Two-Multicast Channel With Confidential Messages

Hassan ZivariFard, *Graduate Student Member, IEEE*, Matthieu R. Bloch, *Senior Member, IEEE*, and Aria Nosratinia, *Fellow, IEEE*

***Abstract*— Motivated in part by the problem of secure multicast distributed storage, we analyze secrecy rates for a channel in which two transmitters simultaneously multicast to two receivers in the presence of an eavesdropper. Achievable rates are calculated via extensions of a technique due to Chia and El Gamal and the method of output statistics of random binning. Outer bounds are derived for both the degraded and non-degraded versions of the channel, and examples are provided in which the inner and outer bounds meet. The inner bounds recover known results for the multiple-access wiretap channel, broadcast channel with confidential messages, and the compound MAC channel. An auxiliary result is also produced that derives an inner bound on the minimal randomness necessary to achieve secrecy in multiple-access wiretap channels.**

***Index Terms*— Multicasting, compound channel, confidential messages, randomness constraint, stochastic encoder, wire-tap channel.**

I. Introduction

WE STUDY the multiuser secure multicast problem (Fig. 1), more specifically, when two transmitters multicast messages securely to two receivers in the presence of an eavesdropper. All senders, receivers, and eavesdropper are at different terminals. This problem is motivated in part by secure access of multiple users to data in a distributed cache [1], [2]. Another application of the considered model is a common situation in cellular networks, in which a user is in the coverage range of two different base stations [3], [4]. This problem is also equivalent to a one-transmitter two-receiver compound channel with confidential messages with two different states [5]. It has been known [6] that problems involving compound channels have an equivalent multicast representation, in which the channel to each multicast receiver is equivalent to one of the states of the compound channel.[1]

Manuscript received July 23, 2020; revised November 25, 2020; accepted January 6, 2021. Date of publication January 27, 2021; date of current version April 1, 2021. The work of Hassan ZivariFard and Aria Nosratinia was supported by the National Science Foundation (NSF) under Grant 1956213. The work of Matthieu R. Bloch was supported by the National Science Foundation (NSF) under Grant 1527387 and Grant 1955401. This article was presented in part at the 55th Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, USA, September 2017. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Stefano Tomasin. *(Corresponding author: Aria Nosratinia.)*

Hassan ZivariFard and Aria Nosratinia are with the Department of Electrical Engineering, The University of Texas at Dallas, Richardson, TX 75080 USA (e-mail: hassan@utdallas.edu; aria@utdallas.edu).

Matthieu R. Bloch is with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332 USA (e-mail: matthieu.bloch@ece.gatech.edu).

Digital Object Identifier 10.1109/TIFS.2021.3055031

[1]The problem studied herein is the secrecy counterpart of the classical problem posed by Ahlswede [7], which proved highly influential for the MAC channel [8] and the interference channel [9].

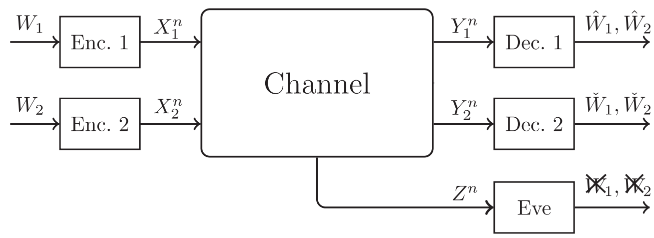

Fig. 1. Two-sender two-receiver channel with an eavesdropper.

This paper takes a two-pronged approach to the analysis of the network mentioned above, producing a number of new results and insights. In Section III, we present an analysis inspired by the work of Chia and El Gamal [10], which uses Marton coding and indirect decoding (also known as non-unique decoding) [11] to achieve an improved secrecy rate for the transmission of *one* common message to two receivers that may experience different channel statistics. In extending the method of Chia and El Gamal to multiple transmitters, we introduce a two-level Marton-type coding with associated non-unique decoding.

In Section VI, we employ the method of output statistics of random binning (OSRB) [12] for analyzing the two-transmitter two-receiver problem (see also [13] for a related approach). OSRB analyzes channel coding problems by conversion to a related source coding problem, where it tests achievability by probability approximation rather than counting arguments on typical sets, followed by a reverse conversion to complete the analysis. OSRB is well suited for secrecy problems because secrecy is tightly related to probability approximation. OSRB encoding is purely by random binning and is enabled by (and named after) the following asymptotic result: apply two independent random binning schemes on the same set and take a random sample from the set. The two bin indices corresponding to the random sample are statistically independent as long as binning rates are sufficiently small [12]–[14]. We extend the tools and techniques of OSRB to match the requirements of the two-transmitter multicast problem.

The different parts of this paper complement each other, producing a more complete picture in the understanding of the problem of multi-transmitter secure multicast. The extension of the method of Chia and El Gamal is utilized to highlight the minimal amount of randomness required to achieve secrecy rates over the multiple-access wiretap channel, and that therein channel prefixing can be replaced with superposition, in a manner reminiscent of Watanabe and Oohama [15] for minimizing the randomness resources for secrecy encoding. The analysis based on OSRB generates the strong secrecy, which interestingly has an expression that is a superset of the achievable region under weak secrecy calculated in the first part. Furthermore, the expression for the strong secrecy region can be greatly simplified via a constraint found in the weak secrecy analysis, highlighting the synergy between the two. More broadly, the developments in these two parts each offer techniques and insights that can potentially be useful in a wider class of problems.

Outer bounds for degraded and non-degraded channels are derived and shown to be tight against inner bounds in some special cases.

A brief outline of the related literature is as follows. Multicasting with common information in the presence of an eavesdropper has been studied in [17], [18], deriving inner bounds on the secrecy capacity, and in some special cases also deriving the secrecy capacity region. Salehkalaibar *et al.* [17] studied a one-receiver, two-eavesdropper broadcast channel with three degraded message sets. Ekrem and Ulukus [18] studied the transmission of public and confidential messages to two legitimate users, in the presence of an eavesdropper. Benammar and Piantanida [19] calculated the secrecy capacity region of some classes of wiretap broadcast channels.

The MAC wiretap channel has been investigated in [20]–[27]. In [20], a discrete memoryless MAC with confidential messages has been studied that consists of a MAC with generalized feedback [28] where each user's message must be kept confidential from the other. The multiple access wiretap channel [21], [22], [26] consists of a MAC with an additional channel output to an eavesdropper. In [21], [22], achievable rate regions for the secrecy capacity region have been derived. Secrecy in the interference channel and broadcast channel has been studied in [29], where inner and outer bounds for the broadcast channel with confidential messages and the interference channel with confidential messages have been compared.

Beside improving and modifying the achievability proof for the weak secrecy regime in [16] and providing details of the proof for Lemma 1, this version studies the two multicast channel with confidential messages under the strong secrecy regime. Also, this version studies the multiple access wiretap channel under randomness constraint.

II. Preliminaries

Throughout this paper, random variables are denoted by capital letters and their realizations by lower case letters. The set of $\epsilon-$strongly jointly typical sequences of length n, according to $p_{X,Y}$, is denoted by $\mathcal{T}_\epsilon^{(n)}(p_{X,Y})$. For convenience in notation, whenever there is no danger of confusion, typicality will reference the random variables rather than the distribution, e.g., $\mathcal{T}_\epsilon^{(n)}(X,Y)$. The set of sequences $\{x^n : (x^n, y^n) \in T_\epsilon^{(n)}(X,Y)\}$ for a fixed y^n, when the fixed sequence y^n is clear from the context, is denoted with the shorthand notation $\mathcal{T}_\epsilon^{(n)}(X|Y)$. Superscripts denote the dimension of a vector, e.g., X^n. The integer set $\{1,\ldots,M\}$ is denoted by $[\![1,M]\!]$, and $X_{[i:j]}$ indicates the set $\{X_i, X_{i+1},\ldots,X_j\}$. The cardinality of a set is denoted by $|\cdot|$. We utilize the total variation between Probability Mass Function (PMF), defined by $||q-p||_1 = \frac{1}{2}\sum_x |p-q|$. Following Cuff [30] and [12, Remark 1], we use the concept of random PMF denoted by capital letters (e.g. P_X).

Definition 1: A $(M_{1,n}, M_{2,n}, n)$ code for the considered model (Fig. 1) consists of the following:

i) *Two message sets $\mathcal{W}_i = [\![1, M_{i,n}]\!]$, $i = 1,2$, from which independent messages W_1 and W_2 are drawn uniformly distributed over their respective sets.*
ii) *Stochastic encoders f_i, $i = 1,2$, which are specified by conditional probability matrices $f_i(X_i^n|w_i)$, where $X_i^n \in \mathcal{X}_i^n$, $w_i \in \mathcal{W}_i$ are channel inputs and private messages, respectively, and $\sum_{x_i^n} f_i(x_i^n|w_i) = 1$. Here, $f_i(x_i^n|w_i)$ is the probability of the encoder producing the codeword x_i^n for the message w_i.*
iii) *A decoding function $\phi_1 : \mathcal{Y}_1^n \to \mathcal{W}_1 \times \mathcal{W}_2$ that assigns $(\hat{w}_1, \hat{w}_2) \in [\![1, M_{1,n}]\!] \times [\![1, M_{2,n}]\!]$ to the received sequence y_1^n.*
iv) *A decoding function $\phi_2 : \mathcal{Y}_2^n \to \mathcal{W}_1 \times \mathcal{W}_2$ that assigns $(\check{w}_1, \check{w}_2) \in [\![1, M_{1,n}]\!] \times [\![1, M_{2,n}]\!]$ to the received sequence y_2^n.*

The probability of error is given by:

$$P_e \triangleq \mathbb{P}\big(\{(\hat{W}_1, \hat{W}_2) \neq (W_1, W_2)\} \cup \{(\check{W}_1, \check{W}_2) \neq (W_1, W_2)\}\big).$$

Definition 2: A rate pair (R_1, R_2) is said to be achievable if there exists a sequence of $(M_{1,n}, M_{2,n}, n)$ codes with $M_{1,n} \geq 2^{nR_1}$, $M_{2,n} \geq 2^{nR_2}$, so that $P_e \underset{n\to\infty}{\longrightarrow} 0$ and [31]

$$\frac{1}{n}\mathbb{I}(W_1, W_2; Z^n) \underset{n\to\infty}{\longrightarrow} 0 \quad \text{for the weak secrecy regime}, \tag{1}$$

$$\mathbb{I}(W_1, W_2; Z^n) \underset{n\to\infty}{\longrightarrow} 0 \quad \text{for the strong secrecy regime}. \tag{2}$$

Definition 3: For any PMFs p_X and q_X over $\mathcal{X}$ we denote $\|p_X - q_X\|_1 < \epsilon$ with $p_X \approx_\epsilon q_X$. Similarly, for any random PMFs P_X and Q_X over $\mathcal{X}$ we denote $\|P_X - Q_X\|_1 < \epsilon$ with $P_X \approx_\epsilon Q_X$. The same notation applies for the sequential PMFs (e.g. $\|p_{X^n} - q_{X^n}\|_1 < \epsilon$ is denoted by $p_{X^n} \approx_\epsilon q_{X^n}$).

III. Achievable Rate Region Under the Weak Secrecy

We start with a lemma that employs Marton coding with indirect decoding in a MAC structure and produces an entropy bound needed in the secrecy analysis. Its basic idea can be highlighted as follows: given X^n, if we *independently* produce 2^{nR} random codevectors Y^n, we will have approximately $2^{nR-\mathbb{I}(X^n;Y^n)}$ *jointly* typical pairs, i.e., the "excess" rate will determine the number of jointly typical pairs. This lemma extends the basic idea of excess rate to multiple codebooks, multiple conditioning, and furthermore, a generalization is made from a counting argument to the entropy of the index of the codebook, which is essential for the subsequent secrecy analysis.

Lemma 1: Consider random variables $(Q, U_0, V_0, U_1, V_1, Z)$ distributed according to $p_Q p_{U_0,U_1|Q} p_{V_0,V_1|Q} p_{Z|U_0,U_1,V_0,V_1}$. Draw random sequences Q^n, U_0^n, V_0^n according to $\prod_{i=1}^n p_Q(q_i)\ p_{U_0|Q}(u_{0,i}|q_i)\ p_{V_0|Q}(v_{0,i}|q_i)$. Conditioned on U_0^n, draw 2^{nS} i.i.d. copies of U_1^n according to $\prod_{i=1}^n p_{U_1|U_0}(u_{1,i}|u_{0,i})$, denoted $U_1^n(\ell)$, $\ell \in [\![1, 2^{nS}]\!]$. Similarly, conditioned on V_0^n, draw 2^{nT} i.i.d. copies of V_1^n according to $\prod_{i=1}^n p_{V_1|V_0}(v_{1,i}|v_{0,i})$, denoted

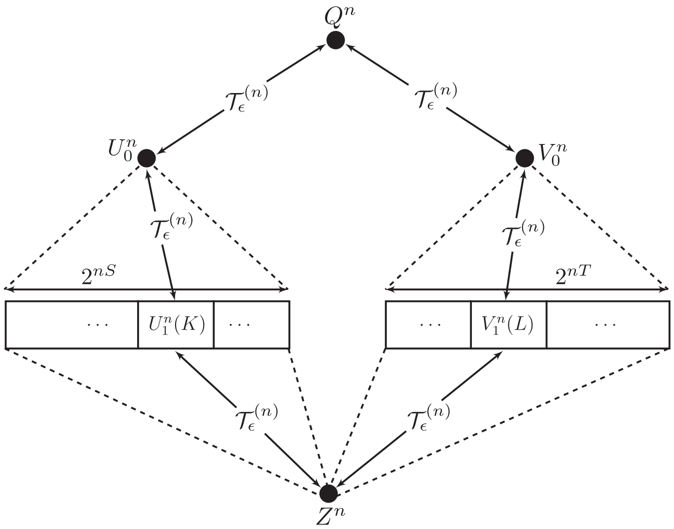

Fig. 2. Structure of Lemma 1: subject to jointly typical sequences $(Q^n, U_0^n, V_0^n, U_1^n(K), V_1^n(L), Z^n)$, finding a bound on the conditional entropy of (K, L), thus implicitly bounding the number of sequence pairs that can be jointly typical with (Q^n, Z^n) from codebooks with certain size.

$V_1^n(k)$, $k \in [\![1, 2^{nT}]\!]$. *Let* $L \in [\![1, 2^{nS}]\!]$ *and* $K \in [\![1, 2^{nT}]\!]$ *be random variables with arbitrary PMF. If*

$$\begin{aligned} S &> \mathbb{I}(U_1; Z|Q, U_0, V_0) + \delta_1(\epsilon) \\ T &> \mathbb{I}(V_1; Z|Q, U_0, V_0) + \delta_1(\epsilon) \\ S + T &> \mathbb{I}(U_1, V_1; Z|Q, U_0, V_0) + \delta_1(\epsilon) \end{aligned}$$

for a positive $\delta_1(\epsilon)$ *and if for an arbitrary sequence* Z^n,

$$\mathbb{P}\big((Q^n, U_0^n, V_0^n, U_1^n(L), V_1^n(K), Z^n) \in \mathcal{T}_\epsilon^{(n)}\big) \xrightarrow[n\to\infty]{} 1, \quad (3)$$

there exists a positive $\delta_2(\epsilon) \xrightarrow[\epsilon\to 0]{} 0$, *such that for n sufficiently large,*

$$\begin{aligned} &\mathbb{H}(L, K|Q^n, U_0^n, V_0^n, Z^n, \mathcal{C}) \\ &\quad \le n(S + T - \mathbb{I}(U_1, V_1; Z|Q, U_0, V_0)) + n\delta_2(\epsilon), \quad (4) \end{aligned}$$

where $\mathcal{C} = \{U_1^n(1), \ldots, U_1^n(2^{nS}), V_1^n(1), \ldots, V_1^n(2^{nT})\}$.

The proof is provided in Appendix A. This result is related to, and contains, [10, Lemma 1]. In particular, [10] considers a single-input channel and explores the properties of codebooks driven by this input, while observing an output Z. In contrast, this paper's Lemma 1 develops a corresponding result for a *multiple-access channel* with respect to Z, motivated by the two-transmitters present in the model of this paper. This accounts for the new features of our Lemma 1, namely three rate constraints instead of one, as well as monitoring the entropy of two index random variables instead of one. Furthermore, the present result has one additional layer of conditioning to allow for indirect decoding of multiple confidential messages in the sequel, while in [10] only one confidential message is decoded.

Remark 1: In addition to establishing the main results of this paper, Lemma 1 also has broader implications on the necessity of prefixing in multi-transmitter secrecy problems [32] and deriving the minimum amount of randomness needed to achieve secrecy. Csiszár and Körner introduced prefixing in [33] to expand the achievable rate region of the non-degraded broadcast channel with confidential messages, a technique that was subsequently used in essentially the same manner in multi-transmitter settings. Subsequently, Chia and El Gamal showed that in a single-transmitter wiretap channel, prefixing can be replaced with superposition coding [10]. Appendix B extends this concept to a multi-transmitter setting and presents an achievability technique for the multiple access wiretap channel that utilizes minimal randomness and matches the best known achievable rates without prefixing.

Theorem 1: An inner bound on the secrecy capacity region of the two-transmitter two-receiver channel with confidential messages is given by the set of non-negative rate pairs (R_1, R_2) *such that*

$$\begin{aligned}
R_1 &< \mathbb{I}(U_0, U_1; Y_1|Q, V_0, V_1) - \mathbb{I}(U_0; Z|Q) \\ &\quad -\mathbb{I}(U_1; Z|U_0, V_0) \\
R_1 &< \mathbb{I}(U_0, U_2; Y_2|Q, V_0, V_2) - \mathbb{I}(U_0; Z|Q) \\ &\quad -\mathbb{I}(U_2; Z|U_0, V_0) \\
R_1 &< \mathbb{I}(U_0, U_1, V_1; Y_1|Q, V_0) - \mathbb{I}(U_0; Z|Q) \\ &\quad -\mathbb{I}(U_1, V_1; Z|U_0, V_0) \\
R_1 &< \mathbb{I}(U_0, U_2, V_2; Y_2|Q, V_0) - \mathbb{I}(U_0; Z|Q) \\ &\quad -\mathbb{I}(U_2, V_2; Z|U_0, V_0) \\
R_2 &< \mathbb{I}(V_0, V_1; Y_1|Q, U_0, U_1) - \mathbb{I}(V_0; Z|Q) \\ &\quad -\mathbb{I}(V_1; Z|U_0, V_0) \\
R_2 &< \mathbb{I}(V_0, V_2; Y_2|Q, U_0, U_2) - \mathbb{I}(V_0; Z|Q) \\ &\quad -\mathbb{I}(V_2; Z|U_0, V_0) \\
R_2 &< \mathbb{I}(U_1, V_0, V_1; Y_1|Q, U_0) - \mathbb{I}(V_0; Z|Q) \\ &\quad -\mathbb{I}(U_1, V_1; Z|U_0, V_0) \\
R_2 &< \mathbb{I}(U_2, V_0, V_2; Y_2|Q, U_0) - \mathbb{I}(V_0; Z|Q) \\ &\quad -\mathbb{I}(U_2, V_2; Z|U_0, V_0) \\
R_1+R_2 &< \mathbb{I}(U_0, U_1, V_0, V_1; Y_1|Q) - \mathbb{I}(U_0, U_1, V_0, V_1; Z|Q) \\
R_1+R_2 &< \mathbb{I}(U_0, U_2, V_0, V_2; Y_2|Q) - \mathbb{I}(U_0, U_2, V_0, V_2; Z|Q) \\
R_1+R_2 &< \mathbb{I}(U_0, U_1; Y_1|Q, V_0, V_1)+\mathbb{I}(U_1, V_0, V_1; Y_1|Q, U_0) \\ &\quad -\mathbb{I}(U_0, U_1, V_0, V_1; Z|Q) - \mathbb{I}(U_1; Z|U_0, V_0) \\
R_1+R_2 &< \mathbb{I}(U_0, U_1; Y_1|Q, V_0, V_1)+\mathbb{I}(V_0, V_2; Y_2|Q, U_0, U_2) \\ &\quad -\mathbb{I}(U_0, V_0; Z|Q) - \mathbb{I}(U_1; Z|U_0, V_0) \\ &\quad -\mathbb{I}(V_2; Z|U_0, V_0) \\
R_1+R_2 &< \mathbb{I}(U_0, U_1; Y_1|Q, V_0, V_1)+\mathbb{I}(U_2, V_0, V_2; Y_2|Q, U_0) \\ &\quad -\mathbb{I}(U_1; Z|U_0, V_0) - \mathbb{I}(U_0, U_2, V_0, V_2; Z|Q) \\
R_1+R_2 &< \mathbb{I}(V_0, V_1; Y_1|Q, U_0, U_1)+\mathbb{I}(U_0, U_1, V_1; Y_1|Q, V_0) \\ &\quad -\mathbb{I}(U_0, U_1, V_0, V_1; Z|Q) - \mathbb{I}(V_1; Z|U_0, V_0) \\
R_1+R_2 &< \mathbb{I}(V_0, V_1; Y_1|Q, U_0, U_1)+\mathbb{I}(U_0, U_2; Y_2|Q, V_0, V_2) \\ &\quad -\mathbb{I}(U_0, V_0; Z|Q) - \mathbb{I}(V_1; Z|U_0, V_0) \\ &\quad -\mathbb{I}(U_2; Z|U_0, V_0) \\
R_1+R_2 &< \mathbb{I}(V_0, V_1; Y_1|Q, U_0, U_1)+\mathbb{I}(U_0, U_2, V_2; Y_2|Q, V_0) \\ &\quad -\mathbb{I}(V_1; Z|U_0, V_0) - \mathbb{I}(U_0, U_2, V_0, V_2; Z|Q) \\
R_1+R_2 &< \mathbb{I}(U_0, U_2; Y_2|Q, V_0, V_2)+\mathbb{I}(U_1, V_0, V_1; Y_1|Q, U_0) \\ &\quad -\mathbb{I}(U_0, U_1, V_0, V_1; Z|Q) - \mathbb{I}(U_2; Z|U_0, V_0) \\
R_1+R_2 &< \mathbb{I}(U_0, U_2; Y_2|Q, V_0, V_2)+\mathbb{I}(U_2, V_0, V_2; Y_2|Q, U_0) \\ &\quad -\mathbb{I}(U_0, U_2, V_0, V_2; Z|Q) - \mathbb{I}(U_2; Z|U_0, V_0)
\end{aligned}$$

$$
\begin{aligned}
R_1+R_2 &< \mathbb{I}(V_0, V_2; Y_2|Q, U_0, U_2)+\mathbb{I}(U_0, U_2, V_2; Y_2|Q, V_0)\\
&\quad -\mathbb{I}(U_0, U_2, V_0, V_2; Z|Q) - \mathbb{I}(V_2; Z|U_0, V_0)\\
R_1+R_2 &< \mathbb{I}(V_0, V_2; Y_2|Q, U_0, U_2)+\mathbb{I}(U_0, U_1, V_1; Y_1|Q, V_0)\\
&\quad -\mathbb{I}(U_0, U_1, V_0, V_1; Z|Q) - \mathbb{I}(V_2; Z|U_0, V_0)\\
R_1+R_2 &< \mathbb{I}(U_0, U_1, V_1; Y_1|Q, V_0)+\mathbb{I}(U_1, V_0, V_1; Y_1|Q, U_0)\\
&\quad -\mathbb{I}(U_0, V_0; Z|Q) - 2\mathbb{I}(U_1, V_1; Z|U_0, V_0)\\
R_1+R_2 &< \mathbb{I}(U_0, U_1, V_1; Y_1|Q, V_0)+\mathbb{I}(U_2, V_0, V_2; Y_2|Q, U_0)\\
&\quad -\mathbb{I}(U_0, V_0; Z|Q) - \mathbb{I}(U_1, V_1; Z|U_0, V_0)\\
&\quad -\mathbb{I}(U_2, V_2; Z|U_0, V_0)\\
R_1+R_2 &< \mathbb{I}(U_1, V_0, V_1; Y_1|Q, U_0)+\mathbb{I}(U_0, U_2, V_2; Y_2|Q, V_0)\\
&\quad -\mathbb{I}(U_0, U_1, V_0, V_1; Z|Q) - \mathbb{I}(U_2, V_2; Z|U_0, V_0)\\
R_1+R_2 &< \mathbb{I}(U_0, U_2, V_2; Y_2|Q, V_0)+\mathbb{I}(U_2, V_0, V_2; Y_2|Q, U_0)\\
&\quad -\mathbb{I}(U_0, V_0; Z|Q) - 2\mathbb{I}(U_2, V_2; Z|U_0, V_0)
\end{aligned}
$$

for some

$$
\begin{aligned}
&p(q)p(u_0|q)p(u_1, u_2|u_0)p(v_0|q)p(v_1, v_2|v_0)\\
&\quad p(x_1|u_0, u_1, u_2)p(x_2|v_0, v_1, v_2)p(y_1, y_2, z|x_1, x_2), \quad (5)
\end{aligned}
$$

such that

$$
\begin{aligned}
&\mathbb{I}(U_1, U_2, V_1, V_2; Z|U_0, V_0) \le \mathbb{I}(U_1, V_1; Z|U_0, V_0)\\
&\quad +\mathbb{I}(U_2, V_2; Z|U_0, V_0) - \mathbb{I}(U_1; U_2|U_0) - \mathbb{I}(V_1; V_2|V_0). \quad (6)
\end{aligned}
$$

The proof uses superposition coding, Wyner's wiretap coding, Marton coding, as well as indirect decoding. The details of the proof are provided in Appendix C. Our coding strategy extends the approach developed in [11] for the broadcast channel with confidential messages to the scenario at hand with two transmitters. For the first transmitter, the message w_1 is encoded into a sequence u_0^n. To deal with multicasting, we superimpose a Marton codebook to u_0^n consisting of sequences u_1^n and u_2^n; formally, given u_0^n, a jointly typical pair (u_1^n, u_2^n) is selected at random from the Marton codebook. For the second transmitter, the codebook structure is identical and the codewords generated are represented by v_0^n, v_1^n, and v_2^n, respectively. The receiver $j \in \{1, 2\}$ decodes w_1 through (u_0^n, u_j^n), and decodes w_2 through (v_0^n, v_j^n). As discovered in [11], note that correctly decoding (w_1, w_2) at the receiver j does not require correctly decoding (u_j^n, v_j^n). Here, a two-step secrecy analysis is necessary because the $(u_{[1:2]}^n, v_{[1:2]}^n)$ sequences should not leak any information about (u_0^n, v_0^n). Therefore, the secrecy constraints for u_0^n and v_0^n sequences should be derived first, and then secrecy constraints for $(u_{[1:2]}^n, v_{[1:2]}^n)$ sequences should be derived, assuming that the eavesdropper has access to (u_0^n, v_0^n, z^n). This two-step secrecy can be seen in Theorem 1; for example in the first constraint on R_1 the first negative term stands for the security of u_0^n and the second negative term stands for the security of u_1^n assuming that eavesdropper has access to (u_0^n, v_0^n, z^n).

This result covers several known earlier results:

- By setting $Z = \emptyset$, $U_0 = U_1 = U_2 = X_1$, and $V_0 = V_1 = V_2 = X_2$, the result in Theorem 1 reduces to the capacity region of compound multiple access channel discussed in [7].
- By setting $Y_2 = \emptyset$ (or $Y_1 = \emptyset$), $U_0 = U_1 = U_2 = X_1$ and $V_0 = V_1 = V_2 = X_2$, the result in Theorem 1 reduces to the achievable rate region of multiple access wiretap channel without common message [21]–[23].
- By setting $X_2 = \emptyset$ (or $X_1 = \emptyset$), $U_0 = U_1 = U_2$, and $Y_2 = \emptyset$ (or $Y_1 = \emptyset$), the result in Theorem 1 reduces to the capacity region of broadcast channel with confidential message [33, Corollary 2].
- By setting $X_2 = \emptyset$ (or $X_1 = \emptyset$), the result in Theorem 1 reduces to the achievable rate region for two-receiver, one-eavesdropper wiretap channel presented in [10, Theorem 1].

Remark 2: By doing some algebraic manipulation we can show that the constraint in (6) *holds only if*

$$\mathbb{I}(U_1, V_1; U_2, V_2|U_0, V_0, Z) = 0. \quad (7)$$

Intuitively speaking, (7) *shows that the Marton coding codebooks remain independent even if the eavesdropper has access to the the cloud centers.*

Corollary 1: An inner bound on the secrecy capacity region of degraded two-transmitter two-receiver channel with confidential messages (Definition 4) is given by the set of non-negative rate pairs (R_1, R_2) *such that*

$$
\begin{aligned}
R_1 &\le \mathbb{I}(U_0; Y_2|V_0, Q) - \mathbb{I}(U_0; Z|Q) &(8)\\
R_2 &\le \mathbb{I}(V_0; Y_2|U_0, Q) - \mathbb{I}(V_0; Z|Q) &(9)\\
R_1 + R_2 &\le \mathbb{I}(U_0, V_0; Y_2|Q) - \mathbb{I}(U_0, V_0; Z|Q) &(10)
\end{aligned}
$$

for some

$$p(q)p(u_0|q)p(v_0|q)p(x_1|u_0)p(x_2|v_0). \quad (11)$$

Proof: The proof follows from Theorem 1 by setting $U_0 = U_1 = U_2$ and $V_0 = V_1 = V_2$ and considering the fact that the channel is degraded. □

IV. An Outer Bound for the Degraded Model

We develop an outer bound for the degraded version of the model and provide an example in which it meets the inner bound of Theorem 1.

Definition 4: The degraded two-transmitter two-receiver channel with confidential messages obeys:

$$p(y_1, y_2, z|x_1, x_2) = p(y_1|x_1, x_2)p(y_2|y_1)p(z|y_2). \quad (12)$$

Theorem 2: The secrecy capacity region for the degraded two-transmitter two-receiver channel with confidential messages is included in the set of rate pairs (R_1, R_2) *satisfying*

$$
\begin{aligned}
R_1 &\le \mathbb{I}(U_0; Y_2|Q) - \mathbb{I}(U_0; Z|Q), &(13)\\
R_2 &\le \mathbb{I}(V_0; Y_2|Q) - \mathbb{I}(V_0; Z|Q), &(14)\\
R_1 + R_2 &\le \mathbb{I}(U_0, V_0; Y_2|Q) - \mathbb{I}(U_0, V_0; Z|Q), &(15)
\end{aligned}
$$

for some joint distribution

$$p(q)p(u_0, v_0|q)p(x_1|u_0)p(x_2|v_0). \quad (16)$$

The details of the proof are provided in Appendix D.

Example (Degraded Switch Model): We consider an example of the two-transmitter two-receiver channel where the first legitimate receiver has access to the noisy version of each of

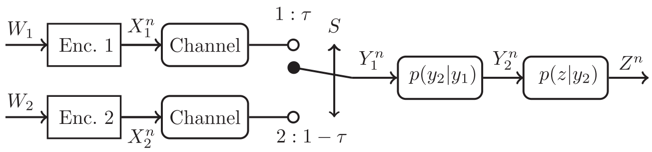

Fig. 3. Degraded switch model.

the two transmitted values in a time-sharing (switched) manner, without interference from the other transmitter (Fig. 3). The second legitimate receiver has access to a noisy version of the first receiver, and the eavesdropper has access to a noisy version of the second receiver. This example illustrates a common situation in cellular networks, in which a user is in the coverage range of two different base stations. The user can only receive signal from a single station in each time slot while an eavesdropper has access to noisy versions of the receiver signals. The switch channel state information is made available to all terminals. In this model the channel outputs are as follows:

$$y_1' = (y_1, s), \tag{17}$$
$$y_2' = (y_2, s), \tag{18}$$
$$z' = (z, s). \tag{19}$$

This model consists of a channel with states that are causally available at both the encoders and decoders.

The statistics of the channel, conditioned on the switch state, are expressed as follows:

$$p(y_1', y_2', z|x_1, , x_2, s) = p(y_1|x_1, x_2, s)\, p(y_2|y_1, s)\, p(z|y_2, s). \tag{20}$$

The switch model describes, e.g., frequency hopping over two frequencies [29]. The state (switch) is a binary random variable that chooses between listening to the Transmitter 1, with probability τ, and listening to the Transmitter 2, with probability $1-\tau$, independently at each time slot. We further assume the state is i.i.d. across time,

$$\begin{aligned} p(y_1|x_1, x_2, s) &= p(y_1|x_1)\mathbb{1}_{\{s=1\}} + p(y_1|x_2)\mathbb{1}_{\{s=2\}}, \\ &= p(y_1|x_s), \end{aligned} \tag{21}$$

where $\mathbb{1}_{\{.\}}$ is the indicator function. Therefore, the channel model for degraded switch model is as follows

$$p(y_1, y_2, z|x, x, s) = p(y_1|x_s)p(y_2|y_1, s)p(z|y_2, s). \tag{22}$$

Theorem 3: The secrecy capacity region for the degraded switch two-transmitter two-receiver channel with confidential messages, is given by the set of rate pairs (R_1, R_2) *satisfying*

$$R_1 \le \mathbb{I}(U_0; Y_2'|V_0, Q) - \mathbb{I}(U_0; Z'|Q), \tag{23}$$
$$R_2 \le \mathbb{I}(V_0; Y_2'|U_0, Q) - \mathbb{I}(V_0; Z'|Q), \tag{24}$$
$$R_1 + R_2 \le \mathbb{I}(U_0, V_0; Y_2'|Q) - \mathbb{I}(U_0, V_0; Z'|Q), \tag{25}$$

for some joint distribution

$$p(q)p(u_0|q)p(v_0|q)p(x_1|u_0)p(x_2|v_0). \tag{26}$$

To prove Theorem 3, we show that given Q, U_0 and V_0 are independent for this example. The details of the proof are provided in Appendix E.

V. A General Outer Bound

We now develop a general outer bound for the model of Fig. 1 and provide an example in which it meets the inner bound of Theorem 1.

Theorem 4: The secrecy capacity region for the two-transmitter two-receiver channel with confidential messages is included in the set of rate pairs (R_1, R_2) *satisfying*

$$R_1 \le \mathbb{I}(U_0; Y_1, Y_2|Q) - \mathbb{I}(U_0; Z|Q), \tag{27}$$
$$R_2 \le \mathbb{I}(V_0; Y_1, Y_2|Q) - \mathbb{I}(V_0; Z|Q), \tag{28}$$
$$R_1 + R_2 \le \mathbb{I}(U_0, V_0; Y_1, Y_2|Q) - \mathbb{I}(U_0, V_0; Z|Q), \tag{29}$$

for some joint distribution

$$p(q)p(u_0, v_0|q)p(x_1|u_0)p(x_2|v_0). \tag{30}$$

The details of the proof are provided in Appendix F.

Example (Noiseless Switch Model): This example is motivated by two transmitters operating on different spectral bands, while the receiving terminals may receive adaptively on one band at a time [29]. The eavesdropper in our example has access to one noiseless interference-free transmitted value at a time. Here, it is assumed that both legitimate receivers operate according to a common random switch s_1 that is connected to Transmitter 1 with probability τ_1 and to Transmitter 2 with probability $1-\tau_1$, and the eavesdropper operates according to another random switch s_2 that is connected to Transmitter 1 with probability τ_2 and to Transmitter 2 with probability $1-\tau_2$. Aside from the switches, the channel is noiseless. Both receivers and the eavesdropper have access to their own switch state information. Therefore the channel outputs are considered

$$y_1' = (y_1, s_1), \tag{31}$$
$$y_2' = (y_2, s_1), \tag{32}$$
$$z' = (z, s_2). \tag{33}$$

Since $y_1 = y_2$, we also have $y_1' = y_2'$.

Theorem 5: The secrecy capacity region for the noiseless switch two-transmitter two-receiver channel with confidential messages is given by the set of rate pairs (R_1, R_2) *satisfying*

$$R_1 \le (\tau_1 - \tau_2)^+\mathbb{H}(X_1), \tag{34}$$
$$R_2 \le (\tau_2 - \tau_1)^+\mathbb{H}(X_2), \tag{35}$$

where $(x)^+ = \max\{0, x\}$.

The details of the proof are provided in Appendix G. The capacity region in Theorem 5 shows that transmitters can securely communicate to receivers as long as $\tau_1 \ne \tau_2$.

VI. Achievable Rate Region Under the Strong Secrecy

Theorem 6: An inner bound on the secrecy capacity region of the two-transmitter two-receiver channel with confidential messages consists of the union of rate pairs (R_1, R_2) *regions satisfying* (156)–(167), (173)–(175), (177), *and* (178), *for some distribution*

$$p(q)p(u_0, u_1, u_2|q)p(v_0, v_1, v_2|q) \times p(x_1|u_0, u_1, u_2)p(x_2|v_0, v_1, v_2)p(y_1, y_2, z|x_1, x_2). \tag{36}$$

The proof is given in Appendix H.

Remark 3: It is customary to eliminate rate variables not associated with external messages via Fourier-Motzkin elimination [34]. In the interest of brevity, in this paper we omit the 73 inequalities resulting from Fourier-Motzkin elimination and instead make them available via [35]. In the sequel, a subset of this achievable rate region will be presented that enjoys a much simpler expression.

Remark 4: Even though the analysis of Theorem 1 is based on typical counting and OSRB is based on distribution approximation here we show that the region in Theorem 6 is a superset of the region in Theorem 1. If we assume that (6)*, and therefore* (7)*, holds, the inequalities* (161) *for* $j = 2$, (162) *for* $j = 1$*, and* (163)–(167) *will be redundant and by applying the Fourier-Motzkin procedure [36], [37] to* (156)–(160)*,* (161) *for* $j = 1$*,* (162) *for* $j = 2$*,* (173)*,* (174)*, and* (178) *the region in Theorem 1 over the distribution* (36) *will be achieved. This shows that the region derived by OSRB is a superset of the region derived in the weak secrecy regime.*

VII. Conclusion

This paper studies the multi-transmitter multicast problem in presence of an eavesdropper, wherein weak and strong secrecy regimes are studied. For the weak secrecy regime, the method of Chia and El Gamal is extended to two transmitters. We show that the achievable region calculated for the weak secrecy regime in this channel configuration is no bigger than the one calculated under strong secrecy. Two examples are presented in which the inner and outer bounds on secrecy region meet. In the process, we also characterize the minimum amount of randomness necessary to achieve secrecy in the multiple-access wiretap channel.

Appendix A
Proof of Lemma 1

Let $N(Q^n, U_0^n, V_0^n, Z^n) = |\{(k,\ell) \in [\![1, 2^{nS}]\!] \times [\![1, 2^{nT}]\!] : (Q^n, U_0^n, V_0^n, U_1^n(k), V_1^n(\ell), Z^n) \in \mathcal{T}_\epsilon^{(n)}\}|$. Next, let's define the following error events.

Let $E_1(Q^n, U_0^n, V_0^n, Z^n) = 1$ if $N(Q^n, U_0^n, V_0^n, Z^n) \geq (1+\delta_1(\epsilon))2^{n(S+T-\mathbb{I}(U_1,V_1;Z|Q,U_0,V_0)+\delta(\epsilon))}$ and $E_1 = 0$ otherwise.

Let $E = 0$ if $(Q^n, U_0^n, V_0^n, U_1^n(K), V_1^n(L), Z^n) \in \mathcal{T}_\epsilon^{(n)}$ and $E_1(Q^n, U_0^n, V_0^n, Z^n, K, L) = 0$, and $E = 1$ otherwise.

We now show that if $S \geq \mathbb{I}(U_1; Z|Q, U_0, V_0) + \delta(\epsilon)$, $T \geq \mathbb{I}(V_1; Z|Q, U_0, V_0) + \delta(\epsilon)$, and $S + T \geq \mathbb{I}(U_1, V_1; Z|Q, U_0, V_0) + \delta(\epsilon)$, then $\mathbb{P}(E = 1) \to 0$ as $n \to \infty$.

By the union bound we have

$$\begin{aligned}\mathbb{P}(E=1) \leq \mathbb{P}\big((Q^n, U_0^n, V_0^n, U_1^n(K), V_1^n(L), Z^n) \notin \mathcal{T}_\epsilon^{(n)}\big)\\ +\mathbb{P}\big(E_1(Q^n, U_0^n, V_0^n, Z^n, K, L) = 1\big). \quad (37)\end{aligned}$$

The first term tends to zero by the main assumption of the Lemma.

We then partition the event $\{E_1 = 1\}$ based on the composition of the typical sequences $(Q^n, U_0^n, V_0^n, U_1^n(k), V_1^n(\ell), Z^n) \in \mathcal{T}_\epsilon^{(n)}$:

- When all such typical sequences share the same $U_1^n(k)$, i.e., correspond to a single k.
- When all such typical sequences share the same $V_1^n(\ell)$, i.e., correspond to a single ℓ.
- Neither of the above

As usual, each of the three partitioned E_1 events gives rise to one rate constraint. We discuss the first in detail; the remaining two follow similarly. Define $A(Q^n, U_0^n, V_0^n, z^n)$ as the event $\{E_1(Q^n, U_0^n, V_0^n, Z^n) = 1\} \cap \{Z^n = z^n\}$,

$$\begin{aligned}&\mathbb{P}\big(E_1(Q^n, U_0^n, V_0^n, Z^n) = 1\big)\\ &\quad= \sum_{(q^n,u_0^n,v_0^n)\in\mathcal{T}_\epsilon^{(n)}} \Big[p(q^n)p(u_0^n|q^n)p(v_0^n|q^n)\\ &\qquad\times\mathbb{P}\Big((E_1(Q^n, U_0^n, V_0^n, Z^n) = 1)\\ &\qquad|Q^n = q^n, U_0^n = u_0^n, V_0^n = v_0^n\Big)\Big]\\ &\quad= \sum_{\substack{(q^n,u_0^n,v_0^n)\in\mathcal{T}_\epsilon^{(n)}(Q,U_0,V_0)\\ z^n\in\mathcal{T}_\epsilon^{(n)}(Z|Q,U_0,V_0)}} p(q^n)p(u_0^n|q^n)p(v_0^n|q^n)\\ &\qquad\times\mathbb{P}\big(A(q^n, u_0^n, v_0^n, z^n)|Q^n = q^n, U_0^n = u_0^n, V_0^n = v_0^n\big)\\ &\quad\leq \sum_{(q^n,u_0^n,v_0^n)\in\mathcal{T}_\epsilon^{(n)}(Q,U_0,V_0)} p(q^n)p(u_0^n|q^n)p(v_0^n|q^n)\\ &\qquad\sum_{z^n\in\mathcal{T}_\epsilon^{(n)}(Z|Q,U_0,V_0)} \mathbb{P}\big((E_1(q^n, u_0^n, v_0^n, z^n) = 1)\\ &\qquad|Q^n = q^n, U_0^n = u_0^n, V_0^n = v_0^n\big). \quad (38)\end{aligned}$$

Then,

$$\begin{aligned}&\mathbb{P}\big(E_1(q^n, u_0^n, v_0^n, z^n) = 1|Q^n = q^n, U_0^n = u_0^n, V_0^n = v_0^n\big)\\ &\quad= \mathbb{P}\big(N(q^n, u_0^n, v_0^n, z^n) \geq (1+\delta_1(\epsilon))2^{n(T-\mathbb{I}(V_1;Z|Q,U_0,V_0)+\delta(\epsilon))}\big).\end{aligned}$$

Define $X_\ell = 1$ if $(q^n, u_0^n, v_0^n, V_1^n(\ell), z^n) \in \mathcal{T}_\epsilon^{(n)}$ and 0 otherwise. Here, X_ℓ, $\ell \in [\![1, 2^{nT}]\!]$, are i.i.d. Bernoulli-$\alpha$ random variables, where

$$2^{-n(\mathbb{I}(V_1;Z|Q,U_0,V_0)+\delta(\epsilon))} \leq \alpha \leq 2^{-n(\mathbb{I}(V_1;Z|Q,U_0,V_0)-\delta(\epsilon))}.$$

Then

$$\begin{aligned}&\mathbb{P}\bigg(N(q^n, u_0^n, v_0^n, z^n) \geq (1+\delta_1(\epsilon))2^{n(T-\mathbb{I}(V_1;Z|Q,U_0,V_0)+\delta(\epsilon))}\\ &\qquad\bigg|Q^n = q^n, U_0^n = u_0^n, V_0^n = v_0^n\bigg)\\ &\quad\leq \mathbb{P}\bigg(\sum_{\ell=1}^{2^{nT}} X_\ell \geq (1+\delta_1(\epsilon))2^{nT}\alpha\bigg|Q^n = q^n, U_0^n = u_0^n, V_0^n = v_0^n\bigg).\end{aligned}$$

Applying the Chernoff Bound (e.g., see [34, Appendix B]), leads to

$$\begin{aligned}&\mathbb{P}\bigg(\sum_{\ell=1}^{2^{nT}} X_\ell \geq (1+\delta_1(\epsilon))2^{nT}\alpha\bigg|Q^n = q^n, U_0^n = u_0^n, V_0^n = v_0^n\bigg)\\ &\quad\leq \exp(-2^{nT}\alpha\delta_1^2(\epsilon)/4)\\ &\quad\leq \exp(-2^{n(T-\mathbb{I}(V_1;Z|Q,U_0,V_0)-\delta(\epsilon))}\delta_1^2(\epsilon)/4). \quad (39)\end{aligned}$$

Therefore,

$$\begin{aligned}
&\mathbb{P}(E_1(Q^n, U_0^n, V_0^n, Z^n) = 1)\\
&\le \sum_{(q^n,u_0^n,v_0^n)\in\mathcal{T}_\epsilon^{(n)}} p(q^n)p(u_0^n|q^n)p(v_0^n|q^n)\\
&\quad\times \sum_{z^n\in\mathcal{T}_\epsilon^{(n)}(Z|Q,U_0,V_0)} \exp(-2^{n(T-\mathbb{I}(V_1;Z|Q,U_0,V_0)-\delta(\epsilon))}\delta_1^2(\epsilon)/4)\\
&\le 2^{n\log|\mathcal{Z}|}\exp(-2^{n(T-\mathbb{I}(V_1;Z|Q,U_0,V_0)-\delta(\epsilon))}\delta_1^2(\epsilon)/4), \qquad (40)
\end{aligned}$$

which tends to zero as $n\to\infty$ if $T \ge \mathbb{I}(V_1; Z|Q, U_0, V_0) + \delta(\epsilon)$.

In a similar manner, the bounding of error probability for the second and third partition of E_1 (please see above) will give rise to the rate constraints $S \ge \mathbb{I}(U_1; Z|Q, U_0, V_0) + \delta(\epsilon)$, and $S+T \ge \mathbb{I}(U_1, V_1; Z|Q, U_0, V_0)+\delta(\epsilon)$, respectively. Details are ommited for brevity.

Finally, we bound $\mathbb{H}(L, K|Q^n, U_0^n, V_0^n, Z^n, \mathcal{C})$ as follows:

$$\begin{aligned}
&\mathbb{H}(L, K, E|Q^n, U_0^n, V_0^n, Z^n, C)\\
&\quad\le 1 + \mathbb{P}(E = 1)\mathbb{H}(L, K|E = 1, Q^n, U_0^n, V_0^n, Z^n, C)\\
&\qquad + \mathbb{P}(E = 0)\mathbb{H}(L, K|E = 0, Q^n, U_0^n, V_0^n, Z^n, C)\\
&\quad\le 1 + \mathbb{P}(E = 1)n(S + T)\\
&\qquad + \log\left((1 + \delta_1(\epsilon))2^{n(S+T-\mathbb{I}(U_1,V_1;Z|Q,U_0,V_0)+\delta(\epsilon))}\right)\\
&\quad\le n(S + T - \mathbb{I}(U_1, V_1; Z|Q, U_0, V_0) + \delta_2(\epsilon)). \qquad (41)
\end{aligned}$$

APPENDIX B
ACHIEVABLE RATE REGION FOR MAC-WTC UNDER RANDOMNESS CONSTRAINT

It is well-known that a stochastic encoding is required to avoid leaking information about the transmitted confidential messages to an eavesdropper. Here, a new achievability technique for characterizing the trade-off between the rate of the random number to realize the stochastic encoding and the communication rates in the multiple access wiretap channel, by employing a variation of superposition coding, is presented.

Consider a MAC-WTC $(\mathcal{X}_1, \mathcal{X}_2, p(y, z|x_1, x_2), \mathcal{Y}, \mathcal{Z})$, in which $\mathcal{X}_1$, $\mathcal{X}_2$ are finite input alphabets and $\mathcal{Y}$ and $\mathcal{Z}$ are finite output alphabets at the legitimate receiver and the eavesdropper, respectively (as depicted in Fig. 4). In this problem, each transmitter sends a confidential message which is supposed to be decoded by the legitimate receiver and must be kept secret from the eavesdropper. Furthermore, for stochastic encoding, Encoder 1 and Encoder 2 are allowed to use a limited amount of randomness. Thus, we are interested in the trade-off between the rate of randomness, and the rates of confidential messages.

Definition 5: A $(M_{1,n}, M_{2,n}, n)$ code for the considered model (Fig. 4) consists of the following:

i) *Two message sets $\mathcal{W}_i = [\![1, M_{i,n}]\!]$, $i = 1, 2$, from which independent messages W_1 and W_2 are drawn uniformly distributed over their respective sets. Also, two dummy message sets $\mathcal{A}_i = [\![1, M'_{i,n}]\!]$, $i = 1, 2$, from which independent dummy messages A_1 and A_2 are drawn uniformly distributed over their respective sets.*

ii) *Deterministic encoders $f_{i,n}$, $i = 1, 2$, are defined by the function $f_{i,n} : \mathcal{W}_i \times \mathcal{A}_i \to \mathcal{X}_i^n$.*

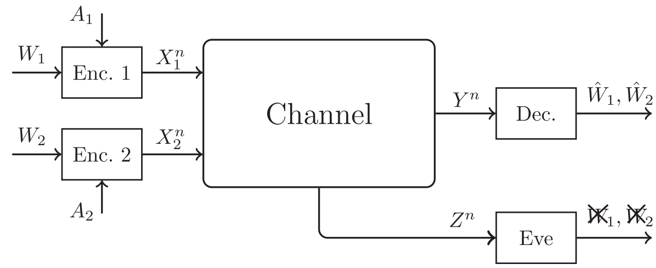

Fig. 4. Multiple access wiretap channel with deterministic encoders.

iii) *A decoding function $\phi : \mathcal{Y}^n \to \mathcal{W}_1 \times \mathcal{W}_2$ that assigns $(\hat{w}_1, \hat{w}_2) \in [\![1, M_{1,n}]\!] \times [\![1, M_{2,n}]\!]$ to the received sequence y^n.*

The probability of error is given by:

$$P_e \triangleq \mathbb{P}\big(\{(\hat{W}_1, \hat{W}_2) \neq (w_1, w_2)\}\big). \qquad (42)$$

Definition 6 [31]: A quadruple $(R_1, R_{d_1}, R_2, R_{d_2})$ is achievable under the weak secrecy if there exists a sequence of $(M_{1,n}, M_{2,n}, M'_{1,n}, M'_{2,n}, n)$ codes with $M_{1,n} \ge 2^{nR_1}, M_{2,n} \ge 2^{nR_2}, M'_{1,n} \le 2^{nR_{d_1}}, M'_{2,n} \le 2^{nR_{d_2}}$, so that $P_e \xrightarrow[n\to\infty]{} 0$ and

$$\frac{1}{n}\mathbb{I}(W_1, W_2; Z^n) \xrightarrow[n\to\infty]{} 0. \qquad (43)$$

Theorem 7: An inner bound on the secrecy capacity region of the multiple access wiretap channel is given by the set of non-negative quadruples $(R_1, R_{d_1}, R_2, R_{d_2})$ such that

$$\begin{aligned}
R_1 &\le \mathbb{I}(U; Y|Q, V) - \mathbb{I}(U; Z|Q), && (44)\\
R_2 &\le \mathbb{I}(V; Y|Q, U) - \mathbb{I}(V; Z|Q), && (45)\\
R_1 + R_2 &\le \mathbb{I}(U, V; Y|Q) - \mathbb{I}(U, V; Z|Q), && (46)\\
R_{d_1} &\ge \mathbb{I}(U; Z|Q) + \mathbb{I}(X_1; Z|Q, U, V), && (47)\\
R_{d_2} &\ge \mathbb{I}(V; Z|Q) + \mathbb{I}(X_2; Z|Q, U, V), && (48)\\
R_{d_1} + R_{d_2} &\ge \mathbb{I}(X_1, X_2; Z|Q), && (49)
\end{aligned}$$

for some

$$p(q)p(u|q)p(v|q)p(x_1|u)p(x_2|v)p(y, z|x_1, x_2). \qquad (50)$$

Remark 5: By setting $U = X_1$, $V = X_2$, and by taking sufficiently large R_{d_1} and R_{d_2}, the result in Theorem 7 reduces to the achievable rate region of multiple access wiretap channel without common message [21]–[23].

Remark 6: By setting $X_2 = \emptyset$ and $V = \emptyset$ (or $X_1 = \emptyset$ and $U = \emptyset$), the result in Theorem 7 reduces to the capacity rate region of broadcast channel with confidential messages under randomness constraint in [15, Corollary 11].

Proof: *Rate Splitting:* Divide the dummy message A_1 into independent dummy messages $A_{1,1} \in [\![1, 2^{nR_{1,1}}]\!]$ and $A_{1,2} \in [\![1, 2^{nR_{1,2}}]\!]$. Also, divide the dummy message A_2 into independent dummy messages $A_{2,1} \in [\![1, 2^{nR_{2,1}}]\!]$ and $A_{2,2} \in [\![1, 2^{nR_{2,2}}]\!]$. Therefore, $R_{d_1} = R_{1,1} + R_{1,2}$ and $R_{d_2} = R_{2,1} + R_{2,2}$.

Codebook Generation: Fix $p(q)$, $p(u|q)$, $p(v|q)$, $p(x_1|u)$, $p(x_2|v)$, and $\epsilon > 0$. Randomly and independently generate a typical sequence q^n according to $p(q^n) = \prod_{i=1}^{n} p(q_i)$. We suppose that all the terminals know q^n.

i) Generate $2^{n(R_1+R_{1,1})}$ sequences according to $\prod_{i=1}^{n} p_{U|Q}(u_i|q_i)$. Then, randomly bin these $2^{n(R_1+R_{1,1})}$ sequences into 2^{nR_1} bins. We index these sequences as $u^n(w_1, a_{1,1})$. For each $(w_1, a_{1,1})$, generate $2^{nR_{1,2}}$ codewords $x_1^n(w_1, a_{1,1}, a_{1,2})$ each according to $\prod_{i=1}^{n} p_{X_1|U}(x_{1,i}|u_i)$.

ii) Generate $2^{n(R_2+R_{2,1})}$ sequences according to $\prod_{i=1}^{n} p_{V|Q}(v_i|q_i)$. Then, randomly bin these $2^{n(R_2+R_{2,1})}$ sequences into 2^{nR_2} bins. We index these sequences as $v^n(w_2, a_{2,1})$. For each $(w_2, a_{2,1})$, generate $2^{nR_{2,2}}$ codewords $x_1^n(w_2, a_{2,1}, a_{2,2})$ each according to $\prod_{i=1}^{n} p_{X_2|V}(x_{2,i}|v_i)$.

Encoding: To send the message w_1, the Encoder 1 splits a_1 into $(a_{1,1}, a_{1,2})$, and chooses $u^n(w_1, a_{1,1})$. Then it chooses codeword $x_1^n(w_1, a_{1,1}, a_{1,2})$ and send it over the channel.

To send the message w_2, the Encoder 2 splits a_2 into $(a_{2,1}, a_{2,2})$, and chooses $v^n(w_2, a_{2,1})$. Then it chooses codeword $x_2^n(w_2, a_{2,1}, a_{2,2})$ and send it over the channel.

Decoding and Error Probability Analysis:

- Decoder decodes (w_1, w_2) by finding a unique pair (w_1, w_2) such that $(q^n, u^n(w_1, a_{1,1}), v^n(w_2, a_{2,1}), y^n) \in \mathcal{T}_\epsilon^{(n)}(p_{U,V,Y})$ for some $(a_{1,1}, a_{2,1})$. The probability of error for Receiver goes to zero as $n \to \infty$ if we choose [34]

$$R_1 + R_{1,1} \leq \mathbb{I}(U; Y|Q, V) - \epsilon, \quad (51)$$
$$R_2 + R_{2,1} \leq \mathbb{I}(V; Y|Q, U) - \epsilon, \quad (52)$$
$$R_1 + R_{1,1} + R_2 + R_{2,1} \leq \mathbb{I}(U, V; Y|Q) - \epsilon. \quad (53)$$

Equivocation Calculation: We analyze mutual information between (W_1, W_2) and Z^n, averaged over all random codebooks

$$\begin{aligned}
&\mathbb{I}(W_1, W_2; Z^n|Q^n, \mathcal{C})\\
&= \mathbb{I}(W_1, W_2, A_{1,1}, A_{1,2}, A_{2,1}, A_{2,2}; Z^n|Q^n, \mathcal{C})\\
&\quad - \mathbb{I}(A_{1,1}, A_{1,2}, A_{2,1}, A_{2,2}; Z^n|W_1, W_2, Q^n, \mathcal{C})\\
&\overset{(a)}{=} \mathbb{I}(W_1, W_2, A_{1,1}, A_{1,2}, A_{2,1}, A_{2,2}, X_1^n, X_2^n; Z^n|Q^n, \mathcal{C})\\
&\quad - \mathbb{I}(A_{1,1}, A_{1,2}, A_{2,1}, A_{2,2}; Z^n|W_1, W_2, Q^n, \mathcal{C})\\
&\overset{(b)}{=} \mathbb{I}(X_1^n, X_2^n; Z^n|Q^n, \mathcal{C})\\
&\quad - \mathbb{I}(A_{1,1}, A_{1,2}, A_{2,1}, A_{2,2}; Z^n|W_1, W_2, Q^n, \mathcal{C})\\
&= \mathbb{I}(X_1^n, X_2^n; Z^n|Q^n, \mathcal{C}) - \mathbb{I}(A_{1,1}, A_{2,1}; Z^n|W_1, W_2, Q^n, \mathcal{C})\\
&\quad - \mathbb{I}(A_{1,2}, A_{2,2}; Z^n|W_1, W_2, A_{1,1}, A_{1,2}, Q^n, \mathcal{C})\\
&= \mathbb{I}(X_1^n, X_2^n; Z^n|Q^n, \mathcal{C}) - \mathbb{H}(A_{1,1}, A_{2,1}|W_1, W_2, Q^n, \mathcal{C})\\
&\quad + \mathbb{H}(A_{1,1}, A_{2,1}|W_1, W_2, Z^n, Q^n, \mathcal{C})\\
&\quad - \mathbb{H}(A_{1,2}, A_{2,2}|W_1, W_2, A_{1,1}, A_{2,1}, Q^n, \mathcal{C})\\
&\quad + \mathbb{H}(A_{1,2}, A_{2,2}|W_1, W_2, A_{1,1}, A_{2,1}, Z^n, Q^n, \mathcal{C}), \quad (54)
\end{aligned}$$

where (a) follows since X_1^n and X_2^n are deterministic functions of $(W_1, A_{1,1}, A_{1,2})$ and $(W_2, A_{2,1}, A_{2,2})$, respectively. Also, (b) follows from the fact that, given X_1^n and X_2^n, the indices W_1, W_2, $A_{1,1}$, $A_{1,2}$,$A_{2,1}$, and $A_{2,2}$ are uniquely determined.

The first term in (54) is bounded as:

$$\mathbb{I}(X_1^n, X_2^n; Z^n|Q^n, \mathcal{C}) \leq n\mathbb{I}(X_1, X_2; Z|Q) + n\epsilon, \quad (55)$$

where $\epsilon \xrightarrow[n\to\infty]{} 0$ similar to [34].

For the second term in (54) we have

$$\mathbb{H}(A_{1,1}, A_{2,1}|W_1, W_2, Q^n, \mathcal{C}) = n(R_{1,1} + R_{2,1}). \quad (56)$$

For the third term, substituting $U_0 \leftarrow Q$, $V_0 \leftarrow Q$, $U_1 \leftarrow U$, and $V_1 \leftarrow V$ in Lemma 1 result that if $\mathbb{P}\big((Q^n, U^n(W_1, A_{1,1}), V^n(W_2, A_{2,1}), Z^n) \in \mathcal{T}_\epsilon^{(n)}\big) \xrightarrow[n\to\infty]{} 1$ and

$$R_{1,1} > \mathbb{I}(U; Z|Q) + \epsilon, \quad (57)$$
$$R_{2,1} > \mathbb{I}(V; Z|Q) + \epsilon, \quad (58)$$
$$R_{1,1} + R_{2,1} > \mathbb{I}(U, V; Z|Q) + \epsilon. \quad (59)$$

Then,

$$\begin{aligned}
&\mathbb{H}(A_{1,1}, A_{2,1}|W_1, W_2, Z^n, Q^n, \mathcal{C})\\
&\qquad \leq n(R_{1,1} + R_{2,1} - \mathbb{I}(U, V; Z|Q) + \epsilon). \quad (60)
\end{aligned}$$

Here, this condition holds because

$$\begin{aligned}
&\mathbb{P}\big((Q^n, U^n(W_1, A_{1,1}), X_1^n(W_1, A_{1,1}, A_{1,2}),\\
&\quad V^n(W_2, A_{2,1}), X_2^n(W_2, A_{2,1}, A_{2,2}), Z^n) \in \mathcal{T}_\epsilon^{(n)}\big) \xrightarrow[n\to\infty]{} 1. \quad (61)
\end{aligned}$$

To bound the fourth term in (54), we have

$$\mathbb{H}(A_{1,2}, A_{2,2}|W_1, W_2, A_{1,1}, A_{2,1}, Q^n, \mathcal{C}) = n(R_{1,2} + R_{2,2}). \quad (62)$$

Now, we bound the last term in (54) by applying Lemma 1,

$$\begin{aligned}
&\mathbb{H}(A_{1,2}, A_{2,2}|W_1, W_2, A_{1,1}, A_{2,1}, Z^n, Q^n, \mathcal{C})\\
&\qquad \leq n(R_{1,2} + R_{2,2} - \mathbb{I}(X_1, X_2; Z|Q, U, V) + \epsilon), \quad (63)
\end{aligned}$$

if (61) holds and

$$R_{1,2} > \mathbb{I}(X_1; Z|Q, U, V) + \epsilon, \quad (64)$$
$$R_{2,2} > \mathbb{I}(X_2; Z|Q, U, V) + \epsilon, \quad (65)$$
$$R_{1,2} + R_{2,2} > \mathbb{I}(X_1, X_2; Z|Q, U, V) + \epsilon. \quad (66)$$

Substituting (55), (56), (60), (62), and (63) into (54) yields

$$\begin{aligned}
&\mathbb{I}(W_1, W_2; Z^n|Q^n, \mathcal{C})\\
&\leq n\mathbb{I}(X_1, X_2; Z|Q) - n(R_{1,1} + R_{2,1})\\
&\quad + n(R_{1,1} + R_{2,1} - \mathbb{I}(U, V; Z|Q) + \epsilon) - n(R_{1,2} + R_{2,2})\\
&\quad + n(R_{1,2} + R_{2,2} - \mathbb{I}(X_1, X_2; Z|Q, U, V) + \epsilon). \quad (67)
\end{aligned}$$

Therefore $\mathbb{I}(W_1, W_2; Z^n|Q^n, \mathcal{C}) \leq 2n\epsilon$. By applying the Fourier-Motzkin procedure [36] to (51)–(53), (57)–(59), (64)–(66), $R_{d_1} = R_{1,1} + R_{1,2}$, and $R_{d_2} = R_{2,1} + R_{2,2}$ we obtain the region in Theorem 7. □

APPENDIX C
PROOF OF THEOREM 1

The coding scheme is based on superposition coding, Wyner's random binning [38], Marton coding, and applying indirect decoding [10].

The random code generation is as follows:

Fix $p(q)$, $p(u_0|q)$, $p(u_1, u_2|u_0)$, $p(v_0|q)$, $p(v_1, v_2|v_0)$, $p(x_1|u_0, u_1, u_2)$, $p(x_2|v_0, v_1, v_2)$, $\epsilon_1 < \min\{\epsilon', \epsilon''\}$, and $\epsilon_2 < \min\{\epsilon', \epsilon''\}$.

Codebook Generation: Randomly and independently generate a typical sequence q^n according to $p(q^n) = \prod_{i=1}^{n} p(q_i)$. We suppose that all the terminals know q^n.

i) Generate $2^{n\tilde{R}_1}$ codewords $u_0^n(\ell_0)$ each according to $\prod_{i=1}^{n} p_{U_0|Q}(u_{0,i}|q_i)$. Then, randomly bin the $2^{n\tilde{R}_1}$ codewords into 2^{nR_1} bins, $\mathcal{B}(w_1)$, $w_1 \in [\![1, 2^{nR_1}]\!]$. For each ℓ_0, generate $2^{n\rho_1}$ codewords $u_1^n(\ell_0, t_1)$ each according to $\prod_{i=1}^{n} p_{U_1|U_0}(u_{1,i}|u_{0,i})$. Then, randomly bin the $2^{n\rho_1}$ codewords into $2^{n\rho_1'}$ bins, $\mathcal{B}(\ell_0, \ell_1)$, $\ell_1 \in [\![1, 2^{n\rho_1'}]\!]$. Similarly, for each ℓ_0, generate $2^{n\tilde{\rho}_1}$ codewords $u_2^n(\ell_0, t_2)$ each according to $\prod_{i=1}^{n} p_{U_2|U_0}(u_{2,i}|u_{0,i})$. Then, randomly bin the $2^{n\tilde{\rho}_1}$ codewords into $2^{n\tilde{\rho}_1'}$ bins, $\mathcal{B}(\ell_0, \ell_2)$, $\ell_2 \in [\![1, 2^{n\tilde{\rho}_1'}]\!]$.

ii) Similarly, generate $2^{n\tilde{R}_2}$ codewords $v_0^n(\ell_0')$ each according to $\prod_{i=1}^{n} p_{V_0|Q}(v_{0,i}|q_i)$. Then, randomly bin the $2^{n\tilde{R}_2}$ codewords into 2^{nR_2} bins, $\mathcal{B}(w_2)$, $w_2 \in [\![1, 2^{nR_2}]\!]$. For each ℓ_0', generate $2^{n\rho_2}$ codewords $v_1^n(\ell_0', s_1)$ each according to $\prod_{i=1}^{n} p_{V_1|V_0}(v_{1,i}|v_{0,i})$. Then, randomly bin the $2^{n\rho_2}$ codewords into $2^{n\rho_2'}$ bins, $\mathcal{B}(\ell_0', \ell_1')$, $\ell_1' \in [\![1, 2^{n\rho_2'}]\!]$. Similarly, for each ℓ_0', generate $2^{n\tilde{\rho}_2}$ codewords $v_2^n(\ell_0', s_2)$ each according to $\prod_{i=1}^{n} p_{V_2|V_0}(v_{2,i}|v_{0,i})$. Then, randomly bin the $2^{n\tilde{\rho}_2}$ codewords into $2^{n\tilde{\rho}_2'}$ bins, $\mathcal{B}(\ell_0', \ell_2')$, $\ell_2' \in [\![1, 2^{n\tilde{\rho}_2'}]\!]$.

Encoding: To send the message w_1, the encoder f_1 first uniformly chooses index $L_0 \in \mathcal{B}(w_1)$. Then, it uniformly chooses a pair of indices (L_1, L_2) and selects a jointly typical sequence pair $(u_1^n(L_0, t_1(L_0, L_1)), u_2^n(L_0, t_2(L_0, L_1))) \in \mathcal{T}_{\epsilon_1}^{(n)}(U_1, U_2|U_0)$ in the product bin. If the encoder f_1 finds more than one such pair, then it chooses one of them uniformly at random. We have an error if there is no such pair, in which the encoder f_1 uniformly at random chooses $t_1 \in \mathcal{B}(L_0, L_1)$, $t_2 \in \mathcal{B}(L_0, L_2)$. The error probability of the last event approaches to zero as $n \to \infty$, if [39]

$$\rho_1' + \tilde{\rho}_1' \leq \rho_1 + \tilde{\rho}_1 - \mathbb{I}(U_1; U_2|U_0) - \epsilon_1. \quad (68)$$

Finally, the encoder f_1 generates a sequence X_1^n at random according to $\prod_{i=1}^{n} p(x_{1,i}|u_{0,i}, u_{1,i}, u_{2,i})$. Encoder 2 proceeds similarly to encode w_2 and sends codeword X_2^n. The probability of not finding a jointly typical sequence pair $(v_1^n(L_0', s_1(L_0', L_1')), v_2^n(L_0', s_2(L_0', L_1'))) \in \mathcal{T}_{\epsilon_2}^{(n)}(V_1, V_2|V_0)$ in the product bin approaches to zero as $n \to \infty$, if [39]

$$\rho_2' + \tilde{\rho}_2' \leq \rho_2 + \tilde{\rho}_2 - \mathbb{I}(V_1; V_2|V_0) - \epsilon_2. \quad (69)$$

Decoding and Error Probability Analysis:

- Let (W_1, L_0, T_1) and (W_2, L_0', S_1) denote the transmitted indices by the first and the second transmitter, respectively, and let $(\hat{W}_1, \hat{L}_0, \hat{T}_1)$ and $(\hat{W}_2, \hat{L}_0', \hat{S}_1)$ denote the corresponding decoded messages by the first receiver, respectively. Receiver 1 decodes (L_0, L_0') and therefore (w_1, w_2) indirectly by finding a unique pair $(\hat{\ell}_0, \hat{\ell}_0')$ such that $(q^n, u_0^n(\hat{\ell}_0), u_1^n(\hat{\ell}_0, t_1), v_0^n(\hat{\ell}_0'), v_1^n(\hat{\ell}_0', s_1), y_1^n) \in \mathcal{T}_{\epsilon'}^{(n)}(U_0, U_1, V_0, V_1, Y_1)$ for some $t_1 \in [\![1, 2^{n\rho_1}]\!]$ and $s_1 \in [\![1, 2^{n\rho_2}]\!]$. The probability of error for Receiver 1 goes to zero as $n \to \infty$ if we choose [34]

$$\tilde{R}_1 + \rho_1 < \mathbb{I}(U_0, U_1; Y_1|Q, V_0, V_1), \quad (70)$$
$$\tilde{R}_2 + \rho_2 < \mathbb{I}(V_0, V_1; Y_1|Q, U_0, U_1), \quad (71)$$
$$\tilde{R}_1 + \rho_1 + \rho_2 < \mathbb{I}(U_0, U_1, V_1; Y_1|Q, V_0), \quad (72)$$
$$\rho_1 + \tilde{R}_2 + \rho_2 < \mathbb{I}(U_1, V_0, V_1; Y_1|Q, U_0), \quad (73)$$
$$\tilde{R}_1 + \rho_1 + \tilde{R}_2 + \rho_2 < \mathbb{I}(U_0, U_1, V_0, V_1; Y_1|Q). \quad (74)$$

The details of error analysis is available in [35] and omitted for brevity here.

- Similarly Receiver 2 decodes (L_0, L_0') and therefore (w_1, w_2) indirectly by finding a unique pair $(\check{\ell}_0, \check{\ell}_0')$ such that $(q^n, u_0^n(\check{\ell}_0), u_2^n(\check{\ell}_0, t_2), v_0^n(\check{\ell}_0'), v_2^n(\check{\ell}_0', s_2), y_2^n) \in \mathcal{T}_{\epsilon''}^{(n)}(U_0, U_2, V_0, V_2, Y_2)$ for some $t_2 \in [\![1, 2^{n\tilde{\rho}_1}]\!]$ and $s_2 \in [\![1, 2^{n\tilde{\rho}_2}]\!]$. The error analysis for the second receiver is similar to the first receiver and for the interest of brevity it is omitted here. Similar to Receiver 1 the The probability of error for Receiver 2 goes to zero as $n \to \infty$ if we choose [34]

$$\tilde{R}_1 + \tilde{\rho}_1 < \mathbb{I}(U_0, U_2; Y_2|Q, V_0, V_2), \quad (75)$$
$$\tilde{R}_2 + \tilde{\rho}_2 < \mathbb{I}(V_0, V_2; Y_2|Q, U_0, U_2), \quad (76)$$
$$\tilde{R}_1 + \tilde{\rho}_1 + \tilde{\rho}_2 < \mathbb{I}(U_0, U_2, V_2; Y_2|Q, V_0), \quad (77)$$
$$\tilde{\rho}_1 + \tilde{R}_2 + \tilde{\rho}_2 < \mathbb{I}(U_2, V_0, V_2; Y_2|Q, U_0), \quad (78)$$
$$\tilde{R}_1 + \tilde{\rho}_1 + \tilde{R}_2 + \tilde{\rho}_2 < \mathbb{I}(U_0, U_2, V_0, V_2; Y_2|Q). \quad (79)$$

Equivocation Calculation: We analyze mutual information between (W_1, W_2) and Z^n, averaged over all random codebooks

$$\begin{aligned}
&\mathbb{I}(W_1, W_2; Z^n|Q^n, \mathcal{C}) \\
&= \mathbb{I}(W_1, W_2, L_0, T_1, T_2, L_0', S_1, S_2; Z^n|Q^n, \mathcal{C}) \\
&\quad -\mathbb{I}(L_0, T_1, T_2, L_0', S_1, S_2; Z^n|W_1, W_2, Q^n, \mathcal{C}) \\
&\leq \mathbb{I}(U_0^n, U_1^n, U_2^n, V_0^n, V_1^n, V_2^n; Z^n|Q^n, \mathcal{C}) \\
&\quad -\mathbb{I}(L_0, L_0'; Z^n|W_1, W_2, Q^n, \mathcal{C}) \\
&\quad -\mathbb{I}(T_1, T_2, S_1, S_2; Z^n|L_0, L_0', Q^n, \mathcal{C}) \\
&= \mathbb{I}(U_0^n, U_1^n, U_2^n, V_0^n, V_1^n, V_2^n; Z^n|Q^n, \mathcal{C}) \\
&\quad -\mathbb{H}(L_0, L_0'|W_1, W_2, Q^n, \mathcal{C}) \\
&\quad +\mathbb{H}(L_0, L_0'|Z^n, W_1, W_2, Q^n, \mathcal{C}) \\
&\quad -\mathbb{I}(T_1, T_2, S_1, S_2; Z^n|L_0, L_0', Q^n, \mathcal{C}),
\end{aligned} \quad (80)$$

where the inequality is due to the data processing inequality. Here, T_1, T_2, S_1, and S_2 are deterministic functions of (L_0, L_1), (L_0, L_2), (L_0', L_1'), and (L_0', L_2'), respectively.

The first term in (80) is bounded as:

$$\begin{aligned}
&\mathbb{I}(U_0^n, U_1^n, U_2^n, V_0^n, V_1^n, V_2^n; Z^n|Q^n, \mathcal{C}) \\
&\qquad \leq n\mathbb{I}(U_0, U_1, U_2, V_0, V_1, V_2; Z|Q) + n\epsilon,
\end{aligned} \quad (81)$$

as $n \to \infty$ where $\epsilon \to 0$ [34].

For the second term in (80) we have

$$\mathbb{H}(L_0, L_0'|W_1, W_2, Q^n, \mathcal{C}) = n(\tilde{R}_1 - R_1 + \tilde{R}_2 - R_2). \quad (82)$$

For the third term, substituting $U_0 \leftarrow Q$, $V_0 \leftarrow Q$, $U_1 \leftarrow U_0$, and $V_1 \leftarrow V_0$ in Lemma 1 result that,

$$\begin{aligned}&\mathbb{H}(L_0, L_0'|Z^n, W_1, W_2, Q^n, \mathcal{C})\\ &\quad\le n(\tilde{R}_1 - R_1 + \tilde{R}_2 - R_2 - \mathbb{I}(U_0, V_0; Z|Q) + \epsilon), \quad (83)\end{aligned}$$

if $\mathbb{P}\big((Q^n, U_0^n(L_0), V_0^n(L_0'), Z^n) \in \mathcal{T}_\epsilon^{(n)}\big) \to 1$ as $n \to \infty$ and

$$\tilde{R}_1 - R_1 > \mathbb{I}(U_0; Z|Q) + \epsilon, \quad (84)$$
$$\tilde{R}_2 - R_2 > \mathbb{I}(V_0; Z|Q) + \epsilon, \quad (85)$$
$$\tilde{R}_1 - R_1 + \tilde{R}_2 - R_2 > \mathbb{I}(U_0, V_0; Z|Q) + \epsilon. \quad (86)$$

Here, the first condition holds because

$$\begin{aligned}&\mathbb{P}\big((Q^n, U_0^n(L_0), U_1^n(L_0, t_1(L_0, L_1)), U_2^n(L_0, t_2(L_0, L_1)),\\ &\quad V_0^n(L_0'), V_1^n(L_0', s_1(L_0', L_1')),\\ &\quad V_2^n(L_0', s_2(L_0', L_1')), Z^n) \in \mathcal{T}_\epsilon^{(n)}\big) \to 1, \quad (87)\end{aligned}$$

as $n \to \infty$. Now, we bound the last term in (80)

$$\begin{aligned}&\mathbb{I}(T_1, T_2, S_1, S_2; Z^n|L_0, L_0', Q^n, \mathcal{C})\\ &= \mathbb{H}(T_1, T_2, S_1, S_2|L_0, L_0', Q^n, \mathcal{C})\\ &\quad -\mathbb{H}(T_1, T_2, S_1, S_2|Z^n, L_0, L_0', Q^n, \mathcal{C})\\ &\overset{(a)}{=} \mathbb{H}(T_1, T_2, S_1, S_2, L_1, L_2, L_1', L_2'|L_0, L_0', Q^n, \mathcal{C})\\ &\quad -\mathbb{H}(T_1, T_2, S_1, S_2|Z^n, L_0, L_0', Q^n, \mathcal{C})\\ &\ge \mathbb{H}(L_1, L_2, L_1', L_2'|L_0, L_0', Q^n, \mathcal{C})\\ &\quad -\mathbb{H}(T_1, S_1|Z^n, L_0, L_0', Q^n, \mathcal{C})\\ &\quad -\mathbb{H}(T_2, S_2|Z^n, L_0, L_0', Q^n, \mathcal{C})\\ &\overset{(b)}{=} \mathbb{H}(L_1, L_2|L_0, L_0', Q^n, \mathcal{C}) + \mathbb{H}(L_1', L_2'|L_0, L_0', Q^n, \mathcal{C})\\ &\quad -\mathbb{H}(T_1, S_1|Z^n, L_0, L_0', Q^n, \mathcal{C})\\ &\quad -\mathbb{H}(T_2, S_2|Z^n, L_0, L_0', Q^n, \mathcal{C}), \quad (88)\end{aligned}$$

where (a) is due to given the codebook $\mathcal{C}$ and (L_0, L_0'), (L_1, L_2, L_1', L_2') is a deterministic function of $(T_1(L_0, L_1), T_2(L_0, L_2), S_1(L_0', L_1'), S_2(L_0', L_2'))$, and (b) holds due to the fact that given $(L_0, L_0', Q^n, \mathcal{C})$, (L_1, L_2) and (L_1', L_2') are independent. Now,

$$\mathbb{H}(L_1, L_2|L_0, L_0', Q^n, \mathcal{C}) = n(\rho_1' + \tilde{\rho}_1'), \quad (89)$$
$$\mathbb{H}(L_1', L_2'|L_0, L_0', Q^n, \mathcal{C}) = n(\rho_2' + \tilde{\rho}_2'), \quad (90)$$
$$\begin{aligned}&\mathbb{H}(T_1, S_1|Z^n, L_0, L_0', Q^n, \mathcal{C})\\ &\quad\overset{(a)}{\le} n(\rho_1 + \rho_2 - \mathbb{I}(U_1, V_1; Z|Q, U_0, V_0) + \epsilon), \quad (91)\\ &\mathbb{H}(T_2, S_2|Z^n, L_0, L_0', Q^n, \mathcal{C})\\ &\quad\overset{(b)}{\le} n(\tilde{\rho}_1 + \tilde{\rho}_2 - \mathbb{I}(U_2, V_2; Z|Q, U_0, V_0) + \epsilon), \quad (92)\end{aligned}$$

where (a) is due to the following. Consider,

$$\begin{aligned}&\mathbb{H}(T_1, S_1|Z^n, L_0, L_0', Q^n, \mathcal{C})\\ &\quad= \mathbb{H}(T_1, S_1|U_0^n(L_0), V_0^n(L_0'), Z^n, L_0, L_0', Q^n, \mathcal{C})\\ &\quad\le \mathbb{H}(T_1, S_1|U_0^n(L_0), V_0^n(L_0'), Z^n, Q^n, \mathcal{C}).\end{aligned}$$

Now we upper bound the term $\mathbb{H}(T_1, S_1|U_0^n(L_0), V_0^n(L_0'), Z^n, Q^n, \mathcal{C})$. From (87) we have $\mathbb{P}\big((Q^n, U_0^n(L_0), U_1^n(L_0, t_1(L_0, L_1)), V_0^n(L_0'), V_1^n(L_0', s_1(L_0', L_1')), Z^n) \in \mathcal{T}_\epsilon^{(n)}\big) \to 1$ as $n \to \infty$. Applying Lemma 1 leads to,

$$\begin{aligned}&\mathbb{H}(T_1, S_1|U_0^n(L_0), V_0^n(L_0'), Z^n, Q^n, \mathcal{C})\\ &\quad\le n(\rho_1 + \rho_2 - \mathbb{I}(U_1, V_1; Z|Q, U_0, V_0) + \epsilon), \quad (93)\end{aligned}$$

if

$$\rho_1 > \mathbb{I}(U_1; Z|Q, U_0, V_0) + \epsilon, \quad (94)$$
$$\rho_2 > \mathbb{I}(V_1; Z|Q, U_0, V_0) + \epsilon, \quad (95)$$
$$\rho_1 + \rho_2 > \mathbb{I}(U_1, V_1; Z|Q, U_0, V_0) + \epsilon. \quad (96)$$

By the same argument the inequality (b) holds, if the following inequalities hold,

$$\tilde{\rho}_1 > \mathbb{I}(U_2; Z|Q, U_0, V_0) + \epsilon,$$
$$\tilde{\rho}_2 > \mathbb{I}(V_2; Z|Q, U_0, V_0) + \epsilon,$$
$$\tilde{\rho}_1 + \tilde{\rho}_2 > \mathbb{I}(U_2, V_2; Z|Q, U_0, V_0) + \epsilon.$$

Substituting (89)–(92) into (88) leads to,

$$\begin{aligned}&\mathbb{I}(T_1, T_2, S_1, S_2; Z^n|L_0, L_0', Q^n, \mathcal{C})\\ &\quad\ge n(\rho_1' + \tilde{\rho}_1') + n(\rho_2' + \tilde{\rho}_2')\\ &\qquad -n(\rho_1 + \rho_2 - \mathbb{I}(U_1, V_1; Z|Q, U_0, V_0) + \epsilon)\\ &\qquad -n(\tilde{\rho}_1 + \tilde{\rho}_2 - \mathbb{I}(U_2, V_2; Z|Q, U_0, V_0) + \epsilon). \quad (97)\end{aligned}$$

Substituting (81)–(83) and (97) into (80) yields

$$\begin{aligned}&\mathbb{I}(W_1, W_2; Z^n|Q^n, \mathcal{C})\\ &\le n\mathbb{I}(U_0, U_1, U_2, V_0, V_1, V_2; Z|Q) - n(\tilde{R}_1 - R_1 + \tilde{R}_2 - R_2)\\ &\quad +n(\tilde{R}_1 - R_1 + \tilde{R}_2 - R_2 - \mathbb{I}(U_0, V_0; Z|Q))\\ &\quad -n(\rho_1' + \tilde{\rho}_1') - n(\rho_2' + \tilde{\rho}_2')\\ &\quad +n(\rho_1 + \rho_2 - \mathbb{I}(U_1, V_1; Z|Q, U_0, V_0) + \epsilon)\\ &\quad +n(\tilde{\rho}_1 + \tilde{\rho}_2 - \mathbb{I}(U_2, V_2; Z|Q, U_0, V_0) + \epsilon). \quad (98)\end{aligned}$$

Therefore $\mathbb{I}(W_1, W_2; Z^n|Q^n, \mathcal{C}) \le n\epsilon$ if

$$\begin{aligned}&\mathbb{I}(U_1, U_2, V_1, V_2; Z|U_0, V_0)\\ &\quad -\rho_1' - \tilde{\rho}_1' - \rho_2' - \tilde{\rho}_2' + \rho_1 + \rho_2 - \mathbb{I}(U_1, V_1; Z|Q, U_0, V_0)\\ &\quad +\tilde{\rho}_1 + \tilde{\rho}_2 - \mathbb{I}(U_2, V_2; Z|Q, U_0, V_0) \le \epsilon. \quad (99)\end{aligned}$$

As a result, the rate constraints derived in equivocation analysis are

$$\tilde{R}_1 - R_1 + \tilde{R}_2 - R_2 > \mathbb{I}(U_0, V_0; Z|Q), \quad (100)$$
$$\tilde{R}_1 - R_1 > \mathbb{I}(U_0; Z|Q), \quad (101)$$
$$\tilde{R}_2 - R_2 > \mathbb{I}(V_0; Z|Q), \quad (102)$$
$$\rho_1 + \rho_2 > \mathbb{I}(U_1, V_1; Z|Q, U_0, V_0), \quad (103)$$
$$\rho_1 > \mathbb{I}(U_1; Z|Q, U_0, V_0), \quad (104)$$
$$\rho_2 > \mathbb{I}(V_1; Z|Q, U_0, V_0), \quad (105)$$
$$\tilde{\rho}_1 + \tilde{\rho}_2 > \mathbb{I}(U_2, V_2; Z|Q, U_0, V_0), \quad (106)$$
$$\tilde{\rho}_1 > \mathbb{I}(U_2; Z|Q, U_0, V_0), \quad (107)$$
$$\tilde{\rho}_2 > \mathbb{I}(V_2; Z|Q, U_0, V_0), \quad (108)$$
$$\begin{aligned}&\rho_1 + \rho_2 + \tilde{\rho}_1 + \tilde{\rho}_2 - \rho_1' - \tilde{\rho}_1' - \rho_2' - \tilde{\rho}_2'\\ &\quad\le \mathbb{I}(U_1, V_1; Z|Q, U_0, V_0) + \mathbb{I}(U_2, V_2; Z|Q, U_0, V_0)\\ &\quad -\mathbb{I}(U_1, U_2, V_1, V_2; Z|U_0, V_0). \quad (109)\end{aligned}$$

Finally, by applying the Fourier-Motzkin procedure [37] to (68), (69), (70)–(79), and (100)–(109) we obtain the inequalities in Theorem 1.

APPENDIX D
PROOF OF THEOREM 2

To prove Theorem 2, we first show that any achievable rate pairs (R_1, R_2) will satisfy (13)-(15) for some distribution factorized as (16).

Applying Fano's inequality [34] results in

$$\mathbb{H}(W_1, W_2|Y_1^n) \leq n\varepsilon_1, \tag{110}$$
$$\mathbb{H}(W_1, W_2|Y_2^n) \leq n\varepsilon_2, \tag{111}$$

where $\varepsilon_i \to 0,\ i = 1, 2$ as $P_e^n \to 0$.

We first derive the bound on R_1. Note that the secrecy condition (1) implies that

$$nR_1 - n\delta \leq \mathbb{H}(W_1|Z^n), \tag{112}$$
$$nR_2 - n\delta \leq \mathbb{H}(W_2|Z^n). \tag{113}$$

We first define

$$Q_i = (Z_{i+1}^n, Y_2^{i-1}), \tag{114}$$
$$U_{0,i} = (W_1, Q_i), \tag{115}$$
$$V_{0,i} = (W_2, Q_i). \tag{116}$$

From (112) we have,

$$\begin{aligned}
nR_1 &\leq \mathbb{H}(W_1|Z^n) + n\delta \\
&= \mathbb{H}(W_1) - \mathbb{I}(W_1; Z^n) + n\delta \\
&\overset{(a)}{\leq} \mathbb{H}(W_1) - \mathbb{H}(W_1|Y_2^n) - \mathbb{I}(W_1; Z^n) + n(\varepsilon_2 + \delta) \\
&\overset{(b)}{=} \mathbb{I}(W_1; Y_2^n) - \mathbb{I}(W_1; Z^n) + n\varepsilon \\
&= \sum_{i=1}^n [\mathbb{I}(W_1; Y_{2,i}|Y_2^{i-1}) - \mathbb{I}(W_1; Z_i|Z_{i+1}^n)] + n\varepsilon \\
&= \sum_{i=1}^n [\mathbb{I}(W_1, Z_{i+1}^n; Y_{2,i}|Y_2^{i-1}) - \mathbb{I}(Z_{i+1}^n; Y_{2,i}|W_1, Y_2^{i-1}) \\
&\quad - \mathbb{I}(W_1, Y_2^{i-1}; Z_i|Z_{i+1}^n) + \mathbb{I}(Y_2^{i-1}; Z_i|W_1, Z_{i+1}^n)] + n\varepsilon \\
&\overset{(c)}{=} \sum_{i=1}^n [\mathbb{I}(W_1, Z_{i+1}^n; Y_{2,i}|Y_2^{i-1}) \\
&\quad - \mathbb{I}(W_1, Y_2^{i-1}; Z_i|Z_{i+1}^n)] + n\varepsilon \\
&= \sum_{i=1}^n [\mathbb{I}(Z_{i+1}^n; Y_{2,i}|Y_2^{i-1}) + \mathbb{I}(W_1; Y_{2,i}|Z_{i+1}^n, Y_2^{i-1}) \\
&\quad - \mathbb{I}(Y_2^{i-1}; Z_i|Z_{i+1}^n) - \mathbb{I}(W_1; Z_i|Z_{i+1}^n, Y_2^{i-1})] + n\varepsilon \\
&\overset{(d)}{=} \sum_{i=1}^n [\mathbb{I}(W_1; Y_{2,i}|Z_{i+1}^n, Y_2^{i-1}) \\
&\quad - \mathbb{I}(W_1; Z_i|Z_{i+1}^n, Y_2^{i-1})] + n\varepsilon \\
&\overset{(e)}{=} \sum_{i=1}^n [\mathbb{I}(U_{0,i}; Y_{2,i}|Q_i) - \mathbb{I}(U_{0,i}; Z_i|Q_i)] + n\varepsilon
\end{aligned} \tag{117}$$

where (a) follows from Fano's inequality, (b) follows by setting $\varepsilon = \varepsilon_2 + \delta$. Equalities in (c) and (d) result from Csiszár's sum identity [33] where we have

$$\sum_{i=1}^n \mathbb{I}(Z_{i+1}^n; Y_{2,i}|W_1, Y_2^{i-1}) = \sum_{i=1}^n \mathbb{I}(Y_2^{i-1}; Z_i|W_1, Z_{i+1}^n), \tag{118}$$

$$\sum_{i=1}^n \mathbb{I}(Z_{i+1}^n; Y_{2,i}|Y_2^{i-1}) = \sum_{i=1}^n \mathbb{I}(Y_2^{i-1}; Z_i|Z_{i+1}^n). \tag{119}$$

The equality (e) follows from definition of random variables in (114)-(116).

Now, based on (117) we have:

$$\begin{aligned}
nR_1 &\leq n \sum_{i=1}^n \frac{1}{n} [\mathbb{I}(U_{0,K}; Y_{2,K}|Q_K, K = i) \\
&\quad - \mathbb{I}(U_{0,K}; Z_K|Q_K, K = i)] + n\varepsilon \\
&= n \sum_{i=1}^n p(K = i)[\mathbb{I}(U_{0,K}; Y_{2,K}|Q_K, K = i) \\
&\quad - \mathbb{I}(U_{0,K}; Z_K|Q_K, K = i)] + n\varepsilon \\
&= n[\mathbb{I}(U_{0,K}; Y_{2,K}|Q_K, K) \\
&\quad - \mathbb{I}(U_{0,K}; Z_K|Q_K, K)] + n\varepsilon \\
&= n[\mathbb{I}(U_0; Y_2|Q) - \mathbb{I}(U_0; Z|Q)] + n\varepsilon
\end{aligned} \tag{120}$$

where $U_{0,K} = U_0$, $Y_{2,K} = Y_2$, $Z_K = Z$, $(Q_K, K) = Q$ and K has a uniform distribution over $\{1, 2, \ldots, n\}$ outcomes.

The bounds on R_2 and $R_1 + R_2$ can be proven similar to the bound on R_1 by substitution of W_1 by W_2 and W_1 by (W_1, W_2), respectively. We omit the details for brevity.

APPENDIX E
PROOF OF THEOREM 3

The proof of achievability follows from Theorem 1 by setting $U_0 = U_1 = U_2$ and $V_0 = V_1 = V_2$ and considering the fact that the channel is degraded. Now, we show that for the degraded switch model the outer bound in Theorem 2 will reduce to the region in Theorem 3. We need to show that the outer bound distribution for the degraded switch case is equal to (26). Therefore, we need to show that given Q, U_0 and V_0 are independent, i.e.,

$$\mathbb{I}(U_0; V_0|Q) = 0. \tag{121}$$

Moreover, we have to show that

$$\mathbb{I}(U_0; Y_2'|V_0, Q) = \mathbb{I}(U_0; Y_2'|Q), \tag{122}$$
$$\mathbb{I}(V_0; Y_2'|U_0, Q) = \mathbb{I}(V_0; Y_2'|Q). \tag{123}$$

To prove (122) and (123) we need to show that

$$\mathbb{I}(U_0; V_0|Y_2', Q) = 0, \tag{124}$$

because if this equation holds we have

$$\begin{aligned}
\mathbb{I}(U_0; Y_2'|Q) &= \mathbb{I}(U_0; V_0|Q) + \mathbb{I}(U_0; Y_2'|V_0, Q) \\
&\quad - \mathbb{I}(U_0; V_0|Y_2', Q) \\
&= \mathbb{I}(U_0; Y_2'|V_0, Q),
\end{aligned} \tag{125}$$

$$\begin{aligned}
\mathbb{I}(V_0; Y_2'|Q) &= \mathbb{I}(V_0; U_0|Q) + \mathbb{I}(V_0; Y_2'|U_0, Q) \\
&\quad - \mathbb{I}(V_0; U_0|Y_2', Q) \\
&= \mathbb{I}(V_0; Y_2'|U_0, Q).
\end{aligned} \tag{126}$$

From (114)-(116) and (17)-(19) the equations in (121) and (124) are equal to the following equalities, respectively,

$$\mathbb{I}(W_1; W_2|Z_{i+1}^n, S_{i+1}^n, Y_2^{i-1}, S^{i-1}) = 0, \quad (127)$$
$$\mathbb{I}(W_1; W_2|Y_{2,i}, S_i, Z_{i+1}^n, S_{i+1}^n, Y_2^{i-1}, S^{i-1}) = 0. \quad (128)$$

First, we prove (127),

$$\begin{aligned}
&\mathbb{I}(W_1; W_2|Z_{i+1}^n, S_{i+1}^n, Y_2^{i-1}, S^{i-1}) \\
&\quad = \sum_{s_{i+1}^n}\sum_{s^{i-1}} p(S_{i+1}^n = s_{i+1}^n, S^{i-1} = s^{i-1}) \times \\
&\qquad \mathbb{I}(W_1; W_2|Z_{i+1}^n, S_{i+1}^n = s_{i+1}^n, Y_2^{i-1}, S^{i-1} = s^{i-1}) \\
&\quad = \sum_{s_{i+1}^n}\sum_{s^{i-1}} \prod_{\substack{j=1\\ j\neq i}}^{n} [p(S_j = s_j)] \\
&\qquad \times \mathbb{I}(W_1; W_2|Z_{i+1}^n, S_{i+1}^n = s_{i+1}^n, Y_2^{i-1}, S^{i-1} = s^{i-1}).
\end{aligned}$$

For a given s_i, (22) implies that $y_{1,i}$ and therefore $y_{2,i}$ and z_i only depend on the channel input $x_{s_i,i}$. By using functional dependence graphs [40], one can show that

$$\mathbb{I}(W_1; W_2|Z_{i+1}^n, S_{i+1}^n = s_{i+1}^n, Y_2^{i-1}, S^{i-1} = s^{i-1}) = 0,$$

for fixed switch state information s^{i-1} and s_{i+1}^n. This completes the proof of the equality (121). By following the same approach, we can also proof (128).

Appendix F
Proof of Theorem 4

To prove Theorem 4, we first show that any achievable rate pairs (R_1, R_2) will satisfy (27)-(29) for some distribution factorized as (30).

Applying Fano's inequality [34] results in

$$\mathbb{H}(W_1, W_2|Y_1^n) \leq n\varepsilon_1 \quad (129)$$
$$\mathbb{H}(W_1, W_2|Y_2^n) \leq n\varepsilon_2 \quad (130)$$

where $\varepsilon_i \to 0,\ i = 1, 2$ as $P_e^n \to 0$.

We first derive the bound on R_1. Note that the perfect secrecy (1) implies that

$$nR_1 - n\delta \leq \mathbb{H}(W_1|Z^n) \quad (131)$$
$$nR_2 - n\delta \leq \mathbb{H}(W_2|Z^n). \quad (132)$$

Define,

$$Q_i = (Z_{i+1}^n, Y_1^{i-1}, Y_2^{i-1}), \quad (133)$$
$$U_{0,i} = (W_1, Q_i), \quad (134)$$
$$V_{1,i} = (W_2, Q_i), \quad (135)$$

From (131) we have,

$$\begin{aligned}
nR_1 &\leq \mathbb{H}(W_1|Z^n) + n\delta \\
&= \mathbb{H}(W_1) - \mathbb{I}(W_1; Z^n) + n\delta \\
&\overset{(a)}{\leq} \mathbb{H}(W_1) - \mathbb{H}(W_1|Y_1^n, Y_2^n) - \mathbb{I}(W_1; Z^n) + n(\varepsilon_2 + \delta) \\
&\overset{(b)}{=} \mathbb{I}(W_1; Y_1^n, Y_2^n) - \mathbb{I}(W_1; Z^n) + n\varepsilon \\
&= \sum_{i=1}^{n} \big[\mathbb{I}(W_1; Y_{1,i}, Y_{2,i}|Y_1^{i-1}, Y_2^{i-1}) \\
&\quad - \mathbb{I}(W_1; Z_i|Z_{i+1}^n)\big] + n\varepsilon \\
&= \sum_{i=1}^{n} \big[\mathbb{I}(W_1, Z_{i+1}^n; Y_{1,i}, Y_{2,i}|Y_1^{i-1}, Y_2^{i-1}) \\
&\quad - \mathbb{I}(Z_{i+1}^n; Y_{1,i}, Y_{2,i}|W_1, Y_1^{i-1}, Y_2^{i-1}) \\
&\quad - \mathbb{I}(W_1, Y_1^{i-1}, Y_2^{i-1}; Z_i|Z_{i+1}^n) \\
&\quad + \mathbb{I}(Y_1^{i-1}, Y_2^{i-1}; Z_i|W_1, Z_{i+1}^n)\big] + n\varepsilon \\
&\overset{(c)}{=} \sum_{i=1}^{n} \big[\mathbb{I}(W_1, Z_{i+1}^n; Y_{1,i}, Y_{2,i}|Y_1^{i-1}, Y_2^{i-1}) \\
&\quad - \mathbb{I}(W_1, Y_1^{i-1}, Y_2^{i-1}; Z_i|Z_{i+1}^n)\big] + n\varepsilon \\
&= \sum_{i=1}^{n} \big[\mathbb{I}(Z_{i+1}^n; Y_{1,i}, Y_{2,i}|Y_1^{i-1}, Y_2^{i-1}) \\
&\quad + \mathbb{I}(W_1; Y_{1,i}, Y_{2,i}|Z_{i+1}^n, Y_1^{i-1}, Y_2^{i-1}) \\
&\quad - \mathbb{I}(Y_1^{i-1}, Y_2^{i-1}; Z_i|Z_{i+1}^n) \\
&\quad - \mathbb{I}(W_1; Z_i|Z_{i+1}^n, Y_1^{i-1}, Y_2^{i-1})\big] + n\varepsilon \\
&\overset{(d)}{=} \sum_{i=1}^{n} \big[\mathbb{I}(W_1; Y_{1,i}, Y_{2,i}|Z_{i+1}^n, Y_1^{i-1}, Y_2^{i-1}) \\
&\quad - \mathbb{I}(W_1; Z_i|Z_{i+1}^n, Y_1^{i-1}, Y_2^{i-1})\big] + n\varepsilon \\
&\overset{(e)}{=} \sum_{i=1}^{n} \big[\mathbb{I}(U_{0,i}; Y_{1,i}, Y_{2,i}|Q_i) - \mathbb{I}(U_{0,i}; Z_i|Q_i)\big] + n\varepsilon
\end{aligned} \quad (136)$$

where (a) follows from Fano's inequality, (b) follows by setting $\varepsilon = \varepsilon_2 + \delta$. Equalities in (c) and (d) result from Csiszár's sum identity [33] where we have

$$\begin{aligned}
&\sum_{i=1}^{n} \mathbb{I}(Z_{i+1}^n; Y_{1,i}, Y_{2,i}|W_1, Y_1^{i-1}, Y_2^{i-1}) \\
&\quad = \sum_{i=1}^{n} \mathbb{I}(Y_1^{i-1}, Y_2^{i-1}; Z_i|W_1, Z_{i+1}^n)
\end{aligned} \quad (137)$$

$$\begin{aligned}
&\sum_{i=1}^{n} \mathbb{I}(Z_{i+1}^n; Y_{1,i}, Y_{2,i}|Y_1^{i-1}, Y_2^{i-1}) \\
&\quad = \sum_{i=1}^{n} \mathbb{I}(Y_1^{i-1}, Y_2^{i-1}; Z_i|Z_{i+1}^n).
\end{aligned} \quad (138)$$

The equality (e) follows from definition of random variables in (133)-(135).

Now, by applying the same time-sharing strategy as (120) we have

$$R_1 \leq \mathbb{I}(U_0; Y_1, Y_2|Q) - \mathbb{I}(U_0; Z|Q) + n\varepsilon. \quad (139)$$

The bounds on R_2 and $R_1 + R_2$ can be proven similar to the bound on R_1 by substitution of W_1 by W_2 and W_1 by (W_1, W_2), respectively. We omit the details for brevity.

Appendix G
Proof of Theorem 5

We show that specializing the achievable rate region in Theorem 1 and the outer bound in Theorem 4 to the noiseless switch model identically yields the rate region in Theorem 5. In the noiseless switch model, the sum-rate constraint is redundant and does not appear.

Corollary 2: By setting $U_0 = U_1 = U_2$ and $V_0 = V_1 = V_2$ and considering the fact that $Y_1 = Y_2$, and therefore $Y_1' = Y_2'$, the achievable rate region in Theorem 1 will reduce to the set of non-negative rate pair (R_1, R_2) such that

$$R_1 \le \mathbb{I}(U_0; Y_1'|Q, V_0) - \mathbb{I}(U_0; Z|Q), \tag{140}$$
$$R_2 \le \mathbb{I}(V_0; Y_1'|Q, U_0) - \mathbb{I}(V_0; Z|Q), \tag{141}$$
$$R_1 + R_2 \le \mathbb{I}(U_0, V_0; Y_1'|Q) - \mathbb{I}(U_0, V_0; Z|Q), \tag{142}$$

for some

$$p(q)p(u_0|q)p(v_0|q)p(x_1|u_0)p(x_2|v_0). \tag{143}$$

Corollary 3: By considering the fact that Y_1' is equal to Y_2' the outer bound in Theorem 4 will reduce to the set of couple rates (R_1, R_2) satisfying

$$R_1 \le \mathbb{I}(U_0; Y_1'|Q) - \mathbb{I}(U_0; Z|Q), \tag{144}$$
$$R_2 \le \mathbb{I}(V_0; Y_1'|Q) - \mathbb{I}(V_0; Z|Q), \tag{145}$$
$$R_1 + R_2 \le \mathbb{I}(U_0, V_0; Y_1'|Q) - \mathbb{I}(U_0, V_0; Z|Q), \tag{146}$$

for some joint distribution

$$p(q)p(u_0, v_0|q)p(x_1|u_0)p(x_2|v_0). \tag{147}$$

By using a similar approach to the proof of Theorem 4 one can show that for the outer bound we have

$$\mathbb{I}(U_0; V_0|Q) = 0, \tag{148}$$
$$\mathbb{I}(U_0; V_0|Q, Y_1') = 0. \tag{149}$$

Therefore, the achievable rate region in Corollary 2 and the outer bound in Corollary 3 meet. By setting $Q = \emptyset$, $U_0 = X_1$, and $V_0 = X_2$ and considering the fact that the channel is noiseless one can verify the region in Theorem 5.

APPENDIX H
PROOF OF THEOREM 6

The achievability proof is inspired by [12], and is based on solving a dual secret key agreement problem in the source model that includes shared randomness at all terminals (see Fig. 5). In this dual model, rate constraints are derived so that the input and output distributions of the dual model approximate that of the original model while satisfying reliability and secrecy conditions in the dual model. The probability approximation then guarantees that reliability *and* secrecy conditions can be achieved in the original model. Finally, it is shown that there exists one realization of shared randomness for which the above mentioned conditions are valid, thus removing the necessity for common randomness.

We develop the encoding and decoding strategies for the source model and the original model, and derive and compare the joint probability distributions arising from these two strategies. We begin with the multi-terminal secret key agreement problem in the source model as depicted in Fig. 5. Let $(U_{[0:2]}^n, V_{[0:2]}^n, X_1^n, X_2^n, Y_1^n, Y_2^n, Z^n)$ be i.i.d. and distributed according to

$$p(u_{[0:2]}, x_1)p(v_{[0:2]}, x_2)p(y_1, y_2, z|x_1, x_2). \tag{150}$$

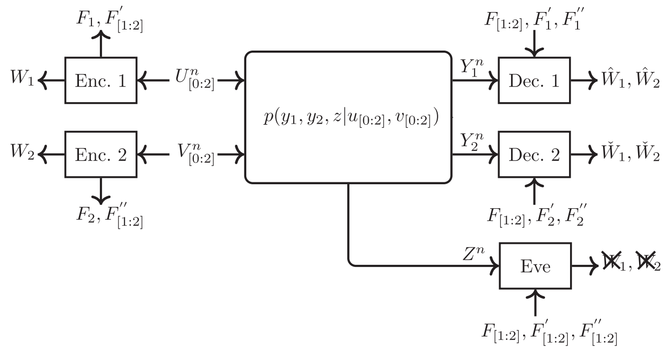

Fig. 5. Dual secret key agreement problem in the source model for the original problem.

Random Binning:

- To *each* u_0^n, uniformly and independently assign two random bin indices $w_1 \in [\![1, 2^{nR_1}]\!]$ and $f_1 \in [\![1, 2^{n\tilde{R}_1}]\!]$.
- To each pair (u_0^n, u_j^n) for $j = 1, 2$ uniformly and independently assign random bin index $f_j' \in [\![1, 2^{n\tilde{R}_j'}]\!]$.
- To each v_0^n uniformly and independently assign two random bin indices $w_2 \in [\![1, 2^{nR_2}]\!]$ and $f_2 \in [\![1, 2^{n\tilde{R}_2}]\!]$.
- To each pair (v_0^n, v_j^n) for $j = 1, 2$ uniformly and independently assign random bin index $f_j'' \in [\![1, 2^{n\tilde{R}_j''}]\!]$.
- The random variables representing bin indices are:

$$W_{[1:2]}\ , \quad F_{[1:2]}\ , \quad F'_{[1:2]}\ , \quad F''_{[1:2]}. \tag{151}$$

- Decoder 1 is a Slepian-Wolf decoder observing $(y_1^n, f_{[1:2]}, f_1', f_1'')$, and producing $(\hat{u}_0^n, \hat{u}_1^n)$ and $(\hat{v}_0^n, \hat{v}_1^n)$, thus declaring $\hat{w}_1 = W_1(\hat{u}_0^n)$ and $\hat{w}_2 = W_2(\hat{v}_0^n)$ to be the estimate of the pair (w_1, w_2).
- Decoder 2 is a Slepian-Wolf decoder observing $(y_2^n, f_{[1:2]}, f_2', f_2'')$, and producing $(\check{u}_0^n, \check{u}_2^n)$ and $(\check{v}_0^n, \check{v}_2^n)$, thus declaring the bin indices $\check{w}_1 = W_1(\check{u}_0^n)$ and $\check{w}_2 = W_2(\check{v}_0^n)$ as the estimate of the pair (w_1, w_2).

To condense the notation, we define the following variables:

$$\mathbf{f} \triangleq \left(f_{[1:2]}, f'_{[1:2]}, f''_{[1:2]}\right), \tag{152}$$
$$\hat{\mathbf{u}} \triangleq \left(\hat{u}_0^n, \check{u}_0^n, \hat{u}_1^n, \check{u}_2^n, \hat{v}_0^n, \check{v}_0^n, \hat{v}_1^n, \check{v}_2^n\right). \tag{153}$$

Each binning leads to a distribution (PMF). Furthermore, in our problem, the binning itself is random and each binning has a probability. Following Cuff [30] and [12, Remark 1], for compact representation and ease of manipulation, we "stack" the ordinary PMF of the individual binnings into a random PMF. The random PMF induced by random binning is then as follows:

$$\begin{aligned}
&P(u_{[0:2]}^n, v_{[0:2]}^n, x_{[1:2]}^n, y_1^n, y_2^n, z^n, w_{[1:2]}, \mathbf{f}, \hat{\mathbf{u}}) \\
&= p(u_{[0:2]}^n, v_{[0:2]}^n, x_{[1:2]}^n, y_1^n, y_2^n, z^n)P(w_{[1:2]}, f_{[1:2]}|u_0^n, v_0^n) \\
&\quad \times P(f'_{[1:2]}, f''_{[1:2]}|u_{[0:2]}^n, v_{[0:2]}^n) \\
&\quad \times P^{SW}(\hat{u}_0^n, \hat{u}_1^n, \hat{v}_0^n, \hat{v}_1^n|y_1^n, f_{[1:2]}, f_1', f_1'') \\
&\quad \times P^{SW}(\check{u}_0^n, \check{u}_2^n, \check{v}_0^n, \check{v}_2^n|y_2^n, f_{[1:2]}, f_2', f_2'') \\
&= P(w_{[1:2]}, f_{[1:2]}, u_0^n, v_0^n)P(f'_{[1:2]}, f''_{[1:2]}, u_{[1:2]}^n, v_{[1:2]}^n|u_0^n, v_0^n) \\
&\quad \times p(x_1^n|u_{[0:2]}^n)p(x_2^n|v_{[0:2]}^n)p(y_1^n, y_2^n, z^n|x_1^n, x_2^n) \\
&\quad \times P^{SW}(\hat{u}_0^n, \hat{u}_1^n, \hat{v}_0^n, \hat{v}_1^n|y_1^n, f_{[1:2]}, f_1', f_1'') \\
&\quad \times P^{SW}(\check{u}_0^n, \check{u}_2^n, \check{v}_0^n, \check{v}_2^n|y_2^n, f_{[1:2]}, f_2', f_2'')
\end{aligned}$$

$$\begin{aligned}&= P(w_{[1:2]}, f_{[1:2]})P(u_0^n, v_0^n|w_{[1:2]}, f_{[1:2]})\\&\quad\times P(f'_{[1:2]}, f''_{[1:2]}|u_0^n, v_0^n)P(u_{[1:2]}^n, v_{[1:2]}^n|u_0^n, v_0^n, f'_{[1:2]}, f''_{[1:2]})\\&\quad\times p(x_1^n|u_{[0:2]}^n)p(x_2^n|v_{[0:2]}^n)p(y_1^n, y_2^n, z^n|x_1^n, x_2^n)\\&\quad\times P^{SW}(\hat{u}_0^n, \hat{u}_1^n, \hat{v}_0^n, \hat{v}_1^n|y_1^n, f_{[1:2]}, f'_1, f''_1)\\&\quad\times P^{SW}(\check{u}_0^n, \check{u}_2^n, \check{v}_0^n, \check{v}_2^n|y_2^n, f_{[1:2]}, f'_2, f''_2). \end{aligned} \tag{154}$$

Here, P^{SW} denotes the PMF of the output of the Slepian-Wolf decoder, which is a random PMF. $\hat{W}_1, \hat{W}_2$ and $\check{W}_1, \check{W}_2$ are omitted because they are functions of other random variables.

We now return to the original problem illustrated in Fig. 1 except that, in addition, a genie provides all terminals with shared randomness described by $(F_{[1:2]}, F'_{[1:2]}, F''_{[1:2]})$, whose distribution will be clarified in the sequel. In this augmented model:

- The messages W_1 and W_2 are mutually independent and uniformly distributed with rates R_1 and R_2 respectively. The shared randomness (F_1, F_2) is uniformly distributed over $[\![1, 2^{n\tilde{R}_1}]\!]$, $[\![1, 2^{n\tilde{R}_2}]\!]$, and independent of W_1, W_2.
- Encoder 1 and 2 are stochastic encoders producing codewords U_0^n and V_0^n according to distributions $P(u_0^n|w_{[1:2]}, f_{[1:2]})$ and $P(v_0^n|w_{[1:2]}, f_{[1:2]})$, respectively, which are the marginals of distribution $P(u_0^n, v_0^n|w_{[1:2]}, f_{[1:2]})$ appearing in (154). This choice of encoder establishes a the connection between the two models.
- The four random variables $F'_{[1:2]}, F''_{[1:2]}$ are mutually independent and uniformly distributed over, $[\![1, 2^{n\tilde{R}'_1}]\!]$ and $[\![1, 2^{n\tilde{R}'_2}]\!]$, $[\![1, 2^{n\tilde{R}''_1}]\!]$ and $[\![1, 2^{n\tilde{R}''_2}]\!]$, respectively. They are also independent of (U_0^n, V_0^n) and therefore are independent of $(W_{[1:2]}, F_{[1:2]})$.
- Encoder 1 and 2 further generate $U_{[1:2]}^n$, $V_{[1:2]}^n$ according to $P(u_{[1:2]}^n|u_0^n, v_0^n, f'_{[1:2]}, f''_{[1:2]})$ and $P(v_{[1:2]}^n|u_0^n, v_0^n, f'_{[1:2]}, f''_{[1:2]})$, respectively, which are marginal distributions of $P(u_{[1:2]}^n, v_{[1:2]}^n|u_0^n, v_0^n, f'_{[1:2]}, f''_{[1:2]})$ from (154).
- Encoder 1 generates X_1^n i.i.d. according to $p(x_1|u_{[0:2]})$. Encoder 2 generates X_2^n i.i.d. according to $p(x_2|v_{[0:2]})$. X_1, X_2 are transmitted over the channel.
- Decoders 1 and 2 are Slepian-Wolf decoders inherited from the source model secret key agreement problem, observing $(y_1^n, f_{[1:2]}, f'_1, f''_1)$ and $(y_2^n, f_{[1:2]}, f'_2, f''_2)$, and producing $(\hat{u}_0^n, \hat{u}_1^n, \hat{v}_0^n, \hat{v}_1^n)$ and $(\check{u}_0^n, \check{u}_2^n, \check{v}_0^n, \check{v}_2^n)$, respectively. Therefore the following random PMFs for the decoder output distributions are inherited from the source model:
$$P^{SW}(\hat{u}_0^n, \hat{u}_1^n, \hat{v}_0^n, \hat{v}_1^n|y_1^n, f_{[1:2]}, f'_1, f''_1),$$
$$P^{SW}(\check{u}_0^n, \check{u}_2^n, \check{v}_0^n, \check{v}_2^n|y_2^n, f_{[1:2]}, f'_2, f''_2).$$
- Decoders 1 and 2 then produce estimates of (W_1, W_2), which are denoted $(\hat{W}_1, \hat{W}_2)$ and $(\check{W}_1, \check{W}_2)$ respectively.

The random PMF induced by the random binning and the encoding/decoding strategy is as follows:

$$\begin{aligned}&\hat{P}(u_{[0:2]}^n, v_{[0:2]}^n, y_1^n, y_2^n, z^n, w_{[1:2]}, \mathbf{f}, \hat{\mathbf{u}})\\&= p^U(w_{[1:2]})p^U(f_{[1:2]})P(u_0^n, v_0^n|w_{[1:2]}, f_{[1:2]})\\&\quad\times p^U(f'_{[1:2]})p^U(f''_{[1:2]})P(u_{[1:2]}^n, v_{[1:2]}^n|u_0^n, v_0^n, f'_{[1:2]}, f''_{[1:2]})\\&\quad\times p(x_1^n|u_{[0:2]}^n)p(x_2^n|v_{[0:2]}^n)p(y_1^n, y_2^n, z^n|x_1^n, x_2^n)\\&\quad\times P^{SW}(\hat{u}_0^n, \hat{u}_1^n, \hat{v}_0^n, \hat{v}_1^n|y_1^n, f_{[1:2]}, f'_1, f''_1)\\&\quad\times P^{SW}(\check{u}_0^n, \check{u}_2^n, \check{v}_0^n, \check{v}_2^n|y_2^n, f_{[1:2]}, f'_2, f''_2),\end{aligned} \tag{155}$$

where $\mathbf{f}$ and $\hat{\mathbf{u}}$ are defined in (152) and (153), respectively, and p^U is the uniform distribution.

We now find constraints that ensure that the PMFs $\hat{P}$ and P are close in total variation distance which is a central step in the analysis of the OSRB. For the source model secret key agreement problem, substituting $X_1 = X_2 \leftarrow U_0$, and $X_3 = X_4 \leftarrow V_0$, in [12, Theorem 1] implies that $W_{[1:2]}$ is nearly independent of $F_{[1:2]}$ and Z^n, if

$$R_1 + \tilde{R}_1 < \mathbb{H}(U_0|Z), \tag{156}$$
$$R_2 + \tilde{R}_2 < \mathbb{H}(V_0|Z), \tag{157}$$
$$R_1 + \tilde{R}_1 + R_2 + \tilde{R}_2 < \mathbb{H}(U_0, V_0|Z). \tag{158}$$

Note that [12, Theorem 1] returns a total of 15 inequalities, but the remaining are redundant because of (156)–(158). The above constraints imply that

$$P(z^n, w_{[1:2]}, f_{[1:2]}) \approx_\epsilon p(z^n)p^U(w_{[1:2]})p^U(f_{[1:2]}).$$

Similarly, substituting $X_1 \leftarrow (U_0, U_1)$, $X_2 \leftarrow (U_0, U_2)$, $X_3 \leftarrow (V_0, V_1)$, $X_4 \leftarrow (V_0, V_2)$, and $Z \leftarrow (U_0, V_0, Z)$ in [12, Theorem 1] implies that $(f'_{[1:2]}, f''_{[1:2]})$ are nearly mutually independent and independent of (U_0, V_0, Z), therefore they are independent of $(w_{[1:2]}, f_{[1:2]})$, if

$$\tilde{R}'_j < \mathbb{H}(U_j|U_0, V_0, Z), \tag{159}$$
$$\tilde{R}''_j < \mathbb{H}(V_j|U_0, V_0, Z), \tag{160}$$
$$\tilde{R}'_1 + \tilde{R}''_j < \mathbb{H}(U_1, V_j|U_0, V_0, Z), \tag{161}$$
$$\tilde{R}'_2 + \tilde{R}''_j < \mathbb{H}(U_2, V_j|U_0, V_0, Z), \tag{162}$$
$$\tilde{R}'_1 + \tilde{R}'_2 < \mathbb{H}(U_1, U_2|U_0, V_0, Z), \tag{163}$$
$$\tilde{R}''_1 + \tilde{R}''_2 < \mathbb{H}(V_1, V_2|U_0, V_0, Z), \tag{164}$$
$$\tilde{R}'_1 + \tilde{R}'_2 + \tilde{R}''_j < \mathbb{H}(U_1, U_2, V_j|U_0, V_0, Z), \tag{165}$$
$$\tilde{R}'_j + \tilde{R}''_1 + \tilde{R}''_2 < \mathbb{H}(U_j, V_1, V_2|U_0, V_0, Z), \tag{166}$$
$$\tilde{R}'_1 + \tilde{R}'_2 + \tilde{R}''_1 + \tilde{R}''_2 < \mathbb{H}(U_1, U_2, V_1, V_2|U_0, V_0, Z), \tag{167}$$

for $j = 1, 2$. The above constraints imply

$$P(z^n, u_0^n, v_0^n, f'_{[1:2]}, f''_{[1:2]}) \approx_\epsilon p(z^n, u_0^n, v_0^n)p^U(f'_{[1:2]})p^U(f''_{[1:2]}). \tag{168}$$

Hence,

$$\begin{aligned}P(w_{[1:2]}, f_{[1:2]}) &\approx_\epsilon \hat{P}(w_{[1:2]}, f_{[1:2]})\\&= p^U(w_{[1:2]})p^U(f_{[1:2]}),\end{aligned} \tag{169}$$
$$\begin{aligned}P(f'_{[1:2]}, f''_{[1:2]}|u_0^n, v_0^n) &\approx_\epsilon \hat{P}(f'_{[1:2]}, f''_{[1:2]}|u_0^n, v_0^n)\\&= p^U(f'_{[1:2]})p^U(f''_{[1:2]}).\end{aligned} \tag{170}$$

In other words, the inequalities (156)–(158) and (159)–(167) imply that

$$\begin{aligned}&P(z^n, w_{[1:2]}, f_{[1:2]}, f'_{[1:2]}, f''_{[1:2]})\\&\quad\approx_\epsilon p(z^n)p^U(w_{[1:2]})p^U(f_{[1:2]})p^U(f'_{[1:2]})p^U(f''_{[1:2]}).\end{aligned} \tag{171}$$

Here, the PMF $P(z^n)$ is equal to $p(z^n)$ because the marginal distribution does not include random binning.

Therefore, the distributions in (154) and (155) are nearly equal, that is

$$P(u_{[0:2]}^n, v_{[0:2]}^n, y_1^n, y_2^n, z^n, w_{[1:2]}, \mathbf{f}, \hat{\mathbf{u}}) \approx_\epsilon \hat{P}(u_{[0:2]}^n, v_{[0:2]}^n, y_1^n, y_2^n, z^n, w_{[1:2]}, \mathbf{f}, \hat{\mathbf{u}}). \quad (172)$$

Similar to indirect decoding for channel coding it is possible to use indirect decoding for source coding. More precisely, the first and the second decoders only need (u_0^n, v_0^n) to decode (w_1, w_2). Decoder 1 and Decoder 2 can indirectly decode (u_0^n, v_0^n) from $(y_1^n, f_{[1:2]}, f_1', f_1'')$ and $(y_2^n, f_{[1:2]}, f_2', f_2'')$, respectively. From [12, Lemma 1] decoding is successful if

$$\tilde{R}_1 + \tilde{R}_j' > \mathbb{H}(U_0, U_j|V_0, V_j, Y_j), \quad (173)$$
$$\tilde{R}_2 + \tilde{R}_j'' > \mathbb{H}(V_0, V_j|U_0, U_j, Y_j), \quad (174)$$
$$\tilde{R}_1 + \tilde{R}_j' + \tilde{R}_j'' > \mathbb{H}(U_0, U_j, V_j|V_0, Y_j), \quad (175)$$
$$\tilde{R}_1 + \tilde{R}_2 + \tilde{R}_j'' > \mathbb{H}(V_0, V_j|U_0, U_j, Y_j), \quad (176)$$
$$\tilde{R}_j' + \tilde{R}_2 + \tilde{R}_j'' > \mathbb{H}(U_j, V_0, V_j|U_0, Y_j), \quad (177)$$
$$\tilde{R}_1 + \tilde{R}_j' + \tilde{R}_2 + \tilde{R}_j'' > \mathbb{H}(U_0, U_j, V_0, V_j|Y_j), \quad (178)$$

for $j = 1, 2$. Note that, inequality (176) is redundant because of (174). It yields

$$P(u_{[0:2]}^n, v_{[0:2]}^n, y_1^n, y_2^n, z^n, w_{[1:2]}, \mathbf{f}, \hat{\mathbf{u}}) \approx_\epsilon P(u_{[0:2]}^n, v_{[0:2]}^n, y_1^n, y_2^n, z^n, w_{[1:2]}, \mathbf{f}) \times \mathbb{1}_{\left\{\hat{u}_0^n=\check{u}_0^n=u_0^n, \hat{u}_1^n=u_1^n, \check{u}_2^n=u_2^n\right\}} \times \mathbb{1}_{\left\{\hat{v}_0^n=\check{v}_0^n=v_0^n, \hat{v}_1^n=v_1^n, \check{v}_2^n=v_2^n\right\}}. \quad (179)$$

From equations (172), (179), and the triangle inequality,

$$\hat{P}(u_{[0:2]}^n, v_{[0:2]}^n, y_1^n, y_2^n, z^n, w_{[1:2]}, \mathbf{f}, \hat{\mathbf{u}}) \approx_\epsilon P(u_{[0:2]}^n, v_{[0:2]}^n, y_1^n, y_2^n, z^n, w_{[1:2]}, \mathbf{f}) \times \mathbb{1}_{\left\{\hat{u}_0^n=\check{u}_0^n=u_0^n, \hat{u}_1^n=u_1^n, \check{u}_2^n=u_2^n\right\}} \times \mathbb{1}_{\left\{\hat{v}_0^n=\check{v}_0^n=v_0^n, \hat{v}_1^n=v_1^n, \check{v}_2^n=v_2^n\right\}}. \quad (180)$$

For convenience, we reintroduce a lemma from [12]:

Lemma 2: ([12, Lemma 4]) Consider distributions p_{X^n}, $p_{Y^n|X^n}$, q_{X^n}, and $q_{Y^n|X^n}$ and random PMFs P_{X^n}, $P_{Y^n|X^n}$, Q_{X^n}, and $Q_{Y^n|X^n}$. Denoting asymptotic equality under total variation with $\approx_\epsilon$, we have:

1)

$$P_{X^n} \approx_\epsilon Q_{X^n} \Rightarrow P_{X^n}P_{Y^n|X^n} \approx_\epsilon Q_{X^n}P_{Y^n|X^n}, \quad (181)$$
$$P_{X^n}P_{Y^n|X^n} \approx_\epsilon Q_{X^n}Q_{Y^n|X^n} \Rightarrow P_{X^n} \approx_\epsilon Q_{X^n}. \quad (182)$$

2) If $p_{X^n}p_{Y^n|X^n} \approx_\epsilon q_{X^n}q_{Y^n|X^n}$, then there exists a sequence $x^n \in \mathcal{X}^n$ such that

$$p_{Y^n|X^n=x^n} \approx_\epsilon q_{Y^n|X^n=x^n}. \quad (183)$$

3) If $P_{X^n} \approx_\epsilon Q_{X^n}$ and $P_{X^n}P_{Y^n|X^n} \approx_\epsilon P_{X^n}Q_{Y^n|X^n}$, then

$$P_{X^n}P_{Y^n|X^n} \approx_\epsilon Q_{X^n}Q_{Y^n|X^n}. \quad (184)$$

Using Lemma 2, Equation (182), the marginal distributions of the two sides of (180) are asymptotically equivalent, i.e.,

$$\hat{P}(u_{[0:2]}^n, v_{[0:2]}^n, z^n, w_{[1:2]}, \mathbf{f}, \hat{\mathbf{u}}) \approx_\epsilon P(u_{[0:2]}^n, v_{[0:2]}^n, z^n, w_{[1:2]}, \mathbf{f}) \times \mathbb{1}_{\left\{\hat{u}_0^n=\check{u}_0^n=u_0^n, \hat{u}_1^n=u_1^n, \check{u}_2^n=u_2^n\right\}} \mathbb{1}_{\left\{\hat{v}_0^n=\check{v}_0^n=v_0^n, \hat{v}_1^n=v_1^n, \check{v}_2^n=v_2^n\right\}}. \quad (185)$$

Using Lemma 2, Equation (181) we multiply the two sides of Equation (185) by the conditional distribution:

$$\hat{P}(\hat{w}_1, \check{w}_1, \hat{w}_2, \check{w}_2|u_{[0:2]}^n, v_{[0:2]}^n, z^n, w_{[1:2]}, \mathbf{f}, \hat{\mathbf{u}}) = \mathbb{1}_{\left\{W_1(\hat{u}_0^n)=\hat{w}_1, W_1(\check{u}_0^n)=\check{w}_1\right\}} \times \mathbb{1}_{\left\{W_2(\hat{v}_0^n)=\hat{w}_2, W_2(\check{v}_0^n)=\check{w}_2\right\}},$$

to get:

$$\begin{aligned}\hat{P}(u_{[0:2]}^n, v_{[0:2]}^n, z^n, w_{[1:2]}, \mathbf{f}, \hat{\mathbf{u}}, \hat{w}_1, \check{w}_1, \hat{w}_2, \check{w}_2) &\approx_\epsilon P(u_{[0:2]}^n, v_{[0:2]}^n, z^n, w_{[1:2]}, \mathbf{f}) \\ &\quad \times \mathbb{1}_{\left\{\hat{u}_0^n=\check{u}_0^n=u_0^n, \hat{u}_1^n=u_1^n, \check{u}_2^n=u_2^n\right\}} \times \mathbb{1}_{\left\{\hat{v}_0^n=\check{v}_0^n=v_0^n, \hat{v}_1^n=v_1^n, \check{v}_2^n=v_2^n\right\}} \\ &\quad \times \mathbb{1}_{\left\{W_1(\hat{u}_0^n)=\hat{w}_1, W_1(\check{u}_0^n)=\check{w}_1\right\}} \times \mathbb{1}_{\left\{W_2(\hat{v}_0^n)=\hat{w}_2, W_2(\check{v}_0^n)=\check{w}_2\right\}} \\ &= P(u_{[0:2]}^n, v_{[0:2]}^n, z^n, w_{[1:2]}, \mathbf{f}) \times \mathbb{1}_{\left\{\hat{u}_0^n=\check{u}_0^n=u_0^n, \hat{u}_1^n=u_1^n, \check{u}_2^n=u_2^n\right\}} \\ &\quad \times \mathbb{1}_{\left\{\hat{v}_0^n=\check{v}_0^n=v_0^n, \hat{v}_1^n=v_1^n, \check{v}_2^n=v_2^n\right\}} \times \mathbb{1}_{\left\{\hat{w}_1=\check{w}_1=w_1, \hat{w}_2=\check{w}_2=w_2\right\}},\end{aligned} \quad (186)$$

where $W_1(u_0^n) = \hat{w}_1$ and $W_2(v_0^n) = \hat{w}_2$ denote the bins assigned to u_0^n and v_0^n, respectively. Using (186) and Lemma 2, Equation (181) leads to

$$\hat{P}(z^n, w_{[1:2]}, \mathbf{f}, \hat{w}_1, \check{w}_1, \hat{w}_2, \check{w}_2) \approx_\epsilon P(z^n, w_{[1:2]}, \mathbf{f}) \times \mathbb{1}_{\left\{\hat{w}_1=\check{w}_1=w_1, \hat{w}_2=\check{w}_2=w_2\right\}}. \quad (187)$$

Using equations (171) and (187) and Lemma 2, Equation (184) leads to

$$\hat{P}(z^n, w_{[1:2]}, \mathbf{f}, \hat{w}_1, \check{w}_1, \hat{w}_2, \check{w}_2) \approx_\epsilon p(z^n)p^U(w_{[1:2]}, f_{[1:2]}) \times p^U(f_{[1:2]}', f_{[1:2]}'') \times \mathbb{1}_{\left\{\hat{w}_1=\check{w}_1=w_1, \hat{w}_2=\check{w}_2=w_2\right\}}. \quad (188)$$

We now eliminate the shared randomness $(F_{[1:2]}, F_{[1:2]}', F_{[1:2]}'')$ without affecting the secrecy and reliability requirements which is a key step in the analysis of OSRB. By using Definition 3, Equation (188) ensures that there exists a fixed binning with corresponding PMF p that, if used in place of the random coding strategy P in (155), will induce the PMF $\hat{p}$ as follows:

$$\hat{p}(z^n, w_{[1:2]}, f_{[1:2]}, f_{[1:2]}', f_{[1:2]}'', \hat{w}_1, \check{w}_1, \hat{w}_2, \check{w}_2) \approx_\epsilon p(z^n)p^U(w_{[1:2]}, f_{[1:2]})p^U(f_{[1:2]}', f_{[1:2]}'') \times \mathbb{1}_{\left\{\hat{w}_1=\check{w}_1=w_1, \hat{w}_2=\check{w}_2=w_2\right\}}. \quad (189)$$

Now, using Lemma 2, Equation (183) shows that there exists an instance of $(f_{[1:2]}, f_{[1:2]}', f_{[1:2]}'')$ such that:

$$\hat{p}(z^n, w_{[1:2]}, \hat{w}_1, \check{w}_1, \hat{w}_2, \check{w}_2|f_{[1:2]}, f_{[1:2]}', f_{[1:2]}'') \approx_\epsilon p(z^n)p^U(w_1)p^U(w_2)\mathbb{1}_{\left\{\hat{w}_1=\check{w}_1=w_1, \hat{w}_2=\check{w}_2=w_2\right\}}. \quad (190)$$

This distribution satisfies the secrecy and reliability requirements as follows:

- Reliability: Using Lemma 2, Equation (182) leads to

$$\hat{p}(w_{[1:2]}, \hat{w}_{1,1}, \hat{w}_{1,2}, \hat{w}_{2,1}, \hat{w}_{2,2}|f_{[1:2]}, f_{[1:2]}', f_{[1:2]}'') \approx_\epsilon \mathbb{1}_{\left\{\hat{w}_1=\check{w}_1=w_1, \hat{w}_2=\check{w}_2=w_2\right\}}, \quad (191)$$

which is equivalent to:

$$\hat{p}\Big(\{(\hat{W}_1, \hat{W}_2) \neq (W_1, W_2)\} \cup \{(\check{W}_1, \check{W}_2) \neq (W_1, W_2)\} \Big| f_{[1:2]}, f_{[1:2]}', f_{[1:2]}''\Big) \to 0.$$

- Security: Again, using Lemma 2, Equation (182)

$$\hat{p}(z^n, w_{[1:2]}|f_{[1:2]}, f'_{[1:2]}, f''_{[1:2]}) \approx_\epsilon p(z^n)p^U(w_1)p^U(w_2).$$

Finally, we identify $p(x_1^n|w_1, f_1, f'_{[1:2]})$ and $p(x_2^n|w_2, f_2, f''_{[1:2]})$ (which is done by generating $u_{[0:2]}$ and $v_{[0:2]}$ first, respectively) as encoders and the Slepian-Wolf decoders as decoders for the channel coding problem. These encoders and decoders lead to reliable and secure encoders and decoders.

By applying a computer generated Fourier-Motzkin procedure [36] to (156)–(167), (173), (174), and (178) the achievable rate region for the strong secrecy regime in Theorem 6 is obtained.

Remark 7: The random distributions $P(u_0^n, v_0^n|w_{[1:2]}, f_{[1:2]})$ *and* $P(u_{[1:2]}^n, v_{[1:2]}^n|u_0^n, v_0^n, f'_{[1:2]}, f''_{[1:2]})$ *factorize as* $P(u_0^n|w_1, f_1)P(v_0^n|w_2, f_2)$ *and* $P(u_{[1:2]}^n|u_0^n, f'_{[1:2]})P(v_{[1:2]}^n|v_0^n, f''_{[1:2]})$*, respectively, which means that Encoders* 1 *and* 2 *are not using the common randomness and the message available at the other encoder to generate the common and private random variables. The common randomness* $(F_1, F'_{[1:2]})$ *represents the realization of Encoder 1's codebook and* $(F_2, F''_{[1:2]})$ *represents the realization of Encoder 2's codebook, which is available at all terminals, but the codebook at one encoder does not depend on the codebook of the other encoder.*

Remark 8: The achievable region described in the proof of Theorem 6 was without time sharing, i.e., $Q = \emptyset$*. One can incorporate this into the proof by generating i.i.d. copies of Q, and sharing it among all terminals and conditioning everything on it.*

References

[1] X. Song, H. Li, M. Yuan, and Y. Huang, "Coverage performance analysis of wireless caching networks with non-orthogonal multiple access-based multicasting," *IEEE Access*, vol. 7, pp. 164009–164020, Nov. 2019.

[2] Z. Zhao, M. Xu, Y. Li, and M. Peng, "A non-orthogonal multiple access-based multicast scheme in wireless content caching networks," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 12, pp. 2723–2735, Dec. 2017.

[3] O. Tervo, L.-N. Tran, H. Pennanen, S. Chatzinotas, B. Ottersten, and M. Juntti, "Energy-efficient multicell multigroup multicasting with joint beamforming and antenna selection," *IEEE Trans. Signal Process.*, vol. 66, no. 18, pp. 4904–4919, Sep. 2018.

[4] A. Cohen, A. Cohen, M. Medard, and O. Gurewitz, "Secure multi-source multicast," *IEEE Trans. Commun.*, vol. 67, no. 1, pp. 708–723, Jan. 2019.

[5] D. Blackwell, L. Breiman, and A. J. Thomasian, "The capacities of certain channel classes under random coding," *Ann. Math. Statist.*, vol. 31, no. 3, pp. 558–567, Sep. 1960.

[6] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz), "Compound wiretap channels," in *Proc. 45th Annu. Allerton Conf. Commun., Control, Comput.*, Monticello, IL, USA, Sep. 2007, pp. 136–143.

[7] R. Ahlswede, "The capacity region of a channel with two senders and two receivers," *Ann. Probab.*, vol. 2, no. 5, pp. 805–814, Oct. 1974.

[8] S. Verdu, "Fifty years of Shannon theory," *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 2057–2078, Oct. 1998.

[9] T. Han and K. Kobayashi, "A new achievable rate region for the interference channel," *IEEE Trans. Inf. Theory*, vol. IT-27, no. 1, pp. 49–60, Jan. 1981.

[10] Y. K. Chia and A. El Gamal, "Three-receiver broadcast channel with common and confidential messages," *IEEE Trans. Inf. Theory*, vol. 58, no. 9, pp. 2748–2765, May 2012.

[11] C. Nair and A. El Gamal, "The capacity region of a class of three-receiver broadcast channels with degraded message sets," *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 4479–4493, Oct. 2009.

[12] M. H. Yassaee, M. R. Aref, and A. Gohari, "Achievability proof via output statistics of random binning," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6760–6786, Nov. 2014.

[13] J. M. Renes and R. Renner, "Noisy channel coding via privacy amplification and information reconciliation," *IEEE Trans. Inf. Theory*, vol. 57, no. 11, pp. 7377–7385, Nov. 2011.

[14] I. Csiszár, "Almost independence and secrecy capacity," *IEEE Trans. Inf. Theory*, vol. 32, no. 1, pp. 40–47, Jan. 1996.

[15] S. Watanabe and Y. Oohama, "The optimal use of rate-limited randomness in broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 61, no. 2, pp. 983–995, Feb. 2015.

[16] H. ZivariFard, M. R. Bloch, and A. Nosratinia, "Two-transmitter two-receiver channel with confidential messages," in *Proc. 55th Annu. Allerton Conf. Commun., Control, Comput.*, Monticello, IL, USA, Sep. 2017, pp. 103–110.

[17] S. Salehkalaibar, M. Mirmohseni, and M. R. Aref, "One-receiver two-eavesdropper broadcast channel with degraded message sets," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 1961–1974, Dec. 2013.

[18] E. Ekrem and S. Ulukus, "Multi-receiver wiretap channel with public and confidential messages," *IEEE Trans. Inf. Theory*, vol. 59, no. 4, pp. 2165–2177, Apr. 2013.

[19] M. Benammar and P. Piantanida, "Secrecy capacity region of some classes of wiretap broadcast channels," *IEEE Trans. Inf. Theory*, vol. 61, no. 10, pp. 5564–5582, Oct. 2015.

[20] L. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 3, no. 3, pp. 976–1002, Mar. 2008.

[21] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5747–5755, Dec. 2008.

[22] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[23] M. H. Yassaee and M. R. Aref, "Multiple access wiretap channels with strong secrecy," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Dublin, Ireland, Sep. 2010, pp. 1–5.

[24] M. Wiese and H. Boche, "Strong secrecy for multiple access channels," in *Information Theory, Combinatorics, and Search Theory*. Cham, Switzerland: Springer, 2013, pp. 71–122.

[25] A. J. Pierrot and M. R. Bloch, "Strongly secure communications over the two-way wiretap channel," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 595–605, Sep. 2011.

[26] H. Zivari-Fard, B. Akhbari, M. Ahmadian-Attari, and M. R. Aref, "Imperfect and perfect secrecy in compound multiple access channel with confidential message," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1239–1251, Jun. 2016.

[27] R. A. Chou and A. Yener, "Polar coding for the multiple access wiretap channel via rate-splitting and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 64, no. 12, pp. 7903–7921, Dec. 2018.

[28] A. Carleial, "Multiple-access channels with different generalized feedback signals," *IEEE Trans. Inf. Theory*, vol. IT-28, no. 6, pp. 841–850, Nov. 1982.

[29] R. Liu, I. Marić, P. Spasojević, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.

[30] P. Cuff, "Distributed channel synthesis," *IEEE Trans. Inf. Theory*, vol. 59, no. 11, pp. 7071–7096, Nov. 2013.

[31] M. R. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, 1st ed. Cambridge, U.K: Cambridge Univ. Press, 2011.

[32] Y. Liang, H. V. Poor, and S. Shamai (Shitz), *Information Theoretic Security*, 1st ed. Hanover, MA, USA: Now, 2009.

[33] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[34] A. El Gamal and Y.-H. Kim, *Network Information Theory*, 1st ed. Cambridge, U.K: Cambridge Univ. Press, 2012.

[35] H. ZivariFard, M. Bloch, and A. Nosratinia, "Two-multicast channel with confidential messages," 2019, *arXiv:1902.08657*. [Online]. Available: http://arxiv.org/abs/1902.08657

[36] I. B. Gattegno, Z. Goldfeld, and H. H. Permuter. (2016). *Fourier-Motzkin Elimination Software for Information Theoretic Inequalities*. [Online]. Available: http://www.ee.bgu.ac.il/~fmeit/

[37] F. S. Chaharsooghi, M. J. Emadi, M. Zamanighomi, and M. R. Aref, "A new method for variable elimination in systems of inequations," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, St. Petersburg, Russia, Jul. 2011, pp. 1215–1219.

[38] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 57, no. 8, pp. 1355–1367, Oct. 1975.

[39] A. El Gamal and E. C. van der Meulen, "A proof of Marton's coding theorem for the discrete memoryless broadcast channel," *IEEE Trans. Inf. Theory*, vol. IT-27, no. 1, pp. 120–122, Jan. 1981.

[40] G. Kramer, "Capacity results for the discrete memoryless network," *IEEE Trans. Inf. Theory*, vol. 49, no. 1, pp. 4–21, Jan. 2003.