A Secret Common Information Duality
for Tripartite Noisy Correlations

Pradeep Kr. Banerjee
Indian Institute of Technology Kharagpur
pradeep.banerjee@gmail.com

Abstract. Given many independent realizations of a tripartite noisy correlation $p_{XYZ}$ shared between honest Alice($X$) and Bob($Y$) and an adversary Eve($Z$), we explore the duality between the secrecy extractable from $p_{XYZ}$ and that required to simulate $p_{XYZ}$. Such a duality mirrors a similar well-known operational duality between the two notions of common information due to Gács and Körner, and Wyner. For the inverse problem of simulating $p_{XYZ}$ from a noiseless secret key and unlimited public communication, we show that Winter’s (2005) result for the key cost in terms of a conditional version of Wyner’s common information can be simply reexpressed in terms of the existence of a tripartite protocol monotone. For the forward problem of key distillation from $p_{XYZ}$ without any communication, we construct simple distributions for which the conditional Gács and Körner common information achieves a tight bound on the secret key rate. We also comment on the interconvertibility of secret correlations under local operations and public communication.

Keywords: Information-theoretic security, secret key agreement, common information, monotones

1 Introduction

Shared secret keys (SKs) are a fundamental resource in many distributed information processing protocols. Unconditionally secure key distribution is impossible to realize from scratch, for instance, if the legitimate parties are only given access to a noiseless public communication channel [1]–[3]. This pessimism can however be relativized if the parties are additionally given access to simple auxiliary devices (e.g., noisy correlations or communication channels) that is not completely under the control of an adversary [14], [15]. Thus, information-theoretic reductions between such primitives are of great interest. Pre-distributed noisy correlations is a simple yet powerful cryptographic resource that takes no inputs from the parties, and generates samples of a given joint distribution, with party-$i$ given access to copies of the $i$-th variable. Interconvertibility of noisy tripartite correlations and a uniformly distributed, noiseless SK have been studied under the rubric of SK agreement by public discussion (called the forward problem, originally attributed to Maurer [1], [2], and Ahlswede and Csiszár [19]) and the dual problem of simulating a noisy correlation from noiseless SK and
public communication (called the inverse problem, due to Winter [4] and Renner and Wolf [3]). In general, there are irreversible losses in exchanging noisy correlations in that, going from one noisy correlation to another and back is not lossless (even asymptotically) [3], [17]. In light of the resource character of noisy correlations in enabling SK agreement, and that of SK in simulating a tripartite correlation, quantifying such resources are of interest.

To make things precise, consider three distant parties, honest Alice and Bob, and an adversary Eve who observe sequences \( X^n = (X_1, ..., X_n) \), \( Y^n = (Y_1, ..., Y_n) \), and \( Z^n = (Z_1, ..., Z_n) \) respectively, where the sequence triple \( (X^n, Y^n, Z^n) \) has the generic component variables \( (X,Y,Z) \sim p_{XYZ} \). We seek to explore the duality implicit in the forward and the inverse problem. Starting with no initially shared SKs, and using only local operations and unlimited public communication (LOPC) via a noiseless, authenticated (but, otherwise insecure and transparent to Eve) public discussion channel, what is the maximum rate at which Alice and Bob can distil a SK (i.e., the maximum possible SK rate), such that Eve’s information \( (Z^n \text{ and the entire public discussion}) \) about the generated SK is arbitrarily small? Conversely, starting with perfect SKs, what is the SK cost of creating the correlated triple \( XYZ \) using only LOPC?

Appealing to the well-known operational duality between the simulation and extraction of common randomness (CR) [12], as measured by respectively, the two notions of common information (CI) due to Wyner [8], and Gács and Körner [7], we explore a similar duality between the simulation and extraction of secret correlations. For the inverse problem of simulating \( p_{XYZ} \) from noiseless SK and unlimited public communication, Winter [4] gave a single-letter characterization of the asymptotic minimal SK cost of formation in terms of a conditional version of Wyner’s CI. We first show that Winter’s (2005) result for the SK cost of formation can be simply reexpressed in terms of the existence of a tripartite protocol monotone. For the forward problem of key distillation from \( p_{XYZ} \) without any communication, we construct simple distributions for which the conditional Gács and Körner CI captures the “explicit” secret CI, thus achieving a tight bound on the SK rate. We also comment on the lossless exchange of secret correlations under LOPC.

2 CI Duality and Secret CI

Random variables (RVs) and their finite alphabets are denoted using uppercase letters \( X \) and script letters \( \mathcal{X} \). \( X^n \) denotes the sequence \( (X_1, ..., X_n) \). \( p_X(x) = \Pr\{X = x\} \) denotes the distribution (pmf) of a discrete RV \( X \). \( X \rightarrow Y \rightarrow Z \) denotes that \( X, Y, Z \) form a Markov chain satisfying \( p_{XYZ} = p_{XY}p_{YZ} \). Likewise, \( X, Y, Z \) is said to form a conditional Markov chain given \( U \) if \( X \rightarrow U \rightarrow Y \rightarrow Z \). The entropy of \( X \) is defined as \( H(X) = -\sum_{x \in \mathcal{X}} p_X(x) \log p_X(x) \) and the mutual information of \( X \) and \( Y \) is given by \( I(X; Y) = H(X) - H(X|Y) \). The total variational distance between \( p_X \) and \( p_{X'} \) is defined as \( TV(p_X, p_{X'}) = \frac{1}{2} \sum_{x \in \mathcal{X}} |p_X(x) - p_{X'}(x)| \).

The zero pattern of \( p_{XY} \) can be specified by its characteristic bipartite graph \( B_{XY} \) with the vertex set \( X \cup \mathcal{Y} \) and an edge connecting two vertices \( x \) and \( y \) iff
\(p_{XY}(x,y) \geq 0\). If \(B_{XY}\) contains only a single connected component, we say that \(p_{XY}\) is indecomposable. An ergodic decomposition of \(p_{XY}(x,y)\) is defined by a unique partition of the space \(X \times Y\) into connected components. The following double markovity lemma [12] (also see Problem 16.25, p. 392 in [11]) is useful.

**Lemma 1.** A triple of RVs \((X,Y,Q)\) satisfies the double Markov conditions

\[
X - Y - Q, \quad Y - X - Q
\]

iff there exists a pmf \(p_{Q|XY}\) such that \(H(Q'|X) = H(Q'|Y) = 0\) and \(X - Y - Q\). Furthermore, (1) implies \(I(Y;Q) \leq H(Q)\) with equality iff \(H(Q'|Q) = 0\).

**Proof.** Given \(p_{Q|XY}\) such that \(X - Y - Q\) and \(Y - X - Q\), it follows that \(p_{XY}(x,y) > 0 \Rightarrow p_{Q|XY}(q|x,y) = p_{Q|X}(q|x) = p_{Q|Y}(q|y) \forall q\). Given an ergodic decomposition of \(p_{XY}(x,y)\) such that \(X = Y = \bigcup_{q} X_{q} \times Y_{q}\), where the \(X_{q}\)'s and \(Y_{q}\)'s having different subscripts are disjoint, define \(p_{Q|XY}\) as \(Q' = q'\) iff \(x \in X_{q'} \Leftrightarrow y \in Y_{q'}\). Clearly \(H(Q'|X) = H(Q'|Y) = 0\). Then, for any \(Q = q\) and for every \(q\), \(p_{Q|XY}(q',.)\) is constant over \(X_{q'} \times Y_{q'}\). This implies that \(p_{Q|XY}(q|x,y) = p_{Q|Q}(q'|q)\) so that \(XY - Q' - Q\). The converse is obvious. Thus, given (1), we get \(Q'\) such that \(I(X;Y;Q') = 0\) so that \(I(X;Y;Q) = I(X;Q') = I(Q';Q) = H(Q') - H(Q'|Q) \leq H(Q')\).

Gács and Körner (GK) [7] defined CI as the maximum rate of CR \((R)\) that Alice and Bob, observing sequences \(X^n\) and \(Y^n\) separately can extract without communication \((R_0 = 0)\), i.e., \(C_{GK}(X;Y) = \max_{Q} \frac{1}{n}H(f_1(X^n))\) where the su is taken over all sequences of pairs of deterministic mappings \((f_1^n, f_2^n)\) such that \(\Pr\{f_1^n(X^n) \neq f_2^n(Y^n)\} \rightarrow 0\) as \(n \rightarrow \infty\) (see setup in Fig. 1(a)). GK showed that

\[
C_{GK}(X;Y) = \max_{Q: H(Q|X) = H(Q|Y) = 0} H(Q) = H(Q_*)
\]

where \(Q_*\) is the maximal common RV of the pair \((X,Y)\) induced by the ergodic decomposition of \(p_{XY}\). For all \(X,Y\), we have \(I(X;Y) = H(Q_*) + I(X;Y|Q_*)\). We say that \(p_{XY}\) is resolvable, if \(I(X;Y|Q_*) = 0\). An alternative characterization of \(C_{GK}(X;Y)\) follows from Lemma 1 [12].

\[
C_{GK}(X;Y) = \max_{Q: Q - X - Y, Q - Y - X} I(X;Q), \quad |Q| \leq |X||Y| + 2
\]

\(C_{GK}(X;Y)\) is identically zero for all indecomposable distributions. For example, a binary symmetric channel with non-zero crossover probability is indecomposable and hence \(C_{GK}(X;Y) = 0\). Thus, CR is a far stronger resource than correlation, in that the latter does not result in common random bits, in general. Nevertheless, when Alice communicates with Bob \((R_0 > 0)\), they can unlock hidden layers of potential CR [9]. With a high enough rate of communication (that is independent of Bob’s output), the CR rate increases to \(I(X;Y)\) [9].

A conditional version of GK CI is defined as follows.

\[
C_{GK}(X;Y|Z) = H(Q_*|Z) = \max_{Q: H(Q|Z) = 0} H(Q) = \max_{Q: H(Q|Y) = 0} I(X;Y|Z)
\]

Conditioning always reduces GK CI, i.e., \(C_{GK}(X;Y|Z) \leq C_{GK}(X;Y)\). We say that \(p_{XYZ}\) is conditionally resolvable, if \(I(X;Y|ZQ_*) = 0\).
Wyner [8] defined CI as the minimum rate of CR ($R$) needed to generate $X^n$ and $Y^n$ separately using local operations (independent noisy channels: $Q \rightarrow X^n$, $Q \rightarrow Y^n$) and no communication ($R_0 = 0$) (see setup in Fig. 1(b)).

$$C_W(X; Y) = \min_{Q : X - Q - Y} I(X; Y | Q)$$ \quad (5)

Likewise, a conditional version of Wyner’s CI is defined as follows.

$$C_W(X; Y | Z) = \min_{Q : X - Q - Z - Y} I(X; Y | Q)$$ \quad (6)

$C_W(X; Y)$ quantifies the resource cost for the distributed approximate simulation of $p_{XY}$. When Alice communicates with Bob ($R_0 > 0$), with a high enough rate of communication (independent of Bob’s output), the CR rate reduces to $I(X; Y)$ [9]. Reversing the direction of Alice’s operation ($X^n \rightarrow Q^n$) (see Fig. 1(c)) leads to two-stage simulation of a noisy channel via the Markov chain $X - Q - Y$.

Now Alice and Bob can use the reverse Shannon theorem [10] to simulate a first stage, with Alice mapping $X^n$ to some intermediate RV $Q^n$ which she sends noiselessly to Bob. In the second stage, Bob locally maps $Q^n$ to get $Y^n$. This gives a nontrivial tradeoff between the (noiseless) communication rate $R_0$ and CR rate $R$ leading to an alternative characterization of Wyner’s CI as the communication cost of distributed channel simulation without any CR ($R = 0$). With unlimited CR, the cost reduces to $I(X; Y)$ [9]. Finally, to complete the duality, we note the following well-known relation between the different notions of CI [12]: $C_{GK}(X; Y) \leq I(X; Y) \leq C_W(X; Y)$ with equality holding iff $p_{XY}$ is resolvable, whence $C_{GK}(X; Y) = I(X; Y) \Leftrightarrow I(X; Y) = C_W(X; Y)$.

The setup for the standard SK agreement scenario [1–3], [14–16] shown in Fig. 1(d) is a generalization of the GK setup (see Fig. 1(a)) that now allows for interactive communication. Consider the following distributed communication protocol, $II_{KA}$. Alice ($X$) and Bob ($Y$) have independent access to unlimited local randomness and communicate interactively with each other over a noiseless public discussion channel (transparent to Eve ($Z$)). The protocol proceeds in rounds, where in each round each party flips private coins, and based on the messages exchanged so far, publicly sends a message to the other party. At the end of the protocol, Alice (Bob) either accepts or rejects the protocol execution, and outputs a key $Q_X$ ($Q_Y$) depending on her (his) view of the protocol, which comprises of $X^n$ ($Y^n$), all local computations, and the entire public communication (encapsulated in the RV $C$). The asymptotic maximum rate of SK distillation is called the SK rate.

**Definition 2.** The SK rate, $S(X; Y | Z)$ is defined as the largest real number $R$ such that for all $\epsilon > 0$, there exists an integer $n$ and a randomized protocol $II_{KA}$ with communication $C$ that with probability $1 - \epsilon$, allows Alice (knowing $X^n$) and Bob (knowing $Y^n$) to compute $Q_X$ and $Q_Y$, respectively, satisfying $\Pr[Q_X = Q_Y = Q] \geq 1 - \epsilon$, $H(Q) = \log |Q| \geq n(R - \epsilon)$, $I(Q; C Z^n) < \epsilon$.

Analogously, there exists an inverse protocol $II_{form}$, and a dual measure, the asymptotic minimal SK cost of formation of the triple $(X, Y, Z)$ ~ $p_{XYZ}$ [3–6]. While the distributed channel synthesis problem [9] (setup in Fig. 1(b))
Fig. 1. Common information duality (with communication): (a) Gács and Körner’s setup \((R_0 = 0)\) [7] (b) Wyner’s setup \((R_0 = 0)\) [8] (c) Inverting Alice’s channel gives an alternative characterization of Wyner’s CI as the communication cost of channel simulation without any CR \((R = 0)\) [9], [10] (d) Setup for SK agreement [1]–[3] (e) Setup for distributed simulation of tripartite correlations from SK and public communication [3]–[6]

explores the role of CR and one-way communication in the formation of bipartite correlations \(p_{XY}\) shared between honest Alice and Bob, the setup in Fig. 1(e) explores the role of secret CR (i.e., SK) and public communication in the distributed simulation of tripartite correlations \(p_{XYZ}\), now additionally shared with an adversary Eve [3]–[6]. To start with, Alice and Bob share a SK in the form of \(R\) perfectly correlated bits, i.e., Alice has \(Q_X\) and Bob, \(Q_Y\) such that \(Q_X = Q_Y = Q\) and \(H(Q) = R\). The goal is to approximately simulate correlated sequence triples of the form \((X^n, Y^n, Z^n)\), up to a local degrading of \(Z^n\). At the end of the protocol, Alice and Bob output \(\hat{X}_n\) and \(\hat{Y}_n\) as deterministic functions of their views, which comprises of the shared SK \(Q\), all the private coins flipped so far, and the entire public communication \((C)\). Discounting the private randomness by allowing for stochastic mappings, \(\Pi_{form}\) can be specified by a joint distribution \(p_{X^nY^n|CQ} = p_{X^n|CQ}p_{Y^n|CQ}p_{CQ}\). The resulting simulation is “good” from Alice and Bob’s point of view, if they end up correctly generating the marginal \(p_{X^nY^n}\). However, this does not discount the fact that Eve \((Z^n)\) might still have some information about \(X^nY^n\). This is formalized by requiring that Eve’s optimal channel \(p_{Z|Z^n}\) is only able to simulate the public communication \((C)\) used by Alice and Bob to generate \((\hat{X}_n, \hat{Y}_n)\). The following definition makes this precise [3].
Definition 3. The SK cost of formation, $SK_c(X;Y|Z)$ is the infimum of all numbers $R \geq 0$ such that for all $\epsilon > 0$, there exists an integer $n$ and a randomized protocol $\Pi_{\text{form}}$ with communication $C$ that with probability $1 - \epsilon$, allows Alice and Bob, knowing a common random $\lfloor nR \rfloor$-bit string $Q$, to compute $\hat{X}^n$ and $\hat{Y}^n$, respectively, such that for some correlated sequence triple $(X^n, Y^n, Z^n)$ that has generic component variables $(X,Y,Z) \sim p_{X,Y,Z}$ and some channel $p_{\bar{Z}|Z^n}$.

$p_{X,Y,Z}$ contains secret correlations if it cannot be generated by LOPC, i.e., $SK_c(X;Y|Z) > 0$ [18]. Both the SK cost of formation and the SK rate are measures of the secrecy content of $p_{X,Y,Z}$ and admit a clear operational interpretation: $SK_c(X;Y|Z)$ quantifies the minimum amount of SK bits required to (approximately) simulate $p_{X,Y,Z}$, whereas $S(X;Y|||Z)$ quantifies the maximum amount of SK bits that one can extract from $p_{X,Y,Z}$.

Winter used resolvability-based arguments [4] to arrive at the full secret correlation vs. public communication trade-off for the inverse problem and defined the SK cost of formation with unlimited public communication as follows.

$$SK_c(X;Y|Z) = \min_{Q,Z} I(X;Y|Q,Z)$$

where the minimum is taken over all RVs $Q$ and $Z$. Cardinalities of the corresponding alphabets are bounded as $|Q| \leq |X||Y|$, and $|Z| \leq |Z|$ respectively. $SK_c(X;Y|Z)$ is bounded from below by the intrinsic information [3], that intuitively speaking, measures the correlation shared between Alice and Bob that Eve cannot access or destroy [2].

$$I(X;Y \downarrow Z) = \min_{Z} I(X;Y|Z)$$

where the cardinality of the alphabet $Z$ of RV $Z$ is bounded as $|Z| \leq |Z|$ [13].

3 Main contributions

3.1 Wyner’s Conditional CI and the SK Cost of Formation

$C_W(X;Y)$ can be interpreted as the SK cost of creating a product distribution with Eve. Now consider Eve’s optimal channel $p_{\bar{Z}|Z}$. To create a (public) correlation, Alice randomly samples $\bar{Z}$ and publicly announces the value of $\bar{Z}$ over a symmetric broadcast channel to Bob and Eve. Then the SK cost of creating the product distribution $p_{X,Y|\bar{Z}}$ is $C_W(X;Y|\bar{Z})$. In this section, we introduce the concept of protocol monotones [6], [14]–[17] for axiomatizing the general properties of upper bounds on the SK rate and show that $C_W(X;Y|\bar{Z})$ qualifies as such an upper bound and is a natural candidate for quantifying the SK cost of formation.

When distant parties wish to establish a SK by manipulating some set of private and public resources, it is natural to restrict attention to LOPC operations.
Since the “resourcefulness” or “secrecy content” of the state is a non-local property that cannot increase under LOPC, this set of transformations is deemed as a free resource. Mathematically, resources can be quantified by monotones, real-valued functions of joint distributions that cannot increase under LOPC. LOPC monotones were first introduced in [17] as classical counterparts of entanglement or LOCC (local operations and classical communication) monotones to study the asymptotic rate of resource conversion under LOPC. A resource cannot increase under LOPC operations by Alice and Bob. Since Eve, in her role as a malicious adversary is always assumed to operate optimally against Alice and Bob, the same resource cannot decrease under her LOPC operations [6], [14], [17]. We define a monotone as follows.

**Definition 4.** For all jointly distributed RVs \((X,Y,Z)\), let \(\mathcal{M}(X;Y|Z)\) be a real-valued function of \(p_{XYZ}\). Then \(\mathcal{M}\) is a monotone if the following hold:

1) Monotonicity under local operations (LO) by Alice and Bob: Suppose Alice modifies \(X\) to \(\tilde{X}\) by sending \(X\) over a channel, characterized by \(p_{X|\tilde{X}}\). Then \(\mathcal{M}\) can only decrease, i.e., for all jointly distributed RVs \((X,Y,Z,\tilde{X})\) with \(X : YZ - \tilde{X}\), \(\mathcal{M}(X;Y|Z) \leq \mathcal{M}(\tilde{X};Y|Z)\), and likewise for Bob.

2) Monotonicity under public communication (PC) by Alice and Bob: Suppose Alice publicly announces the value of \(\tilde{X}\). Then \(\mathcal{M}\) can only decrease, i.e., for all jointly distributed RVs \((X,Y,Z,\tilde{X})\) with \(X : YZ - \tilde{X}\), \(\mathcal{M}(X;Y|Z) \leq \mathcal{M}(\tilde{X};Y|Z)\), and likewise for Bob.

3) Monotonicity under local operations (LO) by Eve: Suppose Eve modifies \(Z\) to \(\tilde{Z}\) by sending \(Z\) over a channel, characterized by \(p_{Z|\tilde{Z}}\). Then \(\mathcal{M}\) can only increase, i.e., for all jointly distributed RVs \((X,Y,Z,\tilde{Z})\) with \(X : XY - \tilde{Z}\), \(\mathcal{M}(X;Y|Z) \geq \mathcal{M}(X;Y|\tilde{Z})\).

4) Monotonicity under public communication (PC) by Eve: Suppose Eve publicly announces the value of \(\tilde{Z}\). Then \(\mathcal{M}\) can only increase, i.e., for all jointly distributed RVs \((X,Y,Z,\tilde{Z})\) with \(H(\tilde{Z}|Z) = 0\), \(\mathcal{M}(\tilde{Z}X;\tilde{Z}Y|Z) \geq \mathcal{M}(X;Y|Z)\).

5) Additivity: \(\mathcal{M}\) is additive on tensor products.

6) Asymptotic continuity: For two pmf sequences \((p_{XYZ})_n,(q_{XYZ})_n\), if \(\text{TV}((p_{XYZ})_n,(q_{XYZ})_n) \to 0\) then \(\frac{1}{\log n}|\mathcal{M}((p_{XYZ})_n) - \mathcal{M}((q_{XYZ})_n)| \to 0\), where \(k_n\) is some constant that depends on \(|X|,|Y|\) and \(|Z|\).

If \(\mathcal{M}\) satisfies the conditions in Definition 4, then \(\mathcal{M}\) is an upper bound on the SK rate [14], [15]. Upper bounds on the rate at which instances of a target primitive can be realized per invocation of the source primitive can be obtained by comparing the value of the monotone on the source and target states. Thus, given the class of LOPC operations and \(n\) independent copies of \(p_{XYZ}\) and a target distribution \(q_{XYZ}\), the optimal rate \(R(p \to q)\) at which transformations \(p^{\otimes n}\overset{\text{LPC}}{\rightarrow} q^{\otimes m}\) are possible is defined as the infimum of \(\frac{1}{n}\). More generally, the asymptotic transition rates satisfy the relation, \(R(p \to q) \leq \frac{\mathcal{M}(\theta^\infty)}{M(\theta^\infty)}\), for each maximal resource \(\theta^\infty\) if \(\mathcal{M}(\theta^\infty) \neq 0\), where \(\mathcal{M}(\theta^\infty) = \limsup \frac{1}{n} \mathcal{M}(p^{\otimes n})\) [6], [17]. Thus if \(p^{S\Delta}_\Delta\) denotes the distribution of a perfect secret bit, i.e., \(p^{S\Delta}_\Delta(0,0,\delta) = p^{S\Delta}_\Delta(1,1,\delta) = \frac{1}{2}\), then
for any pmf $q_{XYZ}$, $S(X;Y||Z) = R(q \rightarrow p^*) \leq \frac{I(XY||Z)}{I(S;\Sigma \Delta)} = I(X;Y \downarrow Z)$, since 
$I(S;S \downarrow \Delta) = 1$, and $I(X;Y \downarrow Z)$ is a monotone [3]. Likewise $R(p^* \rightarrow q) \leq \frac{I(XY||Z)}{I(S;\Sigma \Delta)}$ and hence $SK_c(X;Y|Z) = \frac{1}{R(p^* \rightarrow q)} \geq I(X;Y \downarrow Z)$ [3]. 

$C_W(X;Y|Z)$ violates monotonicity under LO by Eve, and thus fails to achieve an upper bound on the SK rate. To preserve monotonicity under LO by Eve, an additional minimization is required over all stochastic maps $p_{Z|X}$ that can be chosen by Eve for locally processing her observations. This implies a minimization over all Markov chains $XY - Z - \tilde{Z}$. This yields a new quantity called Wyner’s intrinsic conditional CI that satisfies monotonicity under Eve’s LOPC operations.

$$C_W(X;Y \downarrow Z) = \min_{\tilde{Z}:XY - Z - \tilde{Z}} C_W(X;Y|\tilde{Z}) = \min_{\tilde{Z}:XY - Z - \tilde{Z}} I(XY;Q|\tilde{Z}) \quad (9)$$

The cardinality of the alphabet $\tilde{Z}$ of $\tilde{Z}$ is bounded as $|\tilde{Z}| \leq |Z|$. This can be shown following similar arguments as in [3] using Carathéodory’s theorem. From (6), we have $|Q| \leq |X||\tilde{P}|$. We now show that $C_W(X;Y \downarrow Z)$ is indeed a monotone and hence a valid upper bound on the SK rate.

**Lemma 5.** $C_W(X;Y \downarrow Z)$ is a monotone.

**Proof.** Let $p_{Z|X}$ be the minimizer in $C_W(X;Y \downarrow Z)$. Then it suffices to show that $C_W(X;Y|Z)$ satisfies monotonicity under Alice and Bob’s LOPC operations. We shall require the following monotonicity inequalities: (a) $H(Z|f(Y)) \geq H(Z|Y)$, (b) $I(X;Y|f(X)Z) \leq I(X;Y|Z)$. For all jointly distributed RVs $(XY\tilde{Z}X)$ such that $Y\tilde{Z} - X \sim X$, and $X - Q\tilde{Z} - Y$, monotonicity under LO by Alice holds since,

$$I(XY;Q|\tilde{Z}) = H(Q|\tilde{Z}) - H(Q|XY\tilde{Z}) \leq H(Q|\tilde{Z}) - H(Q|XY\tilde{Z}) = I(XY;Q|\tilde{Z}), \quad (a)$$

and likewise for Bob. For all jointly distributed RVs $(XY\tilde{Z}X)$ such that $H(\tilde{X}|X) = 0$ and $X - Q\tilde{Z} - Y$, monotonicity under PC by Alice holds since,

$$I(XY\tilde{X};Q\tilde{X}|\tilde{Z}) = I(XY;Q|\tilde{Z}) \leq I(XY;Q|\tilde{Z}), \quad (b)$$

and likewise for Bob. $C_W(X;Y \downarrow Z)$ is additive on tensor products and super-additive in general (see Proposition 6 in [4]). Asymptotic continuity fails since $C_W(X;Y \downarrow Z)$ is lockable [4], i.e., can fall sharply by an arbitrary large amount on giving away a single bit to Eve. □

Theorem 6 gives the main result of this section.

**Theorem 6.** With unlimited public communication, $SK_c(X;Y|Z) = C_W(X;Y \downarrow Z)$. Furthermore, if $p_{Z|X}$ is the optimal stochastic map achieving the minimum in the characterization of $C_W(X;Y \downarrow Z)$, then $C_W(X;Y \downarrow Z) = I(X;Y \downarrow Z)$ iff there exists a pmf $p_{Q'|XYZ\tilde{Z}}$ s.t. $H(Q'|X\tilde{Z}) = H(Q'|Y\tilde{Z}) = 0$ and $X - ZQ' - Y$.

---

1 Given jointly distributed RVs $(X,Y,Z,\tilde{Z})$ with $\tilde{Z} : XY - Z - \tilde{Z}$, it does not hold in general that $C_W(X;Y|\tilde{Z}) \geq C_W(X;Y|Z)$. 


for non-communicative key agreement models. We also comment on the lossless
achieves a tight bound on the SK rate. We conjecture that this holds in general
problem. GK showed that in a non-communicative model, common codes of a
beyond a certain deterministic interdependence of the sources. Remarkably, they
pair of discrete, memoryless correlated sources cannot exploit any correlation be-
For the general source model (with arbitrary public discussion), calculation of
the exact SK rate remains an open problem [1]–[3], [16]. Without any communi-

cation, the problem is still more complicated in that even the determin ation of

3.2 Gács and Körner (GK) Conditional CI and the SK Rate

For the general source model (with arbitrary public discussion), calculation of the exact SK rate remains an open problem [1]–[3], [16]. Without any communication, the problem is still more complicated in that even the determination of probability distributions that allow for the distillation of SK remains an unsolved problem. GK showed that in a non-communicative model, common codes of a pair of discrete, memoryless correlated sources cannot exploit any correlation beyond a certain deterministic interdependence of the sources. Remarkably, they showed that the asymptotic case is no better than the single shot case and that $C_{GK}(X;Y)$ depends only on the zero pattern of the underlying joint distribution $p_{XY}$. Intuitively, $C_{GK}(X;Y|Z)$ captures the most “explicit” form of secret CI, i.e., the maximum amount of SK that can be extracted without any communication. In this section, we construct simple distributions for which $C_{GK}(X;Y|Z)$ achieves a tight bound on the SK rate. We conjecture that this holds in general for non-communicative key agreement models. We also comment on the lossless interconvertibility of secret correlations.

Example 7. Consider the distribution $p_{XYZ}^1$ with $X = Y = Z = \{0,1,2,3\}$. We write $p_{XYZ}(a,b,c) = (abc)$. Given (000) = (011) = (101) = (110) = $\frac{1}{4}$, and (222) = (333) = $\frac{1}{4}$. Graphically, $p_{XYZ}^1$ is shown in the following table

(with Z’s value given in parentheses): $p_{XYZ}^1 = \frac{1}{4} \begin{pmatrix}
(1,0) & (1,1) & \cdots & \\
(1,1) & (1,0) & \cdots & \\
\vdots & \vdots & \ddots & \\
(2,2) & (2,1) & \cdots & (2,3)
\end{pmatrix}$. Alice, Bob and Eve each have access to this table and many independent copies of $X$, $Y$ and $Z$, respectively. For each independent random experiment generating $(X,Y,Z) \sim p_{XYZ}^1$, Eve can infer Alice and Bob’s values with complete certainty, when she receives either 2 or 3. When she receives either 0 or 1, she can only infer that Alice’s and Bob’s symbols are restricted to the upper left quadrant (i.e., the set $\{0,1\}$), but then in this range, $X$ and $Y$ are uniformly distributed. Clearly, Alice and Bob can share no secret. Now, consider the distributions

Proof. From (7), (9) and Lemma 5, the first equality is obvious. For the second equality, the “only if” part is trivial. For the “if” part, first note that

$$C_W(X;Y \downarrow Z) = \min_{Q_X \sim Q_Z \sim Q_Y} \frac{I(XY;Q|Z)}{Q_{XY} \sim Q_Z \sim Q_Y} = \min_{Q_X \sim Q_Z \sim Q_Y} \frac{I(Y;Q(XZ) + I(X;Q|Z))}{Q_{XY} \sim Q_Z \sim Q_Y}$$

where (a) follows from writing $I(X;Y|Z) = I(X;Y|Z) + I(X;Q|Z)$, and noting that $I(X;Q|Z) = 0$. Then given jointly distributed RVs $(XYZZQ)$ achieving the minimum in (9), if $I(Y;Q|Z) = I(X;Q|Z) = 0$, then by Lemma 1, there exists a pmf $p_{Q|XYZ}$ such that $H(Q|XZ) = H(Q|YZ) = 0$, $XY - Q'Z - Q$ and $I(X;Q|Z) \leq H(Q'|Z)$, with equality iff $H(Q'|Z) = 0$. Finally note that $H(Q'|Z) \leq I(X;Y|Z)$ with equality iff $X - Q'Y - Z$.

$\square$
right). This intuition is borne out by
In the latter case, Alice and Bob can realize one perfect SK bit, since Eve can

\[ p_{XYZ}^2 = \frac{1}{8} \begin{pmatrix} 1(0) 1(1) & 1(1) 1(0) & 2(2) & 2(2) \\ 1(1) 1(0) & 1(1) 1(0) & 2(2) & 2(2) \\ 2(2) & 2(2) & 2(2) & 2(2) \\ 2(2) & 2(2) & 2(2) & 2(2) \end{pmatrix}, \] and \( p_{XYZ}^3 = \frac{1}{8} \begin{pmatrix} 1(0) 1(1) & 1(1) 1(0) & 2(2) & 2(2) \\ 1(1) 1(0) & 1(1) 1(0) & 2(2) & 2(2) \\ 2(2) & 2(2) & 2(2) & 2(2) \\ 2(2) & 2(2) & 2(2) & 2(2) \end{pmatrix}, \) where Eve's
symbol set is successively depleted to \( Z = \{0,1,2\} \) and \( Z = \{0,1\} \), respectively.
In the latter case, Alice and Bob can realize one perfect SK bit, since Eve can
no longer infer anything about their quadrant information (upper left or lower right). This intuition is borne out by \( C_{GR}(X;Y|Z) \), which evaluates to 0, 0.5 and 1, respectively, for \( p^1, p^2 \) and \( p^3 \), \( p^3 \) is resolvable but not conditionally resolvable. A distribution \( p^4 \) that is conditionally resolvable but not resolvable is the following: \( (000) = (100) = (110) = \frac{1}{2}, (001) = (101) = (011) = (111) = \frac{1}{2}, (032) = (042) = \frac{1}{2}, (252) = \frac{1}{2}, (220) = \frac{1}{2}, (221) = \frac{1}{2} \). Finally, \( C_{GR}(X;Y|Z) = 1 \) for the following more general distribution \( p^5 \) that is neither resolvable nor conditionally resolvable: \( (000) = (011) = (020) = (101) = \frac{1}{2}, (110) = (121) = \frac{1}{2}, (230) = (331) = \frac{1}{2} \), where using arguments similar to the ones for \( p^3 \), Alice and Bob can be shown to achieve one perfect SK bit.

**Example 8.** Consider the following sequence of distributions:

\[
(p_{XYZ})_n(x,y,z) = \begin{cases}
\frac{1}{2^n}, & \text{if } x,y \in \{0,\ldots,n-1\}, \ z = x + y \ (\text{mod } n), \\
\frac{1}{2^n}, & \text{if } x \in \{n,\ldots,2n-1\}, y = x, z = x \ (\text{mod } n).
\end{cases}
\]

\[
(q_{XYZ})_n(x,y,z) = \begin{cases}
\frac{1}{\log n}(p_{XYZ})_n, & \text{if } x \neq \Delta, y \neq \Delta, z \neq \Delta, \\
1 - \frac{1}{\log n}, & \text{if } x = y = z = \Delta,
\end{cases}
\]

where \( (p_{XYZ})_n \) is derived from \( (p_{XYZ})_n \) by extending the symbol sets \( (X,Y,Z) \) to include an extra symbol \( \Delta \). Renner and Wolf [3] showed that \( (p_{XYZ})_n \) has asymptotic bound information, i.e., \( (q_{XYZ})_n \) is asymptotically non-distillable \( (S(X(n);Y(n)|Z(n)) = \frac{1}{\log n} \to 0, \text{as } n \to \infty) \), and yet cannot be created by LOPC, since \( SK_*(X(n);Y(n)|Z(n)) \geq I(X(n);Y(n) \downarrow Z(n)) = \frac{1}{\log n}(1 + \frac{1}{2}\log n) > \frac{1}{\log n} \) [3].

Omitting the index \( n \), for a given \( Z \), the pmf of the common core \( p_{Q_i,XY} \) is given by \( p_{Q_i,XY}(0) = \frac{1}{2\log n}, p_{Q_i,XY}(1) = 1 - \frac{1}{\log n}, p_{Q_i,XY}(i) = \frac{1}{2\log n}, i = 2,\ldots,n + 1 \), so that \( C_{GR}(X;Y|Z) = H(Q_i|Z) = \frac{1}{\log n} \), thus achieving the SK rate.

In all the examples considered so far, no assumptions have been made on the nature of the communication protocol (or its lack thereof) between Alice and Bob. For a non-communicative SK agreement model, i.e. a restricted key agreement model where no communication is allowed between Alice and Bob, let \( S_{0-\text{comm}}(X;Y||Z) \) denote the maximum attainable rate at which a SK can be extracted by Alice (knowing \( X^n \)) and Bob (knowing \( Y^n \)) about which Eve (knowing \( Z^n \)) has virtually no information. As usual, \( (X^n,Y^n,Z^n) \) are independent repeated realizations of the random experiment \( p_{XYZ} \). We conjecture that the bound is tight in general for such restricted key agreement models.

**Conjecture 9.** For non-communicative SK agreement models, \( S_{0-\text{comm}}(X;Y||Z) = C_{GR}(X;Y|Z) \). Furthermore, if \( p_{XYZ} \) is conditionally resolvable, then

\[
S_{0-\text{comm}}(X;Y||Z) = C_{GR}(X;Y|Z) = I(X;Y|Z).
\]

The SK rate and the SK cost of formation are intrinsic properties of the underlying joint distribution, and the interconvertibility of noisy correlations and
perfect SK under LOPC is not lossless (even asymptotically) [3]. Given many independent copies of a source distribution \((q_{XYZ})\) and a target distribution of a perfect secret bit \((p_{SS\Delta})\), reversible conversion of \(q_{XYZ}\) and \(p_{SS\Delta}\) is possible iff \(R(q \rightarrow p^\ast)R(p^\ast \rightarrow q) = 1\), i.e., iff \(S(X;Y|Z) = I(X;Y \downarrow Z)\) and \(I(X;Y \downarrow Z) = SK_c(X;Y|Z)\). Theorem 6 gives necessary and sufficient conditions for achieving the second equality. More generally, monotones can be used to derive upper bounds on the asymptotic rate of conversion of \(q_{XYZ}\) to any other distribution \(q_{X'Y'Z'}\) (e.g., one which is relatively less favorable to Eve).

The sequence of distributions \((q_{XYZ})_n\) in Example 8 was originally constructed by Renner and Wolf [3] to show that there exists sequences of distributions with asymptotic bound information, i.e., asymptotically non-distillable correlations with positive SK cost of formation. Unfortunately, this is the best that has been shown so far for the bipartite case. For more than two parties, the possibility of creating different bipartitions across the honest parties immensely simplifies the problem and, indeed, multipartite bound information has been shown to exist [18]. Constructing distributions that can show the existence of bipartite bound information remains an open problem and a scope for future work.

**Acknowledgments**

PKB wishes to thank Amin Gohari for his valuable comments and Paul Cuff for short useful discussions over email. This work is based in part on PKB’s unpublished dissertation [20] and was supported in part by the AVLSI Consortium, IIT Kharagpur.

**References**

1. Maurer, U. M.: Secret key agreement by public discussion from common information. IEEE Transactions on Information Theory, 39(3), 33–742 (1993).
2. Maurer, U. M., Wolf, S.: Unconditionally secure key agreement and the intrinsic conditional information. IEEE Transactions on Information Theory, 45(2), 499–514 (1999).
3. Renner, R., Wolf, S.: New bounds in secret-key agreement: The gap between formation and secrecy extraction. In: Advances in Cryptology—EUROCRYPT 2003, pp. 562–577, Springer (2003).
4. Winter, A.: Secret, public and quantum correlation cost of triples of random variables. in: Proceedings of the IEEE International Symposium on Information Theory (ISIT 2005), pp. 2270–2274 (2005).
5. Chitambar, E., Hsieh, M. H., Winter, A.: The Private and Public Correlation Cost of Three Random Variables with Collaboration. arXiv preprint arXiv:1411.0729 (2014).
6. Horodecki, K., Horodecki, M., Horodecki, P., Oppenheim, J.: Information theories with adversaries, intrinsic information, and entanglement. Foundations of Physics, 35(12), 2027–2040 (2005).
7. Gács, P., Körner, J.: Common information is far less than mutual information. Problems of Control and Information Theory, 2(2), 149–162 (1973).
8. Wyner, A. D.: The common information of two dependent random variables. IEEE Transactions on Information Theory, 21(2), 163–179 (1975).
9. Cuff, P.: Distributed channel synthesis. IEEE Transactions on Information Theory, 59(11), 7071–7096 (2013).
10. Bennett, C. H., Devetak, I., Harrow, A. W., Shor, P. W., Winter, A.: The quantum reverse Shannon theorem and resource tradeoffs for simulating quantum channels. IEEE Transactions on Information Theory, 60(5), 2926–2959 (2014).
11. Csiszár, I., Körner, J.: Information theory: coding theorems for discrete memoryless systems. Cambridge University Press (2011).
12. Ahlswede, R., Körner, J.: On common information and related characteristics of correlated information sources. Preprint. Presented at the 7th Prague Conference on Information Theory (1974).
13. Christandl, M., Renner, R., Wolf, S.: A property of the intrinsic mutual information. In: Proceedings of the IEEE International Symposium on Information theory (ISIT 2003), pp. 258–258 (2003).
14. Maurer, U., Renner, R., Wolf, S.: Unbreakable keys from random noise. In: Security with Noisy Data, pp. 21–44, Springer (2007).
15. Christandl, M., Ekert, A., Horodecki, M., Horodecki, P., Oppenheim, J., Renner, R.: Unifying classical and quantum key distillation. In: Theory of Cryptography, pp. 456–478, Springer (2007).
16. Gohari, A. A., Anantharam, V.: Information-theoretic key agreement of multiple terminals—Part I. IEEE Transactions on Information Theory, 56(8), 3973–3996 (2010).
17. Cerf, N. J., Massar, S., Schneider, S.: Multipartite classical and quantum secrecy monotones. Physical Review A, 66(4), 042309 (2002).
18. Masanes, L., Acín, A.: Multipartite Secret Correlations and Bound Information. IEEE Transactions on Information Theory, 52(10), 4686–4694 (2006).
19. Ahlswede, R., Csiszár, I.: Common randomness in information theory and cryptography. Part I: secret sharing. IEEE Transactions on Information Theory, 39(4), 1121–1132 (1993).
20. Banerjee, P. K.: Synergy, redundancy, and secret common randomness: Some intriguing links. M.S. thesis, Dept. E & ECE, IIT Kharagpur, India (2014).