New Properties of Intrinsic Information and Their Relation to Bound Secrecy

Andrey Khesin
Department of Mathematics, Massachusetts Institute of Technology,
Cambridge, Massachusetts, 02139, USA

Andrew Tung
Menlo School,
Atherton, California, 94027, USA

Karthik Vedula
James S. Rickards High School
Tallahassee, Florida, 32301, USA

(Dated: January 16, 2023)

Abstract: Two parties, Alice and Bob, seek to generate a mutually agreed upon string of bits, unknown to an eavesdropper Eve, by sampling repeatedly from a joint probability distribution. The secret-key rate has been defined as the asymptotic rate at which Alice and Bob can extract secret bits after sampling many times from the probability distribution. The secret-key rate has been bounded above by two information-theoretic quantities, first by the intrinsic information, and more strongly by the reduced intrinsic information. However, in this paper we prove that the reduced intrinsic information is 0 if and only if the intrinsic information is 0. This result implies that at least one of the following two conjectures is false: either the conjecture of the existence of bound secrecy, distributions where the intrinsic information is positive but the secret-key rate is 0, or the conjecture that the reduced intrinsic information equals the secret-key rate. Furthermore, we introduce a number of promising approaches for showing that bound secrecy does indeed exist using the idea of binarization of random variables. We improve on previous work by giving an explicit construction for a particular candidate for bound secrecy of an information-erasing binarization.

Keywords: information theory, bound secrecy, intrinsic information, secret-key rate

CONTENTS

1. INTRODUCTION

A common problem in classical information theory is achieving secure communication over a public channel. Most modern-day cryptographic protocols rely on computational security, a type of security based on the computational difficulty of solving a certain problem. For example, the RSA protocol, widely used today, is based on the problem of factoring large integers. Unfortunately, the security of these types of protocols is always conditional because it relies on the fact that certain problems are computationally difficult, and that the adversary has limited computational power. Protocols based on information theory avoid this problem because the secrecy that they obtain is impossible for the eavesdropper to pierce, simply due to the laws of probability [4].

To achieve information-theoretic secure communication, most protocols begin with a procedure by which the two parties agree on a secret key. Once this secret key is established, the parties can then encode an arbitrary message with the key completely securely. For example, suppose the secret key is composed of a string of bits. Then the message, in the form of another string of bits, can be perfectly secretly encoded by a one-time pad, which in this case can be performed by bitwise XOR. (Note that although it is perfectly secure, using a secret key as a one-time pad is not very efficient, and one often uses a cryptographic key expansion in cases where the secret key is expensive to generate.)

Unfortunately for Alice and Bob, agreeing on an unconditionally secret key is impossible without a source of secrecy to start with [7, 11]. An example of such secrecy is if Alice and Bob could both observe the same random number generator, whose output is not available to an eavesdropper Eve. In this case, the amount of secrecy Alice and Bob share is simply the entropy of the random number generator, but in more complicated situations (e.g. if the output of the generator is partially known to Eve) secrecy is not as easy to quantify. Quantifying how much secrecy Alice and Bob share in a given situation has been attempted by introducing a number of quantities, such as the *intrinsic information* and the *reduced intrinsic information* [4, 10]. A number of properties of these quantities have been discovered [9, 10], suggesting that they are connected with the original problem of determining whether or not Alice and Bob can agree on a secret key (and if so, how long the key can be). For example, it has been proven that the intrinsic information is an upper bound on Alice and Bob's secret-key rate.

However, some surprising results have shown that there is a gap between these information-theoretic quantities and Alice and Bob's ability to generate a secret key [10]. A number of conjectures of this nature are currently unresolved, including the long-standing conjecture of the existence of bound secrecy. This conjecture has its origins in the analogous quantum phenomenon of bound entanglement, discovered in the late 1990s [3–6, 10]; the existence of bound secrecy was conjectured in the early 2000s. Bound secrecy refers to secrecy (i.e. positive intrinsic information) which cannot be extracted (i.e. the secret-key rate is 0). If bound secrecy exists, it would suggest that classical information theory has surprising connections to quantum information theory, which was, in general, thought to be of a different nature.

In this paper, we make an important step toward proving the existence of bound secrecy by showing that, in the crucial case where either intrinsic information or reduced intrinsic information is 0, there is no gap between the two quantities. This is significant because the original purpose of introducing the reduced intrinsic information was to provide a stronger upper bound on the secret-key rate, and one of the prevailing approaches for constructing an example that has bound secrecy was showing the example has a positive intrinsic information but a reduced intrinsic information of 0 (implying that no secrecy can be extracted). This paper shows that this approach cannot work.

On the other hand, we suggest an alternative approach for establishing the existence of bound secrecy, first mentioned in [4], based on the idea of binarizations. Binarizations are ways of processing a random variable stochastically such that the new random variable has two outputs. We show that the existence of bound secrecy can be reduced to a simple statement about binarizations and probability. Finally, based on the idea of binarizations, we suggest a formula for the binarized secret-key rate which we conjecture is equal to the secret-key rate.

The outline of this paper is as follows. In Section 2, we formally define the secret-key rate, the intrinsic information, and the reduced intrinsic information, which will be important in the rest of the paper. We also give context for our result by summarizing the properties of these quantities which have been established previously. Additionally, we provide the formal statements of a number of important conjectures, such as the problem of bound secrecy, which are addressed in this paper. In Section 3, we state and prove our result, which requires a number of intermediate lemmas. In Section 4, we discuss how our result relates to prior work, showing that given the existence of bound secrecy (which is widely believed to be the case), another long-standing conjecture is false. In Section 5, we discuss another path of establishing bound secrecy using binarizations of Alice's and Bob's random variables. Finally, in Section 6, we improve on previous results by giving an explicit construction of a binarization which erases intrinsic information, which appears easier to generalize than previous non-constructive solutions.

2. BACKGROUND

The setup of the problem is as follows. Let P_{XYZ} be a joint probability distribution of three discrete (but possibly infinite) random variables X, Y, and Z, with Alice receiving X, Bob Y, and Eve Z. Throughout this paper we assume that any probability distribution is discrete and has finite entropy. Entropy is denoted by H and is assumed to be Shannon entropy; as such, all logs are assumed to be base 2.

The *secret-key rate* $S(X:Y||Z)$ is, informally, the rate at which Alice and Bob can extract secret bits from many copies of P_{XYZ}. (The notation suggests the interpretation that the secret-key rate is the amount of information between X and Y given the information in Z). We are interested in the secret-key rate because if it is non-zero, Alice and Bob can extract their secret bits and thereby communicate securely. A formal definition of the secret-key rate, first introduced in [7], is as follows.

Definition 2.1. Suppose Alice and Bob are given N independent realizations of a discrete joint probability distribution P_{XYZ}. Call a protocol *ϵ-safe* if, at the end of the protocol, Alice and Bob can compute secret, correlated random variables S_A and S_B such that there exists another random variable S so that

$$P[S_A = S_B = S] > 1 - \epsilon \text{ and } I(S : CZ^N) < \epsilon.$$

Here, C stands for any communications that took place during the protocol.

The first condition ensures that Alice and Bob's variables must agree with probability very close to 1, so that they share some information. The second condition ensures that this information is not accessible to Eve. This is defined formally using the mutual information $I(X;Y) := H(X) + H(Y) - H(X,Y)$, a measure of the amount of information two random variables share. The condition requires that the mutual information between the pieces of data Eve has (Z^N and the communications C) and the secret variable S must be low.

Using the definition of an ϵ-safe protocol, we define the secret-key rate asymptotically.

Definition 2.2. The *secret-key rate* $S(X:Y||Z)$ is the largest number R such that for all $\epsilon > 0$, there exists an N such that for all $n > N$, there exists an ϵ-safe protocol (using n copies of P_{XYZ} and producing the random variable S) with $\frac{H(S)}{N} \geq R$.

Although the secret-key rate is the quantity we are interested in, as it captures the true number of bits Alice and Bob can extract, it has been hard to deal with because it allows any communication string C, and furthermore, is defined asymptotically. Ideally, one would express the secret-key rate $S(X:Y||Z)$ as a simple function of the distribution P_{XYZ}, but so far no one has been able to figure out how [10]. Instead a number of upper bounds have been found. One of the first upper bounds on the secret-key rate was the conditional mutual information $I(X:Y|Z)$ [8], defined as follows.

Definition 2.3. Given a probability distribution P_{XYZ}, the *conditional mutual information* $I(X:Y|Z)$ is defined as $H(X|Z) + H(Y|Z) - H(XY|Z)$, where each term is a conditional entropy conditioned on Z.

One strategy for Eve to extract information about X and Y is to pass her variable Z through a channel $P_{\overline{Z}|Z}$ [9], which in this case takes the form of a stochastic matrix acting on the vector of probabilities for Z. So we define the intrinsic conditional mutual information, first introduced in [8].

Definition 2.4. Given a probability distribution P_{XYZ}, the *intrinsic conditional mutual information* $I(X : Y \downarrow Z)$, sometimes called the *intrinsic information*, is defined as

$$I(X : Y \downarrow Z) := \inf_{P_{\overline{Z}|Z}} I(X : Y|\overline{Z}).$$

Theorem 2.5. *[8, 10] Given a distribution P_{XYZ}, we have $S(X : Y||Z) \leq I(X : Y \downarrow Z)$. However, there exist distributions with $S(X : Y||Z) \neq I(X : Y \downarrow Z)$.*

Motivated by the fact that $S(X : Y||ZU) \leq S(X : Y||Z) - H(U)$ holds but the corresponding inequality for the intrinsic information does not always hold, Renner and Wolf have introduced the *reduced intrinsic conditional mutual information* [9].

Definition 2.6. [10] Given a distribution P_{XYZ}, the *reduced intrinsic conditional mutual information* $I(X : Y \downarrow\downarrow Z)$, sometimes called the *reduced intrinsic information*, is defined as

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

From the definition, we can see that the intrinsic information is an upper bound on the reduced intrinsic information, by setting U to be trivial. The reduced intrinsic information is bounded from below by the secret-key rate, informally because in the infimum we can let U be the secret bit that Alice and Bob can generate.

Theorem 2.7. *[10] Given a probability distribution P_{XYZ}, $S(X : Y||Z) \leq I(X : Y \downarrow\downarrow Z)$.*

Intuitively, the reduced intrinsic information takes into account the fact that Eve may have the additional disadvantage of not knowing how to process her variable Z. Therefore, the knowledge of how to process Z, as represented by U, can reduce the shared information between X and Y by more than the amount of information in U itself. This means that the reduced intrinsic information is sometimes less than the intrinsic information.

Theorem 2.8. *[9] There exists a discrete distribution P_{XYZ} where $I(X : Y \downarrow Z) \neq I(X : Y \downarrow\downarrow Z)$.*

As the reduced intrinsic information is a strictly stronger bound on the secret-key rate than the intrinsic information, it is natural to ask whether it in fact equals the secret-key rate. This is an open problem.

Conjecture 2.9. [10] Given a probability distribution P_{XYZ}, we have $S(X : Y||Z) = I(X : Y \downarrow\downarrow Z)$.

Whereas previous bounds on S, such as the intrinsic information, have been improved by finding properties that were not shared between those quantities and S, so far the reduced intrinsic information appears to share many properties of the secret-key rate. If the conjecture is proven true (i.e. $S(X : Y||Z) = I(X : Y \downarrow\downarrow Z)$ in all cases), then we would have a relatively simple description, based on only the distribution P_{XYZ}, of the secret-key rate. This would fulfill one of the original objectives. If the conjecture is proven false, then it would reveal another potential strategy for Eve. Another significant conjecture is the problem of bound secrecy, namely secrecy between Alice and Bob that cannot be extracted.

Conjecture 2.10. [4] (Bound secrecy) There exists a distribution P_{XYZ} such that $I(X : Y \downarrow Z) > 0$ but $S(X : Y||Z) = 0$.

This conjecture is inspired by the analogous problem of bound entanglement: there are quantum entangled states (analogous to classically correlated random variables) which have secrecy which cannot be distilled [5]. Relatively strong evidence suggesting the existence of bound secrecy has been found in [4, 10] by drawing connections between the classical and quantum problems. Numerical evidence for bound secrecy has been given in [6]. Conjectures 2.9 and 2.10 are addressed indirectly in this paper.

3. THE GAP BETWEEN THE STANDARD AND REDUCED INTRINSIC INFORMATION

We introduce the main result of this paper.

Theorem 3.1. *Given a probability distribution P_{XYZ}, we have*

$$I(X:Y\downarrow\downarrow Z)=0 \iff I(X:Y\downarrow Z)=0.$$

We first observe that the reverse direction follows because the intrinsic information is an upper bound on the reduced intrinsic information, which is nonnegative. We focus on the forward direction, whose proof takes the remainder of this section.

An important tool in the proof is the notion of the trace distance between two random variables.

Definition 3.2. Let two random variables A and B have probability distributions $\{a_i\}$ and $\{b_i\}$ with the same index set. Then the *trace distance* between A and B, denoted $D(A,B)$ is defined to be

$$D(A,B):=\frac{1}{2}\sum_i |a_i-b_i|.$$

To prove the forward direction of Theorem 3.1, we reason as follows. If $I(X:Y\downarrow\downarrow Z)=0$, then by definition $\inf\limits_{P_{U|XYZ}}(I(X:Y\downarrow ZU)+H(U))=0$. First, suppose that this infimum is a minimum. This means that there exists an $XYZU$ such that $I(X:Y\downarrow ZU)+H(U)=0$, so $H(U)=0$ and $I(X:Y\downarrow ZU)=0$. However, since U adds no information, we have $0=I(X:Y\downarrow ZU)=I(X:Y\downarrow Z)$, which is the desired statement.

From now on, assume that the infimum is not a minimum. This means that both quantities in the sum must progressively approach 0 for a carefully chosen sequence of distributions. More rigorously, there must exist a sequence of probability distributions $\{XYZU_i\}$ such that $\lim\limits_{i\to\infty}H(U_i)=0$ and $\lim\limits_{i\to\infty}I(X:Y\downarrow ZU_i)=0$. Due to the definition of intrinsic information, there must also exist a sequence of channels $\{C_i\}$ such that $\lim\limits_{i\to\infty}I(X:Y|C_i(ZU_i))=0$.

In order to prove that $I(X:Y\downarrow Z)=0$, all that we have to do is show that there exists a sequence of channels $\{c_i\}$ such that $\lim\limits_{i\to\infty}I(X:Y|c_i(Z))=0$. We show this by showing $\{c_i\}=\{C_i\}$ works. In order to do this, we incorporate the defining property of the sequence $\{C_i\}$ by showing that $\lim\limits_{i\to\infty}I(X:Y|C_i(Z))-I(X:Y|C_i(ZU_i))=0$ starting from $\lim\limits_{i\to\infty}H(U_i)=0$. In the rest of the proof, the channels $\{C_i\}$ are denoted using bars, and the value of i will be inferred from context.

We first prove a number of lemmas regarding trace distances (denoted as $D(A,B)$) and entropies. As a convention, let e_1 denote a constant random variable, as represented by a unit vector of probabilities with the first component equal to 1. The size of the range of e_1 is taken to be contextual (i.e. equal to the range of U_i).

Also, we assume that if U_i is a random variable, then the probabilities for each outcome of U_i are ordered in descending order. Observe that such an ordering exists because the sum of all the probabilities is 1 and they are nonnegative, so there can only be finitely many probabilities above any threshold $x\in(0,1)$. Then we can order the probabilities that are above x because there are only finitely many, and then order all the probabilities by repeatedly lowering x.

Proof. Our proof of Theorem 3.1 will go as follows.

$$\begin{aligned}
\lim_{i\to\infty}H(U_i)&=0\\
\implies \lim_{i\to\infty}D(U_i,e_1)&=0\\
\implies \lim_{i\to\infty}D(XYZU_i,XYZe_1)&=0\\
\implies \lim_{i\to\infty}D(XY\overline{ZU_i},XY\overline{Ze_1})&=0\\
\implies \lim_{i\to\infty}I(X;Y|\overline{ZU_i})-I(X;Y|\overline{Ze_1})&=0
\end{aligned}$$

The first implication is a result of Lemma 3.3. Using Lemma 3.4 and replacing Z with XYZ gives the second implication. Then, using Lemma 3.7 with modified channels $\{C_i'\}$ that are identical to $\{C_i\}$, but they leave X and Y unchanged gives the third implication. Finally, using Lemma 3.8 gives us the final implication. □

Lemma 3.3. *If* $\lim_{i\to\infty} H(U_i) = 0$ *for some sequence of discrete random variables* U_i*, then* $\lim_{i\to\infty} D(U_i, e_1) = 0$.

Proof. Suppose the probabilities for each outcome of the random variables U_i are $a_{1i}, a_{2i}, \ldots$, with $a_{1i} \geq a_{2i} \geq \ldots$. Then

$$\begin{aligned} H(U_i) &= \sum_j -a_{ji} \log a_{ji} \\ &= \sum_j a_{ji} \log \frac{1}{a_{ji}} \\ &\geq \sum_j a_{ji} \log \frac{1}{a_{1i}} \\ &= \log \frac{1}{a_{1i}}. \end{aligned}$$

Since $\log \frac{1}{a_{1i}}$ is nonnegative, if $H(U_i) \to 0$, we must have $\log \frac{1}{a_{1i}} \to 0$. Therefore $a_{1i} \to 1$. So

$$D(U_i, e_1) = \frac{1}{2}(1 - a_{1i} + 1 - a_{1i}) = 1 - a_{1i}$$

and $D(U_i, e_1) \to 0$. □

Lemma 3.4. *Suppose the sequence of discrete random variables* U_i *satisfies* $\lim_{i\to\infty} D(U_i, e_1) = 0$*, and let* Z *be an arbitrary discrete random variable. Then* $D(ZU_i, Ze_1) = D(U_i, e_1)$.

Proof. For the purposes of this proof, let "1" be the value that e_1 attains with probability 1. It follows almost directly from the definition of trace distance that, summing over all (z, x) so that the expression inside the sum is positive,

$$D(ZU_i, Ze_1) = \sum P(Z = z, e_1 = x) - P(Z = z, U_i = x).$$

Since e_1 is always 1, the probability that $Z = z$ and $e_1 = x$ for any x other than 1 is 0, so the expression inside the sum will not be positive. Thus the trace distance can be reduced to the following sum, where the sum is taken over all z so that the expression inside the sum is positive.

$$D(ZU_i, Ze_1) = \sum P(Z = z, e_1 = 1) - P(Z = z, U_i = 1).$$

But since $e_1 = 1$ with probability 1, and $P(U_i = 1) \leq 1$, it suffices to take

$$D(ZU_i, Ze_1) = \sum_{\text{all } z} P(Z = z) - P(Z = z, U_i = 1)$$

which is just

$$D(ZU_i, Ze_1) = 1 - \sum_z P(Z = z, U_i = 1) = 1 - P(U_i = 1).$$

Since "1" is the value that e_1 attains with probability 1, U_i attains this value with the highest probability (as U_i and e_1 "match up"). So $D(U_i, e_1) = 1 - P(U_i = 1)$ and we are done. □

Remark 3.5. The importance of e_1 is demonstrated by the above lemma, as the lemma becomes false if U_i and e_1 are replaced by arbitrary random variables. A counterexample is if Z is a fair coin flip and $A = Z$ while B is an (independent) fair coin flip. Then $D(A, B) = 0$ because these probability distributions are identical, but $D(ZA, ZB) = 1$ because ZA is either both heads or both tails with probability 0.5, while ZB can be all of the 4 possibilities, each with probability 0.25.

Remark 3.6. The above lemma also shows the importance of transferring the entropies into trace distance rather than some other form of distance, such as the Kullback-Leibler (KL) divergence, which is defined for two probability distributions P and Q, both over the probability space $\mathcal{X}$, as

$$D_{KL}(P||Q) := \sum_{x\in\mathcal{X}} P(x)\log\left(\frac{P(x)}{Q(x)}\right).$$

In particular, the lemma above is false if the trace distances are replaced with KL-divergences because there exists a Z with infinite range such that the KL-divergence of the left-hand side of the lemma diverges. Consider $P(Z = z_n) = 2^{-n}$ and $P(Z = z_n, U_i = 1) = 2^{-n-\frac{2^n}{i}}$ for all U_i (the rest of the ZU_i probability distribution can be filled in arbitrarily). Here, as i becomes larger, $P(U_i = 1)$ becomes closer to 1, but calculating the KL-divergence gives

$$P(Z = z_n)\log\left(\frac{P(Z = z_n)}{P(Z = z_n, U_i = 1)}\right) = \frac{1}{i} \implies D_{KL}(Ze_1, ZU_i) = \frac{|\mathcal{Z}|}{i} = \infty.$$

Lemma 3.7. *Let U_i be a sequence of random variables and let Z be an arbitrary random variable. Suppose C_i is an arbitrary channel whose action is denoted by a bar. Then for all i, $D(\overline{ZU_i}, \overline{Ze_1}) \leq D(ZU_i, Ze_1)$.*

Proof. The proof is similar to that of the analogous quantum result, proven in [2], that trace-preserving quantum operations are contractive.

For ease of writing let $X = ZU_i$ and $Y = Ze_1$. View the probability distributions X and Y by vectors of their probabilities ($\vec{x}$ and $\vec{y}$) and view the channel C_i as a stochastic matrix which we denote A. We also let a subscript i on a vector enclosed by parentheses (e.g. $(\vec{v})_i$) denote the ith component of the vector.

Using this notation, we have that

$$D(X,Y) = \sum_{i\text{ with }(\vec{x})_i-(\vec{y})_i>0} (\vec{x})_i - (\vec{y})_i = \sum_{i\text{ with }(\vec{x}-\vec{y})_i>0} (\vec{x}-\vec{y})_i.$$

Consider the vector $\vec{x}-\vec{y}$. We decompose this vector into its positive and negative components as follows. Let $\vec{a}$ be the vector such that $(\vec{a})_i = 0$ if $(\vec{x})_i - (\vec{y})_i \leq 0$ and $a_i = (\vec{x})_i - (\vec{y})_i$ otherwise. Similarly, let $\vec{b}$ be the vector such that $b_i = 0$ if $(\vec{x})_i - (\vec{y})_i \geq 0$ and $b_i = -((\vec{x})_i - (\vec{y})_i)$ otherwise. By definition, $(\vec{a})_i \geq 0$ for all i and $(\vec{b})_i \geq 0$ for all i. Therefore

$$D(X,Y) = \frac{1}{2}\left(\sum_i (\vec{a})_i + \sum_i (\vec{b})_i\right).$$

We now prove the statement:

$$\begin{aligned}
D(\overline{X},\overline{Y}) &= \frac{1}{2}\sum_i |(A\vec{x})_i - (A\vec{y})_i| \\
&\leq \frac{1}{2}\sum_i |(A\vec{a})_i| + |(A\vec{b})_i| \\
&= \frac{1}{2}\sum_i (A\vec{a})_i + \frac{1}{2}\sum_i (A\vec{b})_i \\
&= \frac{1}{2}\sum_i (\vec{a})_i + \frac{1}{2}\sum_i (\vec{b})_i \\
&= D(X,Y)
\end{aligned}$$

where the second to last step follows because the columns of A sum to 1 (as it is stochastic) and therefore A preserves the sum of the elements of a vector. □

Lemma 3.8. *Given P_{XYZ}, we have that*

$$\lim_{i\to\infty} D\left(XY\overline{ZU_i}, XY\overline{Ze_1}\right) = 0 \implies \lim_{i\to\infty} I\left(X;Y|\overline{ZU_i}\right) - I\left(X;Y|\overline{Ze_1}\right) = 0.$$

Proof. Define the following quantities:

- Let $\mathcal{X}$ and $\mathcal{Y}$ denote the ranges of the random variables X and Y, respectively. For any other variable V, let Range(V) be the range of V.
- For all $x \in \mathcal{X}$, $y \in \mathcal{Y}$, $z \in \text{Range}\left(\overline{ZU_i}\right)$, we have $p_{i,1}(xyz) := p\left(X = x, Y = y, \overline{Ze_1} = z\right)$, and $p_{i,2}\left(xyz\right) := p\left(X = x, Y = y, \overline{ZU_i} = z\right)$.
- Let $Z_i^* := \text{Range}\left(\overline{ZU_i}\right) \setminus \text{Range}\left(\overline{Ze_1}\right)$, and let $S_i := \sum_{XYZ_i^*} p_{i,2}\left(xyz\right)$. Because $S_i \leq D\left(XY\overline{ZU_i}, XY\overline{Ze_1}\right)$, S_i tends to 0 as i tends to infinity.

Also, if there is a group of random variables in the index of a summation, then the summation is summed over all values in the range of each variable, where the lowercase variables correspond to each of the uppercase random variables (e.g. $x \in \mathcal{X}$, $y \in \mathcal{Y}$). Expanding the conditional mutual information expressions gives

$$I\left(X;Y|\overline{ZU_i}\right) - I\left(X;Y|\overline{Ze_1}\right) = \left(H\left(X\overline{ZU_i}\right) - H\left(X\overline{Ze_1}\right)\right) + \left(H\left(Y\overline{ZU_i}\right) - H\left(Y\overline{Ze_1}\right)\right)$$

$$- \left(H\left(XY\overline{ZU_i}\right) - H\left(XY\overline{Ze_1}\right)\right) - \left(H\left(\overline{ZU_i}\right) - H\left(\overline{Ze_1}\right)\right) =$$

$$= \sum_{XY\overline{ZU_i}} \left(p_{i,2}\left(xyz\right)\log p_{i,2}\left(z\right) - p_{i,1}\left(xyz\right)\log p_{i,1}\left(z\right)\right) + \sum_{XY\overline{ZU_i}} \left(p_{i,2}\left(xyz\right)\log p_{i,2}\left(xyz\right) - p_{i,1}\left(xyz\right)\log p_{i,1}\left(xyz\right)\right)$$

$$- \sum_{XY\overline{ZU_i}} \left(p_{i,2}\left(xyz\right)\log p_{i,2}\left(xz\right) - p_{i,1}\left(xyz\right)\log p_{i,1}\left(xz\right)\right) - \sum_{XY\overline{ZU_i}} \left(p_{i,2}\left(xyz\right)\log p_{i,2}\left(yz\right) - p_{i,1}\left(xyz\right)\log p_{i,1}\left(yz\right)\right).$$

Now, we split the summation into two parts: $z \in \text{Range}(\overline{Ze_1})$ or $z \in \text{Range}(Z_i^*)$. We now deal with the first part ($z \in \text{Range}(\overline{Ze_1})$). Note that

$$-H\left(XY\overline{Ze_1}\right) = \sum_{XY\overline{Ze_1}} p_{i,1}\left(xyz\right)\log p_{i,1}\left(xyz\right).$$

However, we also have that

$$-H\left(XY\overline{Ze_1}\right) = -H\left(XY\overline{ZU_i}|z \in \overline{Ze_1}\right) = \sum_{XY\overline{Ze_1}} \frac{p_{i,2}\left(xyz\right)}{1 - S_i} \log\left(\frac{p_{i,2}\left(xyz\right)}{1 - S_i}\right) =$$

$$-\log\left(1 - S_i\right) + \frac{1}{1 - S_i} \sum_{XY\overline{Ze_1}} p_{i,2}\left(xyz\right)\log p_{i,2}\left(xyz\right) \implies$$

$$\sum_{XY\overline{Ze_1}} p_{i,2}\left(xyz\right)\log p_{i,2}\left(xyz\right) = -\left(1 - S_i\right)H\left(XY\overline{Ze_1}\right) + \left(1 - S_i\right)\log\left(1 - S_i\right).$$

This means that

$$\sum_{XY\overline{Ze_1}} \left(p_{i,2}\left(xyz\right)\log p_{i,2}\left(xyz\right) - p_{i,1}\left(xyz\right)\log p_{i,1}\left(xyz\right)\right) = S_iH\left(XY\overline{Ze_1}\right) + \left(1 - S_i\right)\log\left(1 - S_i\right).$$

This approaches 0 as i goes to infinity because S_i tends to 0. For the other summations, we can repeat this logic with $-H\left(X\overline{Ze_1}\right)$, $-H\left(Y\overline{Ze_1}\right)$, and $-H\left(\overline{Ze_1}\right)$. This will produce the expressions $S_iH\left(X\overline{Ze_1}\right) + (1-S_i)\log(1-S_i)$, $S_iH\left(Y\overline{Ze_1}\right) + (1-S_i)\log(1-S_i)$, and $S_iH\left(\overline{Ze_1}\right) + (1-S_i)\log(1-S_i)$, respectively. Therefore, for each of the four summations, the terms of the sum that are a part of $z \in \overline{Ze_1}$ approach 0. This deals with the part $z \in \overline{Ze_1}$.

Now, consider all $z \in \text{Range}(Z_i^*)$. Here, we have $p_{i,1}(\cdot,\cdot,z) = 0$ because of the definition of Z_i^*. This leaves us with

$$\sum_{XYZ_i^*} p_{i,2}(xyz)\left(\log p_{i,2}(z) + \log p_{i,2}(xyz) - \log p_{i,2}(xz) - \log p_{i,2}(yz)\right) =$$

$$\sum_{XYZ_i^*} p_{i,2}(xyz)\log\frac{p_{i,2}(z)}{p_{i,2}(xz)} - \sum_{XYZ_i^*} p_{i,2}(xyz)\log\frac{p_{i,2}(yz)}{p_{i,2}(xyz)} =$$

$$\sum_{XZ_i^*} p_{i,2}(xz)\log\frac{p_{i,2}(z)}{p_{i,2}(xz)} - \sum_{XYZ_i^*} p_{i,2}(xyz)\log\frac{p_{i,2}(yz)}{p_{i,2}(xyz)}.$$

We show that both of these summations tend to 0. For the first summation, for all $x \in \mathcal{X}$, define

$$f(x) := \sum_{Z_i^*} p_{i,2}(xz)\log\frac{p_{i,2}(z)}{p_{i,2}(xz)}.$$

Note that by the concavity of log, we have

$$f(x) = p_{i,2}(x)\sum_{Z_i^*}\frac{p_{i,2}(xz)}{p_{i,2}(x)}\log\frac{p_{i,2}(z)}{p_{i,2}(xz)} \le p_{i,2}(x)\log\left(\sum_{Z_i^*}\frac{p_{i,2}(xz)}{p_{i,2}(x)}\cdot\frac{p_{i,2}(z)}{p_{i,2}(xz)}\right) \le p_{i,2}(x)\log\frac{S_i}{p_{i,2}(x)}.$$

This means that

$$0 \le \sum_{XZ_i^*} p_{i,2}(xz)\log\frac{p_{i,2}(z)}{p_{i,2}(xz)} = \sum_X f(x) \le \sum_X p_{i,2}(x)\log\frac{S_i}{p_{i,2}(x)} = S_i\sum_X\frac{p_{i,2}(x)}{S_i}\log\frac{S_i}{p_{i,2}(x)}$$

$$= S_iH\left(X|z \in Z_i^*\right) \le S_iH(X).$$

This means that the first summation tends to 0. The second summation also tends to 0 by replacing all instances of z in the above proof with yz. Since all parts of the summations from the expanded conditional mutual information expressions tend to 0, we must have $I\left(X;Y|\overline{ZU_i}\right) - I\left(X;Y|\overline{Ze_1}\right)$ tends to 0 as well. □

4. IMPLICATIONS AND EXTENSIONS

Theorem 3.1 is a strengthening of a remark made by Christandl, Renner, and Wolf in [1]. In [1], the authors prove that the infimum is a minimum in the definition of the intrinsic information as long as the range of Z is finite. They remark that an argument analogous to that presented in their paper may prove that the infimum is a minimum in the definition of the reduced intrinsic information, with certain conditions on the size of X, Y, Z. This would imply a subcase of our theorem by the argument made briefly at the start of our proof. Unfortunately, it is unknown whether the arguments in [1] extend to the reduced intrinsic information measure. However, our present result is stronger than results that might be obtained through these means because we only require X, Y, Z to have finite entropy, whereas arguments analogous to those in [1] would require variables to have finite ranges.

Another application of Theorem 3.1 is demonstrated in the following statement, mentioned briefly at the end of the Introduction.

Theorem 4.1. *If bound secrecy exists, then there exists a distribution P_{XYZ} such that $S(X;Y||Z) \neq I(X;Y \downarrow\downarrow Z)$.*

Proof. Let P_{XYZ} be a distribution that is bound secret, so that $I(X;Y \downarrow Z) > 0$ and $S(X;Y||Z) = 0$. However, by the contrapositive of the forward direction of Theorem 3.1, we have $I(X;Y \downarrow Z) > 0 \implies I(X;Y \downarrow\downarrow Z) > 0$. This means that this distribution satisfies $S(X;Y||Z) = 0 < I(X;Y \downarrow\downarrow Z)$, as desired. □

This theorem implies that at least one of the conjectures 2.9 and 2.10 is false. Since a significant amount of evidence suggesting the existence of bound secrecy has already been established, we believe that Conjecture 2.9 is false.

Furthermore, the above theorem implies that the approach of showing that a certain distribution is bound secret by computing a nonzero intrinsic information and a reduced intrinsic information of 0 is guaranteed to fail. In order for this approach to work, a property that would make Theorem 3.1 false when the property is substituted for the reduced intrinsic information must be used. In particular, this property $f(XYZ)$ should satisfy the following:

- Given P_{XYZ}, we have $f(XYZ) \leq I(X;Y \downarrow Z)$, and equality does not always hold.
- $f(XYZ) = 0$ does not imply $I(X;Y \downarrow Z) = 0$.

5. BINARIZATIONS

One possible path for establishing the existence of bound secrecy has been suggested in [4], which we now investigate. In [4], the authors suggest that the existence of positive intrinsic information which vanishes upon binarization may be a candidate for bound secrecy. The authors provide an example of a distribution $X_0Y_0Z_0$ such that for all binarizations of X_0 and Y_0, producing $\overline{X_0}$ and $\overline{Y_0}$ respectively, $I(\overline{X_0};\overline{Y_0} \downarrow Z_0) = 0$ (Proposition 4) [4]. They also show that for *any* distribution XYZ, if the secret-key rate $S(X;Y||Z) > 0$, then for some N there exist binarizations of X^N and Y^N such that $I(\overline{X^N};\overline{Y^N} \downarrow Z^N) > 0$ (Proposition 5) [4]. Therefore, the missing step for establishing bound secrecy for $X_0Y_0Z_0$ is the following:

Conjecture 5.1. [4] Let XYZ be a distribution. If, for all binary output channels $P_{\overline{X}|X}$ and $P_{\overline{Y}|Y}$ we have $I(\overline{X};\overline{Y} \downarrow Z) = 0$, then for all N, for all binary output channels $P_{\overline{X^N}|X^N}$ and $P_{\overline{Y^N}|Y^N}$, we must have $I(\overline{X^N};\overline{Y^N} \downarrow Z^N) = 0$.

In fact, it is only necessary to prove Conjecture 5.1 for the specific distribution $X_0Y_0Z_0$, which we will investigate in the next section. In this section, we reduce Conjecture 5.1 to a much simpler statement which, if proven, would establish Conjecture 5.1 and thereby prove the existence of bound secrecy. (In the statement of the theorem, the symbol $\perp\!\!\!\perp$ is used to denote independence of random variables.)

Theorem 5.2. *Conjecture 5.1 is equivalent to the following:*

$$\forall \overline{X}, \overline{Y}, \exists \overline{Z} \text{ such that } (\overline{X} \perp\!\!\!\perp \overline{Y})|\overline{Z} \implies \forall N, \forall \overline{X^N}, \overline{Y^N},\ \exists \overline{Z^N} \text{ such that } (\overline{X^N} \perp\!\!\!\perp \overline{Y^N})|\overline{Z^N}$$

where the channels processing X, Y, X^N, Y^N are assumed to be binarizations.

The statement of the theorem is noteable because it makes no reference to information-theoretic quantities: it is purely a statement about probabilities. To prove Theorem 5.2, we need the following lemma linking information and probability.

Lemma 5.3. *Given random variables X, Y, Z, we have $I(X;Y|Z) = 0$ if and only if $(X \perp\!\!\!\perp Y)|Z$.*

Proof. For the forward direction, we have

$$\begin{aligned}
0 = -I(X;Y|Z) &= \sum_{xyz} P(X=x,Y=y|Z=z)\log\left(\frac{P(X=x|Z=z)P(Y=y|Z=z)}{P(X=x,Y=y|Z=z)}\right)\\
&\le \frac{1}{\ln 2}\sum_{xyz} P(X=x,Y=y|Z=z)\left(\frac{P(X=x|Z=z)P(Y=y|Z=z)}{P(X=x,Y=y|Z=z)}-1\right)\\
&= \frac{1}{\ln 2}\sum_{xyz}\left(P(X=x|Z=z)P(Y=y|Z=z)-P(X=x,Y=y|Z=z)\right)\\
&= \frac{1}{\ln 2}\sum_{xyz} P(X=x)P(Y=y)-P(X=x,Y=y)\\
&= \frac{1}{\ln 2}\left(\sum_{x} P(X=x)\sum_{y} P(Y=y)-1\right)\\
&= 0
\end{aligned}$$

where the second step follows because $\log_2 x \le \frac{x-1}{\ln 2}$ for all reals x. Since both sides of the above chain are 0, the inequality must be an equality. Since $\log_2 x = \frac{x-1}{\ln 2}$ if and only if $x = 1$, the expression inside the logarithm must always be 1, which means

$$P(X=x|Z=z)P(Y=y|Z=z) = P(X=x,Y=y|Z=z)$$

for all x, y, z. Thus $(X \perp\!\!\!\perp Y)|Z$.

For the reverse direction, we simply note that

$$I(X;Y|Z) = \sum_{xyz} -P(X=x,Y=y|Z=z)\log\left(\frac{P(X=x|Z=z)P(Y=y|Z=z)}{P(X=x,Y=y|Z=z)}\right)$$

and if $(X \perp\!\!\!\perp Y)|Z$, then the expression inside the logarithm is always 1, so each term of the sum becomes 0, and $I(X;Y|Z) = 0$. □

We now prove Theorem 5.2.

Proof. As in the statement of the theorem, all channels that process X, Y, X^N, Y^N are assumed to be binarizations. We observe that by the definition of the intrinsic information,

$$\forall \overline{X}, \overline{Y},\ I(\overline{X};\overline{Y} \downarrow Z) = 0 \iff \forall \overline{X}, \overline{Y}, \exists \overline{Z} \text{ such that } I(\overline{X};\overline{Y}|\overline{Z}) = 0.$$

Then using the lemma, we have

$$\forall \overline{X}, \overline{Y}, \exists \overline{Z} \text{ such that } I(\overline{X};\overline{Y}|\overline{Z}) = 0 \iff \forall \overline{X}, \overline{Y}, \exists \overline{Z} \text{ such that } (\overline{X} \perp\!\!\!\perp \overline{Y})|\overline{Z}.$$

We can repeat the logic for X^N, Y^N, Z^N. Therefore, showing

$$\forall \overline{X}, \overline{Y},\ I(\overline{X};\overline{Y} \downarrow Z) = 0 \iff \forall N, \forall \overline{X^N}, \overline{Y^N},\ I(\overline{X^N};\overline{Y^N} \downarrow Z^N) = 0$$

is equivalent to the statements in terms of independence, which is the desired result. □

6. INDEPENDENCE-INDUCING BINARIZATIONS

We present some progress on proving Conjecture 5.1 for the specific distribution XYZ, as introduced in [4]. This would be sufficient to establish bound secrecy for the distribution, as shown below.

X $Y(Z)$	1	2	3
1	2 (0)	4 (1)	1 (2)
2	1 (3)	2 (0)	4 (4)
3	4 (5)	1 (6)	2 (0)

For this distribution, the value of Z is determined by the values of X and Y, and is indicated by the number in parentheses in the cell. The unnormalized probability for that xyz triplet is given by the number not in parentheses.

One method for proving the statement in Theorem 5.2 for this distribution is by strengthening it to the following statement and not allowing Alice to binarize (Conjecture 6.1).

Conjecture 6.1. For the distribution XYZ, for any $N \geq 1$ we have

$$\forall \overline{Y^N},\ \exists \overline{Z^N} \text{ such that } (X^N \perp\!\!\!\perp \overline{Y^N})|\overline{Z^N}$$

where the channel processing Y^N is assumed to be a binarization.

Note that this conjecture implies Theorem 5.2 because if Alice is not allowed to binarize and Eve can still erase correlation by processing Z^N, then there would still be no correlation even if Alice binarized her variable. To prove Conjecture 6.1, we must show that for any binarization that Bob chooses, Eve is able to process her variable such that Alice and Bob are independent given Eve's information. Here, we primarily investigate the cases $N = 1$ and $N = 2$.

In the case that $N = 1$, it has been proven that for all binarizations $\overline{Y}$ of Y, Eve can always find a $\overline{Z}$ such that $X \perp\!\!\!\perp \overline{Y}|\overline{Z}$ (Proposition 4 of [4]). We have found an explicit construction of the map $\overline{Z}$, based on the following value.

Definition 6.2. We define the *independence target value* (ITV) $\tau(x, y, z)$ for any reals x, y, z as the median of $\frac{2x+1y+0z}{3}$, $\frac{1x+0y+2z}{3}$, and $\frac{0x+2y+1z}{3}$.

Bob's map can be defined using the three numbers $P_{\overline{Y}|Y}(\overline{0}, 1) = r$, $P_{\overline{Y}|Y}(\overline{0}, 2) = s$, and $P_{\overline{Y}|Y}(\overline{0}, 3) = t$. Since Bob's map is a binarization, we have that $P_{\overline{Y}|Y}(\overline{1}, 1) = 1-r$, $P_{\overline{Y}|Y}(\overline{1}, 2) = 1-s$, and $P_{\overline{Y}|Y}(\overline{1}, 3) = 1-t$. The table for the distribution $X\overline{Y}Z$ is as follows, using the same notation as before:

X $\overline{Y}(Z)$	1	2	3
$\overline{0}$	$2r$ (0) s (3) $4t$ (5)	$2s$ (0) $4r$ (1) t (6)	$2t$ (0) r (2) $4s$ (4)
$\overline{1}$	$2-2r$ (0) $1-s$ (3) $4-4t$ (5)	$2-2s$ (0) $4-4r$ (1) $1-t$ (6)	$2-2t$ (0) $1-r$ (2) $4-4s$ (4)

As mentioned in [4], if Eve receives $z \neq 0$, she knows what X is, meaning that $X|Z = z$ is constant and $X \perp\!\!\!\perp \overline{Y}|Z = z$. Therefore, we focus our attention on the case that $Z = 0$. We consider the same map $P_{\overline{Z}|Z}$ as mentioned in the proof of Proposition 4 of [4]. In this map, the nonzero values for Z, namely 1, 2, 3, 4, 5, 6 are mapped to $\overline{0}$ with probabilities c, e, a, f, b, and d respectively, and they are mapped to $\overline{1}, \ldots, \overline{6}$ with probabilities $1-c$, $1-e$, $1-a$, $1-f$, $1-b$, $1-d$ respectively. The value $Z = 0$ is mapped to $\overline{0}$ with probability 1. Under this map, the probability distribution $P_{X\overline{Y}|\overline{Z}=\overline{0}}$ is as follows:

$X\overline{Y}|\overline{Z} = \overline{0}$	1	2	3
$\overline{0}$	$2r + as + 4bt$	$4cr + 2s + dt$	$er + 4fs + 2t$
$\overline{1}$	$(2 + a + 4b) - (2r + as + 4bt)$	$(4c + 2 + d) - (4cr + 2s + dt)$	$(e + 4f + 2) - (er + 4fs + 2t)$

In order to have $(X \perp\!\!\!\perp \overline{Y})|\overline{Z} = \overline{0}$, we must have the following:

$$\frac{2r + as + 4bt}{2 + a + 4b} = \frac{4cr + 2s + dt}{4c + 2 + d} = \frac{er + 4fs + 2t}{e + 4f + 2}.$$

(In the case that the denominators of these fractions are 0 and the numerators nonzero, the independence condition is satisfied. If both the numerator and denominator of a fraction are equal, it can be ignored since it imposes no additional conditions.) In [4], it is proven that for any r, s, t there exist a, b, c, d, e, f satisfying the above equations using a topological argument, but here we demonstrate this in a constructive manner using the ITV:

Theorem 6.3. *For numbers $r, s, t \in \mathbb{R}$, there exist $a, b, c, d, e, f \in [0, 1]$ such that*

$$\frac{2r + as + 4bt}{2 + a + 4b} = \frac{4cr + 2s + dt}{4c + 2 + d} = \frac{er + 4fs + 2t}{e + 4f + 2} = \tau(r, s, t).$$

Proof. Note that $\tau(r, s, t) = \tau(s, t, r) = \tau(t, r, s)$. This means that if we can find satisfactory $a, b \in [0, 1]$ such that

$$\frac{2r + as + 4bt}{2 + a + 4b} = \tau(r, s, t)$$

for any $r, s, t \in \mathbb{R}$, then by symmetry we can find satisfactory $c, d \in [0, 1]$ such that

$$\frac{2s + dt + 4cr}{2 + d + 4c} = \tau(s, t, r) = \tau(r, s, t)$$

for the same set of $r, s, t \in [0, 1]$. Similarly, we can also find $e, f \in [0, 1]$ such that

$$\frac{2t + er + 4fs}{2 + e + 4f} = \tau(t, r, s) = \tau(r, s, t)$$

for the same set of r, s, and t. This means that we only need to show that for all $r, s, t \in \mathbb{R}$, there exist $a, b \in [0, 1]$ such that

$$\frac{2r + as + 4bt}{2 + a + 4b} = \tau(r, s, t).$$

If $r = s = t$, then both sides of the equation above are equal to r regardless of the choice of a, b. Now, assume that not all three of r, s, t are equal. Then we can transform the triple (r, s, t) into some permutation of $(0, x, 1)$ for $x \in [0, 1]$ as follows. Note that since the left and right sides of the equation above are computed from weighted averages of r, s, and t, we can scale the variables by a nonzero constant or add a real number without changing the equation. We can subtract $\min(r, s, t)$ from all of variables and since all of the variables are not equal, we can divide these new variables by $\max(r, s, t) - \min(r, s, t) \neq 0$. We have now transformed (r, s, t) to some permutation of $(0, x, 1)$, where $x \in [0, 1]$.

Our new variables are thus one of the circular shifts of $(0, x, 1)$ or $(0, 1, x)$ for some $x \in [0, 1]$. In the latter case, we can multiply the triple -1 and add 1 to get a circular shift of $(0, 1 - x, 1)$. This means that we can assume without loss of generality that (r, s, t) is some circular shift of $(0, x, 1)$ for some $x \in [0, 1]$.

Since the ITV is invariant under circular shifts, we now have $\tau(r, s, t) = \tau(0, x, 1)$, which is the median of $\frac{x}{3}$, $\frac{2}{3}$, and $\frac{1+2x}{3}$. Note that $\frac{x}{3}$ is the least of these three, so the median is $\frac{\min(2,1+2x)}{3}$. If $x < \frac{1}{2}$, then this is $\frac{1+2x}{3}$, and if $x \geq \frac{1}{2}$, then this is $\frac{2}{3}$.

We now take cases on which of these circular shifts of $(0, x, 1)$ that (r, s, t) has been transformed into:

- $(r, s, t) = (0, x, 1)$: If $x < \frac{1}{2}$, then we can take $a = 0$ and $b = \frac{1+2x}{4-4x}$. If $x \geq \frac{1}{2}$, then we can take $a = 0$ and $b = 1$.
- $(r, s, t) = (1, 0, x)$: If $x < \frac{1}{2}$, then we can take $a = 0$ and $b = 1$. If $x \geq \frac{1}{2}$, then we can take $a = 1$ and $b = 0$.

- $(r, s, t) = (x, 1, 0)$: If $x < \frac{1}{2}$, then we can take $a = 1$ and $b = 0$. If $x \geq \frac{1}{2}$, then we can take $a = 1$ and $b = \frac{3}{8}(2x - 1)$.

This covers all of the cases, so we are done. □

This resolves the $N = 1$ case. We attempt to extend the use of the ITV for $N = 2$. Bob's map may be parameterized by the values $a_{ij} := P_{\overline{Y^2}|Y^2}(0, ij)$ for $i, j \in \{1, 2, 3\}$. In this case, we cannot focus on the $Z^2 = 00$ case alone, because if $Z^2 = 01$ for example, Eve is unsure of whether Alice has $X^2 = 12$, $X^2 = 22$, or $X^2 = 32$. If neither of the first nor second components of Z^2 are 0, Eve will be certain of what Alice has, so these cases are resolved (i.e. no processing is necessary). This means that we must repeat the above procedure for $Z^2 = 00, 01, 02, \ldots, 06, 10, 20, \ldots, 60$. We believe that the target value for the fractions corresponding to these values are the following.

Conjecture 6.4. Define $a_{ij} := P_{\overline{Y^2}|Y^2}(0, rs)$ for $r, s \in \{1, 2, 3\}$, and let the target values $\tau_2 : \{00, 01, 02, \ldots, 06, 10, 20, \ldots, 60\} \to [0, 1]$ be defined as follows:

- $\tau_2(0i) = \tau(a_{1j}, a_{2j}, a_{3j})$, where $j = \lceil \frac{i}{2} \rceil$ and $1 \leq i \leq 6$,
- $\tau_2(i0) = \tau(a_{j1}, a_{j2}, a_{j3})$, where $j = \lceil \frac{i}{2} \rceil$ and $1 \leq i \leq 6$,
- $\tau_2(00) = \tau(\tau(a_{11}, a_{12}, a_{13}), \tau(a_{21}, a_{22}, a_{23}), \tau(a_{31}, a_{32}, a_{33}))$.

Then there exists a channel $P_{\overline{Z^2}|Z^2}$ such that $P(\overline{Y^2} = 0|X^2, \overline{Z^2} = \overline{z}) = \tau_2(z)$ for all z in the domain of τ_2.

The choice of $j = \lceil \frac{i}{2} \rceil$ is motivated by the fact that in this distribution, if Eve receives $Z = i$, then she knows that Bob has $Y = \lceil \frac{i}{2} \rceil = j$. We observe that these target values give the correct values for a particular class of Bob's strategies which we term product strategies:

Definition 6.5. A *product strategy* for Bob (who has $Y^N = Y_1 Y_2 \ldots Y_N$) is a binarization of Y^N so that the N-dimensional matrix of probabilities $P(\overline{Y^N} = 0|Y^N = y)$ for $y \in \mathcal{Y}^N$ is the tensor product of the N vectors $P(\overline{Y^N} = 0|Y_1 = y_1), \ldots, P(\overline{Y^N} = 0|Y_N = y_N)$ where each y_i takes on every value in $\mathcal{Y}$.

The reason that this target value choice works for product strategies is due to the following property of the ITV:

Theorem 6.6. *For real numbers* $b_0, b_1, b_2, c_0, c_1, c_2 \in [0, 1]$,

$$\tau(\tau(b_0c_0, b_1c_0, b_2c_0), \tau(b_0c_1, b_1c_1, b_2c_1), \tau(b_0c_2, b_1c_2, b_2c_2)) = \tau(b_0, b_1, b_2)\tau(c_0, c_1, c_2).$$

Proof. Note that $\tau(b_0c_0, b_1c_0, b_2c_0) = c_0\tau(b_0, b_1, b_2)$ because we can factor the c_0 from the set of weighted averages considered when calculating the ITV. We can use this repeatedly to get that the left-hand side is equal to

$$\tau(c_0\tau(b_0, b_1, b_2), c_1\tau(b_0, b_1, b_2), c_2\tau(b_0, b_1, b_2)) = \tau(b_0, b_1, b_2)\tau(c_0, c_1, c_2).$$

□

Note that if the vectors $P(\overline{Y^2} = 0|Y_1 = 0)$ and $P(\overline{Y^2} = 0|Y_2 = 0)$ are (b_0, b_1, b_2) and (c_0, c_1, c_2), respectively, then the product strategy this corresponds to is the map $a_{ij} = b_ic_j$ for all $i, j \in \{0, 1, 2\}$. Using 6.6, the target value for $Z^2 = 00$ is equal to $\tau(b_0, b_1, b_2)\tau(c_0, c_1, c_2)$. Therefore, we can use our results from the $N = 1$ case for each of components for Y^2, and then multiply them together to construct our map.

We believe that this choice for the target value can also be used for any strategy/map that Bob uses for the $N = 2$ case, and similarly constructed target values (i.e. iterating over triplets) can be used for $N \geq 3$.

7. CONCLUSION

In this paper, we have shown a new relation between two well-known information-theoretic quantities: the intrinsic information and the reduced intrinsic information. Namely, for a given P_{XYZ}, when the reduced intrinsic information of this distribution is 0, then so is the intrinsic information. This relation has many important ramifications for significant conjectures in information theory. For example, out of the two long-standing conjectures of the secret-key rate being equal to the reduced intrinsic information and the conjecture of bound secrecy[10], at least one of them must be incorrect. Another implication is that the reduced intrinsic information cannot be used to prove that a distribution is bound secret. Future work in this direction would be to develop an information-theoretic quantity which has the property that it is not necessarily equal to 0 if the intrinsic information is equal to 0, and use this property to demonstrate that a particular distribution is bound secret.

We have also made progress on a possible approach for showing that a bound secret distribution does exist, using the idea of binarization of random variables[4]. In particular, we have reduced bound secrecy to a problem that does not require the use of information-theoretic quantities to formulate, instead using only basic ideas from probability. We have made progress on proving this statement for the candidate distribution introduced in [4], by creating an explicit construction for an information-erasing binarization. The construction makes generalizing the information-erasing binarization much easier compared to the previous non-constructive results.

8. ACKNOWLEDGEMENTS

We would like to thank the MIT PRIMES-USA program for the opportunity to conduct this research. We would also like to thank Peter Shor for suggesting this problem to us. We also acknowledge Stefan Wolf, Matthias Christandl, and Renato Renner for their helpful answers to our questions regarding their papers.

[1] M. Christandl, R. Renner, and S. Wolf. A property of the intrinsic mutual information. In *IEEE international symposium on information theory*, pages 258–258, 2003.

[2] I. Chuang and M. Nielsen. *Quantum computation and quantum information.* Cambridge University Press, Cambridge, 2000.

[3] N. Gisin, R. Renner, and S. Wolf. Bound information: The classical analog to bound quantum entanglemen. In *European Congress of Mathematics*, pages 439–447. Springer, 2001.

[4] N. Gisin, R. Renner, and S. Wolf. Linking classical and quantum key agreement: Is there a classical analog to bound entanglement? *Algorithmica*, 34(4):389–412, 2002.

[5] M. Horodecki, P. Horodecki, and R. Horodecki. Mixed-state entanglement and distillation: Is there a "bound" entanglement in nature? *Physical Review Letters*, 80(24):5239–5242, jun 1998.

[6] S. Khatri and N. Lütkenhaus. Numerical evidence for bound secrecy from two-way postprocessing in quantum key distribution. *Physical Review A*, 95(4):042320, 2017.

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

[8] U. M. Maurer and S. Wolf. Unconditionally secure key agreement and the intrinsic conditional information. *IEEE Transactions on Information Theory*, 45(2):499–514, 1999.

[9] R. Renner, J. Skripsky, and S. Wolf. A new measure for conditional mutual information and its properties. In *IEEE International Symposium on Information Theory*, pages 259–259, 2003.

[10] R. Renner and S. Wolf. New bounds in secret-key agreement: The gap between formation and secrecy extraction. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 562–577. Springer, 2003.

[11] C. E. Shannon. Communication theory of secrecy systems. *The Bell system technical journal*, 28(4):656–715, 1949.