Dealing Necessary and Sufficient Numbers of Cards for Sharing a One-Bit Secret Key
(Extended Abstract)

Takaaki Mizuki[1], Hiroki Shizuya[2], and Takao Nishizeki[3]

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

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 spanning 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. Our condition immediately yields an efficient linear-time algorithm to determine whether there exists a protocol to achieve such a secret key sharing.

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.

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

J. Stern (Ed.): EUROCRYPT'99, LNCS 1592, pp. 389–401, 1999.

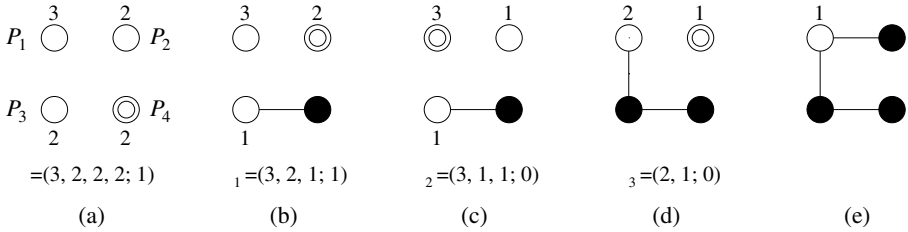

Fig. 1. A generating process of a key exchange graph.

pair of players P_i and P_j sharing a one-bit secret key $r_{ij} \in \{0, 1\}$. (See Figure 1.) Refer to [8] for the graph-theoretic terminology. If the key exchange graph is a spanning tree as illustrated in Figure 1(e), 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 spanning tree; when player P_i sends r to player P_j along an edge (i, j) of the spanning 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, Paterson and Rackoff give a protocol to form a spanning 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 [3,6] 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. Furthermore they give the so-called SFP protocol as a key set protocol. We say that a key set protocol *works for a signature* γ if the protocol always forms a spanning tree as the key exchange graph for any deal $\mathcal{C}$ having the signature γ [2,3,4,5,6]. Let Γ be a set of all signatures, where the number k of players and the total number d of dealt cards are taken over all values. Define sets W and L as follows:

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

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

Thus $\{W, L\}$ is a partition of set Γ. Fischer and Wright show that their SFP protocol works for all $\gamma \in W$ [3,6]. 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 $k \geq 3$ has not been known so far [3,6].

Since the SFP protocol works for all $\gamma \in W$, one can determine whether $\gamma \in W$ or not by simulating the SFP protocol for γ. However, it is necessary to simulate the protocol for all "malicious adversaries," and hence the time required by this simulation is exponential in k and such a simulation is impractical.

In this paper for the case $k \geq 3$ we give a simple necessary and sufficient condition on a signature γ for the existence of a key set protocol to work for γ.

Given a signature $\gamma = (c_1, c_2, \cdots, c_k; c_e)$, one can easily determine in time $O(k)$ whether γ satisfies our condition or not. Thus our condition immediately yields an efficient linear-time algorithm for determining whether there exists a key set protocol to work for a given signature γ. Our condition looks in appearance to be similar to the condition for a given degree sequence to be "graphical," and the proof for our condition is complicated as well as those for a degree sequence [1,7,8,10].

2 Preliminaries

In this section we explain the key set protocol formalized by Fischer and Wright, and present known results on this protocol [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 $y \in C_j$. 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 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, $x \notin (\bigcup_{i=1}^{k} C_i) \cup C_e$. 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 a 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 spanning tree. In the second case the protocol fails to form a spanning tree.

We now illustrate the 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, 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 has four isolated vertices and has no edge, as illustrated in Figure 1(a). In Figure 1 a white circle represents a vertex corresponding to a player remaining in the protocol, and the number attached to a white circle represents the size of the corresponding player's hand. Suppose that P_4 is chosen as a proposer in step 1. In Figure 1 a double white circle represents the vertex corresponding to a proposer. In step 2, P_4 proposes $K = \{x, y\}$ such that $x \in C_4$ and $y \notin C_4$. Assume that $y \in C_3$. Then step 3 is executed, P_3 and P_4 share a one-bit secret key r_{34}, and edge $(3, 4)$ is added to the key exchange graph, as illustrated in Figure 1(b). Since both cards x and y are discarded, the sizes of hands of both P_3 and P_4 decrease by one. Further, since the size of P_3's hand was the same as that of P_4's hand, the proposer P_4 discards all her cards and drops out of the protocol. Thus the resulting signature is $\gamma_1 = (3, 2, 1; 1)$. In Figure 1 a black circle represents a vertex corresponding to a player who has dropped out of the protocol. We now return to step 1. Assume that P_2 is chosen as a proposer and $y \in C_e$. Then step 4 is executed, and the sizes of hands of both P_2 and Eve decrease by one. Thus the resulting signature is $\gamma_2 = (3, 1, 1; 0)$, and no new edge is added to the key exchange graph, as illustrated in Figure 1(c). Since step 4 terminates, we now return to step 1. Assume that P_1 is chosen as a proposer and $y \in C_3$. Then edge $(1, 3)$ is added to the key exchange graph as illustrated in Figure 1(d). Since the size of P_1's hand decreases by one and P_3 drops out of the protocol, the resulting signature is $\gamma_3 = (2, 1; 0)$. We now return to step 1. Assume that P_2 is chosen as a proposer. Then $y \in C_1$ because only P_1 and P_2 remain in the protocol and Eve's hand has already been empty. Thus edge $(1, 2)$ is added to the key exchange graph, and the key exchange graph becomes a spanning tree, as illustrated in Figure 1(e). Thus the protocol terminates. As seen from the example above, during the execution of the key set protocol, each connected component of the key exchange graph always has exactly one vertex (drawn in a white circle) corresponding to a player remaining in the protocol.

Considering various procedures for choosing the proposer P_s in step 1, we obtain the class of *key set protocols*.

First consider the procedure in step 1 for the case $k = 2$. Fischer, Paterson and Rackoff show that, if the procedure always chooses the player with the larger hand as a proposer P_s, then the resulting key set protocol works for any signature $\gamma = (c_1, c_2; c_e)$ such that $c_2 \geq 1$ and $c_1 + c_2 \geq c_e + 2$ [2]. On the other hand, one can easily see that if there exists a key set protocol working for a signature $\gamma = (c_1, c_2; c_e)$ then $c_2 \geq 1$ and $c_1 + c_2 \geq c_e + 2$. Thus the following Theorem 1 holds [3].

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

Next consider the procedure in step 1 for the case $k \geq 3$. As a key set protocol, Fischer and Wright give the SFP (smallest feasible player) procedure which chooses the "feasible" player with the smallest hand as a proposer P_s [3,6]. Let $\gamma = (c_1, c_2, \cdots, c_k; c_e)$ be the current signature. If $c_e \geq 1$, P_i with $c_i = 1$ were chosen as a proposer, and $y \in C_e$ occurred, then P_i's hand would become empty although she remains in the protocol, and hence the key exchange graph would not become a spanning tree. On the other hand, if $c_e = 0$, then $y \in C_e$ does not occur and hence the procedure appears to be able to choose P_i with $c_i = 1$ as a proposer; however, if $y \in C_j$ and $c_j = 1$, then P_j's hand would become empty and hence the key exchange graph would not become a spanning tree. Thus the procedure can choose P_i with $c_i = 1$ as a proposer only when $c_e = 0$ and $c_j \geq 2$ for every j such that $1 \leq j \leq k$ and $j \neq i$, that is, only when $i = k$ and $c_{k-1} \geq 2$. Remember that $c_1 \geq c_2 \geq \cdots \geq c_k$ is assumed. Hence, we say that 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 the 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.

We define a mapping f from Γ to natural numbers, 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.

From now on let $\gamma = (c_1, c_2, \cdots, c_k; c_e)$. Note that the definition of f immediately implies the following Lemma 2. Lemma 2(a) provides a trivial necessary condition for $\gamma \in W$.

Lemma 2. *The following* (a) *and* (b) *hold.*

(a) *If* $k \geq 3$ *and* $\gamma \in W$, *then* $c_k \geq 1$ *and* $f(\gamma) \geq 1$ [3].
(b) *If* $c_k \geq 1$, *then* $c_i = 1$ *for every* i *such that* $f(\gamma) + 1 \leq i \leq k$.

The SFP procedure chooses a proposer P_s as follows:

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

The key set protocol resulting from this procedure is called the *SFP protocol*. The following Theorem 3 has been known on the SFP protocol [3,6].

Theorem 3. [3,6] *Let $\gamma \in \Gamma$. Then there exists a key set protocol working for γ, i.e. $\gamma \in W$, if and only if the SFP protocol works for γ.*

Furthermore the following Lemma 4 is known on a sufficient condition for $\gamma \in W$ [3,6].

Lemma 4. [3,6] *If $c_k \geq 1$ and $c_1 + c_k \geq c_e + k$, then $\gamma \in W$.*

The sufficient condition in Lemma 4 is not a necessary condition in general. For example, $\gamma = (3, 3, 2, 1; 1)$ does not satisfy the condition in Lemma 4, but the SFP protocol works for γ and hence $\gamma \in W$ [3,6]. In this paper we obtain a simple necessary and sufficient condition for $\gamma \in W$ for any $k \geq 3$. As shown later, $\gamma = (3, 3, 2, 1; 1)$ satisfies our necessary and sufficient condition.

3 Necessary and Sufficient Condition

For $k = 3$, we obtain the following Theorem 5 on a necessary and sufficient condition for $\gamma \in W$.

Theorem 5. *Let $k = 3$. Then $\gamma \in W$ if and only if $c_3 \geq 1$ and $c_1 + c_3 \geq c_e + 3$.*

Proof. Given in Section 5.

For $k \geq 4$, we obtain the following Theorem 6 on a necessary and sufficient condition for $\gamma \in W$. Hereafter let $B = \{i \in V \mid c_i = 2\}$, and let $b = \lfloor |B|/2 \rfloor$. Note that, by Lemma 2(a), a trivial necessary condition for $\gamma \in W$ is $c_k \geq 1$ and $f(\gamma) \geq 1$.

Theorem 6. *Let $k \geq 4$, $c_k \geq 1$ and $f \geq 1$. Then $\gamma \in W$ if and only if*

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

where

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

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

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

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

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

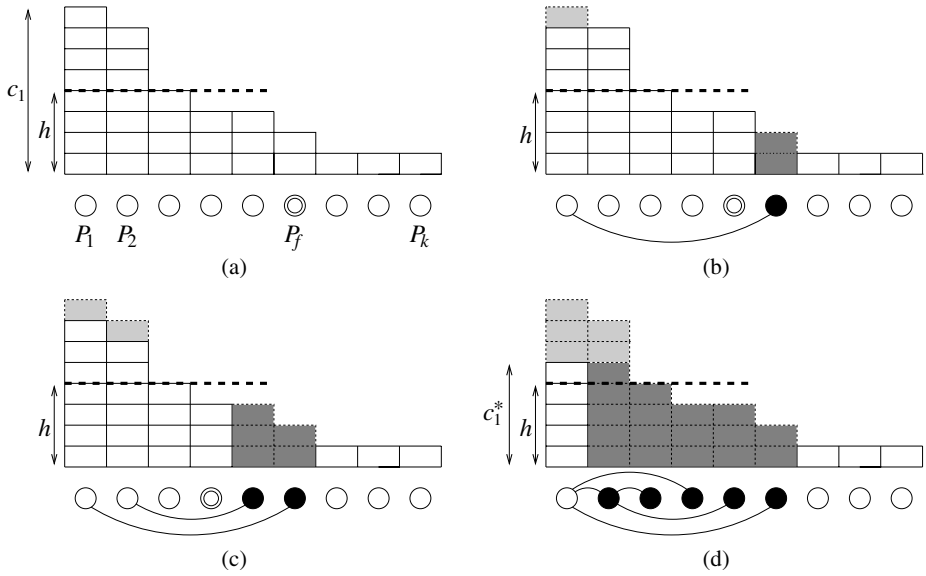

Fig. 2. The evolution of a key exchange graph and the alteration of a signature.

and

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

Proof. Given in Section 6.

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

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

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

Figure 2(a) illustrates Eq. (1); the left hand side of Eq. (1) is equal to the number of cards above the dotted line in Figure 2(a) where the rectangles stacked on a player P_i, $1 \le i \le k$, represent the cards of P_i's hand.

As mentioned in Section 2, the SFP protocol works for $\gamma = (3, 3, 2, 1; 1)$, but γ does not satisfy the sufficient condition in Lemma 4 [3,6]. By the definition of f we have $f = f(\gamma) = 3$. Since $k = 4$, we have $2 \le f = 3 = k - 1$, and hence by Eq. (6) $\delta = 1$. By Eq. (2) $\bar{f} = 3-1 = 2$, and by Eq. (4) $h = 1-1+4-2 = 2$. Since $f = 3 < 5$, by Eq. (7) we have $\epsilon = 0$. Hence by Eq. (3) we have $\widetilde{f} = 2-0 = 2$ and

by Eq. (5) $h^+ = 2+0 = 2$. Therefore $\sum_{i=1}^{\widetilde{f}} \max\{c_i - h^+, 0\} = (3-2)+(3-2) = 2 = \widetilde{f}$. Thus γ satisfies Eq. (1), the necessary and sufficient condition in Theorem 6.

The following Corollary 7 follows from Theorems 1, 5 and 6. This corollary provides a necessary and sufficient condition for $\gamma \in W$ under a natural assumption that all players have hands of the same size.

Corollary 7. *Let $k \geq 2$ and $c_1 = c_2 = \cdots = c_k$. Then $\gamma \in W$ if and only if*

$$c_1 \geq \begin{cases} c_e/2 + 1 & if\ k = 2; \\ c_e/2 + 3/2 & if\ k = 3;\ and \\ c_e/2 + 2 & if\ k \geq 4. \end{cases}$$

Corollary 7 means that the required size c_1 of hands is the same for any $k \geq 4$ when $c_1 = c_2 = \cdots = c_k$. Note that the total number kc_1 of required cards increases when k increases.

The following Corollary 8 is immediate from Corollary 7.

Corollary 8. *Let $k \geq 2$ and $c_1 = c_2 = \cdots = c_k = c_e$. Then $\gamma \in W$ if and only if*

$$c_1 \geq \begin{cases} 2\ if\ k = 2; \\ 3\ if\ k = 3;\ and \\ 4\ if\ k \geq 4. \end{cases}$$

4 Malicious Adversary

In this paper we use a *malicious adversary* in order to prove Theorem 6.

If a key set protocol works for a signature γ, then the key exchange graph must become a spanning 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 spanning tree. The malicious adversary determines who holds the card y. Considering a malicious adversary to make it hard for the key exchange graph to become a spanning tree, we obtain a necessary condition for $\gamma \in W$. On the other hand, if under some condition on a signature γ a key set protocol always forms a spanning tree as the key exchange graph for any malicious adversary, then the condition is a sufficient one for $\gamma \in W$.

We use a function $\mathcal{A} : \Gamma \times V \to V \cup \{e\}$ to represent a malicious adversary, as follows. Remember that Γ is the set of all signatures and that V is the set of indices of all the players remaining in a protocol. Let e be Eve's index. The inputs to the function $\mathcal{A}(\gamma, s)$ are the current signature $\gamma \in \Gamma$ and the index $s \in V$ of a proposer P_s chosen in 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 $y \in C_{\mathcal{A}(\gamma,s)}$.

The definition of a malicious adversary $\mathcal{A}$ immediately implies the following Lemma 9.

Lemma 9. *Let $k \geq 3$. Then $\gamma \in W$ if and only if there exists a proposer P_s such that $\gamma'_{(s,\mathcal{A})} \in W$ for any malicious adversary $\mathcal{A}$. That is,*

$$\gamma \in W \Longleftrightarrow \exists s\ \forall \mathcal{A}\ \ \gamma'_{(s,\mathcal{A})} \in W,$$

in other words,

$$\gamma \in L \Longleftrightarrow \forall s\ \exists \mathcal{A}\ \ \gamma'_{(s,\mathcal{A})} \in L.$$

From now on let $k \geq 3$. If $f = 0$, then by Lemma 2(a) $\gamma \in L$. On the other hand, if $f \geq 1$, then the index s of the proposer P_s chosen by the SFP procedure satisfies $s = f$. Furthermore, by Theorem 3 the SFP protocol works for all $\gamma \in W$. Thus, if $\gamma \in W$, then $\gamma'_{(f,\mathcal{A})} \in W$ for any malicious adversary $\mathcal{A}$. Hence, the following Corollary 10 immediately follows from Theorem 3.

Corollary 10. *Let $k \geq 3$ and $f(\gamma) \geq 1$. Then $\gamma \in W$ if and only if $\gamma'_{(f,\mathcal{A})} \in W$ for any malicious adversary $\mathcal{A}$. That is,*

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

in other words,

$$\gamma \in L \Longleftrightarrow \exists \mathcal{A}\ \ \gamma'_{(f,\mathcal{A})} \in L.$$

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. Furthermore, 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 $c_1 \geq c_2 \geq \cdots \geq c_k$.

The total size $\sum_{i=1}^{k} c_i$ of all the players' hands decreases by two or more if $\mathcal{A}(\gamma, s) = t \neq e$; it decreases by exactly one if $\mathcal{A}(\gamma, s) = e$. If a key set protocol works for γ, then $\mathcal{A}(\gamma, s) = t \neq e$ occurs $k-1$ times until the protocol terminates because the key exchange graph becomes a spanning tree having $k-1$ edges at the end of the protocol. Furthermore $\mathcal{A}(\gamma, s) = e$ would occur c_e times. Hence, if a key set protocol works for γ, then $\sum_{i=1}^{k} c_i \geq 2(k-1) + c_e = c_e + 2k - 2$. Thus we have the following Lemma 11 as a trivial necessary condition for $\gamma \in W$.

Lemma 11. *If $\gamma \in W$, then $\sum_{i=1}^{k} c_i \geq c_e + 2k - 2$.*

5 Proof of Theorem 5

In this section we give a proof of Theorem 5.

Since Lemma 4 implies the sufficiency of the condition in Theorem 5, we prove its necessity. That is, we show that if $k = 3$ and $\gamma \in W$ then $c_3 \geq 1$ and $c_1 + c_3 \geq c_e + 3$. In order to prove this, we use the following malicious adversary $\mathcal{A}^*$:

$$\mathcal{A}^*(\gamma, s) = \begin{cases} 3 \text{ if } s = 1; \\ 1 \text{ if } s = 2; \\ e \text{ if } s = 3. \end{cases}$$

We first have the following Lemma 12.

Lemma 12. *Let $k = 3$, $c_3 \geq 1$ and $c_1 + c_3 \leq c_e + 2$. Then the following* (a) *or* (b) *holds.*

(a) $\gamma \in L$.
(b) $\gamma'_{(f,\mathcal{A}^*)}$ *satisfies* $k' = 3$, $c'_3 \geq 1$ *and* $c'_1 + c'_3 \leq c'_e + 2$.

Proof. Let $k = 3$, $c_3 \geq 1$ and $c_1 + c_3 \leq c_e + 2$. If $f = 0$, then $\gamma \in L$ by Lemma 2(a). Thus one may assume that $1 \leq f \leq 3$. Then there are the following three cases.

Case 1: $f = 1$.

In this case, by Lemma 2(b), we have $\gamma = (c_1, 1, 1; c_e)$ and hence $c_2 = c_3 = 1$. Thus, by $c_1 + c_3 \leq c_e + 2$ we have $c_1 \leq c_e + 1$. Hence $\sum_{i=1}^{3} c_i \leq (c_e + 1) + 1 + 1 = c_e + 2k - 3$. Therefore $\gamma \in L$ by Lemma 11.

Case 2: $f = 2$.

In this case, by Lemma 2(b) we have $\gamma = (c_1, c_2, 1; c_e)$. Since $f = 2$, the definition of f implies $c_2 \geq 2$ and $c_e \geq 1$. Furthermore, since $c_3 = 1$ and $c_1 + c_3 \leq c_e + 2$, we have $c_1 \leq c_e + 1$. Since $f = 2$, let P_2 be a proposer P_s. Since $\mathcal{A}^*(\gamma, s) = 1$ for $s = 2$, the size of the hand of P_1 holding card y decreases by one and the proposer P_2 drops out of the protocol, and hence $\gamma'_{(f,\mathcal{A}^*)} = (c_1 - 1, 1; c_e)$. Therefore $c'_1 + c'_2 = (c_1 - 1) + 1 = c_1$. Since $c_1 \leq c_e + 1$ and $c'_e = c_e$, we have $c'_1 + c'_2 \leq c'_e + 1$. Thus by Theorem 1 $\gamma'_{(f,\mathcal{A}^*)} \in L$. Therefore Corollary 10 implies $\gamma \in L$.

Case 3: $f = 3$.

In this case $c_e \geq 1$; if $c_e = 0$, then by $c_3 \geq 1$ and $c_1 + c_3 \leq c_e + 2 = 2$ we have $c_1 = c_2 = c_3 = 1$, and hence $f = 0$, contrary to $f = 3$. Since $f = 3$, let P_3 be a proposer. Since $\mathcal{A}^*(\gamma, s) = e$ for $s = 3$, the sizes of the hands of both P_3 and Eve decrease by one, and hence $\gamma'_{(f,\mathcal{A}^*)} = (c_1, c_2, c_3 - 1; c_e - 1)$, $k' = 3$ and $c'_e = c_e - 1$. Since P_3 was feasible, we have $c'_3 = c_3 - 1 \geq 1$. Furthermore $c'_1 + c'_3 = c_1 + (c_3 - 1) \leq (c_e + 2) - 1 = c'_e + 2$. Thus (b) holds. ∎

Define the *size* $\mathrm{size}(\gamma)$ of a signature γ as follows: $\mathrm{size}(\gamma) = c_e + k$.

We are now ready to prove the necessity of the condition in Theorem 5.

(Proof for the necessity of the condition in Theorem 5)

Let $k = 3$. We shall show that if $c_3 = 0$ or $c_1 + c_3 \leq c_e + 2$ then $\gamma \in L$. If $c_3 = 0$, then Lemma 2(a) implies $\gamma \in L$. Therefore it suffices to prove the following claim: if $c_3 \geq 1$ and $c_1 + c_3 \leq c_e + 2$ then $\gamma \in L$. We prove the claim by induction on size$(\gamma) = c_e + k$. Let $c_3 \geq 1$ and $c_1 + c_3 \leq c_e + 2$. Since $k = 3$, size$(\gamma) \geq 3$.

First consider the case size$(\gamma) = 3$. In this case, $c_e = 0$, and hence $c_1 + c_3 \leq c_e + 2 = 2$. Thus $c_1 = c_2 = c_3 = 1$, and hence $f = 0$. Therefore by Lemma 2(a) $\gamma \in L$.

Next let $l \geq 4$, and assume inductively that the claim holds when size$(\gamma) = l - 1$.

Consider any signature γ such that size$(\gamma) = l$. By Lemma 12, the following (a) or (b) holds:

(a) $\gamma \in L$; and
(b) $\gamma'_{(f,\mathcal{A}^*)}$ satisfies $k' = 3$, $c'_3 \geq 1$ and $c'_1 + c'_3 \leq c'_e + 2$.

Thus one may assume that (b) holds. Then, since size(γ') = size$(\gamma) - 1 = l - 1$, by the induction hypothesis we have $\gamma'_{(f,\mathcal{A}^*)} \in L$. Therefore Corollary 10 implies $\gamma \in L$. ∎

6 Sketchy Proof of Theorem 6

In this section we outline a proof of Theorem 6.

One can easily prove Theorem 6 for the case $f = 1$ as follows. Let $k \geq 4$, $c_k \geq 1$ and $f = 1$. Then $\delta = \epsilon = 0$ and hence $\widetilde{f} = \bar{f} = f = 1$. By Lemma 2(b) $c_k = 1$ and hence $h^+ = h = c_e - 1 + k - 1 = c_e + k - 2$. Thus, Eq. (1) is equivalent to $\max\{c_1 - c_e - k + 2, 0\} \geq 1$, and hence equivalent to $c_1 \geq c_e + k - 1$. Therefore Theorem 6 for the case $f = 1$ immediately follows from the following Lemma 13.

Lemma 13. *Let $c_k \geq 1$ and $f = 1$. Then $\gamma \in W$ if and only if $c_1 \geq c_e + k - 1$.*

Proof. The sufficiency immediately follows from Lemma 4. Therefore it suffices to prove the necessity. Let $c_k \geq 1$, $f = 1$ and $\gamma \in W$. Then by Lemma 11 we have $\sum_{i=1}^{k} c_i \geq c_e + 2k - 2$. On the other hand, since $f = 1$, by Lemma 2(b) $\gamma = (c_1, 1, 1, \cdots, 1; c_e)$ and hence $\sum_{i=1}^{k} c_i = c_1 + k - 1$. Therefore, $c_1 + k - 1 \geq c_e + 2k - 2$ and hence $c_1 \geq c_e + k - 1$. ∎

We then sketch a proof of Theorem 6 for the case $2 \leq f \leq k$. The detail is omitted in this extended abstract. We sketch a proof only for the necessity of the condition in Theorem 6. (One can prove the sufficiency by induction on size$(\gamma) = c_e + k$.) Let $k \geq 4$, $c_k \geq 1$, $2 \leq f \leq k$ and $\gamma \in W$. Instead of proving Eq. (1) we prove the following equation holds:

$$\sum_{i=1}^{\bar{f}} \max\{c_i - h, 0\} \geq \bar{f}, \tag{9}$$

which is obtained from Eq. (1) by replacing $\widetilde{f}$ and h^+ with $\bar{f}$ and h, respectively.

For simplicity, we assume that $\delta = 1$, i.e. $2 \leq f \leq k-1$. (The proof for $\delta = 2, 3$ is similar.) Then by Lemma 2(b) $c_k = 1$. Furthermore $\bar{f} = f - 1$ and $h = c_e + k - f$. Thus Eq. (9) is equivalent to

$$\sum_{i=1}^{f-1} \max\{c_i - (c_e + k - f), 0\} \geq f - 1. \tag{10}$$

We prove the necessity of Eq. (10). Let $2 \leq f \leq k-1$. Then the signature is $\gamma = (c_1, c_2, \cdots, c_f, 1, 1, \cdots, 1; c_e)$. That is, there are exactly f feasible players $P_1, P_2, \cdots, P_f$, and each of the remaining $k - f$ players $P_{f+1}, P_{f+2}, \cdots, P_k$ has exactly one card. The key exchange graph has exactly k isolated vertices before starting the protocol, as illustrated in Figure 2(a). In Figure 2, a white rectangle represents a card in players' hands. The SFP protocol chooses the feasible player P_f with the smallest hand as a proposer. Consider a malicious adversary that does not choose Eve and always chooses the player with the largest hand as P_t with $y \in C_t$. Then P_f and the player P_t with the largest hand share a one-bit secret key, the size of P_t's hand decreases by one, P_f drops out of the protocol, and an edge joining two vertices corresponding to these two players is added to the key exchange graph, as illustrated in Figure 2(b). In the example of Figure 2, the size of P_1's hand decreases by one, P_f discards all her cards and drops out of the protocol, and edge $(1, f)$ is added to the key exchange graph. In Figure 2(b), we lightly shade the rectangle corresponding to the card y discarded by $P_t = P_1$, and darkly shade the rectangles corresponding to the cards discarded by P_f who drops out of the protocol. At the next execution of steps 1–4, the proposer is P_{f-1}. By considering the same malicious adversary as above, P_{f-1} and the player with the largest hand share a one-bit secret key as illustrated in Figure 2(c). In Figure 2(b), since P_1 has a hand of the same size as P_2, by Assumption 2 $P_t = P_2$ and hence edge $(2, f-1)$ is added to the key exchange graph as illustrated in Figure 2(c). Repeat such an operation until P_1 becomes a proposer, i.e. there exists exactly one feasible player as illustrated in Figure 2(d), and let $\gamma^* = (c_1^*, c_2^*, \cdots, c_{k^*}^*; c_e)$ be the resulting signature. Then $k^* = k - f + 1$, $c_2^* = c_3^* = \cdots = c_{k^*}^* = 1$, $f(\gamma^*) = 1$, and the size of Eve's hand remains c_e. By Corollary 10 we have $\gamma^* \in W$. Therefore, by Lemma 13, $c_1^* \geq c_e + k^* - 1 = c_e + k - f = h$. The malicious adversary has chosen $f - 1$ players P_i in total as P_t so far, and hence there are exactly $f - 1$ lightly shaded rectangles in Figure 2(d). The malicious adversary above implies that such a player P_i, $1 \leq i \leq f-1$, should have a hand of size greater than h when she was chosen by the malicious adversary. Thus there are $f-1$ or more rectangles above the dotted line in Figure 2(a). Therefore we have $\sum_{i=1}^{f-1} \max\{c_i - h, 0\} \geq f - 1$, and hence Eq. (10) holds.

We have sketched a proof of the necessity of Eq. (9). One can similarly prove the necessity of Eq. (1).

7 Conclusion

In this paper we gave a simple necessary and sufficient condition on signature $\gamma = (c_1, c_2, \cdots, c_k; c_e)$ for the existence of a key set protocol to work for γ. In other words we gave a simple complete characterization of the sets W and L.

Since the SFP protocol works for all $\gamma \in W$ (Theorem 3), one can determine whether $\gamma \in W$ or not by simulating the SFP protocol for γ. However, it is necessary to simulate the protocol for all malicious adversaries, and hence the time required by this simulation is exponential in k and such a simulation is impractical. Clearly one can determine in time $O(k)$ whether our necessary and sufficient condition, i.e. Eq. (1) or (8), holds or not. Thus one can determine in time $O(k)$ whether $\gamma \in W$ or not.

This paper addresses only the class of key set protocols, and hence it still remains open to obtain a necessary and sufficient condition for any (not necessarily key set) protocol to work for γ [5].

An Eulerian circuit is more appropriate as a key exchange graph than a spanning tree if it is necessary to acknowledge the secure key distribution. We have given a protocol to achieve such a key exchange [9].

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., 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, 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, 13, pp. 99–118, 1993.
4. M. J. Fischer and R. N. Wright, "An efficient protocol for unconditionally secure secret key exchange," Proceedings 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, 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, 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., 10, 3, pp. 496–506, 1962.
8. F. Harary, "Graph Theory," Addison-Wesley, Reading, Mass., 1969.
9. T. Mizuki, H. Shizuya and T. Nishizeki, "Eulerian secret key exchange," Proc. COCOON '98, Lecture Notes in Computer Science, Springer, 1449, pp. 349–360, 1998.
10. E. F. Schmeichel and S. L. Hakimi, "On planar graphical degree sequences," SIAM J. Appl. Math., 32, 3, pp. 598–609, 1977.