Yale University
Department of Computer Science

An Efficient Protocol for Unconditionally Secure Secret Key Exchange[1]

Michael J. Fischer Rebecca N. Wright

YALEU/DCS/TR-908
May 1992

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

An Efficient Protocol for Unconditionally Secure Secret Key Exchange*

Michael J. Fischer Rebecca N. Wright

Computer Science Department
Yale University
New Haven, CT 06520–2158

May 1992

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

*This research was supported in part by National Science Foundation grant IRI–9015570.

initial values are correlated. In addition, each player has a private source of independent random bits. 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 secret key is an n-bit sequence S satisfying agreement, secrecy, and uniformity. *Agreement* is met if each team player knows S. *Secrecy* is met if the eavesdropper's probability of guessing S correctly is the same before and after hearing the communication between the team players. *Uniformity* requires that S 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 the corresponding preassigned secret key, but since there is an exponential number of possible teams, the amount of initial information is quite high. 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]).

We use the following terminology. A *deck* is a finite set of d *cards*; a *hand* is a subset of the deck. Each player, including Eve, is dealt a hand of cards. The deck is known to all of the players, as is the size of each player's hand, but the actual cards in each player's hand are private to that player. In an $(h_1, h_2, \ldots, h_k; e)$-*deal*, each team player P_i is given a hand H_i from a deck D of size $\sum h_i + e$, such that $H_i \subseteq D$ and $|H_i| = h_i$. The hands are pairwise disjoint, and Eve is dealt the remaining e cards. We call the description of the sizes of the hands, $\xi = (h_1, h_2, \ldots, h_k; e)$, the *signature*[1] of the deal. If all k team players have the same hand size h in a signature, we write $(h^k; e)$. An n-bit secret key exchange protocol that always succeeds in obtaining an n-bit secret key for all legal ξ-deals is said to *work for* ξ. We also say such a protocol *performs* n-bit secret key exchange for ξ.

1.2 Results

In Section 2, 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. Fischer, Paterson, and Rackoff [FPR91] exhibit a protocol that solves this case for $n = 1$, but their required

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

deck size grows super-polynomially in $1/\beta$. Our protocol works for general n, and the required deck size is only $O(n(1/\beta)^{2.71})$. In Section 3, we analyze the transformation protocol. The analysis is based on a nontrivial entropy argument.

In Section 4, we derive applications of the transformation protocol. First, we apply the transformation protocol to the case where each of two players holds a constant fraction β of the deck and we show that the required deck size for the protocol to work for n-bit secret key exchange is $O(n(1/\beta)^{2.71})$. 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. A further problem is that of authentication.

Our results are quite different in flavor from those of public key cryptography, and avoid some of the problems mentioned above. Our results 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 an eavesdropper could then simulate any team player under all possible random choices and thereby learn S. We have not addressed the problem of authentication at this time.

2 The Protocol

Consider a team of size two, and call the two team players Alice and Bob. A set of cards S is called an (s,i,j)*-portion* if $i \geq 1$, $j \geq 1$, $s \geq i+j$, $|S| = s$, S contains exactly i cards from Alice's hand, and S contains exactly j cards from Bob's hand. The remaining $s-(i+j)$ cards belong to Eve. We say that s is the *size* of S, and we define the function size$(S) = s$. We sometimes refer to an $(s,1,1)$-portion simply as an s-portion, and to any (s,i,j)-portion simply as a portion. Throughout the remainder of the paper, it is assumed whenever we refer to an (s,i,j)-portion that s, i, and j are nonnegative integers such that $s \geq i+j$.

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.

If Alice and Bob know an opaque 2-portion $K = \{x,y\}$, they can use it to obtain a 1-bit secret key S. Namely, Alice chooses randomly to say either "$S=0$ if I hold x" or "$S=0$ if I hold y". Alice and Bob each know the location of the cards x and y, so they both know S. Eve considers Alice equally likely to hold either card, so she has no added advantage in guessing S.

Fix a signature $(a,b;d-(a+b))$. Our protocol, called the *transformation protocol*, maintains a collection $\mathcal{C}$ of pairwise disjoint opaque portions. The portions in $\mathcal{C}$ are common knowledge to Alice, Bob, and Eve at all times. $\mathcal{C}$ initially contains a single portion which is the entire deck, a (d,a,b)-portion. There are three types of transformations possible on the collection $\mathcal{C}$, described below. The protocol eventually obtains n opaque 2-portions, each of which is then used to obtain a 1-bit secret key as described above. The 1-bit secret keys are concatenated together to form a single n-bit secret key. The protocol is simply: while a transformation is possible on $\mathcal{C}$, apply some transformation, until n 2-portions have been obtained. If more than one transformation applies, Alice randomly chooses which to apply.

The transformations are *splitting*, *combining*, and *removal*. 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 otherwise. Combining replaces two $(s,1,1)$-portions by a single $(s',1,1)$-portion for some $s' < s$. Removal removes a $(2,1,1)$-portion from $\mathcal{C}$.

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 $j > i$, 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 announces how many cards he holds in each set announced by Alice.
4. Each set in which Bob holds no cards is discarded.
5. Each set in which Bob holds at least one card is added to $\mathcal{C}$.

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

1. S_1 and S_2 are removed from $\mathcal{C}$.
2. Alice randomly labels S_1 and S_2 with the labels P and Q.
3. Alice constructs and announces a new set R consisting of her card from P, $\lfloor s/3 \rfloor - 1$ randomly chosen cards that are not hers from P, and $\lfloor s/3 \rfloor$ randomly chosen cards that are not hers from Q.
4. Bob announces how many cards he holds in R.
   (a) If Bob holds no cards in R, then Alice announces $Q-R$, which is added to $\mathcal{C}$ (where $Q-R$ denotes set difference).

[2] In an abstract setting, $\{x,y\}$ is clearly the same as $\{y,x\}$. In an actual implementation, care must be taken that the communication of a set does not reveal which cards came from Alice's hand.

(b) If Bob holds one card in R, then R is added to $\mathcal{C}$.

(c) If Bob holds two cards in R, then Alice announces $R \cap P$, which is added to $\mathcal{C}$.

Removal: An (s, i, j)-portion S can be removed if $i = j = 1$ and $s = 2$.

1. S is removed from $\mathcal{C}$.

Theorem 2.1 *If the transformation protocol obtains n 2-portions, it performs n-bit secret key exchange.*

Proof: It suffices to show that at all times, all the portions in $\mathcal{C}$ are opaque. This is initially true since the original deal is a random $(a, b; d - (a + b))$-deal. Furthermore, each transformation adds only opaque portions to $\mathcal{C}$. Splitting produces only opaque portions because the players choose the partitions randomly. To see that the portion added to $\mathcal{C}$ as a result of combining is opaque, consider the combining of two i-portions S and S'. Suppose Alice holds card x in S and card x' in S', and Bob holds card y in S and card y' in S'. 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 and y' and Bob holds x and x'. Hence the protocol is partially correct. ■

3 Analysis

We use an "entropy" argument to determine sufficient conditions to guarantee that the transformation protocol can continue until n 2-portions are produced. Given a portion S, we define a quantity $E(S)$, called its *entropy*. For a collection $\mathcal{C}$, we define $E(\mathcal{C}) = \sum_{S \in \mathcal{C}} E(S)$. We show that if $\mathcal{C}'$ results from $\mathcal{C}$ by a splitting or combining transformation, then $E(\mathcal{C}') \geq E(\mathcal{C})$, and if $\mathcal{C}'$ results from $\mathcal{C}$ via a removal transformation, then $E(\mathcal{C}') = E(\mathcal{C}) - 2$. Thus, if $\mathcal{C}'$ results $\mathcal{C}$ via any sequence of transformations, exactly ℓ of which are removal transformations, then $E(\mathcal{C}') \geq E(\mathcal{C}) - 2\ell$. Finally, we define a constant W and show that if $E(\mathcal{C}) > W$, then at least one transformation is applicable to $\mathcal{C}$. No infinite sequence of transformations can be applied to any finite collection of portions, since each transformation reduces the difference between total size of all portions and the number of portions. It follows that if $\mathcal{C}$ initially contains a single (d, a, b)-portion S and $E(S) > W + 2(n - 1)$, then the transformation protocol will eventually terminate after having obtained n 2-portions, for until that time, any collection $\mathcal{C}'$ produced must have $E(\mathcal{C}') > W$, so some transformation can be applied and the protocol can continue. The remainder of this section defines $E(S)$ and proves the above claims.

The constant $c = \log_{3/2} 2 = 1/\log_2(3/2) < 1.7096$ is used throughout the analysis. Given an (s, i, j)-portion S, we recursively define $E(S) = E(s, i, j) =$

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

Hence, $E(s, i, j)$ is symmetric in its last two arguments, and $E(s, 1, 1)$ is monotonically decreasing in s for all integers $s \geq 2$.

We will need the following simple fact.

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

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

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

Lemma 3.1 *Let b be an integer such that $1 \leq b \leq s-1$. Then*

$$b\,E(s,1,1) \leq E(\lceil s/b \rceil, 1, 1).$$

Proof: Let b be an integer such that $1 \leq b \leq s-1$. If $b=1$, then $b\,E(s,1,1) = E(\lceil s/b \rceil, 1, 1)$. Otherwise, $2 \leq b \leq s-1$, and thus $\lceil s/b \rceil \geq 2$. If $\lceil s/b \rceil = 2$ then

$$\begin{aligned} b\,E(s,1,1) &= b(s-2)^{-c} \\ &\leq (s-1)(s-2)^{-c} \\ &\leq 2(s-2)^{(1-c)} \\ &\leq 2 \\ &= E(\lceil s/b \rceil, 1, 1) \end{aligned}$$

If $\lceil s/b \rceil > 2$, then $E(\lceil s/b \rceil, 1, 1) = (\lceil s/b \rceil - 2)^{-c}$. Since $b \geq 2$ and $1 - 1/c > 0$, we have $1/(b^{(1-1/c)}) < 1$. Also, calculus shows that $2 < b^{1/c}(1 + 1/b)$ for all $b \geq 2$. Hence,

$$s/(b^{(1-1/c)}) + 2 < s + b^{1/c}(1+1/b)$$

so $b^{1/c}(s/b + (b-1)/b - 2) < s - 2$. By Fact 1,

$$\lceil s/b \rceil - 2 \leq (s/b + (b-1)/b - 2)$$

Therefore, $b^{1/c}(1/(s-2)) < 1/(\lceil s/b \rceil - 2)$. Raising both sides to the c^{th} power yields the desired result. ■

Lemma 3.2 *Suppose C' results from C by a splitting transformation. Then $E(C') \geq E(C)$.*

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

Then $s_i \in \{\lfloor s/x \rfloor, \lceil s/x \rceil\}$, so $2 \leq s_i \leq \lceil s/x \rceil$. Thus,

$$\begin{aligned} b_i\,E(\lceil s/x \rceil, 1, 1) &\leq b_i\,E(s_i, 1, 1) && (1) \\ &\leq E(\lceil s_i/b_i \rceil, 1, 1) && (2) \\ &= E(s_i, 1, b_i) && (3) \end{aligned}$$

where (1) is by the monotonicity of $E(s,1,1)$, (2) is by Lemma 3.1, and (3) is by the definition of $E(\cdot)$.

Therefore,

$$\begin{aligned} E(s,x,y) &= y\,E(\lceil s/x \rceil, 1, 1) \\ &= \sum_i b_i E(\lceil s/x \rceil, 1, 1) \\ &\leq \sum_i E(s_i, 1, b_i) \end{aligned}$$

as desired. ■

Lemma 3.3 *Suppose C' results from C by a combining transformation. Then $E(C') \geq E(C)$.*

Proof: As before, we need only compare the entropy of the portions that are combined to the entropy 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 $E(S_1) + E(S_2) = 2/(s-2)^c \leq 2$.

Let R be the new set constructed by Alice. Then $|R| = 2\lfloor s/3 \rfloor$. If Bob holds no cards in R, then an $(s - \lfloor s/3 \rfloor)$-portion is added to C. If Bob holds one card in R, then a $(2\lfloor s/3 \rfloor)$-portion is added to C. If Bob holds two cards in R, then a $(\lfloor s/3 \rfloor)$-portion is added to C. (Note that it is not possible for Bob to hold more than two cards in R.) In all cases, we have $s' \leq \lceil 2s/3 \rceil$.

If $s' = 2$, then $E(S') = 2$, so $E(S_1) + E(S_2) \leq E(S')$, as desired. Otherwise, $s' > 2$, so $E(S') = (s'-2)^{-c} \geq (\lceil 2s/3 \rceil - 2)^{-c} \geq (2s/3 + 2/3 - 2)^{-c}$, by Fact 1. Thus we have

$$\begin{aligned} E(S') &\geq (2s/3 + 2/3 - 2)^{-c} \\ &= (2/3)^{-c}(s-2)^{-c} \\ &= 2/(s-2)^c \\ &= E(S_1) + E(S_2) \end{aligned}$$

completing the proof. ■

Lemma 3.4 *Suppose C' results from C by a removal transformation. Then $E(C') = E(C) - 2$.*

Proof: Removal can only be applied to a $(2,1,1)$-portion. Hence the entropy of a removed portion is 2. ■

Let $W = \sum_{s=3}^{\infty} 1/(s-2)^c$. Since $c > 1$, this series converges and W is finite. Calculus shows that $W \leq c/(c-1) < 2.4095$.

Lemma 3.5 *If $E(\mathcal{C}) > W$, then some transformation is possible.*

Proof: Let $\mathcal{C}$ be a collection of portions such that $E(\mathcal{C}) > W$. Since $E(\mathcal{C}) > 0, \mathcal{C}$ is nonempty. If $\mathcal{C}$ contains a 2-portion, then removal is possible. If $\mathcal{C}$ contains an (s,i,j)-portion such that $i+j \geq 3$, then splitting is possible. Otherwise, each portion S_i in $\mathcal{C}$ is an s_i-portion for some $s_i \geq 3$. Then in order to satisfy $E(\mathcal{C}) > W$, it must be the case that there are two s-portions in $\mathcal{C}$ for some s, since W is the entropy of a collection containing one s-portion for every $s \geq 3$. Thus combining can be applied. ■

Lemma 3.6 *Let $\mathcal{C}$ be a finite collection of portions. No infinite sequence of transformations is applicable to $\mathcal{C}$.*

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

$$M(\mathcal{C}) = \left(\sum_{S \in \mathcal{C}} \text{size}(S) \right) - |\mathcal{C}|$$

Since all portions we consider have size at least 2, $M(\mathcal{C}) \geq 0$. If $\mathcal{C}'$ results from $\mathcal{C}$ by any transformation, then $M(\mathcal{C}') < M(\mathcal{C})$. Hence, $M(\mathcal{C})$ is an upper bound on the number of transformations that can be applied to $\mathcal{C}$ before the collection becomes empty. Thus no infinite sequence of transformations can be applied to any finite collection $\mathcal{C}$. ■

Theorem 3.7 *If $E(\mathcal{C}) > W+2(n-1)$, then the transformation protocol succeeds on $\mathcal{C}$ to produce n 2-portions.*

Proof: We show as an induction hypothesis that for any collection $\mathcal{C}$ and any sequence γ of applicable transformations, if $\mathcal{C}'$ results from $\mathcal{C}$ by γ, then $E(\mathcal{C}') \geq E(\mathcal{C}) - 2r(\gamma)$, where $r(\gamma)$ is the number of removal transformations in γ.

Proof is by induction on $|\gamma|$. The base case is obvious. Let $|\gamma| \geq 1$ and assume the induction hypothesis holds for all γ' such that $|\gamma'| < |\gamma|$. Write $\gamma = \gamma'\tau$, where τ is a transformation. Let $\mathcal{C}_0$ result from $\mathcal{C}$ by γ'. By the induction hypothesis, $E(\mathcal{C}_0) \geq E(\mathcal{C}) - 2r(\gamma')$. If τ is a splitting or combining transformation, then $r(\gamma) = r(\gamma')$, and $E(\mathcal{C}') \geq E(\mathcal{C}_0) \geq E(\mathcal{C}) - 2r(\gamma)$ by Lemmas 3.2 and 3.3. If τ is a removal transformation, then $r(\gamma) = r(\gamma') + 1$, and $E(\mathcal{C}') = E(\mathcal{C}_0) - 2 \geq E(\mathcal{C}) - 2r(\gamma') - 2 = E(\mathcal{C}) - 2r(\gamma)$ by Lemma 3.4. This establishes the induction hypothesis.

Now, suppose $E(\mathcal{C}) > W + 2(n-1)$ but the protocol fails to produce n 2-portions. Consider a sequence γ of transformations produced by a run of the transformation protocol starting on $\mathcal{C}$. By Lemma 3.6, γ is finite. Let $\mathcal{C}'$ result from $\mathcal{C}$ by γ. By the induction hypothesis, $E(\mathcal{C}') \geq E(\mathcal{C}) - 2r(\gamma)$. Since the protocol failed to obtain n 2-portions, then no transformation is applicable to $\mathcal{C}'$, for otherwise the protocol would have continued. Hence, $E(\mathcal{C}') \leq W$ by Lemma 3.5. It follows that

$$\begin{aligned} E(\mathcal{C}) &> E(\mathcal{C}') + 2(n-1) \\ &\geq E(\mathcal{C}) - 2r(\gamma) + 2(n-1) \end{aligned}$$

Hence, $r(\gamma) > n-1$, contradicting the assumption that the protocol failed to produce n 2-portions. Thus, the protocol stops because n 2-portions were produced 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 2 *Let x be a positive integer and β be any real number such that $\beta x \geq 1$. Then $\lceil x/\lfloor \beta x \rfloor \rceil \leq 2/\beta + 1$.*

Proof: Let ℓ be an integer such that $\ell \leq \beta x < \ell + 1$. Then $\ell \geq 1$, so $\lfloor \beta x \rfloor = \ell$ and $\lceil x/\ell \rceil \leq (\ell+1)/(\beta\ell) + 1 \leq 2/\beta + 1$. ■

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. Let $c_1 = 2^{(c+1)} < 6.5411$ and $c_2 = (W-2)/2 + 2^{-c}/c_1 < 0.2515$.

Theorem 4.1 *Let $0 < \beta \leq 1/2$, 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. Then the initial collection $\mathcal{C}$ consists of a single $(d, \lfloor \beta d \rfloor, \lfloor \beta d \rfloor)$-portion. By Theorem 3.7, it suffices to show that $E(\mathcal{C}) > W + 2(n-1)$.

If $\lceil d/\lfloor \beta d \rfloor \rceil = 2$, then $E(\lceil d/\lfloor \beta d \rfloor \rceil, 1, 1) = 2 \geq (2/\beta - 1)^{-c}$. If $\lceil d/\lfloor \beta d \rfloor \rceil > 2$, then by Fact 2, $E(\lceil d/\lfloor \beta d \rfloor \rceil, 1, 1) = (\lceil d/\lfloor \beta d \rfloor \rceil - 2)^{-c} \geq (2/\beta - 1)^{-c}$. Hence, in either case,

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

Since $\beta \leq 1/2$, it follows that both $(2\beta)^{-c} \geq 1$ and $2/\beta > 1$. Using the bound on d and the definitions of c_1 and c_2, we get

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

Combining the above, we get

$$\begin{aligned} E(\mathcal{C}) &> \left(\frac{2/\beta}{2/\beta - 1}\right)^c (W + 2(n-1)) \\ &> W + 2(n-1) \end{aligned}$$

Hence the transformation protocol succeeds for ξ. ■

It was shown in [FPR91] that secret bit transmission is possible for two players each holding a constant fraction β of the cards, but the required deck size grew super-polynomially in $1/\beta$. From Theorem 4.1 for $n = 1$, it follows that the transformation protocol can be used to solve secret bit transmission with a deck size that grows as 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 construct a protocol $\mathcal{P}^*$ for signature $\xi^* = (h_1, \ldots, h_k; d - \sum h_i)$ given an arbitrary protocol $\mathcal{P}$ for some signature $\xi = (a, b; d - (a+b))$, as long as each h_i is 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 reduction appears in [FW92]. Applying this reduction to the 2-player transformation protocol yields an efficient multiparty n-bit secret key exchange protocol.

The basic idea behind this reduction allows a subset of a team to 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 $\sigma : \{1, \ldots, k\} \rightarrow \{1, \ldots, k'\}$ with the property that $h_i \leq h'_{\sigma(i)}$, for $1 \leq i \leq k$. Player $P_{\sigma(i)}$ plays the role of player 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, $\mathcal{P}$ works just as it would for a ξ deal, and Eve learns nothing 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 4.2 *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 $2 \leq i \leq k - 1$. Let $\mathcal{P}$ be an n-bit secret key exchange protocol that works 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 and that $\mathcal{P}$ works for ξ. We construct a new protocol $\mathcal{P}^*$ to perform n-bit, k-player secret key exchange. $\mathcal{P}^*$ uses protocol $\mathcal{P}$ a total of $k - 1$ times. The i^{th} use establishes an n-bit secret key B_i between players P_i and P_{i+1}.

Each team player except P_1 and P_k randomly divides her hand into three parts. The first part contains a cards, the second part contains b cards, and the third (possibly empty) part contains her remaining cards. P_1 randomly divides her hand into only two parts, one of size a, the other of size $h_1 - a$ Similarly, P_k randomly divides her hand into two parts, one of size b, the other of size $h_k - b$.

In the i^{th} use of $\mathcal{P}$, neighbors P_i and P_{i+1} are the *active* players and participate to establish a secret key B_i that they share. Player P_i uses the part of her hand containing a cards to play the role of Alice in $\mathcal{P}$. Player P_{i+1} uses the part of her hand containing b cards to play the role of Bob in $\mathcal{P}$. The other players do not participate. We call the $a + b$ cards that the active players are using the *current cards.* During each use of $\mathcal{P}$, all team players behave as if Eve holds all the cards except the current cards, so Eve learns nothing new about the location of any card not among the current cards. 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 S to be the team's secret key. Now the team transmits S from player to player until the whole team knows S. When P_i learns S, she sends $E_i = S \oplus B_i$ to P_{i+1} publicly. P_{i+1} recovers S by computing $E_i \oplus B_i$. In this way, all players learn S while releasing no information about S to Eve. Hence, $\mathcal{P}^*$ works for ξ^*. ■

We can apply Theorem 4.2 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 4.3 *Let $0 < \alpha \leq 1/k$, 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 $\mathcal{P}$ be the transformation protocol. From Theorem 4.1, $\mathcal{P}$ works for $(\lfloor \beta d \rfloor, \lfloor \beta d \rfloor; d - 2 \lfloor \beta d \rfloor)$, where $\beta = \alpha/2$. Since $2 \lfloor \beta d \rfloor \leq \lfloor \alpha d \rfloor$, the conditions of Theorem 4.2

are satisfied. Hence, the protocol $\mathcal{P}^*$ given by that theorem works for ξ^*. ∎

Corollary 4.4 *Assume m divides d, and let each of m players be dealt hands of size d/m from a deck of size d. Assume further that $d \geq c_1(2m)^{(c+1)}(n + c_2)$. Then for any team of size $k \leq m$ that forms, there is a protocol for the team that establishes an n-bit secret key.*

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 entropy 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 4.1 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. An open problem which we are currently working on is to further explore the practical applicability of these ideas.

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 4.2.

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.