Bounds on Secret Key Exchange Using a Random Deal of Cards*

Michael J. Fischer
Computer Science Department, Yale University, New Haven, CT 06520–8285

Rebecca N. Wright
AT&T Bell Laboratories, 600 Mountain Avenue, Room 2T-314
Murray Hill, NJ 07974

Appears in J. Cryptology, Vol. 9, No. 2, Spring 1996, pp. 71–99.

Abstract

We present a general model for communication among a "team" of players overheard by a passive eavesdropper, Eve, in which all players including Eve are given private inputs that may be correlated. We define and explore secret key exchange in this model. Our secrecy requirements are information-theoretic and hold even if Eve is computationally unlimited. In particular, we consider the situation in which the team players are dealt hands of cards of prespecified sizes from a known deck of distinct cards. We explore when the team players can use the information contained in their hands to determine a value that each team player knows exactly but Eve cannot guess.

Key words. Multiparty protocols, Correlated random variables, Key exchange, Perfect secrecy.

1 Introduction

1.1 An example

Consider a scenario in which Alice, Bob, and a computationally-unlimited eavesdropper, Eve, are playing a game of cards with a deck of four cards, J, Q, K, and A. Alice is given two cards, Bob is given one card, and the remaining card may or may not be given to Eve. Can Alice and Bob communicate publicly to agree on a bit that is secret from Eve? The answer to this question depends on what is meant by "secret", whether

*This research was supported in part by National Science Foundation grant IRI–9015570. The second author's research was completed while at Yale University.

Eve is allowed to look at the remaining card, and whether Alice and Bob are allowed to use randomization.

If Eve is not allowed to look at the remaining card, the following deterministic protocol achieves *perfect* secret bit exchange, in which Eve considers both values equally likely at the end of every run of the protocol. Alice says whichever of the following statements is true:

- "I hold $\{J, Q\}$ or $\{K, A\}$."
- "I hold $\{J, K\}$ or $\{Q, A\}$."
- "I hold $\{J, A\}$ or $\{Q, K\}$."

From Alice's message and Bob's hand, Bob can determine Alice's hand, so Alice and Bob both know the truth value of the statement "Alice holds J", and can agree on this value as their secret bit. On the other hand, Eve considers it equally likely that this statement is true or false, so does not learn the secret bit.

If Eve is allowed to look at the remaining card, the following randomized protocol achieves perfect secret bit exchange. First, Alice randomly chooses a card x in her hand and a card y not in her hand, and asks Bob "Do you hold one of the two cards $\{x, y\}$?" If Bob says yes, then Alice and Bob know which of them holds x and which holds y, but Eve considers both situations equally likely. Hence, Alice and Bob can agree on a secret bit, for example, by the truth value of the statement "Alice holds the smaller valued card of x and y." On the other hand, if Bob says no, then Alice and Bob each hold one of the two remaining cards z and q and can determine the truth value of the statement "Alice holds the smaller valued card of z and q," again obtaining the desired secret bit.

Finally, if Eve is allowed to look at the remaining card and Alice and Bob are not allowed to use randomization, then even *weak* secret bit exchange, in which we require only that Eve consider both values possible at the end of each run of the protocol, is not possible. Note that if Eve learns either player's hand, then she can learn the secret bit by simulating that player. It can be shown that if either player sends a message that depends on his or her hand, then it will sometimes be possible for Eve to learn that player's hand. Hence, in order to avoid the possibility of Eve learning the secret bit, neither player can ever send a message that depends on his or her hand. It follows that there is only one possible sequence of messages, and hence each player's output is a function only of his or her hand. Thus, for example, if Bob outputs v when he holds J, Alice must output v whenever she does not hold J in order to guarantee that their outputs always agree. In this case, if Eve holds J, then Eve knows Alice does not hold J and will output v, so she has learned the secret bit. A formal proof of this result involves a detailed case analysis.

To summarize this example, if Eve does not see the remaining card or if Alice and Bob can use randomization, then Alice and Bob can agree on a perfectly secret bit. If

Eve sees the remaining card or Alice and Bob are required to behave deterministically, then Alice and Bob cannot agree even on a weakly secret bit.

The arguments of the correctness of protocols and the nonexistence of protocols presented in the above example are informal and rely on intuition. However, intuition may be misleading when dealing with issues such as secrecy and shared knowledge, so formal definitions of secret key exchange are needed. To this end, we formalize a model for communication among a "team" of players given possibly correlated inputs that are drawn from some known joint distribution. A passive eavesdropper, Eve, hears the communication between the players and is also given an input that may be correlated with the inputs of the players. The use of correlated random variables to solve cryptographic and communication problems has been studied in several different contexts (cf. [1, 2, 3, 5, 7, 8, 9, 10, 13, 15]). Our model is sufficiently general to capture all of these cryptographic and communication problems.

1.2 Our work

We define and explore the problem of *multiparty secret key exchange* in our model. Briefly, the problem of N-valued multiparty secret key exchange is for a team of players to choose a value v from a known set of N values. After the players communicate, each team player must know v, but v must be unknown to Eve. An adequate notion of secrecy must depend not only on the protocol being executed, but on any relevant knowledge Eve may have that is external to the protocol. We provide precise mathematical definitions of the multiparty secret key exchange problem that take Eve's knowledge into account, and allow us to determine whether a given protocol achieves secret key exchange with respect to any particular "type of knowledge" for Eve.

We consider two kinds of secret key exchange, *perfect* and *weak*. N-valued perfect secret key exchange requires that Eve consider all N possible values for v equally likely, while N-valued weak secret key exchange requires only that Eve consider all N values for v possible. The work of [2, 3, 5] can be formalized according to our definition of 2-valued perfect secret key exchange. Two-valued weak secret key exchange is equivalent to the concept of "sharing a secret" used in [1].

We investigate the properties of secret key exchange protocols. It follows easily from our definitions that perfect secrecy implies weak secrecy and that giving Eve external knowledge can only help her. We explore how the requirements of a secret key exchange protocol restrict the inputs and behavior of the players. In particular, we show that secret key exchange is not possible if the players' inputs are not correlated.

Our model is quite general and admits on the extreme ends the case where the players' inputs are equal and the case where the players' inputs are independent. In the first case, the players can use their inputs as a secret key. We show in Section 3 that secret key exchange is not possible in the second case. We are interested in the borderline between possibility and impossibility of secret key exchange. In order to approach this problem, we focus our attention on inputs consisting of hands of prespecified sizes from a randomly shuffled deck of cards.

A random deal of cards is an example of sampling without replacement. 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 indecipherable to the opponents, even though the protocol was known to them [6, 13, 14, 15]. Fischer, Paterson and Rackoff [2] and Beaver, Haber and Winkler [1] carried this idea further, using deals of cards for secret bit transmission between two players. In this paper, we consider the use of a random deal of cards for multiparty, multivalued, secret key exchange. A *signature* $(s_1, \ldots, s_k; d)$ specifies the hand size s_i for each player and the deck size d. The perfect (respectively weak) capacity of a signature is the largest N such that N-valued perfect (weak) secret key exchange is possible when the deal is chosen randomly as specified by the given signature. We investigate bounds on the capacity of different signatures.

Note that if $N = 1$ or if there is only one team player, N-valued secret key exchange is not of interest. Beaver, Haber and Winkler [1] and Fischer, Paterson and Rackoff [2] have studied the case where $N = 2$ and there are only two team players. Protocols performing multiparty secret key exchange for certain classes of deals appear in [3, 5, 16]. Most previous work in this area focuses on exhibiting secret key exchange protocols along with informal arguments establishing their correctness [2, 3, 5]. The previously existing upper bound arguments on the capacity of certain signatures [2, 3] are informal and not mathematically rigorous. Our formal model allows for careful analysis of protocols and careful proof of upper bounds.

We present two bounds on the capacity of signatures. First, we show that the weak capacity of $(1, \ldots, 1; k)$ is 1 if $k \geq 3$ by showing that 2-valued weak secret key exchange is not possible when k team players each hold one card from a deck of k cards. This is the first result showing that even if the team holds all the cards and no player's hand is empty, secret key exchange is not always possible. (By way of contrast, 2-valued secret key exchange is always possible if each of k players holds 2 cards from a deck of $2k$ cards [16].) Second, we exhibit an upper bound on the perfect capacity of any signature.

2 Multiparty Protocols and Systems

We consider a *team* of players P_1 through P_k. We denote the number of team players by k throughout the paper, and denote the set $\{1, \ldots, k\}$ by K. We will frequently use k-tuples to describe a collection of items, one for each player. Given any k-tuple x, we denote the ith component (P_i's component) of x by $\langle x \rangle_i$.

We use a synchronous distributed model of computation in which communication occurs in rounds. All protocols terminate in a fixed finite number of rounds. Each player is given a private input that will generally be chosen at random before the protocol begins. In a round, each of the players simultaneously broadcasts a message to all of the other players. The message sent by P_i at a given round depends on P_i's input and the messages sent by the team in previous rounds. On termination, each player P_i produces a private output that depends on her own input and the messages sent by the team in all rounds. We define protocols formally in Section 2.1.

We describe how the players' random inputs are generated in Sections 2.2. The information given to Eve is formalized in Section 2.3. Briefly, a global value is chosen randomly according to a known, fixed distribution. Each player has a view of the global value that constitutes her private input. Eve also gets a view of the global value. In general, the global value and the players' views will be chosen so that the players' inputs consist of correlated values (such as the hands of a deal of cards) as well as independent random values that play the role of private coin flips or dice rolls for the individual players.

2.1 Protocols

Formally, a *protocol* is a 7-tuple $\mathcal{P} = (k, t, U, V, M, \mu, \nu)$.

- k is the number of players.
- t is the number of rounds.
- $U = U_1 \times \cdots \times U_k$ is the input set.
- V is the output set.
- M is the set of messages.
- μ is a k-tuple $(\mu_1, \ldots, \mu_k)$ of *message functions*.
- ν is a k-tuple $(\nu_1, \ldots, \nu_k)$ of *output functions*.

An element $u \in U$ is called an *input vector* or simply an *input*. The component $\langle u \rangle_i$ is *the input for* P_i. U_i is the input set for P_i.

A k-tuple $m \in M^k$ is called a *message vector*. It represents the messages sent by all team players in a given round; the component $\langle m \rangle_i$ is the message sent by P_i. A sequence of at most t message vectors is called a *conversation*. A conversation τ is *complete* if $|\tau| = t$ and *partial* if $|\tau| < t$. We let c denote the set of conversations, cc denote the set of complete conversations, and pc denote the set of partial conversations. Given a conversation τ, we let τ_j denote the jth message vector of τ, and for $\ell \leq |\tau|$, we write $\tau[\ell] = (\tau_1, \ldots, \tau_\ell)$ to denote the conversation consisting of the length ℓ prefix of τ. We denote the concatenation of a partial conversation τ and a message vector m by $\tau \cdot m$ or τm, so $\tau \cdot m = \tau m = (\tau_1, \ldots, \tau_{|\tau|}, m)$.

The message function $\mu_i : U_i \times \mathsf{pc} \to M$ specifies the messages for P_i to send. Let $a_i \in U_i$, $\ell < t$ and $\tau \in \mathsf{pc}$. The message $\mu_i(a_i, \tau)$ is the message that P_i sends at round $\ell + 1$ when P_i has input a_i and the conversation through round ℓ is τ. The output function $\nu_i : U_i \times \mathsf{cc} \to V$ specifies the output for P_i. Let $a_i \in U_i$ and $\sigma \in \mathsf{cc}$. The value $\nu_i(a_i, \sigma)$ is the output for P_i when P_i has input a_i and the complete conversation is σ.

When the protocol $\mathcal{P}$ is clear from context, we will use the notation k, t, U, U_i, V, M, μ, μ_i, ν, ν_i, c, cc and pc as above. Otherwise, we attach $\mathcal{P}$ as a superscript.

Given an input $u \in U$, we say σ is a *conversation of* u if σ is complete and $\langle \sigma_\ell \rangle_i = \mu_i(\langle u \rangle_i, \sigma[\ell-1])$ for all $i \in K$ and $1 \leq \ell \leq t$. It is easily seen that for each input u, σ is unique. This is because the messages of the first round of σ are completely determined by u, and successive rounds of σ are determined by u and the previous rounds of σ. We denote this unique conversation σ by $\mathrm{conv}(u)$. We denote P_i's output $\nu_i(\langle u \rangle_i, \mathrm{conv}(u))$ by $\mathrm{out}_i(u)$, and we denote the vector $(\mathrm{out}_1(u), \ldots, \mathrm{out}_k(u))$ of all players' outputs by $\mathrm{out}(u)$.

It is possible to "interpolate" between a number of input vectors to construct a new input vector (the "interpolant") by giving each team player P_i his input from one of the original vectors u_i. Let ℓ be the last round where the conversations of all the original vectors are the same. Because the behavior of the team at each round is completely determined by the input vector and the messages received up to that round, the conversation of the interpolant agrees with the original conversations up to round ℓ. Furthermore, each player P_i sends the same message at round $\ell+1$ with the interpolant as input as he did with the original vector u_i as input.

We say that two input vectors u and u' *touch at coordinate* i, or simply *touch*, if $\langle u \rangle_i = \langle u' \rangle_i$. If u and u' touch at coordinate i, we write $u =_i u'$. Obviously, $=_i$ is an equivalence relation.

Let $U' \subseteq U$. We say that u is *an interpolant of* U' (also u *interpolates* U') if for every $i \in K$, there is some $u' \in U'$ such that $u =_i u'$. We call any k-tuple $(u_1, \ldots, u_k)$ a U'*-derivation* of u if $u_i \in U'$ and $u =_i u_i$ for all $i \in K$. Note that u interpolates U' if and only if there exists a U'-derivation of u.

Lemma 2.1 (First Interpolation Lemma) *Let $\mathcal{P}$ be a protocol, let $\tau \in \mathsf{c}$, let $\ell = |\tau|$, and let $U' \subseteq U$ such that $\mathrm{conv}(u)[\ell] = \tau$ for all $u \in U'$. Let $\widehat{u}$ interpolate U' and let $(u_1, \ldots, u_k)$ be a U'-derivation of $\widehat{u}$. Then*

1. $\mathrm{conv}(\widehat{u})[\ell] = \tau$.
2. *If $\ell < t$, then* $\mathrm{conv}(\widehat{u})_{\ell+1} = (\langle \mathrm{conv}(u_1)_{\ell+1} \rangle_1, \ldots, \langle \mathrm{conv}(u_k)_{\ell+1} \rangle_k)$.
3. *If $\ell = t$, then* $\mathrm{out}(\widehat{u}) = (\mathrm{out}_1(u_1), \ldots, \mathrm{out}_k(u_k))$.

Proof: Suppose the conditions of the lemma.

1. Since $\mathrm{conv}(u)[\ell] = \tau$ for all $u \in U'$, we have $\mu_i(\langle u \rangle_i, \tau[j-1]) = \langle \tau_j \rangle_i$ for all $u \in U'$, $i \in K$, and $1 \leq j \leq \ell$. It follows that $\mathrm{conv}(\widehat{u})[\ell] = \tau$.
2. Suppose $\ell < t$. Then by (1), $\mathrm{conv}(\widehat{u})[\ell] = \tau$. It follows that $\mathrm{conv}(\widehat{u})_{\ell+1} = (\mu_1(\langle u_1 \rangle_1, \tau), \ldots, \mu_k(\langle u_k \rangle_k, \tau)) = (\langle \mathrm{conv}(u_1)_{\ell+1} \rangle_1, \ldots, \langle \mathrm{conv}(u_k)_{\ell+1} \rangle_k)$.
3. Suppose $\ell = t$. Then by (1), $\mathrm{conv}(\widehat{u})[\ell] = \mathrm{conv}(\widehat{u}) = \tau$. Thus $\mathrm{out}(\widehat{u}) = (\nu_1(\langle u_1 \rangle_1, \tau), \ldots, \nu_k(\langle u_k \rangle_k, \tau)) = (\mathrm{out}_1(u_1), \ldots, \mathrm{out}_k(u_k))$. ■

2.2 Sources

A protocol specifies the possible inputs to the players and how the players behave given these inputs. We are generally interested in the case that inputs are generated by a random source. Before proceeding, we introduce some definitions and notations from basic probability theory.

Given an arbitrary distribution $\mathcal{G}$ over an arbitrary finite set Γ, we write $\Pr_{\mathcal{G}}(g)$ to denote the probability assigned by $\mathcal{G}$ to $g \in \Gamma$. A subset $X \subseteq \Gamma$ is called an *event*. We write $\Pr_{\mathcal{G}}[X]$ to denote the probability $\sum_{g \in X} \Pr_{\mathcal{G}}(g)$ assigned to X by $\mathcal{G}$. When the distribution $\mathcal{G}$ is clear from context, we omit the subscript and write simply $\Pr(g)$ and $\Pr[X]$. We say an element g is *feasible* if $\Pr(g) > 0$. We say an event X is *feasible* if $\Pr[X] > 0$ or, equivalently, if X contains a feasible element. We write $\mathrm{feas}(X)$ to denote the set $\{g \in X : g \text{ is feasible}\}$.

A function f over domain Γ is called a *random variable*. The event $\{g \in \Gamma : f(g) = x\}$ is denoted by $f^{-1}(x)$. The random variables $f_1, \ldots, f_k$ are *independent* if $\Pr\left[\bigcap_{i=1}^k f_i^{-1}(x_i)\right] = \prod_{i=1}^k \Pr\left[f_i^{-1}(x_i)\right]$ for all $x_1, \ldots, x_k$. The events $X_1, \ldots, X_k$ are *independent* if the random variables $f_1, \ldots, f_k$ defined by $f_i(g) = 1$ if $g \in X$ and $f_i(g) = 0$ if $g \notin X$ are independent. We say an event X *respects* a random variable f if $f(g_1) = f(g_2)$ implies that g_1 and g_2 are either both elements of X or both not elements of X. Note that if $f_1, \ldots, f_k$ are independent random variables and $X_1, \ldots, X_k$ are events such that each X_i respects f_i, then $X_1, \ldots, X_k$ are independent.

Given a set of distributions $\mathcal{G}_i$ on Γ_i, we define the distribution $\mathcal{G} = \mathcal{G}_1 \times \cdots \times \mathcal{G}_k$ on $\Gamma_1 \times \cdots \times \Gamma_k$ by $\Pr_{\mathcal{G}}((g_1, \ldots, g_k)) = \prod_{i=1}^k \Pr_{\mathcal{G}_i}(g_i)$. Note that if $\mathcal{G} = \mathcal{G}_1 \times \cdots \times \mathcal{G}_k$ and $f_1, \ldots, f_k$ are random variables over $\Gamma_1 \times \cdots \times \Gamma_k$ such that each f_i depends only on the i^{th} component of its argument, then $f_1, \ldots, f_k$ are independent.

A source specifies how the inputs to a protocol are generated. Specifically, the players' inputs are chosen randomly according to some fixed distribution described by a source. Formally, a *source* is a quadruple $\mathcal{T} = (\Omega, \mathcal{F}, U, \theta)$, where

- Ω is a finite set.
- $\mathcal{F}$ specifies a probability distribution on Ω.
- $U = U_1 \times \cdots \times U_k$ is a k-tuple of sets.
- $\theta = (\theta_1, \ldots, \theta_k)$, where each $\theta_i : \Omega \to U_i$ is a *view function.*

We sometimes say $\mathcal{T}$ is a *source for* U. When a source is clear from context, we will use the notation Ω, $\mathcal{F}$, U, U_i, θ, and θ_i as specified above. When we wish to make a source $\mathcal{T}$ explicitly clear, we use $\mathcal{T}$ as a superscript.

An element $\omega \in \Omega$ is called a *point* or a *global value*. Each view function θ_i is a random variable. Given a point $\omega \in \Omega$, we define the input $\theta(\omega) = (\theta_1(\omega), \ldots, \theta_k(\omega))$, and given an input u, we write $\theta^{-1}(u)$ to denote the event $\{\omega : \theta(\omega) = u\}$. A source $\mathcal{T}$ for U can itself be regarded as a distribution on U, where $\Pr_{\mathcal{T}}(u) = \Pr_{\mathcal{F}}[\theta^{-1}(u)]$. $\mathcal{T}$ also induces a distribution on each player P_i's input set $U_i^{\mathcal{T}}$.

A source $\mathcal{S}$ for U is *canonical* if $\Omega = U$ and $\theta_i(u) = \langle u \rangle_i$ for all $u \in U$. We allow noncanonical sources in order to allow greater flexibility in the information given to Eve. (See Section 2.3.) The following proposition states that for any distribution on U, it is always possible to construct a canonical source for U that realizes this distribution.

Proposition 2.2 *Let $U = U_1 \times \cdots \times U_k$ be a set, and let $\mathcal{F}$ be a distribution over U. Then there exists a canonical source $\mathcal{S}$ for U such that $\Pr_{\mathcal{S}}(u) = \Pr_{\mathcal{F}}(u)$ for all $u \in U$.*

We say that u *spans* U' if u touches every $u' \in U'$. We say a set $U' \subseteq U$ is *coverable* if there exists a feasible interpolant u of U' that spans U'. We also say u *covers* U'.

The special case of $U' = \{u_0, u_1\}$ arises frequently in the sequel. The following propositions are immediate from the definitions.

Proposition 2.3 *Let $\mathcal{T}$ be a source. If $\{u_0, u_1\} \subseteq \mathrm{feas}(U)$ and u_0 touches u_1, then $\{u_0, u_1\}$ is coverable.*

Proposition 2.4 *Let $\mathcal{T}$ be a source. If $u \in \mathrm{feas}(U) - \{u_0, u_1\}$ and u interpolates $\{u_0, u_1\}$, then $\{u_0, u_1\}$ is coverable.*

The distribution that $\mathcal{T}$ defines on $U^{\mathcal{T}}$ can incorporate both correlated and independent initial information for the team players. In the study of randomized algorithms and protocols, it is often desirable to consider private independent random information (such as coin flips) as being separate from any correlated initial information. To this end, we allow any source $\mathcal{T}$ to be augmented by additional independent randomization. Formally, a source $\mathcal{S}$ is a *randomized extension of* $\mathcal{T}$ if there exist finite sets $R_1, \ldots, R_k$ and distributions $\mathcal{R}_1, \ldots, \mathcal{R}_k$ such that $\mathcal{R}_i$ is a distribution on R_i for each i and

- $U^{\mathcal{S}} = (R_1, U_1^{\mathcal{T}}) \times \cdots \times (R_k, U_k^{\mathcal{T}})$.
- $\Pr_{\mathcal{S}}((r_1, q_1), \ldots, (r_k, q_k)) = \Pr_{\mathcal{T}}(q_1, \ldots, q_k) \cdot \prod_{i=1}^{k} \Pr_{\mathcal{R}_j}(r_i)$.

Here, r_i models the independent private random information for player P_i. Let $u = ((r_1, q_1), \ldots, (r_k, q_k)) \in U^{\mathcal{S}}$. We call $\mathrm{corr}(u) = (q_1, \ldots, q_k) \in U^{\mathcal{T}}$ the *correlated part of the input*; $\langle \mathrm{corr}(u) \rangle_i = q_i$ is *P_i's share* of $\mathrm{corr}(u)$. We call $(r_1, \ldots, r_k)$ the *independent part of the input*, and we denote r_i by $\mathrm{ind}_i(u)$. Note that q is feasible as an input of $\mathcal{T}$ if and only if q is the correlated part of a feasible input in $\mathcal{S}$.

We say two sources $\mathcal{S}$ and $\mathcal{S}'$ are *team-equivalent* if $U^{\mathcal{S}} = U^{\mathcal{S}'}$ and $\Pr_{\mathcal{S}}(u) = \Pr_{\mathcal{S}'}(u)$ for all $u \in U^{\mathcal{S}}$. Team-equivalence defines an equivalence relation on sources. Proposition 2.5 states that team-equivalence and randomized extensions behave nicely together.

Proposition 2.5 *Let $\mathcal{S}$ be a randomized extension of $\mathcal{T}$, let $\mathcal{S}'$ be team-equivalent to $\mathcal{S}$, and let $\mathcal{T}'$ be team-equivalent to $\mathcal{T}$. Then $\mathcal{S}'$ is a randomized extension of $\mathcal{T}'$.*

2.3 Views for Eve

Given a source $\mathcal{S}$ with global value set Ω, a *view function for Eve* is a function $\theta_e : \Omega \to U_e$, where U_e is an arbitrary set. This formalizes the information that Eve is given about the global value. She also hears the conversation of the team players. Thus, if ω is the chosen global value, Eve is given the view $\theta_e(\omega)$ and hears the conversation $\mathrm{conv}(\theta(\omega))$.

A view function θ_e for Eve is *empty* if $\theta_e(\omega) = \theta_e(\omega')$ for all $\omega, \omega' \in \Omega$. Hence, an empty view gives Eve no additional information beyond the conversation. Note that if Eve were only given empty views, it would be sufficient to consider only canonical sources. However, the more general definition of sources allows consideration of information for Eve such as "Eve sees a random card from Alice's hand".

2.4 Systems

Together, a protocol $\mathcal{P}$ and a source $\mathcal{T}$ for $U^{\mathcal{P}}$ are a called a *system*, denoted $\mathcal{P}_{\mathcal{T}}$. We say $\mathcal{P}_{\mathcal{T}}$ is *N-valued* if $|V^{\mathcal{P}}| = N$. Since a source for $U^{\mathcal{P}}$ defines a distribution on $U^{\mathcal{P}} = U^{\mathcal{T}}$, $\mathcal{P}_{\mathcal{T}}$ induces a distribution on conversations and on the players' outputs. We extend the term 'feasible' to conversations: we say τ is *feasible* if there is a feasible input $u \in U^{\mathcal{T}}$ such that $\mathrm{conv}(u)[\ell] = \tau$. We say a system $\mathcal{P}_{\mathcal{S}}$ is a *randomized $\mathcal{T}$-system* if $\mathcal{S}$ is a randomized extension of $\mathcal{T}$.

Lemma 2.6 (Second Interpolation Lemma) *Let $\mathcal{P}_{\mathcal{S}}$ be a randomized $\mathcal{T}$-system, let $U' \subseteq \mathrm{feas}(U^{\mathcal{S}})$, and let $\widehat{u}$ interpolate U'. If $\mathrm{corr}(\widehat{u})$ is feasible, then $\widehat{u}$ is feasible.*

Proof: Suppose the conditions of the lemma and let $(u_1, \ldots, u_k)$ be a U'-derivation of $\widehat{u}$. Then $\Pr_{\mathcal{S}}(\widehat{u}) = \Pr_{\mathcal{T}}(\mathrm{corr}(\widehat{u})) \cdot \prod_{j=1}^{k} \Pr_{\mathcal{R}_j}(\mathrm{ind}_j(\widehat{u}))$. Since every $u \in U'$ is feasible, then for $i \in K$,

$$\Pr_{\mathcal{S}}(u_i) = \Pr_{\mathcal{T}}(\mathrm{corr}(u_i)) \cdot \prod_{j=1}^{k} \Pr_{\mathcal{R}_j}(\mathrm{ind}_j(u_i)) > 0.$$

Thus, in particular, $\Pr_{\mathcal{R}_i}(\mathrm{ind}_i(u_i)) > 0$ for $i \in K$. If, in addition, $\mathrm{corr}(\widehat{u})$ is feasible, then $\Pr_{\mathcal{T}}(\mathrm{corr}(\widehat{u})) > 0$. Hence, $\Pr_{\mathcal{S}}(\widehat{u}) = \Pr_{\mathcal{T}}(\mathrm{corr}(\widehat{u})) \prod_{i=1}^{k} \Pr_{\mathcal{R}_i}(\mathrm{ind}_i(u_i)) > 0$, so $\widehat{u}$ is feasible. ■

3 Secret Key Exchange

"Secret key exchange" is used informally to mean the following. A "key" is a value that is chosen randomly from some fixed set of values. A key is "exchanged" if all the players learn the key. A key is "secret" if a passive computationally-unlimited eavesdropper, Eve, who may have some information about the players' inputs, cannot learn the key. We formalize each of these notions independently, as *uniformity*, *agreement*, and *secrecy*.

Uniformity restricts the *a priori* probability of an output. Secrecy restricts the relation between an output's *a priori* probability and its *a posteriori* probability. Hence, together uniformity and secrecy restrict the *a posteriori* probability. Uniformity and secrecy are both defined in two strengths: perfect and weak. The perfect uniformity and perfect secrecy conditions together imply that Eve has *no information* about the players' outputs, while the weak uniformity and weak secrecy conditions imply that Eve does not learn the players' outputs *with certainty*.

These conditions may also be useful for defining other problems in our model. For example, a system could be considered to perform secret message transmission if secrecy and agreement are satisfied along with a third condition that the output values must be equal to the specified message given to the designated sender as part of his view.

The remainder of this section is organized as follows. Section 3.1 defines the agreement, uniformity and secrecy conditions. Section 3.2 shows two results relating the behavior of individual players and the behavior of the team as a whole. These results are used later in the proof of Theorem 7.2. Finally, Section 3.3 explores how the agreement, uniformity, and secrecy conditions restrict the behavior of the players and shows that secret key exchange is not possible if the players' inputs are not correlated (Theorem 3.11).

3.1 Conditions for secret key exchange

Fix a system $\mathcal{P}_{\mathcal{S}}$ and a view function θ_e for Eve, and let $i, j \in K$, $v \in V$, $\sigma \in \mathsf{cc}$, and $a_e \in U_e$. We define several events over Ω.

$$\begin{aligned} \mathrm{O}_i(v) &= \{\omega : \mathrm{out}_i(\theta(\omega)) = v\} \\ \mathrm{C}(\sigma) &= \{\omega : \mathrm{conv}(\theta(\omega)) = \sigma\} \\ \mathrm{E}(a_e) &= \{\omega : \theta_e(\omega) = a_e\} \end{aligned}$$

Thus $\mathrm{O}_i(v)$ is the event that P_i outputs v, $\mathrm{C}(\sigma)$ is the event that the conversation is σ, and $\mathrm{E}(a_e)$ is the event that Eve has view a_e. The events $\mathrm{O}_i(v)$ and $\mathrm{C}(\sigma)$ depend only on $\mathcal{P}_{\mathcal{S}}$, while the event $\mathrm{E}(a_e)$ depends on $\mathcal{P}_{\mathcal{S}}$ and θ_e.

We say $\mathcal{P}_{\mathcal{S}}$ satisfies agreement if the following condition holds.

- **Agreement**: $\Pr[\mathrm{O}_i(v_1) \cap \mathrm{O}_j(v_2)] = 0$ for all $i, j \in K$ and all pairs $v_1, v_2 \in V$ such that $v_1 \neq v_2$.

Thus, $\mathcal{P}_{\mathcal{S}}$ satisfies agreement if and only if the outputs of all team players agree at every feasible point.

We define two uniformity conditions to capture two types of distributions on the players' outputs.

- **Perfect uniformity**: $\Pr[\mathrm{O}_i(v_1)] = \Pr[\mathrm{O}_i(v_2)]$ for all $i \in K$ and all $v_1, v_2 \in V$.

- **Weak uniformity**: $\Pr[\mathrm{O}_i(v)] > 0$ for all $i \in K$ and all $v \in V$.

Thus, $\mathcal{P}_{\mathcal{S}}$ satisfies perfect uniformity if each team player's output is uniformly distributed over the output set, while $\mathcal{P}_{\mathcal{S}}$ satisfies weak uniformity if each team player outputs each value with positive probability.

Analogously, we define two levels of secrecy that limit the amount of information Eve is given by her view and the conversation. While the agreement and uniformity conditions apply to a system, the secrecy conditions apply to a system together with a view function for Eve. If the perfect (weak) secrecy condition holds, we say $\mathcal{P}_{\mathcal{S}}$ satisfies perfect (weak) secrecy *against* θ_e.

- **Perfect secrecy**: $\Pr[\mathrm{E}(a_e) \cap \mathrm{C}(\sigma) \cap \mathrm{O}_i(v)] = \Pr[\mathrm{E}(a_e) \cap \mathrm{C}(\sigma)] \cdot \Pr[\mathrm{O}_i(v)]$ for all $a_e \in U_e$, $\sigma \in \mathsf{cc}$, $i \in K$, and $v \in V$.
- **Weak secrecy**: If $\Pr[\mathrm{E}(a_e) \cap \mathrm{C}(\sigma)] > 0$ and $\Pr[\mathrm{O}_i(v)] > 0$, then $\Pr[\mathrm{E}(a_e) \cap \mathrm{C}(\sigma) \cap \mathrm{O}_i(v)] > 0$ for all $a_e \in U_e$, $\sigma \in \mathsf{cc}$, $i \in K$, and $v \in V$.

The perfect secrecy condition, formulated as an independence condition, is essentially Shannon's formulation of perfect secrecy [12]. $\mathcal{P}_{\mathcal{S}}$ satisfies perfect secrecy against θ_e if each team player's output is independent of the information available to Eve, i.e. her view and the conversation. Equivalently, perfect secrecy requires that Eve's probability of guessing a player's output correctly be the same whether or not she takes into account her view and the conversation.

Weak secrecy, on the other hand, requires only that an eavesdropper not be able to rule out any output for any player. Specifically, weak secrecy requires that Eve consider each initially possible output for each team player to still be possible after hearing the conversation. Note that the weak secrecy condition could be equivalently formulated based on conditional probability to say that if $\Pr[\mathrm{E}(a_e) \cap \mathrm{C}(\sigma)] > 0$ and $\Pr[\mathrm{O}_i(v)] > 0$, then $\Pr[\mathrm{O}_i(v) \mid \mathrm{E}(a_e) \cap \mathrm{C}(\sigma)] > 0$.

Proposition 3.1 *Let $\mathcal{P}_{\mathcal{S}}$ be a system and let θ_e be a view function for Eve. If $\mathcal{P}_{\mathcal{S}}$ satisfies perfect uniformity, then $\mathcal{P}_{\mathcal{S}}$ satisfies weak uniformity. If $\mathcal{P}_{\mathcal{S}}$ satisfies perfect secrecy against θ_e, then $\mathcal{P}_{\mathcal{S}}$ satisfies weak secrecy against θ_e.*

Proposition 3.2 shows that secrecy against an empty view can be rewritten without reference to Eve's view.

Proposition 3.2 *Let $\mathcal{P}_{\mathcal{S}}$ be a system and let θ_e be an empty view for Eve.*

1. *$\mathcal{P}_{\mathcal{S}}$ satisfies perfect secrecy against θ_e if and only if* $\Pr[\mathrm{C}(\sigma) \cap \mathrm{O}_i(v)] = \Pr[\mathrm{C}(\sigma)] \cdot \Pr[\mathrm{O}_i(v)]$ *for all $\sigma \in \mathsf{cc}$, $i \in K$, and $v \in V$.*
2. *$\mathcal{P}_{\mathcal{S}}$ satisfies weak secrecy against θ_e if and only if* $\Pr[\mathrm{C}(\sigma)] > 0$ *and* $\Pr[\mathrm{O}_i(v)] > 0$ *imply* $\Pr[\mathrm{C}(\sigma) \cap \mathrm{O}_i(v)] > 0$ *for all $\sigma \in \mathsf{cc}$, $i \in K$, and $v \in V$.*

Let θ_e and θ'_e be view functions for Eve. We say θ_e is a *refinement* of θ'_e if for all $\omega_0, \omega_1 \in \Omega$, $\theta_e(\omega_0) = \theta_e(\omega_1) \Rightarrow \theta'_e(\omega_0) = \theta'_e(\omega_1)$. Proposition 3.3 states that giving Eve more information in the form of a refined view can only help her.

Proposition 3.3 *Let θ_e be a refinement of θ'_e. If $\mathcal{P}_{\mathcal{S}}$ satisfies perfect (weak) secrecy against θ_e, then $\mathcal{P}_{\mathcal{S}}$ satisfies perfect (weak) secrecy against θ'_e.*

Among other things, Proposition 3.3 implies that if secrecy against any view is satisfied, then secrecy against any empty view is satisfied. In particular, since every empty view is trivially a refinement of every other empty view, Proposition 3.3 implies that secrecy against one empty view is satisfied if and only if secrecy against any other empty view is satisfied. We consider the empty view θ^*_e defined by $\theta^*_e(x) = \emptyset$ for all x to be a canonical empty view, and we refer to it as *the* empty view. By the above, a system $\mathcal{P}_{\mathcal{S}}$ satisfies secrecy against θ^*_e if and only if $\mathcal{P}_{\mathcal{S}}$ satisfies secrecy against every empty view.

We say a property *respects* team-equivalence if, for every protocol $\mathcal{P}$ and every pair of team-equivalent sources $\mathcal{S}$ and $\mathcal{S}'$ for $U^{\mathcal{P}}$, $\mathcal{P}_{\mathcal{S}}$ satisfies the property if and only if $\mathcal{P}_{\mathcal{S}'}$ satisfies the property. Since the team players behave the same given inputs generated by team-equivalent sources, the following proposition holds.

Proposition 3.4 *The following properties respect team-equivalence: agreement, weak uniformity, perfect uniformity, weak secrecy against the empty view, perfect secrecy against the empty view.*

3.2 Behavior of the players

In this section, we examine the relation between the behavior of individual players and the behavior of the team as a whole. To this end, we define some additional events. For $i \in K$, $v \in V$, and $\sigma \in \mathsf{cc}$, let

$$\begin{array}{rcl} \mathrm{O}(v) & = & \bigcap_{i=1}^{k} \mathrm{O}_i(v) \\ \mathrm{CO}(\sigma, v) & = & \mathrm{C}(\sigma) \cap \mathrm{O}(v) \end{array}$$

Thus $\mathrm{O}(v)$ is the event that v is output by all players and $\mathrm{CO}(\sigma, v)$ is the event that the conversation is σ and all players output v.

We are also interested in the behavior of individual players with regard to an arbitrary complete conversation σ and output v. We define several events that express whether player P_i "would" behave a certain way if given the chance.

$$\begin{array}{rcl} \overline{\mathrm{O}}_i(\sigma, v) & = & \{\omega : \nu_i(\theta_i(\omega), \sigma) = v\} \\ \overline{\mathrm{C}}_i(\sigma) & = & \{\omega : \mu_i(\theta_i(\omega), \sigma[\ell - 1]) = \langle \sigma_\ell \rangle_i \text{ for } 1 \le \ell \le t\} \\ \overline{\mathrm{CO}}_i(\sigma, v) & = & \overline{\mathrm{C}}_i(\sigma) \cap \overline{\mathrm{O}}_i(\sigma, v) \end{array}$$

These events are somewhat subtle, in that they are discussing hypothetical situations. $\overline{\mathrm{O}}_i(\sigma, v)$ is the event that P_i would output v if presented with the conversation σ. $\overline{\mathrm{C}}_i(\sigma)$ is the event that P_i would play according to σ if presented with any prefix of σ. $\overline{\mathrm{CO}}_i(\sigma, v)$ is the event that P_i would play according to σ if presented with any prefix of σ and would output v if presented with σ.

Lemma 3.5 states the intuitive fact that for each point ω, if each player plays according to σ when presented with any prefix of σ, then σ is the conversation of $\theta(\omega)$. Lemma 3.6 states that if each player plays according to σ when presented with any prefix of σ and outputs v when presented with σ, then all players play according to σ and output v.

Lemma 3.5 $\bigcap_{i=1}^k \overline{\mathrm{C}}_i(\sigma) = \mathrm{C}(\sigma)$.

Proof:

$$\begin{aligned}\bigcap_{i=1}^{k} \overline{\mathrm{C}}_i(\sigma) &= \{\omega : \mu_i(\theta_i(\omega), \sigma[\ell-1]) = \langle\sigma_\ell\rangle_i \text{ for } 1 \leq \ell \leq t \text{ and } i \in K\} \\ &= \{\omega : \mathrm{conv}(\theta(\omega)) = \sigma\} \\ &= \mathrm{C}(\sigma)\end{aligned}$$

as desired. ■

Lemma 3.6 $\bigcap_{i=1}^k \overline{\mathrm{CO}}_i(\sigma, v) = \mathrm{CO}(\sigma, v)$.

Proof: This follows from Lemma 3.5 and the fact that when attention is restricted to points where $\mathrm{conv}(\theta(\omega)) = \sigma$, then $\Pr[\mathrm{O}_i(v)] = \Pr\left[\overline{\mathrm{O}}_i(\sigma, v)\right]$.

$$\begin{aligned}\bigcap_{i=1}^{k} \overline{\mathrm{CO}}_i(\sigma, v) &= \mathrm{C}(\sigma) \cap \bigcap_{i=1}^{k} \overline{\mathrm{O}}_i(\sigma, v) \\ &= \{\omega : \mathrm{conv}(\theta(\omega)) = \sigma \text{ and } \nu_i(\theta_i(\omega), \sigma) = v \text{ for } i \in K\} \\ &= \{\omega : \mathrm{conv}(\theta(\omega)) = \sigma \text{ and } \nu_i(\theta_i(\omega), \mathrm{conv}(\theta(\omega))) = v \text{ for } i \in K\} \\ &= \{\omega : \mathrm{conv}(\theta(\omega)) = \sigma \text{ and } \mathrm{out}_i(\theta(\omega)) = v \text{ for } i \in K\} \\ &= \mathrm{C}(\sigma) \cap \mathrm{O}(v) \\ &= \mathrm{CO}(\sigma, v)\end{aligned}$$

as desired. ■

3.3 Secret key exchange systems

Let $\mathcal{P}_\mathcal{S}$ be a system and let θ_e be a view function for Eve. $\mathcal{P}_\mathcal{S}$ performs *N-valued perfect (respectively weak) secret key exchange against θ_e* if $\mathcal{P}_\mathcal{S}$ is N-valued and $\mathcal{P}_\mathcal{S}$ satisfies agreement, perfect (weak) uniformity, and perfect (weak) secrecy against θ_e. We also say $\mathcal{P}_\mathcal{S}$ is a system *for N-valued perfect (weak) secret key exchange against θ_e*. It follows from Proposition 3.1 that any system that performs perfect secret key exchange against θ_e also performs weak secret key exchange against θ_e.

We say that $\mathcal{P}_\mathcal{S}$ performs, or is for, *perfect (weak) secret key exchange* if $\mathcal{P}_\mathcal{S}$ performs perfect (weak) secret key exchange against the empty view. In the remainder of this paper, we consider only empty views for Eve. (Some results concerning nonempty views for Eve appear in [16].)

In this section, we examine how the secret key exchange conditions restrict the inputs, conversation, and outputs of the players. Lemma 3.7 exhibits some consequences of the implication of the agreement condition that at any feasible point, all players output the same value.

Lemma 3.7 *Let $\mathcal{P}_{\mathcal{S}}$ satisfy agreement, let $u \in U$ be feasible, let $v \in V$, let $i, j \in K$, and let $\sigma \in \mathsf{cc}$.*

1. $\mathrm{out}_i(u) = \mathrm{out}_j(u)$.
2. $\mathrm{feas}(\mathrm{O}_i(v)) = \mathrm{feas}(\mathrm{O}(v))$.
3. $\Pr[\mathrm{C}(\sigma) \cap \mathrm{O}_i(v)] = \Pr[\mathrm{CO}(\sigma, v)]$.
4. $\Pr[\mathrm{C}(\sigma)] = \sum_{v \in V} \Pr[\mathrm{CO}(\sigma, v)]$.

Proof: Suppose the conditions of the lemma.

1. By definition, $\theta^{-1}(u) \subseteq \mathrm{O}_i(\mathrm{out}_i(u)) \cap \mathrm{O}_j(\mathrm{out}_j(u))$. Since u is feasible, $\theta^{-1}(u)$ contains a feasible point. Since agreement is satisfied, $\mathrm{out}_i(u) = \mathrm{out}_j(u)$.

2. By definition, $\mathrm{O}(v) \supseteq \mathrm{O}_i(v)$. Therefore, $\mathrm{feas}(\mathrm{O}(v)) \supseteq \mathrm{feas}(\mathrm{O}_i(v))$. Conversely, suppose that $\omega \in \mathrm{feas}(\mathrm{O}_i(v))$. Then ω is feasible and $v = \mathrm{out}_i(\theta(\omega))$. By (1), $\mathrm{out}_{i'}(\theta(\omega)) = v$ for all $i' \in K$. It follows that $\omega \in \mathrm{O}(v)$. Since ω is feasible, $\omega \in \mathrm{O}(v)$.

3. Since only feasible points have positive probability, it follows from (2) that

$$\begin{aligned}
\Pr[\mathrm{C}(\sigma) \cap \mathrm{O}_i(v)] &= \Pr[\mathrm{C}(\sigma) \cap \mathrm{feas}(\mathrm{O}_i(v))] \\
&= \Pr[\mathrm{C}(\sigma) \cap \mathrm{feas}(\mathrm{O}(v))] \\
&= \Pr[\mathrm{C}(\sigma) \cap \mathrm{O}(v)] = \Pr[\mathrm{CO}(\sigma, v)]
\end{aligned}$$

4. $\mathrm{C}(\sigma)$ is the disjoint union over $v \in V$ of $\mathrm{C}(\sigma) \cap \mathrm{O}_i(v)$ since for every point ω there is exactly one v such that $\omega \in \mathrm{O}_i(v)$. Hence by (3),

$$\begin{aligned}
\Pr[\mathrm{C}(\sigma)] &= \sum_{v \in V} \Pr[\mathrm{C}(\sigma) \cap \mathrm{O}_i(v)] \\
&= \sum_{v \in V} \Pr[\mathrm{CO}(\sigma, v)]
\end{aligned}$$

■

Lemma 3.8 shows that if N-valued perfect secret key exchange is to take place, then for each conversation, each output value must occur with probability $1/N$. Similarly, Lemma 3.9 shows that if N-valued weak secret key exchange is to take place, then for each feasible conversation, each output value must occur with nonzero probability.

Lemma 3.8 *Let $\mathcal{P}_{\mathcal{S}}$ perform N-valued perfect secret key exchange, let $\sigma \in \mathsf{cc}$, and let $v \in V$. Then* $\Pr[\mathrm{CO}(\sigma, v)] = \frac{1}{N}\Pr[\mathrm{C}(\sigma)]$.

Proof: Let $\mathcal{P}_{\mathcal{S}}$ perform N-valued perfect secret key exchange, let $\sigma \in \mathsf{cc}$, let $v_1, v_2 \in V$, let $i \in K$. By Lemma 3.7 (part 3) and Proposition 3.2 (part 1),

$$\begin{aligned}\Pr[\mathrm{CO}(\sigma, v_1)] &= \Pr[\mathrm{C}(\sigma) \cap \mathrm{O}_i(v_1)] \\ &= \Pr[\mathrm{C}(\sigma)] \cdot \Pr[\mathrm{O}_i(v_1)]\end{aligned}$$

Similarly, $\Pr[\mathrm{CO}(\sigma, v_2)] = \Pr[\mathrm{C}(\sigma)] \cdot \Pr[\mathrm{O}_i(v_2)]$. By perfect uniformity, $\Pr[\mathrm{O}_i(v_1)] = \Pr[\mathrm{O}_i(v_2)]$. It follows that $\Pr[\mathrm{CO}(\sigma, v_1)] = \Pr[\mathrm{CO}(\sigma, v_2)]$. By Lemma 3.7 (part 4), it follows that for every $v \in V$, $\Pr[\mathrm{CO}(\sigma, v)] = \frac{1}{N}\Pr[\mathrm{C}(\sigma)]$. ∎

Lemma 3.9 *Let $\mathcal{P}_{\mathcal{S}}$ perform N-valued weak secret key exchange, let $\sigma \in \mathsf{cc}$ and let $v \in V$. Then* $\Pr[\mathrm{CO}(\sigma, v)] \geq 0$ *with equality if and only if* $\Pr[\mathrm{C}(\sigma)] = 0$.

Proof: Suppose the conditions of the lemma. If $\Pr[\mathrm{C}(\sigma)] = 0$, then $\Pr[\mathrm{CO}(\sigma, v)] = 0$. Otherwise, $\Pr[\mathrm{C}(\sigma)] > 0$. By weak uniformity, $\Pr[\mathrm{O}_i(v)] > 0$. Hence, by Lemma 3.7 (part 3) and Proposition 3.2 (part 2), $\Pr[\mathrm{CO}(\sigma, v)] = \Pr[\mathrm{C}(\sigma) \cap \mathrm{O}_i(v)] > 0$. ∎

If two inputs that give rise to the same conversation have a nontrivial feasible interpolant (i.e. the set of two inputs is coverable), then some team players can not distinguish the first input vector from the interpolant and some team players can not distinguish the second input vector from the interpolant. It follows that all team players must output the same value on all three inputs. The following lemma formalizes this argument to show that in order for a system to perform secret key exchange, there must be inputs that are not coverable.

Lemma 3.10 *Let $\mathcal{P}_{\mathcal{S}}$ be an N-valued system such that $N \geq 2$, and suppose that every set of two feasible inputs is coverable. Then $\mathcal{P}_{\mathcal{S}}$ does not perform weak (perfect) secret key exchange.*

Proof: By Proposition 3.1, it suffices to show the lemma holds for weak secret key exchange. Suppose the conditions of the lemma and suppose by way of contradiction that $\mathcal{P}_{\mathcal{S}}$ performs weak secret key exchange. Let σ be a complete conversation such that $\Pr[\mathrm{C}(\sigma)] > 0$. Let $\omega, \omega' \in \mathrm{C}(\sigma)$ be feasible. Let $u = \theta(\omega)$ and let $u' = \theta(\omega')$. By assumption, there exists $\widehat{u}$ that covers $\{u, u'\}$. Since $\widehat{u}$ spans $\{u, u'\}$, there exist $i, i' \in K$ such that $\langle u \rangle_i = \langle \widehat{u} \rangle_i$ and $\langle u' \rangle_{i'} = \langle \widehat{u} \rangle_{i'}$. Let $v = \mathrm{out}_i(u)$ and $v' = \mathrm{out}_{i'}(u')$. Then $\omega \in \mathrm{feas}(\mathrm{O}_i(v))$ and $\omega' \in \mathrm{feas}(\mathrm{O}_{i'}(v'))$. It follows from Lemma 3.7 (part 2) that $\omega \in \mathrm{O}(v)$ and $\omega' \in \mathrm{O}(v')$. Hence $\omega \in \mathrm{CO}(\sigma, v)$ and $\omega' \in \mathrm{CO}(\sigma, v')$. By Lemma 2.1 (parts 1 and 3), $\mathrm{conv}(\widehat{u}) = \sigma$, $\mathrm{out}_i(\widehat{u}) = v$, and $\mathrm{out}_{i'}(\widehat{u}) = v'$. Since $\widehat{u}$ is feasible, it follows from Lemma 3.7 (part 1) that $v = v'$, so $\omega' \in \mathrm{CO}(\sigma, v)$.

Since ω and ω' were chosen arbitrarily, it follows that $\omega \in \mathrm{CO}(\sigma, v)$ for all feasible $\omega \in \mathrm{C}(\sigma)$. Let $x \in V - \{v\}$. Then $\Pr[\mathrm{CO}(\sigma, x)] = 0$, a contradiction to Lemma 3.9. We conclude $\mathcal{P}_{\mathcal{S}}$ does not perform weak secret key exchange. ∎

A direct consequence of Lemma 3.10 is the intuitive result that the players' inputs must be correlated in order for secret key exchange to be possible. Specifically, if the team players can be divided into two sets such that the inputs of one set are independent of the other, regardless of the correlations within the sets, then secret key exchange is not possible. Given a set $K' \subseteq K$ and an input $u \in U$, we define the event $\mathrm{I}_{K'}(u) = \{u' : \langle u' \rangle_i = \langle u \rangle_i \text{ for all } i \in K'\}$ over U. Thus $\mathrm{I}_{K'}(u)$ is the event that the team players in K' have inputs as specified by u. In particular, if there are sets K_0 and K_1 such that $\mathrm{I}_{K_0}(u)$ and $\mathrm{I}_{K_1}(u)$ are independent events for every input u, then there is no prior shared secret information between the team players in K_0 and the team players in K_1.

Theorem 3.11 *Let $\mathcal{P}_{\mathcal{S}}$ be an N-valued system such that $N \geq 2$, and suppose there is a partition of K into nonempty sets K_0 and K_1 such that $\mathrm{I}_{K_0}(u)$ and $\mathrm{I}_{K_1}(u)$ are independent events for all $u \in U$. Then $\mathcal{P}_{\mathcal{S}}$ does not perform weak (perfect) secret key exchange.*

Proof: Suppose the conditions of the theorem, and let u and u' be an arbitrary pair of distinct feasible inputs. Let $u_i = u$ for $i \in K_0$, let $u_i = u'$ for $i \in K_1$, and let $\widehat{u} = (\langle u_1 \rangle_1, \ldots, \langle u_k \rangle_k)$. Then $\widehat{u}$ interpolates $\{u, u'\}$. Since K_0 and K_1 are nonempty, $\widehat{u}$ spans $\{u, u'\}$.

By the independence condition,

$$\begin{aligned} \Pr[\mathrm{I}_K(\widehat{u})] &= \Pr[\mathrm{I}_{K_0}(\widehat{u}) \cap \mathrm{I}_{K_1}(\widehat{u})] \\ &= \Pr[\mathrm{I}_{K_0}(\widehat{u})] \cdot \Pr[\mathrm{I}_{K_1}(\widehat{u})] \end{aligned}$$

The input $u \in \mathrm{I}_{K_0}(\widehat{u})$ is feasible, so $\Pr[\mathrm{I}_{K_0}(\widehat{u})] > 0$. Similarly, $\Pr[\mathrm{I}_{K_1}(\widehat{u})] > 0$. It follows that $\Pr[\mathrm{I}_K(\widehat{u})] > 0$. Since by definition $\mathrm{I}_K(\widehat{u}) = \{\widehat{u}\}$, it follows that $\widehat{u}$ is feasible. Hence $\widehat{u}$ covers $\{u, u'\}$. By Lemma 3.10, $\mathcal{P}_{\mathcal{S}}$ does not perform weak (perfect) secret key exchange. ■

Theorem 3.11 implies the folklore result that public key cryptography is not possible in the presence of a computationally-unlimited eavesdropper, since in public key cryptography the participants are assumed to have no prior shared secret information. The first written reference to such results we are aware of is in Rudich's thesis [11], where he shows that public key cryptography is not possible against a suitably powerful adversary.

4 The Capacity of a Source

Theorem 3.11 shows that independent random inputs alone are not sufficient for secret key exchange. However, as seen by the example in the introduction, there are cases where secret key exchange is not possible given correlated inputs alone, but is possible given independent random inputs in addition to the correlated inputs. Thus, independent random inputs can make the difference between possibility and impossibility of secret key exchange.

We imagine a scenario in which a protocol designer is given a source $\mathcal{T}$ of correlated inputs. The designer, whose goal is to obtain the largest secret key possible, is allowed to specify independent randomness (as modeled by a randomized extension of $\mathcal{T}$) and a protocol. We will define the capacity of a source $\mathcal{T}$ to be a measure of the ability any randomized extension of $\mathcal{T}$ has to perform secret key exchange against an empty view for Eve. Specifically, for a given source $\mathcal{T}$, we define the *perfect capacity of* $\mathcal{T}$, denoted $\mathrm{pcap}(\mathcal{T})$ to be the maximum N such that there exists a randomized $\mathcal{T}$-system for N-valued perfect secret key exchange. Since 1-valued perfect secret key exchange is trivial, this maximum is well defined whenever there is an upper bound on N. If there is no upper bound, we take the perfect capacity of $\mathcal{T}$ to be infinite. We similarly define the weak capacity of $\mathcal{T}$, denoted $\mathrm{wcap}(\mathcal{T})$, with respect to weak secret key exchange. It follows from Proposition 3.1 that $1 \leq \mathrm{pcap}(\mathcal{T}) \leq \mathrm{wcap}(\mathcal{T})$. We will see shortly (Theorem 4.4) that the capacity of $\mathcal{T}$ is always finite.

The following proposition, which follows from Propositions 2.5 and 3.4, states that team-equivalent sources have the same capacity.

Proposition 4.1 *Let $\mathcal{T}$ and $\mathcal{T}'$ be team-equivalent sources. Then* $\mathrm{pcap}(\mathcal{T}) = \mathrm{pcap}(\mathcal{T}')$ *and* $\mathrm{wcap}(\mathcal{T}) = \mathrm{wcap}(\mathcal{T}')$.

Wright [16] shows that for every $N \leq \mathrm{pcap}(\mathcal{T})$ (respectively, $N \leq \mathrm{wcap}(\mathcal{T})$), there is a randomized $\mathcal{T}$-system for N-valued perfect (respectively weak) secret key exchange. Thus, the weak and perfect capacities of $\mathcal{T}$ can be interpreted as measures of the information provided to the players by $\mathcal{T}$. Theorem 3.11 implies that if $\mathcal{T}$ is a source in which the views of one set of team players are independent from the views of another set of team players, then $\mathrm{wcap}(\mathcal{T}) = \mathrm{pcap}(\mathcal{T}) = 1$. In the remainder of this paper, we investigate upper bounds on the weak and perfect capacities of various sources.

We begin by showing some general properties of randomized $\mathcal{T}$-systems. Fix a source $\mathcal{T}$ with at least two players. Let $\mathcal{P}_{\mathcal{S}}$ be a randomized $\mathcal{T}$-system, let $q \in U^{\mathcal{T}}$, let $\tau \in \mathsf{c}$, and let $\ell = |\tau|$. We define

$$\mathrm{F}(q, \tau) = \{u \in \mathrm{feas}(U^{\mathcal{S}}) : \mathrm{corr}(u) = q \text{ and } \mathrm{conv}(u)[\ell] = \tau\}$$

Thus $\mathrm{F}(q, \tau)$ consists of the feasible inputs that have correlated part q and give rise to the conversation τ. We say q is *compatible* with τ (and τ is compatible with q) if $\mathrm{F}(q, \tau)$ is nonempty. We define $\mathrm{compat}(\tau) = \{q : \mathrm{F}(q, \tau) \neq \emptyset\}$. Then $\mathrm{compat}(\tau)$ is the set of q compatible with τ. Note that if q is compatible with τ, then q and τ are both feasible.

Let $q \in U^{\mathcal{T}}$ and $\sigma \in \mathsf{cc}$. If there exists a unique $v \in V$ such that $\mathrm{out}_i(u) = v$ for all $i \in K$ and $u \in \mathrm{F}(q, \sigma)$, then we define $\mathrm{out}(q, \sigma) = v$. Hence, if defined, $\mathrm{out}(q, \sigma)$ is the value that all team players output given any feasible input in which the correlated part is q and the conversation is σ.

Lemma 4.2 *Let $\mathcal{P}_{\mathcal{S}}$ be a randomized $\mathcal{T}$-system satisfying agreement such that $k \geq 2$, let $q \in U^{\mathcal{T}}$, and let $\sigma \in \mathsf{cc}$. If q is compatible with σ, then* $\mathrm{out}(q, \sigma)$ *is defined.*

Proof: Suppose the conditions of the lemma and suppose that q is compatible with σ. Then $\mathrm{F}(q, \sigma)$ is nonempty. Let $u, u' \in \mathrm{F}(q, \sigma)$ and let $i, i' \in K$. Let $v = \mathrm{out}_i(u)$ and $v' = \mathrm{out}_{i'}(u')$. It suffices to show that $v' = v$.

Since $u, u' \in \mathrm{F}(q, \sigma)$, it follows that u and u' are feasible and the correlated part $\mathrm{corr}(u) = \mathrm{corr}(u') = q$ is feasible. Let $\widehat{u}$ interpolate $\{u, u'\}$ such that $\widehat{u} =_i u$ and $\widehat{u} =_{i'} u'$. Then $\mathrm{corr}(\widehat{u}) = q$, so $\mathrm{corr}(\widehat{u})$ is feasible. Hence, by Lemma 2.6, $\widehat{u}$ is feasible. By Lemma 2.1 (part 3), $\mathrm{out}_i(\widehat{u}) = v$ and $\mathrm{out}_{i'}(\widehat{u}) = v'$. By Lemma 3.7 (part 1), $v' = v$. ■

Fix a complete conversation σ and two correlated parts $q, q' \in U^{\mathcal{T}}$ compatible with σ. If P_i holds the same share in both correlated parts, then P_i can not determine whether the correlated part is q or q'. It follows that all the team players must output the same value in both situations.

Lemma 4.3 *Let $\mathcal{P}_{\mathcal{S}}$ be a randomized $\mathcal{T}$-system satisfying agreement such that $k \geq 2$, let $\sigma \in \mathsf{cc}$, and let $q, q' \in U^{\mathcal{T}}$ be compatible with σ. If q touches q', then* $\mathrm{out}(q, \sigma) = \mathrm{out}(q', \sigma)$.

Proof: Suppose the conditions of the lemma and suppose that $q =_x q'$ for some x. Since q and q' are compatible with σ, it follows from Lemma 4.2 that $\mathrm{out}(q, \sigma)$ and $\mathrm{out}(q', \sigma)$ are defined. Let $u \in \mathrm{F}(q, \sigma)$ and let $u' \in \mathrm{F}(q', \sigma)$. Let $\widehat{u}$ interpolate $\{u, u'\}$ such that $\widehat{u} =_x u$ and $\widehat{u} =_i u'$ for all $i \neq x$. Then $\mathrm{corr}(\widehat{u}) = q'$, so $\mathrm{corr}(\widehat{u})$ is feasible. By Lemma 2.6, $\widehat{u}$ is feasible. By Lemma 2.1 (part 1), $\mathrm{conv}(\widehat{u}) = \sigma$. It follows that $\widehat{u} \in \mathrm{F}(q', \sigma)$. By Lemma 2.1 (part 3), $\mathrm{out}_x(\widehat{u}) = \mathrm{out}_x(u)$. It follows that $\mathrm{out}(q, \sigma) = \mathrm{out}_x(u) = \mathrm{out}_x(\widehat{u}) = \mathrm{out}(q', \sigma)$. ■

Fix a complete conversation σ. It follows from the results of Section 3.3 that all output values must be possible when the conversation is σ. By the above, all players output the same value whenever P_i holds a given share. Therefore, the number of output values of a secret key exchange system is at most the number of feasible shares for any player P_i. Formally, we have the following.

Theorem 4.4 *Let $\mathcal{T}$ be a source. Then* $\mathrm{wcap}(\mathcal{T}) \leq \min_{i \in K} |\mathrm{feas}(U_i^{\mathcal{T}})|$.

Proof: Suppose $\mathcal{P}_{\mathcal{S}}$ is a randomized $\mathcal{T}$-system for N-valued weak secret key exchange for some N and let $i \in K$. We complete the proof by showing that $|\mathrm{feas}(U_i^{\mathcal{T}})| \geq N$. Let $\sigma \in \mathsf{cc}$ be feasible. It follows from Lemma 3.7 (part 4) and Lemma 3.9 that $\mathrm{feas}(\mathrm{C}(\sigma))$ is partitioned into N equivalence classes $\mathrm{feas}(\mathrm{CO}(\sigma, v))$, and hence that $\mathrm{feas}(\theta(\mathrm{C}(\sigma)))$ is partitioned into N equivalence classes $\mathrm{feas}(\theta(\mathrm{CO}(\sigma, v)))$. Also, $\mathrm{feas}(\theta(\mathrm{C}(\sigma)))$ is partitioned into $|\mathrm{feas}(U_i^{\mathcal{T}})|$ equivalence classes determined by P_i's share of the correlated part of the input. The second partition is a refinement of the first, since by Lemma 4.3, if two inputs have the same share for P_i and the same conversation, then they have the same output value. It follows that $|\mathrm{feas}(U_i^{\mathcal{T}})| \geq N$. ■

Lemma 4.5 generalizes Lemma 2.1 (First Interpolation Lemma) to randomized $\mathcal{T}$-systems.

Lemma 4.5 (Third Interpolation Lemma) *Let $\mathcal{P}_\mathcal{S}$ be a randomized $\mathcal{T}$-system, let $\tau \in \mathsf{c}$, let $U' \subseteq \mathrm{compat}(\tau)$, and suppose that $\widehat{q}$ is a feasible interpolant of U'. Let $(q_1, \ldots, q_k)$ be a U'-derivation of $\widehat{q}$. Then*

1. *$\widehat{q}$ is compatible with τ.*
2. *If $|\tau| < t$ and $m_1, \ldots, m_k$ are message vectors such that q_i is compatible with τm_i for $i \in K$, then $\widehat{q}$ is compatible with $\tau \cdot (\langle m_1\rangle_1, \langle m_2\rangle_2, \ldots, \langle m_k\rangle_k)$.*
3. *If $|\tau| = t$, $\mathcal{P}_\mathcal{S}$ satisfies agreement, and $k \geq 2$, then $\mathrm{out}(\widehat{q}, \tau) = \mathrm{out}(q_i, \tau)$ for $i \in K$.*

Proof: Suppose the conditions of the lemma and let $\ell = |\tau|$.

1. For $i \in K$, $q_i \in \mathrm{compat}(\tau)$, so choose $u_i \in \mathrm{F}(q_i, \tau)$. Then $\widehat{u} = (\langle u_1\rangle_1, \ldots, \langle u_k\rangle_k)$ interpolates $\{u_1, \ldots, u_k\}$ and $\mathrm{corr}(\widehat{u}) = \widehat{q}$. By Lemma 2.1 (part 1), $\mathrm{conv}(\widehat{u})[\ell] = \tau$ and by Lemma 2.6, $\widehat{u}$ is feasible. Thus, $\widehat{u} \in \mathrm{F}(\widehat{q}, \tau)$, so $\widehat{q}$ is compatible with τ.
2. Suppose that $\ell < t$ and q_i is compatible with τm_i for $i \in K$. Let $u_i \in \mathrm{F}(q_i, \tau m_i)$ for $i \in K$. Then $\widehat{u} = (\langle u_1\rangle_1, \ldots, \langle u_k\rangle_k)$ interpolates $\{u_1, \ldots, u_k\}$ and $\mathrm{corr}(\widehat{u}) = \widehat{q}$. By Lemma 2.1 (part 2), $\mathrm{conv}(\widehat{u})[\ell + 1] = \tau \cdot (\langle m_1\rangle_1, \langle m_2\rangle_2, \ldots, \langle m_k\rangle_k)$ and by Lemma 2.6, $\widehat{u}$ is feasible. Thus, $\widehat{u} \in \mathrm{F}(\widehat{q}, \tau \cdot (\langle m_1\rangle_1, \langle m_2\rangle_2, \ldots, \langle m_k\rangle_k))$, so $\widehat{q}$ is compatible with $\tau \cdot (\langle m_1\rangle_1, \langle m_2\rangle_2, \ldots, \langle m_k\rangle_k)$.
3. Suppose $\ell = t$, $\mathcal{P}_\mathcal{S}$ satisfies agreement, $k \geq 2$ and $i \in K$. Since $(q_1, \ldots, q_k)$ is a U'-derivation of $\widehat{q}$, $\widehat{q} =_i q_i$. By Lemma 4.3, $\mathrm{out}(\widehat{q}, \tau) = \mathrm{out}(q_i, \tau)$. ■

Lemma 4.6 *Let $\mathcal{P}_\mathcal{S}$ be a randomized $\mathcal{T}$-system satisfying agreement, let $\sigma \in \mathsf{cc}$, and let $U' \subseteq \mathrm{compat}(\sigma)$ be coverable. Then $\mathrm{out}(q, \sigma) = \mathrm{out}(q', \sigma)$ for all $q, q' \in U'$.*

Proof: Suppose the conditions of the lemma, let $q, q' \in U'$, and let $\widehat{q}$ be a covering of U'. Then $\widehat{q}$ is a feasible spanning interpolant of U'. It follows that there is a U'-derivation $(q_1, \ldots, q_k)$ of $\widehat{q}$ such that $q = q_i$ and $q' = q_{i'}$ for for some $i, i' \in K$. By Lemma 4.5 (part 3), $\mathrm{out}(q, \sigma) = \mathrm{out}(q_i, \sigma) = \mathrm{out}(\widehat{q}, \sigma) = \mathrm{out}(q_{i'}, \sigma) = \mathrm{out}(q', \sigma)$. ■

5 Card Games

In this section, we formalize the use of deals of cards as correlated random variables. A *deck* Δ is a finite set, whose elements we call *cards*; a *hand* is subset of Δ. A *deal* $\delta = (h_1, \ldots, h_k)$ is a sequence of hands, one for each player. (Note that there may be cards in the deck that don't appear in any hand.) The deal δ is *legal* if $h_i \cap h_j = \emptyset$ for $i \neq j$. A deal that may or may not be legal is called a *general* deal. In the real world, where all hands are typically dealt from a single deck of cards, all deals are legal. General deals are of interest to us because they can arise when legal deals are interpolated.

A *signature*[1] $(s_1, s_2, \ldots, s_k; d)$, where $s_1, \ldots, s_k$ and d are nonnegative integers, describes the number k of players, the size s_i of each player's hand, and the number d of cards in the deck. If all k team players have the same hand size s in the signature ξ, we write $\xi = (s^{(k)}; d)$. Let $\xi = (s_1, \ldots, s_k; d)$ be a signature. Without loss of generality, we always fix the deck $\Delta^\xi = \{1, \ldots, d\}$. A ξ*-deal* is a deal $\delta = (h_1, \ldots, h_k)$ such that $|h_i| = s_i$ for $i \in K$. We define $H_i^\xi = \{h : h \subseteq \Delta^\xi \text{ and } |h| = s_i\}$, so H_i^ξ is the set of possible hands for P_i. We write L^ξ to denote the set of legal ξ-deals and D^ξ to denote the set of general ξ-deals, so $L^\xi \subseteq D^\xi = H_1^\xi \times \cdots \times H_k^\xi$.

A source $\mathcal{T}$ for D^ξ is *legal* if $\Pr_{\mathcal{T}}(\delta) = 1/|L^\xi|$ for $\delta \in L^\xi$, and $\Pr_{\mathcal{T}}(\delta) = 0$ for $\delta \in D^\xi - L^\xi$. Hence $\mathcal{T}$ is a legal source if $\mathcal{T}$ assigns zero probability to all illegal deals and equal probability to all legal deals. We say a system $\mathcal{P}_\mathcal{S}$ is a *card game* ξ*-system* if $\mathcal{S}$ is a randomized extension of some legal source for D^ξ. Since all legal sources for D^ξ are team-equivalent, it follows from Proposition 4.1 that they all have the same perfect capacity. We denote this capacity by $\mathrm{pcap}(\xi)$. Similarly, we denote the weak capacity of all legal sources for D^ξ by $\mathrm{wcap}(\xi)$. Hence, if $N \leq \mathrm{pcap}(\xi)$ (respectively, if $N \leq \mathrm{wcap}(\xi)$) then there exists a card game ξ-system $\mathcal{P}_\mathcal{S}$ for N-valued perfect (respectively, weak) secret key exchange.

By Theorem 4.4, $\mathrm{pcap}(\xi) \leq \mathrm{wcap}(\xi) \leq \min_{i \in K} |H_i^\xi|$. In Section 6, we obtain an improved bound on $\mathrm{wcap}(1^{(k)}; k)$ for $k \geq 3$ by considering the particular structure of the set of $(1^{(k)}; k)$-deals. In Section 7, we obtain an improved bound on $\mathrm{pcap}(\xi)$ by taking into account the perfect secrecy requirement.

6 Impossibility of Secret Key Exchange for $(1^{(k)}; k)$

It follows from the work of Fischer, Paterson and Rackoff [2] that for teams of size two, 2-valued perfect secret key exchange is always possible when the team holds all the cards, provided that each player has at least one card. However, for larger teams, this is not the case. In particular, we show that even weak secret key exchange is not possible when each of $k \geq 3$ team players holds one card from a k card deck. By Theorem 4.4, $\mathrm{wcap}(1^{(k)}; k) \leq k$. By examining the structure of the set of legal $(1^{(k)}; k)$-deals, it is possible to show that $\mathrm{wcap}(1^{(k)}; k) = 1$ if $k \geq 3$. We showed this result in [3] for the case $k = 3$. The proof given here generalizes the proof in [3]. An alternate proof appears in [1].

Let $k \geq 3$ and let $\xi = (1^{(k)}; k)$. Since there are k cards in ξ, $\Delta^\xi = K$. Let $\mathcal{P}_\mathcal{S}$ be a card game ξ-system and let L denote the set of legal ξ-deals. Since $\mathcal{P}_\mathcal{S}$ is a card game system, the set of feasible deals is L. (We assume throughout this section that the set of feasible deals is L.) We will denote by j the hand containing the single card

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

j. A legal deal can be regarded as a permutation of K (and every permutation of K corresponds to a legal deal). Thus, if δ is legal, then for every $j \in K$, there is a unique $i \in K$ such that $\langle\delta\rangle_i = j$.

Lemma 6.1 *Suppose $\{\alpha, \beta\} \subseteq L$ is not coverable, and let $x, j \in K$. Then there exists $\delta \in L$ such that $\langle\delta\rangle_x = j$ and for all $i \neq x$, $\delta =_i \alpha$ or $\delta =_i \beta$.*

Proof: Suppose the conditions of the lemma. We will construct the desired deal δ. Figures 1–3 show the result of steps of the construction for the example $\alpha = (2, 1, 5, 4, 6, 3)$, $\beta = (5, 3, 6, 2, 1, 4)$, $x = 5$, and $j = 4$.

We begin by constructing a directed graph $G = (V, E)$ that represents the deals α and β, where $V = K$ and $E = \{(a, b) : \langle\alpha\rangle_a = \langle\beta\rangle_b\}$. We label the edge $(a, b) \in E$ by $\mathcal{L}(a, b) = \langle\alpha\rangle_a = \langle\beta\rangle_b$. Hence the vertices of G are coordinates and the edges of G are labeled by cards. (See Figure 1.)

Since α is a permutation, each vertex i has exactly one incoming edge, labeled $\langle\beta\rangle_i$, which we denote by incoming(i). Symmetrically, since β is a permutation, each vertex i has exactly one outgoing edge, labeled $\langle\alpha\rangle_i$, which we denote by outgoing(i). Hence G is a collection of disjoint cycles. Furthermore, since $\mathcal{L}(\text{outgoing}(i)) = \langle\alpha\rangle_i$ and α is a permutation, $\mathcal{L}(\text{outgoing}(V)) = \{\langle\alpha\rangle_i : i \in V\} = K$. Symmetrically, $\mathcal{L}(\text{incoming}(V)) = K$.

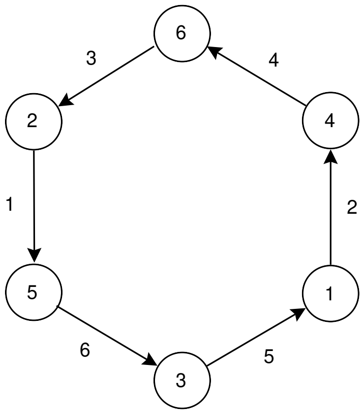

Figure 1: The graph G for $\alpha = (2, 1, 5, 4, 6, 3)$ and $\beta = (5, 3, 6, 2, 1, 4)$.

We will now show that in fact G consists of exactly one cycle. Suppose not. Then G is the union of two disjoint graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$, where G_1 and G_2 are nonempty collections of disjoint cycles. Hence incoming(V_1) = outgoing$(V_1) = E_1$ and incoming(V_2) = outgoing$(V_2) = E_2$. Consider the deal γ defined by

$$\langle\gamma\rangle_i = \begin{cases} \mathcal{L}(\text{incoming}(i)) & \text{if } i \in V_1 \\ \mathcal{L}(\text{outgoing}(i)) & \text{if } i \in V_2 \end{cases}$$

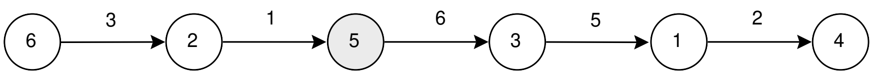

Figure 2: The graph G' for $x = 5$ and $j = 4$.

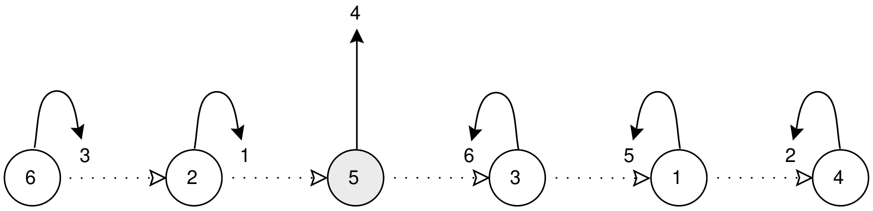

Figure 3: Use of G' to define the deal $\delta = (5, 1, 6, 2, 4, 3)$.

The deal γ is a permutation (and hence feasible) because $\{\langle\gamma\rangle_i : i \in K\} = \mathcal{L}(E_1) \cup \mathcal{L}(E_2) = \mathcal{L}(E) = K$. Since $\mathcal{L}(\text{incoming}(i)) = \langle\beta\rangle_i$ and $\mathcal{L}(\text{outgoing}(i)) = \langle\alpha\rangle_i$, γ interpolates $\{\alpha, \beta\}$. Since V_1 and V_2 are nonempty, γ spans $\{\alpha, \beta\}$. It follows that γ covers $\{\alpha, \beta\}$, a contradiction. We conclude that G consists of a single cycle.

Let $G' = (V', E')$ be the directed graph obtained from G by removing the edge labeled j. Then G' consists of a single chain. (See Figure 2.)

Let $i, i' \in V'$. We write $i \xrightarrow{+} i'$ if there is a nonempty path in G' from i to i'. We define $\text{left}(i) = \{i' \in V' : i' \xrightarrow{+} i\}$ and $\text{right}(i) = \{i' \in V' : i \xrightarrow{+} i'\}$. Note that $V' = \{x\} \cup \text{left}(x) \cup \text{right}(x)$ and $E' = \text{outgoing}(\text{left}(x)) \cup \text{incoming}(\text{right}(x))$. We construct the desired deal δ as follows.

$$\langle\delta\rangle_i = \begin{cases} j & \text{if } i = x \\ \mathcal{L}(\text{outgoing}(i)) & \text{if } i \in \text{left}(x) \\ \mathcal{L}(\text{incoming}(i)) & \text{if } i \in \text{right}(x) \end{cases}$$

(See Figure 3.) Then δ is a permutation because $\{\langle\delta\rangle_i : i \in K\} = \{j\} \cup \mathcal{L}(E') = K$. Hence $\delta \in L$. Clearly $\langle\delta\rangle_x = j$. Since $\mathcal{L}(\text{outgoing}(i)) = \langle\alpha\rangle_i$ and $\mathcal{L}(\text{incoming}(i)) = \langle\beta\rangle_i$, $\delta =_i \alpha$ or $\delta =_i \beta$ for all $i \neq x$. ■

Lemma 6.2 *Let $\alpha, \beta, \delta \in L$ and $x, y \in K$ such that $\langle\alpha\rangle_x = \langle\beta\rangle_y$ and for every $i \in K - \{x, y\}$, $\delta =_i \alpha$ or $\delta =_i \beta$. Then $\delta =_x \alpha$ or $\delta =_y \beta$.*

Proof: Suppose the conditions of the lemma and let $j = \langle\alpha\rangle_x = \langle\beta\rangle_y$. Let $i \in K - \{x, y\}$. Then $j \notin \{\langle\alpha\rangle_i, \langle\beta\rangle_i\}$. Hence since $\delta =_i \alpha$ or $\delta =_i \beta$, it follows that $\langle\delta\rangle_i \neq j$. Hence $\langle\delta\rangle_i \neq j$ for every $i \in K - \{x, y\}$. Since δ is a permutation, it follows that either $\langle\delta\rangle_x = j$ or $\langle\delta\rangle_y = j$, so $\delta =_x \alpha$ or $\delta =_y \beta$. ■

Together, Lemmas 6.1, 6.2, and 4.5 yield the following.

Lemma 6.3 *Let $\alpha, \beta, \gamma \in L$ such that $\{\alpha, \beta\}$ is not coverable and let $x \in K$. Then there exists a deal δ for which the following simultaneously hold.*

1. *δ is a feasible interpolant of $\{\alpha, \beta, \gamma\}$, and $\delta =_x \gamma$.*
2. *Let τ be a partial conversation compatible with α, β, and γ. Let m be a message vector such that α and β are both compatible with τm. Let m' be a message vector such that γ is compatible with $\tau m'$. Let the message vector $\widehat{m}$ be defined by $\langle \widehat{m} \rangle_x = \langle m' \rangle_x$ and $\langle \widehat{m} \rangle_i = \langle m \rangle_i$ for $i \neq x$. Then δ is compatible with $\tau \widehat{m}$.*
3. *Let y and z be such that $\langle \beta \rangle_y = \langle \alpha \rangle_x$ and $\langle \alpha \rangle_z = \langle \beta \rangle_x$. If $\gamma \neq_x \alpha$, then $\delta =_y \beta$. If $\gamma \neq_x \beta$, then $\delta =_z \alpha$.*
4. *If $\gamma \neq_x \alpha$ and $\gamma \neq_x \beta$, then δ covers $\{\alpha, \beta, \gamma\}$, and hence $\{\alpha, \beta, \gamma\}$ is coverable.*

Proof: Let $\alpha, \beta, \gamma \in L$ such that $\{\alpha, \beta\}$ is not coverable and let $x \in K$. Applying Lemma 6.1 to α, β, x, and $\langle \gamma \rangle_x$, we obtain a legal deal δ such that $\delta =_x \gamma$, and for all $i \neq x$, $\delta =_i \alpha$ or $\delta =_i \beta$.

1. Immediate by choice of δ.
2. Let τ, m, m' satisfy the conditions of part 2. We define deals $\delta_1, \ldots, \delta_k$ as follows: $\delta_x = \gamma$, and for $i \neq x$, $\delta_i = \alpha$ if $\delta =_i \alpha$, and $\delta_i = \beta$ if $\delta =_i \beta$. Then $(\delta_1, \ldots, \delta_k)$ is an $\{\alpha, \beta, \gamma\}$-derivation of δ. We similarly define message vectors $m_1, \ldots, m_k$ such that $m_x = m'$, and for $i \neq x$, $m_i = m$. This construction ensures that for all $i \in K$, δ_i is compatible with τm_i and $\widehat{m} = (\langle m_1 \rangle_1, \langle m_2 \rangle_2, \ldots, \langle m_k \rangle_k)$. By Lemma 4.5 (part 2), $\widehat{\delta}$ is compatible with $\widehat{m}$.
3. Let y and z be such that $\langle \beta \rangle_y = \langle \alpha \rangle_x$ and $\langle \alpha \rangle_z = \langle \beta \rangle_x$. (This is possible since α and β are permutations.) Suppose $\gamma \neq_x \alpha$. Since $\delta =_x \gamma$, we have $\delta \neq_x \alpha$. By Lemma 6.2 applied to α, β, δ, x, and y, we have $\delta =_x \alpha$ or $\delta =_y \beta$. Hence, $\delta =_y \beta$. Similarly, suppose $\gamma \neq_x \beta$. Since $\delta =_x \gamma$, we have $\delta \neq_x \beta$. By Lemma 6.2 applied to β, α, δ, x, and z, we have $\delta =_x \beta$ or $\delta =_z \alpha$. Hence, $\delta =_z \alpha$.
4. If $\gamma \neq_x \alpha$ and $\gamma \neq_x \beta$, then by part 3, $\delta =_y \beta$ and $\delta =_z \alpha$. Since $\delta =_x \gamma$, it follows that δ spans $\{\alpha, \beta, \gamma\}$. Since δ is a feasible interpolant of $\{\alpha, \beta, \gamma\}$, it follows that δ covers $\{\alpha, \beta, \gamma\}$, and hence $\{\alpha, \beta, \gamma\}$ is coverable. ■

By definition, a conversation is feasible if it is compatible with some legal deal. Lemma 6.4 shows that in fact each feasible complete conversation must be compatible with exactly two legal deals.

Lemma 6.4 *Let $k \geq 3$ and $N \geq 2$. Let $\mathcal{P}_{\mathcal{S}}$ be a card game $(1^{(k)}; k)$-system for N-valued weak secret key exchange and let $\sigma \in \mathsf{cc}$ be feasible. Then* $\mathrm{compat}(\sigma)$ *is not coverable and* $|\mathrm{compat}(\sigma)| = 2$.

Proof: Suppose the conditions of the lemma. Let $v_0, v_1 \in V$ such that $v_0 \neq v_1$ and let $j \in \{0, 1\}$. By weak uniformity, $\Pr[\mathrm{O}_1(v_j)] > 0$. Since σ is feasible, $\Pr[\mathrm{C}(\sigma)] > 0$. Hence by Lemma 3.7 (part 3) and Proposition 3.2 (part 2), $\Pr[\mathrm{CO}(\sigma, v_j)] = \Pr[\mathrm{C}(\sigma) \cap \mathrm{O}_1(v_j)] > 0$. Thus $\mathrm{CO}(\sigma, v_j)$ contains a feasible point ω_j. Let $u_j = \theta(\omega_j)$. Then $\mathrm{conv}(u_j) = \sigma$ and $\mathrm{out}_i(u_j) = v_j$ for all $i \in K$. Let $\alpha = \mathrm{corr}(u_0)$, and let $\beta = \mathrm{corr}(u_1)$. Hence $u_0 \in \mathrm{F}(\alpha, \sigma)$ and $u_1 \in \mathrm{F}(\beta, \sigma)$. It follows that $\mathrm{compat}(\sigma) \supseteq \{\alpha, \beta\}$. By Lemma 4.2, $\mathrm{out}(\alpha, \sigma)$ and $\mathrm{out}(\beta, \sigma)$ are defined, so $\mathrm{out}(\alpha, \sigma) = v_0$ and $\mathrm{out}(\beta, \sigma) = v_1$. Since $\mathrm{out}(\alpha, \sigma) \neq \mathrm{out}(\beta, \sigma)$, it follows from Lemma 4.6 that Q is not coverable for any set Q such that $\{\alpha, \beta\} \subseteq Q \subseteq \mathrm{compat}(\sigma)$.

We complete the proof by showing that $\mathrm{compat}(\sigma) = \{\alpha, \beta\}$. Suppose by way of contradiction that $\gamma \in \mathrm{compat}(\sigma) - \{\alpha, \beta\}$. Since $\{\alpha, \beta\} \subseteq \{\alpha, \beta, \gamma\} \subseteq \mathrm{compat}(\sigma)$, the set $\{\alpha, \beta, \gamma\}$ is not coverable. The deal γ is feasible since $\gamma \in \mathrm{compat}(\sigma)$. By Proposition 2.4, there is a coordinate x such that $\gamma \neq_x \alpha$ and $\gamma \neq_x \beta$. By Lemma 6.3 (part 4), $\{\alpha, \beta, \gamma\}$ is coverable, a contradiction. We conclude that $\mathrm{compat}(\sigma) = \{\alpha, \beta\}$. ∎

Theorem 6.5 *Let $k \geq 3$. Then* $\mathrm{wcap}(1^{(k)}; k) = 1$.

Proof: Let $k \geq 3$. Since $\mathrm{wcap}(\xi) \geq 1$ for any signature ξ, we need only show that $\mathrm{wcap}(1^{(k)}; k) < 2$. Suppose by way of contradiction that $\mathcal{P}_{\mathcal{S}}$ is a card game $(1^{(k)}; k)$-system for 2-valued weak secret key exchange. We construct a tree whose nodes are the feasible conversations of $\mathcal{P}_{\mathcal{S}}$. Two nodes τ and σ are connected by an edge if τ is a prefix of σ and $|\tau| + 1 = |\sigma|$. Thus, the internal nodes are partial conversations and the leaves are complete conversations. We often identify a node σ with the unique path from the root to σ. If τ is a prefix of σ, we say σ *passes through* τ.

If a deal δ is compatible with a conversation τ, then δ is compatible with every prefix of τ. Also, if τ is not complete, then δ is compatible with at least one extension of τ. Hence, δ is compatible with the parent of τ (provided τ is not empty), and δ is compatible with at least one child of τ (provided τ is not complete). It follows that if δ is compatible with σ, then δ is compatible with every node on the path to σ. Hence, every node on the path to σ is compatible with every deal $\delta \in \mathrm{compat}(\sigma)$. If σ is a leaf, then by Lemma 6.4, $\mathrm{compat}(\sigma)$ is not coverable and $|\mathrm{compat}(\sigma)| = 2$.

Every legal deal is compatible with the empty conversation and there are more than two legal $(1^{(k)}; k)$-deals. Hence, more than two deals are compatible with the root. Since there are exactly two deals compatible with every leaf and the tree is finite, there must be some node τ compatible with more than two deals, each of whose children is compatible with exactly two deals.

Since τ is compatible with more than two distinct deals and every deal compatible with τ is compatible with at least one of its children, τ must have two children τm and $\tau m'$ such that $\mathrm{compat}(\tau m) \neq \mathrm{compat}(\tau m')$. Let $\{\alpha, \beta\} = \mathrm{compat}(\tau m)$ and let $\{\alpha', \beta'\} = \mathrm{compat}(\tau m')$. By the above, $\alpha \neq \beta$ and $\{\alpha, \beta\}$ is not coverable. Similarly, $\alpha' \neq \beta'$ and $\{\alpha', \beta'\}$ is not coverable. Since $\{\alpha, \beta\} \neq \{\alpha', \beta'\}$, either $\alpha' \notin \{\alpha, \beta\}$ or

$\beta' \notin \{\alpha, \beta\}$. We assume without loss of generality that $\alpha' \notin \{\alpha, \beta\}$. (Figure 4 illustrates this construction.)

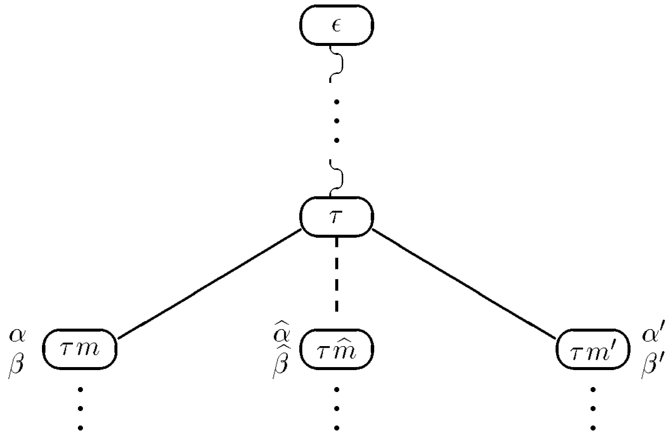

Figure 4: Tree of feasible conversations

By Proposition 2.4, there is a coordinate x such that $\alpha' \neq_x \alpha$ and $\alpha' \neq_x \beta$. Let y and z be such that $\langle\beta\rangle_y = \langle\alpha\rangle_x$ and $\langle\alpha\rangle_z = \langle\beta\rangle_x$. Let the message vector $\widehat{m}$ be defined by $\langle\widehat{m}\rangle_x = \langle m'\rangle_x$ and $\langle\widehat{m}\rangle_i = \langle m\rangle_i$ for $i \neq x$.

By Lemma 6.3 (parts 1–3) applied to α, β, α', and x, there is a deal $\widehat{\alpha}$ such that (by part 1) $\widehat{\alpha}$ is a feasible interpolant of $\{\alpha, \beta, \alpha'\}$,

$$\widehat{\alpha} =_x \alpha' \tag{1}$$

and (by part 2) $\widehat{\alpha}$ is compatible with $\tau\widehat{m}$. Since $\alpha' \neq_x \alpha$ and $\alpha' \neq_x \beta$, it follows (by part 3) that

$$\widehat{\alpha} =_y \beta \tag{2}$$

$$\widehat{\alpha} =_z \alpha \tag{3}$$

Similarly, by Lemma 6.3 (parts 1–3) applied to α, β, β', and x, there is a deal $\widehat{\beta}$ such that (by part 1) $\widehat{\beta}$ is a feasible interpolant of $\{\alpha, \beta, \beta'\}$,

$$\widehat{\beta} =_x \beta' \tag{4}$$

and (by part 2) $\widehat{\beta}$ is compatible with $\tau\widehat{m}$. By Proposition 2.3, since $\{\alpha, \beta\}$ is not coverable, α and β do not touch. In particular, $\alpha \neq_x \beta$. Hence $\widehat{\beta} \neq_x \alpha$ or $\widehat{\beta} \neq_x \beta$. It follows (by part 3) that

$$\widehat{\beta} =_y \beta \text{ or } \widehat{\beta} =_z \alpha \tag{5}$$

Since $\{\alpha', \beta'\}$ is not coverable, it follows from Proposition 2.3 that α' and β' do not touch. Thus, in particular, $\alpha' \neq_x \beta'$. Hence it follows from (1) and (4) that $\widehat{\alpha} \neq_x \widehat{\beta}$.

Therefore $\widehat{\alpha}$ and $\widehat{\beta}$ are distinct. By (2), (3), and (5), $\widehat{\alpha} =_y \widehat{\beta}$ or $\widehat{\alpha} =_z \widehat{\beta}$. Thus $\widehat{\alpha}$ touches $\widehat{\beta}$ at y or z. By Proposition 2.3, $\{\widehat{\alpha}, \widehat{\beta}\}$ is coverable.

Since $\widehat{\alpha}$ and $\widehat{\beta}$ are compatible with $\tau\widehat{m}$, it follows that $\tau\widehat{m}$ is a feasible conversation and $\{\widehat{\alpha}, \widehat{\beta}\} \subseteq \text{compat}(\tau\widehat{m})$. Then $\tau\widehat{m}$ is a child of τ in the tree of feasible conversations, so $\text{compat}(\tau\widehat{m})$ is not coverable and $|\text{compat}(\tau\widehat{m})| = 2$. Since $\{\widehat{\alpha}, \widehat{\beta}\} \subseteq \text{compat}(\tau\widehat{m})$ and $\widehat{\alpha} \neq \widehat{\beta}$, it follows that $\text{compat}(\tau\widehat{m}) = \{\widehat{\alpha}, \widehat{\beta}\}$, a contradiction since $\{\widehat{\alpha}, \widehat{\beta}\}$ is coverable. ■

7 A Bound on the Perfect Capacity of Any Signature

Fischer, Paterson and Rackoff [2] show that 2-valued perfect secret key exchange is not possible for teams of size two if a random legal deal does not provide sufficient shared information for the team. In [3], we generalize their result to arbitrarily large teams. Here, we further generalize this result to show an upper bound on the perfect capacity of any signature. This bound is an improvement over the bound implied by Theorem 4.4. A further generalization of this result yielding an upper bound on the perfect capacity of any source appears in [16].

Fix a signature $\xi = (s_1, \ldots, s_k; d)$. In a card game ξ-system, the team players are dealt a uniformly distributed random *legal* ξ-deal. We define ψ to be the probability that a uniformly distributed random *general* ξ-deal is legal. That is, ψ is the number of legal ξ-deals divided by the number of general ξ-deals. Note that in both a random legal deal and in a random general deal, each hand h_i is uniformly distributed over H_i^{ξ}. The difference is that in a random general deal, the hands $h_1, \ldots, h_k$ are independent, whereas in a random legal deal, they are correlated. Hence, only in the random legal deal does h_i give player P_i any information about the cards in other player's hands. In some sense, the larger ψ, the less shared information a random legal deal contains for the team players. This is made precise in Theorem 7.2 below.

We will need the following lemma about real numbers. It is proved using the arithmetic and geometric means inequality (AGM), which says that if a_1 through a_m are nonnegative, then $\sqrt[m]{\prod_{i=1}^{m} a_i} \leq \left(\sum_{i=1}^{m} a_i\right)/m$.

Lemma 7.1 *Let x_i^j be nonnegative for $1 \leq i \leq p$ and $1 \leq j \leq q$. Then*

$$\min_{j\in\{1,\ldots,q\}} \left(\prod_{i=1}^{p} x_i^j\right) \leq \frac{1}{q^p} \prod_{i=1}^{p} \sum_{j=1}^{q} x_i^j$$

Proof: Let x_i^j be nonnegative for $1 \leq i \leq p$ and $1 \leq j \leq q$. Then

$$\min_{j\in\{1,\ldots,q\}} \left(\prod_{i=1}^{p} x_i^j\right) \leq \sqrt[q]{\prod_{j=1}^{q}\prod_{i=1}^{p} x_i^j} \qquad (6)$$

$$= \prod_{i=1}^{p} \sqrt[q]{\prod_{j=1}^{q} x_i^j} \qquad (7)$$

$$\leq \prod_{i=1}^{p}\left(\frac{\sum_{j=1}^{q} x_i^j}{q}\right) \quad (8)$$

$$= \frac{1}{q^p}\prod_{i=1}^{p}\sum_{j=1}^{q} x_i^j \quad (9)$$

Here, (6) holds because the qth root of the product of q positive numbers is always at least as big as the smallest of the numbers. (8) is by the AGM. (7) and (9) are direct algebraic manipulation. ■

Theorem 7.2 *Let* $\xi = (s_1, \ldots, s_k; d)$. *Then* $\mathrm{pcap}(\xi) \leq \left\lfloor \psi^{\left(\frac{1}{1-k}\right)} \right\rfloor$.

Proof: Let $\xi = (s_1, \ldots, s_k; d)$ and $N = \mathrm{pcap}(\xi)$. We show that $N \leq \left\lfloor \psi^{\left(\frac{1}{1-k}\right)} \right\rfloor$.

By the definition of perfect capacity, there exists a card game ξ-system $\mathcal{P}_\mathcal{S}$ for N-valued perfect secret key exchange. Since $\mathcal{P}_\mathcal{S}$ is a card game system, $\mathcal{S}$ is a randomized extension of a legal source for D^ξ. Let $\mathcal{T}$ be a canonical source that is team-equivalent to $\mathcal{S}$ (such a source exists by Proposition 2.2). It follows from Proposition 2.5 that $\mathcal{P}_\mathcal{T}$ is a card game ξ-system and it follows from Proposition 3.4 that $\mathcal{P}_\mathcal{T}$ performs N-valued perfect secret key exchange. Hence $U^\mathcal{T} = U^\mathcal{P} = (R_1 \times H_1^\xi) \times \ldots \times (R_k \times H_k^\xi)$ for some $R_1, \ldots, R_k$, and for $u \in U^\mathcal{P}$,

$$\Pr_\mathcal{T}(u) = \begin{cases} \frac{1}{|L^\xi|}\prod_{i=1}^{k}\Pr_{\mathcal{R}_i}(\mathrm{ind}_i(u)) & \text{if } \mathrm{corr}(u) \in L^\xi \\ 0 & \text{otherwise} \end{cases}$$

where $\mathcal{R}_i$ is the distribution $\mathcal{T}$ induces on R_i.

We construct another canonical source $\mathcal{T}'$ for $U^\mathcal{P}$ in which the distribution of the independent part is the same as in $\mathcal{T}$, but all deals (including the illegal ones) are given equal probability. Specifically, we let $\mathcal{T}'$ be a canonical source for $U^\mathcal{P}$ such that for every $u \in U^\mathcal{P}$,

$$\Pr_{\mathcal{T}'}(u) = \frac{1}{|D^\xi|}\prod_{i=1}^{k}\Pr_{\mathcal{R}_i}(\mathrm{ind}_i(u)) \quad (10)$$

(Such a source exists by Proposition 2.2.) Then $\Omega^\mathcal{T} = \Omega^{\mathcal{T}'} = U^\mathcal{P}$. Since $\psi = |L^\xi|/|D^\xi|$, $\Pr_\mathcal{T}(u) \leq (sfrac1\psi)\Pr_{\mathcal{T}'}(u)$. It follows that for any event $X \in U^\mathcal{P}$,

$$\Pr_\mathcal{T}[X] \leq \frac{1}{\psi}\Pr_{\mathcal{T}'}[X] \quad (11)$$

Let $\mathcal{H}_i$ be the distribution induced on H_i^ξ by $\mathcal{T}'$. Since $D^\xi = H_1^\xi \times \cdots \times H_k^\xi$, it follows from (10) that $\Pr_{\mathcal{H}_i}(h_i) = 1/|H_i^\xi|$ for every $h_i \in H_i^\xi$. Hence for any $h_1, \ldots, h_k$,

$$\frac{1}{|D^\xi|} = \prod_{i=1}^{k}\Pr_{\mathcal{H}_i}(h_i) \quad (12)$$

It follows from (10) and (12) that

$$\begin{aligned}
\Pr_{\mathcal{T}'}(u) &= \prod_{i=1}^{k} \left(\Pr_{\mathcal{R}_i}(\mathrm{ind}_i(u)) \cdot \Pr_{\mathcal{H}_i}(\langle \mathrm{corr}(u)\rangle_i)\right) \\
&= \prod_{i=1}^{k} \Pr_{(\mathcal{R}_i \times \mathcal{H}_i)}(\langle u \rangle_i)
\end{aligned}$$

That is, $\mathcal{T}' = (\mathcal{R}_1 \times \mathcal{H}_1) \times \cdots \times (\mathcal{R}_k \times \mathcal{H}_k)$. Since $\theta_i^{\mathcal{T}'}(u) = \langle u \rangle_i$, each $\theta_i^{\mathcal{T}'}$ depends only on the i^{th} component of its argument. It follows that the random variables $\theta_1^{\mathcal{T}'}, \ldots, \theta_k^{\mathcal{T}'}$ are independent.

Let $\sigma \in \mathsf{cc}$. The event $\overline{\mathrm{C}}_i(\sigma)$ respects the random variable $\theta_i^{\mathcal{T}'}$ for $i \in K$. It follows that the events $\overline{\mathrm{C}}_1(\sigma), \ldots, \overline{\mathrm{C}}_k(\sigma)$ are independent. Hence, by Lemma 3.5,

$$\Pr_{\mathcal{T}'}[\mathrm{C}(\sigma)] = \prod_{i=1}^{k} \Pr_{\mathcal{T}'}\left[\overline{\mathrm{C}}_i(\sigma)\right] \tag{13}$$

Similarly, if $v \in V$, then the event $\overline{\mathrm{CO}}_i(\sigma, v)$ respects $\theta_i^{\mathcal{T}'}$. Hence, for any $v \in V$, the events $\overline{\mathrm{CO}}_1(\sigma, v), \ldots, \overline{\mathrm{CO}}_k(\sigma, v)$ are independent. By Lemma 3.6,

$$\Pr_{\mathcal{T}'}[\mathrm{CO}(\sigma, v)] = \prod_{i=1}^{k} \Pr_{\mathcal{T}'}\left[\overline{\mathrm{CO}}_i(\sigma, v)\right] \tag{14}$$

Therefore,

$$\begin{aligned}
\Pr_{\mathcal{T}}[\mathrm{C}(\sigma)] &= N \min_{v \in V} \left(\Pr_{\mathcal{T}}[\mathrm{CO}(\sigma, v)]\right) && (15) \\
&\leq N \min_{v \in V} \left(\frac{1}{\psi} \Pr_{\mathcal{T}'}[\mathrm{CO}(\sigma, v)]\right) && (16) \\
&= N \min_{v \in V} \left(\frac{1}{\psi} \prod_{i=1}^{k} \Pr_{\mathcal{T}'}\left[\overline{\mathrm{CO}}_i(\sigma, v)\right]\right) && (17) \\
&\leq \frac{N}{N^k} \cdot \frac{1}{\psi} \prod_{i=1}^{k} \left(\sum_{v \in V} \Pr_{\mathcal{T}'}\left[\overline{\mathrm{CO}}_i(\sigma, v)\right]\right) && (18) \\
&= \frac{1}{\psi \cdot N^{k-1}} \prod_{i=1}^{k} \Pr_{\mathcal{T}'}\left[\overline{\mathrm{C}}_i(\sigma)\right] && (19) \\
&= \frac{1}{\psi \cdot N^{k-1}} \Pr_{\mathcal{T}'}[\mathrm{C}(\sigma)] && (20)
\end{aligned}$$

Here, (15) follows from Lemma 3.8, (16) follows from (11), (17) follows from (14), (18) follows from Lemma 7.1, (19) follows from the fact that $\overline{\mathrm{C}}_i(\sigma)$ is the disjoint union over $v \in V$ of $\overline{\mathrm{CO}}_i(\sigma, v)$, and (20) follows from (13).

Summing over all complete conversations yields

$$1 = \sum_{\sigma \in \mathsf{CC}} \Pr_{\mathcal{T}}[\mathrm{C}(\sigma)] \leq \sum_{\sigma \in \mathsf{CC}} \frac{1}{\psi \cdot N^{k-1}} \Pr_{\mathcal{T}'}[\mathrm{C}(\sigma)] = \frac{1}{\psi \cdot N^{k-1}}$$

Since N is an integer, it follows immediately that

$$N \leq \left\lfloor \psi^{\left(\frac{1}{1-k}\right)} \right\rfloor$$

as desired. ∎

For the case $k = 2$, the bound given by Theorem 7.2 is identical to a bound implied by a result of Maurer ([7], Corollary 1). Maurer's framework is more general than ours for the case $k = 2$ but does not seem to generalize to larger k.

Calculating $\psi = |L^\xi|/|D^\xi|$, we can apply Theorem 7.2 to obtain an upper bound on the perfect capacity of any signature. Some examples follow.

Corollary 7.3 $\mathrm{pcap}(2, 1; 4) = 2$.

Proof: In this case

$$\psi = \frac{\binom{4}{2}\binom{2}{1}}{\binom{4}{2}\binom{4}{1}} = \frac{1}{2}$$

Since $k = 2$, it follows by Theorem 7.2 that $\mathrm{pcap}(2, 1; 4) \leq 2$. As seen in Section 1.1, 2-valued perfect secret key exchange is possible for $(2, 1; 4)$ even if Eve is allowed to look at the remaining card, so $\mathrm{pcap}(2, 1; 4) \geq 2$. Hence $\mathrm{pcap}(2, 1; 4) = 2$. ∎

Corollary 7.4 $\mathrm{pcap}(2, 2, 2; 7) \leq 3$.

Proof: In this case $k = 3$ and

$$\psi = \frac{\binom{7}{2}\binom{5}{2}\binom{3}{2}}{\binom{7}{2}^3} = \frac{10}{147}$$

so $\mathrm{pcap}(2, 2, 2; 7) \leq \left\lfloor \left(\frac{10}{147}\right)^{-\frac{1}{2}} \right\rfloor = 3$. ∎

8 Concluding Remarks

We have presented a model for multiparty communication among players receiving correlated inputs. Our model makes it possible to reason formally about intuitive concepts based on shared knowledge in a multiparty setting. We have defined several variations of the secret key exchange problem in this model. We study *exact* secret key exchange, in which every run of a system succeeds in obtaining a secret key. Further extension of this work might investigate various approximations of exact secret key exchange. There are many possible types of approximations to consider, such as for example, allowing a small probability that the players' outputs do not agree or that Eve learn a player's output, or requiring only that the distribution on outputs given Eve's view and the conversation is close to the *a priori* distribution.

We explored the use of a random deal of cards for secret key exchange and showed several bounds on the capacity of such deals. These bounds hold for all view functions for Eve. We do not know how to use the additional information given to Eve to improve these results for any particular view function. In [4, 5, 16], we exhibit N-valued perfect secret key exchange ξ-protocols for certain values of ξ and N. However, except in some simple cases of ξ, there is a gap between the value N such that we can exhibit an N-valued secret key exchange ξ-protocol and the value N' for which the results in this paper show that no N'-valued secret key exchange ξ-protocol exists. It remains open to improve these bounds and to determine an exact characterization of the weak and perfect capacity of an arbitrary signature ξ. Wright [16] exhibits a source $\mathcal{T}$ such that the perfect capacity of $\mathcal{T}$ is strictly less than the weak capacity of $\mathcal{T}$. It is open whether there exist *signatures* ξ such that the perfect capacity of ξ is strictly less than the weak capacity of ξ. We conjecture that such a signature does not exist because of the symmetry inherent in the structure of a deal.

9 Acknowledgements

We thank Nick Reingold for suggesting a simpler proof of Lemma 7.1.

References

[1] D. Beaver, S. Haber, and P. Winkler. On the isolation of a common secret. Preprint, Bellcore, 1993.

[2] M. J. Fischer, M. S. Paterson, and C. Rackoff. Secret bit transmission using a random deal of cards. In *Distributed Computing and Cryptography*, volume 2 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 173–181. American Mathematical Society, 1991.

[3] 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.

[4] M. J. Fischer and R. N. Wright. An application of game theoretic techniques to cryptography. In *Complexity Theory*, volume 13 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 99–118. American Mathematical Society, 1993.

[5] M. J. Fischer and R. N. Wright. An efficient protocol for unconditionally secure secret key exchange. In *Proc. 4th Annual Symposium on Discrete Algorithms*, pages 475–483, January 1993.

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

[7] U. M. Maurer. Secret key agreement by public discussion from common information. *IEEE Trans. on Information Theory*, 39(3):733–742, May 1993.

[8] A. Orlitsky. Worst-case interactive communication I: Two messages are almost optimal. *IEEE Trans. on Information Theory*, 36(5):1111–1126, September 1990.

[9] A. Orlitsky. Worst-case interactive communication II: Two messages are not optimal. *IEEE Trans. on Information Theory*, 37(4):995–1005, July 1991.

[10] M. Rabin. Cryptography without secrets. Presented at *DIMACS 1990 Workshop on Cryptography*, Princeton, NJ, October 1990.

[11] S. Rudich. *Limits on the Provable Consequences of One-way Functions.* PhD thesis, University of California at Berkeley, 1988.

[12] C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, pages 656–715, 1949.

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

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

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

[16] R. N. Wright. *Achieving Perfect Secrecy Using Correlated Random Variables.* PhD thesis, Yale University, 1994.