An Application of Game Theoretic Techniques to Cryptography*

Michael J. Fischer   Rebecca N. Wright

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

Abstract

This paper provides an application of game theoretic techniques to the analysis of a class of multiparty cryptographic protocols for secret bit exchange.

1 Introduction

A cryptographic protocol is often thought of as a game between the honest participants in the protocol and a malicious adversary who tries to corrupt the protocol. In this paper, we consider a simple combinatorial game that arises in the analysis of the class of multiparty "key set" secret bit exchange protocols introduced in [FW92b]. We find an optimal strategy for the combinatorial game and show how this leads to a key set protocol that is optimal from among the class of all key set protocols. While key set protocols are too limited to be of much practical interest, this result is nevertheless interesting as an illustration of the close connection between protocols and games and the use of nontrivial game theoretic techniques in the analysis of protocols.

The combinatorial game is a simple counting game a little like nim which we call the *stick game*. It is played by two players, called the *chooser* and the *adversary*, on a collection of piles of zero or more "sticks". Unlike the simple game of nim, the stick game is not symmetric between the two players. The stick game is defined in Section 2, and strategies for the chooser are discussed in Section 3.

Section 4, the heart of the paper, shows the optimality of a particular strategy for the chooser. A game theoretic strategy stealing argument allows us to prove the optimality of this strategy, even though we are unable to find an optimal strategy for the adversary.

*Mathematics Subject Classification: Primary 90D80, 94A60; Secondary 68Q22, 90D05, 90D46. This research was supported in part by National Science Foundation grant IRI–9015570.

Appears in *Advances in Computational Complexity Theory*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Volume 13, 1993

Key set protocols and their connection with the stick game are given in Section 5. Briefly, the class of key set protocols is a class of cryptographic protocols for distributing a secret bit among a team of agents who communicate through insecure channels. A single eavesdropper who overhears all conversations between the team members represents a possible coalition of dishonest agents who are attempting to gain partial information about the secret bit. We show that each protocol in this class corresponds to a chooser strategy in the stick game. We use this to find a protocol that is optimal for the class of key set protocols.

2 The Stick Game

The stick game is a game between two players, the *chooser* and the *adversary*. It is played on $k+1$ piles of sticks: k chooser piles P_1 through P_k and a single adversary pile E. Pile P_i contains $|P_i|$ sticks, and pile E contains $|E|$ sticks. On the chooser's turn, the chooser chooses one of her piles, say P_i, that contains at least one stick. On the adversary's turn, the adversary chooses any nonempty pile other than the pile just chosen by the chooser. At this point, the following occurs.

1. If the pile chosen by the adversary is another chooser pile P_j, the smaller of P_i and P_j is removed entirely, and one stick is removed from the larger pile.

2. If the pile chosen by the adversary is the adversary pile E, one stick is removed from each of P_i and E.

Note that removing a pile is not the same as removing all the sticks in the pile; the latter leaves an empty pile. The chooser always moves first.

A configuration of the stick game is described by a tuple $(p_1, \ldots, p_k; e; I)$, where $p_i = |P_i|$ and $e = |E|$. I is called the *index component*. On the chooser's turn, I has the value 0. On the adversary's turn, I is the index of the pile designated by the chooser on her previous turn. We generally talk about a chooser move as a *choice* of P_i, and an adversary move as a *match*, either with some P_j or with E.

Play ends when the player whose turn it is cannot move. If there are one or zero chooser piles left, the chooser *wins*. Otherwise the chooser *loses*. We call the stick game starting from configuration C the C *stick game*.

A *strategy* for the chooser, or chooser strategy, is a function that, given a configuration with index component 0 in which a chooser move is possible, specifies the next chooser move. Similarly, an adversary strategy is a function that, given a configuration with index component $I \neq 0$ in which an adversary move is possible, specifies the next adversary move.

We say a chooser strategy $\mathcal{S}$ *succeeds on* configuration C if the chooser wins when playing the C stick game according to $\mathcal{S}$, regardless of the moves chosen by the adversary. We call C *winning* if some chooser strategy succeeds on C. A chooser strategy $\mathcal{S}$ is *optimal* if it succeeds on every winning configuration. Similarly, we say an adversary strategy $\mathcal{T}$ *succeeds on* configuration C if the chooser loses when the adversary plays the C stick game according to $\mathcal{T}$, regardless of the moves chosen by the chooser. We call C *losing* if some adversary strategy succeeds on C. An adversary strategy $\mathcal{T}$ is *optimal* if it succeeds on every losing configuration.

Note that if C is a configuration in which it is the chooser's turn, then C is winning if and only if there exists a chooser move that results in a winning configuration. If C is a configuration in which it is the adversary's turn, then C is winning if and only if all adversary moves result in a winning configuration.

The stick game is a finite game, since every adversary turn decreases the total number of sticks by at least two. Furthermore, it is a game of complete information, since the chooser and the adversary take turns and all information about the state is known to both the chooser and the adversary. Hence a well known game theoretic result [BCG82] tells us that every configuration is either winning or losing, and there exist both an optimal chooser strategy $\mathcal{S}$ and an optimal adversary strategy $\mathcal{T}$.

The stick game is not as simple as it might at first seem. Clearly, the chooser's goal is to get rid of all but one of her piles, after which a win is guaranteed. The adversary's goal is to cause the game to terminate while the chooser still has two or more piles remaining. Let k be the number of chooser piles and e be the size of the adversary's pile. The adversary can make at most e matches with E, after which E is empty. In order to defeat the chooser, the adversary can make at most $k-2$ matches with chooser piles, for each such match reduces by one the number of chooser piles, and after $k-1$ such matches, the chooser is guaranteed to win.

The chooser is faced with the dilemma of whether to choose a large pile, possibly giving the adversary the opportunity to choose and eliminate another large pile, or to choose a small pile, which may give the adversary the opportunity to produce a still smaller pile. (Note that if any chooser pile becomes empty before the game ends, then the chooser will eventually lose, so it is to the adversary's advantage to make chooser piles smaller.)

The adversary in turn must decide whether to match with a chooser pile or with his own pile, and if he matches with a chooser pile, whether to choose a larger or smaller pile than the one chosen by the chooser. The advantage of choosing a larger pile is that more sticks get removed from the game when the chooser's designated pile is eliminated. The advantage of choosing a smaller pile is that a stick gets removed from the chooser's designated pile, reducing its size.

The reader is invited to think of plausible strategies for the two players before proceeding.

3 Chooser Strategies

Given a configuration $C = (p_1, \ldots, p_k; e; I)$, we define the functions $\mathrm{size}(C) = k + e$ and $\mathrm{piles}(C) = k$. The following proposition is an immediate consequence of the fact that the stick game is a finite game and the number of chooser piles never increases during play.

Proposition 3.1 *If* $\text{piles}(C) \leq 1$*, then* C *is winning, and every chooser strategy succeeds on* C*.*

The following proposition is easily proved by an exhaustive case analysis of possible moves.

Proposition 3.2 *If* $C = (1, 1; 0; 0)$*, then* C *is winning, and every chooser strategy succeeds on* C*.*

We say a chooser pile P_i is *feasible* if either

- $|P_i| \geq 2$, or
- $|P_i| = 1, |E| = 0$ and for all $j \neq i$, $|P_j| \geq 2$.

Note that if all chooser piles are nonempty and the chooser chooses a feasible pile, then, regardless of the match made by the adversary, all chooser piles in the resulting configuration are nonempty. This is obvious when a pile of size 2 or greater is chosen. When a feasible singleton is chosen, all other chooser piles have size at least 2, and the adversary has no choice but to match with a chooser pile.

Theorem 3.3 *Let* $\mathcal{S}$ *be a chooser strategy that always chooses a feasible pile whenever some pile is feasible. Let* $C = (p_1, \ldots, p_k; e; 0)$*, where* $p_i \geq 1$ *for* $1 \leq i \leq k$*, and* $\max p_i + \min p_i \geq \text{size}(C)$*. Then* $\mathcal{S}$ *succeeds on* C*.*

Proof: The proof is by induction on $\text{size}(C)$. Let $\mathcal{S}$ satisfy the conditions of the theorem. Let $C = (p_1, \ldots, p_k; e; 0)$, where $p_i \geq 1$ for $1 \leq i \leq k$ and $\max p_i + \min p_i \geq \text{size}(C)$. Assume inductively that $\mathcal{S}$ succeeds on every configuration $\overline{C}$ that satisfies the conditions of the theorem and has $\text{size}(\overline{C}) < \text{size}(C)$. Let $C_0 = C$. We show that $\mathcal{S}$ succeeds on C_0. The theorem then follows by induction.

We first dispose of some easy cases. If $k \leq 1$, then by Proposition 3.1, $\mathcal{S}$ succeeds on C_0. If $k \geq 2$ and $\max p_i = 1$, then $\min p_i = 1$, and hence $2 = \max p_i + \min p_i \geq \text{size}(C_0)$. Thus, $\text{size}(C_0) = 2$ and $C = (1, 1; 0, 0)$, so by Proposition 3.2, $\mathcal{S}$ succeeds on C_0.

We can assume now that $k \geq 2$ and $\max p_i \geq 2$. Let $M = \max p_i$ and $m = \min p_i$. Thus $M \geq 2$, $M \geq m \geq 1$ and $M + m \geq k + e$. Since there is a nonempty chooser pile, the game is not yet done. Suppose the chooser chooses a pile according to $\mathcal{S}$, resulting in some configuration $C_1 = (p_1, \ldots, p_k; e; i)$. P_i is feasible in C_0 since the pile of size M is feasible, and $\mathcal{S}$ always chooses a feasible pile if there is one. Without loss of generality, let $i = 1$, so $C_1 = (p_1, \ldots, p_k; e; 1)$.

Since $k \geq 2$ and each $p_j \geq 1$, there is some possible adversary move. We show that $\mathcal{S}$ succeeds on C_0 by showing that for every possible adversary move from C_1, $\mathcal{S}$ succeeds on the resulting configuration C_2. Since P_1 is feasible, all chooser piles

P_j in C_2 have $|P_j| \geq 1$. Also, we have $\mathrm{size}(C_2) = \mathrm{size}(C_0) - 1$. Let M' and m' denote the maximum and minimum of the sizes of the chooser piles in C_2, respectively.

If the adversary matches with E, then $e \geq 1$ and $C_2 = (p_1 - 1, p_2, \ldots, p_k; e - 1; 0)$. In going from C_0 to C_2, only one chooser pile, P_1, changes size, from p_1 to $p_1 - 1$. Since only one chooser pile changes size and there are at least 2 chooser piles remaining in C_2, at most one of the maximum or the minimum decreases, and if either decreases, it decreases by one. Thus $M' + m' \geq M + m - 1 \geq \mathrm{size}(C_0) - 1 = \mathrm{size}(C_2)$. Moreover, since P_1 is feasible and $e \geq 1$, we have $p_1 \geq 2$, so all piles in C_2 are nonempty. By induction, $\mathcal{S}$ succeeds on C_2.

If the adversary matches with another chooser pile, without loss of generality P_2, then $C_2 = (\max(p_1, p_2) - 1, p_3, \ldots, p_k; e; 0)$. If $k = 2$, then $\mathrm{piles}(C_2) = 1$, so by Proposition 3.1, $\mathcal{S}$ succeeds on C_2. Otherwise $k \geq 3$, $M' \geq M - 1$ and $m' \geq m - 1$. If $M' = M - 1$, then $\max(p_1, p_2) - 1 = M' \geq p_3$. If $m' = m - 1$, then $\max(p_1, p_2) = m \leq p_3$. Both equalities cannot simultaneously hold, since it is impossible that $\max(p_1, p_2) - 1 \geq p_3 \geq \max(p_1, p_2)$, so either $M' \geq M$ or $m' \geq m$. Hence, $M' + m' \geq M + m - 1 \geq \mathrm{size}(C_0) - 1 = \mathrm{size}(C_2)$. Moreover, since P_1 is feasible, either $p_1 \geq 2$ or $p_2 \geq 2$; hence, $\max(p_1, p_2) - 1 \geq 1$, and all piles in C_2 are nonempty. By induction, $\mathcal{S}$ succeeds on C_2. ■

Corollary 3.4 *Let $C = (p_1, \ldots, p_k; e; 0)$, where $p_i \geq 1$ for $1 \leq i \leq k$, and $\max p_i + \min p_i \geq \mathrm{size}(C)$. Then C is winning.*

Thus, $\max p_i + \min p_i \geq \mathrm{size}(C)$ provides a sufficient condition for C to be winning. However, it is not a necessary condition, since for example the configuration $C = (3, 3, 2, 1; 1; 0)$ has $\max p_i + \min p_i = 4 < \mathrm{size}(C)$, but the SFP strategy, defined below, succeeds on C.

The *smallest feasible pile* strategy (SFP) is defined as follows. The SFP strategy chooses i such that P_i is the feasible pile with the smallest size. In the case of ties, the smallest such i is chosen. If no chooser pile is feasible, then the smallest i such that P_i is nonempty is chosen, if a nonempty pile exists.

Despite the fact that we have been unable to extend Corollary 3.4 to give a simple exact characterization of winning configurations, we are able to show that if C is winning, then SFP succeeds on C. Thus, the SFP strategy is optimal.

4 Optimality of the SFP Strategy

In order to show the optimality of the SFP strategy, it suffices to show the following: for any winning configuration C in which it is the chooser's turn to move next, if the chooser moves according to SFP, then the resulting configuration C' is also winning. We use what is known as a strategy stealing argument to show that C winning implies C' is winning.

The basic idea of the argument is to simultaneously play two stick games, one on C and one on C'. We call the two games G and G', respectively. In game G, the chooser plays using an optimal chooser strategy and we specify the adversary moves. Since the chooser plays optimally, if C is winning, then all resulting configurations in G will be winning, regardless of the moves we specify for the adversary. In G', the adversary plays using an optimal adversary strategy and we specify the chooser moves. Since the adversary plays optimally, if C' is losing, then all resulting configurations in G' are losing, regardless of the moves we specify for the chooser.

In more detail, let $C_0 = C$ and $C'_0 = C'$. We call the C stick game G, and we refer to the G chooser and the G adversary. Similarly, we have the G' game, chooser and adversary. We play G in order to develop a sequence of configurations $C_0, C_1, C_2, \ldots$ that describe a play of the C stick game, and we play G' in order to develop a sequence of configurations $C'_0, C'_1, C'_2, \ldots$ that describe a play of the C' stick game. If C is winning, then all C_i are winning since the chooser plays optimally in G. If C'_0 is losing, then all C'_i are losing since the adversary plays optimally in G'. Hence, if any C'_j can be shown to be winning from the assumption that some C_i is winning, it will follow that $C = C_0$ winning implies $C' = C'_0$ winning. This is illustrated in Figure 1.

$$
\begin{array}{ccc}
C_0 \text{ winning} & & C'_0 \text{ winning} \\
\Downarrow & & \Uparrow \\
\vdots & & \vdots \\
\Downarrow & & \Uparrow \\
C_i \text{ winning} & \Longrightarrow & C'_j \text{ winning}
\end{array}
$$

Figure 1: The strategy stealing argument.

In our strategy stealing argument, adversary moves in G and chooser moves in G' will generally be based on *mirroring*. G and G' will be played simultaneously, with moves alternately chosen from the two games. The G adversary selects its next move by mirroring the G' adversary, matching with the same pile that the G' adversary previously matched with, if possible. Similarly, the G' chooser selects its next move by mirroring the G chooser, choosing the same pile that the G chooser previously selected, if possible. Where mirroring cannot be applied (because, for example, the corresponding pile does not exist), we will be able to either choose an alternate move or prove on the basis of the play constructed so far that C winning implies C' winning. In this latter case, the construction can stop.

Since we do not know the optimal strategy of either chooser or adversary, we must consider all possible moves in our analysis and show for each that the argument works, under the assumption that the given move really was optimal. A large number of cases can result during this process. In order to make the case analysis manageable, we have broken the proof of the optimality of SFP into several lemmas. Lemmas 4.1, 4.3, and 4.4 formalize some useful and intuitively easy facts. Lemmas 4.2, 4.5 and 4.6 start with two configurations C and C' that have a known relationship and show that if C is winning then C' is also winning. These are each proved using a strategy stealing argument. The proof of each Lemma is inductive, so often it is only necessary to play G and G' for one or two steps in order to obtain a pair (C_i, C'_j) to which the inductive hypothesis applies. Lemma 4.7 shows that when there are only two chooser piles, Corollary 3.4 provides an exact characterization of winning configurations. Finally, Theorem 4.8 shows the optimality of SFP.

We start with the intuitively obvious fact that it is impossible for the chooser to win the stick game when there is a chooser pile containing no sticks unless it is the only chooser pile.

Lemma 4.1 *Let $C = (p_1, \ldots, p_k; e; 0)$. If $k \geq 2$ and $p_i = 0$ for some i, then C is losing.*

Proof: We proceed by induction. Let $C = (p_1, \ldots, p_k; e; 0)$, let $k \geq 2$, and suppose, without loss of generality, that $p_1 = 0$. Inductively assume that the lemma holds for all $\overline{C}$ such that $\text{size}(\overline{C}) < \text{size}(C)$. We show that C is losing.

If there is no nonempty chooser pile in C, then the chooser can not move and the game ends. The chooser loses since $k \geq 2$. Otherwise, at least one chooser pile is nonempty and the chooser has a move. We show that no matter which move the chooser makes, either the game ends and the chooser loses, or there is an adversary response that results in a losing configuration. Hence, C is also losing.

Let P_i be the nonempty pile selected by the chooser, so the resulting configuration is $C_1 = (0, p_2, \ldots, p_k; e; i)$ for some $i \neq 1$. If there is no adversary move, then the game ends and the chooser loses. Otherwise, the adversary must choose a nonempty pile to match with. Let C_2 be the resulting configuration. If the adversary matches with E, then C_2 has at least two piles, P_1 and P_i, and $\text{size}(C_2) = k + (e-1) = \text{size}(C) - 1$. If the adversary matches with P_j, then $j \notin \{1, i\}$, so $k \geq 3$. Hence, C_2 has at least two piles, and $\text{size}(C_2) = (k-1) + e = \text{size}(C) - 1$. In either case, $\text{piles}(C_2) \geq 2$, C_2 has a pile of size 0, and $\text{size}(C_2) = \text{size}(C) - 1$. Therefore C_2 is losing by induction. ■

Let $C = (p_1, \ldots, p_k; e; 0)$ and $C' = (p'_1, \ldots, p'_{k'}; e'; 0)$ be two configurations. We say C' *dominates* C if $k = k'$, $e' \leq e$ and there is a permutation π on $\{1, \ldots, k\}$ such that $p'_i \geq p_{\pi(i)}$ for each i. We write $C' \trianglerighteq C$.

The following lemma captures the intuition that increasing the size of the chooser piles or decreasing the size of the adversary pile should only help the chooser.

Lemma 4.2 (Domination Lemma) *Let $C' \trianglerighteq C$. If C is winning, then C' is winning.*

Proof: Let C and C' be two configurations such that $C' \trianglerighteq C$, and suppose that C is winning. Inductively assume that the lemma holds for all $\overline{C}$ and $\overline{C}'$ such that $\text{size}(\overline{C}) < \text{size}(C)$. We use a strategy stealing argument to show that C' is winning by playing the C stick game G and the C' stick game G', as shown in Figure 1. Let $C_0 = C = (p_1, \ldots, p_k; e; 0)$ and let $C'_0 = C' = (p'_1, \ldots, p'_{k'}; e'; 0)$. We show that C'_0 is winning.

If $k \leq 1$, then by Proposition 3.1, C'_0 is winning. Otherwise, $\text{size}(C_0) \geq \text{size}(C'_0) \geq k \geq 2$.

The G chooser chooses a pile, say P_i. Let C_1 be the resulting configuration $(p_1, \ldots, p_k; e; i)$. In game G', we consider the corresponding chooser choice $P_{\pi^{-1}(i)}$, which must be possible because $p'_{\pi^{-1}(i)} \geq p_i$, by the definition of domination. Hence, the resulting configuration is $C'_1 = (p'_1, \ldots, p'_k; e'; \pi^{-1}(i))$. The G' adversary now makes a move, resulting in configuration C'_2.

We construct configuration C_2 by having the G adversary mirror the G' adversary, if possible. If the G' adversary matches with E, then the G adversary can match with E, since $e \geq e'$, by the definition of domination. Then $C'_2 \trianglerighteq C_2$, and so by induction, C'_2 is winning, and hence C'_0 is winning.

Otherwise the G' adversary matches with some P_j. Because C_0 is winning and $k \geq 2$, Lemma 4.1 implies that $p_\ell \geq 1$ for every ℓ. Hence the G adversary can match with $P_{\pi(j)}$. In this case, the resulting C_2 is the same as C_0 except that in place of P_i and $P_{\pi(j)}$ there is a single pile of size $\max(p_i, p_{\pi(j)}) - 1$. Similarly, C'_2 differs from C'_0 only in that piles $P_{\pi^{-1}(i)}$ and P_j are replaced by a single pile of size $\max(p'_{\pi^{-1}(i)}, p'_j) - 1$. Since $C'_0 \trianglerighteq C_0$ (via π), we have that $p'_{\pi^{-1}(i)} \geq p_i$ and $p'_j \geq p_{\pi(j)}$. Hence $\max(p'_{\pi^{-1}(i)}, p'_j) \geq \max(p_i, p_{\pi(j)})$. Therefore, modifying π so that the two new piles correspond, we see that $C'_2 \trianglerighteq C_2$. Also, $\text{size}(C_2) = \text{size}(C_0) - 1$. Hence by induction, C'_2 is winning, so C'_0 is winning. ■

A special case of the domination lemma is that if two configurations differ only by a permutation of the pile sizes, they are either both winning or both losing. We sometimes say two such configurations are *equal up to permutation.*

We call a chooser pile of size 1 a *singleton.* Lemma 4.3 says that whenever a singleton is feasible in a given configuration, the configuration is winning.

Lemma 4.3 *Let $C = (p_1, \ldots, p_k; e; 0)$. If for some i, P_i is feasible and $p_i = 1$, then C is winning.*

Proof: Let $C = (p_1, \ldots, p_k; e; 0)$, and without loss of generality, assume that P_1 is feasible and $p_1 = 1$. Inductively assume that the lemma holds for all configurations $\overline{C}$ such that $\text{size}(\overline{C}) < \text{size}(C)$, and let $C_0 = C$.

If $k \leq 1$ then C is winning by Proposition 3.1. Otherwise $k \geq 2$, and since P_1 is feasible and $p_1 = 1$, then $e = 0$ and for every $\ell \geq 2$, $p_\ell \geq 2$. Let the chooser choose pile P_1, so $C_1 = (1, p_2, \ldots, p_k; 0; 1)$ is the resulting configuration. To show that C_0 is winning, it suffices to show that C_1 is winning.

Since $p_\ell \geq 2$ for every $\ell \geq 2$, the adversary does have some move. Because $e = 0$, the adversary must match with some P_j. Without loss of generality, let $j = 2$, so the resulting configuration is $C_2 = (p_2 - 1, p_3, \ldots, p_k; 0; 0)$. Let $\overline{C} = (1, p_3, \ldots, p_k; 0; 0)$. Since $\text{size}(\overline{C}) = \text{size}(C_0) - 1$, then $\overline{C}$ is winning by induction. Since $C_2 \trianglerighteq \overline{C}$, then C_2 is winning by Lemma 4.2. Hence, C_1, and therefore C_0, are both winning. ■

Lemma 4.3 shows that if a feasible singleton is chosen, the resulting configuration is winning. Lemma 4.4 provides a partial converse. Namely, if a non-feasible singleton is chosen in a configuration with at least three piles, then the resulting configuration is losing.

Lemma 4.4 *Let $C = (p_1, \ldots, p_k; e; 0)$, where $k \geq 3$ and $p_i = 1$. Let $C_1 = (p_1, \ldots, p_k; e; i)$. If P_i is not feasible in C, then C_1 is losing.*

Proof: Without loss of generality, let $C = (1, p_2, \ldots, p_k; e; 0)$, where $k \geq 3$, and let $C_1 = (1, p_2, \ldots, p_k; e; 1)$. Assume P_1 is not feasible in C, and let $C_0 = C$. We show that C_1 is losing.

By Lemma 4.1, if any $p_j = 0$, then C_0, and hence C_1, are both losing. Otherwise, assume all $p_j \geq 1$. Since P_1 is not feasible, then either $e \geq 1$ or $p_j = 1$ for some $j \neq 1$. If $e \geq 1$, then the adversary can match with E yielding a configuration $C_2 = (0, p_2, \ldots, p_k; e - 1; 0)$, which is losing by Lemma 4.1. Similarly, if $p_j = 1$ for some $j \neq 1$, then the adversary can match with P_j. Without loss of generality, $j = 2$ and the resulting configuration is $C_2 = (0, p_3, \ldots, p_k; e; 0)$. Since C_2 has $k - 1 \geq 2$ piles, it is losing by Lemma 4.1. ■

Lemma 4.5 *Let $C = (p_1, \ldots, p_{k-1}, x; e; 0)$ and $C' = (p_1, \ldots, p_{k-1}, x - 1; e - 1; 0)$, where $e \geq 1$, $x \geq 2$, and each p_i satisfies $p_i \geq x$ or $p_i = 1$. Then if C is winning, C' is winning.*

Proof: Let $C = (p_1, \ldots, p_{k-1}, x; e; 0)$ and $C' = (p_1, \ldots, p_{k-1}, x - 1; e - 1; 0)$, and suppose that C is winning, $e \geq 1$, $x \geq 2$, and each p_i satisfies $p_i \geq x$ or $p_i = 1$. Inductively assume that the lemma holds for all $\overline{C}$ and $\overline{C}'$ such that $\text{size}(\overline{C}) < \text{size}(C)$. We use a strategy stealing argument to show that C' is winning by playing the C stick game G and the C' stick game G', as shown in Figure 1. Let $C_0 = C$ and $C'_0 = C'$. We show that C'_0 is winning.

If $k \leq 1$, then C'_0 is winning by Proposition 3.1. Otherwise $k \geq 2$, so the G chooser has not already won in C_0. We assume the G chooser is using an optimal strategy which selects, say, pile P_i. If $p_i = 1$, then the G adversary can match with E. In this case the resulting configuration C_2 still has $k \geq 2$ piles and so is losing by Lemma 4.1, a contradiction. Hence $p_i > 1$, and therefore $p_i \geq x$.

If $p_i = x$, then we have the G adversary match with E. Then the resulting configuration C_2 is equal up to permutation to $(p_1, \ldots, p_{k-1}, x - 1; e - 1; 0) = C'_0$, so C'_0 is winning. Otherwise $p_i > x$, and without loss of generality, $i = 1$. Then C_1 is

$(p_1, \ldots, p_{k-1}, x; e; 1)$. We mirror the G chooser move to G', so $C_1' = (p_1, \ldots, p_{k-1}, x-1; e-1; 1)$.

Given C_1', the G' adversary has some possible move, because $x \geq 2$ and therefore the pile containing $x-1$ sticks is nonempty. We mirror the G' adversary move to G to obtain C_2. We consider three types of adversary moves separately. In each case we show that C_2' is winning.

- G' adversary matches with E. Then $e - 1 \geq 1$, and

$$\begin{aligned} C_2' &= (p_1 - 1, p_2, \ldots, p_{k-1}, x-1; e-2; 0) \\ C_2 &= (p_1 - 1, p_2, \ldots, p_{k-1}, x; e-1; 0) \end{aligned}$$

  Furthermore, $p_1 > x$ implies $p_1 - 1 \geq x$, so by induction, C_2' is winning.

- G' adversary matches with P_j such that $p_j \neq x-1$. Without loss of generality $j = 2$, so

$$\begin{aligned} C_2' &= (\max(p_1, p_2) - 1, p_3, \ldots, p_{k-1}, x-1; e-1; 0) \\ C_2 &= (\max(p_1, p_2) - 1, p_3, \ldots, p_{k-1}, x; e; 0) \end{aligned}$$

  Since $p_1 > x$, we have that $\max(p_1, p_2) - 1 \geq p_1 - 1 \geq x$. By induction, C_2' is winning.

- G' adversary matches with P_j such that $|P_j| = x - 1$ in C_1'. Without loss of generality, $j = k$. Since $p_1 > x$, we have

$$\begin{aligned} C_2' &= (p_1 - 1, p_2, \ldots, p_{k-1}; e-1; 0) \\ C_2 &= (p_1 - 1, p_2, \ldots, p_{k-1}; e; 0) \end{aligned}$$

  Then $C_2' \trianglerighteq C_2$, so C_2' is winning.

In each case, C_2' is winning. Hence, C_0' is winning, as desired. ∎

Lemma 4.6 *Let $C = (p_1, \ldots, p_{k-2}, x, y; e; 0)$ and $C' = (p_1, \ldots, p_{k-2}, y'; e; 0)$, where $k \geq 2$, $y' + 1 \geq y \geq x$, $y' \geq 1$, each p_i satisfies $p_i \geq x$ or $p_i = 1$, and either $y' > 1$ or there is no feasible singleton in C. Then if C is winning, C' is winning.*

Proof: Let $C = (p_1, \ldots, p_{k-2}, x, y; e; 0)$ and $C' = (p_1, \ldots, p_{k-2}, y'; e; 0)$, where $k \geq 2$, $y' + 1 \geq y \geq x$, $y' \geq 1$, each p_i satisfies $p_i \geq x$ or $p_i = 1$, and either $y' > 1$ or there is no feasible singleton in C. Suppose further that C is winning. Inductively assume that the lemma holds for all $\overline{C}$ and $\overline{C}'$ such that $\text{size}(\overline{C}) < \text{size}(C)$. We use a strategy stealing argument to show that C' is winning by playing the C stick game G and the C' stick game G', as shown in Figure 1. Let $C_0 = C$ and $C_0' = C'$. We show that C_0' is winning.

If $k = 2$, then $\text{piles}(C_0') = 1$, so C_0' is winning by Proposition 3.1. Otherwise $k \geq 3$, and Lemma 4.1 implies each pile of C_0 must be of size at least 1. In particular, $y \geq x \geq 1$. Hence the G chooser has a move, and must choose a pile P_i.

1. G chooser chooses P_i such that $|P_i| = x$ (or y). In this case the G adversary matches with a pile P_j with $p_j = y$ (or x). Without loss of generality, $i = k-1$ and $j = k$. Then $C_2 = (p_1, \ldots, p_{k-2}, y-1; e; 0)$. Hence $C_0' \trianglerighteq C_2$, so C_0' is winning.

2. G chooser chooses P_i such that $|P_i| > x \geq 1$ and $|P_i| \neq y$. Without loss of generality, let $i = 1$. We mirror the G chooser move to G' and consider possible G' adversary moves. Note that there is some possible G' adversary move, since the G' adversary can match with pile P_{k-1}, which has size $y' \geq 1$.

   - G' adversary matches with E. Then $e \geq 1$. If $y' > 1$ or $e > 1$, we mirror the match with E back to G. Then

     $$\begin{aligned} C_2' &= (p_1 - 1, p_2, \ldots, p_{k-2}, y'; e-1; 0) \\ C_2 &= (p_1 - 1, p_2, \ldots, p_{k-2}, x, y; e-1; 0) \end{aligned}$$

     If $y' > 1$, then C_2' is winning by induction. If $e > 1$, then C_2 has no feasible singletons, so C_2' is winning by induction.
     Otherwise $y' = 1$ and $e = 1$. In this case, we have the G adversary match with P_{k-1} (of size x). Then

     $$\begin{aligned} C_2' &= (p_1 - 1, p_2, \ldots, p_{k-2}, 1; 0; 0) \\ C_2 &= (p_1 - 1, p_2, \ldots, p_{k-2}, y; 1; 0) \end{aligned}$$

     We have $2 = y' + 1 \geq y \geq 1$. If $y = 1$, then $C_2' \trianglerighteq C_2$, and hence C_2' is winning by Lemma 4.2. If $y = 2$, then since $p_1 - 1 \geq x$, the configurations C_2 and C_2' satisfy Lemma 4.5 and hence C_2' is winning.

   - G' adversary matches with P_j, where $|P_j| \neq y'$. In this case, we mirror the G' adversary move to G. Without loss of generality $j = 2$, so

     $$\begin{aligned} C_2' &= (\max(p_1, p_2) - 1, p_3, \ldots, p_{k-2}, y'; e; 0) \\ C_2 &= (\max(p_1, p_2) - 1, p_3, \ldots, p_{k-2}, x, y; e; 0) \end{aligned}$$

     Hence $p_1 > x$ implies $\max(p_1, p_2) - 1 \geq x$. If $y' > 1$ or there is no feasible singleton in C_2, then by induction C_2' is winning. Otherwise $y' = 1$ and there is a feasible singleton in C_2. We show that this is impossible. We have $e = 0$, $p_1 > x \geq 1$ and $p_2 \neq y' = 1$. Hence, neither of the piles that changed from C_0 to C_2 were singletons in C_0, so C_0 has at most one singleton. By assumption and the fact that $y' = 1$, there is no feasible singleton in C_0, which, together with $e = 0$, implies that there is no singleton at all in C_0. In particular, we have $|P_{k-1}| = x \geq 2$, so since $2 = y' + 1 \geq x$, we conclude that $x = 2$. Furthermore, $p_1 > x$, so $\max(p_1, p_2) - 1 \geq 2$. Hence there are no singletons in C_2, so in particular there is no feasible singleton in C_2.

- G' adversary matches with P_j such that $|P_j| = y'$. Without loss of generality, $j = k-1$. Then the G adversary can match with P_k, so up to permutation,

$$\begin{aligned} C_2' &= (p_2, \ldots, p_{k-2}, \max(p_1, y') - 1; e; 0) \\ C_2 &= (p_2, \ldots, p_{k-2}, x, \max(p_1, y) - 1; e; 0) \end{aligned}$$

  We have $p_1 > x$, so $\max(p_1, y') \geq \max(p_1, y) - 1 \geq x$. Also, $\max(p_1, y') - 1 \geq p_1 - 1 \geq x \geq 1$. If $\max(p_1, y') - 1 > 1$, or if there is no feasible singleton in C_2, then by induction, C_2' is winning. Otherwise $\max(p_1, y') - 1 = 1$ and there is some feasible singleton in C_2. In this case, $p_1 \leq 2$, and thus $x = 1$, hence P_{k-1} is the unique feasible singleton in C_2. Then $e = 0$, $p_1 = 2$, and $p_i \geq 2$ for $2 \leq i \leq k-2$. Then the last pile of C_2' is a feasible singleton, so by Lemma 4.3, C_2' is winning.

Since C_2' is winning in each case, C_0' is winning.

3. G chooser chooses P_i such that $|P_i| = 1$ for some $i \leq k-2$. Without loss of generality, let $i = 1$. Since $k \geq 3$, P_1 is feasible in C_0 by Lemma 4.4 and the fact that C_0 is winning. Therefore, $y' > 1$ and $e = 0$, so P_1 is feasible in C_0'. By Lemma 4.3, C_0' is winning. ■

Lemma 4.7 *If $C = (p_1, p_2; e; 0)$, then $p_1 + p_2 \geq 2 + e$ if and only if C is winning.*

Proof: Let $C = (p_1, p_2; e; 0)$. From Corollary 3.4, we know that if $p_1 + p_2 \geq 2 + e$, then C is winning.

For the converse, we show by induction on size(C) that if $p_1 + p_2 < 2 + e$ then C is losing. Assume $p_1 + p_2 < 2 + e$, and assume the induction hypothesis holds for all configurations $\overline{C}$ for which size$(\overline{C}) <$ size(C). Let $C_0 = C$.

If $p_1 = p_2 = 0$, then the chooser can not move and therefore loses, so C is losing. Otherwise at least one chooser pile is nonempty, and so the chooser must choose a pile P_i. Without loss of generality, let $i = 1$, so the resulting configuration is $C_1 = (p_1, p_2; e; 1)$. If $e = 0$, then $p_1 + p_2 < 2$, so $p_2 = 0$. Hence the adversary can not move and again C is losing. Otherwise $e > 0$, so the adversary can match with E resulting in configuration $C_2 = (p_1 - 1, p_2; e - 1; 0)$. Then size$(C_2) <$ size(C) and $p_1 - 1 + p_2 < 2 + e - 1$, so by induction, C_2 is losing. Hence C is losing. ■

Thus SFP is optimal when there are only two chooser piles. We can now show the optimality of SFP in general.

Theorem 4.8 *The SFP chooser strategy is optimal.*

Proof: By Proposition 3.1 and Lemma 4.7, it remains only to show that SFP is optimal for configurations with at least 3 chooser piles.

Suppose $k \geq 3$ and $C_0 = (p_1, \ldots, p_k; e; 0)$ is winning. Suppose SFP chooses P_i for some i. We may assume without loss of generality that $i = 1$, so the resulting configuration is $C_1' = (p_1, \ldots, p_k; e; 1)$. We use a strategy stealing argument to show that C_1' is winning by playing the C_0 stick game G and the C_1' stick game G'. This shows the optimality of SFP.

We assume the G chooser is using an optimal strategy which selects, say, pile P_j. Let $C_1 = (p_1, \ldots, p_k; e; j)$ be the resulting configuration. If $p_j = p_1$, then up to permutation $C_1' = C_1$, so C_1' is winning, and we are done. Hence we need only consider $p_j \neq p_1$, in which case $j \neq 1$. We may assume without loss of generality that $j = 2$. Also, since $k \geq 3$, Lemma 4.1 implies $p_\ell \geq 1$ for every ℓ.

Suppose $p_1 = 1$. Then $p_2 \geq 2$, so there is a feasible pile in C_0, and P_1 is feasible in C_0. Then by Lemma 4.3, C_0' is winning and we are done. Hence, we may assume $p_1 \geq 2$.

Suppose $p_2 = 1$. Then P_2 is not feasible, or it would have been chosen by SFP. But this contradicts Lemma 4.4, since C_1 is winning. Hence, $p_2 \geq 2$. Furthermore, because p_1 is chosen according to the *smallest* feasible pile rule, it must be the case that $p_2 \geq p_\ell$ or $p_\ell = 1$ for all $\ell \geq 2$. Since also $p_2 \neq p_1$, we have $p_2 > p_1 \geq 2$.

As before, we distinguish the C_1 stick game and the C_1' stick game by calling them the G game and the G' game. We consider possible G' adversary moves from C_1' and show that for every possible G' adversary move from C_1', the resulting configuration C_2' is winning, and hence C_1' is winning.

1. G' adversary matches with E. Then

$$\begin{aligned} C_2' &= (p_1 - 1, p_2, \ldots, p_k; e - 1; 0) \\ C_0 &= (p_1, p_2, \ldots, p_k; e; 0) \end{aligned}$$

   Hence C_0 and C_2' satisfy the conditions of Lemma 4.5, so C_2' is winning.

2. G' adversary matches with P_2. Then

$$C_2' = (p_2 - 1, p_3, \ldots, p_k; e; 0)$$

   We have the G adversary match with P_1. Since P_2 matches with P_1 in both games, $C_2 = C_2'$, so C_2' is winning.

3. G' adversary matches with some P_a, where $a \geq 3$. We may assume without loss of generality that $a = 3$, so the resulting configuration is $C_2' = (\max(p_1, p_3) - 1, p_2, p_4, \ldots, p_k; e; 0)$, up to permutation. (For the remainder of this proof, we omit the phrase "up to permutation".) We consider the possible relationships between p_1 and p_3 separately.

   - If $p_1 < p_3$, then we mirror the G' adversary move to G. Then

$$\begin{aligned} C_2' &= (p_3 - 1, p_2, p_4, \ldots, p_k; e; 0) \\ C_2 &= (p_1, \max(p_2, p_3) - 1, p_4, \ldots, p_k; e; 0) \end{aligned}$$

If $p_2 \geq p_3$, then obviously $C_2' \trianglerighteq C_2$. If $p_2 < p_3$, then by flipping the first two piles of C_2, it becomes apparent that $C_2' \trianglerighteq C_2$. In either case, C_2' is winning by Lemma 4.2.

- If $p_3 < p_1$, we have the G adversary match with P_1. Then

$$\begin{aligned} C_2' &= (p_1 - 1, p_2, p_4, \ldots, p_k; e; 0) \\ C_2 &= (p_2 - 1, p_3, p_4, \ldots, p_k; e; 0) \end{aligned}$$

Since $p_1 - 1 \geq p_3$ and $p_2 \geq p_2 - 1$, we have $C_2' \trianglerighteq C_2$, and C_2' is winning by Lemma 4.2.

- If $p_1 = p_3$, then

$$\begin{aligned} C_2' &= (p_1 - 1, p_2, p_4, \ldots, p_k; e; 0) \\ C_0 &= (p_1, p_2, p_1, p_4, \ldots, p_k; e; 0) \end{aligned}$$

We have $p_1 \geq 2$, and because P_1 was chosen by SFP, C_0 has no feasible singleton. Hence Lemma 4.6 applies to C_0 and C_2', so C_2' is winning.

Since C_2' is winning in each case, C_1' is winning. ■

5 Secret Bit Exchange

In [FW92a, FW92b], we explore the problem of *multiparty secret bit exchange*. Consider a *team* of k players. All communication between the team players is overheard by a computationally unlimited eavesdropper, Eve, whom we also consider to be a player. The team players are dealt hands of prespecified sizes from a deck D of d distinct cards; any remaining cards are dealt to Eve.

The goal of the team is to determine a bit s satisfying agreement, secrecy, and uniformity. *Agreement* is met if each team player knows s. *Secrecy* is met if Eve'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 1 or 0. Each team player has an output tape that is physically protected from the other players.

A *signature* $\xi = (h_1, h_2, \ldots, h_k; e)$, where $k, h_1, h_2, \ldots, h_k, e$ are non-negative integers, describes the sizes of the players' hands. We define $\text{size}(\xi) = k + e$. 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 $e = |E| = d - \sum_{i=1}^{k} h_i$. In addition, we require that $H_1, H_2, \ldots, H_k, E$ partition D. (Such deals are called "legal" in [FW92b].) A randomized protocol is said to *work* for a signature ξ if, when it is run with hands from a randomly selected ξ-deal, the players each output a bit s that satisfies agreement, secrecy, and uniformity. We call such a protocol a *secret bit exchange protocol.*

In a more general setting, we consider n-bit secret key exchange for arbitrary n. The output of an n-bit secret key exchange protocol can then be used for a variety of cryptographic purposes, for example, as the key in private key cryptosystems (cf. [DH76]). We discuss n-bit secret key exchange in [FW92a, FW92b], but here we restrict our attention to a specific class of secret bit exchange protocols that does not generalize to $n > 1$.

We consider the class of *key set protocols*, obtained by generalizing a randomized protocol presented in [FW92b]. The building block of these protocols is the notion of an *opaque key set*, originally developed by Winkler [Win81a, Win81b, Win83] for use in the game of bridge, and later used by Fischer, Paterson, and Rackoff [FPR91] for secret bit exchange between two players. A key set K consists of two cards, one held by a team player P, the other held by a *different* team player Q. A key set $K = \{x, y\}$ is *opaque* if, given the information available to Eve, it is equally likely that P holds x and Q holds y or that P holds y and Q holds x. Once P and Q determine an opaque key set K that they hold, they can use it to communicate a bit r from P to Q or from Q to P that is secret from Eve. For example, if P knows that $r = 0$, then P can publicly announce that $r = 0$ if P holds x and $r = 1$ if P holds y, where x is the card held by P. If instead $r = 1$, then P would make the same statement but with x and y reversed.

During the execution of a protocol, we say a card x is *discarded* from the deck if all team players agree to play as if x is no longer part of the deck. Similarly, we say a team player P *drops out* of the protocol if the team players agree to play as if P were no longer part of the team. The basic key set protocol follows.

1. Let P be a designated team player.

2. P chooses a random card x contained in her hand and a random card y not in her hand and proposes $K = \{x, y\}$ as a key set by asking, "Does any team player hold a card in K?"

3. If another team player Q holds y, she knows that K is a key set, so she announces that she holds a card in K. P and Q are then said to be *connected* by K. The cards x and y are discarded. Whichever player of P and Q holds fewer cards exposes the remaining cards in her hand, which are discarded, and drops out of the protocol. The remaining team players go back to step 1, using the remaining cards in their hands as a "new" deal.

4. If none of the team players holds y, then K is *rejected*. In this case, x and y are discarded, and the players go back to step 1.

The execution of the protocol continues in this manner until either there are not enough cards left to complete steps 1 and 2, or until only one team player is left. In the first case, the protocol is said to *fail*. In the second case, the team players are connected by opaque key sets, and the protocol is said to *finish*. In this case, a designated player, say P_1, chooses a bit s randomly. The bit s is then communicated secretly to all the players using flooding across the key set connections. That is, P_1 communicates s secretly to each team player with whom she shares key sets using the method described above. In turn, each player learning s communicates it to the other team players with whom she shares a key set. Hence, s is a shared secret bit. For a discussion of the correctness of this protocol, see [FW92b].

In step 1, a team player P_i, *the proposer*, is chosen. By considering different rules for choosing the proposer, we obtain the class of *key set protocols.* We call such a rule a *proposing rule* and require a proposing rule to be a deterministic function of the current signature. We call the protocol that results from proposing rule $\mathcal{R}$ the *$\mathcal{R}$ key set protocol.*

Because the $\mathcal{R}$ key set protocol is randomized, it can have many different runs starting with the same ξ-deal δ. We say that the $\mathcal{R}$ key set protocol *works for* δ if it finishes on every run of δ. It follows from the analysis in [FW92b] that if the $\mathcal{R}$ key set protocol works for every ξ-deal, then it works for ξ. That is, not only does it always produce a bit s, but s satisfies secrecy, agreement, and uniformity. Hence, to show that a given $\mathcal{R}$ key set protocol works for a given signature ξ, it is sufficient to show that every run on every ξ-deal finishes; probabilities can be ignored. The following lemma shows that one can in fact restrict attention to the runs that result from a single arbitrary ξ-deal. The proof uses a simple strategy stealing argument.

Lemma 5.1 *Let ξ be a signature, let δ be a ξ-deal, and let $\mathcal{R}$ be a proposing rule. If the $\mathcal{R}$ key set protocol works for δ, then it works for ξ.*

Proof: Let $\delta = (H_1, H_2, \ldots, H_k; E)$ and $\delta' = (H_1', H_2', \ldots, H_k'; E')$ be arbitrary ξ-deals, and suppose that the $\mathcal{R}$ key set protocol works for δ. We show that the $\mathcal{R}$ key set protocol also works for δ'. Since δ' is an arbitrary ξ-deal, it will follow that the $\mathcal{R}$ key set protocol works for ξ.

Inductively assume that for all $\overline{\xi}$-deals $\overline{\delta}$ and $\overline{\delta}'$ such that $\text{size}(\overline{\xi}) < \text{size}(\xi)$, if the $\mathcal{R}$ key set protocol works for $\overline{\delta}$, then it works for $\overline{\delta}'$. Suppose that δ is dealt from deck D, and δ' is dealt from D', and let f be a player-preserving bijection from D' to D, where a bijection $f\colon D' \to D$ is said to be *player-preserving* if $x \in H_i' \Rightarrow f(x) \in H_i$.

We simultaneously construct two runs of the $\mathcal{R}$ key set protocol, one on δ and one on δ'. To distinguish the two, we refer to them as G and G' respectively. If the G' team can not propose a key set, then G' terminates. Since G and G' have the same signature, G also terminates, and either both finish or both fail. Otherwise, a key set $\{x, y\}$ is proposed in G' by some player, say P_i. Since a proposing rule is a deterministic function of the current signature, P_i is also chosen to propose in G. Moreover, it is possible for the proposed key set in G to be $\{f(x), f(y)\}$ since, in the deal δ, $f(x)$ is held by P_i and $f(y)$ is not. Furthermore, since the same player holds y in δ' as holds $f(y)$ in δ, the deals δ_1 and δ_1' that result from one iteration of the $\mathcal{R}$ key set protocol in G and G', respectively, both have the same signature, and the function f restricted to the remaining cards is still a player-preserving bijection.

Since the $\mathcal{R}$ key set protocol works for δ, it must work for δ_1. By induction, the $\mathcal{R}$ key set protocol therefore works for δ'_1. Thus, since we considered an arbitrary choice of key set in G', the $\mathcal{R}$ key set protocol works for δ'. ∎

There is a close connection between the stick game and key set protocols. Namely, a configuration $(h_1, \ldots, h_k; e; 0)$ in which it is the chooser's turn corresponds to a signature $(h_1, \ldots, h_k; e)$. A configuration in which it is the adversary's turn corresponds to a signature plus a choice of proposer. A pile P_i corresponds to team player P_i, and the pile E corresponds to player Eve. A chooser's strategy $\mathcal{S}$ in the stick game corresponds to a proposing rule $\mathcal{R}$ for the key set protocol. That is, the pile P_i is chosen in the stick game if and only if player P_i proposes in the $\mathcal{R}$ key set protocol. The adversary's response in the stick game corresponds to naming the holder of the second card of the proposed key set. Finally, a winning end configuration in the stick game corresponds to a signature in which the team trivially has a secret bit (since the team is of size at most one), and a losing end configuration in the stick game corresponds a configuration in which no key set is possible (since the team has size two or greater and all but possibly one player has run out of cards).

We show that a chooser strategy $\mathcal{S}$ succeeds on a given configuration in the stick game if and only if the $\mathcal{R}$ key set protocol works for the corresponding signature.

Lemma 5.2 (Stick Game Lemma) *Let the stick game strategy $\mathcal{S}$ correspond to the proposing rule $\mathcal{R}$. Then $\mathcal{S}$ succeeds on the configuration $(h_1, \ldots, h_k; e; 0)$ if and only if the $\mathcal{R}$ key set protocol works for $\xi = (h_1, \ldots, h_k; e)$.*

Proof: It is obvious that if the chooser wins in the stick game, then the team succeeds in obtaining a secret bit in the corresponding key set protocol. In the other direction, there is a complication in that the adversary in the stick game has complete control over which pile to match, whereas in the key set protocol, the hand containing the matching card is determined by the *a priori* deal. However, since the key set protocol is required to finish on *all* runs of the given deal, it must in particular work when the matching card of the proposed key set is in the hand corresponding to the pile chosen by the adversary in the stick game.

Specifically, let $\xi = (h_1, \ldots, h_k; e)$, let δ be a ξ-deal, and suppose that the $\mathcal{R}$ key set protocol works for ξ. Let $C = (h_1, \ldots, h_k; e; 0)$ be the stick game configuration corresponding to ξ. Inductively assume that the result holds for all configurations of size smaller than size(C).

Since the $\mathcal{R}$ key set protocol works for ξ-deal δ, either $k \leq 1$, or it is possible for the team to propose a key set. If $k \leq 1$, then by Proposition 3.1, C is winning. Otherwise, let P_i be the player chosen by $\mathcal{R}$, and consider the corresponding configuration $C_1 = (h_1, \ldots, h_k; e; i)$. Since it is possible for P_i to propose a key set, this implies that either $h_j > 0$ for some $j \neq i$, or $e > 0$. Therefore, the stick game adversary can make a move, and matches with some pile, either P_j for $j \neq i$ or

E, resulting in configuration C_2. Let Q be the player of the $\mathcal{R}$ key set protocol (possibly Eve) corresponding to the matched pile.

It is possible in the key set protocol for P_i to propose a key set whose second card is held by Q. In this case, the resulting deal is some deal δ' of signature ξ'. Since the $\mathcal{R}$ key set protocol works for ξ, it must finish for all runs of all ξ-deals. In particular, it finishes for all runs of δ, and hence must work for δ'. By Lemma 5.1, the $\mathcal{R}$ key set protocol therefore works for ξ'. The signature ξ' corresponds to C_2, so by induction, C_2 is winning, and hence C is also winning. ■

Let each team player P_i hold h_i cards and let Eve hold e cards. We define a feasible player in a signature exactly as we defined a feasible pile in a stick game configuration, i.e., P_i is *feasible* if $h_i > 1$, or if $h_i = 1$, $e = 0$, and $h_j > 1$ for all $j \neq i$. We similarly define the SFP proposing rule (where SFP now stands for smallest feasible *player*): If some team player is feasible, the feasible player with the smallest hand is chosen. (Ties are broken in favor of the lower-numbered player.) If no team player is feasible, the lowest-numbered team player with a nonempty hand is chosen, if there is one.

By Lemma 5.2, the SFP key set protocol works whenever the SFP stick game strategy is a successful chooser strategy for the corresponding stick game. In addition, the optimality of the SFP stick game strategy implies the optimality of the corresponding SFP key set protocol within the class of all key set protocols. Thus, for any proposing rule $\mathcal{R}$ and signature ξ, if the $\mathcal{R}$ key set protocol works for ξ, then the SFP key set protocol also works for ξ.

Corollary 5.3 *Let $\xi = (h_1, ..., h_k; e)$. Let $h_i \geq 1$ for $1 \leq i \leq k$, and let $\max h_i + \min h_i \geq k + e$. Then the SFP key set protocol works for ξ.*

Proof: Let $\xi = (h_1, ..., h_k; e)$. Let $h_i \geq 1$ for $1 \leq i \leq k$, and $\max h_i + \min h_i \geq k + e$, and consider the stick game configuration $C = (h_1, \ldots, h_k; e; 0)$. By Theorem 3.3, the SFP stick game strategy succeeds on C. Hence by Lemma 5.2 (Stick Game Lemma), the SFP key set protocol works for ξ. ■

Corollary 5.4 *The SFP key set protocol is optimal within the class of key set protocols.*

Proof: Suppose that the $\mathcal{R}$ key set protocol works for $\xi = (h_1, \ldots, h_k; e)$. Then by Lemma 5.2 (Stick Game Lemma), $C = (h_1, \ldots, h_k; e; 0)$ is a winning configuration. Then by Theorem 4.8, the SFP strategy for the stick game succeeds on C. Finally, by Lemma 5.2, the SFP key set protocol works for ξ. ■

References

[BCG82] E. R. Berlekamp, J. H. Conway, and R. K. Guy. *Winning Ways*, volume I. Academic Press, Inc., London, 1982.

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

[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.

[FW92a] M. J. Fischer and R. N. Wright. An efficient protocol for unconditionally secure secret key exchange. Technical Report YALEU/DCS/TR-908, Yale University, May 1992.

[FW92b] M. J. Fischer and R. N. 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.

[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.