Abstract—The basic two-terminal key generation model is considered, where the communication between the terminals is limited. We introduce a preorder relation on the set of joint distributions called $XY$-absolute continuity, and we reduce the multi-letter characterization of the key-communication tradeoff to the evaluation of the $XY$-concave envelope of a functional. For small communication rates, the key bits per interaction bit is expressed with a “symmetrical strong data processing constant”.

Using hypercontractivity and Rényi divergence, we also prove a computationally friendly strong converse bound for the common randomness bits per interaction bit in terms of the supremum of the maximal correlation coefficient over a set of distributions, which is tight for binary symmetric sources. Regarding the other extreme case, a new characterization of the minimum interaction for achieving the maximum key rate (MIMK) is given, and is used to resolve a conjecture by Tyagi [1] about the MIMK for binary sources.

I. INTRODUCTION

![Interactive key generation model.](image)

Common randomness (CR) generation [2][3] concerns the task of producing a common piece of information by several terminals accessing correlated sources, possibly allowing communications among the terminals. The related key generation problem [4][5][6] imposes the additional constraint that an eavesdropper, knowing the law of the system and observing the communications but not the correlated sources, can learn almost nothing about the common information generated. The importance of CR-key generation in cryptography and information theory is well known [7][4][5][2]. From the theoretical viewpoint, they are fascinating problems because of their connections to various measures of correlation. For a two-terminal stationary memoryless source, the maximum possible rate of key equals the mutual information [5]. In the other extreme where the communication rate vanishes, the key bits per communication bit under the one-way protocol [5] is a monotonic function of the strong data processing constant [8][9]; and under the one-communicator protocol [10], a reflection of the dual convex set of the set of hypercontractive coefficients [10]. The Gács-Körner common information [11] is the maximum CR rate obtainable without any communication. The Wyner common information [12] characterizes an extreme point in the intersection between a hyperplane and the rate region in omniscient helper CR generation [2, Theorem 4.2] or key generation [10]; this can be seen from the rate regions given in [10] and by considering the Markov chain condition in the definition of Wyner common information as a linear equation of mutual information quantities.

Despite the successes in those models involving one directional communication among terminals, many basic problems have remained open in settings involving interactive communications or multi-terminals [3][6]. The existing literature has focused on achieving the maximum possible key rate. Csiszár and Narayan [6] showed that the maximum key rate equals the entropy rate of all sources minus the rate of communication for omniscience [6]. In the two terminal setting, Tyagi [1] provided a multi-letter characterization of the minimum interaction for maximum key rate (MIMK) in terms of the interactive common information [1]. However, a complete characterization of the key-communication tradeoff is more challenging because when the communication rate is not large enough for the terminals to become omniscient, it is not obvious what information they have to agree on. Indeed, as mentioned at the end of Section VII in [1], a characterization of the key rate when the communication rate is less than MIMK, along with a single-letter characterization of MIMK, remains an interesting open problem.

In this paper we consider the two-terminal interactive key generation model in Fig. 1, which is similar to [1], but we adopt completely different approaches and analyze the key-communication tradeoff rather than MIMK only. Generalizing an idea of Ma et al. [13] in interactive source coding to the non-discrete case, we introduce a preorder relation on the set of joint distributions called $XY$-absolute continuity and provide a novel characterization of the key-communication tradeoff in terms of an $XY$-concave envelope. Two extreme cases are examined closely:

- The key bits per interaction bit (KBIB) depicts the tradeoff in the regime of small rates, for which we provide exact characterizations by defining a “symmetrical strong data processing constant”. Also, using hypercontractivity and Rényi divergence, we derive an upper-bound on CR bits per interaction bit which satisfies a strong converse property and is tight for the binary symmetric source.

- We provide a new characterization for MIMK which settles a conjecture in [1]. The proof relies on a saddle point property of a certain optimization problem, which we prove in the discrete case by establishing semicontinuity and convergence properties of $XY$-concave functions.

Omitted proofs in this paper can be found in [14].

II. PRELIMINARIES

A. Problem Setup

In Figure 1 let $Q_{XY}$ be the joint distribution of the sources observed by Terminals A and B, respectively. Terminal A computes an integer $W_1 = W_1(X)$ (possibly stochastically) and sends it to B. Then B computes an integer $W_2 = W_2(W_1, Y)$ and sends it to A, and so on, for a total of $r$ rounds. Then, A and B calculate integers\(^1\) $K = K(X, W^*)$ and $\hat{K} = \hat{K}(Y, W^*)$ possibly stochastically. The objective is that $K = \hat{K}$ with high

\(^1\) $W^*_i := (W_i, W_{i+1}, \ldots, W_j)$ denotes a vector and $W^* := W^*_j$. 

---

Key Generation with Limited Interaction

Jingbo Liu  Paul Cuff  Sergio Verdú
Dept. of Electrical Eng., Princeton University, NJ 08544
{jingbo,cuff,verdu}@princeton.edu

2016 IEEE International Symposium on Information Theory

978-1-5090-1806-2/16/$31.00 ©2016 IEEE
probability and that $K$ is (almost) independent of $W^r$ which is observed by the eavesdropper. Define the secrecy index (see e.g. [15])

$$\Delta_n := \frac{1}{2} |Q_KKW_r - T_{KK}QW_r|$$

(1)

where $T_{KK}(k, k) := \frac{1}{|A|} \{k = k\}$ denotes the target distribution, and the total variation $|P - Q| := \int |dP - dQ|$.

For the asymptotic analysis of stationary memoryless sources, we substitute $X \leftarrow X^N$ and $Y \leftarrow Y^N$, where $n$ is the blocklength.

**Definition 1.** The pair $(R, R_0)$ is said to be $r$-achievable ($r \in \{1, 2, \ldots, \infty\}$) if a sequence of schemes in $r$ rounds can be designed to fulfill the following conditions:

$$\liminf_{n \to \infty} \frac{1}{n} \log |K| \geq R;$$

(2)

$$\limsup_{n \to \infty} \frac{1}{n} \log |W^r| \leq R_0,$$

(3)

and $\lim_{n \to \infty} \Delta_n = 0$ in key generation.

As long as the first order region for stationary memoryless sources and vanishing error probability are concerned, we only discuss key generation, since in this case the region for CR generation is simply a linear transformation of that of key generation (cf. [11][2]).

The set of $r$-achievable tuples for key generation is denoted by $\mathcal{R}_r(X,Y)$. Clearly, $\mathcal{R}_r(X,Y)$ is “increasing” in $r$. It is “continuous” at $r = \infty$, that is, $\mathcal{R}_\infty(X,Y)$ equals the closure of $\bigcup_{r=1}^\infty \mathcal{R}_r(X,Y)$. The less obvious “$\leq$” part is seen from the converse proof for $\mathcal{R}_\infty(X,Y)$.

Proving a multi-letter characterization of the region is tedious but rather standard. The basic idea is similar to Kaspi’s for interactive source coding [16], where each round of communication constitutes a new auxiliary random variable. To state the result conveniently, denote $Z[i] := X$ if $i$ is even and $Z[i] := Y$ if $i$ is odd. Then $\mathcal{R}_r(X,Y)$ is the closure of the set of $(R, R_0)$ satisfying

$$R \leq \sum_{i=1}^{r} I(U_i; Z[i]|U^{i-1}),$$

(4)

$$R_0 \geq \sum_{i=1}^{r} I(U_i; Z[i-1]|U^{i-1}) - \sum_{i=1}^{r} I(U_i; Z[i]|U^{i-1}),$$

(5)

for $U_1, \ldots, U_r$ such that

$$U_i = (Z[i-1], U^{i-1}) - Z[i], \quad i \in \{1, \ldots, r\}.$$  

(6)

**B. $XY$-Absolutely Continuity**

**Definition 2.** A nonnegative finite measure $\nu_{XY}$ is said to be $XY$-absolutely continuous with respect to $\mu_{XY}$, denoted by

$$\nu_{XY} \preceq_X \mu_{XY},$$

(7)

if there exists a measurable function $f$ such that

$$\nu_{XY}(A) = \int_A f(x)d\mu_{XY}(x,y)$$

(8)

for any $A \in \mathcal{F}$. Moreover, $\nu$ is said to be $XY$-absolutely continuous with respect to $\mu$, denoted simply as $\nu \preceq \mu$, if there exists a measurable function $f$ and $g$ such that

$$\nu_{XY}(A) = \int_A f(x)g(y)d\mu_{XY}(x,y).$$

(9)

Observe the similarity between the present definition of “$\preceq_X$” and absolute continuity. An equivalent definition of $\nu_{XY} \preceq_X \mu_{XY}$ is that $\nu_{XY} \ll \mu_{XY}$ and $d\nu_{XY}(x,y)$ only depends on $x$, similarly for “$\ll$”.

Clearly, $\nu \preceq \mu$ if there exists $(\theta_{XY})_{i=1}^\infty$ such that

$$\nu \preceq \theta_{i}^{\ell};$$

(10)

$$\theta_{i}^{\ell} \preceq \theta_{i}^{\ell-1}, \quad i \in \{1, \ldots, t\} \text{ is odd};$$

(11)

$$\theta_{i}^{\ell} \preceq \theta_{i}^{\ell-1}, \quad i \in \{1, \ldots, t\} \text{ is even};$$

(12)

$$\theta_{i}^{\ell} \preceq \mu.$$  

(13)

The converse is also true, and one can choose $t \leq 3$. For finite alphabets, this can be improved to $t = 1$. The latter cannot always be achieved for general alphabet because $\int f(x)d\mu_{XY}(x)$ can be infinite even if $\int f(x)g(y)d\mu_{XY}(x,y) < \infty$.

The relation $\preceq_X$ is a preorder relation on the set of nonnegative finite measures. We denote by

$$\mathcal{M}(\mu) := \{\nu: \nu \preceq_X \mu\}$$

(14)

the $X$-lower set of $\mu$ in the set of nonnegative finite measures. Similarly, $\mathcal{M}(\mu)$ is defined as the lower set of $\mu$ with respect to $\preceq_X$. Both relations also make the set of probability distributions a preordered set. Denote by $P_X(Q_{XY})$ or $\mathcal{P}(Q_{XY})$ the corresponding lower sets.

**Remark 1.** Csiszár [17] showed that the $I$-projection of $Q_{XY}$ onto the linear set of distributions having given marginal distributions, if it exists, must belong to $\mathcal{P}(Q_{XY})$. Due to this, $\mathcal{P}(Q_{XY})$ has naturally emerged in the context of hypercontractivity [18] and multiterminal hypothesis testing [19]. In both [13] and the present paper, the appearance of $\mathcal{P}(Q_{XY})$ is due to the conditioning on auxiliary random variables satisfying Markov structures, cf. (4)-(5).

The $XY$-absolute continuity framework avoids the technicality of defining a conditional distribution from a joint distribution, and allows one to extend the marginal concavity defined in [13] in the discrete setting to general alphabets:

**Definition 3.** A functional $\sigma$ on a lower set $\mathcal{P}$ is $X$-concave if for any $P_{XY}$ and $(P_{XY}', i=0,1)$ on $\mathcal{P}$ and $\alpha \in [0,1]$ satisfying

$$P_{XY}' \preceq_X P_{XY}, \quad i = 0,1;$$

(15)

$$P_{XY} = (1-\alpha)P_{XY}^0 + \alpha P_{XY}^1,$$

(16)

it holds that

$$\sigma(P_{XY}) \geq (1-\alpha)\sigma(P_{XY}^0) + \alpha \sigma(P_{XY}^1).$$

(17)

$\sigma$ is $XY$-concave if it is both $X$-concave and $Y$-concave.

**Definition 4.** Given a functional $\sigma$ on a set $\mathcal{P}$ of distributions, the functional $\sigma'$ is said to be the $X$-concave envelope of $\sigma$, denoted as $\env_{XY}(\sigma)$, if $\sigma'$ is $X$-concave and is dominated by any other $X$-concave functional which dominates $\sigma$. The $XY$-concave envelope, denoted by $\env_{XY}(\sigma)$, is defined similarly.

The existences of the $X$-concave envelope and $XY$-concave envelope follow by a monotone convergence argument.
III. A “SINGLE-LETTER” RATE REGION

Define the total sum rate
\[ S := R + R_0, \]  
and let \( S_r(X,Y) \) be the set of achievable \((S, R)\). For any \( Q_{XYU^r} \), where \( U^r \) satisfies (6), denote by \( R(Q_{XYU^r}) \) the right side of (4) and similarly for \( S(Q_{XYU^r}) \). Using \( U_1 = X - Y \) it is straightforward to check that
\[ I(X; Y) - R(Q_{XYU^r}) = I(Y; X|U_1) - \int R(Q_{XYU^r}|U_1 = u) dQ_{U_1}(u). \]  
Now the key observation is that the right side of (19) is similar to the left except that each term is conditioned on \( U_1 \), the roles of \( X \) and \( Y \) are switched, and (conditioned on \( U_1 \)) there is one fewer auxiliary. A similar relation holds for \( H(X, Y) = S(Q_{XYU^r}) \). In the case of non-discrete \((X, Y)\), we can choose a reference measure and replace the entropy/conditional entropy terms above with relative entropy/conditional relative entropy, at the cost of slightly more cumbersome notations, so there is no loss of generality with this approach.

Given \( Q_{XY} \), and \( s > 0 \), define a functional on \( P(Q_{XY}) \)
\[ \omega_0^s(P_{XY}) := sH(X, Y) - I(X; Y), \]  
where \( P_{XY} \) is \( Q_{XY} \) and \((X, Y) \sim P_{XY} \). For \( r \in \{1, \ldots \} \) define
\[ \omega_r^s := \left\{ \begin{array}{ll} \text{env}_X(\omega_{r-1}^s) & \text{if } r \text{ is odd;} \\ \text{env}_Y(\omega_{r-1}^s) & \text{if } r \text{ is even,} \end{array} \right. \]  
and define \( \omega_\infty^s \) as the \( XY \)-concave envelope of \( \omega_0^s \).

Heuristically, taking all concave envelope in (21) amounts to introducing one auxiliary random variable as in (6). Indeed, from the observation in (19) and the fact that \( S(Q_{XY}) = R(Q_{XY}) = 0 \) when \( r = 0 \), we can show the equivalent characterizations:

**Theorem 1.** \( \omega_r^s(Q_{XY}) = sH(XY) - I(X; Y) + \sup_{U^r} \left\{ R(Q_{XYU^r}) - sS(Q_{XYU^r}) \right\}, \)  
where \( U^r \) satisfies (6).

The sup in Theorem 1 equals \( \sup_{(S, R) \in S_r(X,Y)} (R - sS) \), so characterizing the closed convex set \( \mathcal{S}_r(X,Y) \) is equivalent to computing \( \omega_r^s(Q_{XY}) \) for each \( s > 0 \). The significance of Theorem 1 is that we can sometimes come up with an \( XY \)-concave function that upper-bounds \( \omega_r^s \). If the upper-bounding function evaluated at \( Q_{XY} \) also turns out to be achievable, then we can determine \( \omega_\infty^s(Q_{XY}) \). However, we are not aware of a computationally-efficient approach for computing an \( XY \)-envelope for a general \( Q_{XY} \). It is open to debate whether the characterization of \( \mathcal{R}_\infty(X,Y) \) via Theorem 1 is genuinely single-letter (see [20, P262] for one possible formal definition of single-letter characterizations in terms of the computation complexity).

IV. KEY BITS PER INTERACTION BIT

Similar to the capacity per unit cost [21] in the context of channel coding, we now consider the following fundamental limit in interactive key generation which depicts the maximum amount of key bits that can be “unlocked” by each communication bit.

**Definition 5.** For \( r \in \{1, 2, \ldots, \infty\} \), define the key bits per \( r \)-round interaction bit \( \Gamma_r(X; Y) \) as the maximum real number \( \Gamma \geq 0 \) such that there exists a sequence \((\text{indexed by } k)\) of \( r \)-round key generation schemes which fulfill the following:
\[ \lim_{k \to \infty} \inf \frac{\log |K|}{\log |W^k|} \geq \Gamma; \]  
\[ \lim_{k \to \infty} \log |K| = \infty; \]  
\[ \lim_{k \to \infty} \Delta_k = 0. \]

where \( \Delta_k \) is defined in (1). We shall use key bits per interaction bit (KBIB) as an abbreviation of \( \Gamma_\infty(X; Y) \). For stationary memoryless sources, it turns out that
\[ \Gamma_r(X; Y) = \sup \left\{ \frac{R}{R_0} : (R, R_0) \in \mathcal{R}_r(X, Y) \right\}. \]

A. Symmetrical SDPC and a Formula for \( \Gamma_\infty \)

To begin with, recall that the key bits per communication bit (cf. [8][9]) is the \( r = 1 \) special case of KBIB, and according to (4)-(5), has the formula
\[ \Gamma_1(X; Y) = \sup_{u: u \neq X - Y} \frac{I(U; Y)}{1 - s^*(X; Y)}. \]

Now let us introduce a new data processing constant defined in terms of the \( XY \)-concave envelope:

**Proposition 1.** [23] \( s^*(X; Y) \) is the infimum of \( s \) such that \( \omega^s_1(Q_{XY}) := \text{env}_X \omega^s_0(Q_{XY}) = \omega^s_0(Q_{XY}) \).

Now let us introduce a new data processing constant defined in terms of the \( XY \)-concave envelope:

**Definition 6.** The symmetrical data processing constant (SSDPC) \( s^*_\infty(X; Y) \) is the infimum of \( s > 0 \) such that
\[ \omega^s_\infty(Q_{XY}) := \text{env}_X \omega^s_0(Q_{XY}) = \omega^s_0(Q_{XY}). \]

By the conventional data processing inequality, it is immediate to show that \( s^*_\infty(X; Y) \in [0, 1] \). Moreover from (30), we obtain the symmetric property \( s^*_\infty(X; Y) = s^*_\infty(Y; X) \), in contrast to \( s^*(\cdot) \). Similarly to (28), the SSDPC is related to the operational quantities by the following:

**Theorem 2.** \( s^*_\infty(X; Y) = \sup \left\{ \frac{R}{S} : (S, R) \in \mathcal{R}_\infty(X, Y) \right\}; \)
\[ \Gamma_\infty(X; Y) = \frac{s^*_\infty(X; Y)}{1 - s^*_\infty(X; Y)}. \]

B. Maximal Correlation Upper-bound

**Definition 7.** For \((X, Y) \sim Q_{XY}\), the maximal correlation coefficient [24][25][26] is defined as
\[ \rho_m^2(X; Y) := \sup_{f,g} E[f(X)g(Y)] \]
where the sup is over measurable \( f \) and \( g \) satisfying \( E[f(X)] = E[g(Y)] = 0 \) and \( E[f^2(X)] = E[g^2(Y)] = 1 \). For any \( P_{XY} \) and \((\hat{X}, \hat{Y}) \sim P_{XY}\),
\[ \rho_m^2(\hat{X}; \hat{Y}) \leq s^*(\hat{X}; \hat{Y}) \leq s^*_\infty(\hat{X}; \hat{Y}). \]
Next we simplify the limit in (39) in the discrete case. Let
\[
\sigma_0(P_{XY}) := \begin{cases} 
H(\hat{X}, \hat{Y}) & I(\hat{X}; \hat{Y}) = 0; \\
-\infty & \text{otherwise.}
\end{cases}
\] (40)
and define \(\sigma_\infty\) as the \(XY\)-concave envelope of \(\sigma_0\). We can verify that
\[
\sigma_r(P_{XY}) = \sup_{U,V} \inf_{s \geq 0} \left\{ H(X, Y) - S(Q_{XY} U^r) - \frac{1}{s} \left[ I(X; Y) - R(Q_{XY} U^r) \right] \right\}
\] (42)
where \(\frac{1}{s}\) is a Lagrange multiplier. Next we show that in the finite alphabet case, we can switch the order of the sup and \(\inf\). As is often the case, compactness guarantees such saddle point properties. Here the proof relies on some semicontinuity and convergence properties of \(XY\)-concave envelopes in [14].

**Lemma 1.** Fix a \(Q_{XY}\) on a finite alphabet. For any \(P_{XY} \in \mathcal{P}(Q_{XY})\) and \(r \in \{0, 1, 2, 3, \ldots, \infty\},\)
\[
\sigma_r(P_{XY}) = \lim_{s \downarrow 0} \frac{1}{s} \omega^r_\infty(P_{XY}).
\] (43)
As a consequence of Lemma 1 and Theorem 6,

**Theorem 7.** If \(Q_{XY}\) is a distribution on a finite alphabet, then for \(r \in \{1, \ldots, \infty\}\)
\[
I_r(Q_{XY}) = H(Y|X) + H(X|Y) - \sigma_r(Q_{XY}).
\] (44)

**Corollary 1.** If \(X\) and \(Y\) are both binary under \(Q_{XY}\) and \(I(X; Y) > 0\), then the necessary and sufficient condition for
\[
\min \{I_1(Q_{XY}), I_1(Q_{XY})\} = I_{\infty}(Q_{XY})
\] (45)
is that either \(Q_{Y|X}\) or \(Q_{X|Y}\) is a binary symmetric channel.

**Remark 3.** Tyagi [1, Theorem 9] proved Corollary 1 in the case of binary symmetric \(Q_{XY}\) using a beautiful connection to sufficient statistics, and conjectured that (45) holds for all binary sources. Here we provide a complete answer for the binary case using an entirely different approach which resolves the conjecture in the negative.

**Proof sketch:** The sufficiency is comparatively easy (see [14]). For necessity, there are two nontrivial cases: \(|\text{supp}(Q_{XY})| = 3\) or 4. We analyze the more symmetric and interesting latter case here. There exists \(\epsilon \in (0, \frac{1}{2}) \cup (\frac{1}{2}, 1)\) such that \(\mathcal{P}(Q_{XY})\) can be parameterized by \(f, g \in [0, 1]\) as
\[
P_{XY} = \frac{1}{Z} \begin{pmatrix} 
f \bar{g} & f \bar{g} 
\bar{f} g & \bar{f} g 
\end{pmatrix}
\] (46)
where
\[
Z := f + g + \bar{\epsilon}.
\] (47)
That is, there exists a bijection from \((f, g)\) to \(P_{XY} \in \mathcal{P}(Q_{XY})\). Let \(\pi\) be such a bijection, and \(\pi^X(f, g)\) (resp. \(\pi^Y(f, g)\)) be the \(X\)-write (resp. \(Y\)-marginal) of \(\pi(f, g)\). We will sometimes write functionals like \(\sigma_r(f, g)\) instead of \(\sigma_r(\pi(f, g))\), but note that concavities are always w.r.t. to the distributions rather than \((f, g)\). Observe
\[
\pi^X(f, g) = \frac{1 - f(\epsilon \ast g)}{f(\epsilon \ast g) + g(\epsilon \ast f)}
\] (48)

\[4\]We use the notation \(\tilde{f} := 1 - f\).
so the solution of $\lambda \in [0,1]$ to

$$\lambda \pi^X(1,g) + \bar{\lambda} \pi^X(0,g) = \pi^X\left(\frac{1}{2},g\right) \tag{49}$$

is $\lambda = \epsilon \cdot g$. By definition,

$$\sigma_1\left(\frac{1}{2},g\right) = \lambda \sigma_0(0,g) + \lambda \sigma_0(1,g) \tag{50}$$

$$= \lambda h\left(\frac{\epsilon g}{\epsilon + g}\right) + \lambda h\left(\frac{g}{\epsilon + g}\right) \tag{51}$$

$$= -h(\epsilon \cdot g) + h(\epsilon) + h(g) \tag{52}$$

$$\leq h(\epsilon) \tag{53}$$

$$= \sigma_2\left(\frac{1}{2},g\right) \tag{54}$$

where (50) is because $\sigma_0(f,g) = -\infty$ for $(f,g) \in (0,1)^2$, implying that $\sigma_1(\cdot,g)$ is X-linear for $g \in (0,1)$; (53) is a strict inequality unless $g = \frac{1}{2}$; (54) is because one can verify that (see [14]) $\sigma_r\left(\frac{1}{2},g\right) = h(\epsilon)$ for $r \geq 2$.

For $g \in (0,1)$, $\sigma_1(\cdot,g)$ is X-linear whereas $\sigma_2(\cdot,g)$ is X-concave. If, additionally, $g \neq \frac{1}{2}$, then the strictness of the inequality in (53) shows that $\sigma_2\left(\frac{1}{2},g\right) \geq \sigma_2\left(\frac{1}{2},g\right) > \sigma_1\left(\frac{1}{2},g\right)$, which implies that $\sigma_2(\cdot,g) > \sigma_1(\cdot,g)$ except possibly at the endpoints (i.e. when $f \in \{0,1\}$). In sum, we have shown $\sigma_2(f,g) > \sigma_1(f,g)$ except when $f \in \{0,\frac{1}{2},1\}$ or $g \in \{0,\frac{1}{2},1\}$. In other words, if neither $Q_{Y|X}$ or $Q_{X|Y}$ is a BSC, then $\sigma_{\infty}(Q_{XY}) \geq \sigma_2(Q_{XY}) > \sigma_1(Q_{XY})$, and by symmetry, we also have $\sigma_{\infty}(Q_{XY}) \geq \sigma_2(Q_{XY}) > \sigma_1(Q_{XY})$ implying the left of (45) is strictly larger than the right. ■

VI. DISCUSSION

The tightness of Theorem 4 for BSC (Remark 2) and Corollary 1 imply that allowing interaction does not increase the key capacity for BSC at the extremes of small and large sum communication rates. Thus, it is natural to question whether the same is true for all ranges of communication rates, that is, $R_1(X,Y) = R_{\infty}(X,Y)$ for the BSC. Numerics suggest a positive answer and partial analytical results are reported in [14].

VII. ACKNOWLEDGEMENTS

This work was supported in part by NSF Grants CCF-1116013, CCF-1319299, CCF-1319304, CCF-1350595, and AFOSR FA9550-15-1-0180.

REFERENCES


