Strong secrecy for cooperative broadcast channels

Conference Paper

Author(s):
Goldfeld, Ziv; Kramer, Gerhard; Permuter, Haim H.; Cuff, Paul

Publication date:
2016

Permanent link:
https://doi.org/10.3929/ethz-a-010646754

Rights / license:
In Copyright - Non-Commercial Use Permitted
Strong Secrecy for Cooperative Broadcast Channels

Ziv Goldfeld
Ben Gurion University
gziv@post.bgu.ac.il

Gerhard Kramer
Technische Universität München
gerhard.kramer@tum.de

Haim H. Permuter
Ben Gurion University
haimp@bgu.ac.il

Paul Cuff
Princeton University
cuff@princeton.edu

Abstract—The broadcast channel (BC) with one confidential message and where the decoders cooperate via a one-sided link is considered. A messages triple with one common and two private messages is transmitted. The private message to the cooperative user is kept secret from the cooperation-aided user. An inner bound on the strong-secrecy-capacity region of the BC is derived. The inner bound is achieved by a channel-resolvability-based Marton code construction that double-bins the codebook of the secret message. Both the resolvability and the BC codes use the likelihood encoder to choose the transmitted codeword. The protocol uses the cooperation link to convey information on a portion of the non-confidential message and the common message. The outer bound is shown to be tight for the semi-deterministic and physically degraded cases.

Index Terms—Broadcast channel, resolvability, cooperation, physical-layer security, secrecy.

I. INTRODUCTION

We study broadcast channels (BCs) with one-sided decoder cooperation and one confidential message (Fig. 1). Cooperation is modeled as conferencing, i.e., information exchange via a rate-limited link that extends from one encoder (referred to as the cooperative receiver) to the other (the cooperation-aided receiver). The cooperative receiver possesses confidential information that should be kept secret from the other user.

By extending the coding schemes of Wyner [1] and Csiszár-Körner [2], multiuser settings with secrecy were extensively treated in the literature (e.g., cf. [3], [4] and references therein). These extensions use the so-called weak-secrecy metric, i.e., a vanishing information rate leakage to the eavesdropper. Observe that although the rate leakage vanishes with the blocklength, the eavesdropper can decipher an increasing number of bits from the confidential message. This drawback was highlighted in [5], which instead advocated a secrecy measure referred to as strong-secrecy. We consider strong-secrecy by relying on work by Csiszár [6] and Hayashi [7] to relate the coding mechanism for secrecy to channel-resolvability rather than channel-capacity (see also [8]).

We first consider a state-dependent channel over which an encoder with non-causal access to the channel state sequence transmits a codeword and aims to make the conditional probability mass function (PMF) of the output given the state resemble a conditional product PMF. The underlying codebook coordinates the transmitted codeword with the state sequence by means of multicoding, i.e., by associating with every message a bin that contains enough codewords to ensure joint encoding (similar to a Gelfand-Pinsker codebook). Most encoders use joint typicality tests to determine the transmitted codeword. We instead adopt the likelihood encoder recently proposed in [9].

Our code ensures that the relation between its codewords correspond to the relation between the channel states and the input in the corresponding resolvability problem. A double-binning of the confidential message codebook allows joint encoding (outer bin layer) and preserves confidentiality (inner bin layer). The sizes of the inner bins are determined by conditions on the rates in our resolvability lemma. To match the conditions of the lemma, we use the likelihood encoder as the multicoding mechanism. Our protocol uses the cooperation link to convey information on a public message that is assembled from parts of the non-confidential message and the common message. The outer bound is shown to be tight for semi-deterministic (SD) and physically-degraded (PD) BCs. As a special case, our results captures the strong-secrecy-capacity region of the SD-BC (without cooperation) where the message to the deterministic user is confidential - an unsolved problem that has merit on its own.

We focus on the cooperative scenario to shed light on the interaction between user cooperation and secure communication. Without secrecy constraints, the public message comprises parts of both private messages [10]. This difference is fundamental when coding for secrecy because a cooperation protocol that shares information about the confidential message violates the secrecy constraint. Since the protocol relies on the cooperative user decoding the public message before sharing it, this difference results in an additional loss in the rate of the confidential message (on top of the loss due to secrecy). The restricted cooperation protocol encapsulates the tension between secrecy and cooperation.

To the best of our knowledge, we present here the first resolvability-based Marton code. This is also a first demonstration of the likelihood encoder’s usefulness in the context of secrecy for channel coding problems. From a broader perspective, our resolvability lemma is a tool for upgrading weak-secrecy to strong-secrecy in settings with Marton coding. The reader is referred to [11] for discussion and examples that...
are not presented here due to space limitations.

This paper is organized as follows. Sections II and III provide preliminaries and state a central lemma, respectively. In section IV we introduce the cooperative BC and state our inner bound and capacity results. Proofs are given in Section V.

II. Notations and Preliminaries

We use notation from [11, Section II]. The total variational (TV) distance between two PMFs \( P \) and \( Q \) is

\[
\| P - Q \| = \frac{1}{2} \sum_{x \in \mathcal{X}} | P(x) - Q(x) |
\]

(1)

and the corresponding relative entropy is

\[
D(P||Q) = \sum_{x \in \text{supp}(P)} P(x) \log \left( \frac{P(x)}{Q(x)} \right).
\]

(2)

Remark 1: Pinsker’s inequality shows that relative entropy is larger than TV distance. The reverse relation is not generally true, but there is a “reverse” Pinsker inequality for long sequences of independently and identically distributed (i.i.d.) random variables. That is, if \( P \ll Q \) (i.e., \( P \) is absolutely continuous with respect to \( Q \)), and \( Q \) is an i.i.d. discrete distribution of variables, then

\[
D(P||Q) \in \mathcal{O} \left( \left[ n + \log \frac{1}{\| P - Q \|} \right] \| P - Q \| \right),
\]

(3)

as \( \| P - Q \| \) goes to zero and \( n \) goes to infinity (see [12, Equation (29)]). In particular, (3) implies that an exponential decay of the TV distance produces an exponential decay of the informational divergence with the same exponent.

III. Conditional Relative Entropy Approximation

Consider a state-dependent discrete memoryless channel (DMC) over which an encoder with non-causal access to the i.i.d. state sequence transmits a codeword (Fig. 2). Each channel state is a pair \( (S_0, S) \) of random variables drawn according to \( Q_{S_0,S} \). The encoder superimposes its codeword on \( S_0 \) and then uses the likelihood encoder with respect to \( S \) to choose the channel input sequence. The conditional PMF of the channel output, given the states, should approximate a conditional product distribution in terms of unnormalized relative entropy.

\[ f(n) \in \mathcal{O}(g(n)) \text{ means that } f(n) \leq k \cdot g(n), \text{ for some } k \text{ independent of } n \text{ and sufficiently large } n. \]

As shown in Section V-B, we construct a channel-resolvability-based Marton code for the cooperative BC in which the relations between the codewords correspond to those between the channel states and its input in the resolvability setup. The Marton code combines superposition coding and binning, hence the different roles the the state sequences \( S_0 \) and \( S \) play in the subsequent resolvability codebook. Lemma 1 is then invoked to achieve strong-secrecy.

A. Problem Definition

The random variable \( W \) is uniformly distributed over \( W = \{1 : 2^nR\} \) and is independent of \( (S_0, S) \sim Q_{S_0,S} \). For any fixed \( Q_{U|S_0,S} \), consider the following coding scheme.

Codebook Construction: For every \( s_0 \in S_0 \) generate a codebook \( B_0(s_0) \) that comprises \( 2^nR \) bins, each associated with a different message \( w \in W \) and contains \( 2^nR \) u-codewords that are drawn according to \( Q_{U|S_0=s_0} \). Let \( B_n = \{ B_n(s_0) \}_{s_0 \in S_0} \) denote this collection of codebooks and denote the codewords in the bin associated with \( w \in W \) by \( \{ u(s_0, w, i, B_n) \}_{i \in \mathcal{I}} \), where \( \mathcal{I} = \{1 : 2^nR\} \).

Encoding and Induced PMF: The encoding uses the likelihood encoder described by conditional PMF

\[
f^{(\text{LE})}(i|w, s_0, B_n) = \sum_{i \in \mathcal{I}} Q_{U|S_0=S}(s_0, u(w, i, B_n, s_0)),
\]

(4)

Upon observing \( (w, s_0, s) \), an index \( i \in \mathcal{I} \) is drawn according to (4). The codeword \( u(s_0, w, i, B_n) \) is passed through the DMC \( Q_{U|S_0,S} \). The distribution induced by the resolvability codebook \( B_n \) is

\[
P(B_n)(s_0, w, i, u, v) \approx Q_{S_0,S}^{(n)}(s_0, s) 2^{-nR} f^{(\text{LE})}(i|w, s_0, s, B_n)
\]

(5)

Furthermore, we use \( B_n \) to denote a random codebook that adheres to the above construction.

Lemma 1 (Sufficient Conditions for Approximation) For any \( Q_{S_0,S}, Q_{U|S_0,S} \) and \( Q_{U|S_0,S} \). If \( (R', R') \in \mathbb{R}_+^2 \) satisfies

\[
R' > I(U; S|S_0)
\]

(6a)

then

\[
E_{B_n} D \left( P^{(B_n)}_{U|S_0,S} \left| Q^{(n)}_{S_0,S} \right| Q^{(n)}_{S_0,S} \right) \xrightarrow{n \to \infty} 0.
\]

(7)

The proof of Lemma 1 shows that the TV distance decays exponentially fast with the blocklength \( n \). By Remark 1 this implies an exponential decay of the desired relative entropy. See Section V-A for details.

Another useful property is that the chosen \( u \)-codeword is jointly letter-typical with \( (S_0, S) \) with high probability.

Lemma 2 (Typical with High Probability) If \( (R', R') \in \mathbb{R}_+^2 \) satisfies (6), then for any \( w \in W \) and \( \epsilon > 0 \), we have

\[
E_{B_n} P \left( (S_0, S, U(S_0, w, I, B_n)) \notin T^{(n)}(Q_{S_0,S}, U) \right) \xrightarrow{n \to \infty} 0,
\]

(8)
where $I$ is a random variable that represents the index chosen by the likelihood encoder $f^{(LE)}$.

The proof of Lemma 2 relies on [9, Property 1]: for any $\epsilon > 0$ and $f : X \rightarrow R$ bounded by $b > 0$, if $\left| \|A\| - \|B\| \right| < \epsilon$ then $\mathbb{E}[f(X) - \mathbb{E}[f(X)] < \epsilon b$. The proposition follows by taking $f(S_0, S, U) \triangleq 1\{ (S_0, S, U) \notin T_{i_n}(Q_{s_0, s, u}) \}$ and using (7).

IV. Cooperative Broadcast Channels with One Confidential Message

A. Problem Definition

The discrete memoryless broadcast channel (DMBC) with cooperation and one confidential message is illustrated in Fig. 1. The channel has one sender and two receivers. The sender chooses a triple $(m_0, m_1, m_2)$ of indices uniformly and independently from the set $[1 : 2^nR_0] \times [1 : 2^nR_1] \times [1 : 2^nR_2]$ and maps them to a sequence $x \in \mathcal{X}^n$, which is the channel input. The sequence $x$ is transmitted over a BC with transition probability $Q_{Y_1, Y_2|x}$. If $Q_{Y_1, Y_2|x}$ factors as $Q_{Y_1|X}Q_{Y_2|X}$ or $Q_{Y_1, X}Q_{Y_2, X}$, then we call the BC SD or PD, respectively. The output sequence $y_j \in \mathcal{Y}^n_j$, where $j = 1, 2$, is received by decoder $j$. Decoder $j$ produces a pair of estimates $(\hat{m}_{0j}, \hat{m}_{1j})$ of $(m_0, m_1)$. Furthermore, the message $m_2$ is to be kept secret from Decoder 2. There is a one-sided noiseless cooperation link of rate $R_{12}$ from Decoder 1 to Decoder 2. By conveying a message $m_{12} \in [1 : 2^{nR_{12}}]$ over this link, Decoder 1 can share $m_{12} = m_2$ with Decoder 2 information about $y_1$, $(\hat{m}_0^1, \hat{m}_1^1)$, or both.

Definition 1 (Code) An $(n, R_1, R_0, R_1, R_2)$ code $C_n$ for the BC with cooperation and one confidential message has: (i) Four message sets $\mathcal{M}_{12} = [1 : 2^{nR_{12}}]$ and $\mathcal{M}_j = [1 : 2^{nR_j}]$, for $j = 0, 1, 2$; (ii) A stochastic encoder described by a stochastic matrix $f^{(LE)} : \mathcal{M}_0 \times \mathcal{M}_1 \times \mathcal{M}_2 \rightarrow \mathcal{X}^n$; (iii) A decoder cooperation function $f_{12} : \mathcal{Y}_1^n \rightarrow \mathcal{M}_{12}$; (iv) Two decoding functions $\phi_1 : \mathcal{Y}_1^n \rightarrow \mathcal{M}_0 \times \mathcal{M}_1$ and $\phi_2 : \mathcal{Y}_2^n \times \mathcal{M}_{12} \rightarrow \mathcal{M}_0 \times \mathcal{M}_2$.

Definition 2 (Error Probability) The average error probability for an $(n, R_1, R_0, R_1, R_2)$ code $C_n$ is

$$P_e(C_n) = P_{C_n}\left( (M_0^{(1)}, M_2^{(2)}, M_1^{(3)}), (M_0, M_1, M_2) \right) \neq (M_0, M_0, M_1, M_2),$$

where $P_{C_n}(\cdot)$ means that the probability is calculated with respect to the joint PMF induced by $C_n$. Furthermore, $(M_0^{(1)}, M_1^{(3)}) = \phi_1(Y_1^n)$ and $(M_0^{(2)}, M_2^{(3)}) = \phi_2(Y_2^n, f_{12}(Y_1^n))$.

The information leakage at receiver 2 is measured by $L(C_n) = I_{C_n}(M_1; M_2, Y_2)$, which is also calculated with respect to PMF induced by $C_n$.

Definition 3 (Achievability) A rate tuple $(R_{12}, R_0, R_1, R_2) \in \mathbb{R}_+^4$ is achievable if for any $\epsilon > 0$ there is an $(n, R_{12}, R_0, R_1, R_2)$ code $C_n$ with $P_e(C_n) \leq \epsilon$ and $L(C_n) \leq \epsilon$, for any $n$ sufficiently large.

The strong-secrecy-capacity region $C_S$ is the closure of the set of the achievable rates.

B. Strong-Secrecy-Capacity Bounds and Results

We state an inner bound on the strong-secrecy-capacity region $C_S$ of a cooperative BC with one confidential message.

Theorem 3 (Inner Bound) Let $R_i$ be the closure of the union of the rate tuples $(R_{12}, R_0, R_1, R_2) \in \mathbb{R}_+^4$ satisfying:

$$R_1 \leq I(Y_1; Y_0, U_1) - I(U_1; U_2, Y_2|U_0)$$
$$R_0 + R_1 \leq I(U_0, U_1; Y_1) - I(U_1; U_2, Y_2|U_0)$$
$$R_0 + R_2 \leq I(U_0, U_2; Y_2) + I(U_1; Y_1)$$
$$\sum_{j=0,1,2} R_j \leq I(U_0, U_1; Y_1) + I(U_2; Y_2|U_0) - I(U_1; U_2, Y_2|U_0),$$

(8)

where the union is over all PMFs $Q_{u_0, u_1, u_2, x}Q_{y_1, y_2|x}$. Then the inclusion $R_i \subseteq C_S$ holds.

The proof of Theorem 3 relies on a channel-resolvability-based Marton code and is given in Section V-B. The inner bound in Theorem 3 is tight for SD and PD BCs.

Theorem 4 (Secrecy-Capacity for SD-BC) The strong-secrecy-capacity region $C_S^{(SD)}$ of a cooperative SD-BC with one confidential message is the closure of the union of rate tuples $(R_{12}, R_0, R_1, R_2) \in \mathbb{R}_+^4$ satisfying:

$$R_1 \leq H(Y_1|W, V, Y_2)$$
$$R_0 + R_1 \leq H(Y_1|W, V, Y_2) + I(W; Y_1)$$
$$R_0 + R_2 \leq I(W; Y_2) + R_{12}$$
$$\sum_{j=0,1,2} R_j \leq H(Y_1|W, V, Y_2) + I(W; Y_2|W) + I(W; Y_1),$$

(9)

where the union is over all $Q_{w,y_1,x}Q_{y_2|x}$ with $Y_1 = f(X)$.

The direct part of Theorem 4 follows from Theorem 3 by setting $U_0 = W$, $U_1 = Y_1$, and $U_2 = V$.

Theorem 5 (Secrecy-Capacity for PD-BC) The strong-secrecy-capacity region $C_S^{(PD)}$ of a cooperative PD-BC with one confidential message is the closure of the union of rate tuples $(R_{12}, R_0, R_1, R_2) \in \mathbb{R}_+^4$ satisfying:

$$R_1 \leq I(X; Y_1|W) - I(X; Y_2|W)$$
$$R_0 + R_2 \leq I(W; Y_2) + R_{12}$$
$$\sum_{j=0,1,2} R_j \leq I(X; Y_1) + I(Y_2|X) - I(X; Y_2|W),$$

(10)

where the union is over all $Q_{w,x}Q_{y_1|x}Q_{y_2|x}$ with $Y_1 = f(X)$.

The achievability of $C_S^{(PD)}$ follows by setting $U_0 = W, U_1 = X$ and $U_2 = 0$ in Theorem 3.

Remark 2 (Converse) The converse proofs for Theorems 4 and 5 are omitted due to space limitations (see [11] for details). We remark that we used two distinct converse proofs. In the converse of Theorem 4, the fourth bound in (9) does not involve $R_{12}$. Since the auxiliary random variable $W$ contains $M_1$. With respect to this choice of $W$, showing that $W - X - (Y_1, Y_2)$ forms a Markov chain relies heavily on the SD property of the channel. For the PD-BC, however, such...
an auxiliary is not feasible as it violates the Markov relation \( W - X - Y_1 - Y_2 \) induced by the channel. To circumvent this, in the converse of Theorem 5 we define \( W \), without \( M_1 \) and use the structure of the channel to keep \( R_{12} \) appearing in the third rate bound in (10). Specifically, this argument relies on the relation \( R_{12} = f_{12}(Y_1) \) and that \( Y_2 \) is a degraded version of \( Y_1 \), implying that all three messages \((M_0, M_1, M_2)\) are reliably decodable from \( Y_1 \) only.

V. PROOFS

A. Proof of Lemma 1

Note that the factorization of \( P^{(B_n)} \) from (5) implies that \( P^{(B_n)}_{S_0; S} = Q^S_{S_0; S} \). Therefore, to establish Lemma 1 we show that

\[
\mathbb{E}_a \left[ D \left( P^{(B_n)}_{S_0; S; V} \right) \right] \rightarrow 0 \quad (n \rightarrow \infty).
\]

(11)

For every fixed codebook \( B_n, P^{(B_n)}_{S_0; S; V} \) is absolutely continuous with respect to \( Q^n_{S; S; V} \). Combining this Remark 1, a sufficient condition for (11) is that

\[
\mathbb{E}_a \left[ D \left( P^{(B_n)}_{S_0; S; V} - Q^n_{S_0; S; V} \right) \right] \rightarrow 0 \quad (n \rightarrow \infty).
\]

(12)

To evaluate the TV distance in (12), define the ideal PMF of \((S_0, S, W, I, U, V)\) as

\[
\Gamma^{(B_n)}(s_0, w, i, u, s, v) = \frac{Q^n_{S_0; s}(s_0) 2^{-n(K + R')}}{u(s_0, w, i, b_n) = u} \times Q^n_{S;V(U,S_0; s|u, s_0)} V(U,S_0; s|v, u, s_0)
\]

with respect to the same codebook \( B_n \) as \( P^{(B_n)} \). Note, however, that \( \Gamma \) describes an encoding process where the choice of the \( u \)-codeword from a certain bin is uniform, as opposed to \( P \) that uses the likelihood encoder. Furthermore, the structure of \( \Gamma \) implies that the sequence \( s \) is generated by feeding \( s_0 \) and the chosen \( u \)-codeword into a DMC \( Q^n_{S;V(U,S_0; s)} \).

Using the TV distance triangle inequality, we upper bound the left-hand side of (12) by

\[
\mathbb{E}_a \left[ D \left( P^{(B_n)}_{S_0; S; V} - \Gamma^{(B_n)}_{S_0; S; V} \right) \right] \geq \mathbb{E}_a \left[ D \left( \Gamma^{(B_n)}_{S_0; S; V} - Q^n_{S_0; S; V} \right) \right].
\]

(13)

By [12, Corollary VII.5], the second expected TV distance decays exponentially fast as \( n \rightarrow \infty \) if (6b) holds.

For the first term in (13), we use the following relations between \( \Gamma \) and \( P \). For every fixed codebook \( B_n \), we have

\[
\Gamma^{(B_n)}_{I|W, S_0, S} = \frac{P^{(B_n)}_{I|W, S_0, S}}{P^{(B_n)}_{I|W, S_0}} \quad \Gamma^{(B_n)}_{U|I, W, S_0, S} = \frac{P^{(B_n)}_{U|I, W, S_0, S}}{P^{(B_n)}_{U|I, W, S_0}} \quad \Gamma^{(B_n)}_{V|U, I, W, S_0, S} = \frac{P^{(B_n)}_{V|U, I, W, S_0, S}}{P^{(B_n)}_{V|U, I, W, S_0}}
\]

Consequently, basic properties of the TV distance and the symmetry in constructing \( B_n \) give

\[
\mathbb{E}_a \left[ D \left( P^{(B_n)}_{S_0; S; V} - \Gamma^{(B_n)}_{S_0; S; V} \right) \right] \leq \mathbb{E}_a \left[ D \left( Q^n_{S_0; S} - \Gamma^{(B_n)}_{S_0; S} \right) | W = 1 \right].
\]

(14)

Invoking [12, Corollary VII.5] once more, (6a) implies that

\[
\mathbb{E}_a \left[ D \left( Q^n_{S_0; S} - \Gamma^{(B_n)}_{S_0; S} \right) | W = 1 \right] \rightarrow 0 \quad (n \rightarrow \infty)
\]

B. Proof of Theorem 3

Codebook Generation: Split \( M_2 \) into two independent parts \((M_{20}, M_{22})\) with rates \( R_{20} \) and \( R_{22} \) that satisfy \( R_0 = R_{20} + R_{22} \), and alphabets \( M_{20} \) and \( M_{22} \), respectively. \( M_{20} \) is referred to as a public message while \( M_{22} \) denotes private message number \( 2 \). We also use \( M_p \) \( \cong M_{0} \times M_{20} \) and \( R_p \cong R_0 + R_{20} \). Let \( W \) be a random variable uniformly distributed over \( \mathcal{W} = \{1 : 2^{nR_0} \} \) and independent of \((M_0, M_1, M_2)\).

Generate a public message codebook \( C_0 \) that comprises \( 2^{nR_0} \) \( u_0 \)-codewords \( u_0(m_p, C_0) \), \( m_p \in \mathcal{M}_p \), drawn according to \( Q^n_{U_0} \). Randomly and uniformly partition \( C_0 \) into \( 2^{nR_0} \) bins \( B(m_1) \), where \( m_1 \in \mathcal{M}_{12} \).

For each \( u_0(m_p, C_0) \), \( m_p \in \mathcal{M}_p \), generate a codebook \( C_2(m_p) \) that comprises \( 2^{nR_2} \) \( u_2 \)-codewords \( u_2 \), each drawn according to \( Q^n_{U_2|U_0, C_0} \) independent of all the other \( u_1 \)-codewords. Label these codewords as \( u_1(m_p, m_{11}, i, w, C_1) \), where \( (m_{11}, i, w) \in \mathcal{M}_1 \times \mathcal{I} \times \mathcal{W} \) and \( T \cong \{1 : 2^{nR_1} \} \).

For each \( u_0(m_p, C_0) \), \( m_p \in \mathcal{M}_p \), also generate a codebook \( C_2(m_p) \) that comprises \( 2^{nR_2} \) \( u_2 \)-codewords, each associated with a private message \( m_{22} \in \mathcal{M}_{22} \). Each \( u_2 \)-codeword is drawn according to \( Q^n_{U_2|U_{0}, C_0} \) independent of all the other \( u_2 \)-codewords. Denote \( C_2(m_p) \cong \{u_2(m_p, m_{22}, C_2)\}_{m_{22}} \in \mathcal{M}_{22} \).

The channel input \( x \) associated with a triple \((u_0, u_1, u_2)\) is generated according to \( Q^n_{X|U_0, U_1, U_2} \).

Encoding: To transmit a triple \((m_0, m_{11}, m_{22})\), the encoder transforms it into the triple \((m_0, m_{11}, m_{22})\), and draws \( W \) uniformly over \( \mathcal{W} \). Then, an index \( i \in \mathcal{I} \) is chosen by the likelihood encoder described in (15) at the top of the next page. The corresponding \( x \) is transmitted over the BC.

Decoding and Cooperation: Decoder 1: Searches for a unique triple \((m_{22}, m_{11}, w) \in \mathcal{M}_0 \times \mathcal{M}_1 \times \mathcal{W} \) for which there is an index \( i \in \mathcal{I} \) such that \((u_0(m_p, C_0), u_1(m_p, m_{11}, i, w, C_1), y_1) \in \mathcal{T}_0 \). If such unique triple is found, \((\hat{m}_0, \hat{m}_{11})\) is declared as the decoded message pair.

Cooperation: Having \((\hat{m}_0, \hat{m}_{11}, i, w) \), Decoder 2 sends the bin number of \( u_0(\hat{m}_0, C_0) \) to Decoder 2 via the cooperation link.

Decoder 2: Upon receiving \((\hat{m}_{12}, y_2) \), Decoder 2 searches for a unique pair \((\hat{m}_0, \hat{m}_{22}) \in \mathcal{M}_0 \times \mathcal{M}_{22} \) such that \((u_0(\hat{m}_0, C_0), \hat{u}_2(m_{22}, C_2, y_2) \in \mathcal{T}_0 \). If such a unique pair is found, then \((\hat{m}_0, \hat{m}_{22})\) is declared as the decoded message.

The error probability analysis, which we omit due to space limitations, uses Lemma 2 to first show that the above encoding process result in \( u_{0r}, u_{1r}, u_{2r} \) and \( x \)-sequences that are jointly typical. Then, by standard joint-typicality decoding arguments, reliability is established provided that

\[
R' > I(U_1; U_2|U_0) \quad R' + \hat{R} > I(U_1; U_2, Y_2|U_0)
\]

3The subsequent notations for codebooks omit the blocklength \( n \).
\[ f_{BC}^{(LE)}(i|w, u_0(m_p, C_0), u_2(m_p, m_{22}, C_2), C_1) = \frac{Q_{Y_2|U_1, U_0}^{n}(u_2(m_p, m_{22}, C_2)|u_1(m_p, m_1, i, w, C_1), u_0(m_p, C_0))}{\sum_{i' \in \mathcal{I}} Q_{Y_2|U_1, U_0}^{n}(u_2(m_p, m_{22}, C_2)|u_1(m_p, m_1, i', w, C_1), u_0(m_p, C_0))} . \]  

(15)

\[ I(M_1; M_{12}, Y_2|C) \leq \mathbb{E}_{C} D \left( P_{Y_2|U_1}^{(C)}(M_1, M_{12}, U_1, U_2) \| P_{Y_2|U_1}^{(C)}(M_1, M_{12}, U_1, U_2) \right) \]  

(16)

Security Analysis: Let \( \mathcal{C}_0 \) be random variables that represents a random public message codebook. Furthermore, let \( C_j \triangleq \{C_j(m_p)\}_{m_p \in \mathcal{A}_j} \), for \( j = 1, 2 \), be the private message codebooks 1 and 2, and \( C_1 \) and \( C_2 \) be the corresponding random codebooks. With some abuse of notation, we also use \( C \triangleq (C_0, C_1, C_2) \) and \( C \triangleq (C_0, C_1, C_2) \). Moreover, when clear from the context, we omit the functional dependencies of the messages, \( j = 0, 1, 2 \), on the corresponding indices and codebooks, e.g., we write \( U_2 \) instead of \( U_2(M_p, M_{22}, C_2) \).

We start with the upper bound in (17) at the top of the page. Step (a) uses the independence of the messages \( (M_p, M_1, M_{22}) \), the deterministic dependence of \( (M_{12}, U_0, U_2) \) on \( (M_p, M_{22}) \) and the relative entropy chain rule; (b) follows by the symmetry of the code construction with respect to the messages. To justify (c), first note that for any \( C = (C_0, C_1, C_2) \), the conditional relative entropy is an expectation of unconditional relative entropies with respect to

\[ P_{Y_2}^{(C)}(u_0, u_2 | 1, 1, 1) = \mathbb{E}_{C_0, C_1} \left\{ \mathbb{I} \left( (u_0(1, C_0), u_2(1, 1, C_2) = (u_0, u_2)) \right) \right\} . \]  

(18)

Combining (18) with the law of total expectation (conditioning the inside information on \( C_0 \)) and noting that \( (U_0(1, C_0), U_2(1, 1, C_2)) \) is independent of \( C_0 \), gives (c); finally, (d) relies on the coding PMF being \( Q_{Y_2|U_0}^{n} \).

Remark 3 The main differences between the coding schemes for the cooperative BC with one confidential message and the same channel without secrecy [10] are threefold. First, a randomizer \( W \) is used in the secrecy-achieving scheme. Second, the cooperation message \( M_{12} \) depends on \( M_2 \) rather than on the pair \( (M_{10}, M_{20}) \) (\( M_{10} \) refers to the public part of the message \( M_1 \)). The second difference is because conveying an \( M_{12} \) that holds any \( M_1 \) (in the form of its public part \( M_{10} \)) violates the secrecy requirement. Finally, a prefix channel \( Q_{X|U_0, U_1, U_2}^{n} \) is used to optimize randomness and, in turn, to conceal \( M_1 \) from the 2nd receiver.

Acknowledgements

The work of Z. Goldfeld and H. H. Permuter was supported by the Israel Science Foundation (grant no. 684/11), an ERC starting grant and the Cyber Security Research Grant at Ben-Gurion University of the Negev. The work of G. Kramer was supported by an Alexander von Humboldt Professorship endowed by the German Federal Ministry of Education and Research. The work of P. Cuff was supported by the National Science Foundation (grant CCF-1350595) and the Air Force Office of Scientific Research (grant FA9550-15-1-0180).

References


