Broadcast Channels with Privacy Leakage Constraints

Ziv Goldfeld, Gerhard Kramer and Haim H. Permuter

Abstract

The broadcast channel (BC) with one common and two private messages with leakage constraints is studied, where leakage refers to the normalized mutual information between a message and a channel symbol string. Each private message is destined for a different user and the leakage to the other receiver must satisfy a constraint. This model captures several scenarios concerning secrecy, i.e., when both, either or neither of the private messages are secret. Inner and outer bounds on the leakage-capacity region are derived. Without leakage constraints the inner bound recovers Marton's region and the outer bound reduces to the UVW-outer bound. The bounds match for semi-deterministic (SD) and physically degraded (PD) BCs, as well as for BCs with a degraded message set. The leakage-capacity regions of the SD-BC and the BC with a degraded message set recover past results for different secrecy scenarios. A Blackwell BC example illustrates the results and shows how its leakage-capacity region changes from the capacity region without secrecy to the secrecy-capacity regions for different secrecy scenarios.

Index Terms

Broadcast channel, Marton's inner bound, Privacy Leakage, Secrecy, Physical-layer Security.

I. Introduction

Confidential and non-confidential messages are often transmitted over the same channel. However, the underlying principles for constructing codes without and with secrecy are different. Without secrecy constraints, codes should use all available channel resources to reliably convey information to the destinations. The presence of confidential messages, on the other hand, requires that some resources are allocated to preserve secrecy. We study relationships between the coding strategies and the fundamental limits of communication with and without secrecy. To this end we incorporate secret and non-secret transmissions over a two-user broadcast channel (BC) by considering the BC with privacy leakage constraints (Fig. 1).

Information theoretic secrecy was introduced by Shannon [1] who studied communication between a source and a receiver in the presence of an eavesdropper. Wyner modeled secret communication over noisy channels when he

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 Center (CSRC) 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.

Z. Goldfeld and H. H. Permuter are with the Department of Electrical and Computer Engineering, Ben-Gurion University of the Negev, Beer-Sheva, Israel (gziv@post.bgu.ac.il, haimp@bgu.ac.il). G. Kramer is with the Institute for Communications Engineering, Technische Universität München, Munich D-80333, Germany (gerhard.kramer@tum.de).

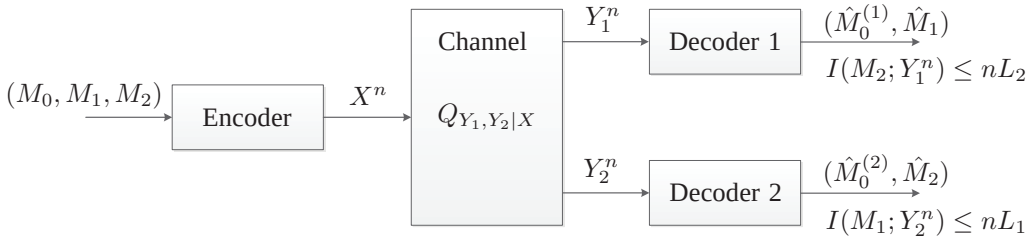

Fig. 1: BC with privacy leakage constraints.

introduced the degraded wiretap channel (WTC) and derived its secrecy-capacity region [2]. Csiszár and Körner [3] extended Wyner's result to a general BC where the source also transmits a common message to both users. The development of wireless communication, whose inherent open nature makes it vulnerable to security attacks, has inspired a growing interest in understanding the fundamental limits of secure communication.

Multiuser settings with secrecy were extensively treated in the literature. Broadcast and interference channels with two confidential messages were studied in [4], where inner and outer bounds on the secrecy-capacity region of both problems were derived. The secrecy-capacity region for the semi-deterministic (SD) BC was established in [5]. The capacity region of a SD-BC where only the message of the stochastic user is kept secret from the deterministic user was derived in [6]. The opposite case, i.e., when the message of the deterministic user is confidential was solved in [7]. Secret communication over multiuser channels was considered in [8], where the authors derive inner and outer bounds on the rate-equivocation region of the relay-BC (RBC) with one or two confidential messages. Gaussian multiple-input multiple-output (MIMO) BCs and WTCs were studied in [9]–[14], while [15]–[17] focused on BCs with an eavesdropper as an external entity from which all messages are kept secret.

We study a two-user BC over which a common message for both users and a pair of private messages, each destined for a different user, are transmitted. A limited amount of rate of each private message may be leaked to the opposite receiver. The leaked rate is quantified as the normalized mutual information between the message of interest and the channel output sequence at the opposite user. Setting either leakage to zero or infinity reduces the problem to the case where the associated message is confidential or non-confidential, respectively. Thus, our problem setting captures as special cases four scenarios concerning secrecy, i.e., when both, either or neither of the private messages are secret. We derive novel inner and outer bounds on the leakage-capacity region of the BC. The bounds are tight for SD-BCs, physically degraded (PD) BCs, and BCs with a degraded message set, thus characterizing their leakage-capacity regions, which were not known before. Furthermore, we derive a condition for identifying the privacy leakage threshold values above which the inner bound saturates.

Various past results are captured as special cases. By taking the leakage thresholds to infinity, our inner bound recovers Marton's inner bound with a common message [18], which is optimal for every BC with a known capacity region. Making the leakage constraint inactive in our outer bound recovers the UVW-outer bound [19] or the New-Jersey outer bound [20]. These bounds are at least as good as previously known bounds (see [21], [22] and [23]).

The leakage-capacity region of the SD-BC reduces to each of the regions in [5]–[7] and [24] by discarding the common message and choosing the leakage constraints appropriately. The capacity result also recovers the optimal regions for the BC with confidential messages [3] and the BC with a degraded message set (without secrecy) [25].

Our code construction splits each private message into a *public* and a *private* part. The public parts along with the common message constitute a public message that is decoded by both users, and therefore, each public part is leaked to the opposite receiver by default. The codebooks of the private parts are double-binned to allow joint encoding and to control the amount of rate leaked from each private part. The bin sizes are chosen to satisfy the total leakage constraints. Our coding scheme is essentially a Marton code with an additional layer of bins, whose sizes correspond to the amount of leakage; the larger these extra bins are, the smaller the leakage. The resulting achievable region is simplified using the Fourier-Motzkin elimination for information theory (FME-IT) software [26]. The outer bound is established by using telescoping identities [27]. A Blackwell BC (BWC) [28], [29] illustrates the results and visualizes the transition of the leakage-capacity region from the capacity region without secrecy to the secrecy-capacity regions for different secrecy scenarios.

This paper is organized as follows. In Section II we describe the BC with privacy leakage constraints. In Section III, we state inner and outer bounds on the leakage-capacity region and characterize the leakage-capacity regions for the SD-BC, the BC with a degraded massage set and the PD-BC. Section IV discusses past results that are captured within our framework. In Section V we study a BWC example and visualise the results, while Section VI provides proofs. Finally, Section VII summarizes the main achievements and insights of this work.

II. Notations and Problem Definition

We use the following notations. Given two real numbers a, b, we denote by $[a:b]$ the set of integers $\big\{n \in \mathbb{N}\big|\lceil a\rceil \leq n \leq \lfloor b\rfloor\big\}$. We define $\mathbb{R}_+ = \{x \in \mathbb{R}|x \geq 0\}$. Calligraphic letters denote discrete sets, e.g., $\mathcal{X}$, while the cardinality of a set $\mathcal{X}$ is denoted by $|\mathcal{X}|$. $\mathcal{X}^n$ stands for the n-fold Cartesian product of $\mathcal{X}$. An element of $\mathcal{X}^n$ is denoted by $x^n = (x_1, x_2, \ldots, x_n)$, and its substrings as $x_i^j = (x_i, x_{i+1}, \ldots, x_j)$; when $i = 1$, the subscript is omitted. Whenever the dimension n is clear from the context, vectors (or sequences) are denoted by boldface letters, e.g., $\mathbf{x}$.

Let $\big(\Omega, \mathcal{F}, \mathbb{P}\big)$ be a probability space, where Ω is the sample space, $\mathcal{F}$ is the σ-algebra and $\mathbb{P}$ is the probability measure. Random variables over $\big(\Omega, \mathcal{F}, \mathbb{P}\big)$ are denoted by uppercase letters, e.g., X, with conventions for random vectors similar to those for deterministic sequences. Namely, X_i^j represents the sequence of random variables $(X_i, X_{i+1}, \ldots, X_j)$, while $\mathbf{X}$ stands for X^n. The probability of an event $\mathcal{A} \in \mathcal{F}$ is denoted by $\mathbb{P}(\mathcal{A})$, while $\mathbb{P}(\mathcal{A}\big|\mathcal{B})$ denotes conditional probability of $\mathcal{A}$ given $\mathcal{B}$. We use $\mathbb{1}_{\mathcal{A}}$ to denote the indicator function of $\mathcal{A}$. The set of all probability mass functions (PMFs) on a finite set $\mathcal{X}$ is denoted by $\mathcal{P}(\mathcal{X})$. PMFs are denoted by the capital letter P, with a subscript that identifies the random variable and its possible conditioning. For example, for two random variables X and Y we use P_X, $P_{X,Y}$ and $P_{X|Y}$ to denote, respectively, the marginal PMF of X, the joint PMF of (X, Y) and the conditional PMF of X given Y. In particular, $P_{X|Y}$ represents the stochastic matrix whose elements are given by $P_{X|Y}(x|y) = \mathbb{P}\big(X = x|Y = y\big)$. We omit subscripts if the arguments of the PMF are

lowercase versions of the random variables. The support of a PMF P and the expectation of a random variable X are denoted by $\text{supp}(P)$ and $\mathbb{E}X$, respectively.

For a discrete measurable space $(\Omega, \mathcal{F})$, a PMF $Q \in \mathcal{P}(\Omega)$ gives rise to a probability measure on $(\Omega, \mathcal{F})$, which we denote by $\mathbb{P}_Q$; accordingly, $\mathbb{P}_Q\big(\mathcal{A}\big) = \sum_{\omega \in \mathcal{A}} Q(\omega)$, for every $\mathcal{A} \in \mathcal{F}$. For a sequence of random variables X^n we also use the following: If the entries of X^n are drawn in an independent and identically distributed (i.i.d.) manner according to P_X, then for every $\mathbf{x} \in \mathcal{X}^n$ we have $P_{X^n}(\mathbf{x}) = \prod_{i=1}^n P_X(x_i)$ and we write $P_{X^n}(\mathbf{x}) = P_X^n(\mathbf{x})$. Similarly, if for every $(\mathbf{x}, \mathbf{y}) \in \mathcal{X}^n \times \mathcal{Y}^n$ we have $P_{Y^n|X^n}(\mathbf{y}|\mathbf{x}) = \prod_{i=1}^n P_{Y|X}(y_i|x_i)$, then we write $P_{Y^n|X^n}(\mathbf{y}|\mathbf{x}) = P_{Y|X}^n(\mathbf{y}|\mathbf{x})$. We often use Q_X^n or $Q_{Y|X}^n$ when referring to an i.i.d. sequence of random variables. The conditional product PMF $Q_{Y|X}^n$ given a specific sequence $\mathbf{x} \in \mathcal{X}^n$ is denoted by $Q_{Y|X=\mathbf{x}}^n$.

The empirical PMF $\nu_{\mathbf{x}}$ of a sequence $\mathbf{x} \in \mathcal{X}^n$ is

$$\nu_{\mathbf{x}}(a) \triangleq \frac{N(a|\mathbf{x})}{n} \tag{1}$$

where $N(a|\mathbf{x}) = \sum_{i=1}^n \mathbb{1}_{\{x_i = a\}}$. We use $\mathcal{T}_\epsilon^n(P_X)$ to denote the set of letter-typical sequences of length n with respect to the PMF P_X and the non-negative number ϵ [30, Ch. 3], [31], i.e., we have

$$\mathcal{T}_\epsilon^n(P_X) = \Big\{\mathbf{x} \in \mathcal{X}^n : \big|\nu_{\mathbf{x}}(a) - P_X(a)\big| \leq \epsilon P_X(a),\ \forall a \in \mathcal{X}\Big\}. \tag{2}$$

The BC with privacy leakage constraints is illustrated in Fig. 1. The channel has one sender and two receivers. The sender randomly chooses a triple (m_0, m_1, m_2) of indices uniformly and independently from the set $\big[1 : 2^{nR_0}\big] \times \big[1 : 2^{nR_1}\big] \times \big[1 : 2^{nR_2}\big]$ and maps them to a sequence $\mathbf{x} \in \mathcal{X}^n$, which is the channel input. The sequence $\mathbf{x}$ is transmitted over a BC with transition probability $Q_{Y_1,Y_2|X}$. If the channel transition matrix factors as $\mathbb{1}_{\{Y_1 = f(X)\}} Q_{Y_2|X}$, for some function $f : \mathcal{X} \to \mathcal{Y}_1$, or as $Q_{Y_1|X} Q_{Y_2|Y_1}$ we call the BC SD or PD, respectively. The output sequence $\mathbf{y}_j \in \mathcal{Y}_j^n$, where $j = 1, 2$, is received by decoder j. Decoder j produces a pair of estimates $\big(\hat{m}_0^{(j)}, \hat{m}_j\big)$ of (m_0, m_j).

Definition 1 (Code Description) *An (n, R_0, R_1, R_2) code $\mathcal{C}_n$ for the BC with leakage constraints is defined with respect to the three message sets $\mathcal{M}_j \triangleq \big[1 : 2^{nR_j}\big]$, $j = 0, 1, 2$, and has:*

1) *A stochastic encoder that is described by a mapping $f_{\text{E}} : \mathcal{M}_0 \times \mathcal{M}_1 \times \mathcal{M}_2 \to \mathcal{P}(\mathcal{X}^n)$.*
2) *Two decoding functions, $\phi_j : \mathcal{Y}_j^n \to \big(\mathcal{M}_0 \times \mathcal{M}_j\big) \cup \{e\}$, for $j = 1, 2$, where $e \notin \mathcal{M}_k$, for $k = 0, 1, 2$, is an error symbol.*

Denote the set of all (n, R_0, R_1, R_2) codes for the BC with leakage constraints by $\mathfrak{C}_n$ and let $\mathbb{C}_n$ be a random variable with alphabet $\mathfrak{C}_n$ distributed according to $P_{\mathbb{C}_n} \in \mathcal{P}(\mathfrak{C}_n)$. The probability measure $\mathbb{P}$ used throughout this work is induced by an underlying PMF on $\mathfrak{C}_n \times \mathcal{M}_0 \times \mathcal{M}_1 \times \mathcal{M}_2 \times \mathcal{X}^n \times \mathcal{Y}_1^n \times \mathcal{Y}_2^n \times \mathcal{M}_0 \times \mathcal{M}_1 \times \mathcal{M}_0 \times \mathcal{M}_2$ given by

$$P\left(\mathcal{C}_n, m_0, m_1, m_2, \mathbf{x}, \mathbf{y}_1, \mathbf{y}_2, \hat{m}_0^{(1)}, \hat{m}_1, \hat{m}_0^{(2)}, \hat{m}_2\right) = P_{\mathbb{C}_n}(\mathcal{C}_n) P^{(\mathcal{C}_n)}\Big(m_0, m_1, m_2, \mathbf{x}, \mathbf{y}_1, \mathbf{y}_2, \hat{m}_0^{(1)}, \hat{m}_1, \hat{m}_0^{(2)}, \hat{m}_2\Big), \tag{3a}$$

where

$$P^{(\mathcal{C}_n)}\Big(m_0, m_1, m_2, \mathbf{x}, \mathbf{y}_1, \mathbf{y}_2, \hat{m}_0^{(1)}, \hat{m}_1, \hat{m}_0^{(2)}, \hat{m}_2\Big) = \frac{1}{|\mathcal{M}_0||\mathcal{M}_1||\mathcal{M}_2|} f_{\mathrm{E}}(\mathbf{x}|m_0, m_1, m_2) Q^n_{Y_1,Y_2|X}(\mathbf{y}_1, \mathbf{y}_2|\mathbf{x}) \mathbb{1}_{\bigcap_{j=1,2}\left\{(\hat{m}_0^{(j)}, m_j) = \phi(\mathbf{y}_j)\right\}}. \quad (3b)$$

is defined by the code $\mathcal{C}_n = (f_{\mathrm{E}}, \phi_1, \phi_2)$.

Definition 2 (Error Probability) *The average error probability for an (n, R_0, R_1, R_2) code $\mathcal{C}_n$ is*

$$P_e(\mathcal{C}_n) = \mathbb{P}\Big((\hat{M}_0^{(1)}, \hat{M}_0^{(2)}, \hat{M}_1, \hat{M}_2) \neq (M_0, M_0, M_1, M_2)\Big|\mathbb{C}_n = \mathcal{C}_n\Big) = \frac{1}{|\mathcal{M}_0||\mathcal{M}_1||\mathcal{M}_2|} \sum_{\substack{(m_0,m_1,m_2)\\ \in \mathcal{M}_0\times\mathcal{M}_2\times\mathcal{M}_2}} \sum_{\substack{(\mathbf{y}_1,\mathbf{y}_2)\in\mathcal{Y}_1^n\times\mathcal{Y}_2^n:\\ \phi_1(\mathbf{y}_1)\neq(m_0,m_1) \text{ or}\\ \phi_2(\mathbf{y}_1)\neq(m_0,m_2)}} Q^n_{Y_1,Y_2|X}\big(\mathbf{y}_1, \mathbf{y}_2\big|f_{\mathrm{E}}(m_0, m_1, m_2)\big), \quad (4a)$$

The average error probability for receiver $j = 1, 2$ is

$$P_{e,j}(\mathcal{C}_n) = \mathbb{P}_{\mathcal{C}_n}\Big((\hat{M}_0^{(j)}, \hat{M}_j) \neq (M_0, M_j)\Big|\mathbb{C}_n = \mathcal{C}_n\Big). \quad (4b)$$

Definition 3 (Information Leakage) *The information leakage of M_1 to receiver 2 under an (n, R_0, R_1, R_2) code $\mathcal{C}_n$ is*

$$L_1(\mathcal{C}_n) = \frac{1}{n} I(M_1; Y_2^n|\mathbb{C}_n = \mathcal{C}_n). \quad (5a)$$

Similarly, the information leakage of M_2 to receiver 1 under $\mathcal{C}_n$ is

$$L_2(\mathcal{C}_n) = \frac{1}{n} I(M_2; Y_1^n|\mathbb{C}_n = \mathcal{C}_n). \quad (5b)$$

When the aforementioned quantities are subsequently used, the conditioning of $\mathcal{C}_n$ may be omitted when it is clear from the context.

Definition 4 (Achievable Rates) *Let $(L_1, L_2) \in \mathbb{R}_+^2$. A rate triple $(R_0, R_1, R_2) \in \mathbb{R}_+^3$ is (L_1, L_2)-achievable if for any $\epsilon, \xi_1, \xi_2 > 0$ there is a sufficiently large n and an (n, R_0, R_1, R_2) code $\mathcal{C}_n$ such that*

$$P_e(\mathcal{C}_n) \leq \epsilon \quad (6a)$$

$$L_1(\mathcal{C}_n) \leq L_1 + \xi_1 \quad (6b)$$

$$L_2(\mathcal{C}_n) \leq L_2 + \xi_2. \quad (6c)$$

The (L_1, L_2)-*leakage-capacity region* $\mathcal{C}(L_1, L_2)$ is the closure of the set of the (L_1, L_2)-achievable rates.

Remark 1 (Inactive Leakage Constraints) *Setting $L_j = R_j$, for $j = 1, 2$, makes* (6b)-(6c) *inactive and reduces the BC with privacy leakage constraints to the classic BC with a common message. This is a simple consequence*

of the non-negativity of entropy, which implies that for any $\mathcal{C}_n \in \mathfrak{C}_n$

$$I(M_1; Y_2^n|\mathbb{C}_n = \mathcal{C}_n) \leq H(M_1) = nR_1 \tag{7}$$

(respectively, $I(M_2; Y_1^n|\mathbb{C}_n = \mathcal{C}_n) \leq nR_2$*) always holds. To simplify notation, when we henceforth refer to leakage threshold values under which* (6b)-(6c) *are automatically satisfied, we write* $L_j \to \infty$*,* $j = 1, 2$*.*

III. Leakage-Capacity Results

This section states novel inner and outer bounds on the (L_1, L_2)-leakage-capacity region $\mathcal{C}(L_1, L_2)$ of a BC with privacy leakage constraints. These bounds match for SD-BCs, BCs with a degraded message set and PD-BCs, which characterizes the leakage-capacity regions for these three cases. We start with the inner bound.

Theorem 1 (Inner Bound) *Let* $(L_1, L_2) \in \mathbb{R}_+^2$ *and* $\mathcal{R}_{\mathrm{I}}(L_1, L_2)$ *be the closure of the union of rate triples* $(R_0, R_1, R_2) \in \mathbb{R}_+^3$ *satisfying:*

$$R_1 \leq I(U_1; Y_1|U_0) - I(U_1; U_2|U_0) - I(U_1; Y_2|U_0, U_2) + L_1 \tag{8a}$$

$$R_0 + R_1 \leq I(U_0, U_1; Y_1) - I(U_1; U_2|U_0) - I(U_1; Y_2|U_0, U_2) + L_1 \tag{8b}$$

$$R_0 + R_1 \leq I(U_0, U_1; Y_1) \tag{8c}$$

$$R_2 \leq I(U_2; Y_2|U_0) - I(U_1; U_2|U_0) - I(U_2; Y_1|U_0, U_1) + L_2 \tag{8d}$$

$$R_0 + R_2 \leq I(U_0, U_2; Y_2) - I(U_1; U_2|U_0) - I(U_2; Y_1|U_0, U_1) + L_2 \tag{8e}$$

$$R_0 + R_2 \leq I(U_0, U_2; Y_2) \tag{8f}$$

$$R_0 + R_1 + R_2 \leq I(U_0, U_1; Y_1) + I(U_2; Y_2|U_0) - I(U_1; U_2|U_0) - I(U_1; Y_2|U_0, U_2) + L_1 \tag{8g}$$

$$R_0 + R_1 + R_2 \leq I(U_1; Y_1|U_0) + I(U_0, U_2; Y_2) - I(U_1; U_2|U_0) - I(U_2; Y_1|U_0, U_1) + L_2 \tag{8h}$$

$$R_0 + R_1 + R_2 \leq I(U_1; Y_1|U_0) + I(U_2; Y_2|U_0) - I(U_1; U_2|U_0) + \min\left\{I(U_0; Y_1), I(U_0; Y_2)\right\} \tag{8i}$$

$$2R_0 + R_1 + R_2 \leq I(U_0, U_1; Y_1) + I(U_0, U_2; Y_2) - I(U_1; U_2|U_0) \tag{8j}$$

where the union is over all PMFs $P_{U_0,U_1,U_2,X} Q_{Y_1,Y_2|X}$*. The following inclusion holds:*

$$\mathcal{R}_{\mathrm{I}}(L_1, L_2) \subseteq \mathcal{C}(L_1, L_2). \tag{9}$$

The proof of Theorem 1 is given in Section VI-A and relies on a leakage-adaptive Marton-like code construction. Rate-splitting is first used to decompose each private message M_j, $j = 1, 2$, into a public part M_{0j} and a private part M_{jj}. A Marton code with an extra layer of bins is then constructed while treating (M_0, M_{10}, M_{20}) as a public message and M_{jj}, for $j = 1, 2$, as private message j. The double-binning of the private message codebooks permits joint encoding (outer layer) and to control the total rate leakage to the other user (inner layer). The leakage analysis takes into account the rate leaked due to the decoding of the public message by both users. Also, additional leakage occurs due to the joint encoding process, which introduces correlation between the private message codewords.

Accounting for the latter is the main difficulty in the leakage analysis; we treat this by relating the bin sizes in the inner and outer coding layers.

Remark 2 *The region $\mathcal{R}_{\mathrm{I}}(L_1, L_2)$ recovers Marton's inner bound for BCs with a common message [18, Theorem 5]. By taking $L_1, L_2 \to \infty$, the rate bounds in* (8a)-(8b), (8d)-(8e) *and* (8g)-(8h) *are redundant. The remaining bounds coincide with those defining Marton's region. A full discussion on the special cases of $\mathcal{R}_{\mathrm{I}}(L_1, L_2)$ is given in Section IV-D.*

The following corollary states a sufficient condition on the leakage thresholds L_1 and L_2 to become inactive in $\mathcal{R}_{\mathrm{I}}(L_1, L_2)$ from Theorem 1 with $R_0 = 0$ (i.e., when no common message is present), when evaluated under a certain input distribution $P_{U_0,U_1,U_2,X} \in \mathcal{P}(\mathcal{U}_0 \times \mathcal{U}_1 \times \mathcal{U}_2 \times \mathcal{X})$. To state the result, let $\tilde{\mathcal{R}}_{\mathrm{I}}(L_1, L_2, P_{U_0,U_1,U_2,X})$ denote the set of rate pairs $(R_1, R_2) \in \mathbb{R}_+^2$ satisfying (8) with $R_0 = 0$ and when the mutual information terms are calculated with respect to $P_{U_0,U_1,U_2,X} Q_{Y_1,Y_2|X}$. Accordingly,

$$\tilde{\mathcal{R}}_{\mathrm{I}}(L_1, L_2) \triangleq \bigcup_{\substack{P_{U_0,U_1,U_2,X}: \\ (U_0,U_1,U_2)-X-(Y_1,Y_2)}} \tilde{\mathcal{R}}_{\mathrm{I}}(L_1, L_2, P_{U_0,U_1,U_2,X}) \tag{10}$$

corresponds to the region obtained by setting $R_0 = 0$ in $\mathcal{R}_{\mathrm{I}}(L_1, L_2)$.

Corollary 2 (Inactive Leakage Constraints) *Let $(L_1, L_2) \in \mathbb{R}_+^2$ and $P_{U_0,U_1,U_2,X} \in \mathcal{P}(\mathcal{U}_0 \times \mathcal{U}_1 \times \mathcal{U}_2 \times \mathcal{X})$. For $j = 1, 2$ define*

$$L_j^\star(P_{U_0,U_1,U_2,X}) = I(U_0; Y_j) + I(U_j; U_{\bar{j}}, Y_{\bar{j}} | U_0), \tag{11}$$

where $\bar{j} = j + (-1)^{j+1}$. We have the following results:

1) *If $L_1 \geq L_1^\star(P_{U_0,U_1,U_2,X})$ then $\tilde{\mathcal{R}}_{\mathrm{I}}(L_1, L_2, P_{U_0,U_1,U_2,X}) = \tilde{\mathcal{R}}_{\mathrm{I}}(\infty, L_2, P_{U_0,U_1,U_2,X})$.*
2) *If $L_2 \geq L_2^\star(P_{U_0,U_1,U_2,X})$ then $\tilde{\mathcal{R}}_{\mathrm{I}}(L_1, L_2, P_{U_0,U_1,U_2,X}) = \tilde{\mathcal{R}}_{\mathrm{I}}(L_1, \infty, P_{U_0,U_1,U_2,X})$.*
3) *If $L_j \geq L_j^\star(P_{U_0,U_1,U_2,X})$, for $j = 1, 2$, then $\tilde{\mathcal{R}}_{\mathrm{I}}(L_1, L_2, P_{U_0,U_1,U_2,X}) = \tilde{\mathcal{R}}_{\mathrm{I}}(\infty, \infty, P_{U_0,U_1,U_2,X})$.*

For the proof of Corollary 2 see Section VI-B. According to the above, if any of the leakage thresholds L_j, $j = 1, 2$ surpasses the critical value from (11), the corresponding inner bound remains unchanged if L_j is further increased, and is therefore equivalent to the region where $L_j \to \infty$.

Remark 3 *Corollary 2 specifies a condition for L_1 and/or L_2 being inactive for each input probability. Getting a condition for the inactivity of the thresholds with respect to the entire region $\tilde{\mathcal{R}}_{\mathrm{I}}(L_1, L_2)$ from* (10) *is a more challenging task. Identifying such a condition involves identifying which input distributions achieve the boundary of $\tilde{\mathcal{R}}_{\mathrm{I}}(L_1, L_2)$. Although, in some communication scenarios this identification is possible (e.g., for the MIMO Gaussian BC with or without secrecy requirements the boundary achieving distributions are Gaussian vectors [32]–[36]), but the structure of the optimizing distribution is unknown in general.*

The merit of Corollary 2 is reflected when explicitly calculating $\tilde{\mathcal{R}}_{\mathrm{I}}(L_1, L_2)$ for a given BC. One can then identify the optimizing distribution (e.g., by means of an analytical characterization or via an exhaustive search), and can,

in turn, calculate the maximum of $L_j^\star(P_{U_0,U_1,U_2,X})$ over those distributions. Denoting by $L_j^\star$ this maximal value, if $L_j < L_j^\star$ then increasing L_j will further shrink the region. If, on the other hand, $L_j \geq L_j^\star$, then the region remains unchanged even if L_j further grows. This notion is demonstrated in Section V, where we calculate the (L_1, L_2)-leakage-capacity region of the Blackwell BC.

Next, we state an outer bound on $\mathcal{C}(L_1, L_2)$. A proof of Theorem 3 is given in Section VI-C.

Theorem 3 (Outer Bound) *Let $(L_1, L_2) \in \mathbb{R}_+^2$ and $\mathcal{R}_{\mathrm{O}}(L_1, L_2)$ be the closure of the union of rate triples $(R_0, R_1, R_2) \in \mathbb{R}_+^3$ satisfying:*

$$R_0 \leq \min\big\{I(W;Y_1), I(W;Y_2)\big\} \tag{12a}$$

$$R_1 \leq I(U;Y_1|W,V) - I(U;Y_2|W,V) + L_1 \tag{12b}$$

$$R_1 \leq I(U;Y_1|W) - I(U;Y_2|W) + L_1 \tag{12c}$$

$$R_0 + R_1 \leq I(U;Y_1|W) + \min\big\{I(W;Y_1), I(W;Y_2)\big\} \tag{12d}$$

$$R_2 \leq I(V;Y_2|W,U) - I(V;Y_1|W,U) + L_2 \tag{12e}$$

$$R_2 \leq I(V;Y_2|W) - I(V;Y_1|W) + L_2 \tag{12f}$$

$$R_0 + R_2 \leq I(V;Y_2|W) + \min\big\{I(W;Y_1), I(W;Y_2)\big\} \tag{12g}$$

$$R_0 + R_1 + R_2 \leq I(U;Y_1|W,V) + I(V;Y_2|W) + \min\big\{I(W;Y_1), I(W;Y_2)\big\} \tag{12h}$$

$$R_0 + R_1 + R_2 \leq I(U;Y_1|W) + I(V;Y_2|W,U) + \min\big\{I(W;Y_1), I(W;Y_2)\big\} \tag{12i}$$

where the union is over all PMFs $P_{W,U,V}P_{X|U,V}Q_{Y_1,Y_2|X}$. $\mathcal{R}_{\mathrm{O}}(L_1, L_2)$ is convex. The following inclusion holds:

$$\mathcal{C}(L_1, L_2) \subseteq \mathcal{R}_{\mathrm{O}}(L_1, L_2). \tag{13}$$

The derivation of the outer bound uses telescoping identities (cf., e.g., [27, Eqs. (9) and (11)]) that result in a relatively concise proof.

Remark 4 *The region $\mathcal{R}_{\mathrm{O}}(L_1, L_2)$ recovers the UVW-outer bound from [19, Bound 2], which is equivalent to the New-Jersey outer bound [20]. This follows by setting $L_1, L_2 \to \infty$ into $\mathcal{R}_{\mathrm{O}}(L_1, L_2)$, which makes (12b)-(12c) and (12e)-(12f) inactive.*

The inner and outer bounds in Theorems 1 and 3 are tight for SD-BCs and give rise to the following theorem.

Theorem 4 (Leakage-Capacity for SD-BC) *Let $(L_1, L_2) \in \mathbb{R}_+^2$. The (L_1, L_2)-leakage-capacity region $\mathcal{C}_{\mathrm{SD}}(L_1, L_2)$ of a SD-BC $\mathbb{1}_{\{Y_1 = f(X)\}}Q_{Y_2|X}$ with privacy leakage constraints is the closure of the union of rate triples $(R_0, R_1, R_2) \in \mathbb{R}_+^3$ satisfying:*

$$R_1 \leq H(Y_1|W,V,Y_2) + L_1 \tag{14a}$$

$$R_0 + R_1 \le H(Y_1|W,V,Y_2) + I(W;Y_1) + L_1 \tag{14b}$$

$$R_0 + R_1 \le H(Y_1) \tag{14c}$$

$$R_2 \le I(V;Y_2|W) - I(V;Y_1|W) + L_2 \tag{14d}$$

$$R_0 + R_2 \le I(W,V;Y_2) - I(V;Y_1|W) + L_2 \tag{14e}$$

$$R_0 + R_2 \le I(W,V;Y_2) \tag{14f}$$

$$R_0 + R_1 + R_2 \le H(Y_1|W,V,Y_2) + I(V;Y_2|W) + I(W;Y_1) + L_1 \tag{14g}$$

$$R_0 + R_1 + R_2 \le H(Y_1|W,V) + I(V;Y_2|W) + \min\left\{I(W;Y_1), I(W;Y_2)\right\} \tag{14h}$$

$$2R_0 + R_1 + R_2 \le H(Y_1|W,V) + I(W,V;Y_2) + I(W;Y_1) \tag{14i}$$

where the union is over all PMFs $P_{W,V,Y_1,X}Q_{Y_2|X}$ for which $Y_1 = f(X)$. $\mathcal{C}_{\mathrm{SD}}(L_1,L_2)$ is convex.

The direct part of Theorem 4 follows from Theorem 1 by taking $U_0 = W$, $U_1 = Y_1$ and $U_2 = V$, while Theorem 3 is used for the converse. See Section VI-D for the full details.

Remark 5 *By taking $L_j = 0$, the SD-BC with leakage constraints is reduced to the corresponding BC in which M_j is secret. Similarly, setting $L_j \to \infty$ results in the problem without a secrecy constraint on M_j. All four cases of the SD-BC concerning secrecy (i.e., when neither, either or both messages are secret) are solved and their solutions are retrieved from $\mathcal{C}_{\mathrm{SD}}(L_1,L_2)$ by inserting the appropriate values of L_j, $j = 1,2$. This property of $\mathcal{C}_{\mathrm{SD}}(L_1,L_2)$ is discussed in Section IV-D.*

The inner and outer bounds in Theorems 1 and 3 also match when the message set is degraded, i.e., when there is only one private message. The leakage-capacity region of the BC where $M_2 = 0$ is defined only by the threshold L_1 and is stated next.[1]

Theorem 5 (Leakage-Capacity for BC with Degraded Message Set) *Let $L_1 \in \mathbb{R}_+$. The L_1-leakage-capacity region $\mathcal{C}_{\mathrm{DM}}(L_1)$ of a BC with a degraded message set and a privacy leakage constraint is the closure of the union of rate pairs $(R_0,R_1) \in \mathbb{R}_+^2$ satisfying:*

$$R_0 \le I(W;Y_2) \tag{15a}$$

$$R_1 \le I(U;Y_1|W) - I(U;Y_2|W) + L_1 \tag{15b}$$

$$R_0 + R_1 \le I(W,U;Y_1) - I(U;Y_2|W) + L_1 \tag{15c}$$

$$R_0 + R_1 \le I(U;Y_1|W) + \min\left\{I(W;Y_1), I(W;Y_2)\right\} \tag{15d}$$

where the union is over all PMFs $P_{W,U}P_{X|U}Q_{Y_1,Y_2|X}$. $\mathcal{C}_{\mathrm{DM}}(L_1)$ is convex.

[1]Equivalently, one may consider the case where $M_1 = 0$

Proof: The direct part follows by setting $R_2 = 0$, $U_1 = U$ and $U_2 = 0$ in Theorem 1. For the converse we show that $\mathcal{R}_{\rm O}(L_1, L_2) \subseteq \mathcal{C}_{\rm DM}(L_1)$. Clearly, (15a), (15b) and (15d) coincide with (12a), (12c) and (12d), respectively. Inequality (15c) follows by merging (12a) and (12c). ■

Remark 6 *The BC with a degraded message set and a privacy leakage constraint captures the BC with confidential messages [3] and the BC with a degraded message set [25]. The former is obtained by taking $L_1 = 0$, while $L_1 \to \infty$ recovers the latter. Setting $L_1 = 0$ or $L_1 \to \infty$ into $\mathcal{C}_{\rm DM}(L_1)$ recovers the capacity regions of these special cases (see Section IV-E for more details).*

Corollary 6 (Leakage-Capacity for PD-BC) *The L_1-leakage-capacity region $\mathcal{C}_{\rm PD}(L_1)$ of a PD-BC without a common message and transition probability $Q_{Y_1|X}Q_{Y_2|Y_1}$ is the closure of the union over the same domain as $\mathcal{C}_{\rm DM}(L_1)$ of rate pairs $(R_1, R_2) \in \mathbb{R}_+^2$ satisfying (15a)-(15b) and (15d), while replacing R_0 with R_2 and noting that* $\min\left\{I(W;Y_1), I(W;Y_2)\right\} = I(W;Y_2)$.

The proof of Corollary 6 is similar to that of Theorem 5 and is omitted.

Remark 7 *Bounds on the cardinality of the auxiliary random variables in Theorems 1, 3, 4 and 5 can be derived using, e.g., the perturbation method [37, Appendix C] or techniques such as in [19] and [38]. The computability of the derived regions is not in the scope of this work.*

IV. Special Cases

A. Marton's Inner Bound

Theorem 1 generalizes Marton's region to the case with privacy leakage constraints, i.e., $\mathcal{R}_{\rm I}(\infty, \infty)$ recovers Marton's region. Moreover, $\mathcal{R}_{\rm I}(L_1, L_2)$ is tight for every BC with a known capacity region.

B. UVW-Outer Bound

The New-Jersey outer bound was derived in [20] and shown to be at least as good as the previously known bounds. A simpler version of this outer bound was established in [19] and was named the UVW-outer bound. The UVW-outer bound is given by $\mathcal{R}_{\rm O}(\infty, \infty)$.

C. Liu-Marić-Spasojević-Yates Inner Bound for BCs with Secrecy

In [4] an inner bound on the secrecy-capacity region of a BC with two confidential messages (each destined for one of the receivers and kept secret from the other) was characterized as the set of rate pairs $(R_1, R_2) \in \mathbb{R}_+^2$ satisfying:

$$R_1 \le I(U_1;Y_1|U_0) - I(U_1;U_2|U_0) - I(U_1;Y_2|U_0,U_2) \tag{16a}$$

$$R_2 \le I(U_2;Y_2|U_0) - I(U_1;U_2|U_0) - I(U_2;Y_1|U_0,U_1) \tag{16b}$$

where the union is over all PMFs $P_{U_0,U_1,U_2}P_{X|U_1,U_2}Q_{Y_1,Y_2|X}$. This inner bound is tight for SD-BCs [5] and MIMO Gaussian BCs [11]. Setting $R_0 = 0$ into $\mathcal{R}_{\mathrm{I}}(0,0)$ recovers (16).

D. SD-BCs with and without Secrecy

The SD-BC without a common message, i.e., when $R_0 = 0$, is solved when both, either or neither private messages are secret (see [5]–[7] and [24], respectively). Setting $L_j = 0$, for $j = 1, 2$, reduces the SD-BC with privacy leakage constraints to the problem where M_j is secret. Taking $L_j \to \infty$ results in a SD-BC without a secrecy constraint on M_j. We use Theorem 4 to obtain the leakage-capacity region of the SD-BC without a common message.

Corollary 7 (Leakage-Capacity for SD-BC without Common Message) *Let $(L_1, L_2) \in \mathbb{R}_+^2$. The (L_1, L_2)-leakage-capacity region $\mathcal{C}_{\mathrm{SD}}^0(L_1, L_2)$ of a SD-BC $\mathbb{1}_{\{Y_1=f(X)\}}Q_{Y_2|X}$ with privacy leakage constraints and without a common message is the closure of the union over the domain stated in Theorem 4 of rate pairs $(R_1, R_2) \in \mathbb{R}_+^2$ satisfying:*

$$R_1 \le H(Y_1|W,V,Y_2) + L_1 \tag{17a}$$

$$R_1 \le H(Y_1) \tag{17b}$$

$$R_2 \le I(V;Y_2|W) - I(V;Y_1|W) + L_2 \tag{17c}$$

$$R_2 \le I(W,V;Y_2) \tag{17d}$$

$$R_1 + R_2 \le H(Y_1|W,V,Y_2) + I(V;Y_2|W) + I(W;Y_1) + L_1 \tag{17e}$$

$$R_1 + R_2 \le H(Y_1|W,V) + I(V;Y_2|W) + \min\big\{I(W;Y_1), I(W;Y_2)\big\}. \tag{17f}$$

1) Neither Message is Secret: If $L_1, L_2 \to \infty$, the SD-BC with leakage reduces to the classic case without secrecy [24], for which the capacity region is the closure of the union of rate pairs $(R_1, R_2) \in \mathbb{R}_+^2$ satisfying:

$$R_1 \le H(Y_1) \tag{18a}$$

$$R_2 \le I(V;Y_2) \tag{18b}$$

$$R_1 + R_2 \le H(Y_1|V) + I(V;Y_2) \tag{18c}$$

where the union is over all PMFs $P_{V,Y_1,X}Q_{Y_2|X}$ for which $Y_1 = f(X)$. The region (18) coincides with $\mathcal{C}_{\mathrm{SD}}^0(\infty,\infty)$ by first noting that the bound

$$R_1 + R_2 \le H(Y_1|W,V) + I(V;Y_2|W) + I(W;Y_1) \tag{19}$$

is redundant because if for some PMF $P_{W,V,X}Q_{Y_1,Y_2|X}$ (19) is active, then setting $\tilde{W} = 0$ and $\tilde{V} = (W,V)$ achieves a larger region. Removing (19) from $\mathcal{C}_{\mathrm{SD}}^0(\infty,\infty)$ and setting $\tilde{V} = (W,V)$ recovers (18). This agrees with

the discussion in Section IV-A since Marton's inner bound is tight for the SD-BC.

2) Only M_1 is Secret: The SD-BC in which M_1 is a secret is obtained by taking $L_1 = 0$ and $L_2 \to \infty$. The secrecy-capacity region was derived in [7, Corollary 4] and is the closure of the union over the same domain as (18) of rate pairs $(R_1, R_2) \in \mathbb{R}_+^2$ satisfying:

$$R_1 \leq H(Y_1|V, Y_2) \tag{20a}$$

$$R_2 \leq I(V; Y_2). \tag{20b}$$

$\mathcal{C}_{\mathrm{SD}}^0(0, \infty)$ and (20) match by dropping

$$R_1 + R_2 \leq H(Y_1|W, V, Y_2) + I(V; Y_2|W) + I(W; Y_1) \tag{21}$$

based on arguments similar to those used to remove (19) from $\mathcal{C}_{\mathrm{SD}}^0(\infty, \infty)$, and setting $\tilde{V} = (W, V)$.

Remark 8 *The optimal code for the SD-BC with a secret message M_1 relies on double-binning the codebook of M_1, while M_2 is transmitted at maximal rate and no binning of its codebook is performed. Referring to the bounds in Section VI-A, inserting $L_1 = 0$ and $L_2 \to \infty$ into our code construction results in (38a) and (47b) becoming inactive since (46b) is the dominant constraint. Furthermore, $L_1 = 0$ combined with (33c) implies that the public message consists of a portion of M_2* only. *Keeping in mind that the public message is decoded by both receivers, unless $R_{10} = 0$ (i.e., unless the public message contains no information about M_1) the secrecy constraint will be violated.*

3) Only M_2 is Secret: The SD-BC in which M_2 is secret is obtained by taking $L_1 \to \infty$ and $L_2 = 0$. The secrecy-capacity region is the closure of the union of rate pairs $(R_1, R_2) \in \mathbb{R}_+^2$ satisfying:

$$R_1 \leq H(Y_1) \tag{22a}$$

$$R_1 \leq H(Y_1|W) + I(W; Y_2) \tag{22b}$$

$$R_2 \leq I(V; Y_2|W) - I(V; Y_1|W) \tag{22c}$$

where the union is over all PMFs $P_{W,V,Y_1,X} Q_{Y_2|X}$ for which $Y_1 = f(X)$ [6, Theorem 1]. Using Corollary 7, $\mathcal{C}_{\mathrm{SD}}^0(\infty, 0)$ is the union over the same domain as (22) of rate pairs $(R_1, R_2) \in \mathbb{R}_+^2$ satisfying:

$$R_1 \leq H(Y_1) \tag{23a}$$

$$R_2 \leq I(V; Y_2|W) - I(V; Y_1|W) \tag{23b}$$

$$R_1 + R_2 \leq H(Y_1|W, V) + I(W, V; Y_2). \tag{23c}$$

The second bound on $R_1 + R_2$ in $\mathcal{C}_{\mathrm{SD}}^0(\infty, 0)$ is redundant since it follows by adding (23a) and (23b). Both (22) and (23) describe the secrecy-capacity region of the SD-BC with a secret message M_2. In Appendix A we prove the equivalence by using bidirectional inclusion arguments. By symmetry of our code construction,

the effect of $L_1 \to \infty$ and $L_2 = 0$ on the scheme in Section VI-A is analogous to the one described in Section IV-D2.

4) Both Messages are Secret: Taking $L_1 = L_2 = 0$ recovers the SD-BC where both messages are secret. The secrecy-capacity region for this case was found in [5, Theorem 1] and is the closure of the union of rate pairs $(R_1, R_2) \in \mathbb{R}_+^2$ satisfying:

$$R_1 \le H(Y_1|W, V, Y_2) \tag{24a}$$

$$R_2 \le I(V; Y_2|W) - I(V; Y_1|W) \tag{24b}$$

where the union is over all PMFs $P_{W,V} P_{X|V} Q_{Y_2|X}$ for which $Y_1 = f(X)$. The region in (24) coincides with $\mathcal{C}_{\mathrm{SD}}^0(0,0)$. Restricting the union in $\mathcal{C}_{\mathrm{SD}}^0(0,0)$ to encompass only PMFs that satisfy the Markov relation $W - V - X$ does not shrink the region. This is since in the proof of Theorem 3 we define $V_q \triangleq (M_2, W_q)$, and therefore, $X_q - V_q - W_q$ forms a Markov chain for every $q \in [1:n]$. The optimality of PMFs in which $X - V - W$ is a Markov chain follows.

Remark 9 *The coding scheme that achieves (24) uses double-binning for the codebooks of both private messages. To preserve confidentiality, the rate bounds of each messages includes the penalty term $I(U_1; U_2|V)$ (without the confidentiality constraints, Marton's coding scheme [39] requires only that the sum-rate has that penalty term). This is evident from our scheme by setting $L_1 = L_2 = 0$ in (46b), (47b) and (33c), which results in (38a) being redundant.*

E. BCs with One Private Message

Consider the BC with leakage constraints in which $M_2 = 0$; its leakage-capacity region $\mathcal{C}_{\mathrm{DM}}(L_1)$ is stated in Theorem 5. We show that $\mathcal{C}_{\mathrm{DM}}(L_1)$ recovers the secrecy-capacity region the BC with confidential messages [3] and the capacity region of the BC with a degraded message set (without secrecy) [25].

1) BCs with Confidential Messages: The secrecy-capacity region of the BC with confidential messages was derived in [3] and is the union over the same domain as in Theorem 5 of rate pairs $(R_0, R_1) \in \mathbb{R}_+^2$ satisfying:

$$R_0 \le I(W; Y_1) \tag{25a}$$

$$R_0 \le I(W; Y_2) \tag{25b}$$

$$R_1 \le I(U; Y_1|W) - I(U; Y_2|W). \tag{25c}$$

Inserting $L_1 = 0$ into the result of Theorem 5 yields $\mathcal{C}_{\mathrm{DM}}(0)$ which is the union over the same domain as (25) of rate pairs $(R_0, R_1) \in \mathbb{R}_+^2$ satisfying:

$$R_0 \le I(W; Y_2) \tag{26a}$$

$$R_1 \le I(U; Y_1|W) - I(U; Y_2|W) \tag{26b}$$

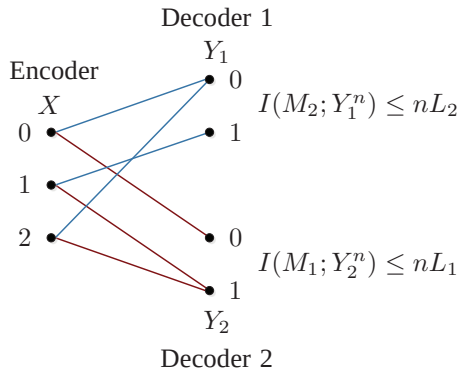

Fig. 2: Blackwell BC with privacy leakage constraints.

$$R_0 + R_1 \leq I(W,U;Y_1) - I(U;Y_2|W). \tag{26c}$$

The regions (25) and (26) are equal and a proof of the equality is given in Appendix B. Inserting $L_1 = 0$ and $U_2 = 0$ into the code construction in Section VI-A reduces it to a superposition code in which the outer codebook (that is associated with the confidential message) is binned.

Remark 10 *The BC with confidential messages captures the WTC by setting $M_0 = 0$. Thus, the WTC is also a special case of the BC with privacy leakage constraints.*

2) BCs with a Degraded Message Set: If $L_1 \to \infty$, we get the BC with a degraded message set [25]. Inserting $L_1 \to \infty$ into $\mathcal{C}_{\mathrm{DM}}(L_1)$ and setting $U = X$ recovers the capacity region which is the union of rate pairs $(R_0, R_1) \in \mathbb{R}_+^2$ satisfying:

$$R_0 \leq I(W;Y_2) \tag{27a}$$

$$R_0 + R_1 \leq I(X;Y_1|W) + I(W;Y_2) \tag{27b}$$

$$R_0 + R_1 \leq I(X;Y_1) \tag{27c}$$

where the union is over all PMFs $P_{V,X}Q_{Y_1,Y_2|X}$. In fact, (27) is an alternative characterization of the capacity region of the BC with a degraded message set, as described in [18, Theorem 7] and [40, Eq. (8.1)].

V. Example

Suppose the channel from the transmitter to receivers 1 and 2 is the BWC without a common message as illustrated in Fig. 2 [28], [29]. Using Corollary 7, the (L_1, L_2)-leakage-capacity region of a deterministic BC (DBC) is the following.

Corollary 8 (Leakage-Capacity Region for DBC) *The (L_1, L_2)-leakage-capacity region $\mathcal{C}_{\mathrm{D}}(L_1, L_2)$ of the DBC*

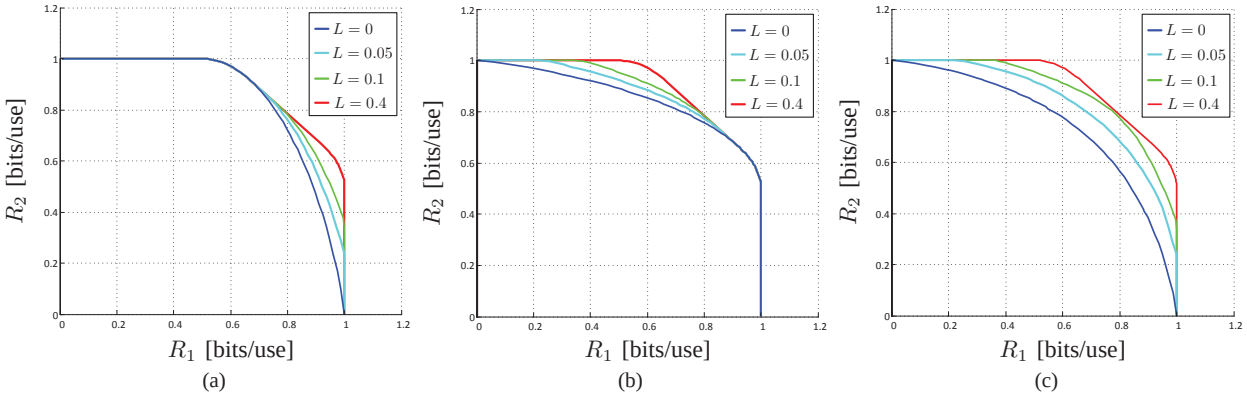

Fig. 3: (L_1, L_2)-leakage-capacity region of the BWC for three cases: (a) $L_1 = L$ and $L_2 \to \infty$; (b) $L_1 \to \infty$ and $L_2 = L$; (c) $L_1 = L_2 = L$.

with privacy leakage constraints and no common message is the union of rate pairs $(R_1, R_2) \in \mathbb{R}_+^2$ *satisfying:*

$$R_1 \leq \min\left\{H(Y_1)\,,\, H(Y_1|Y_2) + L_1\right\} \tag{28a}$$

$$R_2 \leq \min\left\{H(Y_2)\,,\, H(Y_2|Y_1) + L_2\right\} \tag{28b}$$

$$R_1 + R_2 \leq H(Y_1, Y_2) \tag{28c}$$

where the union is over all input PMFs P_X.

The proof of Corollary 8 is relegated to Appendix C. We parameterize the input PMF P_X in Corollary 8 as

$$P_X(0) = \alpha\ ,\ P_X(1) = \beta\ ,\ P_X(2) = 1 - \alpha - \beta, \tag{29}$$

where $\alpha, \beta \in \mathbb{R}_+$ and $\alpha + \beta \leq 1$. Using (29), the (L_1, L_2)-leakage-capacity region $\mathcal{C}_{\text{BWC}}(L_1, L_2)$ of the BWC is descried as the union of rate pairs $(R_1, R_2) \in \mathbb{R}_+^2$ satisfying:

$$R_1 \leq \min\left\{H_b(\beta)\,,\, (1-\alpha)H_b\left(\frac{\beta}{1-\alpha}\right) + L_1\right\} \tag{30a}$$

$$R_2 \leq \min\left\{H_b(\alpha)\,,\, (1-\beta)H_b\left(\frac{\alpha}{1-\beta}\right) + L_2\right\} \tag{30b}$$

$$R_1 + R_2 \leq H_b(\alpha) + (1-\alpha)H_b\left(\frac{\beta}{1-\alpha}\right) \tag{30c}$$

where the union is over all $\alpha, \beta \in \mathbb{R}_+$ with $\alpha + \beta \leq 1$.

Fig. 3 illustrates $\mathcal{C}_{\text{BWC}}(L_1, L_2)$ for three cases. In Fig. 3(a) $L_2 \to \infty$ while $L_1 \in \{0, 0.05, 0.1, 0.4\}$. The blue (inner) line corresponds to $L_1 = 0$ and is the secrecy-capacity region of a BWC where M_1 is secret [7, Fig. 5]. The red (outer) line corresponds to $L_1 = 0.4$ (which is sufficiently large and can be thought of as $L_1 \to \infty$) and depicts the capacity region of the classic BWC. As L_1 grows, the inner (blue) region converges to coincide with

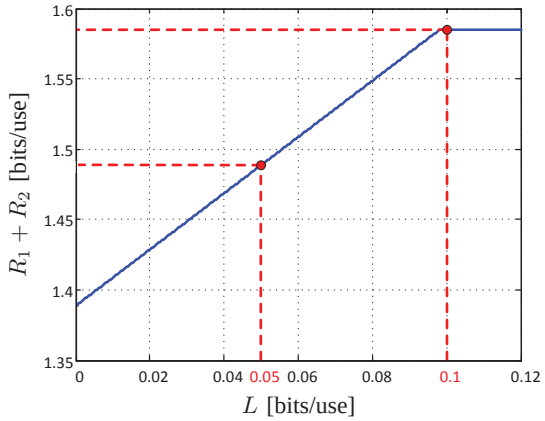

Fig. 4: The sum-rate capacity versus the allowed leakage for $L_1 = L_2 = L$.

the outer (red) region. Fig. 3(b) considers the opposite case, i.e., where $L_1 \to \infty$ and $L_2 \in \{0, 0.05, 0.1, 0.4\}$, and is analogous to Fig. 3(a). In Fig. 3(c) we choose $L_1 = L_2 = L$, where $L \in \{0, 0.05, 0.1, 0.4\}$, and we demonstrate the impact of two leakage constraints on the region. When $L = 0$, one obtains the secrecy-capacity region of the BWC when both messages are confidential [5]. In each case, the capacity region grows with L and saturates at the red (outer) region, for which neither message is secret.

Focusing on the symmetric case in Fig. 3(c), we note that the saturation of the region at $L = 0.4$ is not accidental and is implied by Corollary 2. For the Blackwell BC with $L_1 = L_2 = L$, and some $\alpha, \beta \in \mathbb{R}_+$ with $\alpha + \beta \leq 1$, we denote by $L^\star(\alpha, \beta)$ the threshold from (11), which reduces to

$$L^\star(\alpha, \beta) = I(Y_1; Y_2) = H_b(\beta) - (1 - \alpha) H_b\left(\frac{\beta}{1 - \alpha}\right). \tag{31}$$

As explained in Remark 3, for each leakage value L, Corollary 2 (along with some numerical calculations) can be used to tell whether a further increase of L will induce a larger region or not. Accordingly, for each $L \in \{0, 0.05, 0.1, 0.4\}$, we have calculated the maximum of $L^\star(\alpha, \beta)$ over the distributions that achieve the boundary points of the capacity region $\mathcal{C}_{\mathrm{BWC}}(L, L)$. Denoting the value of the maximal $L^\star$ that corresponds to the allowed leakage $L \in \{0, 0.05, 0.1, 0.4\}$ by $L^\star(L)$, we have

$$L^\star(0) = L^\star(0.05) = 0.15897 \quad ; \quad L^\star(0.1) = 0.20101 \quad ; \quad L^\star(0.4) = 0.38317. \tag{32}$$

For $L = 0.4$, we see that $L^\star(L) \leq L$, and consequently, Corollary 2 and Remark 3 imply that further increasing L will not change the leakage-capacity region. Evidently, $\mathcal{C}_{\mathrm{BWC}}(L, L)$ saturates at $L = 0.4$. For $L \in \{0, 0.05, 0.1\}$, however, $L^\star(L) > L$ and consequently $\mathcal{C}_{\mathrm{BWC}}(L', L') \subsetneq \mathcal{C}_{\mathrm{BWC}}(L, L)$, for $L, L' \in \{0, 0.05, 0.1\}$ with $L' < L$.

The variation of the sum of rates $R_1 + R_2$ as a function of L is shown by the blue curve in Fig. 4; the red dashed vertical lines correspond to the values of L considered in Fig. 3. Note that for $0 \leq L \leq 0.09818$, (30c) is inactive, and therefore, $R_1 + R_2$ is bounded by the summation of (30a) and (30b). Thus, for $0 \leq L \leq 0.09818$, the

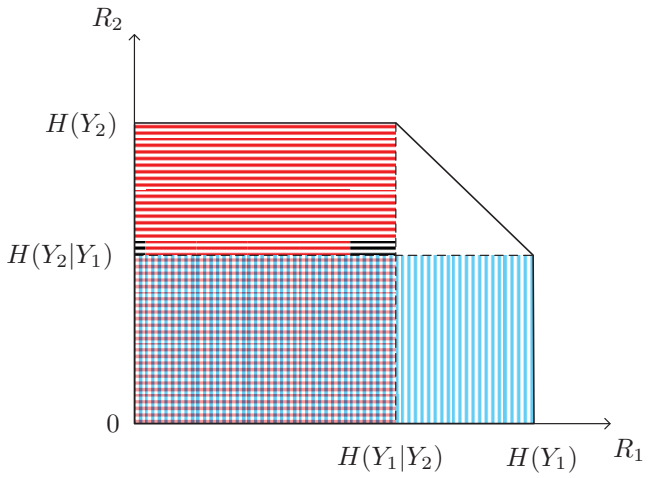

Fig. 5: The pentagons/rectangles whose union produces the capacity region of a BWC for different secrecy cases: The outer pentagon corresponds to the case without secrecy; the red and blue rectangles correspond to $L_1 = 0$ and $L_2 = 0$, respectively; the inner rectangle is associated with $L_1 = L_2 = 0$.

sum of rates $R_1 + R_2$ increases linearly with L. For $L > 0.09818$, the bound in (30c) is no longer redundant, and because it is independent of L, the sum rate saturates.

The regions in Fig. 3 are a union of rectangles or pentagons, each corresponds to a different input PMF P_X. In Fig. 5 we illustrate a typical structure of these rectangles and pentagons for a fixed P_X at the extreme values of L_1 and L_2. When both L_1 and L_2 are sufficiently large, the leakage constraints degenerate and the classic BWC is obtained. Its capacity region (the red (outer) line in, e.g., Fig. 3(c)) is a union of the pentagons depicted in Fig. 5. The secrecy-capacity region for $L_1 = 0$ and $L_2 \to \infty$ (depicted by the blue line in Fig. 3(a)) is a union of the red rectangles in Fig. 5. Similarly, when $L_2 = 0$ and $L_1 \to \infty$ the secrecy-capacity region is a union of the blue rectangles in Fig. 5. Finally, if $L_1 = L_2 = 0$ and both messages are secret, the secrecy-capacity region of the BWC is the union of the dark rectangles in Fig. 5, i.e., the intersection of the blue and the red regions. Fig. 5 highlights that as L_1 and/or L_2 decrease, the underlying pentagons/rectangles (the union of which produces the admissible rate region) shrink and results in a smaller region.

VI. Proofs

A. Proof of Theorem 1

For simplicity, we assume that expressions of the form 2^{nR}, for some $R \in \mathbb{R}_+$, are integers. Fix $(L_1, L_2) \in \mathbb{R}_+^2$, a single-letter PMF $P_{U_0,U_1,U_2,X,Y_1,Y_2} \triangleq P_{U_0,U_1,U_2,X} Q_{Y_1,Y_2|X} \in \mathcal{P}(\mathcal{U}_0 \times \mathcal{U}_\cdot \times \mathcal{U}_1 \times \mathcal{X} \times \mathcal{Y}_1 \times \mathcal{Y}_2)$ and $\epsilon, \xi_1, \xi_2 > 0$.

Codebook $\mathcal{B}_n$: Split each message m_j, $j = 1, 2$, into two sub-messages denoted by (m_{j0}, m_{jj}). The triple $m_p \triangleq (m_0, m_{10}, m_{20})$ is referred to as a *public message* while m_{jj}, $j = 1, 2$, serve as *private message* j. The rates associated with m_{j0} and m_{jj}, $j = 1, 2$, are denoted by R_{j0} and R_{jj}, while the corresponding alphabets are $\mathcal{M}_{j0}$

and $\mathcal{M}_{jj}$, respectively. The partial rates R_{j0} and R_{jj}, $j=1,2$, satisfy

$$R_j = R_{j0} + R_{jj} \tag{33a}$$

$$0 \le R_{j0} \le R_j \tag{33b}$$

$$R_{j0} \le L_j. \tag{33c}$$

The random variables M_{j0} and M_{jj} are independent and uniform over $\mathcal{M}_{j0}$ and $\mathcal{M}_{jj}$. We use the notations $M_p \triangleq (M_0, M_{10}, M_{20})$, $\mathcal{M}_p \triangleq \mathcal{M}_0 \times \mathcal{M}_{10} \times \mathcal{M}_{20}$ and $R_p \triangleq R_0 + R_{10} + R_{20}$. Note that M_p is uniformly distributed over $\mathcal{M}_p$ and that $|\mathcal{M}_p| = 2^{nR_p}$. Moreover, let (W_1, W_2) be a pair of independent random variables, where W_j, $j=1,2$, is uniformly distributed over $\mathcal{W}_j = \big[1 : 2^{n\tilde{R}_j}\big]$ and independent of (M_0, M_1, M_2) (which implies their independence of (M_p, M_{11}, M_{22}) as well).

All subsequent notations of codebooks and codewords omit the blocklength n. Let $\mathbb{B}_0 \triangleq \big\{\mathbf{U}_0(m_p)\big\}_{m_p \in \mathcal{M}_p}$ be a random public message codebook that comprises 2^{nR_p} i.i.d. random vectors $\mathbf{U}_0(m_p)$, each distributed according to $P_{U_0}^n$. A realization of $\mathbb{B}_0$ is denoted by $\mathcal{B}_0 \triangleq \big\{\mathbf{u}_0(m_p, \mathcal{B}_0)\big\}_{m_p \in \mathcal{M}_p}$.

Fix a public message codebook $\mathcal{B}_0$. For every $m_p \in \mathcal{M}_p$, let $\mathbb{B}_j(m_0) \triangleq \big\{\mathbf{U}_j(m_p, m_{jj}, i_j, w_j)\big\}_{(m_{jj}, i_j, w_j) \in \mathcal{M}_{jj} \times \mathcal{I}_j \times \mathcal{W}_j}$, where $\mathcal{I}_j \triangleq \big[1 : 2^{nR'_j}\big]$, be a random codebook of private messages for $j=1,2$, consisting of conditionally independent random vectors each distributed according to $P^n_{U_j|U_0=\mathbf{u}_0(m_p,\mathcal{B}_0)}$. We further set $\mathbb{B}_j = \big\{\mathbb{B}_j(m_p)\big\}_{m_p \in \mathcal{M}_p}$. A realization of $\mathbb{B}_j$ is denoted by $\mathcal{B}_j$ and we also define $\mathcal{B}_{0,j} = \big\{\mathcal{B}_0, \mathcal{B}_j\big\}$, for $j=1,2$, and $\mathcal{B} = \big\{\mathcal{B}_0, \mathcal{B}_1, \mathcal{B}_2\big\}$. For each $m_p \in \mathcal{M}_p$, we use $\mathcal{B}_j(m_p) \triangleq \big\{\mathbf{u}_j(m_p, m_{jj}, i_j, w_j, \mathcal{B}_{0,j})\big\}_{(m_{jj}, i_j, w_j) \in \mathcal{M}_{jj} \times \mathcal{I}_j \times \mathcal{W}_j}$. Based on the above labeling, the codebook $\mathcal{B}_j(m_p)$ has a u_j-bin associated with every pair $(m_{jj}, w_j) \in \mathcal{M}_{jj} \times \mathcal{W}_j$, each containing $2^{nR'_j}$ u_j-codewords.

Denote the set of all possible codebooks of the above structure by $\mathfrak{B}$. The probability of drawing a codebook $\mathcal{B} = \big\{\mathcal{B}_0, \mathcal{B}_1, \mathcal{B}_2\big\} \in \mathfrak{B}$ is

$$P_{\mathbb{B}}(\mathcal{B}) = \prod_{m_p \in \mathcal{M}_p} P_{U_0}^n\big(\mathbf{u}_0(m_p, \mathcal{B}_0)\big) \prod_{j=1,2} \prod_{\substack{(m_p^{(j)}, m_{jj}, i_j, w_j) \\ \in \mathcal{M}_p \times \mathcal{M}_{jj} \times \mathcal{I}_j \times \mathcal{W}_j}} P^n_{U_j|U_0}\Big(\mathbf{u}_j\big(m_p^{(j)}, m_{jj}, i_j, w_j, \mathcal{B}_{0,j}\big)\Big|\mathbf{u}_0\big(m_p^{(j)}, \mathcal{B}_0\big)\Big). \tag{34}$$

For a fixed codebook $\mathcal{B} \in \mathfrak{B}$ we next describe its associated encoding function $f_{\mathrm{E}}^{(\mathcal{B})}$ and decoding functions $\phi_j^{(\mathcal{B})}$, for $j=1,2$.

Encoder $f_{\mathbf{E}}^{(\mathcal{B})}$: To transmit the message pair (m_0, m_1, m_2) the encoder transforms it into the triple $\big(m_p, m_{11}, m_{22}\big)$, and draws W_j uniformly over $\mathcal{W}_j$, $j=1,2$. Then it searches for a pair of indices $(i_1, i_2) \in \mathcal{I}_1 \times \mathcal{I}_2$ such that

$$\Big(\mathbf{u}_0(m_p, \mathcal{B}_0), \mathbf{u}_1(m_p, m_1, i_1, w_1, \mathcal{B}_{0,1}), \mathbf{u}_2(m_p, m_{22}, i_2, w_2, \mathcal{B}_{0,2})\Big) \in \mathcal{T}_\epsilon^n(P_{U_0,U_1,U_2}) \tag{35}$$

where w_j denotes the realization of W_j. If the set of appropriate index pairs contains more than one element, the encoder chooses a pair uniformly over the set; if the set is empty, a pair is chosen uniformly over $\mathcal{I}_1 \times \mathcal{I}_2$. The channel input sequence is then generate according to the conditional product distribution

$P^n_{X|U_0=\mathbf{u}_0(m_p,\mathcal{B}_0),U_1=\mathbf{u}_1(m_p,m_1,i_1,w_1,\mathcal{B}_{0,1}),U_2=\mathbf{u}_2(m_p,m_{22},i_2,w_2,\mathcal{B}_{0,2})}$ and is transmitted over the channel.

Decoder $\phi_j^{(\mathcal{B})}$: Decoder $j=1,2$, searches for a unique triple $(\hat{m}_p,\hat{m}_{jj},\hat{w}_j)\in\mathcal{M}_p\times\mathcal{M}_{jj}\times\mathcal{W}_j$ for which there is an index $\hat{i}_j\in\mathcal{I}_j$ such that

$$\Big(\mathbf{u}_0(\hat{m}_p,\mathcal{B}_0),\mathbf{u}_j(\hat{m}_p,\hat{m}_{jj},\hat{i}_j,\hat{w}_j,\mathcal{B}_{0,j}),\mathbf{y}_j\Big)\in\mathcal{T}^n_\epsilon(P_{U_0,U_j,Y_j}). \tag{36}$$

If such a unique triple is found set $\phi_j(\mathbf{y}_j)=\big(\hat{m}_0,(\hat{m}_{j0},\hat{m}_{jj})\big)$, and otherwise $\phi_j=e$.

The triple $\Big(f_{\mathrm{E}}^{(\mathcal{B})},\phi_1^{(\mathcal{B})},\phi_2^{(\mathcal{B})}\Big)$ defined with respect to a codebook $\mathcal{B}\in\mathfrak{B}$ constitutes an (n,R_0,R_1,R_2) code $\mathcal{C}_n\in\mathfrak{C}_n$ for the BC with privacy leakage constraints. We henceforth omit the blocklength n writing $\mathcal{C}$ and $\mathfrak{C}$ instead of $\mathcal{C}_n$ and $\mathfrak{C}_n$, respectively. When a random codebook $\mathbb{B}$ is used, we denote the corresponding random code by $\mathbb{C}$. Note that $\mathbb{C}$ is distributed according to

$$P_{\mathbb{C}}(\mathcal{C})=P_{\mathbb{C}}\Big(\big(f_{\mathrm{E}}^{(\mathcal{B})},\phi_1^{(\mathcal{B})},\phi_2^{(\mathcal{B})}\big)\Big)=P_{\mathbb{B}}(\mathcal{B}),\quad\forall\mathcal{C}\in\mathfrak{C}, \tag{37}$$

where $P_{\mathbb{B}}$ is specified in (34). The PMF $P_{\mathbb{C}}$ along with (3b) give rise to the PMF from (3a) and to its induced probability measure $\mathbb{P}$.

By standard error probability analysis (see Appendix D), reliability requires

$$R_1'+R_2'>I(U_1;U_2|U_0) \tag{38a}$$

$$R_{11}+R_1'+\tilde{R}_1<I(U_1;Y_1|U_0) \tag{38b}$$

$$R_0+R_{20}+R_1+R_1'+\tilde{R}_1<I(U_0,U_1;Y_1) \tag{38c}$$

$$R_{22}+R_2'+\tilde{R}_2<I(U_2;Y_2|U_0) \tag{38d}$$

$$R_0+R_{10}+R_2+R_2'+\tilde{R}_2<I(U_0,U_2;Y_2). \tag{38e}$$

The leakage analysis requires two properties in addition to reliability. Namely, for a fixed $m_1\in\mathcal{M}_1$ (respectively, $m_2\in\mathcal{M}_2$) Decoder 2 (respectively, Decoder 1) should be able to decode W_1 (respectively, W_2) with an arbitrarily low error probability based on $(\mathbf{U}_0,\mathbf{U}_2,\mathbf{Y}_2)$ (respectively, $(\mathbf{U}_0,\mathbf{U}_1,\mathbf{Y}_1)$). For a fixed code $\mathcal{C}\in\mathfrak{C}$ (specified by a fixed codebook $\mathcal{B}\in\mathfrak{B}$), denote by $\lambda_{m_1}(\mathcal{C})$ the probability that Decoder 1 or Decoder 2 fail to do so using $\mathcal{C}$. As explained in Appendix D, $\mathbb{E}\lambda_{m_1}(\mathbb{C})=\mathbb{E}\lambda_1(\mathbb{C})\to 0$ as $n\to\infty$, for every $m_1\in\mathcal{M}_1$, if

$$\tilde{R}_1<I(U_1;Y_2|U_0,U_2) \tag{39a}$$

$$\tilde{R}_2<I(U_2;Y_1|U_0,U_1). \tag{39b}$$

Leakage Analysis: We compute an upper bound on $\mathbb{E}L_1(\mathbb{C})$ and on $\mathbb{E}L_2(\mathbb{C})$. By symmetry, only the analysis for the expected rate-leakage of M_1 to the 2nd receiver is presented. The corresponding derivation for M_2 follows similar lines.

In all subsequent arguments, the random vectors $\mathbf{U}_0$, $\mathbf{U}_1$ and $\mathbf{U}_2$ stand for the u_0-, u_1- and u_2-codewords chosen

by the encoder. Noting that $\mathbb{E}L_1(\mathbb{C}) = I(M_1; \mathbf{Y}_2|\mathbb{C})$, we have

$$\begin{aligned}
H(M_1|\mathbf{Y}_2,\mathbb{C}) &\overset{(a)}{\geq} H(M_1|\mathbf{U}_0,\mathbf{U}_2,\mathbf{Y}_2,\mathbb{C}) \\
&= H(M_1,\mathbf{Y}_2|\mathbf{U}_0,\mathbf{U}_2,\mathbb{C}) - H(\mathbf{Y}_2|\mathbf{U}_0,\mathbf{U}_2,\mathbb{C}) \\
&= H(M_1,\mathbf{U}_1,\mathbf{Y}_2|\mathbf{U}_0,\mathbf{U}_2,\mathbb{C}) - H(\mathbf{U}_1|M_1,\mathbf{U}_0,\mathbf{U}_2,\mathbf{Y}_2,\mathbb{C}) - H(\mathbf{Y}_2|\mathbf{U}_0,\mathbf{U}_2,\mathbb{C}) \\
&\overset{(b)}{\geq} H(\mathbf{U}_1|\mathbf{U}_0,\mathbf{U}_2,\mathbb{C}) - H(\mathbf{U}_1|M_1,\mathbf{U}_0,\mathbf{U}_2,\mathbf{Y}_2,\mathbb{C}) - H(\mathbf{Y}_2|\mathbf{U}_0,\mathbf{U}_2,\mathbb{C}) \\
&\qquad + H(\mathbf{Y}_2|M_1,\mathbf{U}_0,\mathbf{U}_1,\mathbf{U}_2,\mathbb{C}) \\
&\overset{(c)}{=} H(\mathbf{U}_1|\mathbf{U}_0,\mathbb{C}) - I(\mathbf{U}_1;\mathbf{U}_2|\mathbf{U}_0,\mathbb{C}) - H(\mathbf{U}_1|M_1,\mathbf{U}_0,\mathbf{U}_2,\mathbf{Y}_2,\mathbb{C}) - I(\mathbf{U}_1;\mathbf{Y}_2|\mathbf{U}_0,\mathbf{U}_2,\mathbb{C}) \quad (40)
\end{aligned}$$

where (a) and (b) follow because conditioning cannot increase entropy, while (c) follows since $\mathbf{Y}_2 - (\mathbf{U}_0,\mathbf{U}_1,\mathbf{U}_2,\mathbb{C}) - M_1$ forms a Markov chain (this can be shown using functional dependence graphs [41]).

We evaluate each term in (40) separately using the following lemmas.

Lemma 9 *For any $\epsilon_1,\epsilon_2 > 0$, there is a sufficiently large n for which*

$$I(\mathbf{U}_1;\mathbf{U}_2|\mathbf{U}_0,\mathbb{C}) \leq nI(U_1;U_2|U_0) + n\epsilon_1 \quad (41a)$$

$$I(\mathbf{U}_1;\mathbf{Y}_2|\mathbf{U}_0,\mathbf{U}_2,\mathbb{C}) \leq nI(U_1;Y_2|U_0,U_2) + n\epsilon_2. \quad (41b)$$

Lemma 10 *For any $\epsilon_3 > 0$ there is a sufficiently large n for which*

$$H(\mathbf{U}_1|M_1,\mathbf{U}_0,\mathbf{U}_2,\mathbf{Y}_2,\mathbb{C}) \leq n\epsilon_3. \quad (42)$$

The proofs of Lemmas 9 and 10 are similar to those of [4, Lemmas 2 and 3]. For completeness, we give the proofs in Appendix E. Next, let I_1 denote the random variable that represents the choice of the index $i_1 \in \mathcal{I}_1$ and observe that

$$\begin{aligned}
H(\mathbf{U}_1|\mathbf{U}_0=\mathbf{u}_0,\mathbb{C}) &= H(M_{11},W_1,I_1,\mathbf{U}_1|\mathbf{U}_0=\mathbf{u}_0,\mathbb{C}) - H(M_{11},W_1,I_1|\mathbf{U}_1,\mathbf{U}_0=\mathbf{u}_0,\mathbb{C}) \\
&\overset{(a)}{=} H(M_{11},W_1,I_1|\mathbf{U}_0=\mathbf{u}_0,\mathbb{C}) - H(M_{11},W_1,I_1|\mathbf{U}_1,\mathbf{U}_0=\mathbf{u}_0,\mathbb{C}) \\
&\overset{(b)}{\geq} H(M_{11},W_1,I_1|\mathbf{U}_0=\mathbf{u}_0,\mathbb{C}) - n\epsilon_4 \\
&\overset{(c)}{=} n(R_{11}+\tilde{R}_1+R_1') - n\epsilon_4 \quad (43)
\end{aligned}$$

where:

(a) follows since conditioned on $\mathbf{U}_0=\mathbf{u}_0$ and $\mathbb{C}$, $\mathbf{U}_1$ is defined by (M_{11},W_1,I_1);

(b) follows from Fano's inequality. Namely, by (38b) we have that the error probability in decoding (M_{11},W_1,I_1) from $(\mathbf{u}_0,\mathbf{U}_1)$ is upper bounded by $\eta_\epsilon^{(4)}$, which is arbitrarily small for sufficiently large n. Fano's inequality implies that

$$H(M_{11},W_1,I_1|\mathbf{U}_1,\mathbf{U}_0=\mathbf{u}_0,\mathbb{C}) \leq n\epsilon_4, \quad (44)$$

where $\epsilon_4 = \frac{1}{n} + \eta_\epsilon^{(4)}(R_{11} + \tilde{R}_1 + R'_1)$;
(c) follows by the symmetry of the random codebook, which implies that conditioned on $\mathbf{U}_0 = \mathbf{u}_0$, the triple (M_{11}, W_1, I_1) attains $2^{n(R_{11}+\tilde{R}_1+R'_1)}$ values with equal probabilities.

Based on (43) we have

$$H(\mathbf{U}_1|\mathbf{U}_0, \mathbb{C}) \geq n(R_{11} + \tilde{R}_1 + R'_1) - n\epsilon_4. \tag{45}$$

Inserting (45) into (40) and using Lemmas 9 and 10 yields

$$\begin{aligned} H(M_1|\mathbf{Y}_2, \mathbb{C}) &\geq n\big(R_{11} + \tilde{R}_1 + R'_1 - \epsilon_4 - I(U_1; U_2|U_0) - \epsilon_1 - \epsilon_3 - I(U_1; Y_2|U_0, U_2) - \epsilon_2\big) \\ &\overset{(a)}{=} n\big(R_1 + \tilde{R}_1 + R'_1 - R_{10} - I(U_1; Y_2|U_0, U_2) - I(U_1; U_2|U_0) - \epsilon_5\big) \\ &\overset{(b)}{\geq} nR_1 - n(L_1 + \epsilon_5) \end{aligned}$$

where (a) follows by denoting $\epsilon_5 \triangleq \sum_{i=1}^{4} \epsilon_i$ and using (33a) and (33c), while (b) follows by taking

$$\tilde{R}_1 + R'_1 - R_{10} > I(U_1; Y_2|U_0, U_2) + I(U_1, U_2|U_0) - L_1 \tag{46a}$$

$$R'_1 + L_1 - R_{10} > I(U_1; U_2|U_0). \tag{46b}$$

The bound in (46b) insures that an $\tilde{R}_1 > 0$ that satisfies (39a) and (46a) is feasible. Note that ϵ_5 can be made arbitrarily small with n, which implies that there is an n for which $\mathbb{E}L_1(\mathbb{C}) \leq L_1 + \xi_1$. A similar analysis of the average rate leaked from M_2 to the 1st receiver shows that $\mathbb{E}L_2(\mathbb{C}) \leq L_2 + \xi_2$ for sufficiently large n if

$$\tilde{R}_2 + R'_2 - R_{20} > I(U_2; Y_1|U_0, U_1) + I(U_1, U_2|U_0) - L_2 \tag{47a}$$

$$R'_2 + L_2 - R_{20} > I(U_1; U_2|U_0) \tag{47b}$$

By applying the Selection Lemma [42, Lemma 2.2] to the sequence of random variables $\{\mathbb{C}_n\}_{n\in\mathbb{N}}$ and the functions P_e, L_1 and L_2, we conclude that there exists an $n \in \mathbb{N}$ sufficiently large and a realization $\mathcal{C}_n$ of $\mathbb{C}_n$ that satisfies (6). Finally, we apply FME on (38)-(39) and (46)-(47) while using (33) and the non-negativity of the involved terms, to eliminate R_{j0}, R'_j and $\tilde{R}_j$, for $j = 1, 2$. Since all the above linear inequalities have constant coefficients, the FME can be performed by a computer program, e.g., by the FME-IT software [26]. This shows the sufficiency of (8).

Remark 11 *Applying FME on (38)-(39) and (46)-(47) gives the rate bounds (8) as well as the inequality*

$$I(U_1; Y_1|U_0) + I(U_2; Y_2|U_0) - I(U_1; U_2|U_0) \geq 0. \tag{48}$$

However, if (48) is active then P_{U_0,U_1,U_2} is not a good choice for code design. Setting $U_1 = U_2 = 0$ and keeping the same U_0 (a choice which always satisfies (48)) achieves a larger region than the one achieved by $P_{U_0,U_1,U_2,X}Q_{Y_1,Y_2|X}$.

B. Proof of Corollary 2

Fix $(L_1, L_2) \in \mathbb{R}_+^2$ and $P_{U_0,U_1,U_2,X} \in \mathcal{P}(\mathcal{U}_0 \times \mathcal{U}_1 \times \mathcal{U}_2 \times \mathcal{X})$. The rate bounds describing $\tilde{\mathcal{R}}_{\mathrm{I}}(L_1, L_2, P_{U_0,U_1,U_2,X})$ are:

$$R_1 \leq I(U_1;Y_1|U_0) - I(U_1;U_2|U_0) - I(U_1;Y_2|U_0,U_2) + L_1 \tag{49a}$$

$$R_1 \leq I(U_0,U_1;Y_1) \tag{49b}$$

$$R_2 \leq I(U_2;Y_2|U_0) - I(U_1;U_2|U_0) - I(U_2;Y_1|U_0,U_1) + L_2 \tag{49c}$$

$$R_2 \leq I(U_0,U_2;Y_2) \tag{49d}$$

$$R_1 + R_2 \leq I(U_0,U_1;Y_1) + I(U_2;Y_2|U_0) - I(U_1;U_2|U_0) - I(U_1;Y_2|U_0,U_2) + L_1 \tag{49e}$$

$$R_1 + R_2 \leq I(U_0,U_1;Y_1) + I(U_2;Y_2|U_0) - I(U_1;U_2|U_0) \tag{49f}$$

$$R_1 + R_2 \leq I(U_1;Y_1|U_0) + I(U_0,U_2;Y_2) - I(U_1;U_2|U_0) - I(U_2;Y_1|U_0,U_1) + L_2 \tag{49g}$$

$$R_1 + R_2 \leq I(U_1;Y_1|U_0) + I(U_0,U_2;Y_2) - I(U_1;U_2|U_0). \tag{49h}$$

To prove the first claim, assume that $L_1 \geq L_1^\star(P_{U_0,U_1,U_2,X})$. Consequently, the RHS of (49a) satisfies

$$\begin{aligned} I(U_1;Y_1|U_0) - I(U_1;U_2|U_0) - I(U_1;Y_2|U_0,U_2) + L_1 &= I(U_0,U_1;Y_1) - I(U_0:Y_1) - I(U_1;U_2,Y_2|U_0,U_2) + L_1 \\ &\geq I(U_0,U_1;Y_1), \end{aligned} \tag{50}$$

which makes (49a) inactive due to (49b). Similarly, (49e) is redundant due to (49f), and therefore, $\tilde{\mathcal{R}}_{\mathrm{O}}(L_1, L_2, P_{U_0,U_1,U_2,X}) = \tilde{\mathcal{R}}_{\mathrm{O}}(\infty, L_2, P_{U_0,U_1,U_2,X})$.

An analogous argument with respect to L_2 proves the second claim (essentially by showing that if $L_2 \geq L_2^\star$ then (49c) and (49g) are inactive due (49d) and (49h), respectively). The third claim follows by combining both preceding arguments.

C. Proof of Theorem 3

We show that given an (L_1, L_2)-achievable rate triple (R_0, R_1, R_2), there is a PMF $P_{W,U,V}P_{X|U,V}Q_{Y_1,Y_2|X}$, for which (12) holds. Due to the symmetric structure of the rate bounds defining $\mathcal{R}_{\mathrm{O}}(L_1, L_2)$, we present only the derivation of (12a)-(12d) and (12h). The other inequalities in (12) are established by similar arguments.

Since (R_0, R_1, R_2) is (L_1, L_2)-achievable, for every $\epsilon, \xi_1, \xi_2 > 0$ there is a sufficiently large n and an (n, R_0, R_1, R_2) code $\mathcal{C}_n$ for which (6) holds. The conditioning on $\mathcal{C}_n$ is omitted throughout this proof. Instead, we note that subsequent entropy and information measures are calculated with respect to the PMF from (3b) that is specified by $\mathcal{C}_n$.

Fix $\epsilon, \xi_1, \xi_2 > 0$ and a corresponding n. By Fano's inequality we have

$$H(M_0, M_j|Y_j^n) \leq 1 + n\epsilon R_j \triangleq n\epsilon_n^{(j)}. \tag{51}$$

Define $\epsilon_n = \max\left\{\epsilon_n^{(1)}, \epsilon_n^{(2)}\right\}$. Next, by (6b), we write

$$\begin{aligned} n(L_1+\xi_1) &\geq I(M_1; Y_2^n) \\ &= I(M_1; M_0, M_2, Y_2^n) - I(M_1; M_0, M_2|Y_2^n) \\ &\overset{(a)}{\geq} I(M_1; Y_2^n|M_0, M_2) - H(M_0, M_2|Y_2^n) \\ &\overset{(b)}{\geq} I(M_1; Y_2^n|M_0, M_2) - n\epsilon_n \end{aligned} \tag{52}$$

where (a) follows from the independence of M_1 and (M_0, M_2) and the non-negativity of entropy, while (b) follows from (51). (52) implies

$$I(M_1; Y_2^n|M_0, M_2) \leq nL_1 + n(\xi_1 + \epsilon_n). \tag{53}$$

Similarly, we have

$$I(M_1; Y_2^n|M_0) \leq nL_1 + n(\xi_1 + \epsilon_n). \tag{54}$$

The common message rate R_0 satisfies

$$\begin{aligned} nR_0 &= H(M_0) \\ &\overset{(a)}{\leq} I(M_0; Y_1^n) + n\epsilon_n \\ &= \sum_{i=1}^{n} I(M_0; Y_{1,i}|Y_1^{i-1}) + n\epsilon_n \\ &\leq \sum_{i=1}^{n} I(M_0, Y_1^{i-1}; Y_{1,i}) + n\epsilon_n \qquad (55a) \\ &\overset{(b)}{\leq} \sum_{i=1}^{n} I(W_i; Y_{1,i}) + n\epsilon_n \qquad (55b) \end{aligned}$$

where (a) follows by (51) and (b) follows by defining $W_i \triangleq (M_0, Y_1^{i-1}, Y_{2,i+1}^n)$. By reversing the roles of Y_1^n and Y_2^n and repeating similar steps, we also have

$$\begin{aligned} nR_0 &\leq \sum_{i=1}^{n} I(M_0, Y_{2,i+1}^n; Y_{2,i}) + n\epsilon_n \qquad (56a) \\ &\leq \sum_{i=1}^{n} I(W_i; Y_{2,i}) + n\epsilon_n. \qquad (56b) \end{aligned}$$

For R_1, it follows that

$$\begin{aligned} nR_1 &= H(M_1|M_0, M_2) \\ &\overset{(a)}{\leq} I(M_1; Y_1^n|M_0, M_2) - I(M_1; Y_2^n|M_0, M_2) + nL_1 + n\delta_n^{(1)} \\ &\overset{(b)}{=} \sum_{i=1}^{n} \left[I(M_1; Y_1^i, Y_{2,i+1}^n|M_0, M_2) - I(M_1; Y_1^{i-1}, Y_{2,i}^n|M_0, M_2) \right] + nL_1 + n\delta_n^{(1)} \end{aligned}$$

$$= \sum_{i=1}^{n} \Big[I(M_1; Y_{1,i}|M_2, W_i) - I(M_1; Y_{2,i}|M_2, W_i) \Big] + nL_1 + n\delta_n^{(1)}$$
$$\overset{(c)}{=} \sum_{i=1}^{n} \Big[I(U_i; Y_{1,i}|W_i, V_i) - I(U_i; Y_{2,i}|W_i, V_i) \Big] + nL_1 + n\delta_n^{(1)} \tag{57}$$

where:

(a) follows from (51) and (52), and by denoting $\delta_n^{(1)} = 2\epsilon_n + \xi_1$;

(b) follows from a telescoping identity [27, Eqs. (9) and (11)];

(c) follows by defining $U_i \triangleq (M_1, W_i)$ and $V_i \triangleq (M_2, W_i)$.

R_1 is also upper bounded as

$$\begin{aligned} nR_1 &= H(M_1|M_0) \\ &\overset{(a)}{\leq} I(M_1; Y_1^n|M_0) - I(M_1; Y_2^n|M_0) + nL_1 + n\delta_n^{(1)} \\ &\overset{(b)}{=} \sum_{i=1}^{n} \Big[I(M_1; Y_1^i, Y_{2,i+1}^n|M_0) - I(M_1; Y_1^{i-1}, Y_{2,i}^n|M_0) \Big] + nL_1 + n\delta_n^{(1)} \\ &\overset{(c)}{=} \sum_{i=1}^{n} \Big[I(U_i; Y_{1,i}|W_i) - I(U_i; Y_{2,i}|W_i) \Big] + nL_1 + n\delta_n^{(1)} \end{aligned} \tag{58}$$

where:

(a) follows from (51) and (54);

(b) follows from a telescoping identity;

(c) follows by the definition of (W_i, U_i).

For the sum $R_0 + R_1$, we have

$$\begin{aligned} n(R_0 + R_1) &= H(M_0, M_1) \\ &\overset{(a)}{\leq} I(M_0, M_1; Y_1^n) + n\epsilon_n \\ &= \sum_{i=1}^{n} I(M_0, M_1; Y_{1,i}|Y_1^{i-1}) + n\epsilon_n \\ &\overset{(b)}{\leq} \sum_{i=1}^{n} I(W_i, U_i; Y_{1,i}) + n\epsilon_n \end{aligned} \tag{59}$$

where (a) follows from (51) and (b) follows by the definition of (W_i, U_i). Moreover, consider

$$\begin{aligned} n(R_0 + R_1) &= H(M_1|M_0) + H(M_0) \\ &\overset{(a)}{\leq} I(M_1; Y_1^n|M_0) + I(M_0; Y_2^n) + n\epsilon_n \\ &\leq \sum_{i=1}^{n} \Big[I(M_1, Y_{2,i+1}^n; Y_{1,i}|M_0, Y_1^{i-1}) + I(M_0; Y_{2,i}|Y_{2,i+1}^n) \Big] + n\epsilon_n \\ &= \sum_{i=1}^{n} \Big[I(U_i; Y_{1,i}|W_i) + I(Y_{2,i+1}^n; Y_{1,i}|M_0, Y_1^{i-1}) + I(M_0; Y_{2,i}|Y_{2,i+1}^n) \Big] + n\epsilon_n \end{aligned}$$

$$\stackrel{(b)}{=} \sum_{i=1}^{n} \Big[I(U_i; Y_{1,i}|W_i) + I(Y_1^{i-1}; Y_{2,i}|M_0, Y_{2,i+1}^n) + I(M_0; Y_{2,i}|Y_{2,i+1}^n) \Big] + n\epsilon_n$$
$$\stackrel{(c)}{\leq} \sum_{i=1}^{n} \Big[I(U_i; Y_{1,i}|W_i) + I(W_i; Y_{2,i}) \Big] + n\epsilon_n \tag{60}$$

where (a) follows from (51), (b) follows from Csiszár's sum identity, while (c) follows by the definition of (W_i, U_i).

To bound the sum $R_0 + R_1 + R_2$, we start by writing

$$\begin{aligned} H(M_1|M_0, M_2) &\stackrel{(a)}{\leq} I(M_1; Y_1^n|M_0, M_2) + n\epsilon_n \\ &= \sum_{i=1}^{n} I(M_1; Y_{1,i}|M_0, M_2, Y_1^{i-1}) + n\epsilon_n \\ &\leq \sum_{i=1}^{n} I(M_1, Y_{2,i+1}^n; Y_{1,i}|M_0, M_2, Y_1^{i-1}) + n\epsilon_n \\ &\stackrel{(b)}{=} \sum_{i=1}^{n} \Big[I(U_i; Y_{1,i}|W_i, V_i) + I(Y_{2,i+1}^n; Y_{1,i}|M_0, M_2, Y_1^{i-1}) \Big] + n\epsilon_n \end{aligned} \tag{61}$$

where (a) follows from (51), while (b) follows by the definition of (W_i, U_i, V_i). Moreover, we have

$$\begin{aligned} H(M_2|M_0) &\stackrel{(a)}{\leq} I(M_2; Y_2^n|M_0) + n\epsilon_n \\ &\stackrel{(b)}{=} \sum_{i=1}^{n} \Big[I(M_2; Y_{2,i}^n|M_0, Y_1^{i-1}) - I(M_2; Y_{2,i+1}^n|M_0, Y_1^i) \Big] + n\epsilon_n \\ &\stackrel{(c)}{=} \sum_{i=1}^{n} \Big[I(M_2; Y_{2,i+1}^n|M_0, Y_1^{i-1}) + I(V_i; Y_{2,i}|W_i) - I(M_2; Y_{1,i}, Y_{2,i+1}^n|M_0, Y_1^{i-1}) \\ &\qquad + I(M_2; Y_{1,i}|M_0, Y_1^{i-1}) \Big] + n\epsilon_n \\ &\stackrel{(d)}{=} \sum_{i=1}^{n} \Big[I(V_i; Y_{2,i}|W_i) - I(V_i; Y_{1,i}|W_i) + I(M_2; Y_{1,i}|M_0, Y_1^{i-1}) \Big] + n\epsilon_n \end{aligned} \tag{62}$$

where:

(a) follows from (51);

(b) follows from a telescoping identity;

(c) follows from the mutual information chain rule and the definition of (V_i, U_i);

(d) follows by the mutual information chain rule.

Combining (61) and (62) yields

$$\begin{aligned} n(R_1 + R_2) &\leq \sum_{i=1}^{n} \Big[I(U_i; Y_{1,i}|W_i, V_i) + I(V_i; Y_{2,i}|W_i) - I(V_i; Y_{1,i}|W_i) + I(M_2, Y_{2,i+1}^n; Y_{1,i}|M_0, Y_1^{i-1}) \Big] + 2n\epsilon_n \\ &= \sum_{i=1}^{n} \Big[I(U_i; Y_{1,i}|W_i, V_i) + I(V_i; Y_{2,i}|W_i) + I(Y_{2,i+1}^n; Y_{1,i}|M_0, Y_1^{i-1}) \Big] + 2n\epsilon_n. \end{aligned} \tag{63a}$$

By applying Csiszár's sum identity on the last term in (63a), we have

$$n(R_1+R_2)=\sum_{i=1}^{n}\Big[I(U_i;Y_{1,i}|W_i,V_i)+I(V_i;Y_{2,i}|W_i)+I(Y_1^{i-1};Y_{2,i}|M_0,Y_{2,i+1}^n)\Big]+2n\epsilon_n. \tag{63b}$$

Combining (55a) with (63a) and (56a) with (63b) yields

$$n(R_0+R_1+R_2)\le\sum_{i=1}^{n}\Big[I(U_i;Y_{1,i}|W_i,V_i)+I(V_i;Y_{2,i}|W_i)+I(W_i;Y_{1,i})\Big]+3n\epsilon_n \tag{64}$$

and

$$n(R_0+R_1+R_2)\le\sum_{i=1}^{n}\Big[I(U_i;Y_{1,i}|W_i,V_i)+I(V_i;Y_{2,i}|W_i)+I(W_i;Y_{2,i})\Big]+3n\epsilon_n, \tag{65}$$

respectively.

By repeating similar steps, we obtain bounds related to the remaining rate bounds in (12):

$$nR_2\le\sum_{i=1}^{n}\Big[I(V_i;Y_{2,i}|W_i,U_i)-I(V_i;Y_{1,i}|W_i,U_i)\Big]+nL_2+n\delta_n^{(2)} \tag{66}$$

$$nR_2\le\sum_{i=1}^{n}\Big[I(V_i;Y_{2,i}|W_i)-I(V_i;Y_{1,i}|W_i)\Big]+nL_2+n\delta_n^{(2)} \tag{67}$$

$$n(R_0+R_2)\le\sum_{i=1}^{n}I(W_i,V_i;Y_{2,i})+n\epsilon_n \tag{68}$$

$$n(R_0+R_2)\le\sum_{i=1}^{n}\Big[I(V_i;Y_{2,i}|W_i)+I(W_i;Y_{1,i})\Big]+n\epsilon_n \tag{69}$$

$$n(R_0+R_1+R_2)\le\sum_{i=1}^{n}\Big[I(U_i;Y_{1,i}|W_i)+I(V_i;Y_{2,i}|W_i,U_i)+I(W_i;Y_{1,i})\Big]+3n\epsilon_n \tag{70}$$

$$n(R_0+R_1+R_2)\le\sum_{i=1}^{n}\Big[I(U_i;Y_{1,i}|W_i)+I(V_i;Y_{2,i}|W_i,U_i)+I(W_i;Y_{2,i})\Big]+3n\epsilon_n \tag{71}$$

where $\delta_n^{(2)}=2\epsilon_n+\xi_2$.

The bounds are rewritten by introducing a time-sharing random variable Q that is uniformly distributed over the set $[1:n]$. For instance, the bound (57) is rewritten as

$$\begin{aligned}R_1&\le\frac{1}{n}\sum_{q=1}^{n}\Big[I(U_q;Y_{1,q}|W_q,V_q)-I(U_q;Y_{2,q}|W_q,V_q)\Big]+L_1+\delta_n^{(1)}\\&=\sum_{i=q}^{n}\mathbb{P}\big(Q=q\big)\Big[I(U_Q;Y_{1,Q}|W_Q,V_Q,Q=q)-I(U_Q;Y_{2,Q}|W_Q,V_Q,Q=q)\Big]+L_1+\delta_n^{(1)}\\&\le I(U_Q;Y_{1,Q}|W_Q,V_Q,Q)-I(U_Q;Y_{2,Q}|W_Q,V_Q,Q)+L_1+n\delta_n^{(1)}\end{aligned} \tag{72}$$

Denote $Y_1\triangleq Y_{1,Q},\ Y_2\triangleq Y_{2,Q},\ W\triangleq(W_Q,Q)$, $U\triangleq(U_Q,Q)$ and $V\triangleq(V_Q,Q)$. We thus have the bounds of (12) with small added terms such as ϵ_n and $\delta_n^{(1)}$. But for large n we can make these terms approach 0. The converse is completed by noting that since the channel is memoryless and without feedback, and because $U_q=(M_1,W_q)$ and

$V_q = (M_2, W_q)$, the chain

$$(Y_{1,q}, Y_{2,q}) - X_q - (U_q, V_q) - W_q \tag{73}$$

is Markov for every $q \in [1:n]$. This implies that $(Y_1, Y_2) - X - (U, V) - W$ is a Markov chain.

D. Proof of Theorem 4

To establish the direct part of Theorem 4 we show that $\mathcal{C}_{\mathrm{SD}}(L_1, L_2) \subseteq \mathcal{R}_{\mathrm{I}}(L_1, L_2)$, which follows by setting $U_0 = W$, $U_1 = Y_1$ and $U_2 = V$ in Theorem 1.

For the converse we show that $\mathcal{R}_{\mathrm{O}}(L_1, L_2) \subseteq \mathcal{C}_{\mathrm{SD}}(L_1, L_2)$. For every PMF $P_{W,V,Y_1,X} Q_{Y_2|X}$ for which $Y_1 = f(X)$, we have the following chains of inequalities. The right-hand side (RHS) of (12b) is upper bounded by the RHS of (14a) since

$$\begin{aligned}
R_1 &\le I(U;Y_1|W,V) - I(U;Y_2|W,V) + L_1 \\
&= H(Y_1|W,V) - H(Y_1|W,V,U) - I(U;Y_2|W,V) + L_1 \\
&\overset{(a)}{\le} H(Y_1|W,V) - I(Y_1;Y_2|W,V,U) - I(U;Y_2|W,V) + L_1 \\
&= H(Y_1|W,V) - I(U,Y_1;Y_2|W,V) + L_1 \\
&\overset{(b)}{\le} H(Y_1|W,V,Y_2) + L_1
\end{aligned} \tag{74}$$

where (a) follows by the non-negativity of entropy and (b) follows because conditioning cannot increase entropy. Repeating similar steps while combining (12a) with (12b) yields (14b), i.e., we have

$$R_0 + R_1 \le H(Y_1|W,V,Y_2) + I(W;Y_1) + L_1. \tag{75}$$

Inequality (12d) implies (14c) since

$$R_0 + R_1 \le I(W,U;Y_1) \le H(Y_1). \tag{76}$$

The rate bound (14d) coincides with (12f), combining (12a) with (12f) implies (14e), while (14f) follows from (12g).

For the sum of rates, (14g) follows from (12g) and (74), while (14h) is implied by (12h) since

$$I(U;Y_1|V,W) \le H(Y_1|V,W). \tag{77}$$

Finally, by combining (12a) and (12h) while using (77) we have

$$\begin{aligned}
2R_0 + R_1 + R_2 &\le I(U;Y_1|W,V) + I(V;Y_2|W) + 2\min\big\{I(W;Y_1), I(W;Y_2)\big\} \\
&\le H(Y_1|W,V) + I(W,V;Y_2) + I(W;Y_1),
\end{aligned}$$

which implies (14i). Dropping the rest of the bounds from (12) only increases the region and shows that $\mathcal{R}_{\mathrm{O}}(L_1, L_2) \subseteq \mathcal{C}_{\mathrm{SD}}(L_1, L_2)$ (note that $\mathcal{R}_{\mathrm{O}}(L_1, L_2)$ is described by a union over PMFs that satisfy the Markov

relation $X-(U,V)-W$, while in $\mathcal{C}_{\mathrm{SD}}(L_1,L_2)$ this restriction is dropped). This characterizes $\mathcal{C}_{\mathrm{SD}}(L_1,L_2)$ as the (L_1,L_2)-leakage-capacity region of the SD-BC.

VII. Summary and Concluding Remarks

We considered the BC with privacy leakage constraints. Under this model, all four scenarios concerning secrecy (i.e., when both, either or neither of the private messages are secret) become special cases and are recovered by properly setting the leakage thresholds. Novel inner and outer bounds on the leakage-capacity region were derived and shown to be tight for SD and PD BCs, as well as for BCs with a degraded message set. Furthermore, we derived a condition on the allowed leakage values that differentiates whether a further increase of each leakage induces a larger inner bound or not. The condition effectively lets one (numerically) calculate privacy leakage threshold values above which the inner bound saturates. The coding strategy that achieved the inner bound relied on Marton's coding scheme with a common message, but with an extra layer of binning. Each private message was split into a public and a private part and the codebooks of the private parts were double-binned. Taking into account that the rate of the public parts is always leaked, the sizes of the bins in the extra layer were chosen to satisfy the total leakage constraints. The outer bound was derived by leveraging telescoping identities.

The results for the BC with leakage captures various past works. Large leakage thresholds reduce our inner and outer bounds to Marton's inner bound [18] and the UVW-outer bound [19], respectively. The leakage-capacity region of the SD-BC without a common message recovers the capacity regions where both [5], either [6], [7], or neither [24] private message is secret. The result for the BC with a degraded message set and a privacy leakage constraint captures the capacity regions for the BC with confidential messages [3] and the BC with a degraded message set (without secrecy) [25]. Furthermore, our code construction for the inner bound is leakage-adaptive and recovers the best known codes for the aforementioned cases. A Blackwell BC example visualizes the transition of the leakage-capacity region from the capacity region without secrecy to the secrecy-capacity regions for different cases.

Acknowledgements

The authors would like to thank the associate editor and the anonymous reviewers that helped us improve the presentation of this paper. We also kindly thank Ido B. Gattegno for his work on the FME-IT software [26] that assisted us with technical details of proofs.

Appendix A
Equivalence of the Regions in (22) and (23)

Denote the region in (22) by $\mathcal{C}$ and recall that the region in (23) is denoted by $\mathcal{C}^0_{\mathrm{SD}}(\infty,0)$. The inclusion $\mathcal{C}\subseteq\mathcal{C}^0_{\mathrm{SD}}(\infty,0)$ follows since (23a)-(23b) coincide with (22a)-(22c), while for (23c) we have

$$H(Y_1|W,V)+I(W,V;Y_2)=H(Y_1|W)+I(W;Y_2)+I(V;Y_2|W)-I(V;Y_1|W)\overset{(a)}{\geq}R_1+R_2. \tag{78}$$

Here (a) is due to (22b)-(22c).

To see that $\mathcal{C}_{\mathrm{SD}}^{0}(\infty,0)\subseteq\mathcal{C}$, let $(R_1,R_2)\in\mathcal{C}_{\mathrm{SD}}^{0}(\infty,0)$ be a rate pair achieved by (W,V,X). We show that there is a triple $(W^\star,V^\star,X^\star)$ for which $(R_1,R_2)\in\mathcal{C}$. First, suppose that (23b) holds with equality:

$$R_2 = I(V;Y_2|W) - I(V;Y_1|W). \tag{79}$$

By taking $W^\star = W$, $V^\star = T$ and $X^\star = X$, (22a) and (22c) hold by (23a)-(23b), while (22b) is satisfied since

$$\begin{aligned} H(Y_1|W^\star) + I(W^\star;Y_2) &\overset{(a)}{=} H(Y_1|W) + I(W;Y_2) + I(V;Y_2|W) - I(V;Y_1|W) - R_2 \\ &= H(Y_1|W,V) + I(W,V;Y_2) - R_2 \\ &\overset{(b)}{\geq} R_1, \end{aligned} \tag{80}$$

where (a) and (b) follow from (79) and (23c), respectively.

Next, assume that a strict inequality holds in (23b), i.e., there is a real number $\gamma>0$, such that

$$R_2 = I(V;Y_2|W) - I(V;Y_1|W) - \gamma. \tag{81}$$

Define $W^\star \triangleq (\Theta,\widetilde{W})$, where Θ is a binary random variable independent of (W,V,X) that takes values in $\mathcal{O}=\{\theta_1,\theta_2\}$ with probabilities $\lambda>0$ and $1-\lambda$, respectively, and

$$\widetilde{W} = \begin{cases} W\ , & \Theta=\theta_1 \\ (W,V)\ , & \Theta=\theta_2 \end{cases}. \tag{82}$$

Furthermore, let

$$\lambda = \frac{I(V;Y_2|W) - I(V;Y_1|W) - \gamma}{I(V;Y_2|W) - I(V;Y_2|W)}, \tag{83}$$

$V^\star=(W,V)$ and $X^\star = X$. Note that $X^\star - V^\star - W^\star$ forms a Markov chain and that (22a) follows from (23a). To see that (22c) holds consider:

$$I(V^\star;Y_2|W^\star) - I(V^\star;Y_1|W^\star) \overset{(a)}{=} \lambda\Big[I(V;Y_2|W) - I(V;Y_1|W)\Big] \overset{(b)}{=} I(V;Y_2|W) - I(V;Y_1|W) - \gamma \overset{(c)}{=} R_2 \tag{84}$$

where (a) follows from the definition of $(W^\star,V^\star)$, while (b) and (c) follow from (83) and (81), respectively. We conclude the proof by showing that (22b) also holds. This follows because

$$\begin{aligned} H(Y_1|W^\star) + I(W^\star;Y_2) &\overset{(a)}{=} H(Y_1|W^\star) + I(W^\star;Y_2) + I(V^\star;Y_2|W^\star) - I(V^\star;Y_1|W^\star) - R_2 \\ &= H(Y_1|W^\star,W^\star) + I(W^\star,V^\star;Y_2) - R_2 \\ &\overset{(b)}{=} H(Y_1|W,V) + I(W,V;Y_2) - R_2 \\ &\overset{(c)}{\geq} R_1 \end{aligned} \tag{85}$$

where (a) follows from (84), (b) follows since $Y_1 - V^\star - W^\star$ forms a Markov chain and $V^\star=(W,V)$, while (c)

follows from (23c).

APPENDIX B
EQUIVALENCE OF THE REGIONS IN (25) AND (26)

Denote the region in (25) by $\mathcal{C}_{CK}$ while the region in (26) is denoted by $\mathcal{C}_{\mathrm{DM}}(0)$. Since this proof mostly follows by arguments akin to those presented in Appendix A, we omit some of the detail. First, $\mathcal{C}_{CK} \subseteq \mathcal{C}_{\mathrm{DM}}(0)$ follows since (25b)-(25c) imply that (26a)-(26b) holds, while (26c) follows by combining (25a) and (25c).

For the opposite inclusion $\mathcal{C}_{\mathrm{DM}}(0) \subseteq \mathcal{C}_{CK}$, let $(R_0, R_1) \in \mathcal{C}_{\mathrm{DM}}(0)$ be a rate pair achieved by (W, U, X). We construct a triple $(W^\star, U^\star, X^\star)$ that satisfies $W^\star - U^\star - X^\star - (Y_1, Y_2)$ for which $(R_0, R_1) \in \mathcal{C}_{CK}$. If (26b) holds with equality, i.e., if

$$R_1 = I(U; Y_1|W) - I(U; Y_2|W), \tag{86}$$

then we take $W^\star = W$, $U^\star = U$ and $X^\star = X$. With respect to this choice (25b)-(25c) follows from (26a)-(26b), while (25a) is satisfied by combining (86) with (26c).

If, on the other hand, a strict inequality holds in (26b), i.e., we have

$$R_1 = I(U; Y_1|W) - I(U; Y_2|W) - \gamma \tag{87}$$

where γ is a real and positive number, then we define $W^\star \triangleq (\Theta, \widetilde{W})$. Here Θ is a binary random variable independent of (W, U, X) as in Appendix A, and

$$\widetilde{W} = \begin{cases} W\ , & \Theta = \theta_1 \\ U\ , & \Theta = \theta_2 \end{cases}. \tag{88}$$

Furthermore, set

$$\lambda = \frac{I(U; Y_1|W) - I(U; Y_2|W) - \gamma}{I(U; Y_1|W) - I(U; Y_2|W)}, \tag{89}$$

$U^\star = U$ and $X^\star = X$. Note that $(Y_1, Y_2) - X^\star - U^\star - W^\star$ forms a Markov chain and consider the following.

$$I(W^\star; Y_2) = \lambda I(W; Y_2) + (1-\lambda) I(U; Y_2) \overset{(a)}{=} I(W; Y_2) + (1-\lambda) I(U; Y_2|W) \geq I(W; Y_2) \overset{(b)}{=} R_0 \tag{90}$$

where (a) follows from (89) and (b) follows from (26a). Thus, (25b) is satisfied. To see that (25c) holds consider:

$$I(U^\star; Y_1|W^\star) - I(U^\star; Y_2|W^\star) \overset{(a)}{=} \lambda \Big[I(U; Y_1|W) - I(U; Y_2|W) \Big] \overset{(b)}{=} I(U; Y_1|W) - I(U; Y_2|W) - \gamma \overset{(c)}{=} R_1 \tag{91}$$

where (a) follows from the definition of $(W^\star, U^\star)$, while (b) and (c) follow from (89) and (87), respectively. It remains to show that (25a) also holds. We begin by writing

$$I(U^\star; Y_2|W^\star) \overset{(a)}{=} \lambda I(U; Y_2|W) \leq I(U; Y_2|W), \tag{92}$$

where (a) follows from the definition of $(W^\star, U^\star)$. Finally, (25a) follows because

$$\begin{aligned} I(W^\star;Y_1) &\overset{(a)}{=} I(U^\star;Y_1|W^\star) - I(U^\star;Y_2|W^\star) + I(W^\star;Y_1) - R_1 \\ &\overset{(b)}{\geq} I(W^\star,U;Y_1) - I(U;Y_2|W) - R_1 \\ &\overset{(c)}{\geq} I(W,U;Y_1) - I(U;Y_2|W) - R_1 \\ &\overset{(d)}{\geq} R_0 \end{aligned} \tag{93}$$

where (a) follows from (91); (b) follows because $U^\star = U$ and by using (92); (c) follows since $Y_1 - U - W^\star$ and $Y_1 - U - W$ form Markov chains, which implies that $I(W^\star, U; Y_1) = I(U; Y_1) = I(W, U; Y_1)$; (d) follows from (26c).

APPENDIX C
PROOF OF COROLLARY 8

The region $\mathcal{C}_{\mathrm{D}}(L_1, L_2)$ is obtained from $\mathcal{C}^0_{\mathrm{SD}}(L_1, L_2)$ by setting $W = 0$ and $V = Y_2$, which implies that $\mathcal{C}_{\mathrm{D}}(L_1, L_2) \subseteq \mathcal{C}^\star_{\mathrm{SD}}(L_1, L_2)$. For the converse, the RHS of (17a) is upper bounded by

$$R_1 \leq H(Y_1|W, V, Y_2) + L_1 \leq H(Y_1|Y_2) + L_1. \tag{94}$$

For (17c) and (17d), respectively, we have

$$\begin{aligned} I(V;Y_2|W) - I(V;Y_1|W) + L_2 &\leq I(V;Y_1,Y_2|W) - I(V;Y_1|W) + L_2 \\ &= I(V;Y_2|W,Y_1) + L_2 \\ &\leq H(Y_2|Y_1) + L_2 \end{aligned} \tag{95}$$

and

$$I(W, V; Y_2) \leq H(Y_2). \tag{96}$$

Finally, (28c) is implied by (17f) since

$$\begin{aligned} R_1 + R_2 &\leq H(Y_1|W,V) + I(V;Y_2|W) + \min\left\{I(W;Y_1), I(W;Y_2)\right\} \\ &\leq H(Y_1|W,V) + I(W,V;Y_2) \\ &\leq H(Y_1,Y_2|W,V) + I(W,V;Y_1,Y_2) \\ &= H(Y_1,Y_2). \end{aligned} \tag{97}$$

To complete the proof we drop (17e), which can only increase $\mathcal{C}^{(0)}_{\mathrm{SD}}(L_1, L_2)$.

APPENDIX D
ERROR PROBABILITY ANALYSIS FOR THE PROOF OF THEOREM 1

By the symmetry of the codebook construction with respect to $(M_0, M_1, M_2, W_1, W_2)$ and due to their uniformity, we may assume that $(M_0, M_1, M_2, W_1, W_2) = (1, 1, 1, 1, 1)$. Furthermore, because we are dealing with the expected error probability over the ensemble of codebooks, the subsequent error events are defined with respect to a new PMF $\Gamma \in \mathcal{P}(\mathcal{B} \times \mathcal{I}_1 \times \mathcal{I}_2 \times \mathcal{Y}_1^n \times \mathcal{Y}_2^n)$ that describes the random experiment of transmitting $(M_0, M_1, M_2, W_1, W_2) = (1, 1, 1, 1, 1)$ using a random codebook. Specifically, we have

$$\begin{aligned}
&\Gamma\left(\left\{\mathbf{u}_0(m_p)\right\}_{m_p}, \left\{\mathbf{u}_1(m_p^{(1)}, m_{11}, i_1', w_1)\right\}_{(m_p^{(1)}, m_{11}, i_1', w_1)}, \left\{\mathbf{u}_2(m_p^{(2)}, m_{22}, i_2', w_2)\right\}_{(m_p^{(2)}, m_{22}, i_2', w_2)}, i_1, i_2, \mathbf{y}_1, \mathbf{y}_2\right) \\
&= \prod_{m_p} P_{U_0}^n\big(\mathbf{u}_0(m_p)\big) \prod_{j=1,2} \left(\prod_{(m_p^{(j)}, m_{jj}, i_j', w_j)} P_{U_j|U_0}^n\Big(\mathbf{u}_j(m_p^{(j)}, m_{jj}, i_j', w_j)\Big|\mathbf{u}_0(m_p^{(j)})\Big) \right) \\
&\qquad \times \Gamma\Big(i_1, i_2\Big|\mathbf{u}_0(1), \left\{\mathbf{u}_1(1, 1, i_1', 1)\right\}_{i_1'}, \left\{\mathbf{u}_2(1, 1, i_2', 1)\right\}_{i_2'}\Big) \\
&\qquad \times Q_{Y_1, Y_2|U_0, U_1, U_2}^n\big(\mathbf{y}_1, \mathbf{y}_2\big|\mathbf{u}_0(1), \mathbf{u}_1(1, 1, i_1, 1), \mathbf{u}_2(1, 1, i_2, 1)\big), \quad (98)
\end{aligned}$$

where $\Gamma\Big(i_1, i_2\Big|\mathbf{u}_0(1), \left\{\mathbf{u}_1(1, 1, i_1', 1)\right\}_{i_1'}, \left\{\mathbf{u}_2(1, 1, i_2', 1)\right\}_{i_2'}\Big)$ chooses $(i_1, i_2) \in \mathcal{I}_1 \times \mathcal{I}_2$ according to the encoding rule described in Section VI-A, and

$$Q_{Y_1, Y_2|U_0, U_1, U_2}(y_1, y_2|u_0, u_1, u_2) \triangleq \sum_{x \in \mathcal{X}} P_{X|U_0, U_1, U_2}(x|u_0, u_1, u_2) Q_{Y_1, Y_2|X}(y_1, y_2|x).$$

The probability measure induced by Γ is denote by $\mathbb{P}_\Gamma$.

A. Encoding/Decoding Errors

Consider the following error events.

Encoding errors: An encoding error event is described as

$$\mathcal{E} = \bigcap_{(i_1, i_2) \in \mathcal{I}_1 \times \mathcal{I}_2} \Big\{\big(\mathbf{U}_0(1), \mathbf{U}_1(1, 1, i_1, 1), \mathbf{U}_2(1, 1, i_2, 1)\big) \notin \mathcal{T}_\epsilon^n(P_{U_0, U_1, U_2})\Big\}. \quad (99)$$

Decoding errors: To account for decoding errors, define

$$\mathcal{D}_0 = \Big\{\big(\mathbf{U}_0(1), \mathbf{U}_1(1, 1, I_1, 1), \mathbf{U}_2(1, 1, I_2, 1), \mathbf{Y}_1\big) \in \mathcal{T}_\epsilon^n(P_{U_0, U_1, U_2, Y_j})\Big\} \quad (100a)$$

and

$$\mathcal{D}_j(m_p, m_{jj}, i_j, w_j) = \Big\{\big(\mathbf{U}_0(m_p), \mathbf{U}_1(m_p, m_{jj}, i_j, w_j), \mathbf{Y}_1\big) \in \mathcal{T}_\epsilon^n(P_{U_0, U_j, Y_j})\Big\}, \quad (100b)$$

where $j = 1, 2$.

By the union bound, the expected error probability is bounded as

$$\begin{aligned}
\mathbb{E}P_e(\mathbb{C}) &\leq \mathbb{P}_\Gamma\Bigg(\mathcal{E}\cup\mathcal{D}_0^c\cup\mathcal{D}_1(1,1,I_1,1)^c\cup\mathcal{D}_2(1,1,I_2,1)^c \\
&\qquad\cup\left\{\bigcup_{(\tilde{m}_p,\tilde{m}_{11},\tilde{w}_1)\neq(1,1,1)}\mathcal{D}_1(\tilde{m}_p,\tilde{m}_{11},I_1,\tilde{w}_1)\right\}\cup\left\{\bigcup_{(\tilde{m}_p,\tilde{m}_{22},\tilde{w}_2)\neq(1,1,1)}\mathcal{D}_2(\tilde{m}_p,\tilde{m}_2,I_2,\tilde{w}_2)\right\}\Bigg) \\
&\leq \mathbb{P}_\Gamma\big(\mathcal{E}\big)+\mathbb{P}_\Gamma\big(\mathcal{D}_0^c\cap\mathcal{E}^c\big)+\sum_{j=1,2}\Bigg[\mathbb{P}_\Gamma\Big(\mathcal{D}_j(1,1,I_j,1)^c\cap\mathcal{D}_0\Big) \\
&\qquad+\mathbb{P}_\Gamma\left(\bigcup_{(\tilde{m}_p,\tilde{m}_{jj},\tilde{w}_j)\neq(1,1,1)}\mathcal{D}_j(\tilde{m}_p,\tilde{m}_{jj},I_j,\tilde{w}_j)\right)\Bigg] \\
&\leq \underbrace{\mathbb{P}_\Gamma\big(\mathcal{E}\big)}_{P_0^{[1]}}+\underbrace{\mathbb{P}_\Gamma\big(\mathcal{D}_0^c\cap\mathcal{E}^c\big)}_{P_0^{[2]}}+\sum_{j=1,2}\Bigg[\underbrace{\mathbb{P}_\Gamma\Big(\mathcal{D}_j(1,1,I_j,1)^c\cap\mathcal{D}_0\Big)}_{P_j^{[1]}}+\underbrace{\sum_{\tilde{i}_j\in\mathcal{I}_j}\Gamma\big(\tilde{i}_j\big)\mathbb{P}_\Gamma\left(\bigcup_{m_p\neq 1}\mathcal{D}_j(\tilde{m}_p,1,\tilde{i}_j,1)\right)}_{P_j^{[2]}} \\
&\qquad\underbrace{+\mathbb{P}_\Gamma\left(\bigcup_{\substack{(\tilde{m}_{jj},\tilde{w}_j)\neq(1,1),\\ \tilde{i}_j\in\mathcal{I}_j}}\mathcal{D}_j(1,\tilde{m}_{jj},\tilde{i}_j,\tilde{w}_j)\right)}_{P_j^{[3]}}+\underbrace{\mathbb{P}_\Gamma\left(\bigcup_{\substack{(\tilde{m}_p,\tilde{m}_{jj},\tilde{w}_j)\neq(1,1,1),\\ \tilde{i}_j\in\mathcal{I}_j}}\mathcal{D}_j(\tilde{m}_p,\tilde{m}_{jj},\tilde{i}_j,\tilde{w}_j)\right)}_{P_j^{[4]}}\Bigg]
\end{aligned} \tag{101}$$

Note that $P_0^{[1]}$ is the probability of an encoding error, while $P_0^{[2]}$ and $P_j^{[k]}$, for $k\in[1:4]$, correspond to decoding errors by Decoder j. We proceed with the following steps:

1) By the Multivariate Covering Lemma [40, Lemma 8.2], $P_0^{[1]}\to 0$ as $n\to\infty$ if we have

$$R_1'+R_2'>I(U_1;U_2|U_0), \tag{102}$$

while the Conditional Typicality Lemma [40, Section 2.5] implies that $P_0^{[2]}\to 0$ as n grows. Furthermore, the definitions in (100) clearly imply that $P_j^{[1]}=0$, for all $n\in\mathbb{N}$.

2) For $P_j^{[3]}$, $j=1,2$, we have

$$\begin{aligned} P_j^{[3]} &\overset{(a)}{\leq} \sum_{\substack{(\tilde{m}_{jj},\tilde{w}_j)\neq(1,1),\\ \tilde{i}_j\in\mathcal{I}_j}} 2^{-n\left(I(U_j;Y_j|U_0)-\delta_\epsilon^{[3]}\right)} \\ &\leq 2^{n(R_{jj}+R'_j+\tilde{R}_j)}2^{-n\left(I(U_j;Y_j|U_0)-\delta_\epsilon^{[3]}\right)} \\ &= 2^{n\left(R_{jj}+R'_j+\tilde{R}_j-I(U_j;Y_j|U_0)+\delta_\epsilon^{[3]}\right)} \end{aligned}$$

where (a) follows since for any $(\tilde{m}_{jj},\tilde{w}_j)\neq(1,1)$ and $\tilde{i}_j\in\mathcal{I}_j$, $\mathbf{U}_j(1,\tilde{m}_{jj},\tilde{i}_j,\tilde{w}_j)$ is independent of $\mathbf{Y}_j$ while both of them are drawn conditioned on $\mathbf{U}_0(1)$. Moreover, $\delta_\epsilon^{[3]}\to 0$ as $\epsilon\to 0$. Hence, for the probability $P_j^{[3]}$ to vanish as $n\to\infty$, we take:

$$R_{jj}+R'_j+\tilde{R}_j < I(U_j;Y_j|U_0), \quad j=1,2. \tag{103}$$

3) For $P_j^{[4]}$, $j=1,2$, consider

$$\begin{aligned} P_j^{[4]} &\overset{(a)}{\leq} \sum_{\substack{(\tilde{m}_p,\tilde{m}_{jj},\tilde{w}_j)\neq(1,1,1),\\ \tilde{i}_j\in\mathcal{I}_j}} 2^{-n\left(I(U_0,U_1;Y_1)-\delta_\epsilon^{[4]}\right)} \\ &\leq 2^{n(R_p+R_{jj}+R'_j+\tilde{R}_j)}2^{-n\left(I(U_0,U_j;Y_j)-\delta_\epsilon^{[4]}\right)} \\ &= 2^{n\left(R_p+R_{jj}+R'_j+\tilde{R}_j-I(U_0,U_j;Y_j)+\delta_\epsilon^{[4]}\right)} \end{aligned}$$

where (a) follows since for any $(\tilde{m}_p,\tilde{m}_{jj},\tilde{w}_j)\neq(1,1,1)$ and $\tilde{i}_j\in\mathcal{I}_j$, $\mathbf{U}_0(\tilde{m}_p)$ and $\mathbf{U}_j(\tilde{m}_p,\tilde{m}_{jj},\tilde{i}_j,\tilde{w}_j)$ are correlated with one another but independent of $\mathbf{Y}_j$. As before, $\delta_\epsilon^{[4]}\to 0$ as $\epsilon\to 0$, and therefore, we have that $P_j^{[4]}\to 0$ as $n\to\infty$ if

$$R_p+R_{jj}+R'_j+\tilde{R}_j < I(U_0,U_j;Y_j), \quad j=1,2. \tag{104}$$

4) For $j=1,2$, similar steps as in the upper bounding of $P_j^{[3]}$ show that the rate bound that ensures that $P_j^{[2]}\to 0$ as $n\to\infty$ is redundant. This is since for every $\tilde{m}_p\neq 1$ and $\tilde{i}_j\in\mathcal{I}_j$, the codewords $\mathbf{U}_0(\tilde{m}_p)$ and $\mathbf{U}_j(\tilde{m}_p,1,\tilde{i}_j,1)$ are independent of $\mathbf{Y}_j$. Hence, taking

$$R_p < I(U_0,U_j;Y_j), \quad j=1,2, \tag{105}$$

suffices for $P_j^{[2]}$ to vanish. However, the RHS of (105) coincides with the RHS of (104), while the left-hand side (LHS) of (105) is with respect to R_p only. Clearly, (104) is the dominating constraint.

Summarizing the above results, while substituting $R_p=R_0+R_{10}+R_{20}$, we find that the RHS of (101) decays as the blocklength $n\to\infty$ if the conditions in (38) are met.

B. Leakage Associated Errors

To satisfy the leakage constraints in (6b)-(6c) we account for the error in decoding $\mathbf{U}_j$ from $\big(M_{11}, \mathbf{U}_0(1), \mathbf{U}_{\bar{j}}(1,1,I_{\bar{j}},1), \mathbf{Y}_{\bar{j}}\big)$, where $j=1,2$ and $\bar{j}=j+(-1)^{j+1}$. Since $M_1=1$ is fixed and $\mathbf{U}_0(1)$ and $\mathbf{U}_{\bar{j}}(1,1,I_{\bar{j}},1)$ are given, the code design implies that decoding $\mathbf{U}_j$ boils down to decoding W_j. By repeating similar arguments to those presented in the encoding/decoding error analysis we have the $\mathbb{E}\lambda_1(\mathbb{C})\to 0$ as $n\to\infty$ if (39) hold.

APPENDIX E
PROOF OF LEMMAS 9 AND 10

A. Proof of Lemma 9

We prove (41a) only. The proof of (41b) follows similar lines. For every $(\mathbf{u}_0,\mathbf{u}_1,\mathbf{u}_2)\in\mathcal{U}^n\times\mathcal{U}_1^n\times\mathcal{U}_2^n$ define

$$\nu(\mathbf{u}_0,\mathbf{u}_1,\mathbf{u}_2)=\begin{cases}1, & (\mathbf{u}_0,\mathbf{u}_1,\mathbf{u}_2)\notin\mathcal{T}_\epsilon^n(P_{U_0,U_1,U_2})\\ 0, & \text{otherwise}\end{cases}, \tag{106}$$

which we abbreviate as ν. The multi-letter mutual information term in the LHS of (41a) is expanded as follows

$$\begin{aligned}I(\mathbf{U}_1;\mathbf{U}_2|\mathbf{U}_0,\mathbb{C}) &\le I(\mathbf{U}_1,\nu;\mathbf{U}_2|\mathbf{U}_0,\mathbb{C})\\ &= I(\nu;\mathbf{U}_2|\mathbf{U}_0,\mathbb{C})+I(\mathbf{U}_1;\mathbf{U}_2|\mathbf{U}_0,\nu,\mathbb{C})\\ &= I(\nu;\mathbf{U}_2|\mathbf{U}_0,\mathbb{C})+\sum_{j=0}^{1}\mathbb{P}(\nu=j)I(\mathbf{U}_1;\mathbf{U}_2|\mathbf{U}_0,\nu=j,\mathbb{C}).\end{aligned} \tag{107}$$

Note that

$$\begin{aligned}\mathbb{P}(\nu=1)I(\mathbf{U}_1;\mathbf{U}_2|\mathbf{U}_0,\nu=1,\mathbb{C}) &\le \mathbb{P}\big((\mathbf{U}_0,\mathbf{U}_1,\mathbf{U}_2)\notin\mathcal{T}_\epsilon^n(P_{U_0,U_1,U_2})\big)H(\mathbf{U}_2|\nu=1,\mathbb{C})\\ &\le n\mathbb{P}\big((\mathbf{U}_0,\mathbf{U}_1,\mathbf{U}_2)\notin\mathcal{T}_\epsilon^n(P_{U_0,U_1,U_2})\big)\log|\mathcal{U}_2|\\ &\overset{(a)}{\le} n\eta_\epsilon^{(1)}\log|\mathcal{U}_2|.\end{aligned} \tag{108}$$

Here (a) follows by the properties the random code construction and $\eta_\epsilon^{(1)}$ decreases as e^{-cn} for some constant $c>0$ [31, Lemma 5]. Furthermore, we have

$$\begin{aligned}\mathbb{P}(\nu=0)I(\mathbf{U}_1;\mathbf{U}_2|\mathbf{U}_0,\nu=0,\mathbb{C}) &\le I(\mathbf{U}_1;\mathbf{U}_2|\mathbf{U}_0,\nu=0,\mathbb{C})\\ &= \sum_{(\mathbf{u}_0,\mathbf{u}_1,\mathbf{u}_2)\in\mathcal{T}_\epsilon^n(P_{U_0,U_1,U_2})}P(\mathbf{u}_0,\mathbf{u}_1,\mathbf{u}_2)\log\left(\frac{P(\mathbf{u}_1,\mathbf{u}_2|\mathbf{u}_0)}{P(\mathbf{u}_1|\mathbf{u}_0)P(\mathbf{u}_2|\mathbf{u}_0)}\right)\\ &= \sum_{(\mathbf{u}_0,\mathbf{u}_1,\mathbf{u}_2)\in\mathcal{T}_\epsilon^n(P_{U_0,U_1,U_2})}P(\mathbf{u}_0,\mathbf{u}_1,\mathbf{u}_2)\log\left(\frac{2^{-nH(U_1,U_2|U_0)(1-\epsilon)}}{2^{-nH(U_1|U_0)(1+\epsilon)}2^{-nH(U_2|U_0)(1+\epsilon)}}\right)\\ &\le nI(U_1;U_2|U_0)+n\eta_\epsilon^{(2)}\end{aligned} \tag{109}$$

where $\eta_\epsilon^{(2)} = 3\epsilon H(U_1, U_2|U_0)$. Inserting (108)-(109) into (107) yields

$$\begin{aligned} I(\mathbf{U}_1; \mathbf{U}_2|\mathbf{U}_0, \mathbb{C}) &\overset{(a)}{\leq} n\eta_\epsilon^{(1)} \log|\mathcal{U}_2| + nI(U_1; U_2|U_0) + n\eta_\epsilon^{(2)} + 1 \\ &\overset{(b)}{=} nI(U_1; U_2|U_0) + n\epsilon_1 \end{aligned} \tag{110}$$

where (a) follows since $I(\nu; \mathbf{U}_1|\mathbf{U}_0, \mathbb{C}) \leq H(\nu) \leq 1$, while (b) follows by setting $\epsilon_1 = \eta_\epsilon^{(1)} \log|\mathcal{U}_2| + \eta_\epsilon^{(2)} + \frac{1}{n}$.

B. Proof of Lemma 10

Recall that $\lambda_{m_1}(\mathcal{C})$ denotes the error probability in decoding $\mathbf{u}_1(m_p, m_{11}, i_1, w_1, \mathcal{B}_{0,1})$ from $\big(\mathbf{u}_0(m_p, \mathcal{B}_0), \mathbf{u}_2(m_p, m_{22}, i_2, w_2, \mathcal{B}_{0,2}), \mathbf{y}_2\big)$ when $M_1 = m_1 \in \mathcal{M}_1$ is fixed and the code $\mathcal{C} \in \mathfrak{C}$ is used. By the properties of the random code $\mathbb{C}$ we have

$$\mathbb{E}\lambda_{m_1}(\mathbb{C}) \leq \eta_\epsilon^{(3)}, \quad \forall m_1 \in \mathcal{M}_1, \tag{111}$$

where $\eta_\epsilon^{(3)}$ decreases as $e^{-\gamma n}$ for some real number $\gamma > 0$. By Fano's inequality, we have

$$H(\mathbf{U}_1|M_1 = m_1, \mathbf{U}_0, \mathbf{U}_2, \mathbf{Y}_2, \mathbb{C}) \leq n\epsilon_3, \tag{112}$$

where $\epsilon_3 = \frac{1}{n} + \eta_\epsilon^{(3)} R_1$, which implies

$$H(\mathbf{U}_1|M_1, \mathbf{U}_0, \mathbf{U}_2, \mathbf{Y}_2, \mathbb{C}) = \sum_{m_1 \in \mathcal{M}_1} 2^{-nR_1} H(\mathbf{U}_1|M_1 = m_1, \mathbf{U}_0, \mathbf{U}_2, \mathbf{Y}_2, \mathbb{C}) \leq n\epsilon_3. \tag{113}$$

REFERENCES

[1] C. E. Shannon. Communication theory of secrecy systems. *Bell Sys. Techn.*, 28(4):656715, Oct. 1949.

[2] A. D. Wyner. The wire-tap channel. *Bell Sys. Techn.*, 54(8):1355–1387, Oct. 1975.

[3] I. Csiszár and J. Körner. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 24(3):339–348, May 1978.

[4] R. Liu, I. Maric, P. Spasojević, and R. D. Yates. Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions. *IEEE Trans. Inf. Theory*, 54(6):2493–2507, Jun. 2008.

[5] Y. Zhao, P. Xu, Y. Zhao, W. Wei, and Y. Tang. Secret communications over semi-deterministic broadcast channels. In *Fourth Int. Conf. Commun. and Netw. in China (CHINACOM)*, Xi'an, China, Aug. 2009.

[6] W. Kang and N. Liu. The secrecy capacity of the semi-deterministic broadcast channel. In *Proc. Int. Symp. Inf. Theory*, Seoul, Korea, Jun.-Jul. 2009.

[7] Z. Goldfeld, G. Kramer, and H. H. Permuter. Cooperative broadcast channels with a secret message. In *Proc. Int. Symp. Inf. Theory (ISIT-2015)*, Hong Kong, China, Jun. 2015.

[8] E. Ekrem and S. Ulukus. Secrecy in cooperative relay broadcast channels. *IEEE Trans. Inf. Theory*, 57(1):137–155, Jan. 2011.

[9] R. Liu and H. Poor. Secrecy capacity region of a multiple-antenna Gaussian broadcast channel with confidential messages. *IEEE Trans. Inf. Theory*, 55(3):1235–1249, Mar. 2009.

[10] T. Liu and S. Shamai. A note on the secrecy capacity of the multiple-antenna wiretap channel. *IEEE Trans. Inf. Theory*, 6(6):2547–2553, Jun. 2009.

[11] R. Liu, T. Liu, H. V. Poor, and S. Shamai. Multiple-input multiple-output Gaussian broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 56(9):4215–4227, Sep. 2010.

[12] A. Khisti and G. W. Wornell. Secure transmission with multiple antennas - part II: The MIMOME channel. *IEEE Trans. Inf. Theory*, 56(11):5515–5532, Nov. 2010.

[13] E. Ekrem and S. Ulukus. The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel. *IEEE Trans. Inf. Theory*, 57(4):2083–2114, Apr. 2011.

[14] F. Oggier and B. Hassibi. The secrecy capacity of the MIMO wiretap channel. *IEEE Trans. Inf. Theory*, 57(8):4961–4972, Aug. 2011.

[15] E. Ekrem and S. Ulukus. Secrecy capacity of a class of broadcast channels with an eavesdropper. *EURASIP Journal on Wireless Commun. and Netw.*, 2009(1):1–29, Mar. 2009.

[16] G. Bagherikaram, A. Motahari, and A. Khandani. Secrecy capacity region of Gaussian broadcast channel. In *43rd Annual Conf. on Inf. Sci. and Sys. (CISS) 2009*, pages 152–157, Baltimore, MD, US, Mar. 2009.

[17] M. Benammar and P. Piantanida. Secrecy capacity region of some classes of wiretap broadcast channels. *Available on ArXiv*, Jul. 2014. http://arxiv.org/abs/1407.5572.

[18] Y. Liang and G. Kramer. Rate regions for relay broadcast channels. *IEEE Trans. Inf. Theory*, 53(10):3517–3535, Oct 2007.

[19] C. Nair. *A note on outer bounds for broadcast channel*. Presented at International Zurich Seminar, Jan. 2011. Available on ArXiV at http://arXiv.org/abs/1101.0640.

[20] G. Kramer Y. Liang and S. Shamai. Capacity outer bounds for broadcast channels. In *IEEE Inf. Theory Workshop (ITW-2008)*, Porto, Portugal, 2008.

[21] Y. Liang. *Multiuser communications with relaying and user cooperation*. PhD thesis, Ph.D. dissertation, Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, Illinois, 2005.

[22] C. Nair and A. El Gamal. An outer bound to the capacity region of the broadcast channel. *IEEE Trans. Inf. Theory*, 53(1):350–355, Jan. 2007.

[23] C. Nair and V. W. Zizhou. On the inner and outer bounds for 2-receiver discrete memoryless broadcast channels. In *Inf. Theory and Applic. Workshop*, San Diego, California, US, Jan. 27-Feb. 1 2008.

[24] S. I. Gelfand and M. S. Pinsker. Capacity of a broadcast channel with one deterministic component. *Prob. Pered. Inf. (Problems of Inf. Transm.)*, 16(1):17–25, Jan-Mar 1980.

[25] J. Körner and K. Marton. General broadcast channels with degraded message sets. *IEEE Trans. Inf. Theory*, 23(1):60–64, Jan. 1977.

[26] I. B. Gattegno, Z. Goldfeld, and H. H. Permuter. Fourier-Motzkin Elimination software for information theoretic inequalities. *IEEE Inf. Theory Society Newsletter*, 65(3):25–28, Sep. 2015. Version R0.6 Available at http://www.ee.bgu.ac.il/~fmeit/.

[27] G. Kramer. Teaching IT: An identity for the Gelfand-Pinsker converse. *IEEE Inf. Theory Society Newsletter*, 61(4):4–6, Dec. 2011.

[28] E. C. van der Meulen. Random coding theorems for the general discrete memoryless broadcast channel. *IEEE Trans. Inf. Theory*, IT-21(2):180–190, May 1975.

[29] S. I. Gelfand. Capacity of one broadcast channel. *Probl. Peredachi Inf.*, 13(3):106108, Jul./Sep. 1977.

[30] J. L. Massey. *Applied Digital Information Theory*. ETH Zurich, Zurich, Switzerland, 1980-1998.

[31] A. Orlitsky and J. Roche. Coding for computing. *IEEE Trans. Inf. Theory*, 47(3):903–917, Mar 2001.

[32] H. Weingarten, Y. Steinberg, and S. Shamai. The capacity region of the Gaussian multiple-input multiple-output broadcast channel. *IEEE Trans. Inf. Theory*, 52(9):3936–3964, Sep. 2006.

[33] R. Liu, T. Liu, H. V. Poor, and S. Shamai. Multiple-input multiple-output Gaussian broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 56(9):4215–4227, Sep. 2010.

[34] E. Ekrem and S. Ulukus. Capacity region of Gaussian MIMO broadcast channels with common and confidential messages. *IEEE Trans. Inf. Theory*, 58(9):5669–5680, Sep. 2012.

[35] Y. Geng and C. Nair. The capacity region of the two-receiver vector Gaussian broadcast channel with private and common messages. *IEEE Trans. Inf. Theory*, 60(4):2087–2014, Apr. 2014.

[36] Z. Goldfeld. MIMO Gaussian broadcast channels with common, private and confidential messages. *Submitted to IEEE Trans. Inf. Theory*, 2016.

[37] A. El Gamal and Y.-H. Kim. *Network Information Theory*. Cambridge University Press, 2011.

[38] A. Gohari, C. Nair, and V. Anantharam. Improved cardinality bounds on the auxiliary random variables in Marton's inner bound. In *Proc. Int. Symp. Inf. Theory (ISIT-2013)*, Istanbul, Turkey, Jul. 2013.

[39] K. Marton. A coding theorem for the discrete memoryless broadcast channel. *IEEE Trans. Inf. Theory*, 25(3):306–311, May 1979.

[40] A. El Gamal and Y.-H. Kim. *Network Information Theory*. Cambridge University Press, 2011.

[41] G. Kramer. Capacity results for the discrete memoryless networks. *IEEE. Trans. Inf. Theory*, 49(1):4–21, Jan. 2003.

[42] M. Bloch and J. Barros. *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge Univ. Press, Cambridge, UK, Oct. 2011.