A Secret Common Information Duality for Tripartite Noisy Correlations

Pradeep Kr. Banerjee[(✉)]

Indian Institute of Technology Kharagpur, Kharagpur, India
`pradeep.banerjee@gmail.com`

Abstract. We explore the duality between the simulation and extraction of secret correlations in light of a similar well-known operational duality between the two notions of common information due to Wyner, and Gács and Körner. For the *inverse* problem of simulating a tripartite noisy correlation from 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 bipartite protocol monotone. For the *forward* problem of key distillation from noisy correlations, we construct simple distributions for which the conditional Gács and Körner common information achieves a tight bound on the secret key rate. We conjecture that this holds in general for non-communicative key agreement models. 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

Information-theoretic (IT) or unconditional security—widely acknowledged as the strictest notion of security has witnessed a renaissance since the 90's, arguably following Maurer's seminal work on secret key (SK) agreement by public discussion from correlated source sequences [1,2]. Compared to computational complexity-based approaches, IT-security provides a framework for *provable security* by bounding the adversary's total information. Assumptions are made neither on the latter's computational or memory resources nor on the unproven computational hardness of certain problems. By harnessing noise and appropriate coding and signaling strategies at the *physical layer* (the lowest layer in the protocol stack), IT-security potentially complements conventional upper layer cryptographic protocols (e.g., RSA, Diffie-Hellman key exchange) and is an important component of future communication networks [18]. The paradigm is especially valuable for improving security in large-scale wireless networks and distributed networks with minimal infrastructure (e.g., mobile *ad hoc* sensor

networks) where the broadcast nature of the transmission medium makes it particularly vulnerable to attacks, and key distribution and management is difficult and computationally expensive [18].

But for all its advantages, 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 are not completely under the control of an adversary [14]. Thus, information-theoretic reductions between such primitives are of great interest.

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* [1,2]) and the dual problem of simulating a noisy correlation from noiseless SK and public communication (called the *inverse problem* [3–6]). 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) [3,16]. 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 $X^n = (X_1, \ldots, X_n)$, $Y^n = (Y_1, \ldots, Y_n)$, and $Z^n = (Z_1, \ldots, Z_n)$ respectively, where the sequence triple $(X^n Y^n Z^n)$ has the generic component variables $(XYZ) \sim p_{XYZ}$. Starting with no initially shared SKs, and using only local operations and unlimited public communication (LOPC) over a noiseless, authenticated (but, otherwise insecure) 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 and the entire public discussion) about the generated SK is arbitrarily small? Conversely, starting with perfect SKs, what is the *SK cost* of approximately simulating the correlated triple XYZ using only LOPC?

We explore this duality between the secrecy extractable from p_{XYZ} and that required to simulate p_{XYZ} in light of a similar well-known operational duality between the two notions of common information (CI) due to Gács and Körner [7] and Wyner [8]. 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 the SK cost of formation can be simply reexpressed in terms of the existence of a bipartite protocol monotone. For the *forward* problem of key distillation from p_{XYZ}, 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 interconvertibility 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 $(X_1, \ldots, X_n)$.

$p_X(x) = \Pr\{X = x\}$ denotes the distribution (pmf) of a discrete RV X. $X - Y - Z$ denotes that X, Y, Z form a Markov chain satisfying $p_{XYZ} = p_{XY}p_{Z|Y}$. Likewise, X, Y, Z is said to form a conditional Markov chain given U if $X - UY - Z$. 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 $\mathsf{TV}(p_X, p_{X'}) = \frac{1}{2} \sum_{x \in \mathcal{X}} |p_X(x) - p_{X'}(x)|$.

The zero pattern of p_{XY} can be specified by its characteristic bipartite graph B_{XY} with the vertex set $\mathcal{X} \cup \mathcal{Y}$ 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 $\mathcal{X} \times \mathcal{Y}$ 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*

$$X - Y - Q, \ Y - X - Q \tag{1}$$

iff there exists a pmf $p_{Q'|XY}$ such that $H(Q'|X) = H(Q'|Y) = 0$ and $XY - Q' - Q$. Furthermore, (1) implies $I(XY; Q) \leq H(Q')$ 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 $\mathcal{X} \times \mathcal{Y} = \bigcup_{q'} \mathcal{X}_{q'} \times \mathcal{Y}_{q'}$, where the $\mathcal{X}_{q'}$'s and $\mathcal{Y}_{q'}$'s having different subscripts are disjoint, define $p_{Q'|XY}$ as $Q' = q'$ iff $x \in \mathcal{X}_{q'} \Leftrightarrow y \in \mathcal{Y}_{q'}$. Clearly $H(Q'|X) = H(Q'|Y) = 0$. Then, for any $Q = q$ and for every q', $p_{Q|XY}(q|\cdot, \cdot)$ is constant over $\mathcal{X}_{q'} \times \mathcal{Y}_{q'}$. 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 $I(XY; Q|Q') = 0$ so that $I(XY; Q) = I(XYQ'; Q) = I(Q'; Q) = H(Q') - H(Q'|Q) \leq H(Q')$. $\square$

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

$$C_{GK}(X; Y) = \max_{Q: \ H(Q|X) = H(Q|Y) = 0} H(Q) = H(Q_*) \tag{2}$$

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].

$$C_{GK}(X; Y) = \max_{Q: \ Q - X - Y, \ Q - Y - X} I(XY; Q), \ |\mathcal{Q}| \leq |\mathcal{X}||\mathcal{Y}| + 2 \tag{3}$$

$C_{GK}(X;Y)$ 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.

$$C_{GK}(X;Y|Z) = H(Q_*|Z) = \max_{\substack{Q:H(Q|XZ)=0 \\ H(Q|YZ)=0}} H(Q|Z) = \max_{\substack{Q-XZ-Y \\ Q-YZ-X}} I(XY;Q|Z) \quad (4)$$

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: $Q \to X^n$, $Q \to Y^n$) and no communication ($R_0 = 0$) (see setup in Fig. 1(b)).

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

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

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

$C_W(X;Y)$ 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 ($X^n \to Q^n$) (see Fig. 1(c)) leads to a 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 [1–3,14,15] 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, Π_{KA}. Alice (X) and Bob (Y) communicate interactively over an authenticated (noiseless) public discussion channel (transparent to an adversary, Eve (Z)). Both have independent access to an infinite stream of private randomness. 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
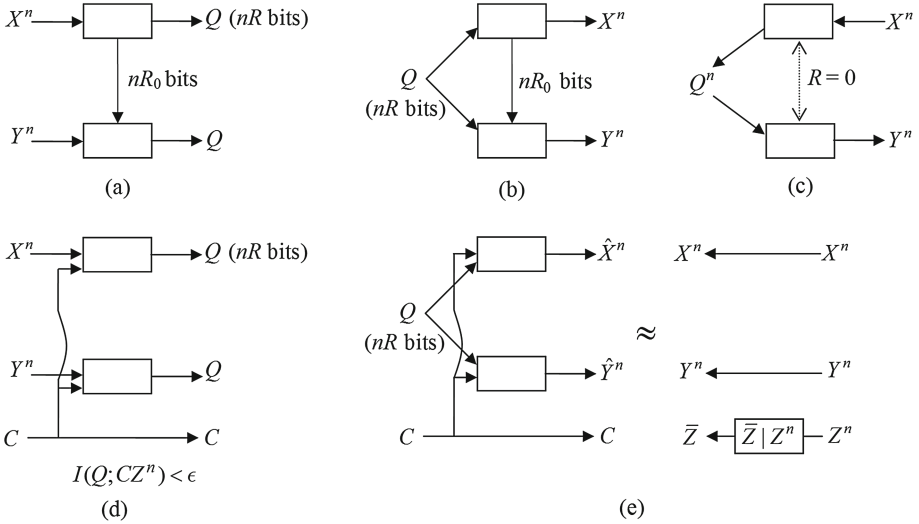
Fig. 1. *Common information duality (with communication)*: (a) Gács and Körner's setup ($R_0 = 0$) [7] (b) Wyner's setup ($R_0 = 0$) [8] (c) Inverting Alice's channel gives an alternative characterization of Wyner's CI as the communication cost of channel simulation without any CR ($R = 0$) [9,10] (d) Setup for SK agreement [1–3] (e) Setup for distributed simulation of p_{XYZ} from SK and public communication [3–6]

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* [1–3].

Definition 1. *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 Π_{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 $\Pr\{Q_X = Q_Y = Q\} \geq 1 - \epsilon$, $H(Q) = \log |\mathcal{Q}| \geq n(R - \epsilon)$, $I(Q;CZ^n) < \epsilon$.*

Analogously, there exists an inverse protocol Π_{form}, and a dual measure, the asymptotic minimal *SK cost of formation* of the triple $(X, Y, Z) \sim p_{XYZ}$ [3–6]. While the distributed channel synthesis problem [9] (setup in Fig. 1(b)) 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), upto a local degrading of Z^n. Both parties have independent access to sources of private randomness. The protocol proceeds in rounds

and at the end of the communication phase, Alice and Bob output $\hat{X}^n$ and $\hat{Y}^n$, respectively, 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, Π_{form} can be specified by the joint distribution $p_{\hat{X}^n\hat{Y}^nCQ}$ $= p_{\hat{X}^n|CQ,\hat{Y}^n|CQ}p_{CQ}$. 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, Eve (Z^n) might still have some information about X^nY^n. This is formalized by requiring that Eve's optimal channel $p_{\bar{Z}|Z^n}$ 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 2. *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 Π_{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 $\Pr\{(\hat{X}^n, \hat{Y}^n, C) = (X^n, Y^n, \bar{Z})\} \geq 1 - \epsilon$ holds for some correlated sequence triple (X^n, Y^n, Z^n) that has generic component variables $(X, Y, Z) \sim p_{XYZ}$ and some channel $p_{\bar{Z}|Z^n}$.*

p_{XYZ} contains secret correlations iff it cannot be generated by LOPC, i.e., $SK_c(X;Y|Z) > 0$ [17]. Both the SK cost of formation and the SK rate are measures of the secrecy content of p_{XYZ} and admit a clear operational interpretation: $SK_c(X;Y|Z)$ quantifies the *minimum* amount of SK bits required to (approximately) *simulate* p_{XYZ}, whereas $S(X;Y||Z)$ quantifies the *maximum* amount of SK bits that one can *extract* from p_{XYZ}.

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

$$SK_c(X;Y|Z) = \min_{\substack{Q:X-Q\bar{Z}-Y \\ \bar{Z}:XY-Z-\bar{Z}}} I(XY;Q|\bar{Z}) \tag{7}$$

where the minimum is taken over all RVs Q and $\bar{Z}$. Cardinalities of the corresponding alphabets are bounded as $|\mathcal{Q}| \leq |\mathcal{X}||\mathcal{Y}|$, and $|\bar{\mathcal{Z}}| \leq |\mathcal{Z}|$ 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].

$$I(X;Y \downarrow Z) = \min_{\bar{Z}:XY-Z-\bar{Z}} I(X;Y|\bar{Z}) \tag{8}$$

where the cardinality of the alphabet $\bar{\mathcal{Z}}$ of RV $\bar{Z}$ is bounded as $|\bar{\mathcal{Z}}| \leq |\mathcal{Z}|$ [13]. Both $I(X;Y \downarrow Z)$ and $SK_c(X;Y|Z)$ are known to be *lockable* [3,4], i.e., can fall sharply by an arbitrary large amount on giving away a single bit to Eve.

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 $p_{XY|\bar{Z}}$ is $C_W(X;Y|\bar{Z})$. In this section, we introduce the concept of protocol monotones [6,14–16] 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 [16] as classical counterparts of entanglement or LOCC (local operations and classical communication) monotones to study the 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 [6,16]. We define a monotone as follows.

Definition 3. *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 $\bar{X}$ by sending X over a channel, characterized by $p_{\bar{X}|X}$. Then $\mathcal{M}$ can only decrease, i.e., for all jointly distributed RVs $(X, Y, Z, \bar{X})$ with $\bar{X} : YZ - X - \bar{X}$, $\mathcal{M}(\bar{X};Y|Z) \leq \mathcal{M}(X;Y|Z)$, and likewise for Bob.*

(2) Monotonicity under public communication (PC) by Alice and Bob: *Suppose Alice publicly announces the value of $\widetilde{X}$. Then $\mathcal{M}$ can only decrease, i.e., for all jointly distributed RVs $(X, Y, Z, \widetilde{X})$ with $H(\widetilde{X}|X) = 0$, $\mathcal{M}(X;Y\widetilde{X}|Z\widetilde{X}) \leq \mathcal{M}(X;Y|Z)$, and likewise for Bob.*

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

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

(5) Additivity and Continuity: $\mathcal{M}$ *is additive on tensor products and is a semi-positive, continuous function of* p_{XYZ}. *A stronger notion of asymptotic continuity requires that for two pmfs* p_{XYZ}, q_{XYZ}, *if* $\mathsf{TV}(p_{XYZ}, q_{XYZ}) = \epsilon$, *then* $|\mathcal{M}(p_{XYZ}) - \mathcal{M}(q_{XYZ})| \leq \epsilon \log d + \delta(\epsilon)$, *where* d *is some constant that depends on* $|\mathcal{X}|$, $|\mathcal{Y}|$ *and* $|\mathcal{Z}|$ *and* $\delta(\epsilon)$ *is any function that depends only on* ϵ *with* $\delta(0) = 0$.

If $\mathcal{M}$ satisfies the conditions in Definition 3, then $\mathcal{M}$ is an upper bound on the SK rate [14]. 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. Given the class of LOPC operations, suppose that the parties are able to convert n copies of p_{XYZ} into some realization of a distribution q'_{XYZ} which is close to m independent realizations of the target distribution q_{XYZ}, i.e., $p^{\otimes n} \overset{LOPC}{\to} q' \simeq q^{\otimes m}$. Then by virtue of Property (5) in Definition 3, we have, $\mathcal{M}(p^{\otimes n}) = n\mathcal{M}(p) \geq \mathcal{M}(q') \simeq m\mathcal{M}(q)$, so that the optimal rate $R(p \to q)$ at which transformations $p^{\otimes n} \overset{LOPC}{\to} q^{\otimes m}$ are possible is upper bounded as $\frac{m}{n} \leq \frac{\mathcal{M}(p)}{\mathcal{M}(q)}$ [16]. Thus if $p^s_{SS\Delta}$ denotes the distribution of a perfect secret bit with $p^s_{SS\Delta}(0,0,\delta) = p^s_{SS\Delta}(1,1,\delta) = \frac{1}{2}$, then for any pmf q_{XYZ}, $S(X;Y||Z) = R(q \to p^s) \leq \frac{I(X;Y\downarrow Z)}{I(S;S\downarrow\Delta)} = I(X;Y\downarrow Z)$, since $I(S;S\downarrow\Delta) = 1$, and $I(X;Y\downarrow Z)$ is a monotone [3]. Likewise $R(p^s \to q) \leq \frac{I(S;S\downarrow\Delta)}{I(X;Y\downarrow Z)} = \frac{1}{I(X;Y\downarrow Z)}$. Hence $SK_c(X;Y|Z) = \frac{1}{R(p^s \to q)} \geq I(X;Y\downarrow Z)$ [3].

$C_W(X;Y|Z)$ violates monotonicity under LO by Eve[1] 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 $p_{\bar{Z}|Z}$ that can be chosen by Eve for locally processing her observations. This implies a minimization over all Markov chains $XY - Z - \bar{Z}$ which is tantamount to the simulation approximation of $(X^n Y^n Z^n)$ upto a local degrading in Z^n in Definition 2 of the SK cost of formation. This yields a new quantity called *Wyner's intrinsic conditional CI* that satisfies monotonicity under Eve's LOPC operations.

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

The cardinality of the alphabet $\bar{\mathcal{Z}}$ of $\bar{Z}$ is bounded as $|\bar{\mathcal{Z}}| \leq |\mathcal{Z}|$. This can be shown following similar arguments as in [13] using Carathéodory's theorem. From (6), we have $|\mathcal{Q}| \leq |\mathcal{X}||\mathcal{Y}|$. 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 2. $C_W(X;Y\downarrow Z)$ *is a monotone.*

Proof. Let $p_{\bar{Z}|Z}$ be the minimizer in $C_W(X;Y\downarrow Z)$. Then it suffices to show that $C_W(X;Y|\bar{Z})$ satisfies monotonicity under Alice and Bob's LOPC operations.

---

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

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 $(XY\bar{Z}Q\bar{X})$ such that $Y\bar{Z} - X - \bar{X}$ and $\bar{X} - Q\bar{Z} - Y$, monotonicity under LO by Alice holds since,

$$I(\bar{X}Y; Q|\bar{Z}) = H(Q|\bar{Z}) - H(Q|\bar{X}Y\bar{Z}) \overset{(a)}{\leq} H(Q|\bar{Z}) - H(Q|XY\bar{Z}) = I(XY; Q|\bar{Z}),$$

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

$$I(XY\widetilde{X}; Q\widetilde{X}|\bar{Z}\widetilde{X}) = I(XY; Q|\bar{Z}\widetilde{X}) \overset{(b)}{\leq} I(XY; Q|\bar{Z}),$$

and likewise for Bob.

Additivity and continuity are valuable properties if the monotone is to provide information on the rate of transformations $p^{\otimes n} \overset{LOPC}{\to} q^{\otimes m}$ in the asymptotic limit $n, m \to \infty$. It is easy to show that for independent triples $(X_1 Y_1 \bar{Z}_1)$ and $(X_2 Y_2 \bar{Z}_2)$, $C_W(X_1 X_2; Y_1 Y_2 | \bar{Z}_1 \bar{Z}_2) = C_W(X_1; Y_1 | \bar{Z}_1) + C_W(X_2; Y_2 | \bar{Z}_2)$. We do not target the stronger notion of asymptotic continuity since it is already known that the SK cost fails this property and admits locking [4]. □

Theorem 3 gives the main result of this section.

Theorem 3. *With unlimited public communication, $SK_c(X;Y|Z) = C_W(X;Y \downarrow Z)$. Furthermore, if $p_{\bar{Z}|Z}$ 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 $p_{Q'|XYZ\bar{Z}}$ s.t. $H(Q'|X\bar{Z}) = H(Q'|Y\bar{Z}) = 0$ and $X - \bar{Z}Q' - Y$.*

Proof. From (7), (9) and Lemma 2, the first equality is obvious. For the second equality, the "only if" part is trivial. For the "if" part, first note that

$$C_W(X;Y \downarrow Z) = \min_{\substack{Q:X-Q\bar{Z}-Y \\ \bar{Z}:XY-Z-\bar{Z}}} I(XY; Q|\bar{Z}) = \min_{\substack{Q:X-Q\bar{Z}-Y \\ \bar{Z}:XY-Z-\bar{Z}}} (I(Y; Q|X\bar{Z}) + I(X; Q|\bar{Z}))$$

$$\overset{(a)}{=} \min_{\substack{Q:X-Q\bar{Z}-Y \\ \bar{Z}:XY-Z-\bar{Z}}} (I(X;Y|\bar{Z}) + I(Y; Q|X\bar{Z}) + I(X; Q|Y\bar{Z})),$$

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

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 [1–3,15]. 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 zero error 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 $C_{GK}(X;Y|Z)$ quantifies the achievable SK rate for non-communicative key agreement models. We also comment on the lossless interconvertibility of secret correlations.

Example 1. Consider the distribution p^1_{XYZ} with $\mathcal{X} = \mathcal{Y} = \mathcal{Z} = \{0,1,2,3\}$. We write $p^1_{XYZ}(a,b,c) = (abc)$. Given $(000) = (011) = (101) = (110) = \frac{1}{8}$, and $(222) = (333) = \frac{1}{4}$. Graphically, p^1_{XYZ} is shown in the following table (with Z's value given in parentheses): $p^1_{XYZ} = \frac{1}{8}\begin{pmatrix} 1(0) & 1(1) & . & . \\ 1(1) & 1(0) & . & . \\ . & . & 2(2) & . \\ . & . & . & 2(3) \end{pmatrix}$. 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 $(X,Y,Z) \sim p^1_{XYZ}$, 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 $p^2_{XYZ} = \frac{1}{8}\begin{pmatrix} 1(0) & 1(1) & . & . \\ 1(1) & 1(0) & . & . \\ . & . & 2(2) & . \\ . & . & . & 2(2) \end{pmatrix}$, and $p^3_{XYZ} = \frac{1}{8}\begin{pmatrix} 1(0) & 1(1) & . & . \\ 1(1) & 1(0) & . & . \\ . & . & 2(0) & . \\ . & . & . & 2(1) \end{pmatrix}$, where Eve's symbol set is successively depleted to $\mathcal{Z} = \{0,1,2\}$ and $\mathcal{Z} = \{0,1\}$, 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 $C_{GK}(X;Y|Z)$, 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: $(000) = (100) = (010) = (110) = \frac{1}{18}$, $(001) = (101) = (011) = (111) = \frac{1}{21}$, $(032) = (042) = \frac{1}{15}$, $(252) = \frac{1}{5}$, $(220) = \frac{1}{9}$, $(221) = \frac{1}{7}$. Finally, $C_{GK}(X;Y|Z) = 1$ for the following more general distribution p^5 that is neither *resolvable* nor *conditionally resolvable*: $(000) = (011) = (020) = (101) = \frac{1}{10}$, $(110) = (121) = \frac{1}{20}$, $(230) = (331) = \frac{1}{4}$, where using arguments similar to the ones for p^3, Alice and Bob can be shown to achieve one perfect SK bit.

Example 2. Consider the following sequence of distributions:

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

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

where $(q_{XYZ})_n$ is derived from $(p_{XYZ})_n$ by extending the symbol sets $(\mathcal{X}, \mathcal{Y}, \mathcal{Z})$ to include an extra symbol Δ. Renner and Wolf [3] showed that $(q_{XYZ})_n$ has *asymptotic bound information*, i.e., $(q_{XYZ})_n$ is asymptotically non-distillable $(S(X_{(n)}; Y_{(n)} || Z_{(n)}) = \frac{1}{\log n} \to 0$, as $n \to \infty)$, and yet cannot be created by LOPC, since $SK_c(X_{(n)}; Y_{(n)} | Z_{(n)}) \geq I(X_{(n)}; Y_{(n)} \downarrow Z_{(n)}) = \frac{1}{\log n}(1 + \frac{1}{2}\log n) > \frac{1}{2}$ [3]. Omitting the index n, for a given Z, the maximal common RV of the pair (X, Y) has the pmf $p_{Q_*}(0) = \frac{1}{2\log n}$, $p_{Q_*}(1) = 1 - \frac{1}{\log n}$, $p_{Q_*}(i) = \frac{1}{2n\log n}$, $i = 2, \dots, n+1$, so that $C_{GK}(X; Y | Z) = H(Q_* | Z) = \frac{1}{\log n}$, thus achieving the SK rate.

In both the examples above, 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 $S_{0-comm}(X; Y || Z)$ 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}.

Conjecture 4. *For non-communicative SK agreement models, $S_{0-comm}(X; Y || Z) = C_{GK}(X; Y | Z)$. Furthermore, if p_{XYZ} is conditionally resolvable, then*

$$S_{0-comm}(X; Y || Z) = C_{GK}(X; Y | Z) = I(X; Y | Z).$$

4 Concluding Remarks

In summary, we have presented two results. The first result demonstrates the power of the framework of resource monotones for axiomatizing the general properties of upper bounds on the SK rate. We showed that $C_W(X; Y | Z)$ violates monotonicity under LO by Eve, which can be used to bootstrap the definition of the SK cost of simulating the triple (XYZ) up to a local degrading of Z. In the past, a similar approach has been put to direct practical use for deriving strong bounds on the SK rate [15]. Given many independent copies of a source distribution (q_{XYZ}) and a target distribution of a perfect secret bit $(p^s_{SS\Delta})$, *reversible* conversion of q_{XYZ} and $p^s_{SS\Delta}$ is possible iff $R(q \to p^s)R(p^s \to q) = 1$, i.e., iff $S(X; Y || Z) = I(X; Y \downarrow Z)$ and $I(X; Y \downarrow Z) = SK_c(X; Y | Z)$. In Theorem 3, we have given 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). Thus, resource theories hold promise in capturing a general calculi of secret correlations.

In the second part, we constructed simple distributions for which the conditional Gács and Körner CI achieves a tight bound on the SK rate. The sequence of distributions $(q_{XYZ})_n$ in Example 2 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. 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 [17]. Constructing distributions that can show the existence of bipartite bound information remains an open problem and a scope for future work. Another problem of independent interest is to consider single shot versions of the SK cost of formation and intrinsic information.

References

1. Maurer, U.M.: Secret key agreement by public discussion from common information. IEEE Trans. Inf. Theor. **39**(3), 33–742 (1993)
2. Maurer, U.M., Wolf, S.: Unconditionally secure key agreement and the intrinsic conditional information. IEEE Trans. Inf. Theor. **45**(2), 499–514 (1999)
3. Renner, R., Wolf, S.: New bounds in secret-key agreement: the gap between formation and secrecy extraction. In: Biham, E. (ed.) Advances in Cryptology-EUROCRYPT 2003. LNCS, vol. 2656, pp. 562–577. Springer, Heidelberg (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 (2014). arXiv preprint arXiv:1411.0729
6. Horodecki, K., Horodecki, M., Horodecki, P., Oppenheim, J.: Information theories with adversaries, intrinsic information, and entanglement. Found. Phys. **35**(12), 2027–2040 (2005)
7. Gács, P., Körner, J.: Common information is far less than mutual information. Prob. Control Inf. Theor. **2**(2), 149–162 (1973)
8. Wyner, A.D.: The common information of two dependent random variables. IEEE Trans. Inf. Theor. **21**(2), 163–179 (1975)
9. Cuff, P.: Distributed channel synthesis. IEEE Trans. Inf. Theor. **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 Trans. Inf. Theor. **60**(5), 2926–2959 (2014)

11. Csiszár, I., Körner, J.: Information theory: coding theorems for discrete memoryless systems. Cambridge University Press, Cambridge (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. Christandl, M., Ekert, A., Horodecki, M., Horodecki, P., Oppenheim, J., Renner, R.S.: Unifying classical and quantum key distillation. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 456–478. Springer, Heidelberg (2007)
15. Gohari, A.A., Anantharam, V.: Information-theoretic key agreement of multiple terminals-Part I. IEEE Trans. Inf. Theor. **56**(8), 3973–3996 (2010)
16. Cerf, N.J., Massar, S., Schneider, S.: Multipartite classical and quantum secrecy monotones. Phys. Rev. A **66**(4), 042309 (2002)
17. Masanes, L., Acin, A.: Multipartite secret correlations and bound information. IEEE Trans. Inf. Theor. **52**(10), 4686–4694 (2006)
18. Liu, R., Trappe, W. (eds.): Securing Wireless Communications at the Physical Layer. Springer, New York (2010)
19. Banerjee, P.K.: Synergy, redundancy, and secret common randomness: Some intriguing links. M.S. thesis, Dept. E & ECE, IIT Kharagpur, India (2014)