ISIT'2013 1569719849

Rate-Distortion Theory for Secrecy Systems

Curt Schieler and Paul Cuff
Dept. of Electrical Engineering,
Princeton University, Princeton, NJ 08544.
E-mail: {schieler, cuff}@princeton.edu

***Abstract*—In this work, secrecy in communication systems is measured by the distortion incurred by the worst-case adversary. The transmitter and receiver share secret key, which they use to encrypt communication and cause distortion at an adversary. In our model, we assume that an adversary not only intercepts the communication between the transmitter and receiver, but also may have access to noisy observations of the system. For example, the adversary may have causal access to a signal that is correlated with the source sequence or with the output of the receiver. Our main contribution is the solution of the optimal tradeoff among communication rate, secret key rate, distortion at the adversary, and distortion at the legitimate receiver. We demonstrate that side information at the adversary plays a pivotal role, and provide a number of examples that motivate and give insight into our results.**

I. Introduction

In [1], Shannon considered a communication system to be perfectly secure if the source and the eavesdropped message are statistically independent. A necessary and sufficient condition for perfect secrecy to hold is that the number of secret key bits per source symbol exceeds the entropy of the source. When the amount of shared key is insufficient, however, one must relax the requirement of statistical independence and invite new measures of secrecy.

In this paper, we consider a measure of secrecy that is directly inspired by rate-distortion theory. Whereas the objective in classical rate-distortion theory is to minimize the distortion at the receiver for a given rate of communication, our goal is to maximize the distortion at the eavesdropper for a given rate of secret key.

In classical rate-distortion theory, the receiver is implicitly modeled as an active participant in a distributed system, whose job is to produce actions that are correlated with the actions at the transmitter (i.e., those given by nature). If the receiver can produce highly correlated actions, then distortion is low. Similarly, when we use distortion as a measure of secrecy, we are modeling an eavesdropper as an active participant whose goal is to produce actions (or, attacks) that are also statistically correlated with the source. Because he plays an active role, the eavesdropper should be thought of as an adversarial entity. To ensure robustness, we design against the worst-case adversarial strategy.

The following example illustrates the care that should be exercised in using distortion as a measure of secrecy and partially motivates a salient feature of our model, *causal disclosure*.

One-bit secrecy and causal disclosure

Consider an i.i.d. source X^n with $X_i \sim \text{Bern}(\frac{1}{2})$. Use one bit of shared key k to encrypt X^n by transmitting Y^n, where $Y_i = X_i \oplus k$. That is, flip all of the bits of X^n if $k = 1$, otherwise simply send X^n. Upon intercepting the public message Y^n, the adversary submits an action sequence Z^n and incurs distortion $\frac{1}{n}\sum_{i=1}^n d(X_i, Z_i)$. If $d(x, z) = 1\{x \neq z\}$, then the adversary's best strategy is to simply set $Z^n = Y^n$, yielding an average distortion of $1/2$. But $1/2$ is the maximum possible average distortion! It appears as though we have maximized secrecy (in the sense of distortion) by only using one bit of secret key, but this view is misleading because the adversary knows that X^n is one of only two candidate sequences.

The example demonstrates the potential fragility of using distortion to measure secrecy without recognizing the ramifications. For, although maximal secrecy is attained, it vanishes altogether if the adversary views just one true bit of the source sequence (the bit allows him to determine whether or not to flip the Y^n sequence). Partly for this reason, our main results feature an assumption of *causal disclosure*, in which we assume the adversary has access to a noisy (or noiseless) version of the past actions of the system. Causal disclosure is a reasonable assumption not only in view of robustness, but also in its own right. If we are regarding the adversary as an active player who interacts with a distributed system, then causal access to the system behavior is natural and, we argue, appropriate. We show that results that seem suspiciously fantastic (e.g., maximal secrecy with little key) become reasonable when we assume that an adversary is able to view the past.

The example also reveals that average distortion can be a weak indicator of secrecy. A more prudent metric is the probability that the adversary can produce a low-distortion sequence. Both measures, and a third, are considered in this work.

The use of rate-distortion to study information-theoretic secrecy was initiated by Yamamoto in [2], wherein inner and outer bounds are obtained and there is no assumption of causal disclosure. Initial work on the causal disclosure case can be found in [3] and [4].

The content of this paper is as follows. In Section II, we present the problem setup and describe the generalized version of the one-bit secrecy example in which the adversary is not assumed to have any causal access. In Section III, we state

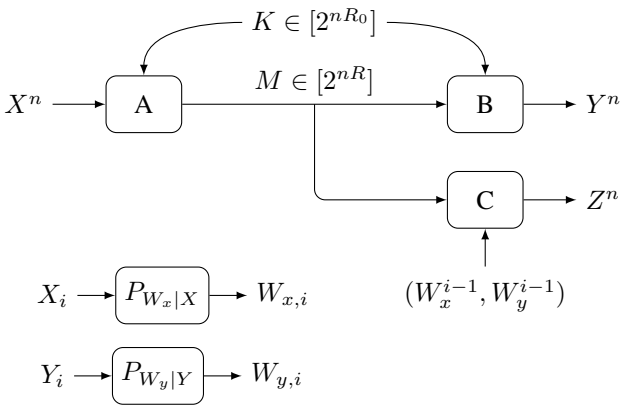


Fig. 1: Nodes A and B use secret key K and public communication M to coordinate against an adversarial Node C. At each step i, Node C can view the past behavior of the system, (W_x^{i-1}, W_y^{i-1}), where W_x^n is the output of a memoryless channel $\prod P_{W_x|X}$ with input X^n, and W_y^n is the output of a memoryless channel $\prod P_{W_y|Y}$ with input Y^n.

our main result, Theorem 2, in which noisy causal disclosure is a primary assumption. Theorem 2 describes the optimal relationship between communication rate, secret key rate, and distortion at the legitimate receiver and eavesdropper. The theorem is broad enough to cover a variety of scenarios, including settings involving side information at the adversary and the absence of causal disclosure. The proof, which we briefly sketch, draws on tools used in strong coordination and distributed channel synthesis [5]. Section IV is devoted to special cases and examples.

II. Preliminaries

The model we will use throughout is shown in Figure 1. The transmitting node, Node A, observes an i.i.d. source $\{X_i\}_{i=1}^{\infty}$, with X_i distributed according to P_X. Nodes A and B share a source of common randomness K, uniformly distributed and independent of $\{X_i\}_{i=1}^{\infty}$, which is also referred to as secret key. In this paper, we will focus exclusively on systems that employ block encoding and decoding; the blocklength is indicated by n. Based on a source block X^n and the common randomness, Node A sends a message M that is received by Node B and eavesdropped by Node C. Upon receipt of M, all three nodes sequentially produce actions: in the ith step, Nodes A, B and C produce X_i, Y_i, and Z_i, respectively. Although Node A has no control over his actions, which are simply given by X^n, he can coordinate with Node B through the use of the public communication and the secret key. The adversarial Node C produces Z_i based on the public message and the past behavior of the system, which is embodied in (W_x^{i-1}, W_y^{i-1}). At each step, the joint actions of the players incur a value $\pi(x, y, z)$, which represents symbol-wise payoff. Nodes A and B want to cooperatively maximize payoff, while Node C wants to minimize payoff through his attacks Z^n. Note that instead of evaluating secrecy and coordination separately, which could be done with two payoff functions $\pi_1(x, y)$ and $\pi_2(x, z)$, we have unified them in a single function $\pi(x, y, z)$. This approach emphasizes the game-theoretic nature of the model, but the use of multiple distortion functions has its own merits, and the results extend readily.

In Figure 1, we depict noisy causal disclosure by (W_x^{i-1}, W_y^{i-1}), where W_x^n is the output of a memoryless channel $\prod_{i=1}^n P_{W_x|X}$ with input X^n, and W_y^n is the output of a memoryless channel $\prod_{i=1}^n P_{W_y|Y}$ with input Y^n. Modeling the side information in this way covers a variety of scenarios. For example, if $P_{W_x|X}$ and $P_{W_y|Y}$ are identity channels, then the adversary has causal access (X^{i-1}, Y^{i-1}). If $W_x = \emptyset$ and $W_y = \emptyset$, then the adversary is completely blind to the past and only views the public message M.

Throughout, we assume that the alphabets $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$ are finite. We use the notation $[m] = \{1, \dots, m\}$.

Definition 1. *An (n, R, R_0) code consists of an encoder $f : \mathcal{X}^n \times [2^{nR_0}] \to [2^{nR}]$ (more generally, a conditional distribution $P_{M|X^n,K}$) and a decoder $g : [2^{nR}] \times [2^{nR_0}] \to \mathcal{Y}^n$ (more generally, $P_{Y^n|M,K}$).*

Permitting the decoder to use randomization is crucial. On the other hand, it is likely that the optimal encoder can be deterministic, although no proof has been obtained except in special cases. The proof of our main result uses a randomized encoder and decoder.

Nodes A and B use an (n, R, R_0) code to coordinate against Node C. To ensure robustness, we consider the payoff that can be assured against the worst-case adversary, i.e., the max-min payoff. There are several ways to define the payoff criterion for a block, and we will consider three: expected average payoff, probability of assured average payoff, and minimum symbol-wise payoff.

Definition 2. *Fix a source distribution P_X, a symbol-wise payoff function $\pi : \mathcal{X} \times \mathcal{Y} \times \mathcal{Z} \to \mathbb{R}$, and causal disclosure channels $P_{W_x|X}$ and $P_{W_y|Y}$. Define $W^n = (W_x^n, W_y^n)$. The triple (R, R_0, Π) is achievable if there exists a sequence of (n, R, R_0) codes such that*

- *Under payoff criterion P_1 (expected average distortion):*

$$\liminf_{n\to\infty} \min_{\{P_{Z_i|M,W^{i-1}}\}_{i=1}^n} \mathbb{E}\,\frac{1}{n}\sum_{i=1}^n \pi(X_i, Y_i, Z_i) \geq \Pi \quad (1)$$

- *Under payoff criterion P_2 (probability of assured average payoff): $\forall\, \varepsilon > 0$,*

$$\lim_{n\to\infty} \min_{\{P_{Z_i|M,W^{i-1}}\}_{i=1}^n} \mathbb{P}[\frac{1}{n}\sum_{i=1}^n \pi(X_i, Y_i, Z_i) \geq \Pi - \varepsilon] = 1 \quad (2)$$

- *Under payoff criterion P_3 (minimum symbol-wise payoff):*

$$\liminf_{n\to\infty} \min_{i\in[n]} \min_{P_{Z_i|M,W^{i-1}}} \mathbb{E}\,\pi(X_i, Y_i, Z_i) \geq \Pi \quad (3)$$

Under P_2, the range of $\pi(x, y, z)$ is extended to include $-\infty$.

Observe that although P_2 and P_3 are incomparable, they are both stronger than P_1. In each of the criteria, we allow

the adversary to employ his best set of probabilistic strategies $\{P_{Z_i|M,W^{i-1}}\}_{i=1}^n$ to minimize payoff. However, since expectation is linear in $P_{Z_i|M,W^{i-1}}$ for all i, it is minimized by extreme points of the probability simplex; thus, we can assume that Node C uses a set of deterministic strategies, $\{z_i(m, w^{i-1})\}_{i=1}^n$. Finally, it is assumed that the adversary has full knowledge of the source statistics and the code that Nodes A and B use.

Definition 3. *The rate-payoff region $\mathcal{R}(\mathsf{P}_1)$ is the closure of achievable triples (R, R_0, Π) under payoff criterion P_1. Regions $\mathcal{R}(\mathsf{P}_2)$ and $\mathcal{R}(\mathsf{P}_3)$ are defined in the same way.*

Before stating the main result, we briefly expand on the scenario in which lossless communication is required between Nodes A and B, and there is no causal disclosure of the system behavior to Node C. Since X^n must equal Y^n with high probability, the payoff function is of the form $\pi(x, z)$. Thus, the achievability criteria for (R, R_0, Π) under P_3 are that

$$\lim_{n\to\infty} \mathbb{P}[X^n \neq Y^n] = 0 \tag{4}$$

and

$$\liminf_{n\to\infty} \min_{i\in[n]} \min_{z_i(m)} \mathbb{E}\,\pi(X_i, z_i(M)) \geq \Pi \tag{5}$$

Theorem 1 ([6])**.** *Fix P_X and $\pi(x, z)$. If lossless communication is required and there is no causal disclosure, then $\mathcal{R}(\mathsf{P}_3)$ is given by*

$$\left\{\begin{array}{l}(R, R_0, \Pi): \\ \quad R \geq H(X) \\ R_0 \geq 0 \\ \quad \Pi \leq \min\limits_z \mathbb{E}\,\pi(X, z)\end{array}\right\} \tag{6}$$

Thus, any positive rate[1] of secret key guarantees maximal secrecy (in the sense of distortion), as Node C can achieve $\min_z \mathbb{E}\,\pi(X, z)$ by only knowing the distribution of the source. In fact, it is proved in [6] that each point in $\mathcal{R}(\mathsf{P}_3)$ of Theorem 1 can be achieved with $\mathcal{K}$ finite (not increasing with n) instead of $\mathcal{K} = [2^{nR_0}]$. This shows that even if the number of secret key bits is not growing with blocklength, one can achieve maximal secrecy *when there is no causal disclosure*. As in the example of one-bit secrecy, such guarantees are shattered if even a small number of source bits are available to the adversary.

III. Main Result

Our main result is the following.

Theorem 2. *Fix P_X, $\pi(x, y, z)$, and causal disclosure channels $P_{W_x|X}$ and $P_{W_y|Y}$. Then $\mathcal{R}(\mathsf{P}_1)$, the closure of achievable (R, R_0, Π) under payoff criterion P_1, is equal to*

$$\bigcup_{W_x - X - (U,V) - Y - W_y} \left\{\begin{array}{l}(R, R_0, \Pi): \\ \quad R \geq I(X; U, V) \\ R_0 \geq I(W_x W_y; V|U) \\ \quad \Pi \leq \min\limits_{z(u)} \mathbb{E}\,\pi(X, Y, z(U))\end{array}\right\}, \tag{7}$$

where $|\mathcal{U}| \leq |\mathcal{X}| + 2$ and $|\mathcal{V}| \leq |\mathcal{X}||\mathcal{Y}|(|\mathcal{X}| + 2) + 1$. Furthermore,

$$\mathcal{R}(\mathsf{P}_1) = \mathcal{R}(\mathsf{P}_2) = \mathcal{R}(\mathsf{P}_3). \tag{8}$$

In general, causal disclosure benefits an adversary, even though it does not aid the legitimate parties. This brings us to an important aspect of the scheme that is used in the proof of the main result. In effect, we design the encoder to use enough common randomness to actually void any benefit of causal disclosure. The method of encryption is not as straightforward as simply applying a one-time pad to part of the message. To elaborate on the effect of the code, suppose that the public message corresponds to a codeword $u^n(M)$ from an auxiliary codebook. Roughly speaking, the code and encryption are such that the adversary's view of the pair (X^n, Y^n) is that it was generated by passing $u^n(M)$ through a memoryless channel $P_{X,Y|U}$. Because the (virtual) channel is memoryless, causal access does not assist the adversary. This effect comes at the expense of secret key.

A. Proof sketch

Due to length restrictions, we only roughly describe some elements of the proof of achievability; the full details, as well as the converse proof, can be found in [7]. The proof relies heavily on the use of the "soft-covering lemma" and its recent generalizations and extensions, which can be found in [5]. In brief, the most basic version of the lemma is as follows. First, generate a random codebook of 2^{nR} independent codewords, each drawn according to $\prod P_U$. Select a codeword, uniformly at random, to be the input to a memoryless channel $P_{X|U}$. The lemma says that if $R > I(X; U)$, then the distribution of the output of the channel converges to $\prod P_X$ in expected total variation, where the expectation is with respect to the random codebook.

The encoder we use is not based on joint-typicality. It is not known, except in a special case, whether joint-typicality coding, or even deterministic encoding, suffices. Instead, the code is defined indirectly in the following manner. First, generate a random codebook of $2^{n(R+R_0)}$ pairs (U^n, V^n). By invoking the cloud-mixing lemma with rate $R_0 \geq I(W_x W_y; V|U)$, we can construct an auxiliary distribution $\overline{P}_{MKX^nY^nW_x^nW_y^n}$ that approximately has the following property:

$$(W_x^{i-1}, W_y^{i-1}) - U_i(M) - (X_i, Y_i),\ \forall i \tag{9}$$

If we can design our encoder and decoder so that this property holds, then the adversary's estimate of (X_i, Y_i) will only depend on $U_i(M)$ and not on the causal side information. To that end, define the encoder as the marginal conditional distribution $\overline{P}_{M|X^n,K}$ and the decoder as $\overline{P}_{Y^n|M,K}$, so that

[1]Note that $R_0 = 0$ is only included in Theorem 1 because we defined the region as the *closure* of achievable triples.

the true distribution P_{M,K,X^nY^n,W^n} corresponding to the system is

$$P \triangleq P_{X^n} P_K \overline{P}_{M|X^n,K} \overline{P}_{Y^n|M,K} P_{W^n|X^n,Y^n} \tag{10}$$

The system will effectively inherit (9) if P and $\overline{P}$ are close in total variation, which can be shown using the cloud-mixing lemma and $R > I(X;U,V)$.

The analysis of the three payoff criteria is omitted (see [7]), but we remark that the analysis of criterion P_2 is more involved than its counterparts; in particular, a martingale analysis is required to account for all possible adversarial strategies.

IV. Special cases and examples

In this section, we state several corollaries to Theorem 2 that are obtained through different choices of the disclosure channels $P_{W_x|X}$ and $P_{W_y|Y}$. We also consider cases in which lossless communication is required between Nodes A and B, which also follow from Theorem 2. The proofs are omitted.

A. Lossless communication

In the following, we require X^n to equal Y^n with high probability. If we use payoff criterion P_2, this is ensured by defining payoff functions $\pi(x,y,z)$ that evaluate to $-\infty$ when $x = y$.

Corollary 1. *Fix P_X, $\pi(x,z)$, and $P_{W_x|X}$. If lossless communication is required, then $\mathcal{R}(\mathsf{P}_2)$ is given by*

$$\bigcup_{U-X-W_x} \left\{ \begin{array}{r} (R, R_0, \Pi): \; R \geq H(X) \\ R_0 \geq I(W_x; X|U) \\ \Pi \leq \min\limits_{z(u)} \mathbb{E}\, \pi(X, z(U)) \end{array} \right\} \tag{11}$$

Corollary 1 spawns two important results, Corollaries 2 and 3, when we let $W_x = \emptyset$ and $W_x = X$, respectively.

Corollary 2. *If lossless communication is required and there is no causal disclosure, then $\mathcal{R}(\mathsf{P}_2)$ is given by*

$$\left\{ \begin{array}{r} (R, R_0, \Pi): \; R \geq H(X) \\ R_0 \geq 0 \\ \Pi \leq \min\limits_{z} \mathbb{E}\, \pi(X, z) \end{array} \right\} \tag{12}$$

This is the same region as Theorem 1. The next result was given in [3] under criterion P_1.

Corollary 3. *If lossless communication is required and X^{i-1} is disclosed, then $\mathcal{R}(\mathsf{P}_2)$ is given by*

$$\bigcup_{P_{U|X}} \left\{ \begin{array}{r} (R, R_0, \Pi): \; R \geq H(X) \\ R_0 \geq H(X|U) \\ \Pi \leq \min\limits_{z(u)} \mathbb{E}\, \pi(X, z(U)) \end{array} \right\} \tag{13}$$

We are able to give an analytical expression (omitted here, but can be found in [7]) for the region in Corollary 3 for any P_X when $\pi(x,z) = 1\{x \neq z\}$, allowing us to illustrate the effect of causal disclosure. Figure 2 shows the tradeoff between R_0 and Π when $P_X \sim \text{Bern}(1/2)$. We see that designing a code under the assumption that the adversary does not view any of the past leads to a fragile guarantee of maximal secrecy. Indeed, at low rates of secret key, the gap that results from causal disclosure is the difference between maximal secrecy and zero secrecy.

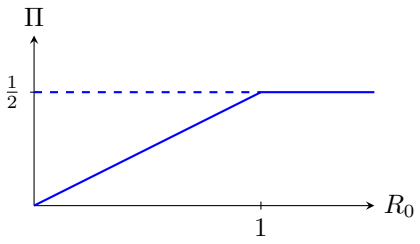


Fig. 2: Tradeoff between rate of secret key and payoff for lossless communication with $P_X \sim \text{Bern}(1/2)$ and $\pi(x,z) = 1\{x \neq z\}$. The dashed line is Corollary 2 (no causal disclosure) and the solid line is Corollary 3 (causal disclosure).

B. Lossy communication

In the previous section, the communication rate lay above $H(X)$ and did not affect the (R_0, Π) tradeoff. However, when the requirement of lossless communication is relaxed, all three quantities interact. There are four natural special cases that are obtained by setting W_x equal to $\emptyset$ or X and W_y equal to $\emptyset$ or Y. We denote the corresponding rate-payoff regions as $\mathcal{R}_\emptyset$, $\mathcal{R}_A$, $\mathcal{R}_B$, and $\mathcal{R}_{AB}$ to distinguish which nodes' actions are causally revealed. These cases were given individually in [4] under criterion P_1.

Corollary 4. *Fix P_X and $\pi(x,y,z)$. In each of the following, $\mathcal{R}$ holds under all three payoff criteria.*

If there is no causal disclosure, then $\mathcal{R}_\emptyset$ is given by

$$\bigcup_{P_{Y|X}} \left\{ \begin{array}{r} (R, R_0, \Pi): \; R \geq I(X;Y) \\ R_0 \geq 0 \\ \Pi \leq \min\limits_{z} \mathbb{E}\, \pi(X, Y, z) \end{array} \right\} \tag{14}$$

If X^{i-1} is disclosed, then $\mathcal{R}_A$ is given by

$$\bigcup_{P_{Y,U|X}} \left\{ \begin{array}{r} (R, R_0, \Pi): \; R \geq I(X;Y,U) \\ R_0 \geq I(X;Y|U) \\ \Pi \leq \min\limits_{z(u)} \mathbb{E}\, \pi(X, Y, z(U)) \end{array} \right\} \tag{15}$$

If Y^{i-1} is disclosed, then $\mathcal{R}_B$ is given by directly substituting $W_x = \emptyset$ and $W_y = Y$ in (7). Similarly, if (X^{i-1}, Y^{i-1}) is disclosed, then $\mathcal{R}_{AB}$ is given by directly substituting $W_x = X$ and $W_y = \emptyset$ in (7).

Consider the payoff function

$$\pi(x,y,z) = \begin{cases} 1 & \text{if } x = y \text{ and } x \neq z \\ 0 & \text{otherwise} \end{cases} \tag{16}$$

For this function, average payoff represents the fraction of symbols in a block that Nodes A and B are able to agree on and keep hidden from Node C. We now give analytic examples of achievable regions for the cases of Corollary 4 when

$P_X \sim \text{Bern}(\frac{1}{2})$. Numerical computation strongly suggests that the regions given are optimal, but it has not been proven.

If we let $U = \emptyset$ and $P_{Y|X} = \text{BSC}(\alpha)$, then we have

$$\mathcal{R}_A \supseteq \bigcup_{\alpha \in [0, \frac{1}{2}]} \left\{ \begin{array}{r} (R, R_0, \Pi): \; R \geq 1 - h(\alpha) \\ R_0 \geq 1 - h(\alpha) \\ \Pi \leq \dfrac{1-\alpha}{2} \end{array} \right\} \tag{17}$$

Letting $U = \emptyset$, $P_{Y|X} = \text{BSC}(\alpha)$, and $P_{V|Y} = \text{BSC}(\beta)$ gives

$$\mathcal{R}_B \supseteq \bigcup_{\alpha, \beta \in [0, \frac{1}{2}]} \left\{ \begin{array}{r} (R, R_0, \Pi): \; R \geq 1 - h(\alpha) \\ R_0 \geq 1 - h(\beta) \\ \Pi \leq \dfrac{1-\alpha \star \beta}{2} \end{array} \right\} \tag{18}$$

and

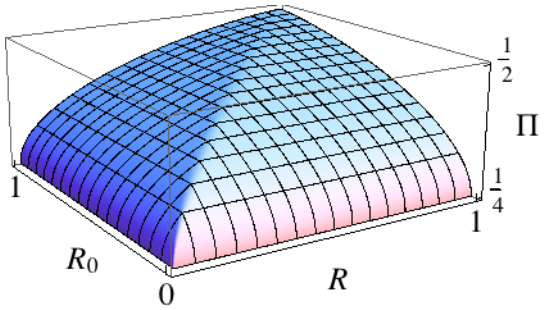
$$\mathcal{R}_{AB} \supseteq \text{conv} \left(\bigcup_{\alpha, \beta \in [0, \frac{1}{2}]} \left\{ \begin{array}{r} (R, R_0, \Pi): \\ R \geq 1 - h(\alpha) \\ R_0 \geq 1 + h(\alpha \star \beta) \\ \qquad -h(\alpha) - h(\beta) \\ \Pi \leq \dfrac{1-\alpha \star \beta}{2} \end{array} \right\} \right) \tag{19}$$

where $\alpha \star \beta = \alpha(1-\beta) + \beta(1-\alpha)$ and $\text{conv}(\cdot)$ denotes the convex hull operation. Regions (17) and (18) are convex as given.

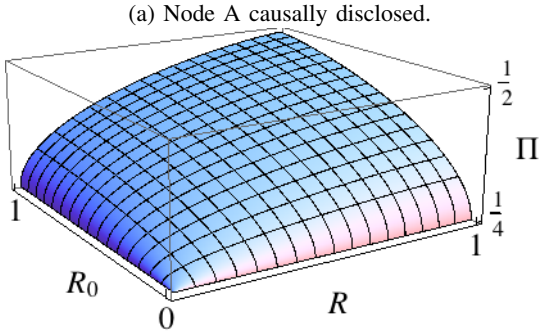
Several observations concerning the regions in Figure 3 are in order. First, the minimum payoff is $1/4$, which occurs when there is no communication or secret key. This is achieved if Node B generates an i.i.d. sequence according to $\text{Bern}(\frac{1}{2})$, and Node C produces an arbitrary sequence. Second, note the strict inclusion from top to bottom: causal access to Node A (Fig. 3a) is better for the adversary than access to Node B (Fig. 3b), and the combination (Fig. 3c) is strictly better for him than Node A alone. Finally, observe the effect of having a higher secret key rate than communication rate, and vice versa. When Node A is revealed, the payoff is a function of $\min(R, R_0)$ and there is no advantage in having excess of either rate. However, when Node B is revealed, both $R_0 > R$ and $R > R_0$ result in higher payoff than $R = R_0$. When both nodes are revealed, an excess of secret key rate increases payoff.

V. Conclusion

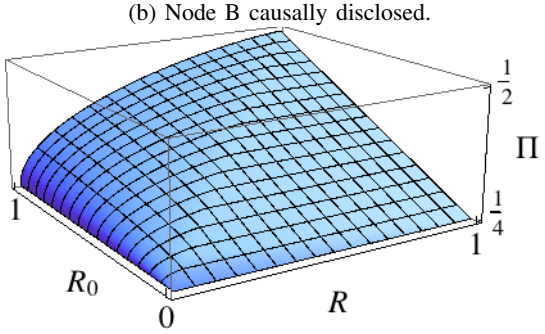
We have given a general solution to the tradeoff between secret key rate, communication rate, and payoff for a distributed system with an adversarial node, under a distortion-based measure of secrecy. We also showed that the main result holds for much stronger criteria than expected average payoff, and is broad enough to subsume lossless and lossy communication, and a number of special cases. Through a number of examples, we gave insight into the interplay of secret key and communication rates, and the effects of causal disclosure. We also showed the fragility of a distortion-based measure of secrecy if there is no assumption of causal disclosure.



(a) Node A causally disclosed.



(b) Node B causally disclosed.



(c) Nodes A and B causally disclosed.

Fig. 3: Achievable regions of Corollary 4 for $P_X \sim \text{Bern}(1/2)$ and $\pi(x, y, z) = 1\{x = y \text{ and } x \neq z\}$. Numerical computation strongly suggests that these regions are optimal.

VI. Acknowledgements

This research was supported in part by the National Science Foundation under Grants CCF-1116013 and CCF-1017431, and also by the Air Force Office of Scientific Research under Grant FA9550-12-1-0196.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, Oct. 1949.

[2] H. Yamamoto, "Rate-distortion theory for the Shannon cipher system," *IEEE Trans. Inf. Theory,* vol. 43, no. 3, pp. 827-835, 1997.

[3] P. Cuff, "A framework for partial secrecy," *IEEE Global Comm. Conf.,* Dec. 2010.

[4] P. Cuff, "Using secret key to foil an eavesdropper," *Proc. 48th Allerton Conf. on Comm., Control, and Comp.,* pp. 1405-1411, Sept. 2010.

[5] P. Cuff, "Distributed channel synthesis,", *arXiv:1208.4415*, Aug. 2012.

[6] C. Schieler and P. Cuff, "Secrecy is cheap if the adversary must reconstruct," in *Proc. IEEE Int. Symp. on Info. Theory*, Cambridge, MA, Jul. 2012.

[7] C. Schieler and P. Cuff, "Rate-distortion theory for secrecy systems," May 2013. [Online]. Available: http://arxiv.org/abs/1305.3905