Necessary and Sufficient Numbers of Cards for the Transformation Protocol
(Extended Abstract)

Koichi Koizumi[1], Takaaki Mizuki[2,3], and Takao Nishizeki[1]

[1] Graduate School of Information Sciences, Tohoku University,
Sendai 980-8579, Japan
koizumi@nishizeki.ecei.tohoku.ac.jp
nishi@ecei.tohoku.ac.jp
[2] Information Synergy Center, Tohoku University,
Sendai 980-8578, Japan
mizuki@isc.tohoku.ac.jp
[3] PRESTO, JST, Saitama, 332-0012, Japan

Abstract. The transformation protocol can make two players share a secret key using a random deal of cards. A sufficient condition on the number of cards for the transformation protocol to succeed was known. However, it has been an open problem to obtain a necessary and sufficient condition. This paper improves the transformation protocol and gives a necessary and sufficient condition for the improved transformation protocol to succeed.

1 Introduction

A random deal of cards can be used for players to share a secret. For example, Winkler [13] gave bidding conventions for the game of bridge whereby one player can send secret information to her partner. This idea was carried further so that two players can share a secret key using a random deal of cards [1]. Since then, several protocols using a random deal of cards have been developed; Fischer and Wright gave two important protocols called the "key set protocol [2, 5]" and the "transformation protocol [3]." The properties of the key set protocol have been investigated extensively [6–12]. For instance, a necessary and sufficient condition on the number of cards for the key set protocol to succeed was known [7, 9]. On the other hand, concerning the transformation protocol, few results have been obtained so far. For instance, a sufficient condition for the transformation protocol to succeed was known [3]. However, it has been an open problem to obtain a necessary and sufficient condition. In this paper, we will address only the transformation protocol, and close the open problem above.

The scenario is as follows. Two players Alice and Bob communicate publicly, while a passive computationally-unlimited eavesdropper Eve overhears all communication. Alice and Bob are assumed to use randomization, that is, they can flip private fair coins. Let n be a positive real number such that $n = \log_2 m$ for some integer $m \geq 2$ and hence $m = 2^n$. Alice and Bob wish to share an n-bit

K.-Y. Chwa and J.I. Munro (Eds.): COCOON 2004, LNCS 3106, pp. 92–101, 2004.

secret key $v \in \{1, 2, 3, \cdots, 2^n (= m)\}$ which Eve cannot learn. That is, they wish to share a value $v \in \{1, 2, 3, \cdots, 2^n\}$ such that, given the information available to Eve, the (conditional) probability of $v = \ell$ is exactly $1/2^n$ for every $\ell \in [1, 2^n]$.

Let $\Delta = \{1, 2, \cdots, d\}$ be a *deck* of d distinct cards; an element in the deck Δ is a card. We call a subset $H \subseteq \Delta$ of Δ a *hand*. A sequence $\delta = (H_a, H_b; H_e)$ of three hands such that $\{H_a, H_b, H_e\}$ is a partition of Δ is called a *deal*. A deal $\delta = (H_a, H_b; H_e)$ means that every card in Δ is dealt to Alice, Bob or Eve so that Alice, Bob and Eve have hands H_a, H_b and H_e, respectively, as in the case of usual card games. We call $\gamma = (a, b; e)$ the *signature* of a deal $\delta = (H_a, H_b; H_e)$ if $a = |H_a|$, $b = |H_b|$ and $e = |H_e|$, where $|X|$ denotes the cardinality of a set X.

Fix a signature $\gamma = (a, b; e)$ with $a, b \geq 1$. For such γ, we always fix the deck $\Delta = \{1, 2, \cdots, a + b + e\}$. Then, there are exactly $\binom{a+b+e}{a} \cdot \binom{b+e}{b}$ deals having the signature γ. Assume that Alice, Bob and Eve have their hands H_a, H_b and H_e, respectively, from a random deal $\delta = (H_a, H_b; H_e)$ whose signature is γ. As in the case of usual card games, all the cards in her/his hand are private to herself/himself. Given such a random deal δ, Alice and Bob wish to share a secret key: the goal is to design a protocol which makes Alice and Bob share an n-bit secret key that Eve cannot learn. We say that a protocol *establishes an n-bit secret key exchange* for a signature $\gamma = (a, b; e)$ if the protocol always makes Alice and Bob share an n-bit secret key $v \in \{1, 2, 3, \cdots, 2^n\}$ for any random deal $\delta = (H_a, H_b; H_e)$ having the signature γ and any random result of flipping their coins.

In this paper, we first improve the transformation protocol. Our "improved transformation protocol" is superior to the transformation protocol. That is, the improved transformation protocol establishes an n-bit secret key exchange for any signature γ for which the (original) transformation protocol does. We then give a necessary and sufficient condition for the improved transformation protocol to establish an n-bit secret key exchange for a signature $\gamma = (a, b; e)$. We thus close the open problem above.

2 Preliminaries

In this section, we define some terms, and describe the transformation protocol [3] given by Fischer and Wright. Fix a signature $\gamma = (a, b; e)$ with $a, b \geq 1$, and let $\delta = (H_a, H_b; H_e)$ be a random deal having the signature γ.

A subset $S \subseteq \Delta$ of the deck Δ is called an (s, i, j)*-portion relative to* δ if $s = |S|$, $i, j \geq 1$, and S contains exactly i cards from Alice's hand H_a, exactly j cards from Bob's hand H_b and exactly $s - i - j$ cards from Eve's hand H_e. We often omit the phrase "relative to δ" if it is clear from the context. An (s, i, j)-portion S is said to be *complete* if $s = i + j$, i.e. Eve has no card in S. Furthermore, an (s, i, j)-portion S is said to be *partial* if $s > i + j$, i.e. Eve has at least one card in S. A portion S is said to be *opaque* if Eve does not know anything about the location of the cards in $S \backslash H_e$. Consider the case where Alice and Bob obtain an opaque complete (s, i, j)-portion S, i.e. an opaque $(i+j, i, j)$-portion S. Since Eve has no card in S, Alice and Bob completely know the

owners of all cards in S, but Eve knows nothing about it. Therefore, from the portion S, Alice and Bob can share a $\log_2 \binom{i+j}{i}$-bit secret key. Thus, an opaque complete portion immediately brings Alice and Bob a secret key.

A set $\mathcal{C}$ of pairwise disjoint portions relative to δ is called a *collection relative to* δ. We often omit the phrase "relative to δ" if it is clear from the context. We say that a collection $\mathcal{C} = \{S_1, S_2, \cdots, S_m\}$ is *opaque* if Eve does not know anything about the location of the cards in $S_1 \setminus H_e, S_2 \setminus H_e, \cdots, S_m \setminus H_e$. If Alice and Bob obtain an opaque collection $\mathcal{C}$ containing complete portions, then they can share a secret key.

During any execution of the transformation protocol, Alice and Bob start with the *initial* collection $\mathcal{C}_0 = \{\Delta\}$, change $\mathcal{C}_0$ into another collection $\mathcal{C}_1$, change $\mathcal{C}_1$ into $\mathcal{C}_2$, and so on. They finally obtain an opaque *terminal* collection $\mathcal{C}_t$. A collection $\mathcal{C}_\ell$ can be changed into another collection $\mathcal{C}_{\ell+1}$, $0 \leq \ell \leq t-1$, by a *splitting transformation* or a *combining transformation*. A splitting transformation replaces an (s, i, j)-portion in the current collection with several smaller portions. A combining transformation replaces two $(s, 1, 1)$-portions in the current collection with a single $(s', 1, 1)$-portion for some $s' < s$.

To simplify the notation, we hereafter denote by $\mathcal{C}$ the current collection which Alice and Bob maintain if it is clear from the context. Alice and Bob start with $\mathcal{C} = \mathcal{C}_0 = \{\Delta\}$. We sometimes use $\mathcal{C}'$ to represent a collection resulting from the current collection $\mathcal{C}$ by some transformation.

We first present how to apply a splitting transformation to $\mathcal{C}$, i.e. how to split a portion S in $\mathcal{C}$.

Splitting: An (s, i, j)-portion S with $i + j \geq 3$ can be split so that several smaller new portions will be acquired. If $i \geq j$, then the splitting transformation proceeds as described below. If $i < j$, then the roles of Alice and Bob are reversed.

1. Alice randomly partitions S into i sets $S'_1, S'_2, \cdots, S'_i$, each of size $\lfloor s/i \rfloor$ or $\lceil s/i \rceil$, such that she has exactly one card in each set, and announces the sets.
2. Bob says how many cards he has in each set announced by Alice.
3. Each set in which Bob has at least one card is acquired as a new portion.

Notice that any $(s, 1, 1)$-portion cannot be split. For an (s, i, j)-portion S, we say that S is *splittable* if $i + j \geq 3$; and S is *non-splittable* if $i + j = 2$, i.e. $i = j = 1$.

Alice and Bob repeat applying a splitting transformation to $\mathcal{C}$ until any portion in $\mathcal{C}$ cannot be split. Then each portion S_ℓ, $1 \leq \ell \leq m$, in the current collection $\mathcal{C} = \{S_1, S_2, \cdots, S_m\}$ is a $(|S_\ell|, 1, 1)$-portion. They next repeat applying the following combining transformation to $\mathcal{C}$, i.e. repeat combining two portions S_1 and S_2 having the same sizes in $\mathcal{C}$.

Combining: Two $(s, 1, 1)$-portions S_1 and S_2 with $s \geq 3$ can be combined so that a new portion S' will be acquired.

1. Alice randomly chooses an integer $p \in \{1, 2\}$. Let $q = 3 - p$.
2. Alice constructs and announces a set T consisting of her card in S_p, $\lfloor s/3 \rfloor - 1$ cards randomly chosen from S_p that are not hers, and $\lfloor s/3 \rfloor$ cards randomly chosen from S_q that are not hers.

3. Bob announces how many cards he has in T.
   (a) If Bob has no card in T, then Alice announces the set difference $S_q \setminus T$, which is acquired as a new portion $S' = S_q \setminus T$.
   (b) If Bob has exactly one card in T, then T is acquired as a new portion $S' = T$.
   (c) If Bob has two cards in T, then Alice announces $S_p \cap T$, which is acquired as a new portion $S' = S_p \cap T$.

As Alice and Bob repeat combining two portions in the current collection $\mathcal{C}$, the sizes of the portions in $\mathcal{C}$ become smaller. Notice that $(2,1,1)$-portions cannot be combined. When they cannot apply a combining transformation to $\mathcal{C}$, they obtain a terminal collection $\mathcal{C} = \mathcal{C}_t$; the terminal collection $\mathcal{C}_t$ possibly contains $(2,1,1)$-portions, which can be used to share a secret key.

We are now ready to give the full description of the transformation protocol. Given a random deal $\delta = (H_a, H_b; H_e)$, the transformation protocol proceeds as follows.

Transformation protocol:

1. The initial collection is $\mathcal{C} = \mathcal{C}_0 = \{\Delta\}$.
2. Splitting is repeated as long as there is a splittable portion, i.e. an (s,i,j)-portion with $i + j \geq 3$, in $\mathcal{C}$: choose such a portion S in $\mathcal{C}$ according to any prearranged rule, remove S from $\mathcal{C}$, apply a splitting transformation to S, and add all the new acquired portions to $\mathcal{C}$.
3. Combining is repeated as long as there is a pair of $(s,1,1)$-portions with $s \geq 3$ in $\mathcal{C}$: choose such two portions S_1 and S_2 in $\mathcal{C}$ according to any prearranged rule, remove both S_1 and S_2 from $\mathcal{C}$, apply a combining transformation to S_1 and S_2, and add the new acquired portion to $\mathcal{C}$.
4. From the terminal collection $\mathcal{C} = \mathcal{C}_t$, Alice and Bob share an n-bit secret key, where n is the number of $(2,1,1)$-portions in $\mathcal{C}_t$.

We now describe the definitions of the "potential function" ϕ and the constant W [3]. Let $c = \log_{3/2} 2$. The potential function $\phi(s,i,j)$ is recursively defined as follows:

$$\phi(s,i,j) = \begin{cases} 2 & \text{if } s = 2 \text{ and } i = j = 1; \\ (s-2)^{-c} & \text{if } s \geq 3 \text{ and } i = j = 1; \\ j\phi(\lceil s/i \rceil, 1, 1) & \text{if } i \geq j \text{ and } i \geq 2; \text{ and} \\ \phi(s,j,i) & \text{if } i < j. \end{cases}$$

The constant W is defined as $W = \sum_{s=3}^{\infty} (s-2)^{-c}$. (One can show that $2.0356 < W < 2.0358$ [3].) Using ϕ and W, we present the sufficient condition given by Fischer and Wright as in the following Theorem 1.

Theorem 1 ([3]) *Let n be a positive integer, and let $\gamma = (a,b;e)$ be a signature with $a, b \geq 1$. If $\phi(a+b+e, a, b) > W + 2(n-1)$, then the transformation protocol establishes an n-bit secret key exchange for γ.*

The condition in Theorem 1, i.e. $\phi(a+b+e,a,b) > W + 2(n-1)$, is a sufficient condition for the transformation protocol to establish an n-bit secret

key exchange for $\gamma = (a, b; e)$. However, it is not a necessary condition in general. It has been an open problem to obtain a necessary and sufficient condition. This paper closes the open problem as in the succeeding section.

3 Improved Transformation Protocol

In this section, we first slightly modify the transformation protocol, and then give a necessary and sufficient condition for our improved transformation protocol to establish an n-bit secret key exchange for a signature $\gamma = (a, b; e)$. There are two main ideas behind the modification. In the remainder of this paper, all logarithms are to the base 2.

3.1 Stopping Useless Splitting Transformations

In this subsection, we explain the first improvement, i.e. stopping a "useless" splitting transformation; the idea behind the improvement is naive.

We now explain a "useless" splitting transformation, as follows. Assume that, during the execution of the transformation protocol, Alice and Bob obtain an opaque complete splittable portion, say an opaque $(3, 1, 2)$-portion S. According to the transformation protocol, S is eventually split into a $(2, 1, 1)$-portion S'_1 and a singleton set S'_2 consisting of one card from Bob's hand. Since the singleton set S'_2 contains no Alice's card, S'_2 is discarded, and hence only the $(2, 1, 1)$-portion S'_1 is acquired as a new portion. Comparing the original $(3, 1, 2)$-portion S and the acquired $(2, 1, 1)$-portion S'_1, S is preferable to S'_1, because a $\log 3$-bit secret key is distilled from S while only a one-bit secret key is distilled from S'_1. Thus, it is "useless" to split S. More generally, one can immediately notice that it is *useless* to split a complete portion, i.e. an $(i + j, i, j)$-portion for some i and j, which can be used to share a $\log \binom{i+j}{i}$-bit secret key. Therefore, we never split a complete portion in our transformation protocol. This is the idea behind the first improvement. The full description of our transformation protocol will be given in Section 3.3.

In the remainder of this subsection, we introduce two functions ψ_{C} and ψ_{P}, which will be used later to describe a necessary and sufficient condition for our transformation protocol to establish an n-bit secret key exchange for a signature $\gamma = (a, b; e)$.

We first introduce a function ψ_{C} which maps a portion S (relative to a deal δ) to a nonnegative real number. (Strictly speaking, the variable of the function ψ_{C} should be a pair (S, δ) instead of S, but we write simply $\psi_{\mathrm{C}}(S)$.) The function ψ_{C} is called the *completely potential function*. Intuitively, it means that a $\psi_{\mathrm{C}}(S)$-bit secret key can be distilled directly from a portion S. Remember that, from a complete portion, namely an $(i + j, i, j)$-portion, Alice and Bob can share a $\log \binom{i+j}{i}$-bit secret key. Hence, we define the completely potential function $\psi_{\mathrm{C}}(S) = \psi_{\mathrm{C}}(s, i, j)$ for an (s, i, j)-portion S as follows:

$$\psi_{\mathrm{C}}(s, i, j) = \begin{cases} \log \binom{i+j}{i} & \text{if } s = i + j; \\ 0 & \text{otherwise.} \end{cases} \tag{1}$$

We next introduce a function ψ_{P} which maps a portion S (relative to a deal δ) to a nonnegative real number. The function ψ_{P} is called the *partially potential function*. Roughly speaking, whereas a $\psi_{\mathrm{C}}(S)$-bit secret key can always be distilled directly from a portion S, a $\psi_{\mathrm{P}}(S)$-bit secret key may be distilled from S by splitting and/or combining.

We first define the partially potential function $\psi_{\mathrm{P}}(S) = \psi_{\mathrm{P}}(s,i,j)$ for a complete portion S, i.e. an (s,i,j)-portion S with $s = i + j$. Since such a portion S is never split and never combined, we define

$$\psi_{\mathrm{P}}(s,i,j) = 0 \quad \text{if } s = i + j. \tag{2}$$

We then define ψ_{P} for a partial portion S, i.e. an (s,i,j)-portion S with $s > i + j$. We will define ψ_{P} for a partial non-splittable portion S in the succeeding subsection; thus, we now consider a partial splittable portion S, i.e. an (s,i,j)-portion S such that $s > i+j \geq 3$. Note that such a portion S will be split. We recursively set $\psi_{\mathrm{P}}(S)$ to be the summation of $\psi_{\mathrm{P}}(S'_1), \psi_{\mathrm{P}}(S'_2), \cdots, \psi_{\mathrm{P}}(S'_m)$, where $S'_1, S'_2, \cdots, S'_m$ are the portions acquired by some particular splitting transformation, called the "worst" splitting. Assume for the moment that $i \geq j$, i.e. Alice does not have fewer cards in S than Bob. Furthermore, assume that Alice does not have more cards in S than Eve, i.e. $s - (i + j) \geq i$, or $s \geq 2i + j$. As the "worst" splitting, we consider the case where Alice would split the portion S into i subportions so that Bob has exactly one card in every S'_ℓ, $1 \leq \ell \leq j$. One may assume that $S'_1, S'_2, \cdots, S'_i$ are sorted in non-increasing order of their cardinalities. Note, in this case, that each of the acquired portions $S'_1, S'_2, \cdots, S'_j$ is either a $(\lceil s/i \rceil, 1, 1)$-portion or a $(\lfloor s/i \rfloor, 1, 1)$-portion. Note, furthermore, that each of the first j subportions $S'_1, S'_2, \cdots, S'_j$ is a partial portion, i.e. $|S'_\ell| \geq 3$ for every ℓ, $1 \leq \ell \leq j$, because Eve has i or more cards. We now count the numbers of $(\lceil s/i \rceil, 1, 1)$-portions and $(\lfloor s/i \rfloor, 1, 1)$-portions. Let r be the remainder when dividing s by i, that is, let $r = s \bmod i$. If $r = 0$, then there are exactly j $(s/i, 1, 1)$-portions. If $1 \leq r < j$, then there are exactly r $(\lceil s/i \rceil, 1, 1)$-portions and exactly $j - r$ $(\lfloor s/i \rfloor, 1, 1)$-portions. If $j \leq r$, then there are exactly j $(\lceil s/i \rceil, 1, 1)$-portions. Thus, for an (s,i,j)-portion S such that $s > i + j \geq 3$, $i \geq j$ and $s \geq 2i + j$, we define

$$\psi_{\mathrm{P}}(s,i,j) = \begin{cases} j\psi_{\mathrm{P}}(s/i,1,1) & \text{if } r = 0; \\ r\psi_{\mathrm{P}}(\lceil s/i \rceil,1,1) + (j-r)\psi_{\mathrm{P}}(\lfloor s/i \rfloor,1,1) & \text{if } 1 \leq r < j; \\ j\psi_{\mathrm{P}}(\lceil s/i \rceil,1,1) & \text{if } j \leq r, \end{cases} \tag{3}$$

where $r = s \bmod i$. Next assume that Alice has more cards than Eve, i.e. $s - (i + j) < i$, or $s < 2i + j$. Then, at least one $(2,1,1)$-portion is always produced, and hence, for an (s,i,j)-portion S such that $s > i + j \geq 3$, $i \geq j$ and $s < 2i + j$, we define

$$\psi_{\mathrm{P}}(s,i,j) = 1 \quad \text{if } s > i + j \geq 3,\ i \geq j \text{ and } s < 2i + j. \tag{4}$$

For the case of $i < j$, we define

$$\psi_{\mathrm{P}}(s,i,j) = \psi_{\mathrm{P}}(s,j,i) \quad \text{if } s > i + j \geq 3 \text{ and } i < j. \tag{5}$$

3.2 Combining with Dummy Cards

In this subsection, we explain the second improvement; we introduce an operation called "combining with dummy cards," whereby Alice and Bob can efficiently utilize "unused" portions.

We first explain an *unused* portion. Consider the case where Alice and Bob obtain a terminal collection $\mathcal{C}_t = \{S_1, S_2, \cdots, S_m\}$ when the transformation protocol terminates. There is no pair of portions S_g and S_ℓ in $\mathcal{C}_t$ with $s_g = s_\ell \geq 3$. If all the m portions in $\mathcal{C}_t$ are $(2,1,1)$-portions, then Alice and Bob share an m-bit secret key, and hence there is no "unused" portion. However, if $\mathcal{C}_t$ contains an $(s,1,1)$-portion with $s \geq 3$, then such a portion is not used to share a secret key, and hence it is unused.

In order to utilize unused portions, we need to combine two portions of different sizes. For this purpose, we add "dummy" cards to the smaller portion. For example, consider a $(6,1,1)$-portion S_1 and a $(5,1,1)$-portion S_2. We add one *dummy* card x to the portion S_2 so that the resulting portion $U_2 = S_2 \cup \{x\}$ has the same size as S_1. The dummy card x is chosen not in $S_1 \cup S_2$. Alice and Bob regard the dummy card x as Eve's card. Then, we apply to S_1 and U_2 a combining transformation described in Section 2. Let U' be the new portion acquired by combining. If U' has the dummy card x, then remove it from U'. That is, let $S' = U' \setminus \{x\}$, which is acquired as a new portion. In this way, one can combine two portions of different sizes. We thus obtain the following operation, called *combining with dummy cards*.

Combining with dummy cards: An $(s_1,1,1)$-portion S_1 and an $(s_2,1,1)$-portion S_2 with $s_1 \geq s_2 \geq 3$ can be combined so that a new portion S' will be acquired, as follows.

1. Let D be any set of dummy cards such that $|D| = s_1 - s_2$ and $D \cap (S_1 \cup S_2) = \emptyset$. All the dummy cards in D are added to S_2, that is, let $U_1 = S_1$ and $U_2 = S_2 \cup D$. Note that D is an empty set if $s_1 = s_2$.
2. Alice randomly chooses an integer $p \in \{1,2\}$. Let $q = 3 - p$.
3. Alice constructs and announces a set T consisting of her card in U_p, $\lfloor s_1/3 \rfloor - 1$ cards randomly chosen from U_p that are not hers, and $\lfloor s_1/3 \rfloor$ cards randomly chosen from U_q that are not hers.
4. Bob announces how many cards he has in T.
   (a) If Bob has no cards in T, then Alice announces the set difference $U_q \setminus T$ and let $U' = U_q \setminus T$.
   (b) If Bob has exactly one card in T, then let $U' = T$.
   (c) If Bob has two cards in T, then Alice announces $U_p \cap T$ and let $U' = U_p \cap T$.
5. If U' has dummy cards, then remove them from U', i.e. let $S' = U' \setminus D$. Alice and Bob acquire S' as a new portion.

When an $(s_1,1,1)$-portion S_1 and an $(s_2,1,1)$-portion S_2 such that $s_1 \geq s_2$ are combined with dummy cards, the acquired portion S' has size at most $\lceil 2s_1/3 \rceil$; in particular, if Alice chooses $p = 2$ in step 2 and Bob has no card in T

announced by Alice, then the acquired portion $S' = (U_1 \setminus T) \setminus D = S_1 \setminus T$ contains no dummy card, and hence $|S'| = \lceil 2s_1/3 \rceil$. Thus, in the "worst" combining, the acquired portion S' always has the size of exactly $\lceil 2s_1/3 \rceil$.

Since we have not defined ψ_{P} for a partial non-splittable portion, i.e. an (s,i,j)-portion with $s > i + j = 2$, we complete the definition of ψ_{P} in the remainder of this subsection. That is, we define $\psi_{\mathrm{P}}(s,1,1)$ for $s \geq 3$. Note that, by combining, two $(3,1,1)$-portions become a $(2,1,1)$-portion which yields a one-bit secret key, and that two $(s,1,1)$-portions with $s \geq 4$ become a $(\lceil 2s/3 \rceil, 1, 1)$-portion in the "worst" case. Thus, we recursively define

$$\begin{cases} \psi_{\mathrm{P}}(3,1,1) = 1/2; \text{ and} \\ \psi_{\mathrm{P}}(s,1,1) = \frac{1}{2}\,\psi_{\mathrm{P}}(\lceil 2s/3 \rceil, 1, 1) \text{ if } s \geq 4. \end{cases} \tag{6}$$

Notice that $\psi_{\mathrm{P}}(s,1,1)$ is monotonically decreasing in s for all integers $s \geq 3$. We have thus completed the definition of ψ_{P}. In our transformation protocol whose full description will appear in the succeeding subsection, we combine an $(s_1,1,1)$-portion S_1 and an $(s_2,1,1)$-portion S_2 with dummy cards only if $\psi_{\mathrm{P}}(S_1) = \psi_{\mathrm{P}}(S_2)$; otherwise, the "partially potential" may decrease; for example, if a $(3,1,1)$-portion S_1 and a $(4,1,1)$-portion S_2 were combined, then a $(3,1,1)$-portion S' would be obtained in the "worst" case, and hence the "partially potential" decreases by $1/2^2$.

3.3 Our Protocol and Results

We generalize a key set protocol [2, 5] to a "multiple key sets protocol," whose definition is omitted in this extended abstract due to page limitation. As explained in Sections 3.1 and 3.2, we modify the transformation protocol and obtain the following *improved transformation protocol*. Given a random deal δ, the improved transformation protocol proceeds as follows.

Improved transformation protocol:

1. If the signature $\gamma = (a, b; e)$ of δ satisfies $0 < e < \max\{a, b\}$, then the multiple key sets protocol is executed so that Alice and Bob share at least a $\min\{a, b, \lfloor (a + b - e)/2 \rfloor\}$-bit secret key, and the improved transformation protocol terminates. If $e = 0$ or $e \geq \max\{a, b\}$, then go to step 2.
2. The initial collection is $\mathcal{C} = \mathcal{C}_0 = \{\Delta\}$.
3. Splitting is repeated as long as $\mathcal{C}$ contains a partial splittable portion, i.e. an (s,i,j)-portion with $s > i + j \geq 3$: choose such a portion S in $\mathcal{C}$ according to any prearranged rule, remove S from $\mathcal{C}$, apply a splitting transformation to S, and add all the new acquired portions to $\mathcal{C}$.
4. The operation of the combining with dummy cards is repeated as long as there are two portions S_1 and S_2 in $\mathcal{C}$ such that S_1 is an $(s_1,1,1)$-portion, S_2 is an $(s_2,1,1)$-portion, $s_1 \geq s_2 \geq 3$, and $\psi_{\mathrm{P}}(S_1) = \psi_{\mathrm{P}}(S_2)$: choose such two portions S_1 and S_2 in $\mathcal{C}$ according to any prearranged rule, remove both S_1 and S_2 from $\mathcal{C}$, apply a combining transformation with dummy cards to S_1 and S_2, and add the new acquired portion to $\mathcal{C}$.

5. Alice and Bob share a $\sum_{S\in\mathcal{C}_t}\psi_{\mathrm{C}}(S)$-bit secret key from the terminal collection $\mathcal{C}=\mathcal{C}_t$, and the improved transformation protocol terminates.

In step 1, we use the multiple key sets protocol because this protocol is effective when a signature $\gamma=(a,b;e)$ satisfies $0<e<\max\{a,b\}$.

We now give the definition of our potential function ψ which maps a collection $\mathcal{C}$ to a nonnegative real number as follows:

$$\psi(\mathcal{C})=\sum_{S\in\mathcal{C}}\psi_{\mathrm{C}}(S)+\left\lfloor\sum_{S\in\mathcal{C}}\psi_{\mathrm{P}}(S)\right\rfloor. \tag{7}$$

(We takes the floor in the second term of the right hand side, because a set of partial portions is transformed into several $(2,1,1)$-portions, each of which yields a one-bit secret key.) We write $\psi(a+b+e,a,b)$ instead of $\psi(\mathcal{C}_0)$ if $\mathcal{C}_0=\{\Delta\}$ is a singleton collection relative to a deal δ having a signature $\gamma=(a,b;e)$.

Considering the case where the multiple key sets protocol runs, we define a function $\Psi(a,b;e)$ for a signature $\gamma=(a,b;e)$ with $a,b\geq 1$, as follows:

$$\Psi(a,b;e)=\begin{cases}\min\{a,b,\lfloor(a+b-e)/2\rfloor\} & \text{if } 0<e<\max\{a,b\};\\ \psi(a+b+e,a,b) & \text{otherwise.}\end{cases} \tag{8}$$

We have the following Theorem 2 as our main result. We omit a proof of Theorem 2 due to the page limitation.

Theorem 2 *Let $n=\log m$ for an integer $m\geq 2$, and let $\gamma=(a,b;e)$ be a signature with $a,b\geq 1$. Then the improved transformation protocol establishes an n-bit secret key exchange for γ if and only if $\Psi(a,b;e)\geq n$.*

4 Conclusions

The transformation protocol can efficiently make players share a perfect secret key using a random deal of cards. A sufficient condition for the transformation protocol to establish an n-bit secret key exchange was known. However, it has been an open problem to obtain a necessary and sufficient condition. This paper improves the transformation protocol, and gives a necessary and sufficient condition for the improved transformation protocol to establish an n-bit secret key exchange as in Theorem 2. Our improved transformation protocol is entirely superior to the original transformation protocol. Thus, Theorem 2 closes the open problem above.

Fischer and Wright [3, 5] proposed a method for reducing the problem of a multiparty n-bit secret key exchange to the problem of a 2-party n-bit secret key exchange. Hence, using this method, one can easily extend our protocol so that it performs a k-party n-bit secret key exchange with $k\geq 3$.

This paper addresses only the transformation protocol. Therefore, it still remains open to obtain a necessary and sufficient condition for any (not necessarily transformation) protocol to establish an n-bit secret key exchange for a signature γ [4, 14].

References

1. 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.
2. 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.
3. M. J. Fischer and R. N. Wright, "An efficient protocol for unconditionally secure secret key exchange," Proc. the 4th Annual Symposium on Discrete Algorithms, pp. 475–483, 1993.
4. 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.
5. 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, vol. 576, pp. 141–155, 1992.
6. T. Mizuki and T. Nishizeki, "Necessary and sufficient numbers of cards for sharing secret keys on hierarchical groups," IEICE Trans. Inf. & Syst., vol. E85-D, no. 2, pp. 333–345, 2002.
7. T. Mizuki, H. Shizuya, and T. Nishizeki, "A complete characterization of a family of key exchange protocols," International Journal of Information Security, vol. 1, no. 2, pp. 131–142, 2002.
8. T. Mizuki, H. Shizuya, and T. Nishizeki, "Characterization of optimal key set protocols," Discrete Applied Mathematics, vol. 131, pp. 213–236, 2003.
9. 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, vol. 1592, pp. 389–401, 1999.
10. T. Mizuki, H. Shizuya, and T. Nishizeki, "Eulerian secret key exchange," Proc. COCOON '98, Lecture Notes in Computer Science, vol. 1449, pp. 349–360, 1998.
11. T. Mizuki, Z. Sui, H. Shizuya, and T. Nishizeki, "On the average length of secret key exchange Eulerian circuits," IEICE Trans. Fundamentals, vol. E83-A, no. 4, pp. 662–670, 2000.
12. R. Yoshikawa, S. Guo, K. Motegi, and Y. Igarashi, "Construction of secret key exchange spanning trees by random deals of cards on hierarchical structures," IEICE Trans. Fundamentals, vol. E84-A, no. 5, pp. 1110–1119, 2001.
13. P. Winkler, "The advent of cryptology in the game of bridge," CRYPTOLOGIA, vol. 7, pp. 327–332, 1983.
14. R. N. Wright, "Achieving Perfect Secrecy Using Correlated Random Variables," PhD Thesis, Yale University, 1994.