Distributions Attaining Secret Key at a Rate of the Conditional Mutual Information

Eric Chitambar[1(✉)], Benjamin Fortescue[1], and Min-Hsiu Hsieh[2]

[1] Department of Physics and Astronomy, Southern Illinois University,
Carbondale, IL 62901, USA
echitamb@siu.edu

[2] Faculty of Engineering and Information Technology (FEIT), Centre
for Quantum Computation & Intelligent Systems (QCIS),
University of Technology Sydney (UTS), Sydney, NSW 2007, Australia

Abstract. In this paper we consider the problem of extracting secret key from an eavesdropped source p_{XYZ} at a rate given by the conditional mutual information. We investigate this question under three different scenarios: (i) Alice (X) and Bob (Y) are unable to communicate but share common randomness with the eavesdropper Eve (Z), (ii) Alice and Bob are allowed one-way public communication, and (iii) Alice and Bob are allowed two-way public communication. Distributions having a key rate of the conditional mutual information are precisely those in which a "helping" Eve offers Alice and Bob no greater advantage for obtaining secret key than a fully adversarial one. For each of the above scenarios, strong necessary conditions are derived on the structure of distributions attaining a secret key rate of $I(X:Y|Z)$. In obtaining our results, we completely solve the problem of secret key distillation under scenario (i) and identify $H(S|Z)$ to be the optimal key rate using shared randomness, where S is the Gács-Körner Common Information. We thus provide an operational interpretation of the conditional Gács-Körner Common Information. Additionally, we introduce simple example distributions in which the rate $I(X:Y|Z)$ is achievable if and only if two-way communication is allowed.

Keywords: Information-theoretic security · Public key agreement · Gács-Körner Common Information

1 Introduction

A basic information-processing task involves the exchange of secret information between Alice (X) and Bob (Y) in the presence of an eavesdropper, Eve (E). If Alice and Bob have some pre-established key that is secret from Eve, then any future message M can be transmitted using the key as a one-time pad. Thus, the problem of private communication can be reduced to the problem of *secret key distillation*, which studies the extraction of secret key $\Phi_{XY} \cdot q_Z$ from some initial tripartite correlation p_{XYZ}. Here, Φ_{XY} is a perfectly correlated bit and q_Z is an arbitrary distribution. Often, the correlations p_{XYZ} are presented as a

R. Gennaro and M. Robshaw (Eds.): CRYPTO 2015, Part II, LNCS 9216, pp. 443–462, 2015.
DOI: 10.1007/978-3-662-48000-7_22

many-copy source p^n_{XYZ}, and Alice and Bob wish to know the optimal rate of secret bits per copy that they can distill from this source.

It turns out that Alice and Bob can often enhance their distillation capabilities by openly disclosing some information about X and Y through public communication [1,8]. In general, Alice and Bob's communication schemes can be interactive with one round of communication depending on what particular messages were broadcasted in previous rounds. Such interactive protocols are known to generate higher key rates than non-interactive protocols, at least in the absence of "noisy" local processing by Alice and Bob [8]. Thus, for a given distribution p_{XYZ}, one obtains a hierarchy of key rates pertaining to the respective scenarios of no communication, one-way communication, and two-way (interactive) communication. It is also possible to consider no-communication scenarios in which Alice and Bob have access to some publically shared randomness that is uncorrelated with their primary source p_{XYZ}. Clearly publically shared randomness is a weaker resource than public communication since the latter is able to generate the former. However, below we will prove even stronger that publically shared randomness offers no advantage whatsoever for secret key distillation.

For the one-way communication scenario, a single-letter characterization of the key rate has been proven by Ahlswede and Csiszár [1]. When the unidirectional communication is from Alice to Bob, we denote the key rate by $\overrightarrow{K}(X:Y|Z)$, while $\overleftarrow{K}(X:Y|Z)$ denotes the rate when communication is from Bob to Alice only. No formula is known for the two-way key rate of a given distribution, which we denote by $K(X:Y|Z)$, and the complexity of protocols utilizing interactive communication makes computing this a highly challenging open problem.

In the special case of an uncorrelated Eve in p_{XYZ}, the key rate is given by the mutual information $I(X:Y)$, and this can be achieved using one-way communication. For more general distributions in which Eve possesses some side information of XY, the conditional mutual information $I(X:Y|Z)$ is a known upper bound for the key rate under two-way communication [1,8]. In general this bound is not tight [9]. Rather, the conditional mutual information quantifies the key rate when Eve helps Alice and Bob by broadcasting her variable Z. Key obtained by a helping Eve is also known as *private key* [4], and private key is still secret from Eve even though she helps Alice and Bob obtain it. The relevance of private key naturally arises in situations where Eve functions as a central server who helps establish secret correlations between Alice and Bob. Thus, distributions with a secret key rate equaling the private key rate of $I(X:Y|Z)$ are precisely those in which nothing is gained by a helping Eve.

The objective of this paper is to investigate the types of distributions for which $I(X:Y|Z)$ is indeed an achievable secret key rate. This will be considered under the scenarios of (i) publically shared randomness but no communication, (ii) one-way communication, and (iii) two-way communication. A full solution to the problem would involve a structural characterization of the distributions p_{XYZ} whose key rates are $I(X:Y|Z)$. We are able to fully achieve this only for the no-communication setting, but we nevertheless derive strong necessary conditions for both the one-way and the two-way scenarios. In the case of one-way communication, our condition makes use of the key-rate formula derived by Ahlswede and Csiszár. For the statement of this formula, recall that three variables A, B, and C satisfy the Markov chain $A - B - C$ if C is conditionally independent of A given B; i.e. $p(c|b,a) = p(c|b)$ for letters in the range of A, B, and C. Then,

Lemma 1 ([1]). *For distribution* p_{XYZ}*,*

$$\overrightarrow{K}(X:Y|Z) = \max_{KU|X} I(K:Y|U) - I(K:Z|U), \tag{1}$$

where the maximization is taken over all auxiliary variables K *and* U *satisfying the Markov chain* $KU - X - YZ$*, with* K *and* U *ranging over sets of size no greater than* $|\mathcal{X}|+1$*. In particular,*

$$\overrightarrow{K}(X:Y|Z) \geqslant I(X:Y) - I(X:Z). \tag{2}$$

In this paper, we consider when variables KU can be found that satisfy both $KU - X - YZ$ and $I(K;Y|U) - I(K;Z|U) = I(X:Y|Z)$. Theorem 2 below offers a necessary condition on the structure of distributions for which this is possible. Turning to the scenario of two-way communication, we utilize the well-known intrinsic information upper bound on $K(X:Y|Z)$. For distribution p_{XYZ}, its intrinsic information is given by

$$I(X:Y\downarrow Z) := \min_{\overline{Z}|Z} I(X:Y|\overline{Z}) \tag{3}$$

where the minimization is taken over over all auxiliary variables $\overline{Z}$ satisfying $XY - Z - \overline{Z}$, with $\overline{Z}$ having the same range as Z [3]. Thus, the intrinsic information is the smallest conditional mutual information achievable after Eve processes her variable Z. The intrinsic information satisfies $K(X:Y|Z) \leqslant I(X:Y\downarrow Z)$. In Theorem 3 below, we identify a large class of distributions for which a channel $\overline{Z}|Z$ can be found satisfying $I(X:Y|\overline{Z}) < I(X:Y|Z)$. This allows us to derive a necessary condition on distributions having $K(X:Y|Z) = I(X:Y|Z)$.

A brief summary of our results is the following:

- For publically shared randomness with no communication, we identify $H(J_{XY}|Z)$ as the secret key rate, where J_{XY} is the Gács-Körner Common Information of Alice and Bob's marginal distribution p_{XY}. Moreover, this rate is achievable without using shared randomness. Using this result, the structure of distributions attaining $I(X:Y|Z)$ can easily be characterized.
- When one-way communication is permitted between Alice and Bob, we show that the distribution p_{XYZ} must satisfy a certain "block-like" structure in order to obtain the key rate $I(X:Y|Z)$. Specifically, given some outcome z of Eve, if there exists collections of events $\mathcal{X}_0$ and $\mathcal{Y}_0$ for Alice and Bob respectively that satisfy $p(\mathcal{Y}_0|\mathcal{X}_0,z) = p(\mathcal{X}_0|\mathcal{Y}_0,z) = 1$, then $p(\mathcal{Y}_0|\mathcal{X}_0) = p(\mathcal{X}_0|\mathcal{Y}_0) = 1$; i.e. conclusive determination of whether an event belongs to $\mathcal{X}_0 \times \mathcal{Y}_0$ can be done by each party, regardless of Eve's outcome.

- For key distillation with two-way communication, we show that distributions attaining a key rate of $I(X : Y|Z)$ must also satisfy a certain type of uniformity similar to the one-way case. One special class of distributions our necessary condition applies to are those obtained by mixing a perfectly correlated distribution p_{XY} with an uncorrelated one such that the marginals have the same range and such that Eve's variable Z specifies which one of the distributions Alice and Bob hold. We show that unless either Alice or Bob can likewise identify the distribution from his or her variable, a key rate of $I(X : Y|Z)$ is unattainable.
- We construct distributions in which a distillation rate of $I(X : Y|Z)$ is unachievable when the communication is restricted from Alice to Bob, and yet it becomes achievable if the communication direction is from Bob to Alice. We further provide an example when $I(X : Y|Z)$ is achievable only if two-way communication is used.

Before presenting these results in greater detail, we begin in Sect. 2 with a more precise overview of the key rates studied in this paper. In Sect. 3, we then present the Gács-Körner Common Information and prove some basic properties. Section 4 contains our main results, with longer proofs postponed to the appendix. Finally, Sect. 5 offers some concluding remarks.

2 Definitions

Let us review the relevant definitions of secret key rate under various communication scenarios. We consider random variables X, Y and Z ranging over finite alphabets $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$ respectively. For a general distribution q, we say its support (denoted by *supp*$[q]$) is the collection of x such that $q(x) > 0$. In all distillation tasks, we assume that Alice and Bob each have access to one part of an i.i.d. (identical and independently distributed) source XYZ whose distribution is p_{XYZ}. Hence, after n realizations of the source, X^n, Y^n and Z^n belong to Alice, Bob, and Eve respectively. In addition, Alice and Bob each possess a local random variable, Q_A and Q_B respectively, which are mutually independent from each other and from $X^nY^nZ^n$. This allows them to introduce local randomness into their processing of X^nY^n.

We first turn to the most restrictive scenario, which is key distillation using publicly shared randomness. The *common randomness (c.r.) key rate* of X, Y, and Z, denoted by $K^{c.r.}(X : Y|Z)$, is defined to be the largest R such that for every $\epsilon > 0$, there is an integer N such that $n \geqslant N$ implies the existence of (a) a random variable W independent of $X^nY^nZ^n$ and ranging over some set $\mathcal{W}$, (b) a random variable K ranging over some set $\mathcal{K}$, and (c) a pair of mappings $f(X^n, Q_A, W)$ and $g(Y^n, Q_B, W)$ for which

(i) $Pr[f = g = K] > 1 - \epsilon$;
(ii) $\log|\mathcal{K}| - H(K|Z^nW) < \epsilon$;
(iii) $\frac{1}{n}\log|\mathcal{K}| \geqslant R$.

We next move to the more general scenario of when Alice and Bob are allowed to engage in public communication. A *local operations and public communication* (LOPC) protocol consists of a sequence of public communication exchanges between Alice and Bob. The i^{th} message exchanged between them is described by the variable M_i. If Alice (resp. Bob) is the broadcasting party in round i, then M_i is a function of X^n and Q_A (resp. Y^n and Q_B) as well as the previous messages $(M_1, M_2, \cdots, M_{i-1})$. The protocol is one-way if there is only one round of a message exchange.

For distribution p_{XYZ}, the *Alice-to-Bob secret key rate* $\overrightarrow{K}(X : Y|Z)$ is the largest R that satisfies the above three conditions except with W being replaced by some message M that is generated by Alice and therefore a function of (X^n, Q_A). We can likewise define the Bob-to-Alice key rate $\overleftarrow{K}(X : Y|Z)$. The *(two-way) secret key rate* of X and Y given Z, denoted by $K(X : Y|Z)$, is defined analogously except with $M = (M_1, M_2, \cdots, M_r)$ being any random variable generated by an LOPC protocol [1,8]. The key rates satisfy the obvious relationship:

$$K^{c.r.}(X : Y|Z) \leqslant \begin{cases} \overrightarrow{K}(X : Y|Z) \\ \overleftarrow{K}(X : Y|Z) \end{cases} \leqslant K(X : Y|Z). \tag{4}$$

3 The Gács-Körner Common Information

In this section, we introduce the Gács-Körner Common Information. For every pair of random variables XY, there exists a *maximal* common variable J_{XY} in the sense that J_{XY} is a function of both X and Y, and any other such common function of both X and Y is itself a function of J_{XY}. Hence, up to relabeling, the variable J_{XY} is unique for each distribution p_{XY}. In terms of its structure, a distribution p_{XY} can always be decomposed as

$$p(x, y) = \sum_{J_{XY}=j} p(x, y|j)p(j), \tag{5}$$

where for any $x, x' \in \mathcal{X}$ and $y, y' \in \mathcal{Y}$, the conditional distributions satisfy $p(x, y|j)p(x, y'|j') = 0$ and $p(x, y|j)p(x', y|j') = 0$ if $j \neq j'$. Gács and Körner identify $H(J_{XY})$ as the common information of XY [6].

It is instructive to rigorously prove the statements of the preceding paragraph. A *common partitioning of length* t for XY are pairs of subsets $(\mathcal{X}_i, \mathcal{Y}_i)_{i=1}^t$ such that

(i) $\mathcal{X}_i \cap \mathcal{X}_j = \mathcal{Y}_i \cap \mathcal{Y}_j = \emptyset$ for $i \neq j$,
(ii) $p(\mathcal{X}_i|\mathcal{Y}_j) = p(\mathcal{Y}_i|\mathcal{X}_j) = \delta_{ij}$, and
(iii) if $(x, y) \in \mathcal{X}_i \times \mathcal{Y}_i$ for some i, then $p_X(x)p_Y(y) > 0$.

For a given common partitioning, we refer to the subsets $\mathcal{X}_i \times \mathcal{Y}_i$ as the "blocks" of the partitioning. The subscript i merely serves to label the different blocks, and for any fixed labeling, we associate a random variable $C(X, Y)$ such that $C(x, y) = i$ if $(x, y) \in \mathcal{X}_i \times \mathcal{Y}_i$. Note that each party can determine the value of

J from their local information, and it is therefore called a *common function* of X and Y. A *maximal common partitioning* is a common partitioning of greatest length. The following proposition is proven in the appendix.

Proposition 1

(a) *Every pair of finite random variables XY has a unique maximal common partitioning, which we denote by J_{XY}.*

(b) *Variable J_{XY} satisfies*

$$H(J_{XY}) = \max_K \{H(K) : 0 = H(K|X) = H(K|Y)\}$$

iff J_{XY} is a common function for the maximal common partitioning of XY.

(c) *If $f(X) = g(Y) = C$ is any other common function of X and Y, then $C(J_{XY})$.*

With property (a), we can speak unambiguously of *the* maximal common partitioning of a distribution p_{XY}. Consequently the variable J_{XY} is unique up to a relabeling of its range. The following proposition from [6] provides a useful characterization of values x and x' that belong to the same block in a maximal common partitioning.

Proposition 2 ([6]). *If $J_{XY}(x) = J_{XY}(x')$ for $x, x' \in J_{XY}$, then there exists a sequence of values*

$$xy_1x_1y_2x_2 \cdots y_nx'$$

such that $p(x, y_1)p(y_1, x_1)p(x_1, y_2) \cdots p(y_n, x') > 0$.

4 Results

4.1 Key Distillation Using Auxiliary Public Randomness

The Gács and Körner Common Information plays a central role in the problem of key distillation with no communication. To see a preliminary connection, we recall an operational interpretation of $H(J_{XY})$ that Gács and Körner prove in Ref. [6]. The task involves Alice and Bob constructing faithful encodings of their respective sources X and Y, and $H(J_{XY})$ quantifies the asymptotic average sequence-length of codewords per copy such that both Alice and Bob's encodings output matching codewords with high probability over this sequence [6].

For the task of key distillation, Alice and Bob are likewise trying to convert their sources into matching sequences of optimal length. However, the key distillation problem is different in two ways. On the one hand there is the additional constraint that the common sequence should be nearly uncorrelated from Eve. On the other hand, unlike the Gács-Körner problem, it is not required that these sequences belong to faithful encodings of the sources X and Y. Nevertheless, we find that $H(J_{XY}|Z)$ quantifies the distillable key when Alice and Bob are unable to communicate with one another. This is also the rate even if Alice and Bob have access to auxillary public randomness which is uncorrelated with their primary distribution.

Theorem 1. *$K^{c.r.}(X : Y|Z) = H(J_{XY}|Z)$. Moreover, $H(J_{XY}|Z)$ is achievable with no additional common randomness.*

Proof. See the appendix. Many parts of the converse proof follow analogously to the converse proof of Theorem 2.6 in Ref. [4] (see also [5]).

One can also consider a related quantity known as the *maximal conditional common function* $J_{XY|Z}$, which is the collection of variables $\{J_{XY|Z=z} : z \in \mathcal{Z}\}$ with $J_{XY|Z=z}$ being a maximal common function of the conditional distribution $p_{XY|Z=z}$. The variable $J_{XY|Z}$ is again unique for every distribution p_{XYZ} up to relabeling. Since $J_{XY|Z=z}$ is computed from both X and Y with the additional information that $Z = z$, maximality of $J_{XY|Z=z}$ ensures that J_{XY} is a function of $J_{XY|Z=z}$ for each $z \in \mathcal{Z}$. In other words, a labeling of J_{XY} and $J_{XY|Z}$ can be chosen so that J_{XY} is a coarse-graining of $J_{XY|Z}$. Therefore, $H(J_{XY}|Z) \leqslant H(J_{XY|Z}|Z)$ with equality iff $H(J_{XY|Z}|ZJ_{XY}) = 0$. When the equality condition holds, it means that for each $z \in \mathcal{Z}$, the value of $J_{XY|Z=z}$ can be determined from J_{XY} alone. Hence, the variables J_{XY} and $J_{XY|Z}$ must be equivalent up to relabeling. From this it follows that a distribution satisfies $H(J_{XY|Z}|ZJ_{XY}) = 0$ iff it admits a decomposition of

$$p(x, y, z) = \sum_{J_{XY}=j} p(x, y|z, j)p(j|z)p(z), \tag{6}$$

where for any $x, x' \in \mathcal{X}$, $y, y' \in \mathcal{Y}$ and $z, z' \in \mathcal{Z}$ the conditional distributions satisfy

$$p(x, y|z, j)p(x, y'|z', j') = 0, \qquad p(x, y|j)p(x', y|z', j') = 0 \quad \text{if} \quad j \neq j'.$$

The class of distributions of this form we shall call *uniform block* (UB) (see Fig. 1).

The quantity $H(J_{XY|Z}|Z)$ is the private key rate when Eve is helping yet Alice and Bob are still prohibited from communicating with one another. Thus, the difference $H(J_{XY|Z}|Z) - H(J_{XY}|Z)$ quantifies how much Eve can assist Alice and Bob in distilling key when no communication is exchanged between the two. From the previous paragraph, it follows that Eve offers no assistance (i.e. the private key rate equals the secret key rate) in the no-communication scenario iff the distribution is UB.

Returning to Theorem 1, we can now answer the underlying question of this paper for no-communication distillation. By using the chain rule of conditional mutual information and the fact that J_{XY} is both a function of X and Y, we readily compute

$$\begin{aligned} I(X : Y|Z) = I(J_{XY}X : Y|Z) &= I(J_{XY} : Y|Z) - I(X : Y|ZJ_{XY}) \\ &= H(J_{XY}|Z) - I(X : Y|ZJ_{XY}). \end{aligned} \tag{7}$$

The conditional mutual information is thus an achievable rate whenever $I(X : Y|ZJ_{XY}) = 0$. Distributions satisfying this equality are uniform block with

(a) Not Uniform Block

		X ⟶		
	Z = 0	0	1	2
Y ↓	0	1/2	·	·
	1	·	1/2	·
	2	·	·	·

Z = 1	0	1	2
0	·	1/3	·
1	·	1/3	·
2	·	·	1/3

(b) Uniform Block

		X ⟶		
	Z = 0	0	1	2
Y ↓	0	1/2	·	·
	1	·	1/2	·
	2	·	·	·

Z = 1	0	1	2
0	·	·	·
1	·	·	1/3
2	·	1/3	1/3

Fig. 1. Example of a distribution that is not uniform block (a) and one that is (b). Each entry corresponds to a conditional probability value $p(x, y|z)$. UB distribution (b) is not uniform block independent (UBI) since the block in the $Z = 1$ plane contains correlations between Alice and Bob.

the extra condition that $p(x, y|z, j) = p(x|z, j)p(y|z, j)$ in Eq. (6). We shall call distributions having this form *uniform block independent* (UBI). Putting everything together, we find that

Corollary 1. *A distribution p_{XYZ} satisfies $K^{c.r.}(X : Y|Z) = I(X : Y|Z)$ if and only if it is uniformly block independent.*

Remark 1. The no-communication results discussed above and proven in the appendix are already implicit in the work of Csiszár and Narayan. In Ref. [4], they study various key distillation scenarios with Eve functioning as a helper and limited communication between Alice and Bob. Included in this is the no-communication scenario with and without helper. However, being very general in nature, Csiszár and Narayan's results involve optimizations over auxiliary random variables, and it is therefore still a non-trivial matter to discern Theorem 1 and Corollary 1 directly from their work. Additionally, they do not consider the scenario of just shared public randomness.

4.2 Obtaining $I(X : Y|Z)$ with One-Way Communication

In this section we want to identify the type of tripartite distributions from which secret key can be distilled at the rate $I(X : Y|Z)$ using one-way communication. Since $K(X : Y|Z) \leqslant I(X : Y|Z)$, our analysis deals with distributions for which one-way communication suffices to optimally distill secret key. Manipulating Eq. (1) of Lemma 1 allows us to determine when $\overrightarrow{K}(X : Y|Z) = I(X : Y|Z)$. We have that

$$\begin{aligned} I(K : Y|U) - I(K : Z|U) &= I(K : Y|ZU) - I(K : Z|YU) \\ &= I(KU : Y|Z) - I(U : Y|Z) - I(K : Z|YU) \\ &= I(X : Y|Z) - I(X : Y|KUZ) - I(U : Y|Z) - I(K : Z|YU), \end{aligned}$$

where K and U satisfy $KU - X - YZ$. From this and Lemma 1, we conclude the following.

Lemma 2. *Distribution p_{XYZ} has $\overrightarrow{K}(X:Y|Z) = I(X:Y|Z)$ iff there exists variables $KUXYZ$ with K and U ranging over sets of size no greater than $|\mathcal{X}|+1$ such that*

$$\begin{array}{llll} (1) & KU - X - YZ, & (2) & X - KUZ - Y, \\ (3) & U - Z - Y, & (4) & K - YU - Z. \end{array} \tag{8}$$

The conditions of Lemma 2 allow for the follow rough interpretation. (1) says that Alice is able to generate variables K and U from knowledge of her variable X. We think of K as containing the key that Alice and Bob will share and U as the public message sent from Alice to Bob. (2) says that from Eve's perspective, Alice and Bob share no more correlations given U and K. Likewise, (3) says that from Eve's perspective, the public message is uncorrelated with Bob. Finally, (4) says that after learning U, Bob can generate the key K that is independent from Eve.

Unfortunately, Lemma 2 does not provide a transparent characterization of the distributions for which $\overrightarrow{K}(X:Y|Z) = I(X:Y|Z)$. We next proceed to obtain a better picture of these distributions by exploring additional consequences of the Markov chains in Eq. (8). The following places a necessary condition on the distributions. We will see in Sect. 4.4, however, that it fails to be sufficient.

Theorem 2. *If distribution p_{XYZ} has either $\overrightarrow{K}(X:Y|Z) = I(X:Y|Z)$ or $\overleftarrow{K}(X:Y|Z) = I(X:Y|Z)$, then p_{XYZ} must have the following property: For any $z \in \mathcal{Z}$, if $\mathcal{X}_i \times \mathcal{Y}_i$ and $\mathcal{X}_j \times \mathcal{Y}_j$ are two distinct blocks in the maximal common partitioning of $p_{XY|Z=z}$, then*

$$p_{XY}(\mathcal{X}_i, \mathcal{Y}_j) = 0.$$

Proof. Without loss of generality, assume that $\overrightarrow{K}(X:Y|Z) = I(X:Y|Z)$. For distribution $p_{XY|Z=z}$ with maximal common partition $(\mathcal{X}_\lambda, \mathcal{Y}_\lambda)_{\lambda=1}^t$, consider arbitrary $(x_i, y_i) \in \mathcal{X}_i \times \mathcal{Y}_i$ and $(x_j, y_j) \in \mathcal{X}_j \times \mathcal{Y}_j$. Note that from the definition of a maximal common partitioning, we have that $p(x_i, z)p(y_i, z) > 0$, but we need not have that $p(x_i, y_i, z) > 0$.

We will prove that $p(x_i, y_j, z') = 0$ for all $z' \in \mathcal{Z}$ (clearly this already holds when $z' = z$). Suppose on the contrary that $p(x_i, y_j, z') > 0$. Since $p(x_i, z) > 0$, there will exist some $y_i' \in \mathcal{Y}_i$ such that $p(x_i, y_i', z) > 0$. Then the Markov chain condition $KU - X - YZ$ implies that for some $(k, u) \in \mathcal{K} \times \mathcal{U}$ such that $p(k, u|x_i) > 0$, we have

$$p(k, u|x_i) = p(k, u|x_i, y_i', z) = p(k, u|x_i, y_j, z') > 0. \tag{9}$$

Equation (9) implies that both $p(k, u|y_i', z) > 0$ and $p(k, u|y_j, z') > 0$. From $p(u|y_i', z) > 0$ and the Markov chain $U - Z - Y$, we have that $p(u|y_j, z) > 0$.

(a)

$X \longrightarrow$, $Y \downarrow$

$Z=0$	0	1	2
0	1/2	·	·
1	·	1/2	·
2	·	·	·

$Z=1$	0	1	2
0	·	·	1/3
1	·	·	1/3
2	·	1/3	·

$Z=2$	0	1	2
0	·	·	·
1	·	·	1/3
2	·	1/3	1/3

(b)

$X \longrightarrow$, $Y \downarrow$

$Z=0$	0	1	2
0	1/2	·	·
1	·	1/2	·
2	·	·	·

$Z=1$	0	1	2
0	·	·	1/3
1	·	1/3	1/3
2	·	·	·

$Z=2$	0	1	2
0	·	·	·
1	·	·	1/3
2	·	1/3	1/3

Fig. 2. (a) The conditions of Theorem 2 are violated for this distribution. To see this, note that the events $(X = 1, Y = 2)$ and $(X = 2, Y = 1)$ are both possible when $Z = 1$. Hence, Theorem 2 necessitates $p(1, 1) = 0$, which is not the case because of the plane $Z = 0$. Distribution (b) lacks this characteristic and therefore it satisfies the conditions of Theorem 2.

Then we can further derive

$$\begin{aligned} 0 < p(k, u|y_j, z') = p(u|y_j, z')p(k|u, y_j, z') &= p(u|y_j, z')p(k|u, y_j, z) \\ &\Rightarrow \quad p(k|u, y_j, z) > 0, \\ &\Rightarrow \quad p(k, u|y_j, z) = p(k|u, y_j, z)p(u|y_j, z) > 0, \end{aligned}$$

where we have used the Markov chain $K - YU - Z$. From the last line, we must be able to find some $x'_j \in \mathcal{X}_j$ such that $p(x'_j, y_j, z) > 0$ and $p(k, u|x'_j, y_j, z) > 0$. Inverting probabilities gives that both $p(x'_j, y_j|k, u, z) > 0$ and $p(x_i, y'_i|k, u, z) > 0$. Hence,

$$\begin{aligned} I(X : Y|KUZ) &= I(J_{XY|Z}X : Y|KUZ) \\ &= I(X : Y|J_{XY|Z}KUZ) + \sum_{k,u,z} H(J_{XY|Z=z}|k, u, z)p(k, u, z) > 0, \end{aligned}$$

since $H(J_{XY|Z=z}|k, u, z) > 0$ because $(x_i, y'_i) \in \mathcal{X}_i \times \mathcal{Y}_i$ and $(x'_j, y_j) \in \mathcal{X}_j \times \mathcal{Y}_j$. However, this strict inequality contradicts the Markov chain condition $X - KUZ - Y$. ■

Figure 2 (a) provides an example distribution which does not satisfy the necessary conditions of Theorem 2 for $I(X : Y|Z)$ to be an achievable one-way key rate. On the other hand, Fig. 2 (b) depicts an distribution for which the conditions of the theorem are met. However, Theorem 3 in the next section will show that both distributions (a) and (b) have $K(X : Y|Z) < I(X : Y|Z)$.

4.3 Obtaining $I(X : Y|Z)$ with Two-Way Communication

We now turn to the general scenario of interactive two-way communication. Our main result is the necessary structural condition of Theorem 3. Its statement requires some new terminology.

For two distributions p_{XY} and q_{XY} over $\mathcal{X}\times\mathcal{Y}$, we say that $q_{XY} \blacktriangleleft p_{XY}$ if, up to a permutation between X and Y, the distributions satisfy $supp[q_X] \subset supp[p_X]$ and one of the three additional conditions: (i) q_{XY} is uncorrelated, (ii) $supp[q_Y] \subset supp[p_Y]$, or (iii) $y \in supp[q_Y] \setminus supp[p_Y]$ implies that $H(X|Y=y)=0$.

Theorem 3. *Let p_{XYZ} be a distribution over $\mathcal{X}\times\mathcal{Y}\times\mathcal{Z}$ such that $p_{XY|Z=z_1} \blacktriangleleft p_{XY|Z=z_0}$ for some $z_0, z_1 \in \mathcal{Z}$. If there exists some pair $(x,y) \in supp[p_{X|Z=0}] \times supp[p_{Y|Z=0}]$ for which $p(x,y|z_1) > 0$ but $p(x,y|z_0)=0$, then $K(X:Y|Z) < I(X:Y|Z)$.*

Proof. The proof will involve showing that there exists a channel $\overline{Z}|Z$ such that $I(X:Y|\overline{Z}) < I(X:Y|Z)$. The channel will involve mixing z_0 and z_1 but leaving all other elements unchanged. Define the function

$$f(t) = I(X:Y)_{(1-t)p_{XY|Z=z_0}+tp_{XY|Z=z_1}} \qquad t \in [0,1], \tag{10}$$

which gives the mutual information of the mixed distribution $(1-t)p_{XY|Z=z_0} + tp_{XY|Z=z_1}$. The function f is continuous and twice differentiable in the open interval $(0,1)$. To prove the theorem, we will need a simple general fact about functions of this sort.

Proposition 3. *Suppose that f is a continuous function on the closed interval $[0,1]$ and twice differentiable in the open interval $(0,1)$. Suppose there exists some $0<\delta<1$ such that f is strictly convex in the interval $\mathcal{I}=(0,\delta]$ and $f(1)-f(0) > f'(t)$ for all $t \in \mathcal{I}$. Then $f(t) < (1-t)f(0)+tf(1)$ for all $t \in \mathcal{I}$.*

Continuing with the proof of Theorem 3, it will suffice to show that the function given by Eq. (10) satisfies the conditions of Proposition 3. For if this is true, then we can argue as follows. Choose ϵ sufficiently small so that $\frac{\epsilon p(z_1)}{p(z_0)+\epsilon p(z_1)} \in (0,\delta]$, where δ is described by the proposition. Define the channel $\overline{Z}|Z$ by $p(\overline{z}_0|z_1)=\epsilon$, $p(\overline{z}_1|z_1) = 1-\epsilon$, and $p(\overline{z}|z)=1$ for all $z \neq z_1 \in \mathcal{Z}$. This means that $p(\overline{z}_0) = p(z_0)+\epsilon p(z_1)$ and $p(\overline{z}_1) = (1-\epsilon)p(z_1)$, and inverting the probabilities gives $p(z_1|\overline{z}_1)=1$, $p(z_1|\overline{z}_0) = \frac{\epsilon p(z_1)}{p(z_0)+\epsilon p(z_1)}$, and $p(z_0|\overline{z}_0) = \frac{p(z_0)}{p(z_0)+\epsilon p(z_1)}$. Since $p(x,y|\overline{Z}=\overline{z}) = \sum_z p(x,y|Z=z)p(Z=z|\overline{Z}=\overline{z})$, the average conditional mutual information is

$$\begin{aligned}
&\sum_{z\neq z_0,z_1\in\mathcal{Z}} I(X:Y|\overline{Z}=\overline{z})p(\overline{z}) + f(\tfrac{\epsilon p(z_1)}{p(z_0)+\epsilon p(z_1)})p(\overline{z}_0) + f(1)p(\overline{z}_1) \\
&< \sum_{z\neq z_0,z_1\in\mathcal{Z}} I(X:Y|Z=z)p(z) \\
&\quad + \left(\tfrac{p(z_0)}{p(z_0)+\epsilon p(z_1)}f(0) + \tfrac{\epsilon p(z_1)}{p(z_0)+\epsilon p(z_1)}f(1)\right)p(\overline{z}_0) + f(1)(1-\epsilon)p(z_1) \\
&= I(X:Y|Z),
\end{aligned} \tag{11}$$

where Proposition 3 at $x = \frac{\epsilon p(z_1)}{p(z_0)+\epsilon p(z_1)}$ has been invoked.

Let us then show that the conditions of Proposition 3 hold true for the function given by Eq. (10) whenever $p_{XY|Z=z_1} \blacktriangleleft p_{XY|Z=z_0}$; i.e. that there exists some interval $(0, \delta]$ for which f is strictly convex and $f(1) - f(0) > f'(t)$. We have

$$\begin{aligned} f(t) = &- \sum_{x\in\mathcal{X}} [(1-t)p(x|z_0) + tp(x|z_1)] \log[(1-t)p(x|z_0) + tp(x|z_1)] \\ &- \sum_{y\in\mathcal{Y}} [(1-t)p(y|z_0) + tp(y|z_1)] \log[(1-t)p(y|z_0) + tp(y|z_1)] \\ &+ \sum_{x\in\mathcal{X}} \sum_{y\in\mathcal{Y}} [(1-t)p(x,y|z_0) + tp(x,y|z_1)] \log[(1-t)p(x,y|z_0) + tp(x,y|z_1)]. \end{aligned} \quad (12)$$

We are interested in $\lim_{t\to 0} f'(t)$ and $\lim_{t\to 0} f''(t)$. To compute these, we use the fact that the function $g(t) = (r + st)\log(r + st)$ satisfies $g'(t) = s(1 + \log(r + st))$ and $g''(t) = \frac{s^2}{r+st}$. We separate the analysis into three cases. Without loss of generality, we will assume $supp[p_{X|Z=z_1}] \subset supp[p_{X|Z=z_0}]$.

Case (i): $\boldsymbol{p_{XY|Z=z_1}}$ is Uncorrelated

Since $supp[p_{X|Z=z_1}] \subset supp[p_{X|Z=z_0}]$, we can assume that $p(x|z_0) \neq 0$ for all x; otherwise there is no term involving x in Eq. (12). Now suppose that $p(y|z_0) = 0$. Then for this fixed y, the summation over x in the third term of Eq. (12) becomes

$$\begin{aligned} &\sum_{x\in\mathcal{X}} [(1-t)p(x,y|z_0) + tp(x,y|z_1)] \log[(1-t)p(x,y|z_0) + tp(x,y|z_1)] \\ &= t \sum_{x\in\mathcal{X}} p(x|z_1)p(y|z_1) \log[tp(x|z_1)p(y|z_1)] \\ &= tp(y|z_1)\log[tp(y|z_1)] + tp(y|z_1) \sum_{x\in\mathcal{X}} p(x|z_1)\log[p(x|z_1)]. \end{aligned} \quad (13)$$

Hence, by letting $\mathcal{B}_I = \{y : p(y|z_I) > 0\}$ for $I \in \{0, 1\}$, we can equivalently write Eq. (12) as

$$\begin{aligned} f(t) = &- \sum_{x\in\mathcal{X}} [(1-t)p(x|z_0) + tp(x|z_1)] \log[(1-t)p(x|z_0) + tp(x|z_1)] \\ &- \sum_{y\in\mathcal{B}_0} [(1-t)p(y|z_0) + tp(y|z_1)] \log[(1-t)p(y|z_0) + tp(y|z_1)] \\ &+ \sum_{y\in\mathcal{B}_0} \sum_{x\in\mathcal{X}} [(1-t)p(x,y|z_0) + tp(x,y|z_1)] \log[(1-t)p(x,y|z_0) + tp(x,y|z_1)] \\ &+ t \sum_{y\in\mathcal{B}_1\setminus\mathcal{B}_0} p(y|z_1) \sum_{x\in\mathcal{X}} p(x|z_1)\log[p(x|z_1)]. \end{aligned} \quad (14)$$

If $p(x,y|z_0) = 0$ for some $(x,y) \in \mathcal{X} \times \mathcal{B}_0$, then the first derivative of (14) will diverge to $-\infty$ as $t \to 0$ while its second derivative will diverge to $+\infty$ whenever $p(x,y|z_1) > 0$. But by assumption, there is at least one pair of (x,y) for which this latter case holds. Hence, an interval $(0, \delta]$ can always be found for which Proposition 3 can be applied to f.

Case (ii): $\boldsymbol{\mathcal{B}_1 \setminus \mathcal{B}_0 = \emptyset}$

This is covered in case (iii).

Case (iii): $\boldsymbol{y \in \mathcal{B}_1 \setminus \mathcal{B}_0 \;\Rightarrow\; p(y|z_1) = p(x_y, y|z_1)}$ for some particular $\boldsymbol{x_y \in \mathcal{X}}$

The condition $p(y|z_1) = p(x_y, y|z_1)$ implies that $p(x, y|z_1) = 0$ for all $x \neq x_y$. Then similar to the previous case, when $y \in \mathcal{B}_1 \setminus \mathcal{B}_0$, the summation over x in the third term of Eq. (12) is

$$\begin{aligned}\sum_{x\in\mathcal{X}} tp(x, y|z_1)\log[tp(x, y|z_1)] &= tp(x_y, y|z_1)\log[tp(x_y, y|z_1)]\\ &= tp(y|z_1)\log[tp(y|z_1)]. \qquad (15)\end{aligned}$$

Hence each term with $y \in \mathcal{B}_1 \setminus \mathcal{B}_0$ becomes canceled in Eq. (12). Then Eq. (12) reduces to

$$\begin{aligned}f(t) = &-\sum_{x\in\mathcal{X}}[(1-t)p(x|z_0) + tp(x|z_1)]\log[(1-t)p(x|z_0) + tp(x|z_1)]\\ &-\sum_{y\in\mathcal{B}_0}[(1-t)p(y|z_0) + tp(y|z_1)]\log[(1-t)p(y|z_0) + tp(y|z_1)]\\ &+\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{B}_0}[(1-t)p(x, y|z_0) + tp(x, y|z_1)]\log[(1-t)p(x, y|z_0) + tp(x, y|z_1)]. \qquad (16)\end{aligned}$$

As in the previous case, the first derivative of this function will diverge to $-\infty$ while its second derivative will diverge to $+\infty$ whenever $p(x, y|z_1) > 0$ and $p(x, y|z_0) = 0$. By assumption, such a pair (x, y) exists, and so again, an interval $(0, \delta]$ can always be found for which Proposition 3 can be applied to f. Note that when $\mathcal{B}_1 \setminus \mathcal{B}_0 = \emptyset$, as in case (ii), Eq. (16) is equivalent to (12). The derivative argument can thus be applied directly to (12). ■

Theorem 3 is quite useful in that it allows us to quickly eliminate many distributions from achieving the rate $I(X : Y|Z)$. For example, consider when $p_{XY|Z=z}$ is uncorrelated for some $z \in \mathcal{Z}$, but $p_{XY|Z=z'}$ is perfectly correlated for some other $z' \in \mathcal{Z}$ with either $supp[p_{X|Z=z}] \subset supp[p_{X|Z=z'}]$ or $supp[p_{Y|Z=z}] \subset supp[p_{Y|Z=z'}]$. Here, perfectly correlated means that $p(x, y|z') = p(x|z')\delta_{x,y}$ up to relabeling. Then from Theorem 3, it follows that $I(X : Y|Z)$ is an achievable rate only if

$$p(x, y|z) > 0 \quad \Rightarrow \quad p(x|z')p(y|z') = 0.$$

In other words, it is always possible for either Alice or Bob to identify when $Z \neq z'$.

Finally, we close this section by comparing Theorems 2 and 3. In short, neither one supersedes the other. As noted above, distribution (b) in Fig. 2 satisfies the necessary condition of Theorem 2 for $\overrightarrow{K}(X : Y|Z) = I(X : Y|Z)$. However, Theorem 3 can be used to show that $K(X : Y|Z) < I(X : Y|Z)$. This is because $p_{XY|Z=1} \blacktriangleleft p_{XY|Z=2}$ yet $p(1, 1|2) = 0$ while $p(1, 1|1) = 1/3$. Therefore its key rate is strictly less than $I(X : Y|Z)$. Figure 3 depicts a distribution for which Theorem 3 cannot be applied but Theorem 2 shows that $\overrightarrow{K}(X : Y|Z) < I(X : Y|Z)$. The two-way key rate for this distribution is still unknown.

$X \longrightarrow$

$Y \downarrow$

$Z=0$	0	1	2
0	1/7	1/7	·
1	1/7	1/7	1/7
2	·	1/7	1/7

$Z=1$	0	1
0	1/2	·
1	·	1/2

Fig. 3. The event $(x, y) = (0, 1)$ has conditional probabilities $p(0, 1|Z = 0) > 0$ and $p(0, 1|Z = 1) = 0$. However, we cannot use these facts in conjunction with Theorem 3 to conclude that $K(X : Y|Z) < I(X : Y|Z)$ since the distribution does not satisfy $p_{XY|Z=0} \blacktriangleleft p_{XY|Z=1}$ (neither $supp[p_{X|Z=0}] \subset supp[p_{X|Z=1}]$ nor $supp[p_{Y|Z=0}] \subset supp[p_{Y|Z=1}]$). On the other hand, since $p(0, 1|Z = 0) > 0$, Theorem 2 can be applied to conclude that the one-way rate is less than $I(X : Y|Z)$.

$X \longrightarrow$

$Y \downarrow$

$Z=0$	0	1
0	1/2	·
1	·	1/2
2	·	·

$p(Z=0) = \frac{1}{|Z|}$

$Z=1$	0	1
0	·	·
1	·	·
2	1/2	1/2

$p(Z=1) = \frac{1}{|Z|}$

$Z=2$	0	1
0	·	·
1	·	·
2	1	·

$p(Z=2) = \frac{1}{|Z|}$

Fig. 4. A distribution requiring communication from Bob to Alice to achieve a key rate of $I(X : Y|Z)$.

4.4 Communication Dependency in Optimal Distillation

We next consider some general features of the public communication when performing optimal key distillation. Our main observations will be that (i) attaining a key rate of $I(X : Y|Z)$ by one-way communication may depend on the direction of the communication, and (ii) two-way communication may be necessary in order to achieve the key rate $I(X : Y|Z)$.

Example 1 (Optimal one-way distillation depends on communication direction). Consider the distribution depicted in Fig. 4 with $I(X : Y|Z) = 1/3$. When Bob is the communicating party, a protocol attaining this as a key rate is obvious: he simply announces whether or not $y \in \{0, 1\}$. If it is, they share one bit, otherwise they fail. Hence, $I(X : Y|Z) = 1/3$ is an achievable key rate.

However, the interesting question is whether or not the key rate $I(X : Y|Z)$ is achievable by one-way communication from Alice to Bob. We will now show that this is not possible. By Lemma 2, in order to obtain the rate $I(X : Y|Z)$, there must exist random variables U and V satisfying Eq. (8). Assume that such variables exist. If $U - Z - Y$, then $p(u|X = 0)p(u|X = 1) > 0$ for all $U = u$; otherwise, U and Y couldn't be independent. But then $X - KUZ - Y$ applied to $Z = 0$ means there must exist a pair $(k, u) \in \mathcal{K} \times \mathcal{U}$ such that

$$p(k, u|X = 0) = 0 \quad \& \quad p(k, u|X = 1) > 0.$$

Hence, $0 = p(k|Y = 2, U = u, Z = 2) < p(k|Y = 2, U = u, Z = 1)$, which contradicts $K - YU - Z$. Thus $\overrightarrow{K}(X : Y|Z) < I(X : Y|Z) = \overleftarrow{K}(X : Y|Z)$.

$X \longrightarrow$

	$Z=3$	0	1	2
Y	0	·	·	1/2
$\downarrow$	1	·	·	1/2

$p(Z=3) = \frac{1}{|Z|}$

$Z=4$	0	1	2
0	·	·	1
1	·	·	·

$p(Z=4) = \frac{1}{|Z|}$

Fig. 5. Additional outcomes augmented to the distribution of Fig. 4. The enlarged distribution can no longer attain a key rate of $I(X:Y|Z)$ unless both parties communicate.

In this example, notice that if we restricted Eve's distribution to $\mathcal{Z} = \{0,1\}$ (i.e. $p(Z=2)=0$), then the rate $I(X:Y|Z)$ would indeed be achievable using one-way communication from Alice to Bob. This is because without the $z=2$ outcome, the Markov Chain $X-Y-Z$ holds. Such a result is counterintuitive since Alice and Bob share no correlations when $z \in \{1,2\}$. And yet the distribution becomes one-way reversible from Alice to Bob when $p(Z=2)=0$, but otherwise it is not.

Example 2 (Optimal distillation requires two-way communication). The previous example can be generalized by adding two more outcomes for Eve so that $|Z|=5$. The additional outcomes are shown in Fig. 5 and this is combined with Fig. 4 to give the full distribution. Notice that the distribution $p_{XY|Z=3}$ is obtained from $p_{XY|Z=1}$ simply by swapping Alice and Bob's variables, and likewise for $p_{XY|Z=4}$ and $p_{XY|Z=2}$. Hence by the argument of the previous example, if Eve were to reveal whether or not $z \in \{0,3,4\}$, then the average Bob-to-Alice distillable key c onditioned on this information would be less than $I(X:Y|Z)$. Likewise, if Eve were to reveal whether or not $z \in \{0,1,2\}$, then the Alice-to-Bob distillable key conditioned on this information would be less than $I(X:Y|Z)$. Thus since the average conditional key rate cannot exceed the key rate with no side information, we conclude that $I(X:Y|Z)$ is unattainable using one one-way communication in either direction. On the other hand, the distribution is easily seen to admit a key rate of $I(X:Y|Z)$ when the parties simply announce whether or not their variable belongs to the set $\{0,1\}$.

5 Conclusion

In this paper, we have considered when a secret key rate of $I(X:Y|Z)$ can be attained by Alice and Bob when working with a variety of auxiliary resources. The conditional mutual information quantifies the private key rate of p_{XYZ}, which is the rate of key private from Eve that is attainable when Eve helps Alice and Bob by announcing her variable. Therefore, distributions for which $K(X:Y|Z) = I(X:Y|Z)$ are those for which nothing is gained when Eve functions as a helper rather than a full adversary.

We have found that with no additional communication, the key rate is $I(X:Y|Z)$ if and only if the distribution is uniform block independent. Furthermore, supplying Alice and Bob with additional public randomness does not increase the distillable key rate. While this may not be overly surprising since the considered common randomness is uncorrelated with the source, it is nevertheless a nontrivial result because in general, randomness can serve a resource in distillation tasks [1,10].

Turning to the one and two-way communication scenarios, we have presented in Theorems 2 and 3 necessary conditions for a distribution to attain the key rate $I(X:Y|Z)$. The conditions we have derived are all single-letter structural characterizations, and they are thus computationally easy to apply. We leave open the question of whether Theorem 3 is also sufficient for attaining $I(X:Y|Z)$, although we have no strong reason to believe this is true. Further improvements to the results of this paper can possibly be obtained by studying tighter bounds on $K(X:Y|Z)$ than the intrinsic information such as those presented in Refs. [11] and [7]. Nevertheless, we hope this paper has shed new light on the problem of secret key distillation under various communication settings.

6 Appendix

6.1 Proof of Propositions 1

Proof. (a) Trivially $\mathcal{X}\times\mathcal{Y}$ gives a common partitioning of length one, and any common partitioning cannot have length exceeding $\min\{|\mathcal{X}|,|\mathcal{Y}|\}$; hence a maximal common partitioning exists. To prove uniqueness, suppose that $(\mathcal{X}_i,\mathcal{Y}_i)_{i=1}^t$ and $(\mathcal{X}'_i,\mathcal{Y}'_i)_{i=1}^t$ are two maximal common partitionings. If they are not equivalent, then there must exist some subset, say $\mathcal{X}_{i_0}$ such that $\mathcal{X}_{i_0}\subset\cup_{\lambda=1}^K\mathcal{X}'_\lambda$ in which $\mathcal{X}_{i_0}\cap\mathcal{X}'_\lambda\neq\emptyset$ for $\lambda=1,\cdots,K\geqslant 2$. Choose any such $\mathcal{X}'_{\lambda_0}$ from this collection and define the new sets $R_{i_0}=\mathcal{X}_{i_0}\cap\mathcal{X}'_{\lambda_0}$ and $\tilde{R}_{i_0}=\mathcal{X}_{i_0}\setminus\mathcal{X}'_{\lambda_0}$, which are both nonempty since $k\geqslant 2$ and the $\mathcal{X}_\lambda$ are disjoint. However, we also have the properties

$$\begin{aligned} &x\in\mathcal{X}_{i_0}\Rightarrow p(\mathcal{Y}_{i_0}|x)=1; && x\in\mathcal{X}'_{\lambda_0}\Rightarrow p(\mathcal{Y}'_{\lambda_0}|x)=1;\\ &x\notin\mathcal{X}_{i_0}\Rightarrow p(\mathcal{Y}_{i_0}|x)=0; && x\notin\mathcal{X}'_{\lambda_0}\Rightarrow p(\mathcal{Y}'_{\lambda_0}|x)=0. \end{aligned}$$

(Here we are implicitly using condition (iii) in the above definition by assuming that $p(x)>0$ thereby defining conditional distributions). Therefore, $p(S_{i_0}|R_{i_0})=p(\tilde{S}_{i_0}|\tilde{R}_{i_0})=1$ and $p(S_{i_0}|\tilde{R}_{i_0})=p(\tilde{S}_{i_0}|R_{i_0})=0$, where $S_{i_0}=\mathcal{Y}_{i_0}\cap\mathcal{Y}'_{\lambda_0}$ and $\tilde{S}_{i_0}=\mathcal{Y}_{i_0}\setminus\mathcal{Y}'_{\lambda_0}$. A similar argument shows that $p(R_{i_0}|S_{i_0})=p(\tilde{R}_{i_0}|\tilde{S}_{i_0})=1$ and $p(R_{i_0}|\tilde{S}_{i_0})=p(\tilde{R}_{i_0}|S_{i_0})=0$. Hence, $(\mathcal{X}_i,\mathcal{Y}_i)_{i\neq i_0}^t\bigcup(S_{i_0},R_{i_0})\bigcup(\tilde{S}_{i_0},\tilde{R}_{i_0})$ is a common partitioning of length $t+1$. But this is a contradiction since $(\mathcal{X}_i,\mathcal{Y}_i)_{i=1}^t$ is a maximal common decomposition.

(b) Suppose that K satisfies $0=H(K|X)=H(K|Y)$ so that $K=f(X)=g(Y)$ for some functions f and g. It is clear that f and g must be constant-valued for any pair of values taken from same block $\mathcal{X}_i\times\mathcal{Y}_i$ in the maximal common partitioning of XY. Hence the maximum possible entropy of K is then attained iff f and g take on a different value for each block in this partitioning.

(c) Suppose that C is not a function of J_{XY}. Then $H(CJ_{XY})>H(J_{XY})$, which contradicts the maximality of J_{XY}. ■

6.2 Proof of Theorem 1

Proof. **Achievability:** We will prove that $H(J_{XY}|Z)$ is an achievable rate without any auxiliary shared public randomness (i.e. W is constant). For n copies of p_{XYZ}, Alice and Bob extract their common information from each copy of p_{XYZ}. This will generate a sequence of J_{XY}^n, with Alice and Bob having identical copies of this sequence. It is now a matter of performing privacy amplification on this sequence to remove Eve's information [2]. The main construction is guaranteed to exist by the following lemma.

Lemma 3 (See Corollary 17.5 in [5]). *For an i.i.d. source of two random variables J_{XY} and Z with J_{XY} ranging over set $\mathcal{J}$, for any $\delta > 0$ and $k < 2^{n[H(J_{XY}|Z)-\delta]}$, there exists an $\epsilon > 0$ and a mapping $\kappa : \mathcal{J}^n \to \mathcal{K} = \{1, 2, \cdots, k\}$ such that*

$$\log |\mathcal{K}| - H(\kappa(J_{XY}^n)|Z^n) < 2^{-n\epsilon}.$$

From this lemma, it follows that $H(J_{XY}|Z)$ is an achievable key rate.

Converse: The converse proof follows analogously to the converse proof of Theorem 2.6 in Ref. [4] (see also [5]). We will first prove the converse under the assumption of no local randomness (i.e. Q_A and Q_B are constant). We will then show that adding local randomness does not change the result. Suppose that $K^{c.r.}(X : Y|Z) = R$. We consider a slightly weaker security condition than the one presented in Sect. 2. This is done by replacing (ii) with (ii'): $\frac{1}{n}(\log |\mathcal{K}| - H(K|Z^nW)) < \epsilon$. Under this weaker assumption, we can assume without loss of generality that K is a function of (X^n, Q_A, W); i.e. $K = f(X^n, Q_A, W)$ [5]. Then, for every $\delta, \epsilon > 0$ and n sufficiently large, there exists a random variable W independent of $X^nY^nZ^n$ along with functions $f(X^n, W)$ and $g(Y^n, W)$ satisfying (i) $Pr[f = g = K] > 1 - \epsilon$, (ii') $\frac{1}{n}(\log |\mathcal{K}| - H(K|Z^nW)) < \epsilon$ and (iii) $\frac{1}{n} \log |\mathcal{K}| \geqslant R$.

Note that from (i) in the security condition, Fano's Inequality together with data processing gives

$$H(K|Y^nW) < h(\epsilon) + \epsilon(\log |\mathcal{K}| - 1). \tag{17}$$

Combining this with (ii') gives

$$\frac{1}{n}(1 - \epsilon) \log |\mathcal{K}| < \frac{1}{n}[H(K|Z^nW) - H(K|Y^nW) + h(\epsilon) - \epsilon],$$

and so

$$R \leqslant \frac{1}{n} \log |\mathcal{K}| + \delta < \frac{1}{1-\epsilon} \cdot \frac{1}{n}[H(K|Z^nW) - H(K|Y^nW)] + \frac{h(\epsilon) - \epsilon}{1 - \epsilon} \cdot \frac{1}{n} + \delta. \tag{18}$$

To analyze the quantity $H(K|Z^nW) - H(K|Y^nW)$, we will use a standard trick.

Lemma 4. *Let J be uniformly distributed over the set $\{1, \cdots, n\}$ and let $A^{(i)}$ denote the i^{th} instance of A in A^n. Likewise, let $A^{(<i)} = A^{(1)} \cdots A^{(i-1)}$ and*

$A^{(>i)} = A^{(i+1)} \cdots A^{(n)}$ *with* $A^{(<1)} := \emptyset$ *and* $A^{(n+1)} := \emptyset$. *Then for random variables* P *and* Q *and sequences of random variables* A^n, B^n

$$H(P|A^nQ) - H(P|B^nQ) = n[I(P : B^{(J)}|TQ) - I(P : A^{(J)}|TQ)], \tag{19}$$

where $T = JA^{(>J)}B^{(<J)}$

Proof. See, e.g., proof of Lemma 17.12 in [5].

Then we can use Lemma 4 to obtain

$$H(K|Z^nW) - H(K|Y^nW) = n[I(K : Y^{(J)}|UW) - I(K : Z^{(J)}|UW)], \tag{20}$$

where $U := JY^{(<J)}Z^{(>J)}$. Notice that for any $i \in \{1, \cdots, n\}$ we have

$$X^{(<i)}X^{(>i)}Y^{(<i)}Z^{(>i)} - X^{(i)} - Y^{(i)}Z^{(i)}, \tag{21}$$

since the sampling is i.i.d.. Therefore, because K is a function of (X^n, W), we have $KU - X^{(J)}W - Y^{(J)}Z^{(J)}$. Removing the superscript "J" and taking $\epsilon, \delta \to 0$, we have the bound

$$R \leqslant I(K : Y|UW) - I(K : Z|UW) \tag{22}$$

such that $KU - XW - YZ$.

Next, Eq. (17) gives

$$\begin{aligned} h(\epsilon) + \epsilon(\log|\mathcal{K}| - 1) &> H(K|Y^nW) - H(K|X^nW) \\ &= n[I(K : X^{(J)}|JY^{(<J)}X^{(>J)}W) - I(K : Y^{(J)}|JY^{(<J)}X^{(>J)}W)], \end{aligned}$$

where the first inequality follows because $H(K|X^nW)$ is nonnegative and the equality follows from Lemma 4. We want to put this in terms of U. To do this, note that

$$\begin{aligned} &I(K : X^{(J)}|JY^{(<J)}X^{(>J)}W) \\ &\quad = I(KY^{(<J)}X^{(>J)} : X^{(J)}|JW) \\ &\quad = I(KY^{(<J)}X^{(>J)}Z^{(>J)} : X^{(J)}|JW) - I(Z^{(>J)} : X^{(J)}|JKY^{(<J)}X^{(>J)}W) \\ &\quad = I(KUX^{(>J)} : X^{(J)}|JW) = I(KU : X^{(J)}|JW) + I(X^{(>J)} : X^{(J)}|KUW), \end{aligned}$$

where the first equality follows from the chain rule and $I(Y^{(<J)}X^{(>J)} : X^{(J)}$ $JW) = 0$, and in the second equality

$$\begin{aligned} I(Z^{(>J)} : X^{(J)}|JKY^{(<J)}X^{(>J)}W) &\leqslant I(Z^{(>J)} : KX^{(J)}|JY^{(<J)}X^{(>J)}W) \\ &= I(Z^{(>J)} : X^{(J)}|JY^{(<J)}X^{(>J)}W) = 0. \end{aligned}$$

Here we use $I(Z^{(>J)} : K|JY^{(<J)}X^{(\geqslant J)}W) = 0$ since $K - JY^{(<J)}X^{(\geqslant J)}W - Z^{(>J)}$ is a Markov chain. Again this follows from the basic Markov condition

$K - WX^n - Y^nZ^n$ and the sampling is i.i.d.. The second equality follows from i.i.d. sampling and W independence of X^n, Y^n, Z^n.

A similar analysis likewise gives

$$\begin{aligned} I(K : Y^{(J)}|JY^{(<J)}X^{(>J)}W) &= I(KU : Y^{(J)}|JW) + I(X^{(>J)} : Y^{(J)}|KUW) \\ &\leqslant I(KU : Y^{(J)}|JW) + I(X^{(>J)} : X^{(J)}|KUW), \end{aligned}$$

where the inequality follows from the Markov condition

$$X^{(>J)} - KUX^{(J)}W - Y^{(J)},$$

a consequence of the more obvious condition $KUX^n - JX^{(J)}W - Y^{(J)}$. Putting everything together yields

$$\begin{aligned} &h(\epsilon) + \epsilon(\log|\mathcal{K}| - 1) \\ &> I(KU : X^{(J)}|JW) - I(KU : Y^{(J)}|JW) \\ &= I(KU : X^{(J)}Y^{(J)}|JW) - I(KU : Y^{(J)}|JX^{(J)}W) - I(KU : Y^{(J)}|JW) \quad (23) \\ &= I(KU : X^{(J)}|JY^{(J)}W) + I(KU : Z^{(J)}|JY^{(J)}X^{(J)}W) \quad (24) \\ &= I(KU : X^{(J)}Z^{(J)}|JY^{(J)}W), \end{aligned}$$

where the second term in Eq. (23) is zero from the already proven Markov chain $KU - XW - YZ$, and in Eq. (24) we use the fact that $I(KU : Z^{(J)}|JY^{(J)}X^{(J)}W) = 0$. Removing the superscript "J" and taking $\epsilon \to 0$ necessitates the Markov chain $KU - YW - XZ$.

It is easy to verify that the double Markov chain $K-XW-Y$ and $K-YW-X$ implies that $I(K : XY|J_{XY}W) = 0$ (see Exercise 16.25 in [5]). Since K is a function of (X, W), we have that $H(K|J_{XY}W) = 0$. Thus, K must also be a function of (Y, W). Continuing Eq. (22) gives the bound

$$\begin{aligned} R \leqslant I(K : Y|UW) - I(K : Z|UW) &= H(K|UW) - I(K : Z|UW) \\ &= H(K|ZUW) \leqslant H(K|ZW). \end{aligned} \quad (25)$$

We have therefore obtained the following:

$$R \leqslant \max H(K|ZW), \quad (26)$$

where the maximization is taken over all variables K such that $H(K|XW) = H(K|YW) = 0$.

This can be further bounded by using the following proposition.

Proposition 4. *If W is independent of XY and $H(K|XW) = H(K|YW) = 0$, then K is a function of (J_{XY}, W).*

Proof. The fact that $H(K|XW) = H(K|YW) = 0$ implies the existence of two functions $f(X, W)$ and $g(Y, W)$ such that $Pr[f(X, W) = g(Y, W)] = 1$. Consequently, if $p(x_1, y_1)p(x_1, y_2) > 0$, then $f(x_1, w) = g(y_1, w) = g(y_2, w)$ for all

$w \in \mathcal{W}$ with $p(w) > 0$. Indeed, if, say, $f(x_1, w) \neq g(y_1, w)$, then $Pr[f(X, W) \neq g(Y, W)] \geqslant p(x_1, y_1, w) = p(x_1, y_2)p(w) > 0$, where we have used the independence between XY and W. By the same reasoning, $p(x_1, y_1)p(y_1, x_2) > 0$ implies that $f(x_1, w) = f(x_2, w) = g(y_1, w)$ for all $w \in \mathcal{W}$. Turning to Proposition 2, if $J_{XY}(x) = J_{XY}(x')$, then there exists a sequence $xy_1x_1y_2x_2 \cdots y_nx'$ such that $p(xy_1)p(y_1x_1)p(x_1y_2) \cdots p(y_nx') > 0$. Therefore, as just argued, we must have that $f(x, w) = f(x', w)$ for all $w \in \mathcal{W}$. Hence K must be a function of (J_{XY}, W).

We now apply Proposition 4 to Eq. (26). Suppose that K obtains the maximization in Eq. (26). Then, since K is a function of (J_{XY}, W), we have that

$$H(K|ZW) \leqslant H(J_{XY}W|ZW) = H(J_{XY}|ZW) \leqslant H(J_{XY}|Z). \tag{27}$$

This proves the desired upper bound under no local randomness.

To consider the case when Alice and Bob have local randomness Q_A and Q_B, respectively, define $\hat{X} := (X, Q_A)$ and $\hat{Y} := (Y, Q_B)$. Then repeating the above argument shows that $R \leqslant H(J_{\hat{X}\hat{Y}}|Z)$. It is straightforward to show that with Q_A and Q_B pairwise independent and independent of XY, we have $J_{\overline{X},\overline{Y}} = J_{XY}$. ■

References

1. Ahlswede, R., Csiszár, I.: Common randomness in information theory and cryptography. i. secret sharing. IEEE Trans. Inf. Theory 39(4), 1121–1132 (1993)
2. Bennett, C., Brassard, G., Crepeau, C., Maurer, U.: Generalized privacy amplification. IEEE Trans. Inf. Theory **41**(6), 1915–1923 (1995)
3. Christandl, M., Renner, R., Wolf, S.: A property of the intrinsic mutual information. In: Proceedings of the IEEE International Symposium on Information Theory 2003, pp. 258–258, June 2003
4. Csiszár, I., Narayan, P.: Common randomness and secret key generation with a helper. IEEE Trans. Inf. Theory **46**(2), 344–366 (2000)
5. Csiszár, I., Körner, J.: Information Theory: Coding Theorems for Discrete Memoryless Systems. Cambridge University Press, Cambridge (2011)
6. Gács, P., Körner, J.: Common information is far less than mutual information. Probl. Control Inf. Theory **2**(2), 149 (1973)
7. Gohari, A., Anantharam, V.: Information-theoretic key agreement of multiple terminals; part i. IEEE Trans. Inf. Theory **56**(8), 3973–3996 (2010)
8. Maurer, U.: Secret key agreement by public discussion from common information. IEEE Trans. Inf. Theory **39**(3), 733–742 (1993)
9. Maurer, U., Wolf, S.: Unconditionally secure key agreement and the intrinsic conditional information. IEEE Trans. Inf. Theory **45**(2), 499–514 (1999)
10. Ozols, M., Smith, G., Smolin, J.A.: Bound entangled states with a private key and their classical counterpart. Phys. Rev. Lett. **112**, 110502 (2014)
11. Renner, R., Wolf, S.: New bounds in secret-key agreement: the gap between formation and secrecy extraction. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 562–577. Springer, Heidelberg (2003)