Chapter 52
An Efficient Protocol for Unconditionally Secure Secret Key Exchange[*]

Michael J. Fischer[†] Rebecca N. Wright[†]

Abstract

The *multiparty secret key exchange* problem is to find a k-player protocol for generating an n-bit random key. At the end of the protocol, the key should be known to each player but remain completely secret from a computationally unlimited eavesdropper, Eve, who overhears all communication among the players. The players are initially dealt hands of cards of prespecified sizes from a deck of distinct cards; any remaining cards are given to Eve. Considered here is the case in which each player receives the same fraction β of the cards in the deck, for β in the interval $(0, 1/k]$. The efficiency of a secret key exchange protocol is measured by the smallest deck size d_0 for which the protocol is guaranteed of success. A secret key exchange protocol is presented with $d_0 = O(n(1/\beta)^{2.71})$. The best previous bound, by Fischer, Paterson, and Rackoff (1991), was super-polynomial in $1/\beta$ and only handled the special case of $k = 2$ and $n = 1$.

1 Introduction

The problem of multiparty secret key exchange is an important problem in cryptography. Consider, for example, a certain government agency that handles security of information on a "community of interest" basis. For each project within the agency, a group of people are chosen to work on the project. We call this group a team. Teams form and dissolve as various projects are started and completed. All communication regarding the project is intended to be shared with those on the team, and to be kept secret from those outside the team. However, the security of the various communication channels—the telephone, interoffice mail, electronic mail, and face-to-face communication—is not guaranteed. Hence, each team that forms would like to exchange a secret key, which it can then use as a part of some cryptographic protocol to securely send all further communication regarding the project. Another place where this problem may arise is in a distributed system, for example a computer network linking a corporation's headquarters and branch offices.

1.1 Secret Key Exchange More formally, we consider a multiparty protocol between a group of m players. The protocol of each player is publicly known, but each player is supplied with some initial private information before the protocol begins. The vector of initial values is chosen randomly from some known distribution, and in general the players' random initial values are correlated. In addition, each player has a private independent random source. At some point in time, a *team* of $k \geq 2$ players P_1 through P_k is selected. The remaining $(m - k)$ players are assumed to conspire against the team, possibly communicating among themselves via private channels. We treat them as a single computationally unlimited eavesdropper, Eve, who possesses the initial information of all of the conspirators and overhears all communication among the team members.

An n-bit sequence B is a *secret key* if it satisfies agreement, secrecy, and uniformity. *Agreement* is met if each team player knows B. *Secrecy* is met if the eavesdropper's probability of guessing B correctly is the same before and after hearing the communication between the team players. *Uniformity* requires that B has equal probability of being any one of the 2^n possible n-bit sequences. Once obtained, the key can then be used for a variety of cryptographic purposes, for example, as the key in private key cryptosystems (cf. [DH76]). We would like to know which distributions of private initial values allow any team that forms to obtain an n-bit secret key.

This framework is very general and admits the trivial solution in which each player is given *a priori* a secret key for each team to which the player might eventually belong. Any team that forms can use

[*] This research was supported in part by National Science Foundation grant IRI-9015570.

[†] Computer Science Department, Yale University.

the corresponding preassigned secret key, but since there is an exponential number of possible teams, the amount of initial information is exponential. Also, the structure of the initial random information is rather complicated. We desire instead correlated random variables that have a simple structure and a small amount of initial information. A familiar example of such correlated random variables is provided by ordinary card games in which players are dealt hands from a randomly shuffled deck of cards. By looking at her own cards, a player gains some information about the other players' hands. Namely, she learns a set of cards that appear in no other player's hand. Peter Winkler developed bidding conventions for the game of bridge whereby one player could send her partner secret information about her hand that was totally unrelated to the actual bid and completely undecipherable to the opponents, even though the protocol was known to them [Fli81, Win81a, Win81b, Win83]. Fischer, Paterson and Rackoff [FPR91] carried this idea further, using deals of cards for secret bit transmission between two players. We consider secret bit exchange protocols based on such card games in the remainder of this paper (see also [FW92]).

A *deck* D is a finite ordered set of elements called *cards*; a *hand* is a subset of D. A *signature*[1] $\xi = (h_1, h_2, \ldots, h_k; e)$, where $k, h_1, h_2, \ldots, h_k, e$ are nonnegative integers, describes the sizes of the players' hands. The deck is known to all players, as is the signature, but the actual cards in each player's hand are private to that player. In a *ξ-deal* $\delta = (H_1, H_2, \ldots, H_k; E)$, each team player P_i is given a hand H_i such that $H_i \subseteq D$ and $|H_i| = h_i$, and Eve is dealt a hand E such that $E \subseteq D$ and $e = |E| = d - \sum_{i=1}^{k} h_i$. The deal δ is *legal* if $H_1, H_2, \ldots, H_k, E$ partition D. If all k team players have the same hand size h in a signature, we write $(h^k; e)$. A protocol that always succeeds in obtaining a secret key at least n-bits long for all legal ξ-deals is said to *perform* n-bit secret key exchange for ξ. We also say such a protocol *works for* ξ.

1.2 Results We present a protocol, the transformation protocol, that performs n-bit secret key exchange for teams of two players who each receive a fixed fraction β of the cards, provided the deck is sufficiently large. We show how to use the transformation protocol to construct for any $n \geq 1$ and $k \geq 2$, a protocol that performs n-bit secret key exchange for teams of k players who each receive a fixed fraction β of the cards, again provided the deck is sufficiently large. Fischer, Paterson, and Rackoff [FPR91] exhibit a protocol that solves the two player case for $n = 1$, but their required deck size grows super-polynomially in $1/\beta$. Our protocol works for general n and arbitrarily large teams, and the required deck size is only $O(n(1/\beta)^{2.71})$.

The transformation protocol is presented in Section 2 and analyzed in Section 3. The analysis is based on a nontrivial potential argument and shows that the protocol works for ξ whenever the potential of ξ is sufficiently large.

Section 4 contains applications of the transformation protocol. We show that there is a function $d_0(n, \beta) = O(n(1/\beta)^{2.71})$ such that for any $n \geq 1$ and $0 < \beta \leq 1/k$, if $d \geq d_0(n, \beta)$ then the transformation protocol performs n-bit secret bit exchange for the $(\lfloor \beta d \rfloor, \lfloor \beta d \rfloor; d - 2\lfloor \beta d \rfloor)$. Second, we show a general reduction of the multiparty case to the two player case. Applying this reduction to the transformation protocol yields a protocol that performs n-bit secret key exchange for teams of arbitrary size k, where each team player receives fraction β of the cards, provided the deck is sufficiently large. The required deck size is again only $O(n(1/\beta)^{2.71})$. If we apply this to the case where the deck is initially divided evenly between m players, the deck size needed to guarantee that any team that forms will be able to obtain an n-bit secret key is $O(nm^{2.71})$.

1.3 Other Approaches The problem of secret key exchange has been considered by others in the context of public key cryptography (cf. [DH76, Mer78]). However, there are several problems with public key cryptography. First, even if, for example, one way permutations are assumed to exist, this may not be useful, for Impagliazzo and Rudich [IR89] provide evidence that most of the standard techniques in cryptography cannot be used to construct a secret key exchange protocol from a one way permutation. Second, public key cryptography is based on unproven assumptions about the computational difficulty of certain problems. Even if public key cryptography is based on a problem that is actually asymptotically hard, it is not at all clear how to choose a key size in order to get the desired security. In the setting of multiparty protocols, there are further complications. If player A wants to send a message secretly to all the other players, she can encrypt it using each player's public key and send the resulting encryptions. However, although each encryption by itself gives no useful information to an eavesdropper, all of the encryptions taken together may divulge some information about the message.

Our results are quite different in flavor from those

[1] This term is borrowed from algebra, and is not intended to have any connection to digital signatures.

of public key cryptography and avoid the problems mentioned above. They are not based on computational difficulty, for we place no computational limitations on our participants. In addition, we require that our protocols always work for a given signature, not just with high probability. Because we allow the eavesdropper to be computationally unlimited, standard cryptographic techniques based on computational difficulty cannot be used. Furthermore, techniques such as those used by Maurer [Mau91] will not work, since we require the key obtained to be *completely* secret from Eve and known *exactly* to all the team players, as prescribed by the secrecy and agreement conditions. In fact, a secret key exchange protocol is not possible in our model without the initial random values, for otherwise an eavesdropper could simulate any team player over all possible random choices and thereby learn B. Similarly, unless the initial random values are correlated, an eavesdropper can simulate any player over all random choices and all possible initial random values and learn B.

2 The Protocol

Consider a team of two players, Alice and Bob. Fix a signature $\xi = (a, b; d - a - b)$ and a deck D, and let Alice and Bob be dealt a random ξ-deal δ of D. A set of cards $S \subseteq D$ is called an *(s, i, j)-portion* (relative to δ) if $|S| = s$ and S contains exactly i cards from Alice's hand and exactly j cards from Bob's hand. The remaining $s - i - j$ cards belong to Eve. We sometimes refer to an $(s, 1, 1)$-portion as an s-portion, and to any (s, i, j)-portion simply as a portion. An (s, i, j)-portion is *useful* if $i, j \geq 1$.

An (s, i, j)-portion S is *opaque* if Eve does not know anything about the location of the cards in S that she does not hold, other than the information provided by the fact that S is an (s, i, j)-portion. More formally, given the information available to Eve, each arrangement of the $i + j$ cards in S that Eve does not hold, in which Alice holds i of these cards and Bob holds the remaining j cards, is equally probable.

A bit B is associated with any 2-portion K. Namely, $B = 0$ if Alice holds the smaller card in K and $B = 1$ if Alice holds the larger card in K. If K is opaque and Alice and Bob know K is a 2-portion, then B is a 1-bit secret key, since Eve considers Alice equally likely to hold either card and therefore considers it equally likely that $B = 0$ or $B = 1$.

Our protocol, called the *transformation protocol*, maintains a collection $\mathcal{C}$ of pairwise disjoint, useful, opaque portions. The portions in $\mathcal{C}$ are common knowledge to Alice, Bob, and Eve at all times. The deck D is a (d, a, b)-portion relative to δ since δ is a $(a, b; d - a - b)$-deal. The initial collection $\mathcal{C}_0$ contains the single portion D.

A step of the protocol modifies $\mathcal{C}$ by removing a set of one or more portions from $\mathcal{C}$ and then adding one or more new portions to $\mathcal{C}$ according to a rule called a *transformation*. A transformation is *applicable* to $\mathcal{C}$ if $\mathcal{C}$ contains portions satisfying the preconditions of the transformation. A collection $\mathcal{C}$ is *terminal* if no transformation is applicable to it.

A sequence $\mathcal{C}_0, \mathcal{C}_1, \mathcal{C}_2, \ldots$ of collections of portions is called a *trace* from $\mathcal{C}_0$ if for each $i \geq 1$, $\mathcal{C}_i$ can result from $\mathcal{C}_{i-1}$ by some transformation. A trace is *complete* if either it is infinite, or it is finite and the last collection in the sequence is terminal.

The protocol is to apply transformations to $\mathcal{C}$ until the resulting collection is terminal. Thus, a run of the transformation protocol generates a complete trace from the initial collection $\mathcal{C}_0$. We show in Section 3 that every trace from a finite collection is finite. Hence every run of the protocol terminates with some collection $\mathcal{C}$. Call the 2-portions in $\mathcal{C}$, in lexicographic order, $S_1, S_2, \ldots, S_n$. Each S_i provides a 1-bit secret key B_i as described above. The 1-bit secret keys are concatenated together to form a single n-bit secret key $B_1 B_2 \cdots B_n$.

The transformation protocol:

1. $\mathcal{C} = \{D\}$ is the initial collection.
2. While $\mathcal{C}$ is not terminal the following steps are repeated:
   (a) Alice randomly chooses an applicable transformation, and announces the transformation and the portions to which it applies.
   (b) The protocol specified below for the announced transformation is carried out.
3. The bits $B_1, \ldots, B_n$ provided by the 2-portions $S_1, \ldots, S_n$ (in lexicographic order) in $\mathcal{C}$ are concatenated together to form the output sequence $B_1 B_2 \cdots B_n$.

Note that if it is desirable to conserve communication and randomness, the transformation chosen in Step 2a can be chosen by any prearranged deterministic function of the public information.

The transformations are *splitting* and *combining*. Splitting replaces an (s, i, j)-portion in $\mathcal{C}$ with several smaller portions, each of which contains exactly one of Alice's cards if $i \geq j$, and exactly one of Bob's cards if $i < j$. Combining replaces two $(s, 1, 1)$-portions by a single $(s', 1, 1)$-portion for some $s' < s$.

Splitting: An (s, i, j)-portion S in $\mathcal{C}$ can be split if $i + j \geq 3$. If $i \geq j$, the splitting proceeds as described below. If $i < j$, the roles of Alice and Bob are reversed.

1. S is removed from $\mathcal{C}$.
2. Alice randomly partitions S into i sets, each of size $\lfloor s/i \rfloor$ or $\lceil s/i \rceil$, such that she holds exactly one card in each set, and announces the sets.[2]
3. Bob says how many cards he holds in each set announced by Alice.
4. Each set in which Bob holds at least one card is added to $\mathcal{C}$.

Combining: Two $(s,1,1)$-portions S_1 and S_2 can be combined if $s \geq 3$.

1. S_1 and S_2 are removed from $\mathcal{C}$.
2. Alice randomly chooses $p \in \{1,2\}$. Let $q = 3 - p$.
3. Alice constructs and announces a new set T consisting of her card from S_p, $\lfloor s/3 \rfloor - 1$ randomly chosen cards that are not hers from S_p, and $\lfloor s/3 \rfloor$ randomly chosen cards that are not hers from S_q.
4. Bob announces how many cards he holds in T.
   (a) If Bob holds no cards in T, then Alice announces the set difference $S_q - T$, which is added to $\mathcal{C}$.
   (b) If Bob holds one card in T, then T is added to $\mathcal{C}$.
   (c) If Bob holds two cards in T, then Alice announces $S_p \cap T$, which is added to $\mathcal{C}$.

LEMMA 2.1. *Let $\mathcal{C}$ be a collection of disjoint, useful, opaque portions, and let $\mathcal{C}'$ be an element in a trace from $\mathcal{C}$. Then $\mathcal{C}'$ is a collection of disjoint, useful, opaque portions.*

Proof. It suffices to show that each transformation preserves the disjointness, usefulness and opaqueness of the portions in a collection. Let $\mathcal{C}$ be a collection of disjoint, useful, opaque portions.

Suppose an (s,i,j)-portion S in $\mathcal{C}$ is split. Splitting preserves the disjointness property because S is removed and the new portions added are disjoint subsets of S. Each portion added to $\mathcal{C}$ is useful because, if $i \geq j$, then Alice holds exactly one card in each set she announces, and only those sets in which Bob holds at least one card are added. Similarly, if $i < j$, then Bob holds exactly one card and Alice holds at least one card in each portion added to $\mathcal{C}$. To see that splitting produces only opaque portions, suppose that $i \geq j$, and consider an $(s',1,j')$-portion S' that is added to $\mathcal{C}$. Since S is opaque and Alice randomly chose the partition for S among all partitions in which she holds one card in each subset, Alice's card is equally likely to be any of the $j'+1$ cards not held by Eve in S', given the communication that takes place.

Now consider the combining of two i-portions S_1 and S_2, resulting in the portion S'. Combining preserves the disjointness property because all the elements in S' are in either S_1 or S_2, both of which have been removed from $\mathcal{C}$. To see that S' is useful, we must consider the possible outcomes. Let p be as chosen by Alice in the process of combining, let $q = 3-p$, and let T be the new set constructed by Alice. Then Alice and Bob both hold one card in each of S_p and S_q, and in particular, Alice holds one card in $S_p \cap T$ and one card in $S_q - T$. If Bob holds no cards in T, Bob's card in S_q must lie in $S_q - T$. Therefore $S_q - T$, which is added to $\mathcal{C}$, is useful. If Bob holds one card in T, then T, which is added to $\mathcal{C}$, is useful. If Bob holds two cards in T, then one of them must lie in $S_p \cap T$ and one in $S_q \cap T$. Therefore $S_p \cap T$, which is added to $\mathcal{C}$, is useful.

To see that S' is opaque, suppose Alice holds card x_1 in S_1 and card x_2 in S_2, and Bob holds card y_1 in S_1 and card y_2 in S_2. Then the sequence of communication taking place during the combining, as well as the resulting set added to $\mathcal{C}$, is equally likely to occur in the symmetric deal where Alice holds y_1 and y_2 and Bob holds x_1 and x_2. ∎

3 Analysis

We use a "potential" argument to analyze how many 2-portions are produced by the transformation protocol. Given a collection $\mathcal{C}$ of useful portions, we define a quantity $\phi(\mathcal{C})$, called its *potential.* We show that if $\mathcal{C}'$ results from $\mathcal{C}$ by any transformation, then $\phi(\mathcal{C}') \geq \phi(\mathcal{C})$. Thus, if $\mathcal{C}'$ results from $\mathcal{C}$ via any sequence of transformations, then $\phi(\mathcal{C}') \geq \phi(\mathcal{C})$. Finally, we define a constant W, and we show that if $\phi(\mathcal{C}) > W + 2p$, where p is the number of 2-portions in $\mathcal{C}$, then at least one transformation is applicable to $\mathcal{C}$. It follows from the above claims that if $\mathcal{C}$ is terminal and $\phi(\mathcal{C}) > W + 2(n-1)$ then the number of 2-portions in $\mathcal{C}$ is at least n. Every trace from a finite collection of portions is finite, since each transformation reduces the difference between total size of all portions and the number of portions. Thus every run of the transformation protocol terminates, and if $a, b \geq 1$ and $d \geq a + b$, the transformation protocol performs $\lceil (\phi(\mathcal{C}_0) - W)/2 \rceil$-bit secret key exchange for $(a, b; d-a-b)$, where $\mathcal{C}_0$ is the initial collection. The remainder of this section defines $\phi(S)$ and proves the above claims.

The constant $c = \log_{3/2} 2 = 1/\log_2(3/2) < 1.7096$

[2] In an abstract setting, the sets $\{x,y\}$ and $\{y,x\}$ are equal. In an actual implementation, to prevent the communication of a set from revealing which cards came from Alice's hand, the set should be communicated in a canonical form.

is used throughout the analysis. Note that $(2/3)^{-c} = 2$ and $1 - 1/c > 0$. Given an (s,i,j)-portion S, we recursively define $\phi(S) = \phi(s,i,j) =$

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

Hence, $\phi(s,i,j)$ is symmetric in its last two arguments, and $\phi(s,1,1)$ is monotonically decreasing in s for all integers $s \geq 2$. We extend the potential function to collections $\mathcal{C}$ of useful portions by defining $\phi(\mathcal{C}) = \sum_{S \in \mathcal{C}} \phi(S)$.

FACT 3.1. *Let y, z be integers, $z \neq 0$. Then $\lceil y/z \rceil \leq (y-1)/z + 1$.*

Proof. We have $y = qz + r$ for integers q and r such that $0 < r \leq z$, so $\lceil y/z \rceil = q + 1 \leq q + (r-1)/z + 1 = (qz + r - 1)/z + 1 = (y-1)/z + 1$. ■

In analyzing the splitting transformation, we will need the following lemma relating the potential of an s-portion to the potential of a $\lceil s/b \rceil$-portion.

LEMMA 3.2. *Let b be an integer such that $1 \leq b \leq s-1$. Then $b\,\phi(s,1,1) \leq \phi(\lceil s/b \rceil, 1, 1)$.*

Proof. Let b be an integer such that $1 \leq b \leq s-1$. If $b = 1$, then trivially $b\,\phi(s,1,1) = \phi(\lceil s/b \rceil, 1, 1)$.

Otherwise, $2 \leq b \leq s-1$, and thus $\phi(s,1,1) = (s-2)^{-c}$ and $\lceil s/b \rceil \geq 2$. If $\lceil s/b \rceil = 2$ then

$$\begin{aligned} b\,\phi(s,1,1) &= b(s-2)^{-c} \\ &\leq (s-1)(s-2)^{-c} \\ &\leq 2(s-2)^{(1-c)} \\ &\leq 2 \\ &= \phi\left(\left\lceil \frac{s}{b} \right\rceil, 1, 1\right) \end{aligned}$$

as desired. Otherwise, $\lceil s/b \rceil \geq 3$, so

$$b\,\phi(s,1,1) = b(s-2)^{-c} \tag{3.1}$$
$$\phi(\lceil s/b \rceil, 1, 1) = (\lceil s/b \rceil - 2)^{-c} \tag{3.2}$$

Since $(1/c) - 1 < 0 < c$, we have $b^{(1/c)-1} < 1 < b^{1/c}$. Also $s - 1 > b$ since $\lceil s/b \rceil \geq 3$, so

$$\begin{aligned} b(s-2)^{-c} &= b((s-1)-1)^{-c} \\ &< b\left(b^{(1/c)-1}(s-1) - b^{1/c}\right)^{-c} \\ &= \left(\frac{s-1}{b} - 1\right)^{-c} \end{aligned} \tag{3.3}$$

By Fact 3.1,

$$\left(\frac{s-1}{b} - 1\right)^{-c} \leq \left(\left\lceil \frac{s}{b} \right\rceil - 2\right)^{-c} \tag{3.4}$$

Combining lines (3.1) through (3.4) yields the desired result. ■

LEMMA 3.3. *Suppose $\mathcal{C}'$ results from $\mathcal{C}$ by a splitting transformation. Then $\phi(\mathcal{C}') \geq \phi(\mathcal{C})$.*

Proof. It suffices to show that the potential of the portion to be split is no more than the total potential of the resulting portions. Let S be an (s,x,y)-portion, and suppose without loss of generality that $x \geq y$ (the case $x < y$ is symmetric). Let $S_1, S_2, \ldots, S_\ell$ be the portions added to $\mathcal{C}'$ as a result of splitting S, where S_i is an $(s_i, 1, b_i)$-portion.

Since each S_i was added to $\mathcal{C}'$, it follows that $1 \leq b_i \leq s_i - 1$ and $s_i \geq 2$. Also, $s_i \in \{\lfloor s/x \rfloor, \lceil s/x \rceil\}$, so $2 \leq s_i \leq \lceil s/x \rceil$. Thus, by the monotonicity of $\phi(s,1,1)$ and Lemma 3.2,

$$\begin{aligned} b_i\,\phi\left(\left\lceil \frac{s}{x} \right\rceil, 1, 1\right) &\leq b_i\,\phi(s_i, 1, 1) \\ &\leq \phi\left(\left\lceil \frac{s_i}{b_i} \right\rceil, 1, 1\right) \\ &= \phi(s_i, 1, b_i) \end{aligned}$$

Therefore,

$$\begin{aligned} \phi(S) &= \phi(s,x,y) \\ &= y\,\phi\left(\left\lceil \frac{s}{x} \right\rceil, 1, 1\right) \\ &= \sum_{i=1}^{\ell} b_i \phi\left(\left\lceil \frac{s}{x} \right\rceil, 1, 1\right) \\ &\leq \sum_{i=1}^{\ell} \phi(s_i, 1, b_i) \\ &= \sum_{i=1}^{\ell} \phi(S_i) \end{aligned}$$

as desired. ■

LEMMA 3.4. *Suppose $\mathcal{C}'$ results from $\mathcal{C}$ by a combining transformation. Then $\phi(\mathcal{C}') \geq \phi(\mathcal{C})$.*

Proof. As before, we need only compare the potential of the portions that are combined to the potential of the resulting portion.

Let S_1 and S_2 be s-portions, and suppose S' is an s'-portion resulting from combining S_1 and S_2. In order for combining to be possible, we must have $s \geq 3$. Hence $\phi(S_1) + \phi(S_2) = 2(s-2)^{-c} \leq 2$.

Let T be the new set constructed by Alice. Then $|T| = 2\lfloor s/3 \rfloor$. If Bob holds no cards in T, then an $(s - \lfloor s/3 \rfloor)$-portion is added to $\mathcal{C}$. If Bob holds one card in T, then a $(2\lfloor s/3 \rfloor)$-portion is added to $\mathcal{C}$. If Bob holds two cards in T, then a $(\lfloor s/3 \rfloor)$-portion is added to $\mathcal{C}$. In all cases, we have $s' \leq \lceil 2s/3 \rceil$.

If $s' = 2$, then $\phi(S') = 2$, so $\phi(S_1) + \phi(S_2) \le \phi(S')$, as desired. Otherwise, $2 < s' \le \lceil 2s/3 \rceil$. Using this and Fact 3.1, we have

$$\begin{aligned} \phi(S') &= (s'-2)^{-c} \\ &\ge (\lceil 2s/3 \rceil - 2)^{-c} \\ &\ge (2s/3 + 2/3 - 2)^{-c} \\ &= 2(s-2)^{-c} \\ &= \phi(S_1) + \phi(S_2) \end{aligned}$$

completing the proof. ■

Let $W = \sum_{s=3}^{\infty}(s-2)^{-c}$. Since $c > 1$, this series converges and W is finite. Numerical analysis shows that $2.0356 < W < 2.0358$. Given a collection $\mathcal{C}$, we define $\pi(\mathcal{C})$ to be the number of 2-portions in $\mathcal{C}$.

LEMMA 3.5. *If $\mathcal{C}$ is terminal, then $\phi(\mathcal{C}) \le W + 2\pi(\mathcal{C})$.*

Proof. Let $\mathcal{C}$ be a collection of portions such that $\phi(\mathcal{C}) > W + 2\pi(\mathcal{C})$. We show that $\mathcal{C}$ is not terminal. Since $\phi(\mathcal{C}) > 0$, $\mathcal{C}$ is nonempty. If $\mathcal{C}$ contains an (s,i,j)-portion such that $i + j \ge 3$, then splitting is possible. Otherwise, each portion S_i in $\mathcal{C}$ is an s_i-portion for some $s_i \ge 2$. In order to satisfy $\phi(\mathcal{C}) > W + 2\pi(\mathcal{C})$, it must be the case that there are two s-portions in $\mathcal{C}$ for some $s \ge 3$, since $W + 2\pi(\mathcal{C})$ is the potential of a collection containing $\pi(\mathcal{C})$ 2-portions and one s-portion for every $s \ge 3$. Thus combining can be applied. ■

LEMMA 3.6. *Let $\mathcal{C}$ be a finite collection of useful portions. Then every trace from $\mathcal{C}$ is finite.*

Proof. For any collection $\mathcal{C}$, let

$$M(\mathcal{C}) = \sum_{S \in \mathcal{C}}(|S| - 1) = \sum_{S \in \mathcal{C}} |S| - |\mathcal{C}|$$

Let $\mathcal{C}$ be a finite collection of useful portions, and suppose $\mathcal{C}'$ results from $\mathcal{C}$ by any transformation. By Lemma 2.1, all portions in $\mathcal{C}'$ are useful, so $M(\mathcal{C}) \ge 0$. If $M(\mathcal{C}) = 0$, then $\mathcal{C}$ is empty, and therefore no transformations can be applied to $\mathcal{C}$. Furthermore, $M(\mathcal{C}') < M(\mathcal{C})$. To see this, we consider splitting and combining separately.

Suppose $\mathcal{C}'$ results from $\mathcal{C}$ by a splitting transformation of an (s,i,j)-portion S with $i \ge j$. (The case $i < j$ is symmetric). Then $\sum_{S \in \mathcal{C}} |S| \ge \sum_{S \in \mathcal{C}'} |S|$ and $|\mathcal{C}| \le |\mathcal{C}'|$, since at least one set gets added. In order for S to be split, $i + j \ge 3$, so $i \ge 2$. Thus if $\sum_{S \in \mathcal{C}} |S| = \sum_{S \in \mathcal{C}'} |S|$, then $|\mathcal{C}| < |\mathcal{C}'|$, since in this case all $i \ge 2$ sets announced by Alice are added to $\mathcal{C}'$. Thus, $M(\mathcal{C}') < M(\mathcal{C})$.

If $\mathcal{C}'$ results from $\mathcal{C}$ by a combining transformation, then $|\mathcal{C}'| = |\mathcal{C}| - 1$. Also $\sum_{S \in \mathcal{C}'} |S| \le \sum_{S \in \mathcal{C}} |S| - 2$ since $\bigcup_{S \in \mathcal{C}} S - \bigcup_{S \in \mathcal{C}'} S$ contains one card from each of Alice's and Bob's hand. Thus $\sum_{S \in \mathcal{C}'} |S| - |\mathcal{C}'| \le \sum_{S \in \mathcal{C}} |S| - |\mathcal{C}| - 1$, and thus $M(\mathcal{C}') < M(\mathcal{C})$.

Hence, $M(\mathcal{C})$ is an upper bound on the length of any trace from $\mathcal{C}$. ■

LEMMA 3.7. *Let $\mathcal{C}$ be a terminal collection of useful portions. If $\phi(\mathcal{C}) > W + 2(n-1)$, then $\pi(\mathcal{C}) \ge n$.*

Proof. Let $\mathcal{C}$ be a terminal collection of useful portions such that $\phi(\mathcal{C}) > W + 2(n-1)$. Since $\mathcal{C}$ is terminal, Lemma 3.5 implies $\phi(\mathcal{C}) \le W + 2\pi(\mathcal{C})$. Thus $W + 2(n-1) < W + 2\pi(\mathcal{C})$, and hence $\pi(\mathcal{C}) > n - 1$, so $\pi(\mathcal{C}) \ge n$. ■

THEOREM 3.8. *Let $a, b \ge 1$, $d \ge a+b$, and $\phi(d,a,b) > W + 2(n-1)$. Then the transformation protocol performs n-bit secret key exchange for $(a, b; d-a-b)$.*

Proof. Assume the conditions of the theorem. Consider a run of the transformation protocol on a random $(a, b; d-a-b)$-deal. The initial collection $\mathcal{C}_0$ contains a single (d,a,b)-portion S. Thus $\phi(\mathcal{C}_0) = \phi(d,a,b) > W + 2(n-1)$. Since $a, b \ge 1$, S is useful. S is opaque because the deal is random. By Lemma 3.6, the run terminates with some terminal collection $\mathcal{C}'$. By Lemmas 3.3 and 3.4, $\phi(\mathcal{C}') \ge \phi(\mathcal{C}_0)$. Thus $\phi(\mathcal{C}') > W + 2(n-1)$. By Lemma 2.1, $\mathcal{C}'$ is a collection of disjoint, useful, opaque portions. Hence by Lemma 3.7, $\pi(\mathcal{C}') \ge n$. Since, in particular, all the 2-portions in $\mathcal{C}'$ are opaque, the output sequence is a secret key of length at least n. ■

COROLLARY 3.9. *Let $a, b \ge 1$, $d \ge a + b$ and $n = \lceil (\phi(d,a,b) - W)/2 \rceil$. Then the transformation protocol performs n-bit secret key exchange for $(a, b; d-a-b)$.*

Proof. Assume the conditions of the corollary and let $\phi_0 = \phi(d,a,b)$. Then $n = \lceil (\phi_0 - W)/2 \rceil$. By Fact 3.1, $n \le (\phi_0 - W + 1)/2$. Thus $W + 2(n-1) \le \phi_0 - 1 < \phi_0$. Hence by Theorem 3.8, the transformation protocol performs n-bit secret key exchange, as desired. ■

4 Applications

In this section, we present two applications of the transformation protocol. The first obtains a much improved bound for a problem studied in [FPR91] in which each player holds a constant fraction of the cards. The second uses the transformation protocol as a building block for constructing a multiparty secret key exchange protocol.

4.1 Two Players Each Holding a Fraction of the Cards

We consider the situation in which each of two players receives a constant fraction β of the cards in the deck, and the remainder go to Eve. This situation arises naturally with $\beta = 1/m$, for example, in protocols where the deck is dealt out evenly to m players. We are interested in how large the deck must be in order for the transformation protocol to work in this situation. We use the following in our analysis.

FACT 4.1. *Let x be a positive integer and β be any real number such that $\beta x \geq 1$. Then $\lceil x/\lfloor \beta x \rfloor \rceil < 2/\beta + 1$.*

Proof. Let $\ell = \lfloor \beta x \rfloor$. Then $1 \leq \ell \leq \beta x < \ell + 1$, so $x < (\ell + 1)/\beta$ and $(\ell + 1)/\ell \leq 2$. Thus $x/\ell \leq (\ell+1)/(\beta\ell) \leq 2/\beta$. It follows that $\lceil x/\lfloor \beta x \rfloor \rceil = \lceil x/\ell \rceil \leq \lceil 2/\beta \rceil < 2/\beta + 1$. ■

The following shows that the transformation protocol performs arbitrary n-bit secret key exchange for two players each holding a fraction β of the cards if the deck is sufficiently large. The required deck size is only $O(n(1/\beta)^{(c+1)})$, which is polynomial in $1/\beta$ and linear in n. Recall that $c = \log_{3/2} 2$ and $W = \sum_{s=3}^{\infty}(s-2)^{-c}$, and let $c_1 = 2^{(c+1)} < 6.5411$ and $c_2 = (W-2)/2 + 2^{-c}/c_1$. Calculation shows that $0.0645 < c_2 < 0.0647$.

THEOREM 4.2. *Let $0 < \beta \leq 1/2$, $n \geq 1$, and suppose that $d \geq c_1(1/\beta)^{(c+1)}(n+c_2)$. Then the transformation protocol performs n-bit secret key exchange for $\xi = (\lfloor \beta d \rfloor, \lfloor \beta d \rfloor; d - 2\lfloor \beta d \rfloor)$.*

Proof. Let β, d, and ξ satisfy the conditions of the theorem. By Theorem 3.8, it suffices to show that $\lfloor \beta d \rfloor \geq 1$, $d \geq 2\lfloor \beta d \rfloor$ and $\phi(d, \lfloor \beta d \rfloor, \lfloor \beta d \rfloor) > W + 2(n-1)$.

Since $\beta \leq 1/2$, it follows that $2\lfloor \beta d \rfloor \leq 2\beta d \leq d$, as desired. Furthermore, $(2\beta)^{-c} \geq 1$ and $2/\beta \geq 4$. Since $n + c_2 \geq 1$, using the bound on d and the definition of c_1 gives

$$\begin{aligned}\beta d &\geq c_1\beta^{-c}(n+c_2)\\ &\geq 2\left(\frac{2}{\beta}\right)^{c}\\ &\geq 8\end{aligned}$$

So $\lfloor \beta d \rfloor \geq 1$, as desired.

We now establish that $\phi(d, \lfloor \beta d \rfloor, \lfloor \beta d \rfloor) > W + 2(n-1)$. We begin by examining $\phi(\lceil d/\lfloor \beta d \rfloor \rceil, 1, 1)$. Note that we have $\lceil d/\lfloor \beta d \rfloor \rceil \geq d/\beta d = 1/\beta \geq 2$. If $\lceil d/\lfloor \beta d \rfloor \rceil = 2$, then $\phi(\lceil d/\lfloor \beta d \rfloor \rceil, 1, 1) = 2 > 1 > 3^{-c} \geq (2/\beta - 1)^{-c}$. If $\lceil d/\lfloor \beta d \rfloor \rceil > 2$, then

$$\begin{aligned}\phi(\lceil d/\lfloor \beta d \rfloor \rceil, 1, 1) &= (\lceil d/\lfloor \beta d \rfloor \rceil - 2)^{-c}\\ &> (2/\beta - 1)^{-c}\end{aligned}$$

by Fact 4.1. Hence, in either case, $\phi(\lceil d/\lfloor \beta d \rfloor \rceil, 1, 1) > (2/\beta - 1)^{-c}$. Thus

$$\begin{aligned}\phi(d, \lfloor \beta d \rfloor, \lfloor \beta d \rfloor) &= \lfloor \beta d \rfloor \phi(\lceil d/\lfloor \beta d \rfloor \rceil, 1, 1)\\ &> (\beta d - 1)(2/\beta - 1)^{-c} \qquad (4.5)\end{aligned}$$

Using the bound on d and the definitions of c_1 and c_2, we get

$$\begin{aligned}\beta d - 1 &\geq c_1\beta^{-c}(n + c_2) - 1\\ &= c_1\beta^{-c}\left(n + \frac{W-2}{2} + \frac{2^{-c}}{c_1}\right) - 1\\ &\geq c_1\beta^{-c}\left(n + \frac{W-2}{2}\right)\\ &= (2/\beta)^c(W + 2(n-1)) \qquad (4.6)\end{aligned}$$

Combining lines (4.5) and (4.6) yields

$$\begin{aligned}\phi(d, \lfloor \beta d \rfloor, \lfloor \beta d \rfloor) &> \left(\frac{2/\beta}{2/\beta - 1}\right)^{c}(W + 2(n-1))\\ &> W + 2(n-1)\end{aligned}$$

Hence, by Theorem 3.8, the transformation protocol performs n-bit secret key exchange for ξ. ■

It was shown in [FPR91] that secret bit transmission is possible for two players each holding a fraction β of the cards, but the minimum deck size for the protocol to work is super-polynomial in $1/\beta$. From Theorem 4.2 with $n = 1$, it follows that the transformation protocol can be used to solve this problem with a minimum deck size that is only $O((1/\beta)^{(c+1)})$.

4.2 Multiparty Secret Key Exchange We reduce the problem of multiparty n-bit secret key exchange to the problem of 2-party n-bit secret key exchange by showing how to use an arbitrary protocol $\mathcal{P}$ for the signature $\xi = (a, b; d - a - b)$ to construct a protocol $\mathcal{P}^*$ for the signature $\xi^* = (h_1, \ldots, h_k; d - \sum h_i)$, where each h_i must be sufficiently large. The construction has the property that if $\mathcal{P}$ performs n-bit secret key exchange for ξ, then $\mathcal{P}^*$ performs n-bit secret key exchange for ξ^*. A similar construction appears in [FW92]. Applying this construction to the 2-player transformation protocol yields an efficient multiparty n-bit secret key exchange protocol.

The main idea of this construction is that a subset of a team can sometimes carry out a protocol $\mathcal{P}$, designed for signature ξ, when the actual signature is ξ^*. Let $\xi = (h_1, \ldots, h_k; d - \sum h_i)$ and $\xi^* = (h_1^*, \ldots, h_{k^*}^*; d - \sum h_i^*)$. The construction works if there is an injection $\sigma : \{1, \ldots, k\} \to \{1, \ldots, k^*\}$ with the property that $h_i \leq h_{\sigma(i)}^*$, for $1 \leq i \leq k$. Player $P_{\sigma(i)}$ in $\mathcal{P}^*$ plays the role of player P_i in $\mathcal{P}$, using a randomly chosen subset H_i of size h_i from her real hand $H_{\sigma(i)}^*$. When carrying out $\mathcal{P}$, she pretends that she holds only the cards in H_i. Players P_j for j not in the range of σ do not participate. Thus, $\mathcal{P}$ runs just as it would for a ξ-deal, and Eve learns nothing in $\mathcal{P}^*$ about the locations of any cards not in the simulated hands of

$\mathcal{P}$, allowing those cards to be used later to carry out another protocol.

THEOREM 4.3. *Let $n \geq 1$ and $k \geq 2$, and let $\xi = (a, b; d-a-b)$ and $\xi^* = (h_1, \ldots, h_k; d - \sum h_i)$ such that $h_1 \geq a$, $h_k \geq b$, and $h_i \geq a + b$ for all $2 \leq i \leq k-1$, and let $\mathcal{P}$ be a protocol that performs n-bit secret key exchange for ξ. Then there is a protocol $\mathcal{P}^*$ that performs n-bit secret key exchange for ξ^*.*

Proof. Assume the conditions of the theorem. We construct a new protocol $\mathcal{P}^*$ to perform n-bit, k-player secret key exchange. Each team player P_i for $1 \leq i \leq k-1$ randomly chooses a subset H_i^a containing a of her cards. Each team player P_i for $2 \leq i \leq k$ randomly chooses a subset H_i^b containing b of her cards not in H_i^a.

$\mathcal{P}^*$ uses protocol $\mathcal{P}$ a total of $k-1$ times. In the i^{th} use, neighbors P_i and P_{i+1} become the *active* players and participate to establish an n-bit secret key X_i that they share. Player P_i uses H_i^a as her hand to play the role of Alice in $\mathcal{P}$. Player P_{i+1} uses H_{i+1}^b as her hand to play the role of Bob in $\mathcal{P}$. The other players do not participate. We call $H_i^a \cap H_{i+1}^b$ the *current cards.* During each use of $\mathcal{P}$, all team players behave as if Eve holds all the cards except the current cards. Thus, Eve may learn, for example, that a card x is held by a non-active player, but she learns nothing about which non-active player holds x. Thus it is possible to use $\mathcal{P}$ again with different active players, provided that the new set of current cards is distinct from all previous such sets.

After the $k-1$ uses of $\mathcal{P}$ are completed, player P_1 becomes the leader and randomly chooses an n-bit string B to be the team's secret key. The team transmits B secretly from player to player as follows until the whole team knows B. When P_i learns B, she sends $E_i = B \oplus X_i$ to P_{i+1} publicly. P_{i+1} recovers B by computing $E_i \oplus X_i$. In this way, all players learn B while releasing no information about B to Eve. Hence, $\mathcal{P}^*$ performs n-bit secret key exchange for ξ^*. ■

We can apply Theorem 4.3 to the transformation protocol to obtain an n-bit, k-player secret key exchange protocol that requires the deck size to be only linear in n and polynomial in $1/\alpha$, where α is the fraction of the deck held by each team player. Recall that $c_1 = 2^{(c+1)}$ and $c_2 = (W-2)/2 + 2^{-c}/c_1$.

COROLLARY 4.4. *Let $k \geq 2$, $0 < \alpha \leq 1/k$, and suppose that $d \geq c_1(2/\alpha)^{(c+1)}(n+c_2)$. Then there is an n-bit secret key exchange protocol for $\xi^* = (\lfloor \alpha d \rfloor^k; d - k\lfloor \alpha d \rfloor)$.*

Proof. Let α and d satisfy the conditions of the corollary, and let $\beta = \alpha/2$. By Theorem 4.2, the transformation protocol performs n-bit secret key exchange for $(\lfloor \beta d \rfloor, \lfloor \beta d \rfloor; d - 2\lfloor \beta d \rfloor)$. Since $2\lfloor \beta d \rfloor \leq \lfloor \alpha d \rfloor$, the conditions of Theorem 4.3 are satisfied, and hence there is a protocol that performs n-bit secret key exchange for ξ^*. ■

COROLLARY 4.5. *Assume $m \geq 2$ divides d, and let each of m players be dealt hands of size d/m from a deck of size $d \geq c_1(2m)^{(c+1)}(n+c_2)$. Then for any team of size $2 \leq k \leq m$ that forms, there is a protocol that establishes an n-bit secret key for the team.*

5 Conclusions

We have developed and analyzed the new transformation protocol for secret key exchange using deals of cards. The protocol maintains a dynamically changing collection of portions. It is analyzed using a nontrivial potential argument.

The transformation protocol is almost efficient enough to have practical applications. For example, consider the dynamic case of m players dealt hands of equal size. The initial deal of cards could be performed in a centralized, secure environment, and the hands of the players written to m portable mass storage media such as optical disks, one for each player. After the disks have been distributed, any subset of players can form a team and use the protocol to obtain a secret key. For $m = 100$ and $n = 1000$, Theorem 4.2 shows that a deck of size about 1.1×10^{10} is sufficient. Each of the 100 hands can be encoded using roughly 10^8 bytes (for example, by storing the differences between successive cards in the hand instead of absolute card values). Storing 100 Megabytes on an optical disk is easily within the capabilities of today's technology.

Naive implementation of our protocol requires a large number of rounds of communication, but many transformations can be applied in parallel, greatly increasing its efficiency.

6 Acknowledgements

We thank Richard Beigel for his suggestion leading to the development of the transformation protocol, and we thank Michael Merritt for suggesting the idea of dividing hands used in the proof of Theorem 4.3.

References

[DH76] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. Inform. Theory*, IT–22,(6):644–654, November 1976.

[Fli81] J. Flint. Cheating by degrees. *The Times Saturday Review*, May 9, 1981.

[FPR91] M. J. Fischer, M. S. Paterson, and C. Rackoff. Secret bit transmission using a random deal of cards.

In *Distributed Computing and Cryptography*, pages 173–181. American Mathematical Society, 1991.

[FW92] M. J. Fischer and R. Wright. Multiparty secret key exchange using a random deal of cards. In *Proceedings of Crypto '91*, volume 576 of *LNCS*, pages 141–155. Springer-Verlag, 1992.

[IR89] R. Impagliazzo and S. Rudich. Limits on the provable consequences of one-way permutations. In *Proc. 21st ACM Symposium on Theory of Computing*, pages 44–61, May 1989.

[Mau91] U. M. Maurer. Perfect cryptographic security from partially independent channels. In *Proc. 23rd ACM Symposium on Theory of Computing*, pages 561–571, May 1991.

[Mer78] R. C. Merkle. Secure communication over insecure channels. *Comm. ACM*, 21(4):294–299, April 1978.

[Win81a] P. Winkler. Cryptologic techniques in bidding and defense: Parts I, II, III, and IV. *Bridge Magazine*, April–July 1981.

[Win81b] P. Winkler. My night at the Cryppie club. *Bridge Magazine*, pages 60–63, August 1981.

[Win83] P. Winkler. The advent of cryptology in the game of bridge. *Cryptologia*, 7(4):327–332, October 1983.