if there is no feasible player. For example, if $\gamma = (4, 3, 2, 2, 1, 1; 3)$, then $f(\gamma) = 4$. If $\gamma = (4, 4, 3, 3, 1; 0)$, then $f(\gamma) = k = 5$ because $c_e = 0$, $c_k = 1$ and $c_{k-1} \geq 2$. If $\gamma = (1, 1, 1; 2)$, then

$f(\gamma) = 0$ because there is no feasible player. Hereafter we often denote $f(\gamma)$ simply by f and $f(\gamma')$ by f'.

The following Lemma 1 immediately holds [3,10].

Lemma 1 ([3,10]) *The following* (a)–(d) *hold.*

(a) *If* $\gamma \in W$, *then* $c_k \geq 1$ [3].
(b) *If* $k \geq 3$ *and* $\gamma \in W$, *then* $f \geq 1$ [3].
(c) *If* $c_k \geq 1$, *then* $c_i = 1$ *for every* i *such that* $f + 1 \leq i \leq k$ [10].
(d) *If* $f \geq 1$ *and* $c_f = 1$, *then* $f = k$, $c_k = 1$, $c_{k-1} \geq 2$, $c_e = 0$, *and* $\gamma \in W$ [3].

2.4 SFP Protocol

Fischer and Wright give the *SFP (smallest feasible player) protocol* as a key set protocol [3,6]. The SFP protocol always chooses the feasible player with the smallest hand as a proposer, that is, chooses the proposer P_s as follows:

$$s = \begin{cases} f(\gamma) \ if \ 1 \leq f(\gamma) \leq k; \\ 1 \qquad if \ f(\gamma) = 0. \end{cases}$$

Fischer and Wright show that the SFP protocol is optimal [3,6].

Theorem 2 ([3,6]) *The SFP protocol is optimal.*

Not only the SFP protocol but also many other key set protocols are optimal. This paper provides a complete characterization of optimal key set protocols.

2.5 Necessary and Sufficient Condition for $\gamma \in W$

For $k = 2$, the following Theorem 3 provides a necessary and sufficient condition for $\gamma \in W$ [3].

Theorem 3 ([3]) *Let* $k = 2$. *Then* $\gamma \in W$ *if and only if* $c_2 \geq 1$ *and* $c_1 + c_2 \geq c_e + 2$.

For $k = 3$, the following Theorem 4 provides a necessary and sufficient condition for $\gamma \in W$ [10].

Theorem 4 ([10]) *Let* $k = 3$. *Then* $\gamma \in W$ *if and only if* $c_3 \geq 1$ *and* $c_1 + c_3 \geq c_e + 3$.

For $k \geq 4$, the following Theorem 5 provides a necessary and sufficient condition for $\gamma \in W$ [10]. Hereafter let $B = \{i \in V \mid c_i = 2\}$, and let $b = \lfloor |B|/2 \rfloor$.

Theorem 5 ([10]) *Let* $k \geq 4$, $c_k \geq 1$ *and* $f \geq 1$. *Then* $\gamma \in W$ *if and only if*

$$\sum_{i=1}^{k} \max\{c_i - h^+, 0\} \geq \widetilde{f}, \tag{1}$$

where

$$\bar{f} = f - \delta, \tag{2}$$

$$\widetilde{f} = \bar{f} - 2\epsilon, \tag{3}$$

$$h = c_e - c_k + k - \bar{f}, \tag{4}$$

$$h^+ = h + \epsilon, \tag{5}$$

$$\delta = \begin{cases} 0 \; if \;\; f = 1; \\ 1 \; if \;\; 2 \le f \le k-1; \\ 2 \; if \;\; f = k \;\; and \;\; c_{k-1} \ge c_k + 1; \;\; and \\ 3 \; if \;\; f = k \;\; and \;\; c_{k-1} = c_k, \end{cases} \tag{6}$$

and

$$\epsilon = \begin{cases} \max\{\min\{c_2 - h, b\}, 0\} & if \;\; 5 \le f \le k-1; \\ \max\{\min\{c_2 - h, b-1\}, 0\} & if \;\; 5 \le f = k \;\; and \;\; c_e \ge 1; \;\; and \\ 0 & otherwise. \end{cases} \tag{7}$$

For example, one can observe a signature $\gamma = (8, 7, 6, 4, 4, 4, 3, 2, 1; 3)$ (see Fig. 1(a)) satisfies Eq. (1) in Theorem 5 as follows. The signature γ satisfies $k = 9$ and $f = 8$. Thus by Eq. (6) $\delta = 1$. Since $B = \{8\}$, $b = 0$ and hence by Eq. (7) $\epsilon = 0$. Thus, by Eqs. (2) and (3) $\widetilde{f} = \bar{f} = 8 - 1 = 7$, and by Eqs. (4) and (5) $h^+ = h = 3 - 1 + 9 - 7 = 4$. Therefore,

$$\sum_{i=1}^{k} \max\{c_i - h^+, 0\} = 4 + 3 + 2 = 9 > 7 = \widetilde{f},$$

and hence the signature γ satisfies Eq. (1). (Note that $\sum_{i=1}^{k} \max\{c_i - h^+, 0\}$ is equal to the number of rectangles above the dotted line in Fig. 1(a).) Thus $\gamma \in W$.

Eq. (1) looks in appearance to be similar to the condition for a given degree sequence to be "graphical" [1,7,8,11].

Since $c_1 \ge c_2 \ge \cdots \ge c_k$ is assumed, Eq. (1) is equivalent to

$$\sum_{i=1}^{\widetilde{f}} \max\{c_i - h^+, 0\} \ge \widetilde{f} \tag{8}$$

where the summation is taken over all i, $1 \le i \le \widetilde{f}$, although the summation in Eq. (1) is taken over all i, $1 \le i \le k$ [10].

We define $\delta', \epsilon', b', \bar{f}', \widetilde{f}', h', {h^+}'$ and B' for γ' as we did for γ.

3 Main Results

In this section we give a complete characterization of optimal key set protocols. We first define some terms in Section 3.1, and then give the characterization in Section 3.2.

3.1 Definition of Selectable Players

In this subsection we define a "selectable" player that can be chosen as a proposer by an optimal key set protocol. We will give a complete characterization of "selectable" players in the succeeding subsection. The characterization immediately provides a complete characterization of optimal key set protocols.

The SFP protocol, which always chooses the feasible player P_f with the smallest hand, is optimal. However, a key set protocol which chooses an arbitrary feasible player is not necessarily optimal. We define a "selectable" player as follows.

Definition 6 *We say that a player P_i is* selectable *for γ if $\gamma'_{(i,\mathcal{A})} \in W$ for any malicious adversary $\mathcal{A}$.*

When $\gamma \in W$, the proposer chosen by an optimal key set protocol is a selectable player, of course. Since the SFP protocol is optimal, P_f is a selectable player if $\gamma \in W$.

Definition 6 implies that $\gamma \in W$ if and only if there exists at least one selectable player. In other words, $\gamma \in L$ if and only if there exists no selectable player.

Furthermore, a key set protocol is optimal if and only if the protocol always chooses a selectable player as a proposer whenever such a player exists. Thus, in the remainder of the paper, we characterize the set of all selectable players.

3.2 Characterization of Selectable Players

In this subsection we give a necessary and sufficient condition for a player to be selectable.

If $\gamma \in L$, then there is no selectable player. Therefore it suffices to obtain a necessary and sufficient condition for a player to be selectable only if $\gamma \in W$.

We first characterize the selectable players for $k = 2$ as in the following Theorem 7.

Theorem 7 *Let $k = 2$ and $\gamma \in W$. Then a player P_i is selectable if and only if $c_i \geq 2$ or $c_e = 0$.*

Proof. Let $k = 2$ and $\gamma \in W$. By Lemma 1(a) $c_2 \geq 1$.

We first prove the necessity. Suppose for a contradiction that $c_i = 1$ and $c_e \geq 1$ although P_i is selectable. Then one may assume that $i = 2$ by Assumption 1 for convenience sake when P_i is chosen as a proposer. Since $\gamma'_{(2,\mathcal{A})} = (c_1, 0; c_e - 1)$ for an adversary $\mathcal{A}$ such that $\mathcal{A}(\gamma, 2) = e$, we have $\gamma'_{(2,\mathcal{A})} \in L$ by Lemma 1(a). Thus P_2, i.e. P_i, is not selectable, a contradiction.

We next prove the sufficiency. Assume that $c_i \geq 2$ or $c_e = 0$. Then it suffices to show that $\gamma'_{(i,\mathcal{A})} \in W$ for any adversary $\mathcal{A}$. There are the following two cases to consider.

Case 1: $\mathcal{A}(\gamma, i) \neq e$.

In this case γ' satisfies $k' = 1$ and hence $\gamma' \in W$.

Case 2: $\mathcal{A}(\gamma, i) = e$.

In this case $c_e \geq 1$, and hence $c_i \geq 2$ because we assumed that $c_i \geq 2$ or $c_e = 0$. If $i = 1$ and $c_1 \geq c_2 + 1$, then $\gamma' = (c_1 - 1, c_2; c_e - 1)$; otherwise, $\gamma' = (c_1, c_2 - 1; c_e - 1)$. Thus, in either case, $c'_1 + c'_2 = (c_1 + c_2) - 1$ and $c'_e = c_e - 1$. On the other hand, since $\gamma \in W$, by Theorem 3 $c_1 + c_2 \geq c_e + 2$. Therefore $c'_1 + c'_2 \geq (c_e + 2) - 1 = c_e + 1 = c'_e + 2$. Furthermore, since $c_i \geq 2$, $c'_2 \geq 1$. Thus, by Theorem 3 $\gamma' \in W$. ▮

We next characterize the selectable players for $k = 3$. It has been known that, if $c_k \geq 1$ and $c_1 + c_k \geq c_e + k$, then any key set protocol choosing an arbitrary feasible player as a proposer works for γ [3,6]; thus the following Lemma 8 immediately holds.

Lemma 8 *Let $c_k \geq 1$ and $c_1 + c_k \geq c_e + k$. Then every player P_i such that $1 \leq i \leq f$ is selectable.*

Furthermore, it is obvious that any non-feasible player is not selectable when $k \geq 3$; thus we have the following Lemma 9.

Lemma 9 *Let $k \geq 3$. If a player P_i is selectable, then $1 \leq i \leq f$.*

By using Theorem 4, Lemmas 8 and 9, one can easily prove that the selectable players for $k = 3$ are characterized as in the following Theorem 10.

Theorem 10 *Let $k = 3$ and $\gamma \in W$. Then a player P_i is selectable if and only if $1 \leq i \leq f$.*

Proof. Let $k = 3$ and $\gamma \in W$. Then by Theorem 4 $c_3 \geq 1$ and $c_1 + c_3 \geq c_e + 3$. Thus Lemma 8 implies the sufficiency. Furthermore Lemma 9 implies the necessity. ▮

We finally characterize the selectable players for $k \geq 4$. Before giving the characterization, we first give some definitions.

In a key set protocol, for every $i, j \in V$ such that $i \neq j$ and $c_i = c_j$,

$$P_i \text{ is selectable} \Longleftrightarrow P_j \text{ is selectable}.$$

Thus, if there exist two or more players holding hands of the same size, then it suffices to determine whether an arbitrary player among such players is selectable or not. For example, if $\gamma = (8, 7, 6, 4, 4, 4, 3, 2, 1; 3)$, then one can choose P_6 as a "representative" player among the three players P_4,P_5 and P_6 who have hands of size 4. As in this example, we choose the player with the largest index among all the players holding hands of the same size as a "representative" player, and determine whether the chosen "representative" player is selectable or not. Let V_r be the set of indices of all the "representative" players. That is,

$$V_r = \{i \in V \mid i = \max X \text{ } and \text{ } X \in V/R\},$$

where V/R is the quotient set of V under the equivalence relation $R = \{(i,j) \in V \times V \mid c_i = c_j\}$. For example, $V_r = \{1,2,3,6,7,8,9\}$ for the above signature γ. It suffices to give a necessary and sufficient condition for a player P_i, $i \in V_r$, to be selectable. Of course, such a necessary and sufficient condition immediately yields a complete characterization of all selectable players (whose indices are not necessarily in V_r).

Let P_{f_m} be the player who holds the hand of the same size as P_f and has the smallest index, that is,

$$f_m = \min\{i \in V \mid c_i = c_f\}.$$

From now on we define

$$M = \sum_{j=1}^{k} \max\{c_j - h^+, 0\}.$$

Note that M is the same as the left side of Eq. (1) in Theorem 5. We define M' for γ' as we did for γ.

Define $\bar{\epsilon}$ by the following Eq. (9), which is obtained by replacing c_2 with c_3 in Eq. (7):

$$\bar{\epsilon} = \begin{cases} \max\{\min\{c_3 - h, b\}, 0\} & \textit{if } 5 \le f \le k-1; \\ \max\{\min\{c_3 - h, b-1\}, 0\} & \textit{if } 5 \le f = k \textit{ and } c_e \ge 1; \textit{ and} \\ 0 & \textit{otherwise.} \end{cases} \tag{9}$$

Since $c_3 \le c_2$, Eqs. (7) and (9) imply

$$0 \le \bar{\epsilon} \le \epsilon. \tag{10}$$

Furthermore, define *Conditions 1* and *2* as follows.

(Condition 1)

$5 \le f = k$ and $c_{k-2} = c_{k-1} = c_k + 1$.

(Condition 2)

$c_{f_m-2} = c_{f_m-1} = 3$, $|B|$ is an odd number, and the following (i) or (ii) holds.

(i) $6 \le f \le k-1$ and $c_2 - h \ge b+1$.
(ii) $6 \le f = k$, $c_e \ge 1$, $b \ge 1$ and $c_2 - h \ge b$.

Define λ as follows:

$$\lambda = \begin{cases} 2 \textit{ if Condition } 1 \textit{ holds}; \\ 3 \textit{ if Condition } 2 \textit{ holds}; \textit{ and} \\ 0 \textit{ otherwise.} \end{cases} \tag{11}$$

Finally, define $\widetilde{\epsilon}$ as follows:

$$\widetilde{\epsilon} = \begin{cases} \max\{\min\{c_2 - h - 1, b-1\}, 0\} & \textit{if } f \ge 8,\ c_k = 1 \textit{ and } \lambda = 2; \textit{ and} \\ 0 & \textit{otherwise.} \end{cases} \tag{12}$$

We are now ready to give a complete characterization of the selectable players for $k \ge 4$ as in the following Theorem 11.

Theorem 11 *Let $k \geq 4$ and $\gamma \in W$. Then a player P_i such that $i \in V_r$ is selectable if and only if $1 \leq i \leq f$ and*

$$\begin{cases} c_2 - h^+ \leq M - \widetilde{f} - (\epsilon - \bar{\epsilon}) & \textit{if } i \leq 2; \\ \sum_{j=1}^{\widetilde{f}-\lambda-2\widetilde{\epsilon}} \max\{c_j - (h^+ + \widetilde{\epsilon} + 1), 0\} \geq \widetilde{f} - \lambda - 2\widetilde{\epsilon} & \\ & \textit{if } i = f_m - 1 \geq 4 \textit{ and } \lambda \neq 0; \textit{ and} \\ c_i - h^+ \leq M - \widetilde{f} & \textit{otherwise.} \end{cases} \tag{13}$$

If (i) $i \leq 2$ and $\epsilon - \bar{\epsilon} = 0$, (ii) $i = 3$, or (iii) $i \geq 4$ and $i \neq f_m - 1$ or $\lambda = 0$, then Eq. (13) in Theorem 11 becomes

$$\begin{cases} c_2 - h^+ \leq M - \widetilde{f} \textit{ if } i \leq 2; \textit{ and} \\ c_i - h^+ \leq M - \widetilde{f} \textit{ if } i \geq 3. \end{cases} \tag{14}$$

Note that the most of signatures satisfy $\epsilon - \bar{\epsilon} = \lambda = 0$ and that very few signatures satisfy $\epsilon - \bar{\epsilon} \geq 1$ or $\lambda \neq 0$.

Consider the signature $\gamma = (8, 7, 6, 4, 4, 4, 3, 2, 1; 3)$ as an example again (see Fig. 1(a)). The signature γ satisfies $\epsilon = 0$ as mentioned in Section 2.5, and hence by Eq. (10) $\epsilon - \bar{\epsilon} = 0$. The signature γ does not satisfy Condition 1. Furthermore, since $f = f_m = 8$, we have $c_{f_m - 2} = 4 \neq 3$ and hence Condition 2 does not hold. Therefore, by Eq. (11) $\lambda = 0$. In addition, since the signature γ satisfies $f = 8$, $M = 9$, $\widetilde{f} = 7$ and $h^+ = 4$ as mentioned in Section 2.5, we have $M - \widetilde{f} = 2$. Therefore, Eq. (13) in Theorem 11, i.e. Eq. (14), implies that all the selectable players are the six players P_3,P_4,P_5,P_6,P_7 and P_8. These six players are the feasible players holding the hands whose sizes do not exceed the solid line in Fig. 1(a).

We now intuitively explain the correctness of Theorem 11. For simplicity, let $\epsilon - \bar{\epsilon} = \lambda = 0$, and consider a player P_i such that $i \geq 2$. Theorem 5 implies that a necessary and sufficient condition for $\gamma \in W$ is that $M \geq \widetilde{f}$, i.e. there are $\widetilde{f}$ or more rectangles above the dotted line in Fig. 1(a). Thus, a signature $\gamma \in W$ has $M - \widetilde{f}$ "spare" rectangles. That is, even if one removes at most $M - \widetilde{f}$ rectangles above the dotted line, γ still remains in W, but if one removed $(M - \widetilde{f}) + 1$ or more rectangles above the dotted line, then γ would be in L. Further, in order for a player P_i to be selectable, there must exist at least $\widetilde{f'}$ rectangles above the dotted line in the figure of $\gamma'_{(i,\mathcal{A})}$ (e.g. Fig. 1(b) or (c)) for any malicious adversary $\mathcal{A}$. For some adversary $\mathcal{A}$, the number of the rectangles above the dotted line decreases by $1 + (c_i - h^+)$ when the proposer is P_i, as one can immediately observe from Fig. 1(b) or (c). Note that these $1 + (c_i - h^+)$ rectangles are lightly shaded in Figs. 1(b) and (c). Furthermore, since the number of the feasible players decreases by exactly one, we have $\widetilde{f'} = \widetilde{f} - 1$. Hence, if $c_i - h^+$ were greater than the number $M - \widetilde{f}$ of the "spare" rectangles, then $M' = M - \{1 + (c_i - h^+)\} < \widetilde{f} - 1 = \widetilde{f'}$ and hence γ' would be in L. Therefore, a player P_i such that $c_i - h^+ > M - \widetilde{f}$ is not selectable. On the other hand, if $c_i - h^+ \leq M - \widetilde{f}$, then γ' will still remain in W, and hence a player P_i such that $c_i - h^+ \leq M - \widetilde{f}$ is selectable. This is the intuitive reason why Theorem 11 holds.

Due to the page limitation, we cannot include a proof of Theorem 11 in this extended abstract; see [9].

4 Conclusion

A key set protocol is determined by giving a procedure for choosing a proposer. In this paper, we defined a player to be selectable if the player can be chosen as a proposer by an optimal key set protocol, and gave a complete characterization of such selectable players in Theorem 11. Thus we succeeded in characterizing the set of *all* optimal key set protocols.

Using Theorem 11, one can efficiently find all selectable players in time $O(k)$. Let P_j be the selectable player having the smallest index j. Then one may intuitively expect that all players P_i such that $j \le i \le f$ are selectable. However, it is surprisingly not the case. Theorem 11 implies that all the players such that $j \le i \le f$ and $c_i \ne c_{f_m-1}$ are selectable but P_{f_m-1} may or may not be selectable. Consider a signature $\gamma = (5,5,5,4,4,3,3,2,1;2)$ as an example. Then γ satisfies $f = 8$, $f_m - 1 = 7$, $\lambda = 3$, $h^+ = 3$, $M = 8$, $\epsilon = \bar{\epsilon} = \widetilde{\epsilon} = 0$ and $\widetilde{f} = 7$. Thus Eq. (13) in Theorem 11 becomes

$$\begin{cases} c_2 - 3 \le 1 & \mathit{if}\ i \le 2; \\ \sum_{\ell=1}^{4} \max\{c_\ell - 4, 0\} \ge 4 & \mathit{if}\ i = 7;\ \mathit{and} \\ c_i - 3 \le 1 & \mathit{otherwise}. \end{cases}$$

Therefore, P_7 is not selectable, and all the selectable players are the three players P_4,P_5 and P_8. As in this example, the indices of selectable players are not necessarily consecutive numbers.

Using the characterization of selectable players, one can design many optimal key set protocols. Assume that $c_1 = c_2 = \cdots = c_k$ and $\gamma \in W$. Then in most cases the SFP protocol forms a spanning path of length k, i.e. a tree of radius $\lfloor k/2 \rfloor$, as the key exchange graph. On the other hand, using various optimal key set protocols, one can produce trees of various shapes as a key exchange graph, some of which would be appropriate for efficient broadcast of a secret message. For example, consider an optimal key set protocol which always chooses, as a proposer, the selectable player holding the largest hand; such a protocol forms a tree of a smaller radius than $\lfloor k/2 \rfloor$. Furthermore, we can choose the selectable player having the largest degree as a proposer and modify step 3 of the key set protocol in a way that either P_s or P_t who has the smaller degree drops out of the protocol whenever the resulting signature remains in W; such a protocol forms a tree of much smaller radius, especially when $c_1 = c_2 = \cdots = c_k$ is large. We have verified these facts by extensive computer simulation.

This paper addresses only the key set protocol, which establishes a one-bit secret key. On the other hand, the "transformation protocol" given by Fischer and Wright [4] establishes an n-bit secret key. For a signature $\gamma = (3,2;4) \in L$, any key set protocol does not work for γ, but the transformation protocol always establishes a one-bit secret key for γ. However, for a signature $\gamma = (4,4,4,4;4) \in$

W, any optimal key set protocol works for γ, but the transformation protocol cannot establish a one-bit secret key for γ. Thus a protocol entirely superior to the key set protocol has not been known.

References

1. T. Asano, "An $O(n \log \log n)$ time algorithm for constructing a graph of maximum connectivity with prescribed degrees," J. Comput. and Syst. Sci., vol. 51, pp. 503–510, 1995.
2. M. J. Fischer, M. S. Paterson, and C. Rackoff, "Secret bit transmission using a random deal of cards," DIMACS Series in Discrete Mathematics and Theoretical Computer Science, AMS, vol. 2, pp. 173–181, 1991.
3. M. J. Fischer and R. N. Wright, "An application of game-theoretic techniques to cryptography," DIMACS Series in Discrete Mathematics and Theoretical Computer Science, AMS, vol. 13, pp. 99–118, 1993.
4. M. J. Fischer and R. N. Wright, "An efficient protocol for unconditionally secure secret key exchange," Proc. of the 4th Annual Symposium on Discrete Algorithms, pp. 475–483, 1993.
5. M. J. Fischer and R. N. Wright, "Bounds on secret key exchange using a random deal of cards," J. Cryptology, vol. 9, pp. 71–99, 1996.
6. M. J. Fischer and R. N. Wright, "Multiparty secret key exchange using a random deal of cards," Proc. Crypto '91, Lecture Notes in Computer Science, Springer-Verlag, vol. 576, pp. 141–155, 1992.
7. S. L. Hakimi, "On realizability of a set of integers as degrees of the vertices of a linear graph. I," J. SIAM Appl. Math., vol. 10, no. 3, pp. 496–506, 1962.
8. F. Harary, "Graph Theory," Addison-Wesley, Reading, Mass., 1969.
9. T. Mizuki, "Sharing unconditionally secure secret keys," Ph.D. Thesis, Tohoku University, Sendai, 2000.
10. T. Mizuki, H. Shizuya, and T. Nishizeki, "Dealing necessary and sufficient numbers of cards for sharing a one-bit secret key," Proc. Eurocrypt '99, Lecture Notes in Computer Science, Springer-Verlag, vol. 1592, pp. 389–401, 1999.
11. E. F. Schmeichel and S. L. Hakimi, "On planar graphical degree sequences," SIAM J. Appl. Math., vol. 32, no. 3, pp. 598–609, 1977.