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 is achieved 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 inner 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 receiver (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 portions of the non-confidential message and the common message. The inner 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
\[ \|P - Q\| = \frac{1}{2} \sum_{x \in \mathcal{X}} |P(x) - Q(x)| \]
and the corresponding relative entropy is
\[ D(P||Q) = \sum_{x \in \text{supp}(P)} P(x) \log \left( \frac{P(x)}{Q(x)} \right). \]

**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\(^1\)
\[ D(P||Q) \in \mathcal{O} \left( \left[ n + \log \frac{1}{\|P - Q\|} \right] \|P - Q\| \right), \tag{3} \]
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.

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 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 $(S_0, S)$ and $Q_{S_0,S}$. 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 $B_n(s_0)$ 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 $Q_{U|S_0=s_0} \leq \prod_{i=1}^n Q_{U_i|S_0=s_0}$. 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 $\{u(s_0, w, i, B_n)\}_{i \in I}$, where $I = [1 : 2^nR]$.

**Encoding and Induced PMF:** The encoding uses the likelihood encoder described by conditional PMF
\[ f^{(LE)}(i|w, s_0, u, B_n) = Q^n_{U|S_0}(s_0|u(s_0, w, i, B_n), s_0) \sum_{\mathcal{V} \in \mathcal{V}_{S_0}} Q^n_{V|U,S_0}(v|u(s_0, w, i, B_n), s_0). \tag{4} \]

Upon observing $(w, s_0, s)$, an index $i \in I$ is drawn according to (4). The codeword $u(s_0, w, i, B_n)$ is passed through the DMC $Q_{V|U,S_0,S}^n$. The distribution induced by the resolvability codebook $B_n$ is
\[ p^{(BS)}(s, w, i, u, v) = Q^n_{S_0,S}(s, w, i) 2^{-nR} f^{(LE)}(i|w, s_0, u, B_n) \times E_{\{u(s_0, w, i, B_n)\}} Q^n_{V|U,S_0,S}(v|u(s_0, w, i, B_n), s_0). \tag{5} \]

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 $Q_{V|U,S_0,S}$, if $(R, R') \in \mathbb{R}^2_+$ satisfies
\[ R' > I(U; S|S_0) \tag{6a} \]
\[ R' + R > I(U; S, V|S_0) \tag{6b} \]
then
\[ E_{B_n} D \left( Q_{V|U,S_0,S}^n \left| Q_{S_0,S}^n \right| B_n \right) \xrightarrow{n \to \infty} 0. \tag{7} \]

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
\[ E_{B_n} P \left( \left( S_0, S, U(s_0, w, I, B_n) \notin T_{\epsilon}^n \right) \left| Q_{S_0,S}^n \right| B_n \right) \xrightarrow{n \to \infty} 0, \]

---

\(^1 f(n) \in \mathcal{O}(g(n))\) means that $f(n) \leq k \cdot g(n)$, for some $k$ independent of $n$ and sufficiently large $n$. 
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 \( f : X \to \mathbb{R} \) bounded by \( b > 0 \), if \( \| f \|_{1} < \epsilon b \).

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 \( \mathcal{C}^{(SD)} \) of a cooperative SD-BC with one confidential message is the closure of the union of rate tuples \((R_{12}, R_{01}, R_{12}) \in \mathbb{R}_{+}^{3}\) satisfying:

\[
R_{1} \leq I(Y_{1}; Y_{0} | W, V, Y_{2})
\]

\[
R_{0} + R_{1} \leq I(U_{0}; Y_{1} | Y_{2}) - I(U_{1}; U_{2}, Y_{2} | U_{0})
\]

\[
R_{0} + R_{2} \leq I(U_{0}; U_{2} | U_{2} | Y_{2}) + R_{12}
\]

\[
\sum_{j=0,1,2} R_{j} \leq I(U_{0}; U_{1}; Y_{1}) + I(U_{2}; Y_{2} | U_{0}) - I(U_{1}; U_{2}; Y_{2} | U_{0}),
\]

where the union is over all PMFs \( Q_{U_{0}, U_{1}, U_{2}, X, Q_{Y_{1}, Y_{2}} | X} \) Then the inclusion \( \mathcal{I}_{1} \subseteq \mathcal{C}^{(SD)} \) 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.
an auxiliary is not feasible as it violates the Markov relation
W - X = Y1 - Y2 induced by the channel. To circumvent this,
in the converse of Theorem 5 we define W, without M12 and
use the structure of the channel to keep R12 from appearing in
the third rate bound in (10). Specifically, this argument relies on
the relation M12 = \( f_{12}(Y_1) \) and that Y2 is a degraded
version of Y1, implying that all three messages (M0, M1, M2)
are reliably decodable from Y1 only.

V. PROOFS

A. Proof of Lemma 1

Note that the factorization of \( P(S_n) \) from (5) implies
that \( P(S_n) = Q(S_n). \) Therefore, to establish Lemma 1 we show that

\[
\mathbb{E}_{S_n} D \left( P(S_n) \bigg| \frac{Q(S_n) + \epsilon}{Q(S_n)} \bigg) \xrightarrow{n \to \infty} 0. \tag{11} \]

\* For every fixed codebook \( B_n \), \( \gamma(S_n) \) is absolutely continuous with respect to \( Q(S_n) \). Combining this with Remark 1, a sufficient condition for (11) is that

\[
\mathbb{E}_{S_n} \left[ \frac{P(S_n)}{Q(S_n)} - \gamma(S_n) \right] \xrightarrow{n \to \infty} 0. \tag{12} \]

To evaluate the TV distance in (12), define the ideal PMF
\( \gamma(S_n) \) associated with a triple \( (m_1, m_2, m_3) \),
such that comprises \( m_1 \) of the other \( u_1 \) codewords.
Label these codewords \( \gamma_1(m_1, m_2, i, w, C_1) \), where \( \gamma(m_1, i, w) \in M_1 \times I \times W \) and \( I \)
\( \equiv \left[ 1, 2^{nR_1} \right] \). For each \( u_0(m_p, C_0) \), \( m_p \in \Phi \), generate a codebook
\( \gamma_2(m_p) \) that comprises \( 2^{nR_2} u_2 \)-codewords, each
associated with a private message \( m_2 \in M_2 \). Each \( u_2-
\text{codeword is drawn according to } Q_{\gamma_2}(u_2) \) independent
of all the other \( u_1 \text{-codewords. Label these codewords as}
\gamma_2(m_p, m_1, i, w, C_1) \), where \( \gamma(m_1, i, w) \in M_1 \times I \times W \) and \( I \)
\( \equiv \left[ 1, 2^{nR_1} \right] \). The channel input \( x \) associated with a triple \( (u_0, u_1, u_2) \) is generated according to \( Q_{\gamma_2}(u_2) \times M_1 \times M_2 \).

Decoding and Cooperation: Decoder 1: Searches for a unique triple \( (m_p, m_1, m_2) \),\nand draws W uniformly over \( W \). Then, an index \( i \) is chosen by the
likelihood encoder described in (15) at the top of the next
generation decoding arguments. reliability is established provided that

\[
R' > I(U_1; U_2|U_0) \quad \text{and } R' > I(U_1; Y_2|U_0) \tag{16} \]

\* The subsequent notations for codebooks omit the blocklength \( n \).
\[ f^{(1E)}_{BC}(i|w, u_0(m_p, C_0), u_2(m_p, m_{22}, C_2), C_1) = \frac{Q^n_{U_2(U_1, U_0)}(u_2(m_p, m_{22}, C_2)|u_1(m_p, m_1, i, w, C_1), u_0(m_p, C_0))}{\sum_{i' \in \mathcal{I}} Q^n_{U_2(U_1, U_0)}(u_2(m_p, m_{22}, C_2)|u_1(m_p, m_1, i', w, C_1), u_0(m_p, C_0))}. \]

\[ I(M_1: M_{12}, Y_2|C) \leq \mathbb{E}_{C} D \left( P^{(C)}_{Y_2|M_p, M_1, M_{22}, U_0, U_2} \|| Q^n_{U_2(U_1, U_0)} \right) \\( a \) \\
\leq \mathbb{E}_{C} D \left( P^{(C)}_{Y_2|M_p=1, M_1=1, M_{22}=1, U_0, U_2} \|| Q^n_{U_2(U_1, U_0)} \right) \\( b \) \\
= \sum_{u_0, u_2} \mathbb{E}_{C_1} \left[ D \left( P^{(C)}_{Y_2|M_p=1, M_1=1, M_{22}=1, U_0=u_0, U_2=u_2} \|| Q^n_{U_2(U_1, U_0)} \right) \right] \\( c \) \\
= \mathbb{E}_{C_1} D \left( P^{(C)}_{Y_2|M_p=1, M_1=1, M_{22}=1, U_1, U_2} \|| Q^n_{U_2(U_1, U_0)} \right) \\( d \). \]

\[ R_1 + R' + \hat{R} < I(U_1; Y_1|U_0) \]
\[ R_0 + R_{20} + R_1 + R' + \hat{R} < I(U_0; U_1; Y_1) \]
\[ R_{22} < I(U_2; Y_2|U_0) \]
\[ R_0 + R_2 - R_{22} < I(U_0; U_2; Y_2). \]

Security Analysis: Let \( C_0 \) be random variables that represents a random public message codebook. Furthermore, let \( C_j \triangleq \{ C_j(m) \}_{m \in \mathcal{A}_j} \), 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 message codewords, \( j = 0, 1, 2 \), on the corresponding indices and codebooks, e.g., we write \( U_2 \) instead of \( U_2(M_{12}, M_{22}, C_2) \).

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 \( C = C_0 \), the conditional relative entropy with respect to \( P^{(C)}(u_0, u_2|1, 1, 1) = I \left( \{ u_0(1, C_0), u_2(1, 1, C_2) = (u_0, u_2) \} \right). \]

Combining (18) with the law of total expectation (conditioning the inner expectation on \( C_1 \)) and noting that \( (U_0(1, C_0), U_2(1, 1, C_2)) \) is independent of \( C_1 \), gives (c); finally, (d) relies on the coding PMF being \( P^n_{U_0, U_2} \).

Note that the code construction and the RHS of (17) fall within the framework of Lemma 1. Invoking the lemma, the first two rate bounds in (16) ensure that the RHS of (17) converges to 0 as \( n \to \infty \), which establishes strong secrecy. By standard existence arguments and Fourier-Motzkin elimination applied to (16), the achievability of \( R^*_2 \) is established.

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 \( Q^n_{X|U_1, U_2} \) 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