Max-Planck-Institut für Mathematik in den Naturwissenschaften Leipzig

Unique Information and Secret Key Decompositions

by

Johannes Rauh, Pradeep Kumar Banerjee, Eckehard Olbrich, and Jürgen Jost

Preprint no.: 104 2019

Unique Information and Secret Key Decompositions

Johannes Rauh*, Pradeep Kr. Banerjee*, Eckehard Olbrich and Jürgen Jost
Max Planck Institute for Mathematics in the Sciences, Leipzig, Germany
Email: {jrauh,pradeep,olbrich,jjost}@mis.mpg.de

Abstract

The *unique information* (UI) is an information measure that quantifies a deviation from the Blackwell order. We have recently shown that this quantity is an upper bound on the *one-way secret key rate*. In this paper, we prove a triangle inequality for the UI, which implies that the UI is never greater than one of the best known upper bounds on the *two-way secret key rate*. We conjecture that the UI lower bounds the two-way rate and discuss implications of the conjecture.

Index Terms

Unique information, secret key rate, Blackwell order, less noisy order.

CONTENTS

I. INTRODUCTION

We consider the well-known *source model* for secret key agreement [1], [2]: Alice, Bob and an adversary Eve observe n i.i.d. copies of random variables S, Y and Z resp., where (S, Y, Z) is distributed according to some joint distribution known to all parties. Alice and Bob wish to agree on a common secret key, by publicly communicating messages over an authenticated and noiseless channel transparent to Eve.

A *two-way* public communication protocol proceeds in rounds, where Alice and Bob exchange messages in alternating order, with Alice sending messages in the odd rounds and Bob in the even rounds. Each message is a function of the sender's observation and all the messages exchanged so far. At the end of the protocol, Alice (resp., Bob) computes a key K (resp., K') as a function of S^n (resp., Y^n) and C, the set of all exchanged messages.

Definition 1 ([1])**.** *The* two-way secret key rate*, denoted $S_{\leftrightarrow}(S;Y|Z)$, is the maximum rate R such that for every $\epsilon > 0$, and for sufficiently large n, there exists a public communication protocol such that K and K' (ranging over some common set $\mathcal{K}$) agree with probability at least $1-\epsilon$, satisfying*

$$\tfrac{1}{n}H(K) > \tfrac{1}{n}\log|\mathcal{K}| - \epsilon, \quad \tfrac{1}{n}I(K;C,Z^n) \leq \epsilon, \tag{1}$$

and achieving $\frac{1}{n}H(K) \geq R - \epsilon$.

(1) ensures that the key is almost uniformly distributed and that the *rate* at which Eve learns information about the key is negligibly small. A still stronger definition requires that Eve's *total* information about the key is negligibly small. For the source model, both these definitions give the same secret key rates [3]. We refer [4, Section 17.3] for a review.

The protocol is *one-way* if there is only one round of communication from Alice to Bob. The corresponding key rate is called the *one-way secret key rate* $S_{\rightarrow}(S;Y|Z)$. The one-way secret key rate is a lower bound on the two-way secret key rate. The former can be expressed as an optimization problem over Markov kernels of bounded size [5], [6]. In contrast,

*The first two authors contributed equally to this work.

no algorithm to compute the two-way key rate is known, and its value is known only for a handful of distributions [6]–[9]. Computing the two-way rate is a fundamental and open area of inquiry in information-theoretic cryptography.

The state-of-the-art upper bounds on the two-way key rate rely on the following key observation [7], [10]: Let $s = S_{\leftrightarrow}(S;Y|Z)$. Imagine a fourth party Charlie who observes i.i.d. copies of a correlated random variable Z'. If we decompose s into two parts: a part s_1 which Charlie does not know, and a part $s_2 = s - s_1$ which Charlie knows about the secret key shared between S and Y w.r.t. Z, then s_1 is at most $S_{\leftrightarrow}(S;Y|Z')$, while s_2 is at most $S_{\rightarrow}(SY;Z'|Z)$. Thus, for any (S,Y,Z,Z'), the secret key rate satisfies the following property [7, Theorem 4].

$$S_{\leftrightarrow}(S;Y|Z) \leq S_{\leftrightarrow}(S;Y|Z') + S_{\rightarrow}(SY;Z'|Z)\,. \tag{2}$$

For any $(S,Y,Z,Z') \sim P$, if the induced channel $P_{Z|SY}$ dominates the channel $P_{Z'|SY}$ in the *less noisy* sense [11], then the second term $S_{\rightarrow}(SY;Z'|Z)$ vanishes. One can thus interpret the second term in (2) as quantifying a deviation from the less noisy order when we replace $P_{Z|SY}$ with $P_{Z'|SY}$ [12].

The secret key rates are similar in spirit to an information theoretic quantity UI, called *unique information*, first proposed in [13]. The value $UI(S;Y\backslash Z)$ is interpreted as the *information about S known to Y, but unknown to Z*. The definition of UI is motivated by the idea that unique information should be *useful*. In [13] this is formalized in terms of decision problems: whenever $UI(S;Y\backslash Z) > 0$, there is a decision problem in which it is better to know Y than to know Z. A second ingredient is the goal to not only measure some aspect of information, but also to define an information decomposition, in the sense of [14], that is,

$$SI(S;Y,Z) = I(S;Y) - UI(S;Y\backslash Z) \tag{3}$$

is nonnegative and can be interpreted as the information about S *shared* between Y and Z, and

$$CI(S;Y,Z) = I(S;Y|Z) - UI(S;Y\backslash Z) \tag{4}$$

is nonnegative and can be interpreted as *synergistic* (or *complementary*) information about S. One can thus interpret the unique information as either the mutual information without the shared information, or as the conditional mutual information without the synergistic information.

The key rates can be described in a similar manner as *information common to S and Y that is unique w.r.t. Z*. Also it is clear by definition in which sense positive values of the key rates are useful. Thus it is natural to ask how the two concepts are related. By studying this question we hope to further both the understanding of the secret key rates and the understanding of information decompositions: in fact, the function UI has been criticized amongst other things for vanishing too often. For example, $UI(S;Y\backslash Z) = 0$ whenever the marginals (S,Y) and (S,Z) are identically distributed. The two-way key rate can still be positive in such a situation (see e.g., [8], [15]).

In [15], we have recently shown that UI is an upper bound on the one-way secret key rate. We have also shown that neither the one-way nor the two-way key rate directly fits into the information decomposition framework, as it violates a so-called consistency condition, but we presented a simple construction to enforce the consistency condition and nevertheless derive an information decomposition.

In this paper, we prove a triangle inequality for the UI which implies the following property that resembles (2): For any (S,Y,Z,Z'),

$$UI(S;Y\backslash Z) \leq UI(S;Y\backslash Z') + UI(SY;Z'\backslash Z). \tag{5}$$

From (5) we conclude that $UI \leq B_1$, where B_1 is one of the best known upper bounds on $S_{\leftrightarrow}$. We conjecture that the UI lower bounds the two-way key rate and discuss implications of the conjecture.

II. The Unique Information and its Properties

For some finite state spaces $\mathcal{S},\mathcal{Y},\mathcal{Z}$, let $\mathbb{P}_{\mathcal{S}\times\mathcal{Y}\times\mathcal{Z}}$ be the set of all joint distributions of (S,Y,Z). Given $P \in \mathbb{P}_{\mathcal{S}\times\mathcal{Y}\times\mathcal{Z}}$, let

$$\Delta_{P(S,Y,Z)} := \left\{Q \in \mathbb{P}_{\mathcal{S}\times\mathcal{Y}\times\mathcal{Z}} \colon Q_{SY}(s,y) = P_{SY}(s,y),\ Q_{SZ}(s,z) = P_{SZ}(s,z)\right\} \tag{6}$$

be the set of joint distributions of (S,Y,Z) that have the same marginals on (S,Y) and (S,Z) as P. For brevity, we sometimes write $\Delta_{P(S,Y,Z)} \equiv \Delta_P$. [13] define the unique information that Y conveys about S w.r.t. Z as

$$UI(S;Y\backslash Z) := \min_{Q\in\Delta_{P(S,Y,Z)}} I_Q(S;Y|Z), \tag{7}$$

where the subscript Q in I_Q denotes the joint distribution on which the mutual information I is computed. Since Δ_P is compact and I_Q is continuous in Q, the minimum exists. Δ_P is a convex polytope of dimension $|\mathcal{S}|(|\mathcal{Y}|-1)(|\mathcal{Z}|-1)$, and the optimization problem (7) is a convex program [13], actually a convex cone program [16]. An algorithm to compute the UI has been proposed in [17][1].

[1]Link to source code is available at https://github.com/infodeco/computeUI.

The function UI satisfies the following consistency condition, which implies that SI and CI (defined in (3) and (4)) are symmetric in Y, Z [13].

P.1 (*Consistency condition*).

$$I(S;Y) + UI(S;Z\backslash Y) = I(S;Z) + UI(S;Y\backslash Z). \tag{8}$$

UI also satisfies the following intuitive property.

P.2 (*Blackwell property*). For $(S,Y,Z) \sim P$, write $Z \succeq_S Y$ if there exists a random variable Y' such that $S - Z - Y'$ is a Markov chain and $P_{SY'} = P_{SY}$. Then $UI(S;Y\backslash Z)$ vanishes if and only if $Z \succeq_S Y$ [13, Lemma 6].

Blackwell's theorem [18], [19] implies that this property is equivalent to the fact that decision problems can be solved using Z at least as well as with Y. We call $\succeq_S$ the *Blackwell order* (also called the degradation order). The UI then quantifies a deviation from the Blackwell order.

A. Monotonicity properties of the unique information

In this section, we review basic properties that the function UI shares with the two-way secret key rate. We first note the following trivial bounds [13].

$$I(S;Y) - I(S;Z) \leq UI(S;Y\backslash Z) \leq \min\{I(S;Y), I(S;Y|Z)\}. \tag{9}$$

These bounds match the trivial bounds on the two-way secret key rate [2] (note that $S_{\leftrightarrow}(S;Y|Z)$ is symmetric under permutations of S, Y, while $UI(S;Y\backslash Z)$ is not):

$$\max\{I(S;Y) - I(S;Z), I(Y;S) - I(Y;Z)\} \leq S_{\leftrightarrow}(S;Y|Z) \leq \min\{I(S;Y), I(S;Y|Z)\}. \tag{10}$$

In a secret key agreement task, if either Eve has less information about S than Bob or, by symmetry, less information about Y than Alice, then Alice and Bob can exploit this difference to extract a secret key.

In [15], we proved the following properties of the UI.

P.3 (*Monotonicity under local operations of Alice and Bob*). For all (S,S',Y,Z) such that YZ–S–S' is a Markov chain, $UI(S;Y\backslash Z) \geq UI(S';Y\backslash Z)$ (and likewise for local operations on Y).

P.4 (*Monotonicity under public communication by Alice*). For all (S,Y,Z) and functions f over the support of S,

$$UI((S,f(S));(Y,f(S))\backslash(Z,f(S))) \leq UI(S;Y\backslash Z).$$

P.5 (*Normalization*). For a perfect secret bit $P_{SSZ}(0,0|z) = P_{SSZ}(1,1|z) = \frac{1}{2}$, $UI(S;S\backslash Z) = 1$.

P.6 (*Additivity on tensor products*). For n i.i.d. copies of $(S,Y,Z) \sim P$, $UI(S^n;Y^n\backslash Z^n) = n \cdot UI(S;Y\backslash Z)$.

P.7 (*Asymptotic continuity*). For any $P, P' \in \mathbb{P}_{\mathcal{S}\times\mathcal{Y}\times\mathcal{Z}}$, and $\epsilon \in [0,1]$, if $\|P - P'\|_1 = \epsilon$, then

$$UI_{P'}(S;Y\backslash Z) - UI_P(S;Y\backslash Z) \leq \zeta(\epsilon) + 5\epsilon \log \min\{|\mathcal{S}|, |\mathcal{Y}|\}$$

for some bounded, continuous function $\zeta : [0,1] \to \mathbb{R}_+$ such that $\zeta(0) = 0$.

B. A triangle inequality for the unique information

In this section, we prove the following triangle inequality.

Proposition 2. *For any* (S,Y,Z,Z'), $UI(S;Y\backslash Z) \leq UI(S;Y\backslash Z') + UI(S;Z'\backslash Z)$.

To prove Proposition 2, we need the following monotonicity property of the function UI that is proved in the appendix.

P.8 (*Monotonicity under local operations of Eve*). For all (S,Y,Z,Z') such that SY–Z–Z' is a Markov chain, $UI(S;Y\backslash Z) \leq UI(S;Y\backslash Z')$.

For the special case when Z' is a deterministic function of Z, Property **P.8** was shown in [20].

One can gain an intuitive understanding of Proposition (2) by iterating the basic information decomposition idea as follows. In the presence of a fourth variable Z', we would like to decompose $u := UI(S;Y\backslash Z)$ into two parts: a part u_1, which Z' also knows, and the remainder $u_2 = u - u_1$, which Z' does not know. Clearly, u_1 should be upper bounded by $UI(S;Z'\backslash Z)$ since Z' alone knows what Z' and Y share. Furthermore, $u_2 \leq UI(S;Y\backslash Z')$ since what neither Z nor Z' knows is less than what Z' does not know. In total this gives a heuristic argument why the triangle inequality should hold.

Proof. Let $(S,Y,Z,Z') \sim P$. We use the following notation: For $A, B \subseteq \{Y,Z,Z'\}$, $\Delta_{P(S,A,B)}$ is the set of all joint distributions of (S,A,B) that have the same marginals on the pairs (S,A) and (S,B) as P.

Let $Q^* \in \arg\min_{Q\in\Delta_{P(S,Z',Z)}} I(S;Z'|Z)$. Extend Q^* to a distribution of S,Y,Z',Z via

$$Q^*(s,y,z',z) = Q^*(s,z',z)P(y|s,z') \text{ if } P(s,z') > 0,$$

and $Q^*(s,y,z',z)=0$ otherwise. Then $Q^*(S,Y,Z')=P(S,Y,Z')$ and $Q^*(S,Y,Z)\in\Delta_{P(S,Y,Z)}$. Thus,

$$\begin{aligned}\min_{Q\in\Delta_{Q^*(S,Y,Z'Z)}} I(S;YZ'|Z) &\overset{(a)}{=} \min_{Q\in\Delta_{Q^*(S,Y,Z'Z)}} I(S;Z'|Z)+I(S;Y|Z'Z)\\ &\overset{(b)}{=} UI(S;Z'\backslash Z)+\min_{Q\in\Delta_{Q^*(S,Y,Z'Z)}} I_Q(S;Y|Z'Z)\\ &\overset{(c)}{=} UI(S;Z'\backslash Z)+UI_{Q^*}(S;Y\backslash Z'Z)\\ &\overset{(d)}{\leq} UI(S;Z'\backslash Z)+UI_{Q^*}(S;Y\backslash Z')=UI(S;Z'\backslash Z)+UI(S;Y\backslash Z').\end{aligned}$$

(a) follows from the chain rule of mutual information. (b) follows since the (S,Z,Z')-marginal is fixed in $\Delta_{Q^*(S,Y,Z'Z)}$ and by definition of Q^*, $I_{Q^*}(S;Z'|Z)=UI(S;Z'\backslash Z)$. (c) follows because the second minimization in (b) defines $UI_{Q^*}(S;Y\backslash Z'Z)$. Finally, (d) follows from Property **P.8**.

Let $Q^+\in\arg\min_{Q\in\Delta_{Q^*(S,Y,Z'Z)}} I(S;YZ'|Z)$. Then

$$Q^+(S,Y,Z)\in\Delta_{Q^*(S,Y,Z)}=\Delta_{P(S,Y,Z)}.$$

Therefore,

$$\min_{Q\in\Delta_{Q^*(S,YZ',Z)}} I(S;YZ'|Z)=I_{Q^+}(S;YZ'|Z)\geq UI_{Q^+}(S;YZ'\backslash Z)\geq UI_{Q^+}(S;Y\backslash Z)=UI(S;Y\backslash Z),$$

where in the last step we have used Property **P.3** and the fact that $Q^+(S,Y,Z)\in\Delta_{P(S,Y,Z)}$. This completes the proof. ■

From Proposition 2 and Property **P.3** we conclude:

Corollary 3. *For any (S,Y,Z,Z'), $UI(S;Y\backslash Z)\leq UI(S;Y\backslash Z')+UI(SY;Z'\backslash Z)$.*

We can interpret Corollary 3 like inequality (2): Given $(S,Y,Z,Z')\sim P$, if the induced channel $P_{Z|SY}$ dominates the channel $P_{Z'|SY}$ in the Blackwell sense (see Property **P.2**). then the second term $UI(SY;Z'\backslash Z)$ vanishes. One can interpret $UI(SY;Z'\backslash Z)$ as quantifying a deviation from the Blackwell order when we replace $P_{Z|SY}$ with $P_{Z'|SY}$.

III. Bounds on Secret Key Rates

A. An upper bound on the one-way secret key rate

$S_{\rightarrow}$ admits the following characterization.

Theorem 4 ([6, Theorem 1])**.** *The* one-way secret key rate $S_{\rightarrow}(S;Y|Z)$ *for the source model is*

$$S_{\rightarrow}(S;Y|Z)=\max_{P_{UV|SYZ}} I(U;Y|V)-I(U;Z|V)$$

for random variables U, V of bounded cardinalities $|\mathcal{U}|\leq|\mathcal{S}|^2$ and $|\mathcal{V}|\leq|\mathcal{S}|$, such that V–U–S–YZ is a Markov chain.

The bounds on the cardinalities imply that the optimization domain is a set of stochastic matrices of finite size, which makes it possible to turn this theorem into an algorithm to compute $S_{\rightarrow}$.

Like the UI, $S_{\rightarrow}(S;Y|Z)$ depends only on the marginal distributions of the pairs (S,Y) and (S,Z) [6]. Using Properties **P.3** – **P.7** and results about protocol monotones [7], [10], [21], [22], one can show the following:

Theorem 5 ([15, Theorem 37])**.** *$UI(S;Y\backslash Z)$ is an upper bound for the one-way secret key rate $S_{\rightarrow}(S;Y|Z)$.*

B. Known upper bounds on the two-way secret key rate

As noted in (10), a trivial upper bound on $S_{\leftrightarrow}(S;Y|Z)$ is $\min\{I(S;Y),I(S;Y|Z)\}$ [1]. An improved upper bound is given by the *intrinsic information* [2].

$$S_{\leftrightarrow}(S;Y|Z)\leq I(S;Y\downarrow Z):=\min_{P_{Z'|Z}} I(S;Y|Z'),\tag{11}$$

where Z' may be assumed to have a range of size at most $|\mathcal{Z}|$ [23].

[24] noted that the intrinsic information exhibits a property called "locking", i.e., it can drop by an arbitrarily large amount on giving away a bit of information to Eve. In contrast, the two-way rate satisfies

$$S_{\leftrightarrow}(S;Y|ZU)\geq S_{\leftrightarrow}(S;Y|Z)-H(U)\tag{12}$$

for jointly distributed random variables (S,Y,Z,U) [24, Theorem 3], and the conditional mutual information satisfies an analogous property. The same is true for the UI:

P.9 (UI *does not lock*). For jointly distributed random variables (S, Y, Z, U),

$$UI(S;Y\backslash ZU) \geq UI(S;Y\backslash Z) - H(U). \tag{13}$$

The proof of Property **P.9** is in the appendix.

[24] proposed an improved upper bound called the *reduced intrinsic information*, which does not exhibit locking:

$$I(S;Y{\downarrow\downarrow}Z) := \inf_{P_{U|SYZ}} I(S;Y{\downarrow}ZU) + H(U).$$

Property **P.9** implies that $UI(S;Y \setminus Z) \leq I(S;Y{\downarrow\downarrow}Z)$; a fact that will be generalized later in Thereom 7.

The tightest known upper bound on the two-way rate is [7]

$$B_2(S;Y|Z) := \inf_{p_{Z'|SYZ}} I(S;Y|Z') + S_{\rightarrow}(SY;Z'|Z)\,. \tag{14}$$

Unfortunately, B_2 cannot be computed explicitly, as no bound on the size of Z' is known.

A slightly weaker but computable upper bound is given by the *minimum intrinsic information* [7].

$$B_1(S;Y|Z) := \min_{P_{Z'|SYZ}} I(S;Y|Z') + I(SY;Z'|Z), \tag{15}$$

where $|\mathcal{Z}'| \leq |\mathcal{S}||\mathcal{Y}||\mathcal{Z}|$.

C. Unique information based bounds on the two-way rate and a conjecture

We now investigate some properties of the function UI in relation to upper bounds on the two-way rate. We first list the following known chain of bounds on the two-way rate.

$$S_{\rightarrow}(S;Y|Z) \leq S_{\leftrightarrow}(S;Y|Z) \leq B_2(S;Y|Z) \leq B_1(S;Y|Z) \leq I(S;Y{\downarrow\downarrow}Z) \leq I(S;Y{\downarrow}Z) \leq I(S;Y|Z). \tag{16}$$

Corollary 3 implies the following result.

Proposition 6. $UI(S;Y\backslash Z) \leq B_1(S;Y|Z)$.

From Theorem 5 and Proposition 6, we have the following chain of inequalities relating the bounds on the two-way rate.

Theorem 7. $S_{\rightarrow}(S;Y|Z) \leq UI(S;Y\backslash Z) \leq B_1(S;Y|Z) \leq I(S;Y{\downarrow\downarrow}Z) \leq I(S;Y{\downarrow}Z) \leq I(S;Y|Z)$.

Given $(S, Y, Z) \sim P$, let

$$Q^* \in \operatorname*{arg\,min}_{Q \in \Delta_{P(S,Y,Z)}} I_Q(S;Y|Z). \tag{17}$$

The distribution Q^* is called a *minimum synergy* distribution, as $CI(S;Y,Z) = 0$ if and only if $P = Q^*$. By definition, $I_{Q^*}(S;Y|Z) = UI(S;Y\backslash Z)$. An immediate consequence of Theorem 7 is the following: Choosing $P = Q^*$, all known upper bounds on the two-way rate collapse to the UI and the conditional mutual information, respectively.

Examples are known which show that UI is not an upper bound on $S_{\leftrightarrow}$ (see e.g., [15, Example 41], [8, Appendix]). We make the following conjecture.

Conjecture 8. $UI(S;Y\backslash Z) \leq S_{\leftrightarrow}(S;Y|Z)$.

Let us briefly mention why we believe that this conjecture is true. Firstly, while the function $UI(S;Y\backslash Z)$ depends only on the marginals of the pairs (S, Y) and (S, Z), the same is not true for $S_{\leftrightarrow}(S;Y|Z)$ which depends on the full joint distribution of (S, Y, Z). Secondly, unlike $S_{\leftrightarrow}(S;Y|Z)$ which is symmetrical in S and Y, the function UI is asymmetric in all three variables. This asymmetry is manifest, for instance, when we note that $UI(S;Y\backslash Z)$ is not monotone under public communication by Bob.

Remark 9 (Sandwich bound on $S_{\leftrightarrow}(S;Y|Z)$)**.** *If Conjecture 8 is true, then*

$$UI(S;Y\backslash Z) = I_{Q^*}(S;Y|Z) \leq S_{\leftrightarrow}(S;Y|Z) \leq I_P(S;Y|Z). \tag{18}$$

(18) implies that the set of all Q^* as in (17) is a set of distributions for which the UI equals the two-way rate.

A related work [9] gives necessary conditions for when the two-way rate equals the conditional mutual information.

Definition 10. *Define the following functions on $\mathbb{P}_{\mathcal{S}\times\mathcal{Y}\times\mathcal{Z}}$.*

$$B_{sUI}(S;Y|Z) := \inf_{P_{Z'|SYZ}} UI(S;Y\backslash Z') + UI(SY;Z'\backslash Z).$$

$$B_{gUI}(S;Y|Z) := \inf_{P_{Z'|SYZ}} I(S;Y|Z') + UI(SY;Z'\backslash Z).$$

As the following proposition shows, $B_{gUI}(S;Y|Z)$ is a new upper bound on the two-way rate which is juxtaposed between the two best known bounds B_2 and B_1.

Proposition 11.

$$B_{sUI}(S;Y|Z) = UI(S;Y\backslash Z) \leq B_{gUI}(S;Y|Z) \tag{19}$$
$$B_2(S;Y|Z) \leq B_{gUI}(S;Y|Z) \leq B_1(S;Y|Z) \tag{20}$$

Proof. The left equality in (19) follows from Corollary 3 and

$$B_{sUI}(S;Y|Z) = \inf_{P_{Z'|SYZ}} UI(S;Y\backslash Z') + UI(SY;Z'\backslash Z) \leq \inf_{P_{Z'|Z}:SY-Z-Z'} UI(S;Y\backslash Z') = UI(S;Y\backslash Z),$$

where the last equality uses Property **P.8**. The right inequality in (19) follows from Corollary 3 and from $UI(S;Y\backslash Z') \leq I(S;Y|Z')$.

Statement (20) follows from Theorem 5 by noting that $S_{\rightarrow}(SY;Z'|Z) \leq UI(SY;Z'\backslash Z) \leq I(SY;Z'|Z)$. ■

IV. Conclusion

We showed a triangle inequality for the unique information which implies that the UI is never greater than one of the best known upper bounds on the two-way secret key rate. We conjecture that the UI is indeed a lower bound on the two-way rate. Assuming that the conjecture is true, we characterized a set of distributions for which the two-way rate equals the conditional mutual information and the UI. This provides an operational characterization of the UI.

Appendix

*Proof of Property **P.8**.* Let $(S,Y,Z) \sim P$ and $(S,Y,Z,Z') \sim P'$. By definition, P is a marginal of P'. Let $Q \in \Delta_{P(S,Y,Z)}$, and let $Q'(s,y,z,z') = Q(s,y,z)P'(z'|s,z)$ if $P(s,z) > 0$ and $Q'(s,y,z,z') = 0$ otherwise. Then $Q' \in \Delta_{P'(S,Y,ZZ')}$. Moreover, Q is the (S,Y,Z)-marginal of Q', and Y–SZ–Z' is a Markov chain w.r.t. Q' by construction. Therefore,

$$\begin{aligned} I_{Q'}(S;Y|ZZ') &= I_{Q'}(SZ';Y|Z) - I_{Q'}(Z';Y|Z) \\ &\leq I_{Q'}(SZ';Y|Z) = I_{Q'}(S;Y|Z) + I_{Q'}(Z';Y|SZ) = I_{Q'}(S;Y|Z) = I_Q(S;Y|Z). \end{aligned}$$

Taking the minimum over $Q \in \Delta_{P(S,Y,Z)}$, we conclude that

$$UI(S;Y\backslash Z,Z') \leq UI(S;Y\backslash Z). \tag{21}$$

If SY–Z–Z' is a Markov chain by assumption, then

$$\begin{aligned} UI(S;Y\backslash Z,Z') &= \min_{Q' \in \Delta_{P'(S,Y,ZZ')}} I_{Q'}(S;Y|ZZ') \\ &\overset{(a)}{=} \min_{Q' \in \Delta_{P'(S,Y,ZZ')}} I_{Q'}(S;Y|Z) - I_{Q'}(S;Z'|Z) + I_{Q'}(S;Z'|ZY) \\ &\overset{(b)}{\geq} \min_{Q' \in \Delta_{P'(S,Y,ZZ')}} I_{Q'}(S;Y|Z) \\ &\overset{(c)}{\geq} \min_{Q \in \Delta_{P(S,Y,Z)}} I_Q(S;Y|Z) = UI(S;Y\backslash Z), \end{aligned} \tag{22}$$

where (a) follows from the chain rule of mutual information, (b) follows since SY–Z–Z' w.r.t. P' implies $I_{Q'}(S;Z'|Z) = 0$, and (c) follows since Q is the (S,Y,Z)-marginal of Q' and $Q' \in \Delta_{P'}$ implies $Q \in \Delta_P$. (21) and (22) together imply $UI(S;Y\backslash Z) = UI(S;Y\backslash Z,Z')$.

Since (21) holds for any (S,Y,Z,Z'), exchanging Z' and Z in (21) gives $UI(S;Y\backslash Z) = UI(S;Y\backslash Z,Z') \leq UI(S;Y\backslash Z')$ which completes the proof. ■

*Proof of Property **P.9**.* Let $(S,Y,Z,U) \sim \widetilde{P}$ and let P be the (S,Y,Z)-marginal of $\widetilde{P}$. Let

$$\widetilde{Q}^* \in \operatorname*{arg\,min}_{\widetilde{Q} \in \Delta_{\widetilde{P}(S,Y,ZU)}} I_{\widetilde{Q}}(S;Y|ZU), \text{ and } Q^* \in \operatorname*{arg\,min}_{Q \in \Delta_{P(S,Y,Z)}} I_Q(S;Y|Z).$$

Then

$$UI(S;Y\backslash ZU) = I_{\widetilde{Q}^*}(S;Y|ZU) \geq I_{\widetilde{Q}^*}(S;Y|Z) - H(U) \geq I_{Q^*}(S;Y|Z) - H(U) = UI(S;Y\backslash Z) - H(U),$$

where in the third step we have used the fact that for any $\widetilde{Q} \in \Delta_{\widetilde{P}}$, the (S,Y,Z)-marginal of $\widetilde{Q}$ lies in Δ_P. ■

REFERENCES

[1] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, 1993.

[2] U. M. Maurer and S. Wolf, "Unconditionally secure key agreement and the intrinsic conditional information," *IEEE Transactions on Information Theory*, vol. 45, no. 2, pp. 499–514, 1999.

[3] ——, "From weak to strong information-theoretic key agreement," in *Proc. IEEE ISIT*, 2000, p. 18.

[4] I. Csiszár and J. Körner, *Information theory: coding theorems for discrete memoryless systems*. Cambridge University Press, 2011.

[5] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[6] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.

[7] A. A. Gohari and V. Anantharam, "Information-theoretic key agreement of multiple terminals: Part I," *IEEE Transactions on Information Theory*, vol. 56, no. 8, pp. 3973–3996, 2010.

[8] ——, "Comments on "Information-theoretic key agreement of multiple terminals–Part I"," *IEEE Transactions on Information Theory*, vol. 63, no. 8, pp. 5440–5442, 2017.

[9] E. Chitambar, B. Fortescue, and M.-H. Hsieh, "Distributions attaining secret key at a rate of the conditional mutual information," in *Annual Cryptology Conference*. Springer, 2015, pp. 443–462.

[10] K. Keykhosravi, M. Mahzoon, A. A. Gohari, and M. R. Aref, "From source model to quantum key distillation: An improved upper bound," in *Proc. IEEE IWCIT*. IEEE, 2014, pp. 1–6.

[11] J. Körner and K. Marton, "Comparison of two noisy channels," in *Topics in information theory*. Keszthely (Hungary): Colloquia Mathematica Societatis Janos Bolyai, 1975, vol. 16, pp. 411–423.

[12] A. A. Gohari, O. Günlü, and G. Kramer, "Coding for positive rate in the source model key agreement problem," *arXiv preprint arXiv:1709.05174*, 2018.

[13] N. Bertschinger, J. Rauh, E. Olbrich, J. Jost, and N. Ay, "Quantifying unique information," *Entropy*, vol. 16, no. 4, pp. 2161–2183, 2014.

[14] P. Williams and R. Beer, "Nonnegative decomposition of multivariate information," *arXiv:1004.2515v1*, 2010.

[15] P. K. Banerjee, E. Olbrich, J. Jost, and J. Rauh, "Unique informations and deficiencies," *arXiv preprint arXiv:1807.05103*, 2018, Allerton 2018 (to appear).

[16] A. Makkeh, D. O. Theis, and R. Vicente, "Bivariate partial information decomposition: The optimization perspective," *Entropy*, vol. 19, no. 10, p. 530, 2017.

[17] P. K. Banerjee, J. Rauh, and G. Montúfar, "Computing the unique information," in *Proc. IEEE ISIT*. IEEE, 2018, pp. 141–145.

[18] D. Blackwell, "Equivalent comparisons of experiments," *The Annals of Mathematical Statistics*, vol. 24, no. 2, pp. 265–272, 1953.

[19] N. Bertschinger and J. Rauh, "The Blackwell relation defines no lattice," in *Proc. IEEE ISIT*. IEEE, 2014, pp. 2479–2483.

[20] J. Rauh, N. Bertschinger, E. Olbrich, and J. Jost, "Reconsidering unique information: Towards a multivariate information decomposition," in *Proc. IEEE ISIT*, 2014, pp. 2232–2236.

[21] U. Maurer, R. Renner, and S. Wolf, "Unbreakable keys from random noise," in *Security with Noisy Data*. Springer, 2007, pp. 21–44.

[22] M. Christandl, A. Ekert, M. Horodecki, P. Horodecki, J. Oppenheim, and R. Renner, "Unifying classical and quantum key distillation," in *Theory of Cryptography Conference*. Springer, 2007, pp. 456–478.

[23] M. Christandl, R. Renner, and S. Wolf, "A property of the intrinsic mutual information," in *Proc. IEEE ISIT*, 2003, pp. 258–258.

[24] R. Renner and S. Wolf, "New bounds in secret-key agreement: The gap between formation and secrecy extraction," in *Advances in Cryptology - EUROCRYPT 2003, Warsaw, Poland*, 2003, pp. 562–577.