RESOLVABILITY AND STRONG SECRECY FOR THE MULTIPLE ACCESS CHANNEL WITH COOPERATION

by

Noha Helal

APPROVED BY SUPERVISORY COMMITTEE:

Aria Nosratinia, Chair

Matthieu Bloch

Yiorgos Makris

Naofal Al-Dhahir

Hlaing Minn

To my family and friends.

RESOLVABILITY AND STRONG SECRECY FOR THE MULTIPLE ACCESS CHANNEL WITH COOPERATION

by

NOHA HELAL, BS, MS

DISSERTATION

Presented to the Faculty of

The University of Texas at Dallas

in Partial Fulfillment

of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY IN

ELECTRICAL ENGINEERING

THE UNIVERSITY OF TEXAS AT DALLAS

May 2020

ACKNOWLEDGMENTS

This dissertation would not have been possible without the advice, encouragement and support of my advisor, Prof. Aria Nosratinia. He has not only been my academic advisor, but also a mentor. I am grateful to Prof. Matthieu Bloch for the fun and fruitful collaborations. I appreciate the valuable remarks of my PhD committee members, Prof. Yiorgos Makris, Prof. Naofal Al-Dhahir and Prof. Hlaing Minn. I acknowledge Prof. Karim Seddik for his constant encouragement, and my deepest gratitude to Prof. Ahmed Sultan, who made me recognize my interest in pursuing a PhD during my junior year in college.

I owe everything to the unconditional love and support of my family. Thanks to the best mother, Azza Fouad and to my super dad, Mohamed Helal. Thanks to my lovely sister, Heba Helal. Their care and support has sustained me in difficult times throughout my life.

I am grateful to my dear friends for their support and encouragement: Hala Badr, Menna Nogomi, Nahla Soheim, Shrouk Mokhtar, Ahmed Shama, Khaled Gad, Moustafa Soheim, Moustafa Elsherif, Ahmed Helmy and Christine Ghattas. I am lucky for knowing them. I appreciate the friendly environment I had in my lab with my colleagues, particularly, Ahmed Hindy and Hussein Saad, who were not only colleagues but supporting friends. I appreciate Hassan Zivari-Fard for all the useful discussions.

Saving the best for last, I express my gratitude to my husband Mohamed Awadin, without whose support I could not have completed this journey. He endured my ups and downs with me, always a shoulder to lean on.

Finally, and most importantly, thanks to Allah for all His blessings throughout my life. It is in His remembrance that hearts find rest.

March 2020

RESOLVABILITY AND STRONG SECRECY FOR THE MULTIPLE ACCESS CHANNEL WITH COOPERATION

Noha Helal, PhD
The University of Texas at Dallas, 2020

Supervising Professor: Aria Nosratinia, Chair

We study secret communication over the discrete memoryless multiple-access channel with the following cooperation strategies: (i) degraded message sets, (ii) a common message, (iii) conferencing, (iv) cribbing, (v) feedback, and (vi) generalized feedback. For developing strong secrecy results, we utilize the methods and techniques of channel resolvability, which involves the characterization of the amount of randomness required at the inputs of the channel to approximately produce a chosen i.i.d. output distribution.

For the multiple-access with degraded message sets, a common message, conferencing and feedback, we exactly characterize the channel resolvability region. For the multiple access channel with cribbing, we exactly characterize the channel resolvability region for the causal cribbing and non-causal cribbing scenarios. For the strictly-causal cribbing scenario, inner and outer bounds are provided. For the multiple-access channel with generalized feedback, we provide two inner bounds representing the role of decoding and randomness extraction, which can also be combined.

Finally, leveraging the resolvability results, we derive achievable strong secrecy rate regions for each of the cooperation scenarios.

TABLE OF CONTENTS

ACKNOWLEDGMENTS v

ABSTRACT vi

LIST OF FIGURES ix

CHAPTER 1 INTRODUCTION 1

1.1 Notation 3

1.2 MAC with non-Cooperating Encoders 4

CHAPTER 2 MAC WITH DEGRADED MESSAGE SETS, MAC WITH COMMON MESSAGE AND MAC WITH CONFERENCING 7

2.1 MAC with Degraded Message Sets 7

2.2 MAC with Common Message 10

2.3 MAC with Conferencing 11

2.4 Strong Secrecy from Channel Resolvability 13

2.5 Proofs 16

2.5.1 Channel resolvability of MAC with degraded message sets 16

2.5.2 Strong secrecy of MAC with degraded message sets 22

2.5.3 Channel resolvability of MAC with common message 24

2.5.4 Strong secrecy of MAC with common message 31

2.5.5 Channel resolvability of MAC with conferencing 33

2.5.6 Strong secrecy of MAC with conferencing 36

2.5.7 Convexity proof of channel resolvability of MAC with degraded message sets 39

2.5.8 Convexity proof of channel resolvability of MAC with common message 40

CHAPTER 3 MAC WITH CRIBBING 42

3.1 MAC with One-Sided Cribbing 42

3.1.1 MAC with one-sided strictly-causal cribbing 44

3.1.2 MAC with one-sided causal cribbing 44

3.1.3 MAC with one-sided non-causal cribbing 45

3.2 MAC with Two-Sided Cribbing 46

3.2.1 MAC with two-sided strictly-causal cribbing 46

3.3 Strong Secrecy from Channel Resolvability 48

3.4 Proofs 51

3.4.1 Channel resolvability of MAC with one-sided strictly-causal cribbing . 51

3.4.2 Strong secrecy of MAC with one-sided strictly-causal cribbing 60

3.4.3 Channel resolvability of MAC with one-sided causal cribbing 70

3.4.4 Strong secrecy of MAC with one-sided causal cribbing 73

3.4.5 Channel resolvability of MAC with one-sided non-causal cribbing . . 74

3.4.6 Strong secrecy of MAC with one-sided non-causal cribbing 82

3.4.7 Channel resolvability of MAC with two-sided strictly-causal cribbing 84

3.4.8 Strong secrecy of MAC with two-sided strictly-causal cribbing 98

3.4.9 Convexity proof of channel resolvability of MAC with one-sided strictly-causal cribbing 108

3.4.10 Convexity proof of channel resolvability of MAC with one-sided causal/non-causal cribbing 110

3.4.11 Proof of Equations (3.24)-(3.27) 111

CHAPTER 4 MAC WITH FEEDBACK AND MAC WITH GENERALIZED FEEDBACK 115

4.1 MAC with Feedback 115

4.2 MAC with Generalized Feedback 117

4.3 Strong Secrecy from Channel Resolvability 120

4.4 Proofs 124

4.4.1 Channel resolvability of MAC with feedback 124

4.4.2 Strong secrecy of MAC with feedback 127

4.4.3 Channel resolvability of MAC with generalized feedback 137

CHAPTER 5 CONCLUSION 150

REFERENCES 151

BIOGRAPHICAL SKETCH 154

CURRICULUM VITAE

LIST OF FIGURES

1.1 The multiple access channel. 4

1.2 The multiple access wiretap channel. 5

2.1 The multiple access channel with degraded message sets. 7

2.2 The multiple access channel with a common message. 10

2.3 The multiple access channel with conferencing. 11

2.4 The multiple access wiretap channel with degraded message sets. 13

2.5 The multiple access wiretap channel with a common message. 13

2.6 The multiple access wiretap channel with conferencing. 14

3.1 The multiple access channel with one-sided strictly-causal cribbing. 42

3.2 The multiple access channel with one-sided causal cribbing. 43

3.3 The multiple access wiretap channel with one-sided non-causal cribbing. 43

3.4 The multiple access channel with two-sided strictly-causal cribbing. 46

3.5 The multiple access wiretap channel with one-sided strictly-causal cribbing. . . . 48

3.6 The multiple access wiretap channel with one-sided causal cribbing. 48

3.7 The multiple access wiretap channel with one-sided non-causal cribbing. 48

3.8 The multiple access wiretap channel with two-sided strictly-causal cribbing. . . . 49

3.9 Wiretap channel embedded in MAC with strictly-causal cribbing. 53

3.10 Functional dependence graph for the block-Markov encoding scheme for MAC with one-sided strictly-causal cribbing. 64

3.11 MAC induced by Shannon strategy. 70

3.12 State-dependent point-to-point channel. 73

3.13 Functional dependence graph for the block-Markov encoding scheme for MAC with two-sided strictly-causal cribbing. 101

4.1 The multiple access channel with feedback. 115

4.2 The multiple access channel with generalized feedback. 117

4.3 The multiple access wiretap channel with feedback. 120

4.4 The multiple access wiretap channel with generalized feedback. 120

CHAPTER 1

INTRODUCTION

The field of physical layer security dates back to Wyner's wiretap channel [1]. The modern approach to physical layer security involves strong secrecy, and increasingly leverages tools and techniques from channel resolvability.

Channel resolvability is defined as producing an approximation of a desired statistic at a channel output via application of minimal randomness at its input. The origins of this problem can be traced back to Wyner's work [2] on the characterization of common randomness among two dependent random variables, in which he used a normalized KL divergence as a measure of approximation. The problem was subsequently formalized and generalized for total variation using information-spectrum methods [3]. Subsequent works have simplified proofs, both for total variation [4] and Kullback-Leibler (KL) divergence [5], and studied multi-user settings, such as multiple-access channel (MAC) with non-cooperative encoders [6, 7, 8, 9].

In this work we study the role of user cooperation in enhancing channel resolvability. One-sided and two-sided cooperation scenarios are considered. In the category of noiseless cooperation, in which one or both users have access to the other user's message or transmitted signal noiselessly, we investigate MAC with degraded message sets, MAC with a common message, MAC with conferencing and MAC with cribbing. In the category of cooperation in the presence of noisy communication, we investigate MAC with feedback and MAC with generalized feedback.

For MAC with degraded message sets, MAC with a common message and MAC with conferencing, we exactly characterize the channel resolvability via tight inner and outer bounds. For MAC with cribbing, we analyze resolvability rates under (i) strictly-causal cribbing, (ii) causal cribbing and (iii) non-causal cribbing. For scenarios (ii)-(iii), we exactly characterize the channel resolvability region. For (i), we provide inner and outer bounds for the channel resolvability region; the crux of our achievability result is to handle the strict causality constraint with a block-Markov coding scheme in which dependencies across blocks are suitably hidden.

For MAC with feedback, one of the highlights of this work is a converse that shows feedback does not improve the resolvability of MAC. Since this converse is tight against the results of [7], no new achievable rate is needed for MAC with feedback. This result is significant because it is known that MAC *capacity* can be improved by feedback [10, 11], thus MAC capacity and resolvability react differently to feedback. For MAC with generalized feedback, we give two achievable resolvability regions representing the roles of decoding and randomness extraction, which can also be combined. The essence of the achievability proofs is carefully applying block-Markov encoding to handle the strict causality imposed by the channel feedback; randomness is appropriately recycled to break the dependence across blocks created by the encoding scheme. Furthermore, we harness the randomness that stems from the channel noise independent of the channel input [12] via a random binning argument to introduce fresh randomness at the encoders and assist in the approximation of the output distribution.

Finally, strong secrecy [13, 14] achievable rates are obtained. We develop a wiretap coding scheme that achieves strong secrecy, fueled by the resolvability results. For the cases of strictly-causal cribbing, feedback and generalized feedback, a contribution of this work is a new superposition coding strategy that uses all components of the cooperation signal to achieve efficient decoding at the legitimate receiver, while at the same time forcing a part of the randomness within the cooperation signal to remain non-cooperative *from the viewpoint of the eavesdropper.* This feature is needed for randomness recycling and is crucial to avoid secrecy rate loss.

Strong secrecy for MAC with *non-cooperating* encoders has been studied in [7, 8, 9]. To the best of our knowledge, strong secrecy in multi-terminal settings under cooperating encoders has not been comprehensively studied. For completeness we highlight examples of the investigation of *weak* secrecy under cooperation: MAC with cooperating or partially cooperating encoders [15, 16, 17, 18], interference channel with cooperating encoders [19, 20, 21], relay channel with an external eavesdropper [22, 23] and broadcast channel with cooperating receivers [24]. These works follow the classical approach of Wyner [1] and Csiszár [25] to develop weak secrecy results. To the best of our understanding there has been limited work on any type of cooperative strong secrecy; notable examples are Goldfeld *et al.* [26] on *receive side* cooperation in the broadcast channel, Watanabe and Oohama [27] on the cognitive interference channel with confidential messages, and Chou and Yener [28] on Polar coding for MAC wiretap channel with cooperative jamming.

1.1 Notation

Random variables are represented by upper case letters and their realizations by the corresponding lower case letters, e.g., x is a realization of the random variable X. Superscripts denote the length of a sequence of symbols and subscripts denote the position of a symbol in a sequence. Calligraphic letters represent sets, the cardinality of which is denoted by $|\cdot|$. For example, $X^n = \{X_1, \ldots, X_n\}$ where X_i belongs to the alphabet $\mathcal{X}$ of size $|\mathcal{X}|$. P_X and P_{XY} denote probability distributions on $\mathcal{X}$ and $\mathcal{X} \times \mathcal{Y}$, respectively. We sometimes omit the subscripts in probability distributions if they are clear from the context, i.e., we write $P(x)$ instead of $P_X(x)$.

For two distributions P and Q on the same alphabet, the KL divergence is defined by $\mathbb{D}(P||Q) \triangleq \sum_x P(x) \log \frac{P(x)}{Q(x)}$ and the total variational distance is defined by $\mathbb{V}(P, Q) \triangleq \sum_x |P(x) - Q(x)|$. Throughout the dissertation, log denotes the base 2 logarithm. For an i.i.d. vector whose components are distributed according to P_X, the product distribution is denoted by $P_X^{\otimes n}(x^n) \triangleq \prod_{i=1}^n P_X(x_i)$. The set of ϵ-strongly-typical sequences of length n with respect to P_X is defined as:

$$\mathcal{T}_\epsilon^n(P_X) \triangleq \left\{x^n : \left|\frac{N(a|x^n)}{n} - P_X(a)\right| \leq \epsilon P_X(a), \forall a \in \mathcal{X}\right\}.$$

For a set of random variables $\{X_i\}_{i\in\mathcal{M}}$ indexed over a countable set $\mathcal{M}$, $\mathbb{E}_{\setminus m}(\cdot)$ denotes the expectation over all random variables with indices in $\mathcal{M}$ except that with index m. $\mathbb{E}_X(\cdot)$ is the expectation w.r.t. the random variable X and $\mathbb{1}_{\{.\}}$ is the indicator function. $[x]^+ = \max\{0, x\}$.

1.2 MAC with non-Cooperating Encoders

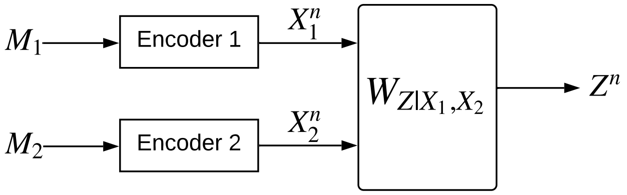

Figure 1.1. The multiple access channel.

We first recall the known MAC resolvability region with non-cooperating encoders [6, 7], which will serve as a reference to assess the benefits of cooperation. The discrete memoryless MAC consists of finite input alphabets $\mathcal{X}_1$ and $\mathcal{X}_2$, and finite output alphabet Z with a channel transition probability $W_{Z|X_1,X_2}$, see Figure 1.1. For a distribution $P_{X_1}P_{X_2}$ on $\mathcal{X}_1 \times \mathcal{X}_2$, the output is distributed according to $Q_Z(z) = \sum_{x_1,x_2} P_{X_1}P_{X_2}(x_1, x_2)W_{Z|X_1,X_2}(z|x_1, x_2)$. A $(2^{nR_1}, 2^{nR_2}, n)$ channel resolvability code consists of two encoders f_1 and f_2 with $M_1 \in [\![1, 2^{nR_1}]\!]$ and $M_2 \in [\![1, 2^{nR_2}]\!]$. The encoding functions are defined as follows:

$$f_1 : \mathcal{M}_1 \to \mathcal{X}_1^n, \tag{1.1}$$

$$f_2 : \mathcal{M}_1 \to \mathcal{X}_2^n. \tag{1.2}$$

Definition 1. *A rate pair (R_1, R_2) is said to be achievable for the discrete memoryless MAC $(\mathcal{X}_1 \times \mathcal{X}_2, W_{Z|X_1,X_2}, \mathcal{Z})$ if for a given*[1] *Q_Z there exists a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes with increasing block length such that $\lim_{n\to\infty} \mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) = 0$. The MAC resolvability region is the closure of the set of achievable rate tuples (R_1, R_2).*

Theorem 1. *[7] The resolvability region for MAC with non-cooperating encoders is the set of rate pairs (R_1, R_2) such that*

$$R_1 \geq I(X_1; Z|V), \tag{1.3}$$

$$R_2 \geq I(X_2; Z|V), \tag{1.4}$$

$$R_1 + R_2 \geq I(X_1, X_2; Z|V), \tag{1.5}$$

for some joint distribution $P_{VX_1X_2Z} \triangleq P_V P_{X_1|V} P_{X_2|V} W_{Z|X_1X_2}$ with marginal Q_Z.

While the resolvability region in [7] was established w.r.t. total variation, it can be shown to also hold w.r.t. KL divergence.

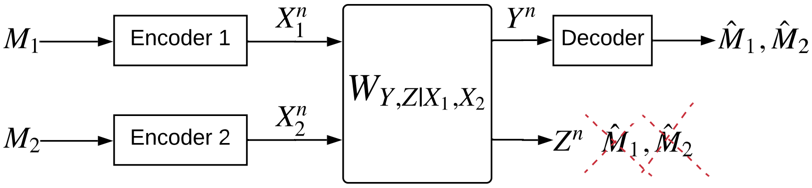

Figure 1.2. The multiple access wiretap channel.

In [8], a strong secrecy achievable region for MAC with non-cooperating encoders was provided. The multiple-access wiretap channel (Figure 1.2) consists of two encoders f_1 and f_2 and a decoder g. The encoders are defined similar to definitions presented in (1.1) and (1.2),

[1] Originally in [3] the resolvability rate was defined as "the number of random bits required per channel use in order to generate an input that achieves arbitrarily accurate approximation of the output statistics *for any given input process*." More recent works consider a fixed but arbitrary Q_Z, leaving out the implied intersection of rate regions over different Q_Z. This is more convenient in several ways, including in the application of resolvability to secrecy problems where only the simulation of a certain Q_Z is of interest.

but the functions f_1 and f_2 are now stochastic and not deterministic. The decoding function at the legitimate receiver is defined as:

$$g : \mathcal{Y}^n \rightarrow \hat{\mathcal{M}}_1 \times \hat{\mathcal{M}}_2. \tag{1.6}$$

The probability of error at the legitimate receiver is defined as $P_e^{(n)} = \mathbb{P}\Big((\hat{M}_1, \hat{M}_2) \neq (M_1, M_2)\Big)$. The strong secrecy metric adopted in this dissertation is the total amount of leaked confidential information per codeword, defined as $L^{(n)} = I(M_1, M_2; Z^n)$.

Definition 2. *A strong secrecy rate pair (R_1, R_2) is said to be achievable for the discrete memoryless wiretap MAC if there exists a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes such that $P_e^{(n)}$ and $L^{(n)}$ vanish as $n \rightarrow \infty$.*

Proposition 1. *[8] For the multiple-access wiretap channel with non-cooperating encoders, the following strong-secrecy rate region is achievable:*

$$(R_1, R_2) = \bigcup_{P_{X_1} P_{X_2} W_{Y,Z|X_1,X_2}} \mathcal{R}_{\text{no-co}}^{(\text{in})},$$

$$\mathcal{R}_{\text{no-co}}^{(\text{in})} = \left\{ \begin{array}{l} R_1, R_2 \geq 0 \\ R_1 \leq I(X_1; Y|X_2) - I(X_1; Z) \\ R_2 \leq I(X_2; Y|X_1) - I(X_2; Z) \\ R_1 + R_2 \leq I(X_1, X_2; Y) - I(X_1, X_2; Z) \end{array} \right\}. \tag{1.7}$$

CHAPTER 2

MAC WITH DEGRADED MESSAGE SETS, MAC WITH COMMON MESSAGE AND MAC WITH CONFERENCING [1] [2] [3]

In this chapter we present the discrete memoryless MAC with three noiseless cooperation models: MAC with degraded message sets, MAC with common message and MAC with conferencing. MAC with degraded message sets is the case where one encoder knows a priori the message of the other encoder. In MAC with a common message, each encoder possesses an individual message in addition to a message shared between both encoders. In MAC with conferencing, both encoders cooperate over communication links with finite capacities.

For each of these MAC models, we exactly characterize the channel resolvability region. We then provide inner bounds for the strong secrecy regions building on the results of channel resolvability.

2.1 MAC with Degraded Message Sets

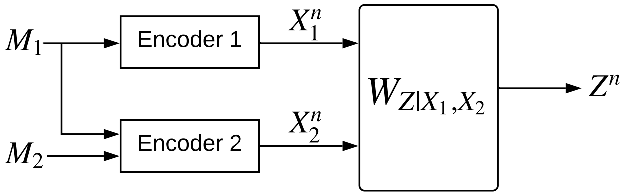

Figure 2.1. The multiple access channel with degraded message sets.

[1] © N. Helal and M. Bloch and A. Nosratinia, "Multiple-Access Channel Resolvability with Cribbing," 2018 IEEE International Symposium on Information Theory (ISIT), pp. 2052-2056, 2018.

[2] © N. Helal and M. Bloch and A. Nosratinia, "Cooperative Resolvability and Secrecy in the Cribbing Multiple Access Channel," in IEEE Transactions on Information Theory.

[3] © N. Helal and M. Bloch and A. Nosratinia, "Resolvability of the Multiple Access Channel with Two-Sided Cooperation," 2020 IEEE International Symposium on Information Theory (ISIT).

The discrete memoryless MAC with degraded message sets (Figure 2.1) consists of finite input alphabets $\mathcal{X}_1$ and $\mathcal{X}_2$, and finite output alphabet Z with a channel transition probability $W_{Z|X_1,X_2}$. For a joint distribution P_{X_1,X_2} on $\mathcal{X}_1 \times \mathcal{X}_2$, the output is distributed according to $Q_Z(z) = \sum_{x_1,x_2} P_{X_1,X_2}(x_1,x_2)W_{Z|X_1,X_2}(z|x_1,x_2)$. A $(2^{nR_1}, 2^{nR_2}, n)$ channel resolvability code consists of two encoders f_1 and f_2 with $M_1 \in [\![1, 2^{nR_1}]\!]$ and $M_2 \in [\![1, 2^{nR_2}]\!]$. The encoding functions are defined as follows:

$$f_1 : \mathcal{M}_1 \to \mathcal{X}_1^n \qquad f_2 : \mathcal{M}_1 \times \mathcal{M}_2 \to \mathcal{X}_2^n. \tag{2.1}$$

Definition 3. *A rate pair (R_1, R_2) is said to be achievable for the discrete memoryless MAC with degraded message sets $(\mathcal{X}_1 \times \mathcal{X}_2, W_{Z|X_1,X_2}, \mathcal{Z})$ if for a given Q_Z there exists a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes with increasing block length such that $\lim_{n\to\infty} \mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) = 0$. The MAC resolvability region is the closure of the set of achievable rate pairs (R_1, R_2).*

Note that one could define achievability by requiring instead that $\lim_{n\to\infty} \mathbb{V}(P_{Z^n}, Q_Z^{\otimes n}) = 0$. For two distributions P and Q on a finite alphabet $\mathcal{A}$, Pinsker's inequality ensures that

$$\mathbb{V}(P,Q) \leq \sqrt{\frac{1}{2\ln 2}\mathbb{D}(P||Q)}.$$

Consequently, if rate is achievable in terms of KL divergence, it is achievable in terms of total variational distance. One of the best reverse Pinsker inequality is proved in [29, Eq. (323)] and recalled in the following lemma.

Lemma 1. *Let P and Q be two probability distributions on a finite alphabet $\mathcal{A}$ such that P is absolutely continuous w.r.t. Q. If $\mu \triangleq \min_{a\in\mathcal{Q}:Q(a)>0} Q(a)$, we have*

$$\mathbb{D}(P||Q) \leq \log\left(\frac{1}{\mu}\right)\mathbb{V}(P,Q).$$

Specialized to our setting, this means that $\mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) \leq n \log \frac{1}{\mu}\mathbb{V}(P_{Z^n}, Q_Z^{\otimes n})$ with $\mu = \min_{z:Q_Z(z)>0} Q_Z(z)$. Therefore, only if the total variation decays fast enough as $o(1/n)$

can we conclude that the KL divergence vanishes. More generally, this suggests that the channel resolvability region under a total variation constraint could be larger than that under a KL divergence constraint. In achievability proofs of channel resolvability over discrete memoryless channel, one can usually show that total variation decays exponentially with n so that an achievable rate in terms of total variational distance is also achievable in terms of KL divergence. Similarly, in converse proofs for channel resolvability over memoryless channel, one usually obtains the same bounds irrespective of which metric is used. Unfortunately, these are not general results and whether the channel resolvability regions under total variation or KL divergence are the same must be systematically checked.

Theorem 2. *The resolvability region for MAC with degraded message sets is the set of rate pairs* (R_1, R_2) *such that*

$$R_1 \geq I(X_1; Z), \tag{2.2}$$

$$R_1 + R_2 \geq I(X_1, X_2; Z), \tag{2.3}$$

for some joint distribution $P_{X_1X_2Z} \triangleq P_{X_1X_2}W_{Z|X_1X_2}$ *with marginal* Q_Z*.*

Proof. See Section 2.5.1. □

The absence of the individual rate constraint R_2 is a direct consequence of the degraded message model that allows Encoder 2 to benefit from the randomness provided via R_1, reducing the *required* individual rate constraint for User 2 to $R_2 \geq 0$, which is omitted. Another difference between the regions described by Theorem 1 and Theorem 2 is that the former includes a convexifying auxiliary random variable that is missing in the latter. The region described by Theorem 2 is already convex due to the larger set of available input distributions, as proved in Section 2.5.7.

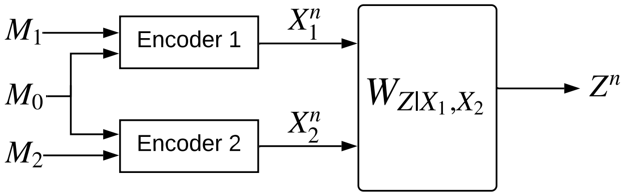

Figure 2.2. The multiple access channel with a common message.

2.2 MAC with Common Message

The discrete memoryless MAC with common message (Figure 2.2) consists of finite input alphabets $\mathcal{X}_1$ and $\mathcal{X}_2$, and finite output alphabet Z with a channel transition probability $W_{Z|X_1,X_2}$. For a joint distribution P_{X_1,X_2} on $\mathcal{X}_1 \times \mathcal{X}_2$, the output is distributed according to $Q_Z(z) = \sum_{x_1,x_2} P_{X_1,X_2}(x_1,x_2) W_{Z|X_1,X_2}(z|x_1,x_2)$. A $(2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n)$ channel resolvability code consists of two encoders f_1 and f_2 with inputs $M_0 \in [\![1, 2^{nR_0}]\!]$, $M_1 \in [\![1, 2^{nR_1}]\!]$ and $M_2 \in [\![1, 2^{nR_2}]\!]$. The encoding functions are defined as follows:

$$f_1 : \mathcal{M}_0 \times \mathcal{M}_1 \to \mathcal{X}_1^n \qquad f_2 : \mathcal{M}_0 \times \mathcal{M}_2 \to \mathcal{X}_2^n. \tag{2.4}$$

Definition 4. *A rate tuple (R_0, R_1, R_2) is said to be achievable for the discrete memoryless MAC with common message $(\mathcal{X}_1 \times \mathcal{X}_2, W_{Z|X_1,X_2}, \mathcal{Z})$ if for a given Q_Z there exists a sequence of $(2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n)$ codes with increasing block length such that $\lim_{n\to\infty} \mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) = 0$. The MAC resolvability region is the closure of the set of achievable rate tuples (R_0, R_1, R_2).*

Theorem 3. *The resolvability region for the discrete-memoryless MAC with common message is the set of rate tuples (R_0, R_1, R_2) such that*

$$R_0 \geq I(U;Z) \tag{2.5}$$

$$R_0 + R_1 \geq I(U, X_1; Z) \tag{2.6}$$

$$R_0 + R_2 \geq I(U, X_2; Z) \tag{2.7}$$

$$R_0 + R_1 + R_2 \geq I(X_1, X_2; Z) \tag{2.8}$$

for some joint distribution $P_{U,X_1,X_2,Z} \triangleq P_U P_{X_1|U} P_{X_2|U} W_{Z|X_1,X_2}$ *with marginal* Q_Z.

Proof. See Section 2.5.3. □

The region described by Theorem 3 is convex as proved in Section 2.5.8.

Remark 1. *The resolvability of MAC with non-cooperating encoders [7] can be retrieved from Theorem 3 by setting* $R_0 = 0$.

Remark 2. *The resolvability of MAC with degraded message sets [30, 31] can be retrieved from Theorem 3 by setting* $R_1 = 0$, $R_0 = R_1$ *and* $U = X_1$.

2.3 MAC with Conferencing

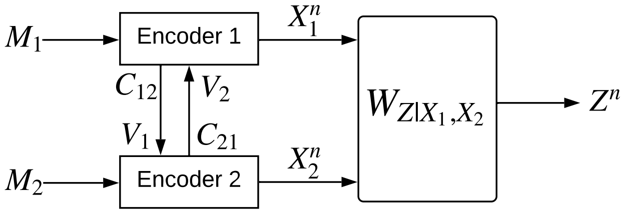

Figure 2.3. The multiple access channel with conferencing.

The discrete memoryless MAC with conferencing (Figure 2.3) consists of finite input alphabets $\mathcal{X}_1$ and $\mathcal{X}_2$, and finite output alphabet Z with a channel transition probability $W_{Z|X_1,X_2}$. For a joint distribution P_{X_1,X_2} on $\mathcal{X}_1 \times \mathcal{X}_2$, the output is distributed according to $Q_Z(z) = \sum_{x_1,x_2} P_{X_1,X_2}(x_1,x_2) W_{Z|X_1,X_2}(z|x_1,x_2)$. A conference between the encoders consists of K subsequent pairs of communications defined by the communicating functions g_1 and g_2. A $(2^{nR_1}, 2^{nR_2}, n)$ channel resolvability code consists of two encoders f_1 and f_2 with inputs $M_1 \in [\![1, 2^{nR_1}]\!]$ and $M_2 \in [\![1, 2^{nR_2}]\!]$. The encoding functions are defined as follows:

$$g_{1k} : \mathcal{M}_1 \times \mathcal{V}_2^{k-1} \to \mathcal{V}_{1k}, \text{ for } k \in [\![1, K]\!], \tag{2.9}$$

$$g_{2k} : \mathcal{M}_2 \times \mathcal{V}_1^{k-1} \to \mathcal{V}_{2k}, \text{ for } k \in \llbracket 1, K \rrbracket, \tag{2.10}$$

$$f_1 : \mathcal{M}_1 \times \mathcal{V}_2^K \to \mathcal{X}_1^n, \tag{2.11}$$

$$f_2 : \mathcal{M}_2 \times \mathcal{V}_1^K \to \mathcal{X}_2^n. \tag{2.12}$$

The amount of information exchanged during conferencing is bounded by capacities, C_{12} and C_{21}, of the communication links between the encoders. C_{12} is the capacity of the link used by Encoder 1 to communicate to Encoder 2 and C_{21} is the capacity of the other link such that

$$\sum_{k=1}^{K} \log |\mathcal{V}_{1k}| \leq nC_{12} \tag{2.13}$$

$$\sum_{k=1}^{K} \log |\mathcal{V}_{2k}| \leq nC_{21} \tag{2.14}$$

Definition 5. *A rate pair (R_1, R_2) is said to be achievable for the discrete memoryless MAC with conferencing $(\mathcal{X}_1 \times \mathcal{X}_2, W_{Z|X_1,X_2}, \mathcal{Z})$ if for a given Q_Z there exists a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes with increasing block length such that $\lim_{n\to\infty} \mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) = 0$. The MAC resolvability region is the closure of the set of achievable rate pairs (R_1, R_2).*

Theorem 4. *The resolvability region for the discrete-memoryless MAC with conferencing is the set of rate pairs (R_1, R_2) such that*

$$C_{12} + C_{21} \geq I(U; Z) \tag{2.15}$$

$$R_1 \geq I(U, X_1; Z) - C_{21} \tag{2.16}$$

$$R_2 \geq I(U, X_2; Z) - C_{12} \tag{2.17}$$

$$R_1 + R_2 \geq I(X_1, X_2; Z) \tag{2.18}$$

for some joint distribution $P_{U,X_1,X_2,Z} \triangleq P_U P_{X_1|U} P_{X_2|U} W_{Z|X_1,X_2}$ with marginal Q_Z.

Proof. See Section 2.5.5. □

Similar to MAC with common message, it can be proved that the region described by Theorem 4 is convex. The idea behind the achievability proof is converting this cooperation scheme into a setting that corresponds to a MAC with common message. The common message is constructed from the information exchanged during conferencing. We then provide a matching converse.

Remark 3. *The resolvability of MAC with non-cooperating encoders [7] can be retrieved from Theorem 3 by setting* $C_{12} = C_{21} = 0$.

2.4 Strong Secrecy from Channel Resolvability

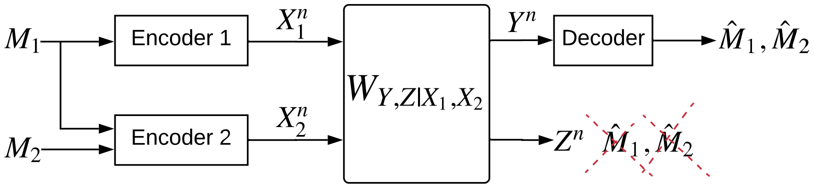

Figure 2.4. The multiple access wiretap channel with degraded message sets.

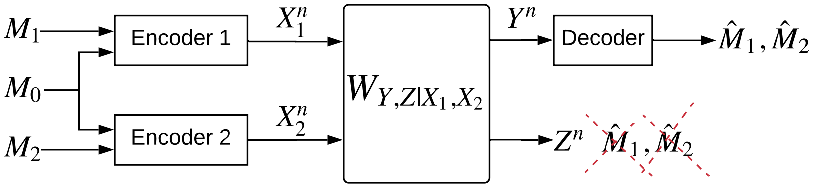

Figure 2.5. The multiple access wiretap channel with a common message.

In this section we use the resolvability results to study the multiple-access wiretap channel with degraded message sets, the multiple-access wiretap channel with a common message and the multiple-access wiretap channel with conferencing (Figures 2.4, 2.5 and 2.6 respectively). For each of these cooperation models, an achievable strong secrecy rate region is presented.

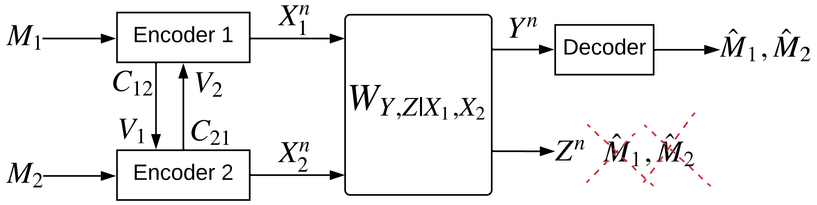

Figure 2.6. The multiple access wiretap channel with conferencing.

The multiple-access wiretap channel consists of two encoders f_1 and f_2 and a decoder g. The encoders of each model are defined similar to definitions presented earlier in this chapter, but the functions f_1 and f_2 are now stochastic and not deterministic. The decoding function at the legitimate receiver is defined as:

$$g : \mathcal{Y}^n \to \hat{\mathcal{M}}_1 \times \hat{\mathcal{M}}_2. \tag{2.19}$$

For MAC with common message,

$$g : \mathcal{Y}^n \to \hat{\mathcal{M}}_0 \times \hat{\mathcal{M}}_1 \times \hat{\mathcal{M}}_2, \tag{2.20}$$

in which case a second decoder is defined at the wiretapper:

$$g : \mathcal{Z}^n \to \hat{\hat{\mathcal{M}}}_0. \tag{2.21}$$

The probability of error at the legitimate receiver is defined as $P_e^{(n)} = \mathbb{P}\Big((\hat{M}_1, \hat{M}_2) \neq (M_1, M_2)\Big)$ or $P_e^{(n)} = \mathbb{P}\Big((\hat{M}_0, \hat{M}_1, \hat{M}_2) \neq (M_0, M_1, M_2)$ or $\hat{\hat{M}}_0 \neq M_0\Big)$ for MAC with common message. As mentioned in the introduction, the strong secrecy metric is defined as the total amount of leaked confidential information per codeword, $L^{(n)} = I(M_1, M_2; Z^n)$.

Definition 6. *A strong secrecy rate pair* (R_1, R_2) *(or rate tuple* (R_0, R_1, R_2)*) is said to be achievable for the discrete memoryless wiretap MAC if there exists a sequence of* $(2^{nR_1}, 2^{nR_2}, n)$ *(or* $(2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n)$*) codes such that* $P_e^{(n)}$ *and* $L^{(n)}$ *vanish as* $n \to \infty$*.*

Proposition 2. *For the multiple-access wiretap channel with degraded message sets, the following strong-secrecy rate region is achievable:*

$$(R_1, R_2) = \bigcup_{P_{X_1,X_2} W_{Y,Z|X_1,X_2}} \mathcal{R}_{\text{DM}}^{(\text{in})},$$

$$\mathcal{R}_{\text{DM}}^{(\text{in})} = \left\{ \begin{array}{l} R_1, R_2 \geq 0 \\ R_2 \leq I(X_2; Y|X_1) \\ R_1 + R_2 \leq I(X_1, X_2; Y) - I(X_1, X_2; Z) \end{array} \right\}. \tag{2.22}$$

Proof. See Section 2.5.2. □

Proposition 3. *For the multiple-access wiretap channel with common message, the following strong-secrecy rate region is achievable:*

$$(R_0, R_1, R_2) = \bigcup_{P_U P_{X_1|U} P_{X_2|U} W_{Y,Z|X_1,X_2}} \mathcal{R}_{\text{CM}}^{(\text{in})},$$

$$\mathcal{R}_{\text{CM}}^{(\text{in})} = \left\{ \begin{array}{l} R_1, R_2 \geq 0 \\ R_0 \leq I(U; Z) \\ R_1 \leq I(X_1; Y|X_2, U) - I(X_1; Z|U) \\ R_2 \leq I(X_2; Y|X_1, U) - I(X_2; Z|U) \\ R_1 + R_2 \leq I(X_1, X_2; Y|U) - I(X_1, X_2; Z|U) \\ R_0 + R_1 + R_2 \leq I(X_1, X_2; Y) - I(X_1, X_2; Z|U) \end{array} \right\}. \tag{2.23}$$

Proof. See Section 2.5.4. □

Remark 4. *The achievable strong secrecy rate region of the multiple-access wiretap channel with non-cooperating encoders can be obtained from Proposition 3 by setting $R_0 = 0$.*

Proposition 4. *For the multiple-access wiretap channel with conferencing, the following strong-secrecy rate region is achievable:*

$$(R_1, R_2) = \bigcup_{P_U P_{X_1|U} P_{X_2|U} W_{Y,Z|X_1,X_2}} \mathcal{R}_{\text{C}}^{(\text{in})},$$

$$\mathcal{R}_{\mathrm{C}}^{(\mathrm{in})} = \left\{ \begin{array}{l} R_1, R_2 \geq 0, C_{12} + C_{21} \geq I(U;Z) \\ R_1 \leq I(X_1;Y|X_2,U) - I(U,X_1;Z) + C_{12} + C_{21} \\ R_2 \leq I(X_2;Y|X_1,U) - I(U,X_2;Z) + C_{21} + C_{12} \\ R_1 + R_2 \leq I(X_1,X_2;Y|U) - I(X_1,X_2;Z) + C_{12} + C_{21} \\ R_1 + R_2 \leq I(X_1,X_2;Y) - I(X_1,X_2;Z) \end{array} \right\}. \tag{2.24}$$

Proof. See Section 2.5.6. □

Remark 5. *The achievable strong secrecy rate region of the multiple-access wiretap channel with non-cooperating encoders can be obtained from Proposition 3 by setting* $C_{12} = C_{21} = 0$.

2.5 Proofs

2.5.1 Channel resolvability of MAC with degraded message sets

Achievability:

Codebook generation: Consider a distribution $P(x_1, x_2) = P(x_1)P(x_2|x_1)$ such that $\sum_{x_1,x_2} P(x_1, x_2)W(z|x_1, x_2) = Q_Z(z)$.

- Independently generate 2^{nR_1} codewords x_1^n each with probability $P(x_1^n) = P_{X_1}^{\otimes n}(x_1^n)$. Label them $x_1^n(m_1)$, $m_1 \in [\![1, 2^{nR_1}]\!]$.
- For every m_1, independently generate 2^{nR_2} codewords x_2^n each with probability $P(x_2^n|x_1^n(m_1)) = P_{X_2|X_1}^{\otimes n}(x_2^n|x_1^n(m_1))$. Label them $x_2^n(m_1, m_2)$, $m_2 \in [\![1, 2^{nR_2}]\!]$.

This defines the codebook

$$\mathcal{C}_n = \{x_1^n(m_1), x_2^n(m_1, m_2), m_1 \in [\![1, 2^{nR_1}]\!], m_2 \in [\![1, 2^{nR_2}]\!]\} \tag{2.25}$$

and we denote the random codebook by

$$\mathfrak{C}_n = \{X_1^n(m_1), X_2^n(m_1, m_2), m_1 \in [\![1, 2^{nR_1}]\!], m_2 \in [\![1, 2^{nR_2}]\!]\} \tag{2.26}$$

The average KL divergence is:

$$\mathbb{E}_{\mathfrak{C}_n}\big(\mathbb{D}(P_{Z^n}||Q_Z^{\otimes n})\big)$$

$$= \mathbb{E}_{\mathfrak{C}_n}\left(\sum_{z^n} P_{Z^n}(z^n)\log\frac{P_{Z^n}(z^n)}{Q_Z^{\otimes n}(z^n)}\right)$$

$$= \mathbb{E}_{\mathfrak{C}_n}\Bigg(\sum_{z^n}\frac{1}{2^{n(R_1+R_2)}}\sum_{m_1}\sum_{m_2} W^{\otimes n}(z^n|X_1^n(m_1),X_2^n(m_1,m_2)) \log\frac{\sum_{m_1'}\sum_{m_2'}W^{\otimes n}(z^n|X_1^n(m_1'),X_2^n(m_1',m_2'))}{2^{n(R_1+R_2)}Q_Z^{\otimes n}(z^n)}\Bigg)$$

$$=\sum_{x_1^n(1)}\sum_{x_2^n(1,1)}\cdots\sum_{x_1^n(2^{nR_1})}\sum_{x_2^n(2^{nR_1},2^{nR_2})}\prod_{(K_1,K_2)=(1,1)}^{(2^{nR_1},2^{nR_2})}P(x_1^n(k_1),x_2^n(k_1,k_2)) \sum_{z^n}\frac{1}{2^{n(R_1+R_2)}}\sum_{m_1}\sum_{m_2}W^{\otimes n}(z^n|x_1^n(m_1),x_2^n(m_1,m_2)) \log\frac{\sum_{m_1'}\sum_{m_2'}W^{\otimes n}(z^n|x_1^n(m_1'),x_2^n(m_1',m_2'))}{2^{n(R_1+R_2)}Q_Z^{\otimes n}(z^n)}$$

$$=\sum_{z^n}\frac{1}{2^{n(R_1+R_2)}}\sum_{m_1}\sum_{m_2}\sum_{x_1^n(m_1)}\sum_{x_2^n(m_1,m_2)}P(x_1^n(m_1),x_2^n(m_1,m_2))W^{\otimes n}(z^n|x_1^n(m_1),x_2^n(m_1,m_2)) \sum_{(k_1,k_2)\neq(m_1,m_2)}^{(2^{nR_1},2^{nR_2})}\sum_{x_1^n(k_1)}\sum_{x_2^n(k_1,k_2)}\prod_{(l_1,l_2)\neq(m_1,m_2)}^{(2^{nR_1},2^{nR_2})}P(x_1^n(l_1),x_2^n(l_1,l_2)) \log\frac{\sum_{m_1'}\sum_{m_2'}W^{\otimes n}(z^n|x_1^n(m_1'),x_2^n(m_1',m_2'))}{2^{n(R_1+R_2)}Q_Z^{\otimes n}(z^n)}$$

$$=\sum_{z^n}\frac{1}{2^{n(R_1+R_2)}}\sum_{m_1}\sum_{m_2}\sum_{x_1^n(m_1)}\sum_{x_2^n(m_1,m_2)}P(x_1^n(m_1),x_2^n(m_1,m_2),z^n) \mathbb{E}_{\backslash(m_1,m_2)}\log\frac{\sum_{m_1'}\sum_{m_2'}W^{\otimes n}(z^n|X_1^n(m_1'),X_2^n(m_1',m_2'))}{2^{n(R_1+R_2)}Q_Z^{\otimes n}(z^n)}$$

$$\overset{(a)}{\leq}\frac{1}{2^{n(R_1+R_2)}}\sum_{m_1}\sum_{m_2}\sum_{z^n}\sum_{x_1^n(m_1)}\sum_{x_2^n(m_1,m_2)}P(x_1^n(m_1),x_2^n(m_1,m_2),z^n) \log\mathbb{E}_{\backslash(m_1,m_2)}\frac{\sum_{m_1'}\sum_{m_2'}W^{\otimes n}(z^n|X_1^n(m_1'),X_2^n(m_1',m_2'))}{2^{n(R_1+R_2)}Q_Z^{\otimes n}(z^n)}$$

$$=\frac{1}{2^{n(R_1+R_2)}}\sum_{m_1}\sum_{m_2}\sum_{z^n}\sum_{x_1^n(m_1)}\sum_{x_2^n(m_1,m_2)}P(x_1^n(m_1),x_2^n(m_1,m_2),z^n)$$

$$\log \mathbb{E}_{\backslash(m_1,m_2)}\Bigg(\frac{W^{\otimes n}(z^n|x_1^n(m_1),x_2^n(m_1,m_2))}{2^{n(R_1+R_2)}Q_Z^{\otimes n}(z^n)} \quad + \sum_{m_2'\neq m_2}\frac{W^{\otimes n}(z^n|x_1^n(m_1),X_2^n(m_1,m_2'))}{2^{n(R_1+R_2)}Q_Z^{\otimes n}(z^n)}$$

$$+\sum_{m_1'\neq m_1}\sum_{m_2'}\frac{W^{\otimes n}(z^n|X_1^n(m_1'),X_2^n(m_1',m_2'))}{2^{n(R_1+R_2)}Q_Z^{\otimes n}(z^n)}\Bigg)$$

$$\overset{(b)}{\leq}\frac{1}{2^{n(R_1+R_2)}}\sum_{m_1}\sum_{m_2}\sum_{z^n}\sum_{x_1^n(m_1)}\sum_{x_2^n(m_1,m_2)}P^{\otimes n}(x_1^n(m_1),x_2^n(m_1,m_2),z^n)$$

$$\log\left(\frac{W^{\otimes n}(z^n|x_1^n(m_1),x_2^n(m_1,m_2))}{2^{n(R_1+R_2)}Q_Z^{\otimes n}(z^n)}+\sum_{m_2'\neq m_2}\frac{P^{\otimes n}(z^n|x_1^n(m_1))}{2^{n(R_1+R_2)}Q_Z^{\otimes n}(z^n)}+1\right) \tag{2.27}$$

where

(a) follows by Jensen's inequality where $\mathbb{E}\log(\cdot)\leq\log\mathbb{E}(\cdot)$. Recall $\mathbb{E}_{\backslash(m_1,m_2)}(\cdot)$ is the expectation over $X_1^n(i)$ and $X_2^n(i,j)$ for $(i,j)\neq(m_1,m_2)$;

(b) follows by applying the expectation $\mathbb{E}_{\backslash(m_1,m_2)}$ to each term inside the bracket.

We finally write the right-hand side of (2.27) as $\Psi_1+\Psi_2$ with

$$\Psi_1 \triangleq \frac{1}{2^{n(R_1+R_2)}}\sum_{m_1}\sum_{m_2}\sum_{(x_1^n,x_2^n,z^n)\in\mathcal{T}_\epsilon^n(P_{X_1,X_2,Z})}P^{\otimes n}(x_1^n(m_1),x_2^n(m_1,m_2),z^n)$$

$$\log\left(\frac{W^{\otimes n}(z^n|x_1^n(m_1),x_2^n(m_1,m_2))}{2^{n(R_1+R_2)}Q_Z^{\otimes n}(z^n)}+\sum_{m_2'\neq m_2}\frac{P^{\otimes n}(z^n|x_1^n(m_1))}{2^{n(R_1+R_2)}Q_Z^{\otimes n}(z^n)}+1\right)$$

$$\leq\log\left(\frac{2^{-n(1-\epsilon)H(Z|X_1,X_2)}}{2^{n(R_1+R_2)}2^{-n(1+\epsilon)H(Z)}}+\frac{2^{nR_2}2^{-n(1-\epsilon)H(Z|X_1)}}{2^{n(R_1+R_2)}2^{-n(1+\epsilon)H(Z)}}+1\right)$$

$$\leq\log\left(2^{-n(R_1+R_2-I(X_1,X_2;Z)-2\epsilon H(Z))}+2^{-n(R_1-I(X_1;Z)-2\epsilon H(Z))}+1\right)$$

and

$$\Psi_2 \triangleq \frac{1}{2^{n(R_1+R_2)}}\sum_{m_1}\sum_{m_2}\sum_{(x_1^n,x_2^n,z^n)\notin\mathcal{T}_\epsilon^n(P_{X_1,X_2,Z})}P^{\otimes n}(x_1^n(m_1),x_2^n(m_1,m_2),z^n)$$

$$\log\left(\frac{W^{\otimes n}(z^n|x_1^n(m_1),x_2^n(m_1,m_2))}{2^{n(R_1+R_2)}Q_Z^{\otimes n}(z^n)}+\sum_{m_2'\neq m_2}\frac{P^{\otimes n}(z^n|x_1^n(m_1))}{2^{n(R_1+R_2)}Q_Z^{\otimes n}(z^n)}+1\right)$$

$$\leq 2|\mathcal{X}_1||\mathcal{X}_2||\mathcal{Z}|e^{-n\epsilon^2\mu_{X_1X_2Z}}n\log(\frac{2}{\mu_Z}+1)$$

where

$$\mu_Z = \min_{\substack{z \in \mathcal{Z} \\ \text{s.t. } Q(z)>0}} Q(z)$$

$$\mu_{X_1X_2Z} = \min_{\substack{(x_1,x_2,z)\in(\mathcal{X}_1,\mathcal{X}_2,\mathcal{Z}) \\ \text{s.t. } Q(x_1,x_2,z)>0}} Q(x_1,x_2,z)$$

Combining the bounds on Ψ_1 and Ψ_2, we obtain $\mathbb{E}_{\mathfrak{C}_n}(\mathbb{D}(P_{Z^n}||Q_Z^{\otimes n})) \to 0$ exponentially with n if $R_1 > I(X_1;Z)+2\epsilon H(Z)$ and $R_1+R_2 > I(X_1,X_2;Z)+2\epsilon H(Z)$. This implies, by Markov's inequality, that $\Pr(\mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) > \eta_n) \xrightarrow{n\to\infty} 0$ for a suitable choice of η_n; $\eta_n = e^{-n\alpha}$ for $\alpha > 0$.

Converse:

We consider a $(2^{nR_1}, 2^{nR_2}, n)$ code such that $\mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) \leq \epsilon$, where $\epsilon \xrightarrow{n\to\infty} 0$.

By assumption,

$$\begin{aligned}
\epsilon &\geq \mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) \\
&= \sum_{z^n} P(z^n) \log \frac{P(z^n)}{Q_Z^{\otimes n}(z^n)} \\
&= \sum_{i=1}^{n} \Big(\sum_{z_i} P_Z(z_i) \log \frac{1}{Q(z_i)} - H(Z_i|Z^{i-1}) \Big) \\
&\overset{(a)}{\geq} \sum_{i=1}^{n} \Big(\sum_{z_i} P(z_i) \log \frac{1}{Q(z_i)} - H(Z_i) \Big) \\
&= \sum_{i=1}^{n} \mathbb{D}(P_{Z_i}||Q_Z) \\
&\overset{(b)}{\geq} n\mathbb{D}(\tilde{P}_Z||Q_Z)
\end{aligned}$$

where (a) follows because conditioning does not increase entropy and (b) follows by Jensen's inequality and the convexity of $\mathbb{D}(\cdot||\cdot)$ with $\tilde{P}_Z(z) \triangleq \frac{1}{n}\sum_{i=1}^{n} P_{Z_i}(z)$. Note that

$$nR_1 = H(M_1) \tag{2.28}$$

$$
\begin{aligned}
&\geq I(M_1; Z^n)\\
&\overset{(a)}{=} I(M_1, X_1^n; Z^n)\\
&\geq I(X_1^n; Z^n)\\
&= I(X_1^n, X_2^n; Z^n) - I(X_2^n; Z^n|X_1^n)\\
&\overset{(b)}{\geq} \sum_{x_1^n}\sum_{x_2^n}\sum_{z^n} P(x_1^n, x_2^n, z^n) \log \frac{W^{\otimes n}(z^n|x_1^n, x_2^n)}{P_{Z^n}(z^n)} - \sum_i I(X_{2i}; Z_i|X_{1i})\\
&= \sum_{x_1^n}\sum_{x_2^n}\sum_{z^n} P(x_1^n, x_2^n, z^n) \log \frac{W^{\otimes n}(z^n|x_1^n, x_2^n)}{Q_Z^{\otimes n}(z^n)} - \mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) - \sum_i I(X_{2i}; Z_i|X_{1i})\\
&\geq \sum_{x_1^n}\sum_{x_2^n}\sum_{z^n} P(x_1^n, x_2^n, z^n) \log \frac{W^{\otimes n}(z^n|x_1^n, x_2^n)}{Q_Z^{\otimes n}(z^n)} - \sum_i I(X_{2i}; Z_i|X_{1i}) - \epsilon\\
&= \sum_i \sum_{x_{1i}}\sum_{x_{2i}}\sum_{z_i} P(x_{1i}, x_{2i}, z_i)\Bigg(\log \frac{W(z_i|x_{1i}, x_{2i})}{Q(z_i)} - \log \frac{W(z_i|x_{1i}, x_{2i})}{P(z_i|x_{1i})}\Bigg) - \epsilon\\
&= \sum_i \sum_{x_{1i}}\sum_{x_{2i}}\sum_{z_i} P(x_{1i}, x_{2i}, z_i) \log \frac{P(z_i|x_{1i})}{Q(z_i)} - \epsilon\\
&= \sum_i \sum_{x_{1i}}\sum_{z_i} P(x_{1i}, z_i) \log \frac{P(z_i|x_{1i})}{Q(z_i)} - \epsilon\\
&= \sum_i \mathbb{D}(P_{X_{1i}Z_i}||P_{X_{1i}}Q_{Z_i}) - \epsilon\\
&\overset{(c)}{\geq} n\mathbb{D}\Bigg(\frac{\sum_i P_{X_{1i}Z_i}}{n}\Bigg|\Bigg|\frac{\sum_i P_{X_{1i}}}{n}Q_Z\Bigg) - \epsilon\\
&\overset{(d)}{=} n\mathbb{D}(\tilde{P}_{X_1,Z}||\tilde{P}_{X_1}Q_Z) - \epsilon\\
&= n\sum_{x_1}\sum_z \tilde{P}_{X_1,Z}(x_1, z) \log \frac{\tilde{P}_{X_1,Z}(x_1, z)}{\tilde{P}_{X_1}(x_1)Q_Z(z)} - \epsilon\\
&= n\sum_{x_1}\sum_z \tilde{P}_{X_1,Z}(x_1, z) \log \frac{\tilde{P}_{X_1,Z}(x_1, z)}{\tilde{P}_{X_1}(x_1)\tilde{P}_Z(z)} + n\sum_{x_1}\sum_z \tilde{P}_{X_1,Z}(x_1, z) \log \frac{\tilde{P}_Z(z)}{Q_Z(z)} - \epsilon\\
&= nI(\tilde{X}_1; \tilde{Z}) + n\mathbb{D}(\tilde{P}_Z||Q_Z) - \epsilon\\
&\geq nI(\tilde{X}_1; \tilde{Z}) - \epsilon \qquad (2.29)
\end{aligned}
$$

where

(a) follows from the definition of the deterministic encoding functions in (2.1);

(b) follows because conditioning does not increase entropy and the channel is discrete memoryless, therefore $I(X_2^n; Z^n|X_1^n) = \sum H(Z_i|Z^{i-1}, X_1^n) - H(Z_i|Z^{i-1}, X_1^n, X_2^n) \leq \sum H(Z_i|X_{1i}) - H(Z_i|X_{1i}, X_{2i}) \leq \sum_{i=1}^n I(X_{2i}; Z_i|X_{1i})$;

(c) follows by Jensen's inequality and the convexity of $\mathbb{D}(\cdot||\cdot)$;

(d) follows by defining $\tilde{P}_{X_1,Z}(x_1, z) \triangleq \frac{1}{n}\sum_i P_{X_{1i},Z_i}(x_1, z)$ and $\tilde{P}_{X_1}(x_1) \triangleq \frac{1}{n}\sum_i P_{X_{1i}}(x_1)$ where $\tilde{P}_{X_1,X_2}(x_1, x_2) \triangleq \frac{1}{n}\sum_i P_{X_{1i},X_{2i}}(x_1, x_2)$, $\tilde{P}_{X_1,X_2,Z}(x_1, x_2, z) \triangleq \frac{1}{n}\sum_i P_{X_{1i},X_{2i},Z_i}(x_1, x_2, z) = W_{Z|X_1,X_2}(z|x_1, x_2)\tilde{P}_{X_1,X_2}(x_1, x_2)$ and $\tilde{P}_{X_1,Z}(x_1, z) = \sum_{x_2} \tilde{P}_{X_1,X_2,Z}(x_1, x_2, z)$.

Next, observe that

$$\begin{aligned}
&n(R_1 + R_2) \\
&\quad = H(M_1, M_2) && (2.30) \\
&\quad \geq I(M_1, M_2; Z^n) \\
&\quad \geq I(X_1^n, X_2^n; Z^n) + \mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) - \epsilon \\
&\quad = \sum_{x_1^n}\sum_{x_2^n}\sum_{z^n} P(x_1^n, x_2^n, z^n) \log \frac{P(x_1^n, x_2^n, z^n)}{P(x_1^n, x_2^n)P_{Z^n}(z^n)} + \sum_{z^n} P(z^n) \log \frac{P_{Z^n}(z^n)}{Q_Z^{\otimes n}(z^n)} - \epsilon \\
&\quad = \sum_{x_1^n}\sum_{x_2^n}\sum_{z^n} P(x_1^n, x_2^n, z^n) \log \frac{W^{\otimes n}(z^n|x_1^n, x_2^n)}{Q_Z^{\otimes n}(z^n)} - \epsilon \\
&\quad = \sum_{i}\sum_{x_{1i}}\sum_{x_{2i}}\sum_{z_i} P(x_{1i}, x_{2i}, z_i) \log \frac{W(z_i|x_{1i}, x_{2i})}{Q(z_i)} - \epsilon \\
&\quad = \sum_{i} \mathbb{D}(P_{X_{1i},X_{2i},Z_i}||P_{X_{1i},X_{2i}}Q_{Z_i}) - \epsilon \\
&\quad \overset{(a)}{\geq} n\mathbb{D}\left(\frac{\sum_i P_{X_{1i},X_{2i},Z_i}}{n}\middle|\middle|\frac{\sum_i P_{X_{1i},X_{2i}}}{n}Q_Z\right) - \epsilon \\
&\quad \overset{(b)}{=} n\mathbb{D}(\tilde{P}_{X_1,X_2,Z}||\tilde{P}_{X_1,X_2}Q_Z) - \epsilon \\
&\quad = n\mathbb{D}(\tilde{P}_{X_1,X_2,Z}||\tilde{P}_{X_1,X_2}\tilde{P}_Z) + n\mathbb{D}(\tilde{P}_Z||Q_Z) - \epsilon \\
&\quad \geq nI(\tilde{X}_1, \tilde{X}_2; \tilde{Z}) - \epsilon && (2.31)
\end{aligned}$$

where

(a) follows by Jensen's inequality and the convexity of $\mathbb{D}(\cdot||\cdot)$;

(b) follows by defining $\tilde{P}_{X_1,X_2,Z}(x_1,x_2,z) \triangleq \frac{1}{n}\sum_i P_{X_{1i},X_{2i},Z_i}(x_1,x_2,z)$ and $\tilde{P}_{X_1,X_2}(x_1,x_2) \triangleq \frac{1}{n}\sum_i P_{X_{1i},X_{2i}}(x_1,x_2)$ with $\tilde{P}_{X_1,X_2,Z}(x_1,x_2,z) = W_{Z|X_1,X_2}(z|x_1,x_2)\tilde{P}_{X_1,X_2}(x_1,x_2,z)$.

The final step of this converse proof, and other converse proofs in this dissertation, is to show the continuity of the resolvability region at $\epsilon \to 0$. For a proof of this statement, we refer the reader to [4, Section VI.C], which can be extended to a MAC.

2.5.2 Strong secrecy of MAC with degraded message sets

Achievability:

Consider a distribution $P(x_1,x_2) = P(x_1)P(x_2|x_1)$ such that $\sum_{x_1,x_2} P(x_1,x_2)W(z|x_1,x_2) = Q_Z(z)$.

Code Construction:

- Independently generate $2^{n(R_1+R_1')}$ codewords x_1^n each with probability $P(X_1^n) = P_{X_1}^{\otimes n}(x_1^n)$. Label them $x_1^n(m_1,m_1')$, $m_1 \in [\![1,2^{nR_1}]\!]$ and $m_1' \in [\![1,2^{nR_1'}]\!]$.

- For every $x_1^n(m_1,m_1')$, independently generate $2^{n(R_2+R_2')}$ codewords x_2^n each with probability $P(x_2^n|x_1^n(m_1,m_1')) = P_{X_2|X_1}^{\otimes n}(x_2^n|x_1^n(m_1,m_1'))$. Label them $x_2^n(m_1,m_1',m_2,m_2')$, $m_2 \in [\![1,2^{nR_2}]\!]$ and $m_2' \in [\![1,2^{nR_2'}]\!]$.

Encoding: To send m_1, Encoder 1 transmits $x_1^n(m_1,m_1')$. To send m_2, Encoder 2 cooperatively sends $x_2^n(m_1,m_1',m_2,m_2')$. m_1' and m_2' are independently chosen at random from $[\![1,2^{nR_1'}]\!]$ and $[\![1,2^{nR_2'}]\!]$ respectively.

Decoding: The decoder finds (m_1,m_1',m_2,m_2') such that

$$(x_1^n(m_1,m_1'),x_2^n(m_1,m_1',m_2,m_2'),y^n) \in \mathcal{T}_\epsilon^{(n)}(P_{X_1,X_2,Y}).$$

Probability of error analysis: Using standard arguments, the probability of error averaged over all codebooks vanishes exponentially with n if

$$R_2 + R_2' < I(X_2; Y|X_1) \tag{2.32}$$

$$R_1 + R_1' + R_2 + R_2' < I(X_1, X_2; Y) \tag{2.33}$$

Secrecy analysis: We will show that the information leakage, averaged over all codebooks, vanishes exponentially with n. We use the results of Theorem 2 to bound $\mathbb{E}_{M_1,M_2}[\mathbb{D}(P_{Z^n|M_1,M_2}||Q_Z^{\otimes n})]$ such that the channel output distribution at the wiretapper is, on average, independent of the transmitted messages and follows the i.i.d distribution $Q_Z^{\otimes n}$. This is sufficient to ensure secrecy because $I(M_1, M_2; Z^n)$ can be bounded by $\mathbb{E}_{M_1,M_2}[\mathbb{D}(P_{Z^n|M_1,M_2}||Q_Z^{\otimes n})]$, as follows:

$$\begin{aligned}
I(M_1, M_2; Z^n) &= \mathbb{D}(P_{M_1,M_2,Z^n}||P_{M_1,M_2}P_{Z^n}) && (2.34)\\
&= \sum_{m_1,m_2,z^n} P_{M_1,M_2,Z^n}(m_1, m_2, z^n) \log \frac{P_{M_1,M_2,Z^n}(m_1, m_2, z^n)}{P_{M_1,M_2}(m_1, m_2)P_{Z^n}(z^n)} && (2.35)\\
&= \sum_{m_1,m_2} P_{M_1,M_2}(m_1, m_2)\mathbb{D}(P_{Z^n|M_1,M_2}||P_{Z^n}) && (2.36)\\
&\overset{(a)}{\leq} \mathbb{E}_{M_1,M_2}\left(\mathbb{D}(P_{Z^n|M_1,M_2}||Q_Z^{\otimes n})\right) \ , && (2.37)
\end{aligned}$$

where (a) follows by adding $\mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) \geq 0$ to (2.36). With $P_{Z^n|M_1M_2}(z^n|m_1, m_2) = 2^{-n(R_1'+R_2')}\sum_{i,j} W^{\otimes n}(z^n|x_1^n(m_1, i), x_2^n(m_1, i, m_2, j))$ and applying Theorem 2 to (2.37), $I(M_1, M_2; Z^n)$ vanishes exponentially with n if

$$R_1' > I(X_1; Z) \tag{2.38}$$

$$R_1' + R_2' > I(X_1, X_2; Z) \tag{2.39}$$

Combining (2.32), (2.33), (2.38) and (2.39), and using Fourier-Motzkin elimination, the following rate region is achievable

$$R_2 < I(X_2; Z|X_1), \tag{2.40}$$

$$R_1 + R_2 < I(X_1, X_2; Y) - I(X_1, X_2; Z). \tag{2.41}$$

2.5.3 Channel resolvability of MAC with common message

Achievability:

Codebook Construction:

Consider a distribution $P_{U,X_1,X_2} = P_U P_{X_1|U} P_{X_2|U}$ such that $\sum_{u,x_1,x_2} P_{U,X_1,X_2} W_{Z|X_1,X_2} = Q_Z$

- Independently generate 2^{nR_0} codewords $u^n(m_0)$ each with probability $P_{U^n} = P_U^{\otimes n}$. Label them $u^n(m_0)$, $m_0 \in [\![1, 2^{nR_0}]\!]$.
- For every m_0, independently generate 2^{nR_1} codewords x_1^n each with probability $P_{X_1^n|U^n} = P_{X_1|U}^{\otimes n}$. Label them $x_1^n(m_0, m_1)$, $m_1 \in [\![1, 2^{nR_1}]\!]$.
- For every m_0, independently generate 2^{nR_2} codewords x_2^n each with probability $P_{X_2^n|U^n} = P_{X_2|U}^{\otimes n}$. Label them $x_2^n(m_0, m_2)$, $m_2 \in [\![1, 2^{nR_2}]\!]$.

This defines the codebook

$$\mathcal{C}_n = \{x_1^n(m_0, m_1), x_2^n(m_0, m_2), m_0 \in [\![1, 2^{nR_0}]\!], m_1 \in [\![1, 2^{nR_1}]\!], m_2 \in [\![1, 2^{nR_2}]\!]\} \tag{2.42}$$

and we denote the random codebook by

$$\mathfrak{C}_n = \{X_1^n(m_0, m_1), X_2^n(m_0, m_2), m_0 \in [\![1, 2^{nR_0}]\!], m_1 \in [\![1, 2^{nR_1}]\!], m_2 \in [\![1, 2^{nR_2}]\!]\} \tag{2.43}$$

$$\mathbb{E}_{\mathfrak{C}_n}\left(\mathbb{D}(P_{Z^n}||Q_Z^{\otimes n})\right)$$

$$
\begin{aligned}
&= \mathbb{E}_{\mathfrak{C}_n}\left(\sum_{z^n} P(z^n)\log\frac{P(z^n)}{Q_Z^{\otimes n}}\right) && (2.44)\\
&= \mathbb{E}_{\mathfrak{C}_n}\Bigg(\sum_{z^n}\sum_{m_0}\sum_{m_1}\sum_{m_2} 2^{-n(R_0+R_1+R_2)} W^{\otimes n}(z^n|U^n(m_0), X_1^n(m_0,m_1), X_2^n(m_0,m_2))\\
&\qquad \times \log\frac{\sum_{i,j,k} W^{\otimes n}(z^n|U^n(i), X_1^n(i,j), X_2^n(i,k))}{2^{n(R_0+R_1+R_2)}Q_Z^{\otimes n}}\Bigg) && (2.45)\\
&\overset{(a)}{\leq} \sum_{z^n}\sum_{m_0}\sum_{m_1}\sum_{m_2}\sum_{u^n(m_0)}\sum_{x_1^n(m_0,m_1)}\sum_{x_2^n(m_0,m_2)} \frac{P^{\otimes n}(u^n(m_0), x_1^n(m_0,m_1), x_2^n(m_0,m_2))}{2^{n(R_0+R_1+R_2)}}\\
&\qquad \times \log\mathbb{E}_{\setminus(m_0,m_1,m_2)}\frac{\sum_{i,j,k} W^{\otimes n}(z^n|U^n(i), X_1^n(i,j), X_2^n(i,k))}{2^{n(R_0+R_1+R_2)}Q_Z^{\otimes n}}\Bigg) && (2.46)\\
&= \sum_{z^n}\sum_{m_0}\sum_{m_1}\sum_{m_2}\sum_{u^n(m_0)}\sum_{x_1^n(m_0,m_1)}\sum_{x_2^n(m_0,m_2)} \frac{P^{\otimes n}(u^n(m_0), x_1^n(m_0,m_1), x_2^n(m_0,m_2))}{2^{n(R_0+R_1+R_2)}}\\
&\qquad \times \log\mathbb{E}_{\setminus(m_0,m_1,m_2)}\Bigg(\frac{W^{\otimes n}(z^n|u^n(m_0), x_1^n(m_0,m_1), x_2^n(m_0,m_2))}{2^{n(R_0+R_1+R_2)}Q_Z^{\otimes n}}\\
&\qquad\qquad + \frac{\sum_{j\neq m_1} W^{\otimes n}(z^n|u^n(m_0), X_1^n(m_0,j), x_2^n(m_0,m_2))}{2^{n(R_0+R_1+R_2)}Q_Z^{\otimes n}}\\
&\qquad\qquad + \frac{\sum_{k\neq m_2} W^{\otimes n}(z^n|u^n(m_0), x_1^n(m_0,m_1), X_2^n(m_0,k))}{2^{n(R_0+R_1+R_2)}Q_Z^{\otimes n}}\\
&\qquad\qquad + \frac{\sum_{\substack{j\neq m_1\\ k\neq m_2}} W^{\otimes n}(z^n|u^n(m_0), X_1^n(m_0,j), X_2^n(m_0,k))}{2^{n(R_0+R_1+R_2)}Q_Z^{\otimes n}}\\
&\qquad\qquad + \frac{\sum_{\substack{i\neq m_0\\ j,k}} W^{\otimes n}(z^n|U^n(i), X_1^n(i,j), X_2^n(i,k))}{2^{n(R_0+R_1+R_2)}Q_Z^{\otimes n}}\Bigg) && (2.47)\\
&\leq \sum_{z^n}\sum_{m_0}\sum_{m_1}\sum_{m_2}\sum_{u^n(m_0)}\sum_{x_1^n(m_0,m_1)}\sum_{x_2^n(m_0,m_2)} \frac{P^{\otimes n}(u^n(m_0), x_1^n(m_0,m_1), x_2^n(m_0,m_2))}{2^{n(R_0+R_1+R_2)}}\\
&\qquad \times \log\Bigg(\frac{W^{\otimes n}(z^n|u^n(m_0), x_1^n(m_0,m_1), x_2^n(m_0,m_2))}{2^{n(R_0+R_1+R_2)}Q_Z^{\otimes n}}\\
&\qquad\qquad + \frac{\sum_{j\neq m_1} P^{\otimes}(z^n|u^n(m_0), x_2^n(m_0,m_2))}{2^{n(R_0+R_1+R_2)}Q_Z^{\otimes n}}\\
&\qquad\qquad + \frac{\sum_{k\neq m_2} P^{\otimes}(z^n|u^n(m_0), x_1^n(m_0,m_1))}{2^{n(R_0+R_1+R_2)}Q_Z^{\otimes n}}\\
&\qquad\qquad + \frac{\sum_{\substack{j\neq m_1\\ k\neq m_2}} P^{\otimes n}(z^n|u^n(m_0))}{2^{n(R_0+R_1+R_2)}Q_Z^{\otimes n}} + 1\Bigg) && (2.48)\\
&= \Psi_1 + \Psi_2 && (2.49)
\end{aligned}
$$

where Ψ_1 and Ψ_2 are defined as following

$$\begin{aligned}
\Psi_1 \triangleq \sum_{z^n}\sum_{m_0}\sum_{m_1}\sum_{m_2}\sum_{(u^n(m_0),x_1^n(m_0,m_1),x_2^n(m_0,m_2))\in\mathcal{T}_\epsilon^n} & \frac{P^{\otimes n}(u^n(m_0),x_1^n(m_0,m_1),x_2^n(m_0,m_2))}{2^{n(R_0+R_1+R_2)}} \\
\times \log\Bigg(& \frac{W^{\otimes n}(z^n|u^n(m_0),x_1^n(m_0,m_1),x_2^n(m_0,m_2))}{2^{n(R_0+R_1+R_2)}Q_Z^{\otimes n}} \\
& + \frac{\sum_{j\neq m_1} P^{\otimes}(z^n|u^n(m_0),x_2^n(m_0,m_2))}{2^{n(R_0+R_1+R_2)}Q_Z^{\otimes n}} \\
& + \frac{\sum_{k\neq m_2} P^{\otimes}(z^n|u^n(m_0),x_1^n(m_0,m_1))}{2^{n(R_0+R_1+R_2)}Q_Z^{\otimes n}} \\
& + \frac{\sum_{\substack{j\neq m_1\\ k\neq m_2}} P^{\otimes n}(z^n|u^n(m_0))}{2^{n(R_0+R_1+R_2)}Q_Z^{\otimes n}} + 1\Bigg) && (2.50)\\
\leq \log\Bigg(& \frac{2^{-n(1-\epsilon)H(Z|X_1,X_2)}}{2^{n(R_0+R_1+R_2)}2^{-n(1+\epsilon)H(Z)}} + \frac{2^{nR_1}2^{-n(1-\epsilon)H(Z|U,X_2)}}{2^{n(R_0+R_1+R_2)}2^{-n(1+\epsilon)H(Z)}} \\
& + \frac{2^{nR_2}2^{-n(1-\epsilon)H(Z|U,X_1)}}{2^{n(R_0+R_1+R_2)}2^{-n(1+\epsilon)H(Z)}} + \frac{2^{n(R_1+R_2)}2^{-n(1-\epsilon)H(Z|U)}}{2^{n(R_0+R_1+R_2)}2^{-n(1+\epsilon)H(Z)}} + 1\Bigg) && (2.51)\\
\leq \log\Bigg(& 2^{-n(R_0+R_1+R_2-I(X_1,X_2;Z)-2\epsilon H(Z))} + 2^{-n(R_0+R_2-I(U,X_2;Z)-2\epsilon H(Z))} \\
& + 2^{-n(R_0+R_1-I(U,X_1;Z)-2\epsilon H(Z))} + 2^{-n(R_0-I(U;Z)-2\epsilon H(Z))} + 1\Bigg) && (2.52)
\end{aligned}$$

$$\begin{aligned}
\Psi_2 \triangleq \sum_{z^n}\sum_{m_0}\sum_{m_1}\sum_{m_2}\sum_{(u^n(m_0),x_1^n(m_0,m_1),x_2^n(m_0,m_2))\notin\mathcal{T}_\epsilon^n} & \frac{P^{\otimes n}(u^n(m_0),x_1^n(m_0,m_1),x_2^n(m_0,m_2))}{2^{n(R_0+R_1+R_2)}} \\
\times \log\Bigg(& \frac{W^{\otimes n}(z^n|u^n(m_0),x_1^n(m_0,m_1),x_2^n(m_0,m_2))}{2^{n(R_0+R_1+R_2)}Q_Z^{\otimes n}} \\
& + \frac{\sum_{j\neq m_1} P^{\otimes}(z^n|u^n(m_0),x_2^n(m_0,m_2))}{2^{n(R_0+R_1+R_2)}Q_Z^{\otimes n}} \\
& + \frac{\sum_{k\neq m_2} P^{\otimes}(z^n|u^n(m_0),x_1^n(m_0,m_1))}{2^{n(R_0+R_1+R_2)}Q_Z^{\otimes n}} \\
& + \frac{\sum_{\substack{j\neq m_1\\ k\neq m_2}} P^{\otimes n}(z^n|u^n(m_0))}{2^{n(R_0+R_1+R_2)}Q_Z^{\otimes n}} + 1\Bigg) && (2.53)\\
\leq 2|\mathcal{U}||\mathcal{X}_1||\mathcal{X}_2||\mathcal{Z}| & e^{-n\epsilon^2\mu_{UX_1X_2Z}} n\log(\frac{4}{\mu_z}+1) && (2.54)
\end{aligned}$$

where

$$\mu_Z = \min_{\substack{z \in \mathcal{Z} \\ \textbf{s.t. } Q(z)>0}} Q(z)$$

$$\mu_{UX_1X_2Z} = \min_{\substack{(x_1,x_2,z) \in (\mathcal{X}_1,\mathcal{X}_2,\mathcal{Z}) \\ \textbf{s.t. } Q(x_1,x_2,z)>0}} Q(x_1,x_2,z)$$

Combining the bounds on Ψ_1 and Ψ_2, we obtain $\mathbb{E}_{\mathfrak{C}_n}\left(\mathbb{D}(P_{Z^n}||Q_Z^{\otimes n})\right) \to 0$ exponentially with n if

$$\begin{aligned} R_0 &> I(U;Z) + 2\epsilon H(Z) \\ R_0 + R_1 &> I(U,X_1;Z) + 2\epsilon H(Z) \\ R_0 + R_2 &> I(U,X_2;Z) + 2\epsilon H(Z) \\ R_0 + R_1 + R_2 &> I(X_1,X_2;Z) + 2\epsilon H(Z) \end{aligned}$$

Converse:

By assumption,

$$\begin{aligned} \epsilon &\geq \mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) \\ &= \sum_{z^n} P(z^n) \log \frac{P(z^n)}{Q_Z^{\otimes n}(z^n)} \\ &= \sum_{i=1}^{n} \left(\sum_{z_i} P_Z(z_i) \log \frac{1}{Q(z_i)} - H(Z_i|Z^{i-1}) \right) \\ &\overset{(a)}{\geq} \sum_{i=1}^{n} \left(\sum_{z_i} P(z_i) \log \frac{1}{Q(z_i)} - H(Z_i) \right) \\ &= \sum_{i=1}^{n} \mathbb{D}(P_{Z_i}||Q_Z) \\ &\overset{(b)}{\geq} n\mathbb{D}(\tilde{P}_Z||Q_Z) \end{aligned}$$

where

(a) follows because conditioning does not increase entropy;

(b) follows by Jensen's inequality and the convexity of $\mathbb{D}(\cdot||\cdot)$ with $\tilde{P}_Z(z) \triangleq \frac{1}{n}\sum_{i=1}^{n} P_{Z_i}(z)$.

$$nR_0 = H(M_0) \tag{2.55}$$

$$\geq I(M_0; Z^n) \tag{2.56}$$

$$\overset{(a)}{=} I(M_0, U^n; Z^n) \tag{2.57}$$

$$\geq I(U^n; Z^n) \tag{2.58}$$

$$= I(U^n, X_1^n, X_2^n; Z^n) - I(X_1^n, X_2^n; Z^n|U^n) \tag{2.59}$$

$$= \sum_{u^n, x_1^n, x_2^n, z^n} P(u^n, x_1^n, x_2^n, z^n) \log \frac{W^{\otimes n}(z^n|u^n, x_1^n, x_2^n)}{P(z^n)} - \sum_i I(X_1^n, X_2^n; Z_1|U^n, Z^{i-1}) \tag{2.60}$$

$$= \sum_{u^n, x_1^n, x_2^n, z^n} P(u^n, x_1^n, x_2^n, z^n) \log \frac{W^{\otimes n}(z^n|u^n, x_1^n, x_2^n)}{Q_Z^{\otimes n}(z^n)} - \mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) - \sum_i I(X_1^n, X_2^n; Z_1|U^n, Z^{i-1}) \tag{2.61}$$

$$= \sum_i \sum_{u_i, x_{1i}, x_{2i}, z_i} P(u_i, x_{1i}, x_{2i}, z_i) \log \frac{W(z_i|u_i, x_{1i}, x_{2i})}{Q_Z(z_i)} - \mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) - \sum_i I(X_1^n, X_2^n; Z_i|U^n, Z^{i-1}) \tag{2.62}$$

$$\overset{(b)}{\geq} \sum_i \sum_{u_i, x_{1i}, x_{2i}, z_i} P(u_i, x_{1i}, x_{2i}, z_i) \log \frac{W(z_i|u_i, x_{1i}, x_{2i})}{Q_Z(z_i)} - \sum_i I(X_{1i}, X_{2i}; Z_i|U_i) - \epsilon \tag{2.63}$$

$$= \sum_i \sum_{u_i, x_{1i}, x_{2i}, z_i} P(u_i, x_{1i}, x_{2i}, z_i) \bigg(\log \frac{W(z_i|u_i, x_{1i}, x_{2i})}{Q_Z(z_i)} - \log \frac{W(z_i|u_i, x_{1i}, x_{2i})}{P(z_i|u_i)} \bigg) - \epsilon \tag{2.64}$$

$$= \sum_i \sum_{u_i, z_i} P(u_i, z_i) \log \frac{P(z_i|u_i)}{Q_Z(z_i)} - \epsilon \tag{2.65}$$

$$= \sum_i \mathbb{D}(P_{U_i, Z_i}||P_{U_i} Q_{Z_i}) - \epsilon \tag{2.66}$$

$$\overset{(c)}{\geq} n\mathbb{D}\biggl(\frac{\sum_i P_{U_i,Z_i}}{n}\bigg|\bigg|\frac{\sum_i P_{U_i}}{n}Q_Z\biggr)-\epsilon \tag{2.67}$$

$$\overset{(d)}{=} n\mathbb{D}(\tilde{P}_{U,Z}||\tilde{P}_U Q_Z)-\epsilon \tag{2.68}$$

$$= n\sum_{u,z} P(u,z)\log\frac{\tilde{P}(u,z)}{\tilde{P}(u)Q_Z(z)}-\epsilon \tag{2.69}$$

$$= n\sum_{u,z} P(u,z)\log\frac{\tilde{P}(u,z)}{\tilde{P}(u)\tilde{P}(z)}+n\sum_{u,z} P(u,z)\log\frac{\tilde{P}(z)}{Q_(z)}-\epsilon \tag{2.70}$$

$$= nI(\tilde{U};\tilde{Z})+n\mathbb{D}(\tilde{P}_Z||Q_Z)-\epsilon \tag{2.71}$$

$$\geq nI(\tilde{U};\tilde{Z})-\epsilon \tag{2.72}$$

where

(a) follows by setting $U_i \triangleq M_0$;

(b) follows since $I(X_1^n, X_2^n; Z_i|U^n, Z^{i-1}) = H(Z_i|U^n, Z^{i-1}) - H(Z_i|U^n, Z^{i-1}, X_1^n, X_2^n) \leq H(Z_i|U_i, Z^{i-1}) - H(Z_i|U_i, X_{1i}, X_{2i})$;

(c) follows by Jensen's inequality and the convexity of $\mathbb{D}(\cdot||\cdot)$;

(d) follows by defining $\tilde{P}_U = \frac{1}{n}\sum_i P_{U_i}$, $\tilde{P}_{U,X_1,X_2} = \frac{1}{n}\sum_i P_{U_i,X_{1i},X_{2i}}$ and $\tilde{P}_{U,Z} = \sum_{x_1,x_2}\tilde{P}_{U,X_1,X_2,Z} = \tilde{P}_{U,X_1,X_2}W_{Z|X_1,X_2}$.

$$n(R_0+R_1) = H(M_0, M_1) \tag{2.73}$$

$$\geq I(M_0, M_1; Z^n) \tag{2.74}$$

$$\overset{(a)}{=} I(M_0, M_1, U^n, X_1^n; Z^n) \tag{2.75}$$

$$\geq I(U^n, X_1^n; Z^n) \tag{2.76}$$

$$= I(U^n, X_1^n, X_2^n; Z^n) - I(X_1^n, X_2^n; Z^n|U^n, X_1^n) \tag{2.77}$$

$$\overset{(b)}{\geq} nI(\tilde{U}, \tilde{X}_1; \tilde{Z}) - \epsilon \tag{2.78}$$

where

(a) follows by setting $U_i \triangleq M_0$ and from the encoding function in (2.4);

(b) follows by steps similar to (2.59)-(2.72).

$$\begin{aligned} n(R_0+R_2) &= H(M_0,M_2) && (2.79)\\ &\geq I(M_0,M_2;Z^n) && (2.80)\\ &\overset{(a)}{=} I(M_0,M_2,U^n,X_2^n;Z^n) && (2.81)\\ &\geq I(U^n,X_2^n;Z^n) && (2.82)\\ &= I(U^n,X_1^n,X_2^n;Z^n) - I(X_1^n,X_2^n;Z^n|U^n,X_2^n) && (2.83)\\ &\overset{(b)}{\geq} nI(\tilde{U},\tilde{X}_2;\tilde{Z}) - \epsilon && (2.84) \end{aligned}$$

where

(a) follows by setting $U_i \triangleq M_0$ and from the encoding function in (2.4);

(b) follows by steps similar to to (2.59)-(2.72).

$$\begin{aligned} n(R_0+R_1+R_2) &= H(M_0,M_1,M_2) && (2.85)\\ &\geq I(M_0,M_1,M_2;Z^n) && (2.86)\\ &\overset{(a)}{=} I(M_0,M_1,M_2,X_1^n,X_2^n;Z^n) && (2.87)\\ &\geq I(X_1^n,X_2^n;Z^n) && (2.88)\\ &\overset{(b)}{\geq} nI(\tilde{X}_1,\tilde{X}_2;\tilde{Z}) - \epsilon && (2.89) \end{aligned}$$

where

(a) follows from the encoding functions in (2.4);

(b) follows by steps similar to (2.59)-(2.72).

2.5.4 Strong secrecy of MAC with common message

Achievability:

Consider a distribution $P(u, x_1, x_2) = P(u)P(x_1|u)P(x_2|u)$ such that $\sum_{u,x_1,x_2} P(u, x_1, x_2)W(z|x_1, x_2) = Q_Z(z)$.

Code Construction:

- Independently generate 2^{nR_0} codewords u^n, each with probability $P(u^n) = P_U^{\otimes n}(u^n)$. Label them $u^n(m_0)$, $m_0 \in [\![1, 2^{nR_0}]\!]$.

- For every $u^n(m_0)$, independently generate $2^{n(R_1+R_1')}$ codewords x_1^n each with probability $P(X_1^n|u^n) = P_{X_1|U}^{\otimes n}(x_1^n|u^n)$. Label them $x_1^n(m_0, m_1, m_1')$, $m_1 \in [\![1, 2^{nR_1}]\!]$ and $m_1' \in [\![1, 2^{nR_1'}]\!]$.

- For every $u^n(m_0)$, independently generate $2^{n(R_2+R_2')}$ codewords x_2^n each with probability $P(x_2^n|u^n) = P_{X_2|U}^{\otimes n}(x_2^n|u^n)$. Label them $x_2^n(m_0, m_2, m_2')$, $m_2 \in [\![1, 2^{nR_2}]\!]$ and $m_2' \in [\![1, 2^{nR_2'}]\!]$.

Encoding: To send (m_0, m_1), Encoder 1 sends $x_1^n(m_0, m_1, m_1')$. To send $(m_0 m_2)$, Encoder 2 cooperatively sends $x_2^n(m_0, m_2, m_2')$.

Decoding at the receiver: The decoder finds $\hat{m}_0, \hat{m}_1, \hat{m}_1', \hat{m}_2, \hat{m}_2'$ such that $(u^n(\hat{m}_0), x_1^n(\hat{m}_0, \hat{m}_1, \hat{m}_1'), x_2^n(\hat{m}_0, \hat{m}_2, \hat{m}_2'), y^n) \in \mathcal{T}_\epsilon^{(n)}(P_{U,X_1,X_2,Y})$.

Decoding at the wiretapper: The wiretapper finds $\hat{\hat{m}}_0$ such that $(u^n(\hat{\hat{m}}_0), z^n) \in \mathcal{T}_\epsilon^{(n)}(P_{U,Z})$.

Probability of error analysis: Using standard arguments, the probability of error averaged over all codebooks vanishes exponentially with n if

$$R_0 \leq I(U; Z) \tag{2.90}$$

$$R_1 + R_1' \leq I(X_1; Y|X_2, U) \tag{2.91}$$

$$R_2 + R_2' \leq I(X_2; Y|X_1, U) \tag{2.92}$$

$$R_1 + R_1' + R_2 + R_2' \leq I(X_1, X_2; Y|U) \tag{2.93}$$

$$R_0 + R_1 + R_1' + R_2 + R_2' \leq I(X_1, X_2; Y) \tag{2.94}$$

Secrecy analysis: We will show that the information leakage, averaged over all codebooks, vanishes exponentially with n. We use the results of Theorem 3 to bound $\mathbb{E}_{M_1,M_2}[\mathbb{D}(P_{Z^n|M_1,M_2}||Q_Z^{\otimes n})]$ such that the channel output distribution at the wiretapper is, on average, independent of the transmitted messages and follows the i.i.d distribution $Q_Z^{\otimes n}$. This is sufficient to ensure secrecy because $I(M_1, M_2; Z^n)$ can be bounded by $\mathbb{E}_{M_1,M_2}[\mathbb{D}(P_{Z^n|M_1,M_2}||Q_Z^{\otimes n})]$, as follows:

$$\begin{aligned}
I(M_1, M_2; Z^n) &= \mathbb{D}(P_{M_1,M_2,Z^n}||P_{M_1,M_2}P_{Z^n}) && (2.95)\\
&= \sum_{m_1,m_2,z^n} P_{M_1,M_2,Z^n}(m_1, m_2, z^n) \log \frac{P_{M_1,M_2,Z^n}(m_1, m_2, z^n)}{P_{M_1,M_2}(m_1, m_2)P_{Z^n}(z^n)} && (2.96)\\
&= \sum_{m_1,m_2} P_{M_1,M_2}(m_1, m_2)\mathbb{D}(P_{Z^n|M_1,M_2}||P_{Z^n}) && (2.97)\\
&\overset{(a)}{\leq} \mathbb{E}_{M_1,M_2}\left(\mathbb{D}(P_{Z^n|M_1,M_2}||Q_Z^{\otimes n})\right) && (2.98)
\end{aligned}$$

where (a) follows by adding $\mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) \geq 0$ to (2.97). With $P_{Z^n|M_1M_2}(z^n|m_1, m_2) = 2^{-n(R_0+R_1'+R_2')} \sum_{i,j,k} W^{\otimes n}(z^n|u^n(i), x_1^n(i, m_1, j), x_2^n(i, m_2, k))$ and applying Theorem 3 to (2.98), $I(M_1, M_2; Z^n)$ vanishes exponentially with n if

$$R_0 \geq I(U; Z) \tag{2.99}$$

$$R_0 + R_1' \geq I(U, X_1; Z) \tag{2.100}$$

$$R_0 + R_2' \geq I(U, X_2; Z) \tag{2.101}$$

$$R_0 + R_1' + R_2' \geq I(X_1, X_2; Z) \tag{2.102}$$

Combining (2.90)-(2.94) and (2.99)-(2.102), and using Fourier-Motzkin elimination, the following rate region is achievable

$$R_0 < I(U;Z) \tag{2.103}$$

$$R_1 < I(X_1;Y|X_2,U) - I(X_1;Z|U), \tag{2.104}$$

$$R_2 < I(X_2;Y|X_1,U) - I(X_2;Z|U), \tag{2.105}$$

$$R_1 + R_2 < I(X_1,X_2;Y|U) - I(X_1,X_2;Z|U), \tag{2.106}$$

$$R_0 + R_1 + R_2 < I(X_1,X_2;Y) - I(X_1,X_2;Z|U) \tag{2.107}$$

2.5.5 Channel resolvability of MAC with conferencing

Achievability:

From MAC with common message we know that

$$\tilde{R}_0 \geq I(U;Z) \tag{2.108}$$

$$\tilde{R}_0 + \tilde{R}_1 \geq I(U,X_1;Z) \tag{2.109}$$

$$\tilde{R}_0 + \tilde{R}_2 \geq I(U,X_2;Z) \tag{2.110}$$

$$\tilde{R}_0 + \tilde{R}_1 + \tilde{R}_2 \geq I(X_1,X_2;Z) \tag{2.111}$$

Let us define the following rates

$$\tilde{R}_0 = C_{12} + C_{21} \tag{2.112}$$

$$\tilde{R}_1 = R_1 - C_{12} \tag{2.113}$$

$$\tilde{R}_2 = R_2 - C_{21} \tag{2.114}$$

i.e., we defined the common message as the randomness exchanged via conferencing. Combining (2.108)-(2.114) yields the desired region.

Remark 6. *The same achievable result can be obtained via a binning approach. The set* $\{1, \cdots, 2^{nR_1}\}$ *is partitioned into* $2^{nR_{12}}$ *bins, each containing* $2^{n(R_1-R_{12})}$ *elements where* $R_{12} \leq C_{12}$*. In the same way, the set* $\{1, \cdots, 2^{nR_2}\}$ *is partitioned into* $2^{nR_{21}}$ *bins, each containing* $2^{n(R_2-R_{21})}$ *elements where* $R_{21} \leq C_{21}$*. Therefore, the message represented by the bin index pair* $(\{1, \cdots, 2^{nR_{12}}\}, \{1, \cdots, 2^{nR_{21}}\})$ *can be considered as the cooperation random variable.*

Converse:

$$\begin{aligned}
nR_1 &= H(M_1) && (2.115)\\
&\geq I(M_1; Z^n) && (2.116)\\
&= I(M_1, V_1^K, V_2^K; Z^n) - I(V_1^K, V_2^K; Z^n|M_1) && (2.117)\\
&\overset{(a)}{=} I(M_1, V_1^K, V_2^K, U^n, X_1^n; Z^n) - I(V_1^K, V_2^K; Z^n|M_1) && (2.118)\\
&\geq I(U^n, X_1^n; Z^n) - I(V_1^K, V_2^K; Z^n|M_1) && (2.119)\\
&= I(U^n, X_1^n; Z^n) - \sum_{k=1}^{K} I(V_{1k}, V_{2k}; Z^n|M_1, V_1^{k-1}, V_2^{k-1}) && (2.120)\\
&\overset{(b)}{=} I(U^n, X_1^n; Z^n) - \sum_{k=1}^{K} I(V_{2k}; Z^n|M_1, V_1^{k-1}, V_2^{k-1}) && (2.121)\\
&\geq I(U^n, X_1^n; Z^n) - \sum_{k=1}^{K} H(V_{2k}) && (2.122)\\
&\geq I(U^n, X_1^n; Z^n) - \sum_{k=1}^{K} \log(|\mathcal{V}_{2k}|) && (2.123)\\
&\geq I(U^n, X_1^n; Z^n) - nC_{21} && (2.124)\\
&\overset{(c)}{\geq} nI(\tilde{U}, \tilde{X}_1; \tilde{Z}) - nC_{21} && (2.125)
\end{aligned}$$

where

(a) follows by setting $U_i \triangleq (V_1^K, V_2^K)$ and from the encoding function in (2.11);

(b) follows from the communicating function in (2.9);

(c) follows by similar steps to (2.59)-(2.72).

Similarly,

$$nR_2 = nI(\tilde{U}, \tilde{X}_2; \tilde{Z}) - nC_{12} \tag{2.126}$$

$$\begin{align}
n(R_1 + R_2) &= H(M_1, M_2) \tag{2.127}\\
&\geq I(M_1, M_2; Z^n) \tag{2.128}\\
&= I(M_1, M_2, V_1^K, V_2^K; Z^n) - I(V_1^K, V_2^K; Z^n|M_1, M_2) \tag{2.129}\\
&\overset{(a)}{=} I(M_1, M_2, V_1^K, V_2^K, X_1^n, X_2^n; Z^n) - I(V_1^K, V_2^K; Z^n|M_1, M_2) \tag{2.130}\\
&\geq I(X_1^n, X_2^n; Z^n) - I(V_1^K, V_2^K; Z^n|M_1, M_2) \tag{2.131}\\
&= I(X_1^n, X_2^n; Z^n) - \sum_{k=1}^{K} I(V_{1k}, V_{2k}; Z^n|M_1, M_2, V_1^{k-1}, V_2^{k-1}) \tag{2.132}\\
&\overset{(b)}{=} I(X_1^n, X_2^n; Z^n) \tag{2.133}\\
&\overset{(c)}{\geq} nI(\tilde{X}_1, \tilde{X}_2; \tilde{Z}) \tag{2.134}
\end{align}$$

where

(a) follows from the encoding functions in (2.11) and (2.12) ;

(b) follows from the communicating functions in (2.9) and (2.10) ;

(c) follows by similar steps to (2.59)-(2.72).

$$\begin{align}
n(C_{12} + C_{21}) &\geq \sum_{k=1}^{K} \log(|\mathcal{V}_{1k}|) + \sum_{k=1}^{K} \log(|\mathcal{V}_{2k}|) \tag{2.135}\\
&\geq \sum_{k=1}^{K} H(V_{1k}) + \sum_{k=1}^{K} H(V_{2k}) \tag{2.136}
\end{align}$$

$$\geq \sum_{k=1}^{K} H(V_{1k}, V_{2k}) \tag{2.137}$$

$$\geq H(V_1^K, V_2^K) \tag{2.138}$$

$$\geq I(V_1^K, V_2^K; Z^n) \tag{2.139}$$

$$\overset{(a)}{=} I(V_1^K, V_2^K, U^n; Z^n) \tag{2.140}$$

$$\geq I(U^n; Z^n) \tag{2.141}$$

$$\overset{(b)}{\geq} nI(\tilde{U}; \tilde{Z}) \tag{2.142}$$

where

(a) follows by setting $U_i \triangleq (V_1^K, V_2^K)$;

(b) follows by similar steps to (2.59)-(2.72).

2.5.6 Strong secrecy of MAC with conferencing

Consider a distribution $P(u, x_1, x_2) = P(u)P(x_1|u)P(x_2|u)$ such that $\sum_{u,x_1,x_2} P(u, x_1, x_2)W(z|x_1, x_2) = Q_Z(z)$. Split the secret message m_1 into two independent secrecy messages m_{12} and m_{1p} . Similarly, split the secret message m_2 into two independent secrecy messages m_{21} and m_{2p}.

Code Construction:

- Independently generate $2^{n(R_{12}+nR'_{12}+R_{21}+R'_{21})}$ codewords u^n, each with probability $P(u^n) = P_u^{\otimes n}(u^n)$. Label them $u^n(m_{12}, m'_{12}, m_{21}, m'_{21})$, $m_{12} \in [\![1, 2^{nR_{12}}]\!]$, $m'_{12} \in [\![1, 2^{nR'_{12}}]\!]$, $m_{21} \in [\![1, 2^{nR_{21}}]\!]$ and $m'_{21} \in [\![1, 2^{nR'_{21}}]\!]$. Let $w_0 = (m_{12}, m'_{12}, m_{21}, m'_{21})$.
- For every $u^n(w_0)$, independently generate $2^{n(R_1-R_{12}+R'_1-R'_{12})}$ codewords x_1^n each with probability $P(x_1^n|u^n) = P_{X_1|U}^{\otimes n}(x_1^n|u^n)$. Label them $x_1^n(w_0, m_{1p}, m'_{1p})$, $m_{1p} \in [\![1, 2^{n(R_1-R_{12})}]\!]$ and $m'_{1p} \in [\![1, 2^{n(R'_1-R'_{12})}]\!]$.

- For every $u^n(w_0)$, independently generate $2^{n(R_2-R_{21}+R_2'-R_{21}')}$ codewords x_2^n each with probability $P(x_2^n|u^n) = P_{X_2|U}^{\otimes n}(x_2^n|u^n)$. Label them $x_2^n(w_0, m_{2p}, m_{2p}')$, $m_{2p} \in [\![1, 2^{n(R_2-R_{21})}]\!]$ and $m_{2p}' \in [\![1, 2^{n(R_2'-R_{21}')}]\!]$.

Encoding: To send m_1, Encoder 1 transmits $x_1^n(w_0, m_{1p}, m_{1p}')$. To send m_2, Encoder 2 cooperatively sends $x_2^n(w_0, m_{2p}, m_{2p}')$.

Decoding: The decoder finds $(\hat{w}_0, \hat{m}_{1p}, \hat{m}_{1p}', \hat{m}_{2p}, \hat{m}_{2p}')$ such that

$$(u^n(\hat{w}_0), x_1^n(\hat{w}_0, \hat{m}_{1p}, \hat{m}_{1p}'), x_2^n(\hat{w}_0, \hat{m}_{2p}, \hat{m}_{2p}'), y^n) \in \mathcal{T}_\epsilon^{(n)}(P_{U,X_1,X_2,Y}).$$

Probability of error analysis: Using standard arguments, the probability of error averaged over all codebooks vanishes exponentially with n if

$$R_{12} + R_{12}' < C_{12} \tag{2.143}$$

$$R_{21} + R_{21}' < C_{21} \tag{2.144}$$

$$R_1 + R_1' - R_{12} - R_{12}' < I(X_1; Y|X_2, U) \tag{2.145}$$

$$R_2 + R_2' - R_{21} - R_{21}' < I(X_2; Y|X_1, U) \tag{2.146}$$

$$R_1 + R_1' + R_2 + R_2' < I(X_1, X_2; Y) \tag{2.147}$$

$$R_1 + R_1' - R_{12} - R_{12}' + R_2 + R_2' - R_{21} - R_{21}' < I(X_1, X_2; Y|U) \tag{2.148}$$

which can be simplified as

$$R_1 + R_1' < I(X_1; Y|X_2, U) + C_{12} \tag{2.149}$$

$$R_2 + R_2' < I(X_2; Y|X_1, U) + C_{21} \tag{2.150}$$

$$R_1 + R_1' + R_2 + R_2' < I(X_1, X_2; Y) \tag{2.151}$$

$$R_1 + R_1' + R_2 + R_2' < I(X_1, X_2; Y|U) + C_{12} + C_{21} \tag{2.152}$$

Secrecy analysis: We will show that the information leakage, averaged over all codebooks, vanishes exponentially with n. We use the results of Theorem 4 to bound

$\mathbb{E}_{M_1,M_2}[\mathbb{D}(P_{Z^n|M_1,M_2}||Q_Z^{\otimes n})]$ such that the channel output distribution at the wiretapper is, on average, independent of the transmitted messages and follows the i.i.d distribution $Q_Z^{\otimes n}$. This is sufficient to ensure secrecy because $I(M_1, M_2; Z^n)$ can be bounded by $\mathbb{E}_{M_1,M_2}[\mathbb{D}(P_{Z^n|M_1,M_2}||Q_Z^{\otimes n})]$, as follows:

$$I(M_1, M_2; Z^n) = \mathbb{D}(P_{M_1,M_2,Z^n}||P_{M_1,M_2}P_{Z^n}) \tag{2.153}$$

$$= \sum_{m_1,m_2,z^n} P_{M_1,M_2,Z^n}(m_1, m_2, z^n) \log \frac{P_{M_1,M_2,Z^n}(m_1, m_2, z^n)}{P_{M_1,M_2}(m_1, m_2)P_{Z^n}(z^n)} \tag{2.154}$$

$$= \sum_{m_1,m_2} P_{M_1,M_2}(m_1, m_2)\mathbb{D}(P_{Z^n|M_1,M_2}||P_{Z^n}) \tag{2.155}$$

$$\overset{(a)}{\leq} \mathbb{E}_{M_1,M_2}\left(\mathbb{D}(P_{Z^n|M_1,M_2}||Q_Z^{\otimes n})\right) \ , \tag{2.156}$$

where (a) follows by adding $\mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) \geq 0$ to (2.155). With $P_{Z^n|M_1M_2}(z^n|m_1, m_2) = 2^{-n(R_1'+R_2')} \sum_{i,j,k,l} W^{\otimes n}(z^n|u^n(m_{12}, i, m_{21}, j), x_1^n(m_{12}, i, m_{21}, j, m_{1p}, k), x_2^n(m_{12}, i, m_{21}, j, m_{2p}, l))$ and applying Theorem 4 to (2.156), $I(M_1, M_2; Z^n)$ vanishes exponentially with n if

$$C_{12} + C_{21} \geq I(U; Z) \tag{2.157}$$

$$R_1' \geq I(U, X_1; Z) - C_{21} \tag{2.158}$$

$$R_2' \geq I(U, X_2; Z) - C_{12} \tag{2.159}$$

$$R_1' + R_2' \geq I(X_1, X_2; Z) \tag{2.160}$$

Combining (2.149)-(2.152) and (2.157)-(2.160), and using Fourier-Motzkin elimination, the following rate region is achievable

$$C_{12} + C_{21} \geq I(U; Z) \tag{2.161}$$

$$R_1 < I(X_1; Y|X_2, U) - I(U, X_1; Z) + C_{12} + C_{21} \tag{2.162}$$

$$R_2 < I(X_2; Y|X_1, U) - I(U, X_2; Z) + C_{12} + C_{21} \tag{2.163}$$

$$R_1 + R_2 < I(X_1, X_2; Y) - I(X_1, X_2; Z) \tag{2.164}$$

$$R_1 + R_2 < I(X_1, X_2; Y|U) - I(X_1, X_2; Z) + C_{12} + C_{21} \tag{2.165}$$

2.5.7 Convexity proof of channel resolvability of MAC with degraded message sets

Assume that $(R_1^{(1)}, R_2^{(1)})$ and $(R_1^{(2)}, R_2^{(2)})$ are achievable, which implies the existence of two distributions $P^{(1)}_{X_1,X_2,Z}$ and $P^{(2)}_{X_1,X_2,Z}$ with marginal Q_Z such that,

$$\begin{gathered} R_1^{(1)} \geq I(X_1^{(1)}; Z^{(1)}), \\ R_1^{(1)} + R_2^{(1)} \geq I(X_1^{(1)}, X_2^{(1)}; Z^{(1)}), \\ \text{and} \\ R_1^{(2)} \geq I(X_1^{(2)}; Z^{(2)}), \\ R_1^{(2)} + R_2^{(2)} \geq I(X_1^{(2)}, X_2^{(2)}; Z^{(2)}). \end{gathered}$$

Let $P^{(3)}_{X_1,X_2|Z} = \lambda P^{(1)}_{X_1,X_2|Z} + (1-\lambda) P^{(2)}_{X_1,X_2|Z}$ for $\lambda \in [\![0,1]\!]$ and $P^{(3)}_{X_1|Z} = \lambda P^{(1)}_{X_1|Z} + (1-\lambda) P^{(2)}_{X_1|Z}$. Note that $P^{(3)}_{X_1,X_2,Z}$ resulting from a convex combination of $P^{(1)}_{X_1,X_2,Z}$ and $P^{(2)}_{X_1,X_2,Z}$ exists unlike MAC with non-cooperating encoders, where the convex combination does not necessarily factorize into a product distribution.

From the convexity of $I(X_1, X_2; Z)$ with respect to $P_{X_1,X_2|Z}$ and the convexity of $I(X_1; Z)$ with respect to $P_{X_1|Z}$, it follows that for a fixed Q_Z:

$$\begin{gathered} I(X_1^{(3)}; Z^{(3)}) \leq \lambda I(X_1^{(1)}; Z^{(1)}) + (1-\lambda) I(X_1^{(2)}; Z^{(2)}), \\ I(X_1^{(3)}, X_2^{(3)}; Z^{(3)}) \leq \lambda I(X_1^{(1)}, X_2^{(1)}; Z^{(1)}) + (1-\lambda) I(X_1^{(2)}, X_2^{(2)}; Z^{(2)}). \end{gathered}$$

Therefore we have

$$\begin{gathered} I(X_1^{(3)}; Z^{(3)}) \leq \lambda R_1^{(1)} + (1-\lambda) R_1^{(2)}, \\ I(X_1^{(3)}, X_2^{(3)}; Z^{(3)}) \leq \lambda (R_1^{(1)} + R_2^{(1)}) + (1-\lambda)(R_1^{(2)} + R_2^{(2)}). \end{gathered}$$

which implies that $\big(\lambda R_1^{(1)} + (1-\lambda)R_1^{(2)}, \lambda R_2^{(1)} + (1-\lambda)R_2^{(2)}\big)$ is inside the achievable region defined by $P^{(3)}_{X_1,X_2,Z}$.

2.5.8 Convexity proof of channel resolvability of MAC with common message

Assume that $(R_0^{(1)}, R_1^{(1)}, R_2^{(1)})$ and $(R_0^{(2)}, R_1^{(2)}, R_2^{(2)})$ are achievable, which implies the existence of two distributions $P^{(1)}_{U,X_1,X_2,Z} = P^{(1)}_U P^{(1)}_{X_1|U} P^{(1)}_{X_2|U} W^{(1)}_{Z|X_1,X_2}$ and $P^{(2)}_{U,X_1,X_2,Z} = P^{(2)}_U P^{(2)}_{X_1|U} P^{(2)}_{X_2|U} W^{(2)}_{Z|X_1,X_2}$ with marginal Q_Z such that,

$$\begin{aligned} R_0^{(1)} &\geq I(U^{(1)}; Z^{(1)}), \\ R_0^{(1)} + R_1^{(1)} &\geq I(U^{(1)}, X_1^{(1)}; Z^{(1)}), \\ R_0^{(1)} + R_2^{(1)} &\geq I(U^{(1)}, X_2^{(1)}; Z^{(1)}), \\ R_0^{(1)} + R_1^{(1)} + R_2^{(1)} &\geq I(X_1^{(1)}, X_2^{(1)}; Z^{(1)}), \end{aligned}$$

and

$$\begin{aligned} R_0^{(2)} &\geq I(U^{(2)}; Z^{(2)}), \\ R_0^{(2)} + R_1^{(2)} &\geq I(U^{(2)}, X_1^{(2)}; Z^{(2)}), \\ R_0^{(2)} + R_2^{(2)} &\geq I(U^{(2)}, X_2^{(2)}; Z^{(2)}), \\ R_0^{(2)} + R_1^{(2)} + R_2^{(2)} &\geq I(X_1^{(2)}, X_2^{(2)}; Z^{(2)}). \end{aligned}$$

Let $P^{(3)}_{U,X_1,X_2|Z} = P^{(3)}_U P^{(3)}_{X_1|U} P^{(3)}_{X_2|U} W^{(3)}_{Z|X_1,X_2} = \lambda P^{(1)}_{U,X_1,X_2|Z} + (1-\lambda) P^{(2)}_{U,X_1,X_2|Z}$ for $\lambda \in [\![0,1]\!]$. From the convexity of $I(\cdot; Z)$ with respect to $P_{\cdot|Z}$, it follows that for a fixed Q_Z:

$$\begin{aligned} I(U^{(3)}; Z^{(3)}) &\leq \lambda I(U^{(1)}; Z^{(1)}) + (1-\lambda) I(U^{(2)}; Z^{(2)}), \\ I(U^{(3)}, X_1^{(3)}; Z^{(3)}) &\leq \lambda I(U^{(1)}, X_1^{(1)}; Z^{(1)}) + (1-\lambda) I(U^{(2)}, X_1^{(2)}; Z^{(2)}), \\ I(U^{(3)}, X_2^{(3)}; Z^{(3)}) &\leq \lambda I(U^{(1)}, X_2^{(1)}; Z^{(1)}) + (1-\lambda) I(U^{(2)}, X_2^{(2)}; Z^{(2)}), \\ I(X_1^{(3)}, X_2^{(3)}; Z^{(3)}) &\leq \lambda I(X_1^{(1)}, X_2^{(1)}; Z^{(1)}) + (1-\lambda) I(X_1^{(2)}, X_2^{(2)}; Z^{(2)}). \end{aligned}$$

Therefore we have

$$\begin{aligned}
I(U^{(3)}; Z^{(3)}) &\leq \lambda R_0^{(1)} + (1-\lambda) R_0^{(2)}, \\
I(U^{(3)}, X_1^{(3)}; Z^{(3)}) &\leq \lambda (R_0^{(1)} + R_1^{(1)}) + (1-\lambda)(R_0^{(2)} + R_1^{(2)}), \\
I(U^{(3)}, X_2^{(3)}; Z^{(3)}) &\leq \lambda (R_0^{(1)} + R_2^{(1)}) + (1-\lambda)(R_0^{(2)} + R_2^{(2)}), \\
I(X_1^{(3)}, X_2^{(3)}; Z^{(3)}) &\leq \lambda (R_0^{(1)} + R_1^{(1)} + R_2^{(1)}) + (1-\lambda)(R_0^{(2)} + R_1^{(2)} + R_2^{(2)}).
\end{aligned}$$

which implies that $\big(\lambda R_0^{(1)} + (1-\lambda) R_0^{(2)}, \lambda R_1^{(1)} + (1-\lambda) R_1^{(2)}, \lambda R_2^{(1)} + (1-\lambda) R_2^{(2)}\big)$ is inside the achievable region defined by $P^{(3)}_{U,X_1,X_2,Z}$.

CHAPTER 3

MAC WITH CRIBBING [1] [2]

In this chapter we study MAC with cribbing. In this channel model, one or both encoders have access to the output of the other encoder subject to various causality constraints. The goal is to capture the essence of cooperation and produce results and insights that are independent of cooperation signaling mechanisms. In each cribbing model, we provide inner and outer bounds for the channel resolvability region which are tight for most of the cases. We then provide inner bounds for the strong secrecy regions building on the results of channel resolvability.

3.1 MAC with One-Sided Cribbing

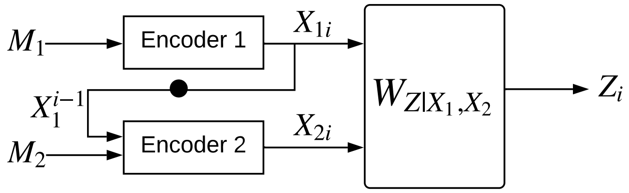

Figure 3.1. The multiple access channel with one-sided strictly-causal cribbing.

We consider three scenarios for the two-user discrete memoryless MAC with one-sided cribbing. The discrete memoryless MAC $(\mathcal{X}_1 \times \mathcal{X}_2, W_{Z|X_1,X_2}, \mathcal{Z})$ consists of finite input alphabets $\mathcal{X}_1$ and $\mathcal{X}_2$, and finite output alphabet $\mathcal{Z}$, together with a channel transition probability $W_{Z|X_1X_2}$. For a joint input distribution P_{X_1,X_2} on $\mathcal{X}_1 \times \mathcal{X}_2$, the output is distributed according to $Q_Z(z) = \sum_{x_1,x_2} P_{X_1,X_2}(x_1,x_2) W_{Z|X_1,X_2}(z|x_1,x_2)$. A $(2^{nR_1}, 2^{nR_2}, n)$ channel resolvability

[1] © N. Helal and M. Bloch and A. Nosratinia, "Multiple-Access Channel Resolvability with Cribbing," 2018 IEEE International Symposium on Information Theory (ISIT), pp. 2052-2056, 2018.

[2] © N. Helal and M. Bloch and A. Nosratinia, "Cooperative Resolvability and Secrecy in the Cribbing Multiple Access Channel," in IEEE Transactions on Information Theory.

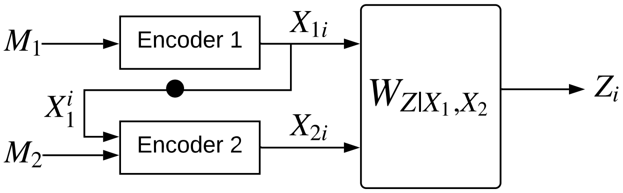

Figure 3.2. The multiple access channel with one-sided causal cribbing.

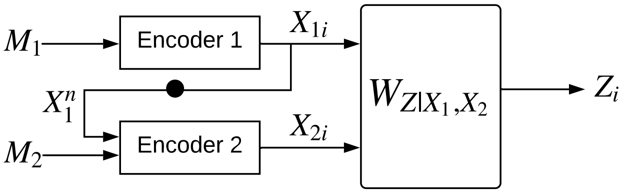

Figure 3.3. The multiple access wiretap channel with one-sided non-causal cribbing.

code consists of two encoders f_1 and f_2 with inputs M_1 and M_2 defined on $\mathcal{M}_1 = [\![1, 2^{nR_1}]\!]$ and $\mathcal{M}_2 = [\![1, 2^{nR_2}]\!]$. In the four scenarios studied in this dissertation, the per-symbol encoding functions are defined as follows.

In MAC with one-sided strictly-causal cribbing (Figure 3.1), Encoder 2 has access to the output of Encoder 1 with a one-symbol delay

$$f_{1i} : \mathcal{M}_1 \to \mathcal{X}_1 \qquad f_{2i} : \mathcal{M}_2 \times \mathcal{X}^{i-1} \to \mathcal{X}_2. \tag{3.1}$$

In MAC with one-sided causal cribbing (Figure 3.2), Encoder 2 has access to the output of Encoder 1 with zero delay

$$f_{1i} : \mathcal{M}_1 \to \mathcal{X}_1 \qquad f_{2i} : \mathcal{M}_2 \times \mathcal{X}_1^i \to \mathcal{X}_2. \tag{3.2}$$

In MAC with one-sided non-causal cribbing (Figure 3.3), Encoder 2 has non-causal access to the entire current codeword of Encoder 1

$$f_{1i} : \mathcal{M}_1 \to \mathcal{X}_1 \qquad f_{2i} : \mathcal{M}_2 \times \mathcal{X}_1^n \to \mathcal{X}_2. \tag{3.3}$$

Definition 7. *A rate pair* (R_1, R_2) *is said to be achievable for the discrete memoryless MAC* $(\mathcal{X}_1 \times \mathcal{X}_2, W_{Z|X_1X_2}, \mathcal{Z})$ *if for a given* Q_Z *there exists a sequence of* $(2^{nR_1}, 2^{nR_2}, n)$ *codes such that* $\lim_{n\to\infty} \mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) = 0$*. The MAC resolvability region is the closure of the set of achievable rate pairs* (R_1, R_2)*.*

3.1.1 MAC with one-sided strictly-causal cribbing

Theorem 5. *The resolvability region for the MAC with one-sided strictly-causal cribbing is included in the set of rate pairs* (R_1, R_2) *such that*

$$R_1 \geq I(U, X_1; Z), \tag{3.4}$$

$$R_2 \geq I(X_1, X_2; Z) - H(X_1|U), \tag{3.5}$$

$$R_1 + R_2 \geq I(X_1, X_2; Z), \tag{3.6}$$

for some joint distribution $P_{UX_1X_2Z} \triangleq P_U P_{X_1|U} P_{X_2|U} W_{Z|X_1X_2}$ *with marginal* Q_Z*. An achievable region is characterized by the same rate constraints and distribution, but subject to the additional constraint* $H(X_1|U) > I(U, X_1; Z)$*.*

Proof. See Section 3.4.1. □

The achievable region provided by Theorem 5 does not provably match the outer bound because the set of probability distributions available in the achievable region is smaller than in the converse, due to the additional constraint $H(X_1|U) > I(U, X_1; Z)$. The rate regions defined by the inner and outer bounds are convex (see Section 3.4.9).

3.1.2 MAC with one-sided causal cribbing

Theorem 6. *The resolvability region for the MAC with one-sided causal cribbing is the set of rate pairs* (R_1, R_2) *such that*

$$R_1 \geq I(X_1; Z) \tag{3.7}$$

$$R_2 \geq I(X_1, X_2; Z) - H(X_1) \tag{3.8}$$

$$R_1 + R_2 \geq I(X_1, X_2; Z) \tag{3.9}$$

for some joint distribution $P_{X_1X_2Z} \triangleq P_{X_1X_2}W_{Z|X_1X_2}$ with marginal Q_Z.

Proof. See Section 3.4.3. □

Remark 7. *Theorem 6 is established from Theorem 5 using Shannon strategies as in [32], yet Theorem 6 has an achievable region that is tight against the outer bound when Theorem 5 does not. Perhaps surprisingly, this happens because the choice of random variables in the Shannon strategy automatically satisfies the constraint imposed in the achievability of Theorem 5.*

This rate region is convex (see Section 3.4.10).

3.1.3 MAC with one-sided non-causal cribbing

Theorem 7. *The resolvability region for MAC with one-sided non-causal cribbing is the set of rate pairs (R_1, R_2) such that*

$$R_1 \geq I(X_1; Z), \tag{3.10}$$

$$R_2 \geq I(X_1, X_2; Z) - H(X_1), \tag{3.11}$$

$$R_1 + R_2 \geq I(X_1, X_2; Z), \tag{3.12}$$

for some joint distribution $P_{X_1X_2Z} \triangleq P_{X_1X_2}W_{Z|X_1X_2}$ with marginal Q_Z.

Proof. See 3.4.5 □

Similar to what was observed for the MAC reliability region [32], the MAC resolvability region with non-causal cribbing is *identical* to that obtained for causal cribbing.

The achievability result was derived in [4, Corollary VII.8] for approximation of the output statistics in terms of total variational distance. Our contribution here is to provide achievability and converse proofs for approximation in terms of KL divergence. Compared with MAC with degraded message sets, more randomness is required as seen by the presence of an individual rate constraint for User 2. As already discussed in [4], this stems from the impossibility for Encoder 2 to extract uniform randomness from the observation of the output of Encoder 1 at a rate exceeding $H(X_1)$. This rate region is convex (see Section 3.4.10).

3.2 MAC with Two-Sided Cribbing

3.2.1 MAC with two-sided strictly-causal cribbing

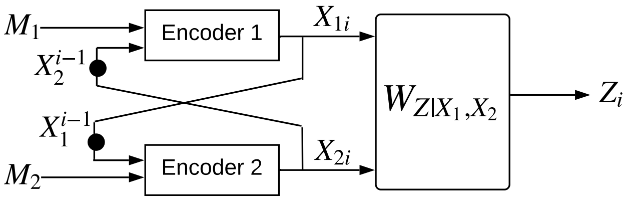

Figure 3.4. The multiple access channel with two-sided strictly-causal cribbing.

The discrete memoryless MAC with two-sided strictly-causal cribbing (Figure 3.4) consists of finite input alphabets $\mathcal{X}_1$ and $\mathcal{X}_2$, and finite output alphabet Z with a channel transition probability $W_{Z|X_1,X_2}$. For a joint distribution P_{X_1,X_2} on $\mathcal{X}_1 \times \mathcal{X}_2$, the output is distributed according to $Q_Z(z) = \sum_{x_1,x_2} P_{X_1,X_2}(x_1,x_2) W_{Z|X_1,X_2}(z|x_1,x_2)$. A $(2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n)$ channel resolvability code consists of two encoders f_1 and f_2 with inputs $M_1 \in [\![1, 2^{nR_1}]\!]$ and $M_2 \in [\![1, 2^{nR_2}]\!]$. The encoding functions are defined as follows:

$$f_{1i} : \mathcal{M}_1 \times \mathcal{X}_2^{i-1} \to \mathcal{X}_{1i} \qquad f_{2i} : \mathcal{M}_2 \times \mathcal{X}_1^{i-1} \to \mathcal{X}_{2i}. \tag{3.13}$$

Proposition 5. *For the discrete memoryless MAC channel with two-sided strictly-causal cribbing, the following region is achievable if there exists a joint distribution* $P_{U,U_1,U_2,X_1,X_2,Z} = P_U P_{U_1|U} P_{U_2|U} P_{X_1|U,U_1} P_{X_2|U,U_2} W_{Z|X_1,X_2}$ *with marginal* Q_Z *satisfying*

$H(X_1|U, U_1) + H(X_2|U, U_2) > I(X_1, X_2; Z)$ *for which:*

$$
\begin{aligned}
R_1 &\geq I(X_1, X_2; Z) - H(X_2|U, U_2) \\
R_2 &\geq I(X_1, X_2; Z) - H(X_1|U, U_1) \\
R_1 + R_2 &\geq I(X_1, X_2; Z)
\end{aligned}
$$

Proof. See Section 3.4.7. □

Proposition 6. *For the discrete memoryless MAC channel with two-sided strictly-causal cribbing, the following region is achievable if there exists a joint distribution* $P_{U,X_1,X_2,Z} = P_U P_{X_1|U} P_{X_2|U} W_{Z|X_1,X_2}$ *with marginal* Q_Z *satisfying* $H(X_1|U) + H(X_2|U) > I(X_1, X_2; Z)$ *for which:*

$$
\begin{aligned}
R_1 &\geq I(X_1, X_2; Z) - H(X_2|U) \\
R_2 &\geq I(X_1, X_2; Z) - H(X_1|U) \\
R_1 + R_2 &\geq I(X_1, X_2; Z)
\end{aligned}
$$

Proof. See Section 3.4.7. □

Proposition 7. *For the discrete memoryless MAC channel with two-sided strictly-causal cribbing, an outer bound for the resolvability region for which* $P_{U_1,U_2,X_1,X_2,Z} = P_{U_1,U_2} P_{X_1|U_1,U_2} P_{X_2|U_1,U_2} W_{Z|X_1,X_2}$ *is given by:*

$$
\begin{aligned}
R_1 &\geq I(X_1, X_2; Z) - H(X_2|U_2) \\
R_2 &\geq I(X_1, X_2; Z) - H(X_1|U_1) \\
R_1 + R_2 &\geq I(X_1, X_2; Z)
\end{aligned}
$$

Proof. See Section 3.4.7. □

Similar to MAC with one-sided strictly-causal cribbing, it can be proven that the resolvability regions provided by Propositions 5, 6 and 7 are convex.

3.3 Strong Secrecy from Channel Resolvability

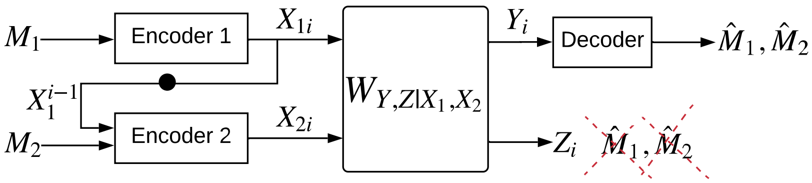

Figure 3.5. The multiple access wiretap channel with one-sided strictly-causal cribbing.

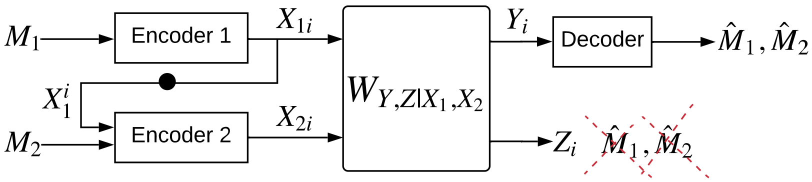

Figure 3.6. The multiple access wiretap channel with one-sided causal cribbing.

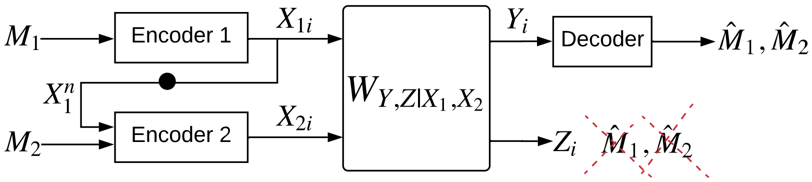

Figure 3.7. The multiple access wiretap channel with one-sided non-causal cribbing.

In this section we use the resolvability results to study the multiple-access wiretap channel with cribbing (Figures 3.5, 3.6, 3.7 and 3.8). For each of the cribbing models previously

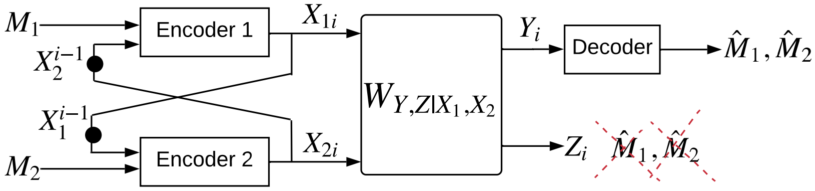

Figure 3.8. The multiple access wiretap channel with two-sided strictly-causal cribbing.

discussed, an achievable strong secrecy rate region is presented. Consider a MAC with cribbing $(\mathcal{X}_1 \times \mathcal{X}_2, W_{Z|X_1,X_2}, \mathcal{Y}, \mathcal{Z})$ where $\mathcal{X}_1$ and $\mathcal{X}_2$ are finite input alphabets, $\mathcal{Y}$ and $\mathcal{Z}$ are the finite output alphabets of the legitimate receiver and the wiretapper, respectively. A $(2^{nR_1}, 2^{nR_2}, n)$ code consists of two encoders f_1 and f_2 and a decoder g. The encoders are defined similar to (3.1)-(3.3) and (3.13) but the functions f_{1i} and f_{2i} are now stochastic and not deterministic. The decoding function at the legitimate receiver is defined as:

$$g : \mathcal{Y}^n \to \hat{\mathcal{M}}_1 \times \hat{\mathcal{M}}_2. \tag{3.14}$$

The probability of error at the legitimate receiver is defined as $P_e^{(n)} = \mathbb{P}\Big((\hat{M}_1, \hat{M}_2) \neq (M_1, M_2)\Big)$. The strong secrecy metric adopted is defined as $L^{(n)} = I(M_1, M_2; Z^n)$.

Definition 8. *A strong secrecy rate pair (R_1, R_2) is said to be achievable for the discrete memoryless MAC $(\mathcal{X}_1 \times \mathcal{X}_2, W_{Z|X_1X_2}, \mathcal{Y}, \mathcal{Z})$ if there exists a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes such that $P_e^{(n)}$ and $L^{(n)}$ vanish as $n \to \infty$.*

Proposition 8. *For the multiple-access wiretap channel with strictly-causal cribbing, the following strong-secrecy rate region is achievable:*

$$(R_1, R_2) = \bigcup_{P_U P_{X_1|U} P_{X_2|U} W_{YZ|X_1X_2}} \mathcal{R}_{\text{SC}}^{(\text{in})},$$

$$\mathcal{R}_{\text{SC}}^{(\text{in})} = \left\{ \begin{array}{l} R_1, R_2 \geq 0 \\ R_1 \leq H(X_1|U) - I(U, X_1; Z) \\ R_2 \leq I(X_2; Y|X_1, U) \\ R_1 + R_2 \leq H(X_1|U) + I(X_2; Y|X_1, U) - I(X_1, X_2; Z) \\ R_1 + R_2 \leq I(X_1, X_2; Y) - I(X_1, X_2; Z) \end{array} \right\}. \tag{3.15}$$

Proof. See Section 3.4.2. □

Remark 8. *Recall the resolvability achievable rate region under the strictly-causal cribbing had a constraint $H(X_1|U) > I(U, X_1; Z)$ on the allowable probability distributions. This constraint is implicit in Proposition 8 in the form of the non-negativity constraint on R_1.*

Proposition 9. *For the multiple-access wiretap channel with causal cribbing, the following strong-secrecy rate region is achievable:*

$$(R_1, R_2) = \bigcup_{P_{X_1 X_2} W_{YZ|X_1 X_2}} \mathcal{R}_{\text{C}}^{(\text{in})},$$

$$\mathcal{R}_{\text{C}}^{(\text{in})} = \left\{ \begin{array}{l} R_1, R_2 \geq 0 \\ R_1 \leq H(X_1) - I(X_1; Z) \\ R_2 \leq I(X_2; Y|X_1) \\ R_1 + R_2 \leq I(X_1, X_2; Y) - I(X_1, X_2; Z) \end{array} \right\}. \tag{3.16}$$

Proof. See Section 3.4.4. □

Proposition 10. *For the multiple-access wiretap channel with non-causal cribbing, the following strong-secrecy rate region is achievable:*

$$(R_1, R_2) = \bigcup_{P_{X_1 X_2} W_{YZ|X_1 X_2}} \mathcal{R}_{\text{NC}}^{(\text{in})},$$

$$\mathcal{R}_{\text{NC}}^{(\text{in})} = \left\{ \begin{array}{l} R_1, R_2 \geq 0 \\ R_1 \leq H(X_1) - I(X_1; Z) \\ R_2 \leq I(X_2; Y|X_1) \\ R_1 + R_2 \leq I(X_1, X_2; Y) - I(X_1, X_2; Z) \end{array} \right\}. \tag{3.17}$$

Proof. See Section 3.4.6 □

Proposition 11. *For the multiple-access wiretap channel with two-sided strictly-causal cribbing, the following strong-secrecy rate region is achievable:*

$$(R_1, R_2) = \bigcup_{P_U P_{X_1|U} P_{X_2|U} W_{YZ|X_1X_2}} \mathcal{R}^{(\text{in})}_{\text{SC},2},$$

$$\mathcal{R}^{(\text{in})}_{\text{SC},2} = \left\{ \begin{array}{l} R_1, R_2 \geq 0 \\ R_1 \leq H(X_1|U) \\ R_2 \leq H(X_2|U) \\ R_1 + R_2 \leq H(X_1|U) + H(X_2|U) - I(X_1, X_2; Z) \\ R_1 + R_2 \leq I(X_1, X_2; Y) - I(X_1, X_2; Z) \end{array} \right\}. \tag{3.18}$$

Proof. See Section 3.4.8. □

3.4 Proofs

3.4.1 Channel resolvability of MAC with one-sided strictly-causal cribbing

Achievability:

To handle the strict causality constraint, we adopt a block-Markov encoding scheme over $B > 0$ consecutive and dependent blocks, each consisting of r transmissions such that $n = rB$. The vector of n channel outputs Z^n may then be described as $Z^n \triangleq (Z_1^r, \cdots, Z_B^r)$, where each Z_b^r for $b \in [\![1, B]\!]$ describes the observations in block b. The distribution induced by the coding scheme is the joint distribution $P_Z^n \triangleq P_{Z_1^r, \cdots, P_{Z_B^r}}$, while the target output distribution is a product distribution of product distributions $Q_Z^{\otimes n} \triangleq \prod_{j=1}^{B} Q_Z^{\otimes r}$.

Codebook generation: Consider a distribution $P_{UX_1X_2Z} = P_U P_{X_1|U} P_{X_2|U} W_{Z|X_1X_2}$ with marginal Q_Z that satisfies $H(X_1|U) > I(UX_1; Z)$. For every block $b \in [\![1, B]\!]$:

- Independently generate $2^{r\rho_0}$ codewords according to $P_U^{\otimes r}$ and label them $u^r(m_0^{(b)})$, where $m_0^{(b)} \in [\![1, 2^{r\rho_0}]\!]$.

- For every $m_0^{(b)}$, independently generate $2^{r(\rho_1'+\rho_1'')}$ codewords according to $\prod_{i=1}^r P_{X_1|U=u_i^r(m_0^{(b)})}$; label them $x_1^r(m_0^{(b)}, m_1'^{(b)}, m_1''^{(b)})$ for $m_1'^{(b)} \in [\![1, 2^{r\rho_1'}]\!]$ and $m_1''^{(b)} \in [\![1, 2^{r\rho_1''}]\!]$. Note that $m_1^{(b)} = (m_1'^{(b)}, m_1''^{(b)})$.
- For every $m_0^{(b)}$, independently generate $2^{r\rho_2}$ codewords according to $\prod_{i=1}^r P_{X_2|U=u_i^r(m_0^{(b)})}$; label them $x_2^r(m_0^{(b)}, m_2^{(b)})$, $m_2^{(b)} \in [\![1, 2^{r\rho_2}]\!]$.

This defines the codebook in block b

$$\mathcal{C}_r = \{u^r(m_0^{(b)}), x_1^r(m_0^{(b)}, m_1'^{(b)}, m_1''^{(b)}), x_2^r(m_0^{(b)}, m_2^{(b)}), m_0^{(b)} \in [\![1, 2^{r\rho_0}]\!], m_1'^{(b)} \in [\![1, 2^{r\rho_1'}]\!], \\ m_1''^{(b)} \in [\![1, 2^{r\rho_1''}]\!], m_2^{(b)} \in [\![1, 2^{r\rho_2}]\!]\} \quad (3.19)$$

and we denote the random codebook in block b by

$$\mathfrak{C}_r = \{U^r(m_0^{(b)}), X_1^r(m_0^{(b)}, m_1'^{(b)}, m_1''^{(b)}), X_2^r(m_0^{(b)}, m_2^{(b)}), m_0^{(b)} \in [\![1, 2^{r\rho_0}]\!], m_1'^{(b)} \in [\![1, 2^{r\rho_1'}]\!], \\ m_1''^{(b)} \in [\![1, 2^{r\rho_1''}]\!], m_2^{(b)} \in [\![1, 2^{r\rho_2}]\!]\} \quad (3.20)$$

The message $M_1''^{(b)}$ is the part of $M_1^{(b)}$ that we wish to recycle toward the creation of $M_0^{(b+1)}$, which itself constitutes the cooperating message between the two encoders. The codes hence obtained are chained across B blocks as follows. In Block 1, we assume that the encoders have access to a common message $M_0^{(1)}$ through some private common randomness (see Remark 9 for justification). In block $b > 1$, we assume for now that Encoder 2 knows $M_0^{(b)}$. It is then able to form estimates $\hat{M}_1'^{(b)}, \hat{M}_1''^{(b)}$, which are correct with high probability. Assuming $\rho_1'' > \rho_0$, an amount ρ_0 of the rate ρ_1'' (which represents $M_1''^{(b)}$) may be *recycled* toward the creation of $M_0^{(b+1)}$. Furthermore, for $\gamma \in [\![0, 1]\!]$, an amount $\gamma(\rho_1'' - \rho_0)$ may be recycled toward the creation of $M_1'^{(b+1)}$, and an amount $(1-\gamma)(\rho_1'' - \rho_0)$ may be recycled toward the creation of $M_2^{(b+1)}$.

The key observations here are that (i) this procedure ensures that, with high probability, *both* Encoder 1 and Encoder 2 know messages $M_0^{(b)}, M_1'^{(b)}, M_1''^{(b)}$ at the end of block b, so that they can coordinate their choices of $M_0^{(b+1)}$; and (ii) the dependencies across blocks are only created through $M_1''^{(b)}$. This dependency between blocks can be hidden at the output of the channel by transmitting $M_1''^{(b)}$ securely over the wiretap channel shown in Figure 3.9.

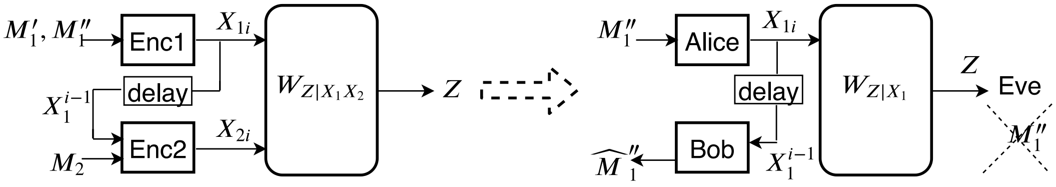

Figure 3.9. Wiretap channel embedded in MAC with strictly-causal cribbing.

Next we bound $\mathbb{D}(P_{Z^n}||Q_Z^{\otimes n})$ and show that the dependencies across blocks created by block-Markov coding can be eliminated by suitably recycling randomness from one block to the next.

$$
\begin{aligned}
&\mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) = \mathbb{D}(P_{Z_1^r \dots Z_B^r}||Q_Z^{\otimes rB}) \\
&\overset{(a)}{=} \sum_{b=1}^{B} \mathbb{D}(P_{Z_b^r}||Q_Z^{\otimes r}) + \sum_{b=1}^{B} \mathbb{D}(P_{Z_b^r|Z^{(b+1:B),r}}||P_{Z_b^r}|P_{Z^{(b+1:B),r}}) \\
&= \sum_{b=1}^{B} \mathbb{D}(P_{Z_b^r}||Q_Z^{\otimes r}) + \sum_{b=1}^{B} I(Z_b^r; Z^{(b+1:B),r}) \\
&\overset{(b)}{\leq} \sum_{b=1}^{B} \mathbb{D}(P_{Z_b^r, M_1''^{(b)}}||Q_Z^{\otimes r} P_{M_1''^{(b)}}) + \sum_{b=1}^{B} I(Z_b^r; M_1''^{(b)}, \hat{M}_1''^{(b)}, Z^{(b+1:B),r}) \\
&\overset{(c)}{=} \sum_{b=1}^{B} \mathbb{D}(P_{Z_b^r, M_1''^{(b)}}||Q_Z^{\otimes r} P_{M_1''^{(b)}}) + \sum_{b=1}^{B} I(Z_b^r; M_1''^{(b)}, \hat{M}_1''^{(b)}) \\
&= \sum_{b=1}^{B} \mathbb{D}(P_{Z_b^r, M_1''^{(b)}}||Q_Z^{\otimes r} P_{M_1''^{(b)}}) + \sum_{b=1}^{B} I(Z_b^r; M_1''^{(b)}) + \sum_{b=1}^{B} I(Z_b^r; \hat{M}_1''^{(b)}|M_1''^{(b)}) \\
&\overset{(d)}{\leq} 2\sum_{b=1}^{B} \mathbb{D}(P_{Z_b^r, M_1''^{(b)}}||Q_Z^{\otimes r} P_{M_1''^{(b)}}) + \sum_{b=1}^{B} H(\hat{M_1}''^{(b)}|M_1''^{(b)})
\end{aligned}
$$

where

(a) follows from the definition $Z^{(b+1:B),r} = \{Z_{b+1}^r, \dots Z_B^r\}$;

(b) follows since $\mathbb{D}(P_{Z_b^r}||Q_Z^{\otimes r}) = \mathbb{D}(P_{Z_b^r, M_1^{\prime\prime(b)}}||Q_Z^{\otimes r} P_{M_1^{\prime\prime(b)}}) - \mathbb{D}(P_{Z_b^r, M_1^{\prime\prime(b)}}||P_{Z_b^r} P_{M_1^{\prime\prime(b)}})$;

(c) follows since $Z_b^r \to M_1^{\prime\prime(b)}, \hat{M}_1^{\prime\prime(b)} \to Z^{(b+1:B),r}$ holds;

(d) follows since $I(Z_b^r; M_1^{\prime\prime(b)}) = \mathbb{D}(P_{Z_b^r, M_1^{\prime\prime(b)}}||P_{Z_b^r} P_{M_1^{\prime\prime(b)}}) \leq \mathbb{D}(P_{Z_b^r, M_1^{\prime\prime(b)}}||Q_Z^{\otimes r} P_{M_1^{\prime\prime(b)}})$.

Let $P_e^{(b)}$ be the average error probability of Encoder 2 decoding $(M_1^{\prime(b)}, M_1^{\prime\prime(b)})$. From Fano's inequality, we can write $H(\hat{M}_1^{\prime\prime(b)}|M_1^{\prime\prime(b)}) \leq H(P_e^{(b)}) + r\rho_1^{\prime\prime} P_e^{(b)}$. By random coding we know that $\mathbb{E}_{\mathfrak{C}_r}\left(P_e^{(b)}\right) < 2^{-\alpha r}$ for some $\alpha > 0$ and all r large enough if

$$\rho_1' + \rho_1'' < H(X_1|U) \tag{3.21}$$

Let P be the probability distribution induced when Encoder 1 uses $M_0^{(b)}$ and Encoder 2 uses an estimate $\hat{M}_0^{(b)}$ derived from his estimate $\hat{M}_1^{\prime\prime(b-1)}$. Define $\bar{P}$ as the probability distribution induced when both encoders are using the same $M_0^{(b)}$, i.e., $\hat{M}_0^{(b)} = M_0^{(b)}$ or $\hat{M}_1^{\prime\prime(b-1)} = M_1^{\prime\prime(b-1)}$.

$$P_{Z_b^r} = \sum_{\substack{m_0^{(b)}, \hat{m}_0^{(b)}, \\ m_1^{\prime(b)}, m_1^{\prime\prime(b)}, \\ m_2^{(b)}}} 2^{-r(2\rho_0+\rho_1'+\rho_1''+\rho_2)} W^{\otimes r}(z_b^r|u^r(m_0^{(b)}), u^r(\hat{m}_0^{(b)}), x_1^r(m_0^{(b)}, m_1^{\prime(b)}, m_1^{\prime\prime(b)}), x_2^r(\hat{m}_0^{(b)}, m_2^{(b))})), \tag{3.22}$$

$$\bar{P}_{Z_b^r} = \sum_{\substack{m_0^{(b)}, m_1^{\prime(b)}, \\ m_1^{\prime\prime(b)}, m_2^{(b)}}} 2^{-r(\rho_0+\rho_1'+\rho_1''+\rho_2)} W^{\otimes r}(z_b^r|u^r(m_0^{(b)}), x_1^r(m_0^{(b)}, m_1^{\prime(b)}, m_1^{\prime\prime(b)}), x_2^r(m_0^{(b)}, m_2^{(b))})). \tag{3.23}$$

If we let $D^{(b)} \triangleq \mathbb{D}(\bar{P}_{Z_b^r M_1^{\prime\prime(b)}}||Q_Z^{\otimes r} \bar{P}_{M_1^{\prime\prime(b)}})$, a standard argument (see [33, Section III] for a similar result with total variational distance and Section 3.4.11 for more detailed steps) shows that, when averaging over the randomly generated codes, $\mathbb{E}_{\mathfrak{C}_n}\left(D^{(b)}\right) < 2^{-\beta r}$ for some $\beta > 0$ and all r large enough if

$$\rho_0 > I(U;Z), \tag{3.24}$$

$$\rho_0 + \rho_1' > I(U, X_1; Z), \tag{3.25}$$

$$\rho_0 + \rho_1' + \rho_2 > I(X_1, X_2; Z), \tag{3.26}$$

$$\rho_0 + \rho_2 > I(U, X_2; Z). \tag{3.27}$$

Let $\epsilon > 0$ and set

$$\rho_0 = I(U; Z) + \epsilon, \tag{3.28}$$

$$\rho_1' = I(X_1; Z|U) + \epsilon, \tag{3.29}$$

$$\rho_1'' = H(X_1|U) - I(X_1; Z|U) - 2\epsilon, \tag{3.30}$$

$$\rho_2 = I(X_2; Z|U, X_1) + \epsilon, \tag{3.31}$$

which is compatible with constraints (3.21)-(3.25). The choice is also compatible with (3.26) because $I(U, X_1, X_2; Z) = I(X_1, X_2; Z)$. The choice is finally compatible with (3.27) because $I(X_2; Z|U, X_1) = H(X_2|UX_1) - H(X_2|U, X_1, Z) = H(X_2|U) - H(X_2|U, X_1, Z) \geq H(X_2|U) - H(X_2|U, Z) = I(X_2; Z|U)$. Hence, by an expurgation argument, for every $b \in [\![1, B]\!]$ there exists a code for block b such that

$$P_e^{(b)} < 2^{-\alpha' r} \quad \text{and} \quad D^{(b)} < 2^{-\beta' r} \tag{3.32}$$

for some α', $\beta' > 0$ and all r large enough.

Note that the effective rate of *new* randomness for Encoder 1 in block b is

$$R_1 \triangleq \rho_1' + \rho_1'' - \gamma(\rho_1'' - \rho_0) = \rho_1' + (1-\gamma)\rho_1'' + \gamma\rho_0, \tag{3.33}$$

and the effective rate for Encoder 2 is

$$R_2 \triangleq \rho_2 - (1-\gamma)(\rho_1'' - \rho_0). \tag{3.34}$$

Using the values of $\rho_0, \rho_1', \rho_1'', \rho_2$ chosen in (3.28)-(3.31), we may obtain all[1] rate pairs such that

$$R_1 \geq \rho_1' + \rho_0 = I(U, X_1; Z) + 2\epsilon,$$

[1] For R_1 we choose $\gamma = 1$ and for R_2 we choose $\gamma = 0$, in each case finding the smallest single-user rate constraint so that the entire rate region is captured. The sum-rate constraint is independent of γ.

$$R_2 \geq \rho_2 - \rho_1'' + \rho_0 = I(X_1, X_2; Z) - H(X_1|U) + 4\epsilon,$$

$$R_1 + R_2 \geq \rho_1' + \rho_1'' + \rho_2 - (\rho_1'' - \rho_0) = I(X_1, X_2; Z) + 3\epsilon,$$

which is the desired rate region.

Finally we show that $\mathbb{E}_{\mathfrak{C}_r}\left(\mathbb{D}(\bar{P}_{Z_b^r, M_1''^{(b)}} || Q_Z^{\otimes r} \bar{P}_{M_1''^{(b)}})\right) \xrightarrow{r\to\infty} 0$ implies $\mathbb{E}_{\mathfrak{C}_r}\left(\mathbb{D}(P_{Z_b^r, M_1''^{(b)}} || Q_Z^{\otimes r} P_{M_1''^{(b)}})\right) \xrightarrow{r\to\infty} 0$. The total variation $\mathbb{V}(P_{Z_b^r M_1''^{(b)}}, \bar{P}_{Z_b^r M_1''^{(b)}})$ satisfies

$$\mathbb{V}(P_{Z_b^r M_1''^{(b)}}, \bar{P}_{Z_b^r M_1''^{(b)}}) \leq \mathbb{V}(P_{Z_b^r M_0^{(b)} M_1'^{(b)} M_1''^{(b)} \hat{M}_0^{(b)} M_2^{(b)}}, \bar{P}_{Z_b^r M_0^{(b)} M_1'^{(b)} M_1''^{(b)} M_0^{(b)} M_2^{(b)}}) \tag{3.35}$$

$$= \mathbb{V}(P_{M_0^{(b)} \hat{M}_0^{(b)}}, \bar{P}_{M_0^{(b)} M_0^{(b)}}) \tag{3.36}$$

$$= 2\mathbb{P}(M_0^{(b)} \neq \hat{M}_0^{(b)}) \tag{3.37}$$

$$\leq 2\mathbb{P}(M_1''^{(b-1)} \neq \hat{M}_1''^{(b-1)}). \tag{3.38}$$

Consequently, since $\bar{P}_{M_1''^{(b-1)}} = P_{M_1''^{(b-1)}}$, we obtain

$$\begin{aligned} \mathbb{V}(P_{Z_b^r M_1''^{(b)}}, Q_Z^{\otimes r} P_{M_1''^{(b)}}) &\leq \mathbb{V}(P_{Z_b^r M_1''^{(b)}}, \bar{P}_{Z_b^r M_1''^{(b)}}) + \mathbb{V}(\bar{P}_{Z_b^r M_1''^{(b)}}, Q_Z^{\otimes r} P_{M_1''^{(b)}}) \\ &\leq 2 \times 2^{-\alpha' r} + 2^{-\frac{\beta'}{2} r}, \end{aligned} \tag{3.39}$$

where we have used Pinsker's inequality to bound the last term. To conclude that $\mathbb{D}(P_{Z_b^r M_1''^{(b)}} || Q_Z^{\otimes r} P_{M_1''^{(b)}})$ vanishes, we recall the following result [29, Eq. (323)].

Lemma 2. *Let P and Q be two distributions on a finite alphabet $\mathcal{A}$ such that P is absolutely continuous w.r.t. Q. If $\mu \triangleq \min_{a \in \mathcal{Q}: Q(a)>0} Q(a)$, we have*

$$\mathbb{D}(P||Q) \leq \log\left(\frac{1}{\mu}\right) \mathbb{V}(P, Q).$$

Note that $P_{Z_b^r M_1''^{(b)}}$ is absolutely continuous w.r.t. $Q_Z^{\otimes r} P_{M_1''^{(b)}}$ by definition of Q_Z and the code construction. Hence, using (3.39) together with Lemma 2 shows that there exists $\eta > 0$ such that for all r large enough

$$\mathbb{D}(P_{Z_b^r M_1''^{(b)}} || Q_Z^{\otimes r} P_{M_1''^{(b)}}) < 2^{-\eta r}. \tag{3.40}$$

Remark 9. *Recall that some private common randomness is required to jump-start the block-Markov encoding; this common randomness can be collected during a non-cooperative starting phase in the following manner. The two encoders will start transmitting with rates* $R_1 = H(X_1)$ *and* $R_2 = 0$*, which exceeds the single-user resolvability rate. Simultaneously, via the usual arguments in the degraded wiretap channel* $M_1 \to X_1^n \to Z^n$*, one can convey* $\frac{1}{n}(I(M_1; X_1^n) - I(M_1; Z^n)) = H(X_1|Z)$ *bits of randomness from User 1 to User 2 while keeping it independent of* Z *and maintaining an i.i.d. distribution* $Q^{\otimes n}(z)$*. By collecting this randomness for* $\frac{\rho_0}{H(X_1|Z)}$ *blocks, sufficient common randomness will be available to start the block-Markov process. The difference of rates* (R_1, R_2) *in the starting phase will be amortized over* B *blocks, with* B *growing without bound, thus the average rates remain as described. The concept of starting the block-Markov transmission with a non-cooperative phase goes back to the inception of block-Markov encoding [34].*

Remark 10. *The above mentioned initialization of block-Markov coding leaves open the possibility that some* $Q(z)$ *may be compatible with some joint distribution* $p(x_1, x_2)$ *but incompatible with all product distributions* $p(x_1)p(x_2)$*. Such a* $Q(z)$ *is valid for cooperative transmission but cannot be generated during the non-cooperative initialization of block-Markov encoding. Thus, for a more precise definition of the model for MAC with* strictly-causal *cribbing, in the context of resolvability, we are presented with three distinct choices: Either (a) some private shared randomness (with rate that amortizes asymptotically to zero) is made available to the model, or (b) the distribution* $Q(z)$ *is limited to the set that can be generated via product distributions* $p(x_1)p(x_2)$*, or (c) the distribution of* Z^n*, although still i.i.d., is allowed to deviate from the target* $Q(z)$ *for a finite number of blocks at the beginning of transmission. Options (b) and (c) are both reasonable for secrecy applications of resolvability; option (b) may affect secrecy rates.*

Converse:

We consider a $(2^{nR_1}, 2^{nR_2}, n)$ code such that $\mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) \leq \epsilon$, where $\epsilon \xrightarrow{n\to\infty} 0$. Then,

$$nR_1 = H(M_1)$$

$$\geq I(M_1; Z^n)$$

$$\overset{(a)}{=} I(M_1, X_1^n; Z^n) \tag{3.41}$$

$$\geq I(X_1^n; Z^n)$$

$$= I(X_1^n, X_2^n; Z^n) - I(X_2^n; Z^n|X_1^n)$$

$$\overset{(b)}{\geq} \sum_{x_1^n} \sum_{x_2^n} \sum_{z^n} P(x_1^n, x_2^n, z^n) \log \frac{W^{\otimes n}(z^n|x_1^n, x_2^n)}{P_{Z^n}(z^n)} - \sum_i I(X_{2i}; Z_i|X_{1i}, X_1^{i-1}) \tag{3.42}$$

$$\overset{(c)}{=} \sum_{x_1^n} \sum_{x_2^n} \sum_{z^n} P(x_1^n, x_2^n, z^n) \log \frac{W^{\otimes n}(z^n|x_1^n, x_2^n)}{Q_Z^{\otimes n}(z^n)} - \mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) - \sum_i I(X_{2i}; Z_i|X_{1i}, U_i) \tag{3.43}$$

$$\geq \sum_i \sum_{u_i} \sum_{x_{1i}} \sum_{x_{2i}} \sum_{z_i} P(u_i, x_{1i}, x_{2i}, z_i) \log \frac{W(z_i|x_{1i}, x_{2i})}{Q(z_i)}$$

$$- \sum_i \sum_{u_i} \sum_{x_{1i}} \sum_{x_{2i}} \sum_{z_i} P(u_i, x_{1i}, x_{2i}, z_i) \log \frac{W(z_i|x_{1i}, x_{2i})}{P(z_i|x_{1i}, u_i)} - \epsilon \tag{3.44}$$

$$= \sum_i \sum_{u_i} \sum_{x_{1i}} \sum_{x_{2i}} \sum_{z_i} P(u_i, x_{1i}, x_{2i}, z_i) \log \frac{P(z_i|x_{1i}, u_i)}{Q(z_i)} - \epsilon$$

$$= \sum_i \sum_{u_i} \sum_{x_{1i}} \sum_{z_i} P(u_i, x_{1i}, z_i) \log \frac{P(z_i|x_{1i}, u_i)}{Q(z_i)} - \epsilon$$

$$= \sum_i \mathbb{D}(P_{U_i, X_{1i}, Z_i}||P_{U_i, X_{1i}} Q_{Z_i}) - \epsilon$$

$$= \sum_i I(U_i X_{1i}; Z_i) + \sum_i \mathbb{D}(P_{Z_i}||Q_Z) - \epsilon \tag{3.45}$$

$$\overset{(d)}{\geq} nI(U_Q X_{1Q}; Z_Q|Q) - \epsilon \tag{3.46}$$

$$= nI(QU_Q X_{1Q}; Z_Q) - nI(Q; Z_Q) - \epsilon \tag{3.47}$$

$$\overset{(e)}{\geq} nI(UX_1; Z) - n\epsilon' \tag{3.48}$$

where

(a) follows from the definition of the deterministic encoding functions in (3.1);

(b) follows from $I(X_2^n; Z^n|X_1^n) \leq \sum_{i=1}^n I(X_{2,i}; Z_i|X_{1,i}X_1^{i-1})$ since the channel is memoryless and because conditioning does not increase entropy;

(c) follows setting $U_i \triangleq X_1^{i-1}$;

(d) follows by introducing a random variable Q uniformly distributed on $\llbracket 1, n \rrbracket$ and independent of all others;

(e) follows by [4, Lemma VI.3] for some $\epsilon' > 0$ with $\lim_{\epsilon \to 0} \epsilon' = 0$ and by setting $U = (Q, U_Q)$, $X_1 = X_{1Q}$ and $Z = Z_Q$.

Notice that upon setting $X_2 = X_{2Q}$ and recalling that the cribbing is strictly-causal such that X_{2Q} is a function of (M_2, Q, U_Q), and that the Markov chains $M_1, X_1 \to U \to M_2$ and $X_{1Q} \to Q, U_Q \to X_{2Q}$ hold, we have

$$P_{QU_QX_{1Q}X_{2Q}Z_Q} = P_{QU_Q}P_{X_{1Q}|U_QQ}P_{X_{2Q}|U_QQ}W_{Z_Q|X_{1Q}X_{2Q}}, \tag{3.49}$$

and

$$P_{UX_1X_2Z} = P_U P_{X_1|U} P_{X_2|U} W_{Z|X_1X_2}. \tag{3.50}$$

Next, note that

$$\begin{aligned}
nR_2 &= H(M_2) \\
&\geq H(M_2|X_1^n) \\
&\geq I(M_2; Z^n|X_1^n) \\
&\overset{(a)}{=} I(M_2, X_2^n; Z^n|X_1^n) && (3.51) \\
&\geq I(X_2^n; Z^n|X_1^n) \\
&= I(X_1^n, X_2^n; Z^n) - I(X_1^n; Z^n) && (3.52)
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{x_1^n}\sum_{x_2^n}\sum_{z^n} P(x_1^n, x_2^n, z^n) \log \frac{W^{\otimes n}(z^n|x_1^n, x_2^n)}{P_{Z^n}(z^n)} - I(X_1^n; Z^n) \\
&\geq \sum_{x_1^n}\sum_{x_2^n}\sum_{z^n} P(x_1^n, x_2^n, z^n) \log \frac{W^{\otimes n}(z^n|x_1^n, x_2^n)}{Q_Z^{\otimes n}(z^n)} - \mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) - H(X_1^n) \\
&\geq \sum_{i}\sum_{x_{1i}}\sum_{x_{2i}}\sum_{z_i} P(x_{1i}, x_{2i}, z_i) \log \frac{W(z_i|x_{1i}, x_{2i})}{Q(z_i)} - \sum_i H(X_{1i}|U_i) - \epsilon \\
&= \sum_{i}\sum_{i}\sum_{x_{1i}}\sum_{x_{2i}} P(x_{1i}, x_{2i}, z_i) \log \frac{W(z_i|x_{1i}, x_{2i})}{P(z_i)} + \mathbb{D}(P_{Z_i}||Q_Z) - \sum_i H(X_{1i}|U_i) - \epsilon \\
&\geq \sum_i I(X_{1i}, X_{2i}; Z_i) - \sum_i H(X_{1i}|U_i) - \epsilon \\
&= nI(X_{1Q}X_{2Q}; Z_Q|Q) - nH(X_{1Q}|U_Q Q) - \epsilon \\
&= nI(QX_{1Q}X_{2Q}; Z_Q) - nI(Q; Z_Q) - nH(X_{1Q}|U_Q Q) - \epsilon \\
&\overset{(b)}{\geq} nI(X_{1Q}X_{2Q}; Z_Q) - nH(X_{1Q}|U_Q Q) - n\epsilon' \\
&= nI(X_1X_2; Z) - nH(X_1|U) - n\epsilon' \qquad (3.53)
\end{aligned}
$$

where (a) follows from the definition of the encoding function and (b) follows by [4, Lemma VI.3] for some $\epsilon' > 0$ with $\lim_{\epsilon \to 0} \epsilon' = 0$. Finally,

$$
\begin{aligned}
n(R_1 + R_2) &= H(M_1, M_2) \\
&\geq I(M_1, M_2; Z^n) \\
&\geq I(X_1^n, X_2^n; Z^n) + \mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) - \epsilon \\
&\geq nI(X_1, X_2; Z) - n\epsilon'
\end{aligned}
$$

where we have merely repeated the steps in (3.52)-(3.53).

3.4.2 Strong secrecy of MAC with one-sided strictly-causal cribbing

Achievability:

The interesting challenge being addressed in this section is that the decoding at output Y and secrecy at output Z have dissonant requirements under strictly-causal cribbing. For decoding, Willems and van der Muelen [32] proposed a block-Markov superposition coding technique where all the information carried by the cribbing signal is used as cloud centers for the purpose of cooperation between the two encoders. The tightness of the inner and outer bounds in [32] strongly suggests (via continuity arguments in joint probability distributions) that leaving out any part of cribbing information from cooperation can incur a rate loss for decoding at Y. On the other hand, the resolvability results of this dissertation strongly suggest that for simulating a desired probability distribution at Z, it is beneficial to have a local randomness component at X_1 that does not take part in cooperation with X_2. The contribution of this section is to produce a coding strategy that reconciles these two dissonant requirements.

We begin by informally describing the main idea of this section with a simplified notation. The codebook for X_1 is driven by three variables: (M_1, M_1', M_1''). M_1 is the secret message, and M_1', M_1'' are uniformly distributed dithers. The encoder for X_2 will decode the cribbing signal X_1 and use all its three components as cloud center for the next transmission, which we call M_0, M_0', M_0''. This, as mentioned earlier, is crucial for decoding at Y. Now we introduce an additional constraint (enforced by proper assignment of rates) so that Z is independent of M_0', one of the dither components of X_1. Thus, as far as the distribution of Z is concerned, one of the two dither components of X_1 is local (private) to X_1 and is not used by X_2. To elaborate further, due to the imposed independence, the cloud centers that only differ in their M_0' index must give rise to the same distribution in Z, therefore Encoder 2 has been effectively enjoined from cooperation or coordination with part of the dither of Encoder 1, which for all practical purposes becomes local to X_1 as far as the eavesdropper is concerned. We now make these ideas precise in full detail, which includes direct reference to block indices as well as accounting for discrepancies between message/dither indices and their estimated values.

We use a combination of block-Markov encoding and backward decoding. Independently and uniformly distributed messages $m_1^{(b)} \in [\![1, 2^{rR_1}]\!]$ and $m_2^{(b)} \in [\![1, 2^{rR_2}]\!]$ will be sent over

B blocks. Each block consists of r transmissions so that $n = rB$. Consider a distribution $P(u, x_1, x_2) = P(u)P(x_1|u)P(x_2|u)$ such that $\sum_{u,x_1,x_2} P(u, x_1, x_2)W(z|x_1, x_2) = Q_Z(z)$.

Code Construction: In each block $b \in [\![1, B]\!]$:

- Independently generate $2^{r(R_1+\rho_1'+\rho_1'')}$ codewords u_b^r each with probability $P(u^r) = P_U^{\otimes r}(u^r)$. Label them $u^r(m_0^{(b)}, m_0'^{(b)}, m_0''^{(b)})$, $m_0^{(b)} \in [\![1, 2^{rR_1}]\!]$, $m_0'^{(b)} \in [\![1, 2^{r\rho_1'}]\!]$ and $m_0''^{(b)} \in [\![1, 2^{r\rho_1''}]\!]$.

- For every $u^r(m_0^{(b)}, m_0'^{(b)}, m_0''^{(b)})$, independently generate $2^{r(R_1+\rho_1'+\rho_1'')}$ codewords x_{1b}^r each with probability $P(x_1^r|u^r(m_0^{(b)}, m_0'^{(b)}, m_0''^{(b)})) = P_{X_1|U}^{\otimes r}(x_1^r|u^r(m_0^{(b)}, m_0'^{(b)}, m_0''^{(b)}))$. Label them $x_1^r(m_0^{(b)}, m_0'^{(b)}, m_0''^{(b)}, m_1^{(b)}, m_1'^{(b)}, m_1''^{(b)})$, $m_1^{(b)} \in [\![1, 2^{rR_1}]\!]$, $m_1'^{(b)} \in [\![1, 2^{r\rho_1'}]\!]$ and $m_1''^{(b)} \in [\![1, 2^{r\rho_1''}]\!]$.

- For every $u^r(m_0^{(b)}, m_0'^{(b)}, m_0''^{(b)})$, independently generate $2^{r(R_2+\rho_2)}$ codewords x_{2b}^r each with probability $P(x_2^r|u^r(m_0^{(b)}, m_0'^{(b)}, m_0''^{(b)})) = P_{X_2|U}^{\otimes r}(x_2^r|u^r(m_0^{(b)}, m_0'^{(b)}, m_0''^{(b)}))$. Label them $x_2^r(m_0^{(b)}, m_0'^{(b)}, m_0''^{(b)}, m_2^{(b)}, m_2'^{(b)})$, $m_2^{(b)} \in [\![1, 2^{rR_2}]\!]$ and $m_2'^{(b)} \in [\![1, 2^{r\rho_2}]\!]$.

We intend to use these codebooks in the following manner:

1. Block Markov encoding via $M_0^{(b)} = M_1^{(b-1)}$, $M_0'^{(b)} = M_1'^{(b-1)}$ and $M_0''^{(b)} = M_1''^{(b-1)}$;

2. $M_1^{(b)}$, $M_1'^{(b)}$ and $M_1''^{(b)}$ can be decoded from X_{1b}^r knowing $(M_0^{(b)}, M_0'^{(b)}, M_0''^{(b)})$;

3. $\{M_1^{(1)}, \dots, M_1^{(B)}\}$ and $\{M_2^{(1)}, \dots, M_2^{(B)}\}$ are secret from $\{Z_1^r, \dots, Z_B^r\}$;

4. $M_1''^{(b)}$ is the common randomness to be used by both encoders in block $b + 1$;

5. $M_1'^{(b)}$ is local randomness used by Encoder 1 and $M_2'^{(b)}$ is local randomness used by Encoder 2;

6. The messages $M_0^{(b)}$, $M_0'^{(b)}$, $M_0''^{(b)}$, $M_1^{(b)}$, $M_1'^{(b)}$, $M_1''^{(b)}$, $M_2^{(b)}$ and $M_2'^{(b)}$ can be decoded at the receiver from Y_b^r and the messages decoded in future blocks $b+1$ to B (backward decoding).

As a result of cribbing, after block b, Encoder 2 finds estimates $(\hat{m}_1^{(b)}, \hat{m}_1'^{(b)}, \hat{m}_1''^{(b)})$ for $(m_1^{(b)}, m_1'^{(b)}, m_1''^{(b)})$ such that

$$(u^r(\hat{m}_0^{(b)}, \hat{m}_0'^{(b)}, \hat{m}_0''^{(b)}), x_1^r(\hat{m}_0^{(b)}, \hat{m}_0'^{(b)}, \hat{m}_0''^{(b)}, \hat{m}_1^{(b)}, \hat{m}_1'^{(b)}, \hat{m}_1''^{(b)}), x_{1b}^r) \in \mathcal{T}_\epsilon^{(r)}(P_{U,X_1,X_1}). \quad (3.54)$$

where $(\hat{m}_0^{(b)}, \hat{m}_0'^{(b)}, \hat{m}_0''^{(b)}) = (\hat{m}_1^{(b-1)}, \hat{m}_1'^{(b-1)}, \hat{m}_1''^{(b-1)})$.

Encoding: We apply block-Markov encoding as follows. In block b, the encoders send:

$$\begin{aligned} x_{1b}^r &= x_1^m(m_0^{(b)}, m_0'^{(b)}, m_0''^{(b)}, m_1^{(b)}, m_1'^{(b)}, m_1''^{(b)}) \\ x_{2b}^r &= x_2^m(\hat{m}_0^{(b)}, \hat{m}_0'^{(b)}, \hat{m}_0''^{(b)}, m_2^{(b)}, m_2'^{(b)}) \end{aligned}$$

where $(m_0^{(b)}, m_0'^{(b)}, m_0''^{(b)}) = (m_1^{(b-1)}, m_1'^{(b-1)}, m_1''^{(b-1)})$ and $(\hat{m}_0^{(b)}, \hat{m}_0'^{(b)}, \hat{m}_0''^{(b)}) = (\hat{m}_1^{(b-1)}, \hat{m}_1'^{(b-1)}, \hat{m}_1''^{(b-1)})$. We also assume that the encoders and decoder have access to $(M_0^{(1)}, M_0'^{(1)}, M_0''^{(1)}, M_1^{(B)}, M_1'^{(B)}, M_1''^{(B)}, M_2^{(B)}, M_2'^{(B)})$ through private common randomness.

Decoding at the receiver: The legitimate receiver waits until all B blocks are transmitted and then performs backward decoding. The decoder first finds $(\hat{\hat{m}}_0^{(B)}, \hat{\hat{m}}_0'^{(B)}, \hat{\hat{m}}_0''^{(B)})$ such that

$$\begin{aligned} (u^r(\hat{\hat{m}}_0^{(B)}, \hat{\hat{m}}_0'^{(B)}, \hat{\hat{m}}_0''^{(B)}), x_1^r(\hat{\hat{m}}_0^{(B)}, \hat{\hat{m}}_0'^{(B)}, \hat{\hat{m}}_0''^{(B)}, \hat{\hat{m}}_1^{(B)}, \hat{\hat{m}}_1'^{(B)}, \hat{\hat{m}}_1''^{(B)}), \\ x_2^r(\hat{\hat{m}}_0^{(B)}, \hat{\hat{m}}_0'^{(B)}, \hat{\hat{m}}_0''^{(B)}, \hat{\hat{m}}_2^{(B)}, \hat{\hat{m}}_2'^{(B)}), y_B^r) \in \mathcal{T}_\epsilon^{(r)}(P_{U,X_1,X_2,Y}). \end{aligned}$$

Assuming that $(m_0^{(B)}, m_0'^{(B)}, m_0''^{(B)})$, $(m_0^{(B-1)}, m_0'^{(B-1)}, m_0''^{(B-1)})$, $\ldots$, $(m_0^{(b+1)}, m_0'^{(b+1)}, m_0''^{(b+1)})$ have been decoded, the decoder sets $(\hat{\hat{m}}_1^{(b)}, \hat{\hat{m}}_1'^{(b)}, \hat{\hat{m}}_1''^{(b)}) = (\hat{\hat{m}}_0^{(b+1)}, \hat{\hat{m}}_0'^{(b+1)}, \hat{\hat{m}}_0''^{(b+1)})$ and finds $(\hat{\hat{m}}_0^{(b)}, \hat{\hat{m}}_0'^{(b)}, \hat{\hat{m}}_0''^{(b)})$ and $(\hat{\hat{m}}_2^{(b)}, \hat{\hat{m}}_2'^{(b)})$ such that

$$\begin{aligned} (u^r(\hat{\hat{m}}_0^{(b)}, \hat{\hat{m}}_0'^{(b)}, \hat{\hat{m}}_0''^{(b)}), x_1^r(\hat{\hat{m}}_0^{(b)}, \hat{\hat{m}}_0'^{(b)}, \hat{\hat{m}}_0''^{(b)}, \hat{\hat{m}}_1^{(b)}, \hat{\hat{m}}_1'^{(b)}, \hat{\hat{m}}_1''^{(b)}), \\ x_2^r(\hat{\hat{m}}_0^{(b)}, \hat{\hat{m}}_0'^{(b)}, \hat{\hat{m}}_0''^{(b)}, \hat{\hat{m}}_2^{(b)}, \hat{\hat{m}}_2'^{(b)}), y_b^r) \in \mathcal{T}_\epsilon^{(r)}(P_{U,X_1,X_2,Y}). \end{aligned}$$

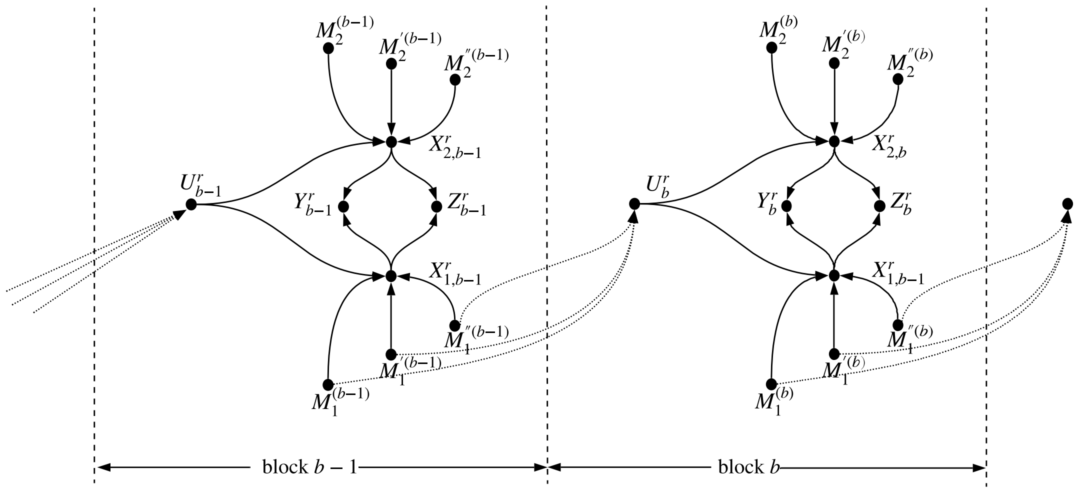

Figure 3.10. Functional dependence graph for the block-Markov encoding scheme for MAC with one-sided strictly-causal cribbing.

Probability of error analysis: Using the arguments for error analysis from [35, Lemma 4], the probability of error of each block vanishes exponentially with r and in turn vanishes across blocks if

$$R_1 + \rho_1' + \rho_1'' < H(X_1|U), \tag{3.55}$$

$$R_2 + \rho_2 < I(X_2; Y|X_1, U), \tag{3.56}$$

$$R_1 + \rho_1' + \rho_1'' + R_2 + \rho_2 < I(X_1, X_2; Y). \tag{3.57}$$

Secrecy analysis: Let $\bar{P}$ be the probability induced when both encoders use $(M_0^{(b)}, M_0'^{(b)}, M_0''^{(b)})$. Let P be the probability when Encoder 1 uses $(M_0^{(b)}, M_0'^{(b)}, M_0''^{(b)})$ and Encoder 2 uses the estimate $(\hat{M}_0^{(b)}, \hat{M}_0'^{(b)}, \hat{M}_0''^{(b)})$. For the secrecy analysis, we find conditions so that $I(M_0^{(b)}, M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)}, \hat{M}_0^{(b)}, \hat{M}_0'^{(b)}, M_2^{(b)}; Z_b^r)$ vanishes exponentially with r. This is motivated by:

- $(M_1^{(b)}, M_0^{(b)}, \hat{M}_0^{(b)}, M_2^{(b)})$ are the Encoder 1 secret message in the present and the past, the estimate of the latter (at Encoder 2), and Encoder 2 secret message, which must be kept secret from Z_b^r, obviously.

- $(M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)})$ must be kept independent of Z_b^r according to the functional dependence graph (Figure 3.10) to ensure the distribution of Z remains i.i.d. across blocks
- $\hat{M}_0'^{(b)}$ is kept independent from Z_b^r to allow Encoder 1 to possess a *local* randomness that is separate from the common randomness shared with Encoder 2: Resolvability analysis showed us that having a local randomness at Encoder 1 can be beneficial for achievable rates.

Let $\bar{I}(\cdot;\cdot)$ be the mutual information according to $\bar{P}$

$$\begin{aligned}
&\bar{I}(M_0^{(b)}, M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)}, \hat{M}_0^{(b)}, \hat{M}_0'^{(b)}, M_2^{(b)}; Z_b^r) \\
&\qquad = \mathbb{D}(\bar{P}_{M_0^{(b)} M_1^{(b)} M_1'^{(b)} M_1''^{(b)} \hat{M}_0^{(b)} \hat{M}_0'^{(b)} M_2^{(b)} Z_b^r} || \bar{P}_{M_0^{(b)} M_1^{(b)} M_1'^{(b)} M_1''^{(b)} \hat{M}_0^{(b)} \hat{M}_0'^{(b)} M_2^{(b)}} \bar{P}_{Z_b^r}) \\
&\qquad \leq \mathbb{D}(\bar{P}_{M_0^{(b)} M_1^{(b)} M_1'^{(b)} M_1''^{(b)} \hat{M}_0^{(b)} \hat{M}_0'^{(b)} M_2^{(b)} Z_b^r} || \bar{P}_{M_0^{(b)} M_1^{(b)} M_1'^{(b)} M_1''^{(b)} \hat{M}_0^{(b)} \hat{M}_0'^{(b)} M_2^{(b)}} Q_Z^{\otimes r}) \qquad (3.58)
\end{aligned}$$

$\mathbb{D}(\bar{P}_{M_0^{(b)} M_1^{(b)} M_1'^{(b)} M_1''^{(b)} \hat{M}_0^{(b)} \hat{M}_0'^{(b)} M_2^{(b)} Z_b^r} || \bar{P}_{M_0^{(b)} M_1^{(b)} M_1'^{(b)} M_1''^{(b)} \hat{M}_0^{(b)} \hat{M}_0'^{(b)} M_2^{(b)}} Q_Z^{\otimes r})$ can be shown, similar to Section 3.4.11, to vanish exponentially with r if:

$$\rho_1'' > I(U; Z), \qquad (3.59)$$

$$\rho_1' + \rho_1'' > I(U, X_1; Z), \qquad (3.60)$$

$$\rho_1' + \rho_1'' + \rho_2 > I(X_1, X_2; Z), \qquad (3.61)$$

$$\rho_1'' + \rho_2 > I(U, X_2; Z). \qquad (3.62)$$

Define $M^{(a:b)} = \{M^{(a)}, \dots, M^{(b)}\}$ and $Z^{(1:b),r} = \{Z_1^r, \dots, Z_b^r\}$.

$$\begin{aligned}
&\bar{I}(M_1^{(1:b)}, M_2^{(1:b)}; Z^{(1:b),r}) \\
&\leq \bar{I}(M_0^{(b)}, M_1^{(1:b)}, M_1'^{(b)}, M_1''^{(b)}, \hat{M}_0^{(b)}, \hat{M}_0'^{(b)}, M_2^{(1:b)}; Z^{(1:b),r}) \qquad (3.63) \\
&= \bar{I}(M_0^{(b)}, M_1^{(1:b)}, M_1'^{(b)}, M_1''^{(b)}, \hat{M}_0^{(b)}, \hat{M}_0'^{(b)}, M_2^{(1:b)}; Z_b^r) \\
&\quad + \bar{I}(M_0^{(b)}, M_1^{(1:b)}, M_1'^{(b)}, M_1''^{(b)}, \hat{M}_0^{(b)}, \hat{M}_0'^{(b)}, M_2^{(1:b)}; Z^{(1:b-1),r} | Z_b^r) \qquad (3.64)
\end{aligned}$$

$$
\begin{aligned}
&= \bar{I}(M_0^{(b)}, M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)}, \hat{M}_0^{(b)}, \hat{M}_0'^{(b)}, M_2^{(b)}; Z_b^r) \\
&\quad + \bar{I}(M_1^{(1:b-1)}, M_2^{(1:b-1)}; Z_b^r | M_0^{(b)}, M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)}, \hat{M}_0^{(b)}, \hat{M}_0'^{(b)}, M_2^{(b)}) \\
&\quad + \bar{I}(M_0^{(b)}, M_1^{(1:b)}, M_1'^{(b)}, M_1''^{(b)}, \hat{M}_0^{(b)}, \hat{M}_0'^{(b)}, M_2^{(1:b)}; Z^{(1:b-1),r} | Z_b^r) \qquad (3.65) \\
&\leq \bar{I}(M_0^{(b)}, M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)}, \hat{M}_0^{(b)}, \hat{M}_0'^{(b)}, M_2^{(b)}; Z_b^r) \\
&\quad + \bar{I}(M_1^{(1:b-1)}, M_2^{(1:b-1)}; M_1''^{(b-1)}, Z_b^r | M_0^{(b)}, M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)}, \hat{M}_0^{(b)}, \hat{M}_0'^{(b)}, M_2^{(b)}) \\
&\quad + \bar{I}(M_0^{(b)}, M_1^{(1:b)}, M_1'^{(b)}, M_1''^{(b)}, \hat{M}_0^{(b)}, \hat{M}_0'^{(b)}, M_2^{(1:b)}; Z^{(1:b-1),r} | Z_b^r) \qquad (3.66) \\
&\overset{(a)}{=} \bar{I}(M_0^{(b)}, M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)}, \hat{M}_0^{(b)}, \hat{M}_0'^{(b)}, M_2^{(b)}; Z_b^r) \\
&+\bar{I}(M_1^{(1:b-1)}, M_2^{(1:b-1)}; Z_b^r | M_0^{(b)}, M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)}, \hat{M}_0^{(b)}, \hat{M}_0'^{(b)}, M_2^{(b)}, M_1^{(b-1)}, M_1'^{(b-1)}, M_1''^{(b-1)}) \\
&+ \bar{I}(M_0^{(b)}, M_1^{(1:b)}, M_1'^{(b)}, M_1''^{(b)}, \hat{M}_0^{(b)}, \hat{M}_0'^{(b)}, M_2^{(1:b)}; Z^{(1:b-1),r} | Z_b^r) \qquad (3.67) \\
&\overset{(b)}{\leq} 2^{-\alpha r} + \bar{I}(M_0^{(b)}, M_1^{(1:b)}, M_1'^{(b)}, M_1''^{(b)}, \hat{M}_0^{(b)}, \hat{M}_0'^{(b)}, M_2^{(1:b)}; Z^{(1:b-1),r} | Z_b^r) \qquad (3.68) \\
&\leq 2^{-\alpha r} \\
&+\bar{I}(M_0^{(b)},M_1^{(1:b)},M_1'^{(b)},M_1''^{(b)},\hat{M}_0^{(b)},\hat{M}_0'^{(b)},M_2^{(1:b)}, Z_b^r,M_0^{(b-1)},M_1'^{(b-1)},M_1''^{(b-1)},\hat{M}_0^{(b-1)}, \hat{M}_0'^{(b-1)};Z^{(1:b-1),r}) \\
&\qquad (3.69) \\
&\overset{(c)}{=} 2^{-\alpha r} + \bar{I}(M_0^{(b-1)}, M_1^{(1:b-1)}, M_1'^{(b-1)}, M_1''^{(b-1)}, \hat{M}_0^{(b-1)}, \hat{M}_0'^{(b-1)}, M_2^{(1:b-1)}; Z^{(1:b-1),r}) \qquad (3.70) \\
&\overset{(d)}{\leq} b \times 2^{-\alpha r}
\end{aligned}
$$

Therefore $\bar{I}(M_1, M_2; Z^n) \leq B \times 2^{-\alpha r}$ where,

(a) holds because $M_0^{(b)} = \hat{M}_0^{(b)} = M_1^{(b-1)}$, $\hat{M}_0'^{(b)} = M_1'^{(b-1)}$ and $M_1''^{(b-1)}$ is independent of $(M_1^{(1:b-1)}, M_2^{(1:b-1)})$ by construction;

(b) holds because $\bar{I}(M_0^{(b)}, M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)}, \hat{M}_0^{(b)}, \hat{M}_0'^{(b)}, M_2^{(b)}; Z_b^r) \leq 2^{-\alpha r}$ by (3.58)-(3.62) and $M_1^{(1:b-1)}, M_2^{(1:b-1)} \to M_0^{(b)}, M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)}, \hat{M}_0^{(b)}, \hat{M}_0'^{(b)}, M_2^{(b)}, M_1^{(b-1)}, M_1'^{(b-1)}, M_1''^{(b-1)} \to Z_b^r$ (see Figure 3.10);

(c) holds because $M_0^{(b)}, M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)}, \hat{M}_0^{(b-1)}, \hat{M}_0'^{(b)}, M_2^{(b)}, Z_b^r \to M_0^{(b-1)}, M_1^{(1:b-1)}, M_1'^{(b-1)}, M_1''^{(b-1)}, \hat{M}_0^{(b-1)}, \hat{M}_0'^{(b-1)}, M_2^{(1:b-1)} \to Z^{(1:b-1),r}$ (see Figure 3.10).

(d) holds by repeating (3.63)-(3.70) $b-1$ times.

Next we show that $I(M_1^{(1:b)}, M_2^{(1:b)}; Z^{(1:b),r})$ is not too different from $\bar{I}(M_1^{(1:b)}, M_2^{(1:b)}; Z^{(1:b),r})$.

$$\begin{aligned}
&I(M_1^{(1:b)}, M_2^{(1:b)}; Z^{(1:b),r}) \\
&\quad = \mathbb{D}(P_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}} || P_{M_1^{(1:b)} M_2^{(1:b)}} P_{Z^{(1:b),r}}) \\
&\quad \overset{(a)}{\leq} \mathbb{D}(P_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}} || P_{M_1^{(1:b)} M_2^{(1:b)}} Q_Z^{\otimes br}) \\
&\quad = \sum_{m_1^{(1:b)}, m_2^{(1:b)}, z^{(1:b),r}} P(m_1^{(1:b)}, m_2^{(1:b)}, z^{(1:b),r}) \log \frac{P(m_1^{(1:b)}, m_2^{(1:b)}, z^{(1:b),r})}{\bar{P}(m_1^{(1:b)}, m_2^{(1:b)}, z^{(1:b),r})} \\
&\qquad\quad + \sum_{m_1^{(1:b)}, m_2^{(1:b)}, z^{(1:b),r}} P(m_1^{(1:b)}, m_2^{(1:b)}, z^{(1:b),r}) \log \frac{\bar{P}(m_1^{(1:b)}, m_2^{(1:b)}, z^{(1:b),r})}{P(m_1^{(1:b)}, m_2^{(1:b)}) Q_Z^{\otimes br}} \\
&\qquad\quad + \mathbb{D}(\bar{P}_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b,r)}} || P_{M_1^{(1:b)} M_2^{(1:b)}} Q_Z^{\otimes br}) - \mathbb{D}(\bar{P}_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}} || P_{M_1^{(1:b)} M_2^{(1:b)}} Q_Z^{\otimes br}) \\
&\quad = \mathbb{D}(P_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}} || \bar{P}_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}}) + \mathbb{D}(\bar{P}_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}} || P_{M_1^{(1:b)} M_2^{(1:b)}} Q_Z^{\otimes br}) \\
&\qquad\quad + \sum_{m_1^{(1:b)}, m_2^{(1:b)}, z^{(1:b),r}} (P_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}} - \bar{P}_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}}) \log \frac{\bar{P}(m_1^{(1:b)}, m_2^{(1:b)}, z^{(1:b),r})}{P(m_1^{(1:b)}, m_2^{(1:b)}) Q_Z^{\otimes br}} \\
&\quad \overset{(b)}{\leq} \mathbb{D}(P_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}} || \bar{P}_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}}) + \mathbb{D}(\bar{P}_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}} || \bar{P}_{M_1^{(1:b)} M_2^{(1:b)}} Q_Z^{\otimes br}) \\
&\qquad\quad + \log \frac{1}{\mu} \mathbb{V}(P_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}}, \bar{P}_{M_1^{(1:b)} M_2^{(1:b)} Z^{b,r}}) \\
&\quad \overset{(c)}{\leq} 2 \log \frac{1}{\mu} \mathbb{V}(P_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}}, \bar{P}_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}}) + \mathbb{D}(\bar{P}_{M_1^{(1:b)} M_2^{(1:b)} Z^{b,r}} || \bar{P}_{M_1^{(1:b)} M_2^{(1:b)}} \bar{P}_{Z^{(1:b),r}}) \\
&\qquad\quad + \mathbb{D}(\bar{P}_{Z^{(1:b),r}} || Q_Z^{\otimes br}) \\
&\quad = 2 \log \frac{1}{\mu} \mathbb{V}(P_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}}, \bar{P}_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}}) + \bar{I}(M_1^{(1:b)}, M_2^{(1:b)}; Z^{(1:b),r}) \\
&\qquad\quad + \mathbb{D}(\bar{P}_{Z^{(1:b),r}} || Q_Z^{\otimes br}) \qquad (3.71)
\end{aligned}$$

where

(a) follows by adding $\mathbb{D}(P_{Z^{b,r}} || Q_Z^{\otimes br})$;

(b) follows because $\bar{P}_{M_1^{(1:b)},M_2^{(1:b)}} = P_{M_1^{(1:b)},M_2^{(1:b)}}$, $(P_{M_1^{(1:b)}M_2^{(1:b)}Z^{(1:b),r}} - \bar{P}_{M_1^{(1:b)}M_2^{(1:b)}Z^{(1:b),r}}) \leq |P_{M_1^{(1:b)}M_2^{(1:b)}Z^{(1:b),r}} - \bar{P}_{M_1^{(1:b)}M_2^{(1:b)}Z^{(1:b),r}}|$ and by defining $\mu \triangleq \min_{z^{b,r}} Q_Z^{\otimes br}(z^{b,r})$;

(c) follows by Lemma 2 and because $\mathbb{D}(\bar{P}_{M_1^{(1:b)}M_2^{(1:b)}Z^{(1:b),r}}||\bar{P}_{M_1^{(1:b)}M_2^{(1:b)}}Q_Z^{\otimes br}) = \mathbb{D}(\bar{P}_{M_1^{(1:b)}M_2^{(1:b)}Z^{b,r}}||\bar{P}_{M_1^{(1:b)}M_2^{(1:b)}}\bar{P}_{Z^{(1:b),r}}) + \mathbb{D}(\bar{P}_{Z^{(1:b),r}}||Q_Z^{\otimes br})$.

The first and third terms of (3.71) vanish exponentially with br similar to Section 3.4.1.

We now derive an achievable rate region by choosing values for ρ_1', ρ_1'', ρ_2, R_1 and R_2 that satisfy the constraints for secrecy and probability of error. We find it more convenient to separately derive achievable rate regions under the two conditions $H(X_1|U) \lessgtr I(U, X_1; Y)$, and then merge them.

When $H(X_1|U) > I(U, X_1; Y)$, The following rates satisfy all error and secrecy constraints:

$$\begin{aligned}
\rho_1'' &= I(U; Z) + \epsilon,\\
\rho_1' &= I(X_1; Z|U) + \epsilon,\\
\rho_2 &= I(X_2; Z|X_1, U) + \epsilon,\\
R_1 &= H(X_1|U) - I(U, X_1; Z) - 2\epsilon,\\
R_2 &= I(X_1, X_2; Y) - I(X_2; Z|X_1, U) - H(X_1|U) - \epsilon,
\end{aligned}$$

and the same is true for the following rates:

$$\begin{aligned}
\rho_1'' &= I(U, X_2; Z) + \epsilon,\\
\rho_1' &= I(X_1, X_2; Z) - I(U, X_2; Z) + \epsilon,\\
\rho_2 &= \epsilon,\\
R_1 &= I(X_1, X_2; Y) - I(X_2; Y|X_1, U) - I(X_1, X_2; Z) - 2\epsilon,\\
R_2 &= I(X_2; Y|X_1, U) - \epsilon.
\end{aligned}$$

Considering the above two corner points, the following rate region is achievable.

$$\begin{aligned} R_1 &\leq H(X_1|U) - I(U, X_1; Z) \\ R_2 &\leq I(X_2; Y|X_1, U) \\ R_1 + R_2 &\leq I(X_1, X_2; Y) - I(X_1, X_2; Z) \end{aligned}$$

which is identical to Eq. (3.15) absent one of the two sum rate constraints.

When $H(X_1|U) \leq I(U, X_1; Y)$, the following rates satisfy all error and secrecy constraints:

$$\begin{aligned} \rho_1'' &= I(U; Z) + \epsilon, \\ \rho_1' &= I(X_1; Z|U) + \epsilon, \\ \rho_2 &= I(X_2; Z|X_1, U) + \epsilon, \\ R_1 &= H(X_1|U) - I(U, X_1; Z) - 2\epsilon, \\ R_2 &= I(X_2; Y|X_1, U) - I(X_2; Z|X_1, U) - \epsilon, \end{aligned}$$

and the same is true for the following rates:

$$\begin{aligned} \rho_1'' &= I(U, X_2; Z) + \epsilon, \\ \rho_1' &= I(X_1, X_2; Z) - I(U, X_2; Z) + \epsilon, \\ \rho_2 &= \epsilon, \\ R_1 &= H(X_1|U) - I(X_1, X_2; Z) - 2\epsilon, \\ R_2 &= I(X_2; Y|X_1, U) - \epsilon. \end{aligned}$$

Considering the above two corner points, the following rate region is achievable.

$$\begin{aligned} R_1 &\leq H(X_1|U) - I(U, X_1; Z) \\ R_2 &\leq I(X_2; Y|X_1, U) \\ R_1 + R_2 &\leq H(X_1|U) + I(X_2; Y|X_1, U) - I(X_1, X_2; Z) \end{aligned}$$

which is again identical to Eq. (3.18) absent one of the two sum rate constraints.

Thus far, we have two achievable rate regions for the two conditions $H(X_1|U) \lesseqgtr I(U, X_1; Y)$, and the overall achievable rate region is usually specified as the union of the two. However, a more compact representation is possible via the following useful information inequality:

$$H(X_1|U) \lesseqgtr I(U, X_1; Y) \quad \Rightarrow \quad H(X_1|U) + I(X_2; Y|X_1, U) \lesseqgtr I(X_1, X_2; Y)$$

which holds because of $I(X_1, X_2; Y) = I(U, X_1, X_2; Y)$ and the chain rule. It then follows that the smaller of the two derived sum rate constraints is always active. Therefore we can simplify the expression of the achievable region by using the intersection of the two sum rate constraints.

This concludes the proof of Proposition 8.

3.4.3 Channel resolvability of MAC with one-sided causal cribbing

Achievability:

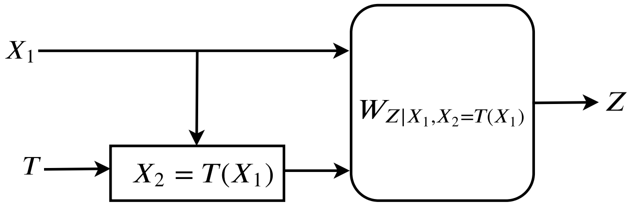

Figure 3.11. MAC induced by Shannon strategy.

The proof of MAC with causal cribbing is similar to MAC with strictly-causal cribbing, however, we use a Shannon strategy to generate X_2 rather than codewords [32]. Let $\mathscr{T} \triangleq \mathcal{X}_2^{|\mathcal{X}_1|}$ be the set of all strategies that map $\mathcal{X}_1$ into $\mathcal{X}_2$, and for $t \in \mathcal{T}$ denote by $t(x_1) \in \mathcal{X}_2$ the image of $x_1 \in \mathcal{X}_1$. See Figure 3.11 for illustration. The MAC induced by the Shannon strategy is denoted by $(\mathcal{X}_1 \times \mathscr{T}, W^+_{Z|X_1,T}, \mathcal{Z})$ where $W^+_{Z|X_1,T} \triangleq W_{Z|X_1,X_2=T(X_1)}$.

By Theorem 5, rate pairs (R_1, R_2) satisfying the following conditions are achievable for MAC with strictly-causal cribbing.

$$R_1 > I(U, X_1; Z), \tag{3.72}$$

$$R_2 > I(X_1, T; Z) - H(X_1|U), \tag{3.73}$$

$$R_1 + R_2 > I(X_1, T; Z), \tag{3.74}$$

with $H(X_1|U) > I(U, X_1; Z)$ for any joint distribution $P_{UX_1TZ} \triangleq P_U P_{X_1|U} P_{T|U} W^+_{Z|X_1T}$ with marginal Q_Z. Therefore, for MAC with causal cribbing the rate pairs (R_1, R_2) in (3.72)-(3.74) must be achievable. Restricting the distribution to satisfy $P_{UX_1TZ} \triangleq P_U P_{X_1} P_T W^+_{Z|X_1T}$ yields:

$$\begin{aligned} H(X_1|U) &= H(X_1), \\ I(U, X_1; Z) &= I(X_1; Z), \\ I(X_1, T; Z) &= I(X_1, X_2, T; Z) = I(X_1, X_2; Z), \end{aligned}$$

and $P(x_1, x_2, z) = P(x_1) \sum_{t:t(x_1)=x_2} P(t) W(z|x_1, x_2)$. This is possible because of the fact that for an arbitrary distribution $P^*(x_1, x_2)$, there always exists a product distribution $P(x_1, t) = P(x_1)P(t)$ such that $P^*(x_1, x_2) = P(x_1) \sum_{t:t(x_1)=x_2} P(t)$. This is achieved by choosing [32, Eq. (44)]

$$\begin{aligned} P(x_1) &= \sum_{x_2} P^*(x_1, x_2), \\ P(t) &= \prod_{x_1} \frac{P^*(x_1, x_2 = t(x_1))}{P(x_1)}. \end{aligned}$$

Note that the constraint $H(X_1|U) > I(U, X_1; Z)$ is now automatically satisfied if $H(X_1|Z) > 0$. From the above we conclude that all rate pairs (R_1, R_2) satisfying the following conditions are achievable for MAC with causal cribbing.

$$\begin{aligned} R_1 &> I(X_1; Z), \\ R_2 &> I(X_1, X_2; Z) - H(X_1), \end{aligned}$$

$$R_1 + R_2 > I(X_1, X_2; Z),$$

with $H(X_1|Z) > 0$ for any joint distribution $P_{X_1,X_2,Z} \triangleq P_{X_1,X_2}W_{Z|X_1,X_2}$ with marginal Q_Z.

The achievability scheme presented thus far depends on $H(X_1|Z) > 0$. The same achievable rates can be attained for $H(X_1|Z) = 0$, however, a different scheme is required for this extremal case, which is presented below.

Consider a distribution $P(x_1, x_2) = P(x_1)P(x_2|x_1)$ such that $\sum_{x_1,x_2} P(x_1, x_2)W(z|x_1, x_2) = Q_Z$.

- Independently generate 2^{nR_1} codewords x_1^n each with probability $P(x_1^n)$. Label them $x_1^n(m_1)$, $m_1 \in [\![1, 2^{nR_1}]\!]$.
- For every $x_1^n(m_1)$, independently generate 2^{nR_2} codewords x_2^n each with probability $P(x_2^n|x_1^n(m_1)) = P^{\otimes n}_{X_2|X_1(m_1)}(x_2^n|x_1^n(m_1))$. Label them $x_2^n(x_1^n(m_1), m_2)$, $m_2 \in [\![1, 2^{nR_2}]\!]$.

This defines the codebook

$$\mathcal{C}_n = \{x_1^n(m_1), x_2^n(x_1^n(m_1), m_2), m_1 \in [\![1, 2^{nR_1}]\!], m_2 \in [\![1, 2^{nR_2}]\!]\} \tag{3.75}$$

and we denote the random codebook by

$$\mathfrak{C}_n = \{X_1^n(m_1), X_2^n(X_1^n(m_1), m_2), m_1 \in [\![1, 2^{nR_1}]\!], m_2 \in [\![1, 2^{nR_2}]\!]\} \tag{3.76}$$

The average KL divergence is:

$$\begin{aligned}
\mathbb{E}_{\mathfrak{C}_n}\left(\mathbb{D}(P_{Z^n}||Q_Z^{\otimes n})\right) &= \mathbb{E}_{\mathfrak{C}_n}\left(\sum_{z^n}\sum_{x_1^n} P(x_1^n, z^n) \log \frac{\sum_{x_1^n} P(x_1^n, z^n)}{\sum_{x_1^n} Q^{\otimes n}_{X_1,Z}(x_1^n, z^n)}\right)\\
&\overset{(a)}{\leq} \mathbb{E}_{\mathfrak{C}_n}\left(\sum_{z^n}\sum_{x_1^n} P(x_1^n, z^n) \log \frac{P(x_1^n, z^n)}{Q^{\otimes n}_{X_1,Z}(x_1^n, z^n)}\right)\\
&= \mathbb{E}_{\mathfrak{C}_n}\left(\mathbb{D}(P_{X_1^n,Z^n}||Q^{\otimes n}_{X_1,Z})\right)\\
&\overset{(b)}{=} \mathbb{E}_{\mathfrak{C}_n}\left(\mathbb{D}(P_{Z^n|X_1^n}||Q^{\otimes n}_{Z|X_1}|P_{X_1^n})\right) + \mathbb{E}_{\mathfrak{C}_n}\left(\mathbb{D}(P_{X_1^n}||P^{\otimes n}_{X_1})\right)
\end{aligned} \tag{3.77}$$

where

$Q_{X_1,Z} = \sum_{x_2} P(x_1, x_2)W(z|x_1, x_2)$;

(a) follows by the log-sum inequality;

(b) follows from the chain rule of KL divergence.

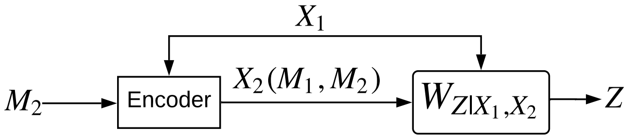

Figure 3.12. State-dependent point-to-point channel.

Let $R_1 > H(X_1)$, in which case the second term of (3.77) vanishes as $n \to \infty$ and the channel is effectively a state-dependent point-to-point channel (Fig. 3.12). Using similar bounding techniques as those used earlier in this dissertation (e.g. the proof of (3.24)-(3.27)), the first term of (3.77) vanishes as $n \to \infty$ if $R_2 > I(X_2; Z|X_1)$. Since $H(X_1|Z) = 0$, the achievable region is

$$\begin{aligned} R_1 &> H(X_1) = I(X_1; Z), \\ R_2 &> I(X_2; Z|X_1) = I(X_1, X_2; Z) - H(X_1), \\ R_1 + R_2 &> H(X_1) + I(X_2; Z|X_1) = I(X_1, X_2; Z). \end{aligned}$$

Converse:

Since MAC with causal cribbing is a special case of MAC with non-causal cribbing, it follows that the converse of the latter holds for the causal cribbing scenario. The converse of MAC with non-causal cribbing is presented in 3.4.5

3.4.4 Strong secrecy of MAC with one-sided causal cribbing

Achievability:

This proof is similar to the achievability proof of the strictly-causal case and we again use a Shannon strategy for generating X_2 rather than codewords [32]. Using the same notation as in Section 3.4.3 for the strategies T, we find from Proposition 8 that rate pairs (R_1, R_2) satisfying the following secrecy are achievable with strictly-causal cribbing:

$$
\begin{aligned}
R_1 &< H(X_1|U) - I(U, X_1; Z),\\
R_2 &< I(T; Y|X_1, U),\\
R_1 + R_2 &< I(X_1, T; Y) - I(X_1, T; Z),
\end{aligned}
$$

for any joint distribution $P_{UX_1TYZ} \triangleq P_U P_{X_1|U} P_{T|U} W^{+}_{YZ|X_1T}$ with marginal Q_Z. Restricting the distribution to satisfy $P_{UX_1TYZ} \triangleq P_U P_{X_1} P_T W^{+}_{YZ|X_1T}$ yields:

$$
\begin{aligned}
H(X_1|U) &= H(X_1),\\
I(U, X_1; Z) &= I(X_1; Z)\\
I(T; Y|X_1, U) &= I(T, X_2; Y|X_1, U) = I(X_2; Y|X_1),\\
I(X_1, T; Y) &= I(X_1, X_2, T; Y) = I(X_1, X_2; Y),\\
I(X_1, T; Z) &= I(X_1, X_2, T; Z) = I(X_1, X_2; Z),
\end{aligned}
$$

and $P(x_1, x_2, y, z) = P(x_1) \sum_{t:t(x_1)=x_2} P(t) W(y, z|x_1, x_2)$. To complete the proof, we again follow [32, Eq. (44)] to note that for an arbitrary distribution $P^*(x_1, x_2)$ there exists a product distribution $P(x_1, t) = P(x_1)P(t)$ such that $P^*(x_1, x_2) = P(x_1) \sum_{t:t(x_1)=x_2} P(t)$.

3.4.5 Channel resolvability of MAC with one-sided non-causal cribbing

Achievability:

Codebook generation: Consider a distribution $P(x_1, x_2) = P(x_1)P(x_2|x_1)$ such that $\sum_{x_1,x_2} P(x_1, x_2) W(z|x_1, x_2) = Q_Z(z)$.

- Independently generate 2^{nR_1} codewords x_1^n each with probability $P(x_1^n) = P_{X_1}^{\otimes n}(x_1^n)$. Label them $x_1^n(m_1)$, $m_1 \in [\![1, 2^{nR_1}]\!]$.

- For every $x_1^n(m_1)$, independently generate 2^{nR_2} codewords x_2^n each with probability $P(x_2^n|x_1^n(m_1)) = P_{X_2|X_1}^{\otimes n}(x_2^n|x_1^n(m_1))$. Label them $x_2^n(x_1^n(m_1), m_2)$, $m_2 \in [\![1, 2^{nR_2}]\!]$.

This defines the codebook

$$\mathcal{C}_n = \{x_1^n(m_1), x_2^n(x_1^n(m_1), m_2), m_1 \in [\![1, 2^{nR_1}]\!], m_2 \in [\![1, 2^{nR_2}]\!]\} \tag{3.78}$$

and we denote the random codebook by

$$\mathfrak{C}_n = \{X_1^n(m_1), X_2^n(X_1^n(m_1), m_2), m_1 \in [\![1, 2^{nR_1}]\!], m_2 \in [\![1, 2^{nR_2}]\!]\} \tag{3.79}$$

The average KL divergence is:

$$\begin{aligned}
&\mathbb{E}_{\mathfrak{C}_n}\big(\mathbb{D}(P_{Z^n}||Q_Z^{\otimes n})\big)\\
&= \mathbb{E}_{\mathfrak{C}_n}\big(\sum_{z^n} P_{Z^n}(z^n) \log \frac{P_{Z^n}(z^n)}{Q_Z^{\otimes n}(z^n)}\big)\\
&= \mathbb{E}_{\mathfrak{C}_n}\Bigg(\sum_{z^n} \frac{1}{2^{n(R_1+R_2)}} \sum_{m_1,m_2} W^{\otimes n}(z^n|X_1^n(m_1), X_2^n(X_1^n(m_1), m_2))\\
&\qquad\qquad\qquad \log \frac{\sum_{m_1',m_2'} W^{\otimes n}(z^n|X_1^n(m_1'), X_2^n(X_1^n(m_1'), m_2'))}{2^{n(R_1+R_2)}Q_Z^{\otimes n}(z^n)}\Bigg)\\
&= \sum_{x_1^n(1)} \sum_{x_2^n(x_1^n(1),1)} \cdots \sum_{x_1^n(2^{nR_1})} \sum_{x_2^n(x_1^n(2^{nR_1}),2^{nR_2})} \prod_{(k_1,k_2)=(1,1)}^{(2^{nR_1},2^{nR_2})} P(x_1^n(k_1), x_2^n(x_1^n(k_1), k_2))\\
&\qquad\qquad \sum_{z^n} \frac{1}{2^{n(R_1+R_2)}} \sum_{m_1,m_2} W^{\otimes n}(z^n|x_1^n(m_1), x_2^n(x_1^n(m_1), m_2))\\
&\qquad\qquad \log \frac{\sum_{m_1',m_2'} W^{\otimes n}(z^n|x_1^n(m_1'), x_2^n(x_1^n(m_1'), m_2'))}{2^{n(R_1+R_2)}Q_Z^{\otimes n}(z^n)}\\
&=\sum_{z^n} \frac{1}{2^{n(R_1+R_2)}} \sum_{m_1,m_2} \sum_{\substack{x_1^n(m_1),\\ x_2^n(x_1^n(m_1),m_2)}} P(x_1^n(m_1), x_2^n(x_1^n(m_1), m_2))W^{\otimes n}(z^n|x_1^n(m_1), x_2^n(x_1^n(m_1), m_2))\\
&\qquad\qquad \sum_{(k_1,k_2)\neq(m_1,m_2)}^{(2^{nR_1},2^{nR_2})} \sum_{x_1^n(k_1)} \sum_{x_2^n(x_1^n(k_1),k_2)} \prod_{(l_1,l_2)\neq(m_1,m_2)}^{(2^{nR_1},2^{nR_2})} P(x_1^n(l_1), x_2^n(x_1^n(l_1), l_2))\\
&\qquad\qquad \log \frac{\sum_{m_1'} \sum_{m_2'} W^{\otimes n}(z^n|x_1^n(m_1'), x_2^n(x_1^n(m_1'), m_2'))}{2^{n(R_1+R_2)}Q_Z^{\otimes n}(z^n)}
\end{aligned} \tag{3.80}$$

$$
\begin{aligned}
=&\sum_{z^n} \frac{1}{2^{n(R_1+R_2)}} \sum_{m_1,m_2} \sum_{x_1^n(m_1)} \sum_{x_2^n(x_1^n(m_1),m_2)} P(x_1^n(m_1), x_2^n(x_1^n(m_1), m_2), z^n) \\
&\qquad \mathbb{E}_{\setminus(m_1,m_2)} \log \frac{\sum_{m_1'} \sum_{m_2'} W^{\otimes n}(z^n|X_1^n(m_1'), X_2^n(X_1^n(m_1'), m_2'))}{2^{n(R_1+R_2)} Q_Z^{\otimes n}(z^n)}
\end{aligned} \tag{3.81}
$$

$$
\begin{aligned}
\overset{(a)}{\leq}& \frac{1}{2^{n(R_1+R_2)}} \sum_{m_1,m_2} \sum_{z^n} \sum_{x_1^n(m_1)} \sum_{x_2^n(x_1^n(m_1),m_2)} P(x_1^n(m_1), x_2^n(x_1^n(m_1), m_2), z^n) \\
&\qquad \log \mathbb{E}_{\setminus(m_1,m_2)} \frac{\sum\limits_{m_1',m_2'} W^{\otimes n}(z^n|X_1^n(m_1'), X_2^n(X_1^n(m_1'), m_2'))}{2^{n(R_1+R_2)} Q_Z^{\otimes n}(z^n)} \\
=& \frac{1}{2^{n(R_1+R_2)}} \sum_{m_1,m_2} \sum_{z^n} \sum_{x_1^n(m_1)} \sum_{x_2^n(x_1^n(m_1),m_2)} P(x_1^n(m_1), x_2^n(x_1^n(m_1), m_2), z^n) \\
&\quad \log \mathbb{E}_{\setminus(m_1,m_2)} \Bigg(\frac{W^{\otimes n}(z^n|x_1^n(m_1), x_2^n(x_1^n(m_1), m_2))}{2^{n(R_1+R_2)} Q_Z^{\otimes n}(z^n)} \\
&\qquad + \sum_{m_1' \neq m_1} \Big[\mathbb{1}_{\{x_1^n(m_1') = x_1^n(m_1)\}} \frac{W^{\otimes n}(z^n|X_1^n(m_1'), x_2^n(X_1^n(m_1'), m_2))}{2^{n(R_1+R_2)} Q_Z^{\otimes n}(z^n)} \\
&\qquad + \mathbb{1}_{\{x_1^n(m_1') \neq x_1^n(m_1)\}} \frac{W^{\otimes n}(z^n|X_1^n(m_1'), x_2^n(X_1^n(m_1'), m_2))}{2^{n(R_1+R_2)} Q_Z^{\otimes n}(z^n)} \Big] \\
&\qquad + \sum_{m_2' \neq m_2} \frac{W^{\otimes n}(z^n|x_1^n(m_1), X_2^n(x_1^n(m_1), m_2'))}{2^{n(R_1+R_2)} Q_Z^{\otimes n}(z^n)} \\
&\qquad + \sum_{\substack{m_2' \neq m_2 \\ m_1' \neq m_1}} \frac{W^{\otimes n}(z^n|X_1^n(m_1'), X_2^n(X_1^n(m_1'), m_2'))}{2^{n(R_1+R_2)} Q_Z^{\otimes n}(z^n)} \Bigg) \\
\overset{(b)}{\leq}& \frac{1}{2^{n(R_1+R_2)}} \sum_{m_1,m_2} \sum_{z^n} \sum_{x_1^n(m_1)} \sum_{x_2^n(x_1^n(m_1),m_2)} P(x_1^n(m_1), x_2^n(x_1^n(m_1), m_2), z^n) \\
&\quad \log \Bigg(\frac{W^{\otimes n}(z^n|x_1^n(m_1), x_2^n(x_1^n(m_1), m_2))}{2^{n(R_1+R_2)} Q_Z^{\otimes n}(z^n)} \\
&\qquad + \mathbb{E}_{\setminus(m_1,m_2)} \Big(\sum_{m_1' \neq m_1} \Big[\mathbb{1}_{\{x_1^n(m_1') = x_1^n(m_1)\}} \frac{W^{\otimes n}(z^n|X_1^n(m_1'), X_2^n(X_1^n(m_1'), m_2))}{2^{n(R_1+R_2)} Q_Z^{\otimes n}(z^n)} \\
&\qquad + \mathbb{1}_{\{x_1^n(m_1') \neq x_1^n(m_1)\}} \frac{W^{\otimes n}(z^n|X_1^n(m_1'), X_2^n(X_1^n(m_1'), m_2))}{2^{n(R_1+R_2)} Q_Z^{\otimes n}(z^n)} \Big] \Big)
\end{aligned}
$$

$$+\sum_{m_2'\neq m_2}\frac{P^{\otimes n}(z^n|x_1^n(m_1))}{2^{n(R_1+R_2)}Q_Z^{\otimes n}(z^n)}+1\Bigg) \tag{3.82}$$

$$\overset{(c)}{=} \Psi_1+\Psi_2$$

where

(a) follows by Jensen's inequality where $\mathbb{E}\log(\cdot)\leq\log\mathbb{E}(\cdot)$. Recall $\mathbb{E}_{\setminus(m_1,m_2)}(\cdot)$ is the expectation over $X_1^n(i)$ and $X_2^n(X_1^n(i),j)$ for $(i,j)\neq(m_1,m_2)$; $\mathbb{E}_{\setminus(m_1,m_2)}$ to each term inside the bracket;

(b) Ψ_1 is taking the summation $\sum_{x_1^n,x_2^n,z^n}$ in (3.82) over $(x_1^n,x_2^n,z^n)\in\mathcal{T}_\epsilon^n(P_{X_1,X_2,Z})$ and Ψ_2 is taking the same summation over $(x_1^n,x_2^n,z^n)\notin\mathcal{T}_\epsilon^n(P_{X_1,X_2,Z})$.

Hence,

$$\begin{aligned}\Psi_1 \leq \log\Big(&2^{-n(R_1+R_2)}2^{-n(1-\epsilon)H(Z|X_1,X_2)}2^{n(1+\epsilon)H(Z)}+2^{-nR_2}2^{-n(1-\epsilon)(H(X_1)+H(Z|X_1,X_2))}2^{n(1+\epsilon)H(Z)}\\ &+2^{-nR_2}+2^{-nR_1}2^{-n(1-\epsilon)(H(Z|X_1))}2^{n(1+\epsilon)H(Z)}+1\Big) \qquad (3.83)\\ \Psi_2 \leq{}& 2|\mathcal{X}_1||\mathcal{X}_2||\mathcal{Z}|e^{-n\epsilon^2\mu_{X_1X_2Z}}n\log(\frac{4}{\mu_Z}+1) \qquad (3.84)\end{aligned}$$

where

$$\mu_Z=\min_{\substack{z\in\mathcal{Z}\\ \text{s.t. } Q(z)>0}} Q(z)$$

$$\mu_{X_1X_2Z}=\min_{\substack{(x_1,x_2,z)\in(\mathcal{X}_1,\mathcal{X}_2,\mathcal{Z})\\ \text{s.t. } Q(x_1,x_2,z)>0}} Q(x_1,x_2,z)$$

Now $\mathbb{E}(\mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}))\xrightarrow{n\to\infty}0$ if $R_1>I(X_1;Z)+2\epsilon H(Z)$, $R_2>I(X_1,X_2;Z)-H(X_1)+2\epsilon H(Z)$ and $R_1+R_2>I(X_1,X_2;Z)+2\epsilon H(Z)$. This implies, by Markov's inequality, that $\Pr(\mathbb{D}(P_{Z^n}||Q_Z^{\otimes n})>\eta_n)\xrightarrow{n\to\infty}0$ for a suitable choice of η_n; $\eta_n=e^{-n\alpha}$ for $\alpha>0$.

Converse:

We consider a $(2^{nR_1}, 2^{nR_2}, n)$ code such that $\mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) \leq \epsilon$, where $\epsilon \xrightarrow{n\to\infty} 0$.

By assumption,

$$\begin{aligned}
\epsilon &\geq \mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) \\
&= \sum_{z^n} P(z^n) \log \frac{P(z^n)}{Q_Z^{\otimes n}(z^n)} \\
&= \sum_{i=1}^{n} \Big(\sum_{z_i} P_Z(z_i) \log \frac{1}{Q(z_i)} - H(Z_i|Z^{i-1}) \Big) \\
&\overset{(a)}{\geq} \sum_{i=1}^{n} \Big(\sum_{z_i} P(z_i) \log \frac{1}{Q(z_i)} - H(Z_i) \Big) \\
&= \sum_{i=1}^{n} \mathbb{D}(P_{Z_i}||Q_Z) \\
&\overset{(b)}{\geq} n\mathbb{D}(\tilde{P}_Z||Q_Z)
\end{aligned}$$

where

(a) follows because conditioning does not increase entropy;

(b) follows by Jensen's inequality and the convexity of $\mathbb{D}(\cdot||\cdot)$ with $\tilde{P}_Z(z) \triangleq \frac{1}{n}\sum_{i=1}^{n} P_{Z_i}(z)$.

Note that,

$$\begin{aligned}
nR_1 &= H(M_1) \qquad (3.85) \\
&\geq I(M_1; Z^n) \\
&\overset{(a)}{=} I(M_1, X_1^n; Z^n) \\
&\geq I(X_1^n; Z^n) \\
&= I(X_1^n, X_2^n; Z^n) - I(X_2^n; Z^n|X_1^n) \\
&\overset{(b)}{\geq} \sum_{x_1^n} \sum_{x_2^n} \sum_{z^n} P(x_1^n, x_2^n, z^n) \log \frac{W^{\otimes n}(z^n|x_1^n, x_2^n)}{P_{Z^n}(z^n)} - \sum_{i} I(X_{2i}; Z_i|X_{1i})
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{x_1^n}\sum_{x_2^n}\sum_{z^n} P(x_1^n, x_2^n, z^n) \log \frac{W^{\otimes n}(z^n|x_1^n, x_2^n)}{Q_Z^{\otimes n}(z^n)} - \mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) - \sum_i I(X_{2i}; Z_i|X_{1i}) \\
&\geq \sum_{x_1^n}\sum_{x_2^n}\sum_{z^n} P(x_1^n, x_2^n, z^n) \log \frac{W^{\otimes n}(z^n|x_1^n, x_2^n)}{Q_Z^{\otimes n}(z^n)} - \sum_i I(X_{2i}; Z_i|X_{1i}) - \epsilon \\
&= \sum_i \sum_{x_{1i}}\sum_{x_{2i}}\sum_{z_i} P(x_{1i}, x_{2i}, z_i) \Big(\log \frac{W(z_i|x_{1i}, x_{2i})}{Q(z_i)} - \log \frac{W(z_i|x_{1i}, x_{2i})}{P(z_i|x_{1i})} \Big) - \epsilon \\
&= \sum_i \sum_{x_{1i}}\sum_{x_{2i}}\sum_{z_i} P(x_{1i}, x_{2i}, z_i) \log \frac{P(z_i|x_{1i})}{Q(z_i)} - \epsilon \\
&= \sum_i \sum_{x_{1i}}\sum_{z_i} P(x_{1i}, z_i) \log \frac{P(z_i|x_{1i})}{Q(z_i)} - \epsilon \\
&= \sum_i \mathbb{D}(P_{X_{1i}Z_i}||P_{X_{1i}}Q_{Z_i}) - \epsilon \\
&\overset{(c)}{\geq} n\mathbb{D}\left(\frac{\sum_i P_{X_{1i}Z_i}}{n} \middle|\middle| \frac{\sum_i P_{X_{1i}}}{n} Q_Z \right) - \epsilon \\
&\overset{(d)}{=} n\mathbb{D}(\tilde{P}_{X_1,Z}||\tilde{P}_{X_1}Q_Z) - \epsilon \\
&= n \sum_{x_1}\sum_{z} \tilde{P}_{X_1,Z}(x_1, z) \log \frac{\tilde{P}_{X_1,Z}(x_1, z)}{\tilde{P}_{X_1}(x_1)Q_Z(z)} - \epsilon \\
&= n \sum_{x_1}\sum_{z} \tilde{P}_{X_1,Z}(x_1, z) \log \frac{\tilde{P}_{X_1,Z}(x_1, z)}{\tilde{P}_{X_1}(x_1)\tilde{P}_Z(z)} + n \sum_{x_1}\sum_{z} \tilde{P}_{X_1,Z}(x_1, z) \log \frac{\tilde{P}_Z(z)}{Q_Z(z)} - \epsilon \\
&= nI(\tilde{X}_1; \tilde{Z}) + n\mathbb{D}(\tilde{P}_Z||Q_Z) - \epsilon \\
&\geq nI(\tilde{X}_1; \tilde{Z}) - \epsilon
\end{aligned}
\tag{3.86}
$$

where

(a) follows from the definition of the deterministic encoding functions in (3.3);

(b) follows because conditioning does not increase entropy and the channel is discrete memoryless, therefore $I(X_2^n; Z^n|X_1^n) = \sum H(Z_i|Z^{i-1}, X_1^n) - H(Z_i|Z^{i-1}, X_1^n, X_2^n) \leq \sum H(Z_i|X_{1i}) - H(Z_i|X_{1i}, X_{2i}) \leq \sum_{i=1}^n I(X_{2i}; Z_i|X_{1i})$;

(c) follows by Jensen's inequality and the convexity of $\mathbb{D}(\cdot||\cdot)$;

(d) follows by defining $\tilde{P}_{X_1,Z}(x_1,z) \triangleq \frac{1}{n}\sum_i P_{X_{1i},Z_i}(x_1,z)$ and $\tilde{P}_{X_1}(x_1) \triangleq \frac{1}{n}\sum_i P_{X_{1i}}(x_1)$ where $\tilde{P}_{X_1,X_2}(x_1,x_2) \triangleq \frac{1}{n}\sum_i P_{X_{1i},X_{2i}}(x_1,x_2)$, $\tilde{P}_{X_1,X_2,Z}(x_1,x_2,z) \triangleq \frac{1}{n}\sum_i P_{X_{1i},X_{2i},Z_i}(x_1,x_2,z) = W_{Z|X_1,X_2}(z|x_1,x_2)\tilde{P}_{X_1,X_2}(x_1,x_2)$ and $\tilde{P}_{X_1,Z}(x_1,z) = \sum_{x_2}\tilde{P}_{X_1,X_2,Z}(x_1,x_2,z)$.

$$
\begin{aligned}
nR_2 &= H(M_2) \\
&\geq H(M_2|X_1^n) \\
&\geq I(M_2;Z^n|X_1^n) \\
&\overset{(a)}{=} I(M_2,X_2^n;Z^n|X_1^n) \\
&\geq I(X_2^n;Z^n|X_1^n) \\
&= I(X_1^n,X_2^n;Z^n) - I(X_1^n;Z^n) \\
&= \sum_{x_1^n}\sum_{x_2^n}\sum_{z^n} P(x_1^n,x_2^n,z^n)\log\frac{P(x_1^n,x_2^n,z^n)}{P(x_1^n,x_2^n)P_{Z^n}(z^n)} - H(X_1^n) + H(X_1^n|Z^n) \\
&\geq \sum_{x_1^n}\sum_{x_2^n}\sum_{z^n} P(x_1^n,x_2^n,z^n)\log\frac{W^{\otimes n}(z^n|x_1^n,x_2^n)}{Q_Z^{\otimes n}(z^n)} - \mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) - H(X_1^n) \\
&\geq \sum_i\sum_{x_{1i}}\sum_{x_{2i}}\sum_{z_i} P(x_{1i},x_{2i},z_i)\log\frac{W(z_i|x_{1i},x_{2i})}{Q(z_i)} - \sum_i H(X_{1i}) - \epsilon \\
&= \sum_i \mathbb{D}(P_{X_{1i},X_{2i},Z_i}||P_{X_{1i},X_{2i}}Q_{Z_i}) - \sum_i H(X_{1i}) - \epsilon \\
&\overset{(b)}{\geq} n\mathbb{D}(\tilde{P}_{X_1,X_2,Z}||\tilde{P}_{X_1,X_2}Q_Z) - nH(\tilde{X}_1) - \epsilon \\
&= n\mathbb{D}(\tilde{P}_{X_1,X_2,Z}||\tilde{P}_{X_1,X_2}\tilde{P}_Z) + n\mathbb{D}(\tilde{P}_Z||Q_Z) - nH(\tilde{X}_1) - \epsilon \\
&\geq nI(\tilde{X}_1,\tilde{X}_2;\tilde{Z}) - nH(\tilde{X}_1) - \epsilon
\end{aligned}
$$

where

(a) follows from the definition of the deterministic encoding functions in (3.3);

(b) follows by Jensen's inequality, the convexity of $\mathbb{D}(\cdot||\cdot)$, concavity of $H(\cdot)$ and defining $\tilde{P}_{X_1,X_2,Z}(x_1,x_2,z) \triangleq \frac{1}{n}\sum_i P_{X_{1i},X_{2i},Z_i}(x_1,x_2,z)$ and $\tilde{P}_{X_1,X_2}(x_1,x_2) \triangleq \frac{1}{n}\sum_i P_{X_{1i},X_{2i}}(x_1,x_2)$ with $\tilde{P}_{X_1,X_2,Z}(x_1,x_2,z) = W_{Z|X_1,X_2}(z|x_1,x_2)\tilde{P}_{X_1,X_2}(x_1,x_2)$.

Next, observe that

$$\begin{align}
&n(R_1+R_2) \notag\\
&\quad= H(M_1,M_2) \tag{3.87}\\
&\quad\geq I(M_1,M_2;Z^n) \notag\\
&\quad\geq I(X_1^n,X_2^n;Z^n)+\mathbb{D}(P_{Z^n}||Q_Z^{\otimes n})-\epsilon \notag\\
&\quad= \sum_{x_1^n}\sum_{x_2^n}\sum_{z^n}P(x_1^n,x_2^n,z^n)\log\frac{P(x_1^n,x_2^n,z^n)}{P(x_1^n,x_2^n)P_{Z^n}(z^n)}+\sum_{z^n}P(z^n)\log\frac{P_{Z^n}(z^n)}{Q_Z^{\otimes n}(z^n)}-\epsilon \notag\\
&\quad= \sum_{x_1^n}\sum_{x_2^n}\sum_{z^n}P(x_1^n,x_2^n,z^n)\log\frac{W^{\otimes n}(z^n|x_1^n,x_2^n)}{Q_Z^{\otimes n}(z^n)}-\epsilon \notag\\
&\quad= \sum_{i}\sum_{x_{1i}}\sum_{x_{2i}}\sum_{z_i}P(x_{1i},x_{2i},z_i)\log\frac{W(z_i|x_{1i},x_{2i})}{Q(z_i)}-\epsilon \notag\\
&\quad= \sum_{i}\mathbb{D}(P_{X_{1i},X_{2i},Z_i}||P_{X_{1i},X_{2i}}Q_{Z_i})-\epsilon \notag\\
&\quad\overset{(a)}{\geq} n\mathbb{D}\left(\frac{\sum_i P_{X_{1i},X_{2i},Z_i}}{n}\middle|\middle|\frac{\sum_i P_{X_{1i},X_{2i}}}{n}Q_Z\right)-\epsilon \notag\\
&\quad\overset{(b)}{=} n\mathbb{D}(\tilde{P}_{X_1,X_2,Z}||\tilde{P}_{X_1,X_2}Q_Z)-\epsilon \notag\\
&\quad= n\mathbb{D}(\tilde{P}_{X_1,X_2,Z}||\tilde{P}_{X_1,X_2}\tilde{P}_Z)+n\mathbb{D}(\tilde{P}_Z||Q_Z)-\epsilon \notag\\
&\quad\geq nI(\tilde{X}_1,\tilde{X}_2;\tilde{Z})-\epsilon \tag{3.88}
\end{align}$$

where

(a) follows by Jensen's inequality and the convexity of $\mathbb{D}(\cdot||\cdot)$;

(b) follows by defining $\tilde{P}_{X_1,X_2,Z}(x_1,x_2,z)\triangleq\frac{1}{n}\sum_i P_{X_{1i},X_{2i},Z_i}(x_1,x_2,z)$ and $\tilde{P}_{X_1,X_2}(x_1,x_2)\triangleq\frac{1}{n}\sum_i P_{X_{1i},X_{2i}}(x_1,x_2)$ with $\tilde{P}_{X_1,X_2,Z}(x_1,x_2,z)=W_{Z|X_1,X_2}(z|x_1,x_2)\tilde{P}_{X_1,X_2}(x_1,x_2,z)$.

3.4.6 Strong secrecy of MAC with one-sided non-causal cribbing

Achievability:

Consider a distribution $P(x_1, x_2) = P(x_1)P(x_2|x_1)$ such that $\sum_{x_1,x_2} P(x_1, x_2)W(z|x_1, x_2) = Q_Z(z)$.

Code Construction:

- Independently generate $2^{n(R_1+R'_1)}$ codewords x_1^n each with probability $P(X_1^n) = P_{X_1}^{\otimes n}(x_1^n)$. Label them $x_1^n(m_1, m'_1)$, $m_1 \in [\![1, 2^{nR_1}]\!]$ and $m'_1 \in [\![1, 2^{nR'_1}]\!]$.

- For every $x_1^n(m_1, m'_1)$, independently generate $2^{n(R_2+R'_2)}$ codewords x_2^n each with probability $P(x_2^n|x_1^n(m_1, m'_1)) = P_{X_2|X_1}^{\otimes n}(x_2^n|x_1^n(m_1, m'_1))$. Label them $x_2^n(x_1^n(m_1, m'_1), m_2, m'_2)$, $m_2 \in [\![1, 2^{nR_2}]\!]$ and $m'_2 \in [\![1, 2^{nR'_2}]\!]$.

We assume that each message is chosen independently and uniformly from its corresponding set. As a result of cribbing, Encoder 2 knows x_1^n in advance, therefore before transmission, it finds $(\hat{m}_1, \hat{m}'_1)$ such that $(x_1^n(\hat{m}_1, \hat{m}'_1), x_1^n) \in \mathcal{T}_\epsilon^{(n)}(P_{X_1,X_1})$ where $(\hat{m}_1, \hat{m}'_1)$ are the estimates of (m_1, m'_1).

Encoding: To send m_1, Encoder 1 sends $x_1^n(m_1, m'_1)$. To send m_2, Encoder 2 cooperatively sends $x_2^n(x_1^n(\hat{m}_1, \hat{m}'_1), m_2, m'_2)$.

Decoding at the receiver: The decoder finds $(\hat{\hat{m}}_1, \hat{\hat{m}}'_1, \hat{\hat{m}}_2, \hat{\hat{m}}'_2)$ such that $(x_1^n(\hat{\hat{m}}_1, \hat{\hat{m}}'_1), x_2^n(x_1^n(\hat{\hat{m}}_1, \hat{\hat{m}}'_1), \hat{\hat{m}}_2, \hat{\hat{m}}'_2), y^n) \in \mathcal{T}_\epsilon^{(n)}(P_{X_1,X_2,Y})$.

Probability of error analysis: Using standard arguments, the probability of error averaged over all codebooks vanishes exponentially with n if

$$R_1 + R'_1 < H(X_1) \tag{3.89}$$

$$R_2 + R'_2 < I(X_2; Y|X_1) \tag{3.90}$$

$$R_1 + R'_1 + R_2 + R'_2 < I(X_1, X_2; Y) \tag{3.91}$$

Secrecy analysis: We will show that the information leakage, averaged over all codebooks, vanishes exponentially with n. We use the results of Theorem 7 to bound $\mathbb{E}_{M_1,M_2}[\mathbb{D}(P_{Z^n|M_1,M_2}||Q_Z^{\otimes n})]$ such that the channel output distribution at the wiretapper is, on average, independent of the transmitted messages and follows the i.i.d distribution $Q_Z^{\otimes n}$. This is sufficient to ensure secrecy because $I(M_1, M_2; Z^n)$ can be bounded by $\mathbb{E}_{M_1,M_2}[\mathbb{D}(P_{Z^n|M_1,M_2}||Q_Z^{\otimes n})]$, as follows:

$$
\begin{aligned}
I(M_1, M_2; Z^n) &= \mathbb{D}(P_{M_1,M_2,Z^n}||P_{M_1,M_2}P_{Z^n}) && (3.92)\\
&= \sum_{m_1,m_2,z^n} P_{M_1,M_2,Z^n}(m_1, m_2, z^n) \log \frac{P_{M_1,M_2,Z^n}(m_1, m_2, z^n)}{P_{M_1,M_2}(m_1, m_2)P_{Z^n}(z^n)} && (3.93)\\
&= \sum_{m_1,m_2} P_{M_1,M_2}(m_1, m_2)\mathbb{D}(P_{Z^n|M_1,M_2}||P_{Z^n}) && (3.94)\\
&\overset{(a)}{\leq} \mathbb{E}_{M_1,M_2}\left(\mathbb{D}(P_{Z^n|M_1,M_2}||Q_Z^{\otimes n})\right), && (3.95)
\end{aligned}
$$

where (a) follows by adding $\mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) \geq 0$ to (3.94). With $P_{Z^n|M_1M_2}(z^n|m_1, m_2) = 2^{-n(R_1'+R_2')} \sum_{i,j} W^{\otimes n}(z^n|x_1^n(m_1, i), x_2^n(m_1, i, m_2, j))$ and applying Theorem 7 to (3.95), $I(M_1, M_2; Z^n)$ vanishes exponentially with n if

$$
\begin{aligned}
R_1' &> I(X_1; Z) && (3.96)\\
R_2' &> I(X_1, X_2; Z) - H(X_1) && (3.97)\\
R_1' + R_2' &> I(X_1, X_2; Z) && (3.98)
\end{aligned}
$$

Combining (3.89)-(3.91) and (3.96)-(3.98), and using Fourier-Motzkin elimination, the following rate region is achievable

$$
\begin{aligned}
R_1 &< H(X_1) - I(X_1; Z), && (3.99)\\
R_2 &< I(X_2; Y|X_1), && (3.100)\\
R_1 + R_2 &< I(X_1, X_2; Y) - I(X_1, X_2; Z). && (3.101)
\end{aligned}
$$

3.4.7 Channel resolvability of MAC with two-sided strictly-causal cribbing

Achievability (Proposition 5):

To handle the strict causality constraint, we adopt a block-Markov encoding scheme over $B > 0$ consecutive and dependent blocks, each consisting of r transmissions such that $n = rB$. The vector of n channel outputs Z^n may then be described as $Z^n \triangleq (Z_1^r, \cdots, Z_B^r)$, where each Z_b^r for $b \in [\![1, B]\!]$ describes the observations in block b. The distribution induced by the coding scheme is the joint distribution $P_Z^n \triangleq P_{Z_1^r,\cdots,P_{Z_B^r}}$, while the target output distribution is a product distribution of product distributions $Q_Z^{\otimes n} \triangleq \prod_{j=1}^B Q_Z^{\otimes r}$.

Codebook Construction:

Consider a distribution $P_{U,U_1,U_2,X_1,X_2} = P_U P_{U_1|U} P_{U_2|U} P_{X_1|U,U_1} P_{X_2|U,U_2}$ such that $\sum_{u,u_1,u_2,x_1,x_2} P_{U,U_1,U_2,X_1,X_2} W_{Z|X_1,X_2} = Q_Z$ that satisfies $H(X_1|U,U_1) + H(X_2|U,U_2) > I(X_1, X_2; Z)$. For every $b \in [\![1, B]\!]$:

- Independently generate $2^{r\rho_0}$ codewords $u^r(m_0^{(b)})$ each with probability $P_{U^r} = P_U^{\otimes r}$. Label them $u^r(m_0^{(b)})$, $m_0^{(b)} \in [\![1, 2^{n\rho_0}]\!]$.

- For every $u^r(m_0^{(b)})$, independently generate $2^{r\rho_{01}}$ codewords $u_1^r(m_0^{(b)}, m_{01}^{(b)})$ each with probability $P_{U_1^r|U^r} = P_{U_1^r|U^r}^{\otimes r}$. Label them $u_1^r(m_0^{(b)}, m_{01}^{(b)})$, $m_{01}^{(b)} \in [\![1, 2^{r\rho_{01}}]\!]$.

- For every $(u^r(m_0^{(b)}), u_1^r(m_0^{(b)}, m_{01}^{(b)}))$, independently generate $2^{r(\rho_1' + \rho_1'')}$ codewords $x_1^r(m_0^{(b)}, m_{01}^{(b)}, m_1'^{(b)}, m_1''^{(b)})$ each with probability $P_{X_1^r|U_1^r,U^r} = P_{X_1^r|U_1^r,U^r}^{\otimes r}$. Label them $x_1^r(m_0^{(b)}, m_{01}^{(b)}, m_1'^{(b)}, m_1''^{(b)})$, $m_1'^{(b)} \in [\![1, 2^{r\rho_1'}]\!]$ and $m_1''^{(b)} \in [\![1, 2^{r\rho_1''}]\!]$.

- For every $u^r(m_0^{(b)})$, independently generate $2^{r\rho_{02}}$ codewords $u_2^r(m_0^{(b)}, m_{02}^{(b)})$ each with probability $P_{U_2^r|U^r} = P_{U_2^r|U^r}^{\otimes r}$. Label them $u_2^r(m_0^{(b)}, m_{02}^{(b)})$, $m_{02}^{(b)} \in [\![1, 2^{r\rho_{02}}]\!]$.

- For every $(u^r(m_0^{(b)}), u_2^r(m_0^{(b)}, m_{02}^{(b)}))$, independently generate $2^{r(\rho_2' + \rho_2'')}$ codewords $x_2^r(m_0^{(b)}, m_{02}^{(b)}, m_2'^{(b)}, m_2''^{(b)})$ each with probability $P_{X_2^r|U_2^r,U^r} = P_{X_2^r|U_2^r,U^r}^{\otimes r}$. Label them $x_2^r(m_0^{(b)}, m_{02}^{(b)}, m_2'^{(b)}, m_2''^{(b)})$, $m_2'^{(b)} \in [\![1, 2^{r\rho_2'}]\!]$ and $m_2''^{(b)} \in [\![1, 2^{r\rho_2''}]\!]$.

This defines the codebook in block b

$$\begin{aligned}\mathcal{C}_r = \Big\{ & u^r(m_0^{(b)}), u_1^r(m_0^{(b)}, m_{01}^{(b)}), u_2^r(m_0^{(b)}, m_{02}^{(b)}), x_1^r(m_0^{(b)}, m_{01}^{(b)}, m_1'^{(b)}, m_1''^{(b)}), \\ & x_2^r(m_0^{(b)}, m_{02}^{(b)}, m_2'^{(b)}, m_2''^{(b)}), m_0^{(b)} \in \llbracket 1, 2^{r\rho_0} \rrbracket, m_{01}^{(b)} \in \llbracket 1, 2^{r\rho_{01}} \rrbracket, m_{02}^{(b)} \in \llbracket 1, 2^{r\rho_{02}} \rrbracket, \\ & m_1'^{(b)} \in \llbracket 1, 2^{r\rho_1'} \rrbracket, m_1''^{(b)} \in \llbracket 1, 2^{r\rho_1''} \rrbracket, m_2'^{(b)} \in \llbracket 1, 2^{r\rho_2'} \rrbracket, m_2''^{(b)} \in \llbracket 1, 2^{r\rho_2''} \rrbracket \Big\} \end{aligned} \tag{3.102}$$

and we denote the random codebook in block b by

$$\begin{aligned}\mathfrak{C}_r = \Big\{ & U^r(m_0^{(b)}), U_1^r(m_0^{(b)}, m_{01}^{(b)}), U_2^r(m_0^{(b)}, m_{02}^{(b)}), X_1^r(m_0^{(b)}, m_{01}^{(b)}, m_1'^{(b)}, m_1''^{(b)}), \\ & X_2^r(m_0^{(b)}, m_{02}^{(b)}, m_2'^{(b)}, m_2''^{(b)}), m_0^{(b)} \in \llbracket 1, 2^{r\rho_0} \rrbracket, m_{01}^{(b)} \in \llbracket 1, 2^{r\rho_{01}} \rrbracket, m_{02}^{(b)} \in \llbracket 1, 2^{r\rho_{02}} \rrbracket, \\ & m_1'^{(b)} \in \llbracket 1, 2^{r\rho_1'} \rrbracket, m_1''^{(b)} \in \llbracket 1, 2^{r\rho_1''} \rrbracket, m_2'^{(b)} \in \llbracket 1, 2^{r\rho_2'} \rrbracket, m_2''^{(b)} \in \llbracket 1, 2^{r\rho_2''} \rrbracket \Big\} \end{aligned} \tag{3.103}$$

The messages $M_1'^{(b)}$ and $M_2'^{(b)}$ are part of $M_1^{(b)}$ and $M_2^{(b)}$ respectively and represent the local randomness at each encoder. The messages $M_1''^{(b)}$ and $M_2''^{(b)}$ are part of $M_1^{(b)}$ and $M_2^{(b)}$ respectively that are used by both encoders toward the creation of $M_0^{(b+1)}$, $M_{01}^{(b+1)}$ and $M_{02}^{(b+1)}$, assuming $\rho_1'' + \rho_2'' > \rho_0 + \rho_{01} + \rho_{02}$. Furthermore, for $\gamma \in \llbracket 0, 1 \rrbracket$, an amount $\gamma(\rho_1'' + \rho_2'' - \rho_0 - \rho_{01} - \rho_{02})$ is recycled towards the creation of $M_1'^{(b+1)}$ and an amount $(1-\gamma)(\rho_1'' + \rho_2'' - \rho_0 - \rho_{01} - \rho_{02})$ is recycled towards the creation of $M_2'^{(b+1)}$.

Next we bound $\mathbb{D}(P_{Z^n}||Q_Z^{\otimes n})$ and show that dependencies across blocks created by block-Markov encoding can be eliminated by appropriately recycling randomness from one block to the next.

$$\mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) \tag{3.104}$$

$$= \mathbb{D}(P_{Z_1^r \ldots Z_B^r}||Q_Z^{\otimes rB})$$

$$= \sum_{b=1}^{B} \mathbb{D}(P_{Z_j^r|Z_{b+1}^{B,r}}||Q_Z^{\otimes r}|P_{Z_{b+1}^{B,r}}) \tag{3.105}$$

$$= \sum_{b=1}^{B} \mathbb{D}(P_{Z_j^r}||Q_Z^{\otimes r}) + \sum_{b=1}^{B} \mathbb{D}(P_{Z_j^r|Z_{b+1}^{B,r}}||P_{Z_j^r}|P_{Z_{b+1}^{B,r}}) \tag{3.106}$$

$$= \sum_{b=1}^{B} \mathbb{D}(P_{Z_b^r}||Q_Z^{\otimes r}) + \sum_{b=1}^{B} I(Z_b^r; Z_{b+1}^{B,r}) \tag{3.107}$$

$$\overset{(a)}{\leq} \sum_{b=1}^{B} \mathbb{D}(P_{M_1''^{(b)},M_2''^{(b)},Z_b^r}||P_{M_1''^{(b)},M_2''^{(b)}}Q_Z^{\otimes r}) + \sum_{b=1}^{B} I(Z_b^r; M_1''^{(b)}, \hat{M}_1''^{(b)}, M_2''^{(b)}, \hat{M}_2''^{(b)}, Z_{b+1}^{B}) \tag{3.108}$$

$$\overset{(b)}{=} \sum_{b=1}^{B} \mathbb{D}(P_{M_1''^{(b)},M_2''^{(b)},Z_b^r}||P_{M_1''^{(b)},M_2''^{(b)}}Q_Z^{\otimes r}) + \sum_{b=1}^{B} I(Z_b^r; M_1''^{(b)}, \hat{M}_1''^{(b)}, M_2''^{(b)}, \hat{M}_2''^{(b)}) \tag{3.109}$$

$$\overset{(c)}{\leq} \sum_{b=1}^{B} 2 \times \mathbb{D}(P_{M_1''^{(b)},M_2''^{(b)},Z_b^r}||P_{M_1''^{(b)},M_2''^{(b)}}Q_Z^{\otimes r}) + \sum_{b=1}^{B} H(\hat{M}_1''^{(b)}, \hat{M}_2''^{(b)}|M_1''^{(b)}, M_2''^{(b)}) \tag{3.110}$$

where

- (a) follows since $\mathbb{D}(P_{Z_b^r}||Q_Z^{\otimes r}) = \mathbb{D}(P_{Z_b^r,M_1''^{(b)},M_2''^{(b)}}||P_{M_1''^{(b)},M_2''^{(b)}}Q_Z^{\otimes r}) - \mathbb{D}(P_{Z_b^r,M_1''^{(b)},M_2''^{(b)}}||P_{M_1''^{(b)},M_2''^{(b)}}P_{Z_b^r})$;
- (b) follows since $Z_b^r \to M_1''^{(b)}, \hat{M}_1''^{(b)}, M_2''^{(b)}, \hat{M}_2''^{(b)} \to Z_{b+1}^{B,r}$ holds; follows since $I(Z_b^r; M_1''^{(b)}, M_2''^{(b)}) = \mathbb{D}(P_{Z_b^r,M_1''^{(b)},M_2''^{(b)}}||P_{M_1''^{(b)},M_2''^{(b)}}P_{Z_b^r}) \leq \mathbb{D}(P_{Z_b^r,M_1''^{(b)},M_2''^{(b)}}||P_{M_1''^{(b)},M_2''^{(b)}}Q_Z^{\otimes r})$.

Let $P_e^{(b)}$ be the average error probability of both encoders decoding the other encoder's message. From Fano's inequality, we can write $H(\hat{M}_1''^{(b)}, \hat{M}_2''^{(b)}|M_1''^{(b)}, M_2''^{(b)}) \leq H(\hat{M}_1''^{(b)}|M_1''^{(b)}) + H(\hat{M}_2''^{(b)}|M_2''^{(b)}) \leq 2H(P_e^{(b)}) + r(\rho_1'' + \rho_2'')P_e^{(b)}$. By random coding we know that $\mathbb{E}_{\mathfrak{C}_r}\left(P_e^{(b)}\right) < 2^{-\alpha r}$ for some $\alpha > 0$ and all r large enough if $\rho_1' + \rho_1'' < H(X_1|U, U_1)$ and $\rho_2' + \rho_2'' < H(X_2|U, U_2)$.

Let $\bar{P}$ be the probability distribution induced when both encoders are using the same $M_0^{(b)}$, i.e., $(\hat{M}_1''^{(b-1)}, \hat{M}_2''^{(b-1)}) = (M_1''^{(b-1)}, M_2''^{(b-1)})$.

$$\mathbb{E}_{\mathfrak{C}_r}\big(\mathbb{D}(\bar{P}_{Z_b^r,M_1''^{(b)},M_2''^{(b)}}||\bar{P}_{M_1''^{(b)},M_2''^{(b)}}Q_Z^{\otimes r})\big)$$

$$= \mathbb{E}_{\mathfrak{C}_r} \sum_{m_1''^{(b)},m_2''^{(b)},z_b^r} \bar{P}_{Z_b^r,M_1''^{(b)},M_2''^{(b)}} \log \frac{\bar{P}_{Z_b^r|M_1''^{(b)},M_2''^{(b)}}}{Q_Z^{\otimes r}} \tag{3.111}$$

$$= \mathbb{E}_{\mathfrak{C}_r} \sum_{m_1''^{(b)}, m_2''^{(b)}, z_b^r} 2^{-r(\rho_1''+\rho_2'')} \sum_{m_0^{(b)}, m_{01}^{(b)}, m_{02}^{(b)}, m_1'^{(b)}, m_2'^{(b)}} 2^{-r(\rho_0+\rho_{01}+\rho_{02}+\rho_1'+\rho_2')}$$

$$W^{\otimes r}(z_b^r|U^r(m_0^{(b)}), U_1^r(m_0^{(b)}, m_{01}^{(b)}), U_2^r(m_0^{(b)}, m_{02}^{(b)}), X_1^r(m_0^{(b)}, m_{01}^{(b)}, m_1'^{(b)}, m_1''^{(b)}),$$

$$X_2^r(m_0^{(b)}, m_{02}^{(b)}, m_2'^{(b)}, m_2''^{(b)}))$$

$$\times \log \sum_{a,b,c,d,e} \frac{W^{\otimes r}(z_b^r|U^r(a), U_1^r(a,b), U_2^r(a,c), X_1^r(a,b,d,m_1''^{(b)}), X_2^r(a,c,e,m_2''^{(b)}))}{2^{r(\rho_0+\rho_{01}+\rho_{02}+\rho_1'+\rho_2')} Q_Z^{\otimes r}} \tag{3.112}$$

$$\overset{(a)}{\leq} \sum_{m_1''^{(b)}, m_2''^{(b)}, z_b^r} 2^{-r(\rho_1''+\rho_2'')} \sum_{m_0^{(b)}, m_{01}^{(b)}, m_{02}^{(b)}, m_1'^{(b)}, m_2'^{(b)}} 2^{-r(\rho_0+\rho_{01}+\rho_{02}+\rho_1'+\rho_2')}$$

$$\sum_{u^r(m_0^{(b)}), u_1^r(m_0^{(b)}, m_{01}^{(b)}), u_2^r(m_0^{(b)}, m_{02}^{(b)}), x_1^r(m_0^{(b)}, m_{01}^{(b)}, m_1'^{(b)}, m_1''^{(b)}), x_2^r(m_0^{(b)}, m_{02}^{(b)}, m_2'^{(b)}, m_2''^{(b)})}$$

$$\bar{P}^{\otimes r}(u^r(m_0^{(b)}), u_1^r(m_0^{(b)}, m_{01}^{(b)}), u_2^r(m_0^{(b)}, m_{02}^{(b)}), x_1^r(m_0^{(b)}, m_{01}^{(b)}, m_1'^{(b)}, m_1''^{(b)}),$$

$$x_2^r(m_0^{(b)}, m_{02}^{(b)}, m_2'^{(b)}, m_2''^{(b)}), z_b^r)$$

$$\times \log \mathbb{E}_{\setminus(m_0^{(b)}, m_{01}^{(b)}, m_{02}^{(b)}, m_1'^{(b)}, m_2'^{(b)})}$$

$$\sum_{a,b,c,d,e} \frac{W^{\otimes r}(z_b^r|U^r(a), U_1^r(a,b), U_2^r(a,c), X_1^r(a,b,d,m_1''^{(b)}), X_2^r(a,c,e,m_2''^{(b)}))}{2^{r(\rho_0+\rho_{01}+\rho_{02}+\rho_1'+\rho_2')} Q_Z^{\otimes r}} \tag{3.113}$$

$$= \sum_{m_1''^{(b)}, m_2''^{(b)}, z_b^r} 2^{-r(\rho_1''+\rho_2'')} \sum_{m_0^{(b)}, m_{01}^{(b)}, m_{02}^{(b)}, m_1'^{(b)}, m_2'^{(b)}} 2^{-r(\rho_0+\rho_{01}+\rho_{02}+\rho_1'+\rho_2')}$$

$$\sum_{u^r(m_0^{(b)}), u_1^r(m_0^{(b)}, m_{01}^{(b)}), u_2^r(m_0^{(b)}, m_{02}^{(b)}), x_1^r(m_0^{(b)}, m_{01}^{(b)}, m_1'^{(b)}, m_1''^{(b)}), x_2^r(m_0^{(b)}, m_{02}^{(b)}, m_2'^{(b)}, m_2''^{(b)})}$$

$$\bar{P}^{\otimes r}(u^r(m_0^{(b)}), u_1^r(m_0^{(b)}, m_{01}^{(b)}), u_2^r(m_0^{(b)}, m_{02}^{(b)}), x_1^r(m_0^{(b)}, m_{01}^{(b)}, m_1'^{(b)}, m_1''^{(b)}),$$

$$x_2^r(m_0^{(b)}, m_{02}^{(b)}, m_2'^{(b)}, m_2''^{(b)}), z_b^r)$$

$$\times \log \mathbb{E}_{\setminus(m_0^{(b)}, m_{01}^{(b)}, m_{02}^{(b)}, m_1'^{(b)}, m_2'^{(b)})} \frac{1}{2^{r(\rho_0+\rho_{01}+\rho_{02}+\rho_1'+\rho_2')} Q_Z^{\otimes r}}$$

$$\Bigg[W^{\otimes r}(z_b^r|u^r(m_0^{(b)}), u_1^r(m_0^{(b)}, m_{01}^{(b)}), u_2^r(m_0^{(b)}, m_{02}^{(b)}), x_1^r(m_0^{(b)}, m_{01}^{(b)}, m_1'^{(b)}, m_1''^{(b)}),$$

$$x_2^r(m_0^{(b)}, m_{02}^{(b)}, m_2'^{(b)}, m_2''^{(b)}))$$

$$+\sum_{d\neq m_1'^{(b)}} W^{\otimes r}(z_b^r|u^r(m_0^{(b)}), u_1^r(m_0^{(b)}, m_{01}^{(b)}), u_2^r(m_0^{(b)}, m_{02}^{(b)}), X_1^r(m_0^{(b)}, m_{01}^{(b)}, d, m_1''^{(b)}),$$

$$x_2^r(m_0^{(b)}, m_{02}^{(b)}, m_2'^{(b)}, m_2''^{(b)}))$$

$$+\sum_{e\neq m_2'^{(b)}} W^{\otimes r}(z_b^r|u^r(m_0^{(b)}), u_1^r(m_0^{(b)}, m_{01}^{(b)}), u_2^r(m_0^{(b)}, m_{02}^{(b)}), x_1^r(m_0^{(b)}, m_{01}^{(b)}, m_1'^{(b)}, m_1''^{(b)}),$$

$$X_2^r(m_0^{(b)}, m_{02}^{(b)}, e, m_2''^{(b)}))$$

$$+\sum_{\substack{d\neq m_1'^{(b)}\\ e\neq m_2'^{(b)}}} W^{\otimes r}(z_b^r|u^r(m_0^{(b)}), u_1^r(m_0^{(b)}, m_{01}^{(b)}), u_2^r(m_0^{(b)}, m_{02}^{(b)}), X_1^r(m_0^{(b)}, m_{01}^{(b)}, d, m_1''^{(b)}),$$

$$X_2^r(m_0^{(b)}, m_{02}^{(b)}, e, m_2''^{(b)}))$$

$$+\sum_{\substack{a\neq m_0^{(b)}\\ b,c,d,e}} W^{\otimes r}(z_b^r|U^r(a), U_1^r(a,b), U_2^r(a,c), X_1^r(a,b,d,m_1''^{(b)}), X_2^r(a,c,e,m_2''^{(b)}))$$

$$+\sum_{\substack{b\neq m_{01}^{(b)}\\ d,e}} W^{\otimes r}(z_b^r|u^r(m_0^{(b)}), U_1^r(m_0^{(b)}, b), u_2^r(m_0^{(b)}, m_{02}^{(b)}), X_1^r(m_0^{(b)}, b, d, m_1''^{(b)}),$$

$$X_2^r(m_0^{(b)}, m_{02}^{(b)}, e, m_2''^{(b)}))$$

$$+\sum_{\substack{c\neq m_{02}^{(b)}\\ d,e}} W^{\otimes r}(z_b^r|u^r(m_0^{(b)}), u_1^r(m_0^{(b)}, m_{01}^{(b)}), U_2^r(m_0^{(b)}, c), X_1^r(m_0^{(b)}, m_{01}^{(b)}, d, m_1''^{(b)}),$$

$$X_2^r(m_0^{(b)}, c, e, m_2''^{(b)}))$$

$$+\sum_{\substack{b\neq m_{01}^{(b)}\\ c\neq m_{02}^{(b)}\\ d,e}} W^{\otimes r}(z_b^r|u^r(m_0^{(b)}), U_1^r(m_0^{(b)}, b), U_2^r(m_0^{(b)}, c), X_1^r(m_0^{(b)}, b, d, m_1''^{(b)}),$$

$$X_2^r(m_0^{(b)}, c, e, m_2''^{(b)}))\Bigg] \tag{3.114}$$

$$\overset{(b)}{\leq} \sum_{m_1''^{(b)}, m_2''^{(b)}, z_b^r} 2^{-n(\rho_1''+\rho_2'')} \sum_{m_0^{(b)}, m_{01}^{(b)}, m_{02}^{(b)}, m_1'^{(b)}, m_2'^{(b)}} 2^{-r(\rho_0+\rho_{01}+\rho_{02}+\rho_1'+\rho_2')}$$

$$\sum_{u^r(m_0^{(b)}), u_1^r(m_0^{(b)}, m_{01}^{(b)}), u_2^r(m_0^{(b)}, m_{02}^{(b)}), x_1^r(m_0^{(b)}, m_{01}^{(b)}, m_1'^{(b)}, m_1''^{(b)}), x_2^r(m_0^{(b)}, m_{02}^{(b)}, m_2'^{(b)}, m_2''^{(b)})}$$

$$
\begin{aligned}
&\bar{P}^{\otimes r}(u^r(m_0^{(b)}), u_1^r(m_0^{(b)}, m_{01}^{(b)}), u_2^r(m_0^{(b)}, m_{02}^{(b)}), x_1^r(m_0^{(b)}, m_{01}^{(b)}, m_1'^{(b)}, m_1''^{(b)}), \\
&\qquad\qquad\qquad\qquad x_2^r(m_0^{(b)}, m_{02}^{(b)}, m_2'^{(b)}, m_2''^{(b)}), z_b^r) \\
&\times \log \frac{1}{2^{r(\rho_0+\rho_{01}+\rho_{02}+\rho_1'+\rho_2')} Q_Z^{\otimes r}} \\
&\Bigg[W^{\otimes r}(z_b^r | u^r(m_0^{(b)}), u_1^r(m_0^{(b)}, m_{01}^{(b)}), u_2^r(m_0^{(b)}, m_{02}^{(b)}), x_1^r(m_0^{(b)}, m_{01}^{(b)}, m_1'^{(b)}, m_1''^{(b)}), \\
&\qquad\qquad\qquad\qquad x_2^r(m_0^{(b)}, m_{02}^{(b)}, m_2'^{(b)}, m_2''^{(b)})) \\
&+ \sum_{d \neq m_1'^{(b)}} \bar{P}^{\otimes r}(z_b^r | u^r(m_0^{(b)}), u_1^r(m_0^{(b)}, m_{01}^{(b)}), u_2^r(m_0^{(b)}, m_{02}^{(b)}), x_2^r(m_0^{(b)}, m_{02}^{(b)}, m_2'^{(b)}, m_2''^{(b)})) \\
&+ \sum_{e \neq m_2'^{(b)}} \bar{P}^{\otimes r}(z_b^r | u^r(m_0^{(b)}), u_1^r(m_0^{(b)}, m_{01}^{(b)}), u_2^r(m_0^{(b)}, m_{02}^{(b)}), x_1^r(m_0^{(b)}, m_{01}^{(b)}, m_1'^{(b)}, m_1''^{(b)})) \\
&+ \sum_{\substack{d \neq m_1'^{(b)} \\ e \neq m_2'^{(b)}}} \bar{P}^{\otimes r}(z_b^r | u^r(m_0^{(b)}), u_1^r(m_0^{(b)}, m_{01}^{(b)}), u_2^r(m_0^{(b)}, m_{02}^{(b)})) \\
&+ \sum_{\substack{a \neq m_0^{(b)} \\ b,c,d,e}} \bar{P}^{\otimes r}(z_b^r) \\
&+ \sum_{\substack{b \neq m_{01}^{(b)} \\ d,e}} \bar{P}^{\otimes r}(z_b^r | u^r(m_0^{(b)}), u_2^r(m_0^{(b)}, m_{02}^{(b)})) \\
&+ \sum_{\substack{c \neq m_{02}^{(b)} \\ d,e}} \bar{P}^{\otimes r}(z_b^r | u^r(m_0^{(b)}), u_1^r(m_0^{(b)}, m_{01}^{(b)})) \\
&+ \sum_{\substack{b \neq m_{01}^{(b)} \\ c \neq m_{02}^{(b)} \\ d,e}} \bar{P}^{\otimes r}(z_b^r | u^r(m_0^{(b)})) \Bigg] \qquad (3.115) \\
&\overset{(c)}{=} \Psi_1 + \Psi_2 \qquad (3.116)
\end{aligned}
$$

where

(a) follows by Jensen's Inequality;

(b) follows by taking the expectation inside the log of the previous step;

(c) Ψ_1 is found by restricting the sum in the previous step over $(u^r, u_1^r, u_2^r, x_1^r, x_2^r, z_b^r) \in \mathcal{T}_\epsilon^r(P_{U,U_1,U_2,X_1,X_2,Y,Z})$ and Ψ_2 is found by restricting that sum over $(u^r, u_1^r, u_2^r, x_1^r, x_2^r, z_b^r) \notin \mathcal{T}_\epsilon^r(P_{U,U_1,U_2,X_1,X_2,Z})$.

Solving Ψ_1 and Ψ_2 like in previous sections we find that $\mathbb{D}(\bar{P}_{Z_b^r, M_1''^{(b)}, M_2''^{(b)}} || \bar{P}_{M_1''^{(b)}, M_2''^{(b)}} Q_Z^{\otimes r}) \xrightarrow{r\to\infty} 0$ if:

$$\rho_0 + \rho_{01} + \rho_{02} + \rho_1' + \rho_2' > I(X_1, X_2; Z) \tag{3.117}$$

$$\rho_0 + \rho_{01} + \rho_{02} + \rho_2' > I(U, U_1, U_2, X_2; Z) \tag{3.118}$$

$$\rho_0 + \rho_{01} + \rho_{02} + \rho_1' > I(U, U_1, U_2, X_1; Z) \tag{3.119}$$

$$\rho_0 + \rho_{01} + \rho_{02} > I(U, U_1, U_2; Z) \tag{3.120}$$

$$\rho_0 + \rho_{02} > I(U, U_2; Z) \tag{3.121}$$

$$\rho_0 + \rho_{01} > I(U, U_1; Z) \tag{3.122}$$

$$\rho_0 > I(U; Z) \tag{3.123}$$

Let $\epsilon > 0$, set

$$\rho_0 = I(U; Z) + \epsilon \tag{3.124}$$

$$\rho_{01} = I(U_1; Z|U) + \epsilon \tag{3.125}$$

$$\rho_{02} = I(U_2; Z|U) + \epsilon \tag{3.126}$$

$$\rho_1' = I(X_1; Z|U, U_1) + \epsilon \tag{3.127}$$

$$\rho_1'' = H(X_1|U, U_1) - I(X_1; Z|U, U_1) - 2\epsilon \tag{3.128}$$

$$\rho_2' = I(X_2; Z|U, U_1, X_1) + \epsilon \tag{3.129}$$

$$\rho_2'' = H(X_2|U, U_2) - I(X_2; Z|U, U_1, X_1) - 2\epsilon \tag{3.130}$$

We can write the effective rates of new randomness at both encoders as:

$$R_1 \triangleq \rho_1' + \rho_1'' - \gamma(\rho_1'' + \rho_2'' - \rho_0 - \rho_{01} - \rho_{02}) \tag{3.131}$$

$$R_2 \triangleq \rho_2' + \rho_2'' - (1-\gamma)(\rho_1'' + \rho_2'' - \rho_0 - \rho_{01} - \rho_{02}) \tag{3.132}$$

$$R_1 + R_2 \triangleq \rho_1' + \rho_2' + \rho_0 + \rho_{01} + \rho_{02} \tag{3.133}$$

Using the values of ρ_0, ρ_{01}, ρ_{02}, ρ_1', ρ_1'', ρ_2' and ρ_2'' chosen above, we obtain the rate region as follows:

$$R_1 \geq I(X_1, X_2; Z) - H(X_2|U, U_2) + 2\epsilon \tag{3.134}$$

$$R_2 \geq I(X_1, X_2; Z) - H(X_1|U, U_1) + 2\epsilon \tag{3.135}$$

$$R_1 + R_2 \geq I(X_1, X_2; Z) + 5\epsilon \tag{3.136}$$

Finally we note that $\mathbb{E}\big(\mathbb{D}(\bar{P}_{Z_b^r, M_1''^{(b)}, M_2''^{(b)}} || \bar{P}_{M_1''^{(b)}, M_2''^{(b)}} Q_Z^{\otimes r})\big) \xrightarrow{r\to\infty} 0$ implies $\mathbb{E}\big(\mathbb{D}(P_{Z_b^r, M_1''^{(b)}, M_2''^{(b)}} || P_{M_1''^{(b)}, M_2''^{(b)}} Q_Z^{\otimes r})\big) \xrightarrow{r\to\infty} 0$ (see discussion in Section 3.4.1) if

$$\rho_1' + \rho_1'' < H(X_1|U, U_1) \tag{3.137}$$

$$\rho_2' + \rho_2'' < H(X_2|U, U_2) \tag{3.138}$$

Achievability (Proposition 6):

To handle the strict causality constraint, we adopt a block-Markov encoding scheme over $B > 0$ consecutive and dependent blocks, each consisting of r transmissions such that $n = rB$. The vector of n channel outputs Z^n at the channel output may then be described as $Z^n \triangleq (Z_1^r, \cdots, Z_B^r)$, where each Z_b^r for $b \in [\![1, B]\!]$ describes the observations in block b. The distribution induced by the coding scheme is the joint distribution $P_Z^n \triangleq P_{Z_1^r, \cdots, P_{Z_B^r}}$, while the target output distribution is a product distribution of product distributions $Q_Z^{\otimes n} \triangleq \prod_{j=1}^{B} Q_Z^{\otimes r}$.

Codebook Construction:

Consider a distribution $P_{U,X_1,X_2} = P_U P_{X_1|U} P_{X_2|U}$ such that $\sum_{u,x_1,x_2} P_{U,X_1,X_2} W_{Z|X_1,X_2} = Q_Z$ that satisfies $H(X_1|U) + H(X_2|U) > I(X_1, X_2; Z)$. For every $b \in [\![1, B]\!]$:

- Independently generate $2^{r\rho_0}$ codewords $u^r(m_0^{(b)})$ each with probability $P_{U^r} = P_U^{\otimes r}$. Label them $u^r(m_0^{(b)})$, $m_0^{(b)} \in [\![1, 2^{n\rho_0}]\!]$.

- For every $u^r(m_0^{(b)})$, independently generate $2^{r(\rho_1'+\rho_1'')}$ codewords $x_1^r(m_0^{(b)}, m_1'^{(b)}, m_1''^{(b)})$ each with probability $P_{X_1^r|U^r} = P_{X_1^r|U^r}^{\otimes r}$. Label them $x_1^r(m_0^{(b)}, m_1'^{(b)}, m_1''^{(b)})$, $m_1'^{(b)} \in [\![1, 2^{r\rho_1'}]\!]$ and $m_1''^{(b)} \in [\![1, 2^{r\rho_1''}]\!]$.

- For every $u^r(m_0^{(b)})$, independently generate $2^{r(\rho_2'+\rho_2'')}$ codewords $x_2^r(m_0^{(b)}, m_2'^{(b)}, m_2''^{(b)})$ each with probability $P_{X_2^r|U^r} = P_{X_2^r|U^r}^{\otimes r}$. Label them $x_2^r(m_0^{(b)}, m_2'^{(b)}, m_2''^{(b)})$, $m_2'^{(b)} \in [\![1, 2^{r\rho_2'}]\!]$ and $m_2''^{(b)} \in [\![1, 2^{r\rho_2''}]\!]$.

This defines the codebook in block b

$$\begin{aligned}\mathcal{C}_r = \{&u^r(m_0^{(b)}), x_1^r(m_0^{(b)}, m_1'^{(b)}, m_1''^{(b)}), x_2^r(m_0^{(b)}, m_2'^{(b)}, m_2''^{(b)}), m_0^{(b)} \in [\![1, 2^{r\rho_0}]\!],\\ &m_1'^{(b)} \in [\![1, 2^{r\rho_1'}]\!], m_1''^{(b)} \in [\![1, 2^{r\rho_1''}]\!], m_2'^{(b)} \in [\![1, 2^{r\rho_2'}]\!], m_2''^{(b)} \in [\![1, 2^{r\rho_2''}]\!]\} \qquad (3.139)\end{aligned}$$

and we denote the random codebook in block b by

$$\begin{aligned}\mathfrak{C}_r = \{&U^r(m_0^{(b)}), X_1^r(m_0^{(b)}, m_1'^{(b)}, m_1''^{(b)}), X_2^r(m_0^{(b)}, m_2'^{(b)}, m_2''^{(b)}), m_0^{(b)} \in [\![1, 2^{r\rho_0}]\!],\\ &m_1'^{(b)} \in [\![1, 2^{r\rho_1'}]\!], m_1''^{(b)} \in [\![1, 2^{r\rho_1''}]\!], m_2'^{(b)} \in [\![1, 2^{r\rho_2'}]\!], m_2''^{(b)} \in [\![1, 2^{r\rho_2''}]\!]\} \qquad (3.140)\end{aligned}$$

The messages $M_1'^{(b)}$ and $M_2'^{(b)}$ are part of $M_1^{(b)}$ and $M_2^{(b)}$ respectively and represent the local randomness at each encoder. The messages $M_1''^{(b)}$ and $M_2''^{(b)}$ are part of $M_1^{(b)}$ and $M_2^{(b)}$ respectively that are used by both encoders toward the creation of $M_0^{(b+1)}$, assuming $\rho_1'' + \rho_2'' > \rho_0$. Furthermore, for $\gamma \in [\![0, 1]\!]$, an amount $\gamma(\rho_1'' + \rho_2'' - \rho_0)$ is recycled towards the creation of $M_1'^{(b+1)}$ and an amount $(1-\gamma)(\rho_1'' + \rho_2'' - \rho_0)$ is recycled towards the creation of $M_2'^{(b+1)}$.

Next we bound $\mathbb{D}(P_{Z^n}||Q_Z^{\otimes n})$ and show that dependencies across blocks created by block-Markov encoding can be eliminated by appropriately recycling randomness from one block to the next.

$$
\begin{aligned}
&\mathbb{D}(P_{Z^n}||Q_Z^{\otimes n})\\
&\quad= \mathbb{D}(P_{Z_1^r\dots Z_B^r}||Q_Z^{\otimes rB})\\
&\quad= \sum_{b=1}^{B} \mathbb{D}(P_{Z_j^r|Z_{b+1}^{B,r}}||Q_Z^{\otimes r}|P_{Z_{b+1}^{B,r}}) && (3.141)\\
&\quad= \sum_{b=1}^{B} \mathbb{D}(P_{Z_j^r}||Q_Z^{\otimes r}) + \sum_{b=1}^{B} \mathbb{D}(P_{Z_j^r|Z_{b+1}^{B,r}}||P_{Z_j^r}|P_{Z_{b+1}^{B,r}}) && (3.142)\\
&\quad= \sum_{b=1}^{B} \mathbb{D}(P_{Z_b^r}||Q_Z^{\otimes r}) + \sum_{b=1}^{B} I(Z_b^r;Z_{b+1}^{B,r}) && (3.143)\\
&\quad\overset{(a)}{\le} \sum_{b=1}^{B} \mathbb{D}(P_{M_1''^{(b)},M_2''^{(b)},Z_b^r}||P_{M_1''^{(b)},M_2''^{(b)}}Q_Z^{\otimes r}) + \sum_{b=1}^{B} I(Z_b^r;M_1''^{(b)},\hat{M}_1''^{(b)},M_2''^{(b)},\hat{M}_2''^{(b)},Z_{b+1}^{B})\\
& && (3.144)\\
&\quad\overset{(b)}{=} \sum_{b=1}^{B} \mathbb{D}(P_{M_1''^{(b)},M_2''^{(b)},Z_b^r}||P_{M_1''^{(b)},M_2''^{(b)}}Q_Z^{\otimes r}) + \sum_{b=1}^{B} I(Z_b^r;M_1''^{(b)},\hat{M}_1''^{(b)},M_2''^{(b)},\hat{M}_2''^{(b)}) && (3.145)\\
&\quad\overset{(c)}{\le} \sum_{b=1}^{B} 2\times\mathbb{D}(P_{M_1''^{(b)},M_2''^{(b)},Z_b^r}||P_{M_1''^{(b)},M_2''^{(b)}}Q_Z^{\otimes r}) + \sum_{b=1}^{B} H(\hat{M}_1''^{(b)},\hat{M}_2''^{(b)}|M_1''^{(b)},M_2''^{(b)}) && (3.146)
\end{aligned}
$$

where

(a) follows since $\mathbb{D}(P_{Z_b^r}||Q_Z^{\otimes r}) = \mathbb{D}(P_{Z_b^r,M_1''^{(b)},M_2''^{(b)}}||P_{M_1''^{(b)},M_2''^{(b)}}Q_Z^{\otimes r}) - \mathbb{D}(P_{Z_b^r,M_1''^{(b)},M_2''^{(b)}}||P_{M_1''^{(b)},M_2''^{(b)}}P_{Z_b^r})$;

(b) follows since $Z_b^r \to M_1''^{(b)},\hat{M}_1''^{(b)},M_2''^{(b)},\hat{M}_2''^{(b)} \to Z_{b+1}^{B,r}$ holds; follows since $I(Z_b^r;M_1''^{(b)},M_2''^{(b)}) = \mathbb{D}(P_{Z_b^r,M_1''^{(b)},M_2''^{(b)}}||P_{M_1''^{(b)},M_2''^{(b)}}P_{Z_b^r}) \le \mathbb{D}(P_{Z_b^r,M_1''^{(b)},M_2''^{(b)}}||P_{M_1''^{(b)},M_2''^{(b)}}Q_Z^{\otimes r})$.

Let $P_e^{(b)}$ be the average error probability of both encoders decoding the other encoder's message. From Fano's inequality, we can write $H(\hat{M}_1''^{(b)},\hat{M}_2''^{(b)}|M_1''^{(b)},M_2''^{(b)}) \le H(\hat{M}_1''^{(b)}|M_1''^{(b)}) + H(\hat{M}_2''^{(b)}|M_2''^{(b)}) \le 2H(P_e^{(b)}) + r(\rho_1''+\rho_2'')P_e^{(b)}$. By random coding we know that $\mathbb{E}_{\mathfrak{C}_r}\left(P_e^{(b)}\right) < 2^{-\alpha r}$ for some $\alpha > 0$ and all r large enough if $\rho_1' + \rho_1'' < H(X_1|U)$ and $\rho_2' + \rho_2'' < H(X_2|U)$.

Let $\bar{P}$ be the probability distribution induced when both encoders are using the same $M_0^{(b)}$, i.e., $(\hat{M}_1''^{(b-1)}, \hat{M}_2''^{(b-1)}) = (M_1''^{(b-1)}, M_2''^{(b-1)})$.

$$
\begin{aligned}
&\mathbb{E}_{\mathfrak{C}_r}\big(\mathbb{D}(\bar{P}_{Z_b^r, M_1''^{(b)}, M_2''^{(b)}} || \bar{P}_{M_1''^{(b)}, M_2''^{(b)}} Q_Z^{\otimes r})\big) \\
&\quad = \mathbb{E}_{\mathfrak{C}_r} \sum_{m_1''^{(b)}, m_2''^{(b)}, z_b^r} \bar{P}_{Z_b^r, M_1''^{(b)}, M_2''^{(b)}} \log \frac{\bar{P}_{Z_b^r | M_1''^{(b)}, M_2''^{(b)}}}{Q_Z^{\otimes r}} && (3.147) \\
&\quad = \mathbb{E}_{\mathfrak{C}_r} \sum_{m_1''^{(b)}, m_2''^{(b)}, z_b^r} 2^{-r(\rho_1''+\rho_2'')} \sum_{m_0^{(b)}, m_1'^{(b)}, m_2'^{(b)}} 2^{-r(\rho_0+\rho_1'+\rho_2')} \\
&\qquad\quad W^{\otimes r}(z_b^r | U^r(m_0^{(b)}), X_1^r(m_0^{(b)}, m_1'^{(b)}, m_1''^{(b)}), X_2^r(m_0^{(b)}, m_2'^{(b)}, m_2''^{(b)})) \\
&\qquad\quad \times \log \sum_{i,j,k} \frac{W^{\otimes r}(z_b^r | U^r(i), X_1^r(i,j,m_1''^{(b)}), X_2^r(i,k,m_2''^{(b)}))}{2^{r(\rho_0+\rho_1'+\rho_2')} Q_Z^{\otimes r}} && (3.148) \\
&\quad \overset{(a)}{\leq} \sum_{m_1''^{(b)}, m_2''^{(b)}, z_b^r} 2^{-r(\rho_1''+\rho_2'')} \sum_{m_0^{(b)}, m_1'^{(b)}, m_2'^{(b)}} 2^{-r(\rho_0+\rho_1'+\rho_2')} \sum_{u^r(m_0^{(b)}), x_1^r(m_0^{(b)}, m_1'^{(b)}, m_1''^{(b)}), x_2^r(m_0^{(b)}, m_2'^{(b)}, m_2''^{(b)})} \\
&\qquad\quad \bar{P}^{\otimes r}(u^r(m_0^{(b)}), x_1^r(m_0^{(b)}, m_1'^{(b)}, m_1''^{(b)}), x_2^r(m_0^{(b)}, m_2'^{(b)}, m_2''^{(b)}), z_b^r) \\
&\qquad\quad \times \log \mathbb{E}_{\setminus(m_0^{(b)}, m_1'^{(b)}, m_2'^{(b)})} \\
&\qquad\quad \sum_{i,j,k} \frac{W^{\otimes r}(z_b^r | U^r(i), X_1^r(i,j,m_1''^{(b)}), X_2^r(i,k,m_2''^{(b)}))}{2^{r(\rho_0+\rho_1'+\rho_2')} Q_Z^{\otimes r}} && (3.149) \\
&\quad = \sum_{m_1''^{(b)}, m_2''^{(b)}, z_b^r} 2^{-r(\rho_1''+\rho_2'')} \sum_{m_0^{(b)}, m_1'^{(b)}, m_2'^{(b)}} 2^{-r(\rho_0+\rho_1'+\rho_2')} \sum_{u^r(m_0^{(b)}), x_1^r(m_0^{(b)}, m_1'^{(b)}, m_1''^{(b)}), x_2^r(m_0^{(b)}, m_2'^{(b)}, m_2''^{(b)})} \\
&\qquad\quad \bar{P}^{\otimes r}(u^r(m_0^{(b)}), x_1^r(m_0^{(b)}, m_1'^{(b)}, m_1''^{(b)}), x_2^r(m_0^{(b)}, m_2'^{(b)}, m_2''^{(b)}), z_b^r) \\
&\qquad\quad \times \log \mathbb{E}_{\setminus(m_0^{(b)}, m_1'^{(b)}, m_2'^{(b)})} \frac{1}{2^{r(\rho_0+\rho_1'+\rho_2')} Q_Z^{\otimes r}} \\
&\qquad\quad \Bigg[W^{\otimes r}(z_b^r | u^r(m_0^{(b)}), x_1^r(m_0^{(b)}, m_1'^{(b)}, m_1''^{(b)}), x_2^r(m_0^{(b)}, m_2'^{(b)}, m_2''^{(b)}))
\end{aligned}
$$

$$+ \sum_{j \neq m_1'^{(b)}} W^{\otimes r}(z_b^r | u^r(m_0^{(b)}), X_1^r(m_0^{(b)}, j, m_1''^{(b)}), x_2^r(m_0^{(b)}, m_2'^{(b)}, m_2''^{(b)}))$$

$$+ \sum_{k \neq m_2'^{(b)}} W^{\otimes r}(z_b^r | u^r(m_0^{(b)}), x_1^r(m_0^{(b)}, m_1'^{(b)}, m_1''^{(b)}), X_2^r(m_0^{(b)}, e, m_2''^{(b)}))$$

$$+ \sum_{\substack{j \neq m_1'^{(b)} \\ k \neq m_2'^{(b)}}} W^{\otimes r}(z_b^r | u^r(m_0^{(b)}), X_1^r(m_0^{(b)}, j, m_1''^{(b)}), X_2^r(m_0^{(b)}, k, m_2''^{(b)}))$$

$$+ \sum_{\substack{i \neq m_0^{(b)} \\ j,k}} W^{\otimes r}(z_b^r | U^r(a), X_1^r(i, j, m_1''^{(b)}), X_2^r(i, k, m_2''^{(b)}))\Bigg] \tag{3.150}$$

$$\overset{(b)}{\leq} \sum_{m_1''^{(b)}, m_2''^{(b)}, z_b^r} 2^{-n(\rho_1'' + \rho_2'')} \sum_{m_0^{(b)}, m_1'^{(b)}, m_2'^{(b)}} 2^{-r(\rho_0 + \rho_1' + \rho_2')} \sum_{u^r(m_0^{(b)}), x_1^r(m_0^{(b)}, m_1'^{(b)}, m_1''^{(b)}), x_2^r(m_0^{(b)}, m_2'^{(b)}, m_2''^{(b)})}$$

$$\bar{P}^{\otimes r}(u^r(m_0^{(b)}), x_1^r(m_0^{(b)}, m_1'^{(b)}, m_1''^{(b)}), x_2^r(m_0^{(b)}, m_2'^{(b)}, m_2''^{(b)}), z_b^r)$$

$$\times \log \frac{1}{2^{r(\rho_0 + \rho_1' + \rho_2')} Q_Z^{\otimes r}}$$

$$\Bigg[W^{\otimes r}(z_b^r | u^r(m_0^{(b)}), x_1^r(m_0^{(b)}, m_1'^{(b)}, m_1''^{(b)}), x_2^r(m_0^{(b)}, m_2'^{(b)}, m_2''^{(b)}))$$

$$+ \sum_{j \neq m_1'^{(b)}} \bar{P}^{\otimes r}(z_b^r | u^r(m_0^{(b)}), x_2^r(m_0^{(b)}, m_2'^{(b)}, m_2''^{(b)}))$$

$$+ \sum_{k \neq m_2'^{(b)}} \bar{P}^{\otimes r}(z_b^r | u^r(m_0^{(b)}), x_1^r(m_0^{(b)}, m_1'^{(b)}, m_1''^{(b)}))$$

$$+ \sum_{\substack{j \neq m_1'^{(b)} \\ k \neq m_2'^{(b)}}} \bar{P}^{\otimes r}(z_b^r | u^r(m_0^{(b)}))$$

$$+ \sum_{\substack{i \neq m_0^{(b)} \\ j,k}} \bar{P}^{\otimes r}(z_b^r)\Bigg] \tag{3.151}$$

$$\overset{(c)}{=} \Psi_1 + \Psi_2 \tag{3.152}$$

where

(a) follows by Jensen's Inequality;

(b) follows by taking the expectation inside the log of the previous step;

(c) Ψ_1 is found by restricting the sum in the previous step over $(u^r, x_1^r, x_2^r, z_b^r) \in \mathcal{T}_\epsilon^r(P_{U,X_1,X_2,Y,Z})$ and Ψ_2 is found by restricting that sum over $(u^r, x_1^r, x_2^r, z_b^r) \notin \mathcal{T}_\epsilon^r(P_{U,X_1,X_2,Z})$.

Solving Ψ_1 and Ψ_2 like in previous sections we find that $\mathbb{D}(\bar{P}_{Z_b^r, M_1''^{(b)}, M_2''^{(b)}} || \bar{P}_{M_1''^{(b)}, M_2''^{(b)}} Q_Z^{\otimes r}) \xrightarrow{r\to\infty} 0$ if:

$$\rho_0 + \rho_1' + \rho_2' > I(X_1, X_2; Z) \tag{3.153}$$

$$\rho_0 + \rho_2' > I(U, X_2; Z) \tag{3.154}$$

$$\rho_0 + \rho_1' > I(U, X_1; Z) \tag{3.155}$$

$$\rho_0 > I(U; Z) \tag{3.156}$$

Let $\epsilon > 0$, set

$$\rho_0 = I(U; Z) + \epsilon \tag{3.157}$$

$$\rho_1' = I(X_1; Z|U) + \epsilon \tag{3.158}$$

$$\rho_1'' = H(X_1|U) - I(X_1; Z|U) - 2\epsilon \tag{3.159}$$

$$\rho_2' = I(X_2; Z|U, X_1) + \epsilon \tag{3.160}$$

$$\rho_2'' = H(X_2|U) - I(X_2; Z|U, X_1) - 2\epsilon \tag{3.161}$$

We can write the effective rates of new randomness at both encoders as:

$$R_1 \triangleq \rho_1' + \rho_1'' - \gamma(\rho_1'' + \rho_2'' - \rho_0) \tag{3.162}$$

$$R_2 \triangleq \rho_2' + \rho_2'' - (1-\gamma)(\rho_1'' + \rho_2'' - \rho_0) \tag{3.163}$$

$$R_1 + R_2 \triangleq \rho_1' + \rho_2' + \rho_0 \tag{3.164}$$

Using the values of ρ_0, ρ_1', ρ_1'', ρ_2' and ρ_2'' chosen above, we obtain the rate region as follows:

$$R_1 \geq I(X_1, X_2; Z) - H(X_2|U) + 4\epsilon \tag{3.165}$$

$$R_2 \geq I(X_1, X_2; Z) - H(X_1|U) + 4\epsilon \tag{3.166}$$

$$R_1 + R_2 \geq I(X_1, X_2; Z) + 3\epsilon \tag{3.167}$$

Finally we note that $\mathbb{E}_{\mathfrak{C}_r}\big(\mathbb{D}(\bar{P}_{Z_b^r, M_1''^{(b)}, M_2''^{(b)}}||\bar{P}_{M_1''^{(b)}, M_2''^{(b)}} Q_Z^{\otimes r})\big) \xrightarrow{r\to\infty} 0$ implies $\mathbb{E}_{\mathfrak{C}_r}\big(\mathbb{D}(P_{Z_b^r, M_1''^{(b)}, M_2''^{(b)}}||P_{M_1''^{(b)}, M_2''^{(b)}} Q_Z^{\otimes r})\big) \xrightarrow{r\to\infty} 0$ (see discussion in Section 3.4.1) if

$$\rho_1' + \rho_1'' < H(X_1|U) \tag{3.168}$$

$$\rho_2' + \rho_2'' < H(X_2|U) \tag{3.169}$$

Converse:

$$\begin{aligned}
nR_1 &= H(M_1) \\
&\geq H(M_1|X_2^n) \\
&\geq I(M_1; Z^n|X_2^n) \\
&\overset{(a)}{=} I(M_1, X_1^n; Z^n|X_2^n) && (3.170) \\
&\geq I(X_1^n; Z^n|X_2^n) \\
&= I(X_1^n, X_2^n; Z^n) - I(X_2^n; Z^n) && (3.171) \\
&= \sum_{x_1^n}\sum_{x_2^n}\sum_{z^n} P(x_1^n, x_2^n, z^n) \log \frac{W^{\otimes n}(z^n|x_1^n, x_2^n)}{P_{Z^n}(z^n)} - I(X_2^n; Z^n) \\
&\geq \sum_{x_1^n}\sum_{x_2^n}\sum_{z^n} P(x_1^n, x_2^n, z^n) \log \frac{W^{\otimes n}(z^n|x_1^n, x_2^n)}{Q_Z^{\otimes n}(z^n)} - \mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) - H(X_2^n) \\
&\overset{(b)}{\geq} \sum_{i}\sum_{x_{1i}}\sum_{x_{2i}}\sum_{z_i} P(x_{1i}, x_{2i}, z_i) \log \frac{W(z_i|x_{1i}, x_{2i})}{Q(z_i)} - \sum_i H(X_{2i}|U_{2i}) - \epsilon \\
&= \sum_{i}\sum_{i}\sum_{x_{1i}}\sum_{x_{2i}} P(x_{1i}, x_{2i}, z_i) \log \frac{W(z_i|x_{1i}, x_{2i})}{P(z_i)} + \mathbb{D}(P_{Z_i}||Q_Z) - \sum_i H(X_{2i}|U_{2i}) - \epsilon
\end{aligned}$$

$$
\begin{aligned}
&\geq \sum_i I(X_{1i}, X_{2i}; Z_i) - \sum_i H(X_{2i}|U_{2i}) - \epsilon \\
&= nI(X_{1Q}X_{2Q}; Z_Q|Q) - nH(X_{2Q}|U_{2Q}Q) - \epsilon \\
&= nI(QX_{1Q}X_{2Q}; Z_Q) - nI(Q; Z_Q) - nH(X_{2Q}|U_{2Q}Q) - \epsilon \\
&\overset{(c)}{\geq} nI(X_{1Q}X_{2Q}; Z_Q) - nH(X_{2Q}|U_{2Q}Q) - n\epsilon' \\
&= nI(X_1X_2; Z) - nH(X_2|U_2) - n\epsilon' \qquad (3.172)
\end{aligned}
$$

where

(a) follows from the definition of the encoding function in (3.13),

(b) follows by setting $U_{2i} \triangleq X_2^{i-1}$,

(c) follows by [4, Lemma VI.3] for some $\epsilon' > 0$ with $\lim_{\epsilon \to 0} \epsilon' = 0$.

Similarly we get,

$$nR_2 \geq nI(X_1X_2; Z) - nH(X_1|U_1) - n\epsilon' \qquad (3.173)$$

and

$$n(R_1 + R_2) \geq nI(X_1X_2; Z) - n\epsilon' \qquad (3.174)$$

3.4.8 Strong secrecy of MAC with two-sided strictly-causal cribbing

Achievability:

We use a combination of block-Markov encoding and backward decoding. Independently and uniformly distributed messages $m_1^{(b)} \in [\![1, 2^{rR_1}]\!]$ and $m_2^{(b)} \in [\![1, 2^{rR_2}]\!]$ will be sent over B blocks. Each block consists of r transmissions so that $n = rB$. Consider a distribution $P(u, x_1, x_2) = P(u)P(x_1|u)P(x_2|u)$ such that $\sum_{u,x_1,x_2} P(u, x_1, x_2)W(z|x_1, x_2) = Q_Z(z)$.

Code Construction: In each block $b \in [\![1, B]\!]$:

- Independently generate $2^{r(R_1+\rho_1'+\rho_1''+R_2+\rho_2'+\rho_2'')}$ codewords u_b^r each with probability $P(u^r) = P_U^{\otimes r}(u^r)$. Label them $u^r(m_0^{(b)}, m_0'^{(b)}, m_0''^{(b)})$, $m_0^{(b)} \in [\![1, 2^{r(R_1+R_2)}]\!]$, $m_0'^{(b)} \in [\![1, 2^{r(\rho_1'+\rho_2')}]\!]$ and $m_0''^{(b)} \in [\![1, 2^{r(\rho_1''+\rho_2'')}]\!]$.

- For every $u^r(m_0^{(b)}, m_0'^{(b)}, m_0''^{(b)})$, independently generate $2^{r(R_1+\rho_1'+\rho_1'')}$ codewords x_{1b}^r each with probability $P(x_1^r|u^r(m_0^{(b)}, m_0'^{(b)}, m_0''^{(b)})) = P_{X_1|U}^{\otimes r}(x_1^r|u^r(m_0^{(b)}, m_0'^{(b)}, m_0''^{(b)}))$. Label them $x_1^r(m_0^{(b)}, m_0'^{(b)}, m_0''^{(b)}, m_1^{(b)}, m_1'^{(b)}, m_1''^{(b)})$, $m_1^{(b)} \in [\![1, 2^{rR_1}]\!]$, $m_1'^{(b)} \in [\![1, 2^{r\rho_1'}]\!]$ and $m_1''^{(b)} \in [\![1, 2^{r\rho_1''}]\!]$.

- For every $u^r(m_0^{(b)}, m_0'^{(b)}, m_0''^{(b)})$, independently generate $2^{r(R_2+\rho_2'+\rho_2'')}$ codewords x_{2b}^r each with probability $P(x_2^r|u^r(m_0^{(b)}, m_0'^{(b)}, m_0''^{(b)})) = P_{X_2|U}^{\otimes r}(x_2^r|u^r(m_0^{(b)}, m_0'^{(b)}, m_0''^{(b)}))$. Label them $x_2^r(m_0^{(b)}, m_0'^{(b)}, m_0''^{(b)}, m_2^{(b)}, m_2'^{(b)}, m_2''^{(b)})$, $m_2^{(b)} \in [\![1, 2^{rR_2}]\!]$, $m_2'^{(b)} \in [\![1, 2^{r\rho_2'}]\!]$ and $m_2''^{(b)} \in [\![1, 2^{r\rho_2''}]\!]$.

We intend to use these codebooks in the following manner:

1. Block Markov encoding via $M_0^{(b)} = (M_1^{(b-1)}, M_2^{(b-1)})$, $M_0'^{(b)} = (M_1'^{(b-1)}, M_2'^{(b-1)})$ and $M_0''^{(b)} = (M_1''^{(b-1)}, M_2''^{(b-1)})$;

2. $M_1^{(b)}$, $M_1'^{(b)}$ and $M_1''^{(b)}$ can be decoded (at Encoder 2) from X_{1b}^r knowing $(M_0^{(b)}, M_0'^{(b)}, M_0''^{(b)})$;

3. $M_2^{(b)}$, $M_2'^{(b)}$ and $M_2''^{(b)}$ can be decoded (at Encoder 1) from X_{2b}^r knowing $(M_0^{(b)}, M_0'^{(b)}, M_0''^{(b)})$;

4. $\{M_1^{(1)}, \ldots, M_1^{(B)}\}$ and $\{M_2^{(1)}, \ldots, M_2^{(B)}\}$ are secret from $\{Z_1^r, \ldots, Z_B^r\}$;

5. $M_1''^{(b)}$ and $M_2''^{(b)}$ are the common randomness to be used by both encoders in block $b+1$;

6. $M_1'^{(b)}$ is local randomness used by Encoder 1 and $M_2'^{(b)}$ is local randomness used by Encoder 2;

7. The messages $M_0^{(b)}$, $M_0'^{(b)}$, $M_0''^{(b)}$, $M_1^{(b)}$, $M_1'^{(b)}$, $M_1''^{(b)}$, $M_2^{(b)}$, $M_2'^{(b)}$ and $M_2''^{(b)}$ can be decoded at the receiver from Y_b^r and the messages decoded in future blocks $b+1$ to B (backward decoding).

As a result of cribbing, after block b, Encoder 2 finds estimates $(\hat{m}_1^{(b)}, \hat{m}_1'^{(b)}, \hat{m}_1''^{(b)})$ for $(m_1^{(b)}, m_1'^{(b)}, m_1''^{(b)})$ such that

$$(u^r(\hat{m}_0^{(b)}, \hat{m}_0'^{(b)}, \hat{m}_0''^{(b)}), x_1^r(\hat{m}_0^{(b)}, \hat{m}_0'^{(b)}, \hat{m}_0''^{(b)}, \hat{m}_1^{(b)}, \hat{m}_1'^{(b)}, \hat{m}_1''^{(b)}), x_{1b}^r) \in \mathcal{T}_\epsilon^{(r)}(P_{U,X_1,X_1}). \quad (3.175)$$

where $(\hat{m}_0^{(b)}, \hat{m}_0'^{(b)}, \hat{m}_0''^{(b)}) = (\hat{m}_1^{(b-1)}, m_2^{(b-1)}, \hat{m}_1'^{(b-1)}, m_2'^{(b-1)}, \hat{m}_1''^{(b-1)}, m_2''^{(b-1)})$. Also, Encoder 1 finds estimates $(\tilde{M}_2^{(b)}, \tilde{M}_2'^{(b)}, \tilde{M}_2''^{(b)})$ for $(m_2^{(b)}, m_2'^{(b)}, m_2''^{(b)})$ such that

$$(u^r(\tilde{M}_0^{(b)}, \tilde{M}_0'^{(b)}, \tilde{M}_0''^{(b)}), x_2^r(\tilde{M}_0^{(b)}, \tilde{M}_0'^{(b)}, \tilde{M}_0''^{(b)}, \tilde{M}_2^{(b)}, \tilde{M}_2'^{(b)}, \tilde{M}_2''^{(b)}), x_{2b}^r) \in \mathcal{T}_\epsilon^{(r)}(P_{U,X_2,X_2}). \quad (3.176)$$

where $(\tilde{m}_0^{(b)}, \tilde{m}_0'^{(b)}, \tilde{m}_0''^{(b)}) = (m_1^{(b-1)}, \tilde{m}_2^{(b-1)}, m_1'^{(b-1)}, \tilde{m}_2'^{(b-1)}, m_1''^{(b-1)}, \tilde{m}_2''^{(b-1)})$.

Encoding: We apply block-Markov encoding as follows. In block b, the encoders send:

$$x_{1b}^r = x_1^m(m_0^{(b)}, m_0'^{(b)}, m_0''^{(b)}, m_1^{(b)}, m_1'^{(b)}, m_1''^{(b)})$$
$$x_{2b}^r = x_2^m(\hat{m}_0^{(b)}, \hat{m}_0'^{(b)}, \hat{m}_0''^{(b)}, m_2^{(b)}, m_2'^{(b)}, m_2''^{(b)})$$

We also assume that the encoders and decoder have access to $(M_0^{(1)}, M_0'^{(1)}, M_0''^{(1)}, M_1^{(B)}, M_1'^{(B)}, M_1''^{(B)}, M_2^{(B)}, M_2'^{(B)})$ through private common randomness.

Decoding at the receiver: The legitimate receiver waits until all B blocks are transmitted and then performs backward decoding. The decoder first finds $(\hat{\hat{m}}_0^{(B)}, \hat{\hat{m}}_0'^{(B)}, \hat{\hat{m}}_0''^{(B)})$ such that

$$\begin{aligned}(u^r(\hat{\hat{m}}_0^{(B)}, \hat{\hat{m}}_0'^{(B)}, \hat{\hat{m}}_0''^{(B)}), x_1^r(\hat{\hat{m}}_0^{(B)}, \hat{\hat{m}}_0'^{(B)}, \hat{\hat{m}}_0''^{(B)}, \hat{\hat{m}}_1^{(B)}, \hat{\hat{m}}_1'^{(B)}, \hat{\hat{m}}_1''^{(B)}),\\ x_2^r(\hat{\hat{m}}_0^{(B)}, \hat{\hat{m}}_0'^{(B)}, \hat{\hat{m}}_0''^{(B)}, \hat{\hat{m}}_2^{(B)}, \hat{\hat{m}}_2'^{(B)}, \hat{\hat{m}}_2''^{(B)}), y_B^r) \in \mathcal{T}_\epsilon^{(r)}(P_{U,X_1,X_2,Y}).\end{aligned}$$

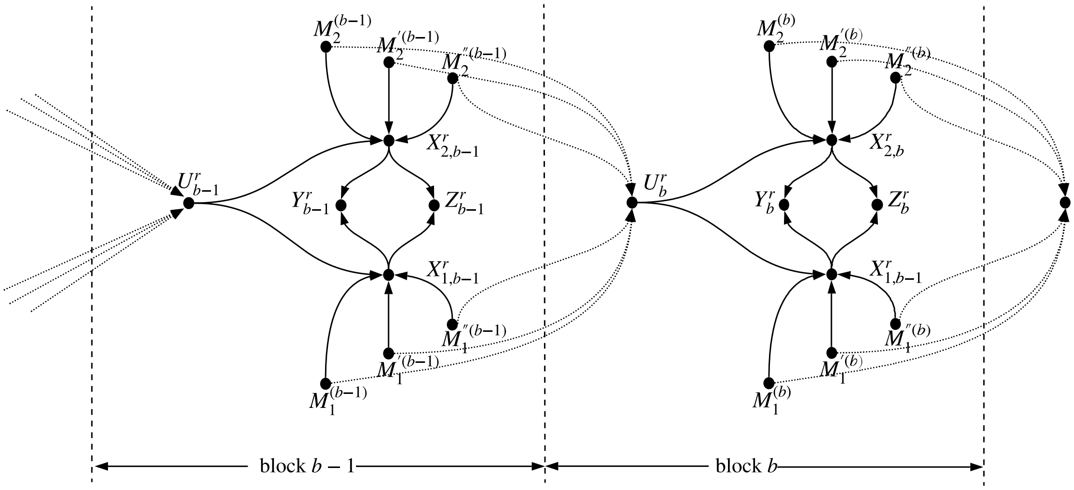

Figure 3.13. Functional dependence graph for the block-Markov encoding scheme for MAC with two-sided strictly-causal cribbing.

Assuming that $(m_0^{(B)}, m_0'^{(B)}, m_0''^{(B)})$, $(m_0^{(B-1)}, m_0'^{(B-1)}, m_0''^{(B-1)})$, $\ldots$, $(m_0^{(b+1)}, m_0'^{(b+1)}, m_0''^{(b+1)})$ have been decoded, the decoder sets $(\hat{\hat{m}}_1^{(b)}, \hat{\hat{m}}_1'^{(b)}, \hat{\hat{m}}_1''^{(b)}) = (\hat{\hat{m}}_0^{(b+1)}, \hat{\hat{m}}_0'^{(b+1)}, \hat{\hat{m}}_0''^{(b+1)})$ and finds $(\hat{\hat{m}}_0^{(b)}, \hat{\hat{m}}_0'^{(b)}, \hat{\hat{m}}_0''^{(b)})$ and $(\hat{\hat{m}}_2^{(b)}, \hat{\hat{m}}_2'^{(b)})$ such that

$$\begin{aligned}&(u^r(\hat{\hat{m}}_0^{(b)}, \hat{\hat{m}}_0'^{(b)}, \hat{\hat{m}}_0''^{(b)}), x_1^r(\hat{\hat{m}}_0^{(b)}, \hat{\hat{m}}_0'^{(b)}, \hat{\hat{m}}_0''^{(b)}, \hat{\hat{m}}_1^{(b)}, \hat{\hat{m}}_1'^{(b)}, \hat{\hat{m}}_1''^{(b)}),\\ &\qquad x_2^r(\hat{\hat{m}}_0^{(b)}, \hat{\hat{m}}_0'^{(b)}, \hat{\hat{m}}_0''^{(b)}, \hat{\hat{m}}_2^{(b)}, \hat{\hat{m}}_2'^{(b)}, \hat{\hat{m}}_2''^{(b)}), y_b^r) \in \mathcal{T}_\epsilon^{(r)}(P_{U,X_1,X_2,Y}).\end{aligned}$$

Probability of error analysis: Using the arguments for error analysis from [35, Lemma 4], the probability of error of each block vanishes exponentially with r and in turn vanishes across blocks if

$$R_1 + \rho_1' + \rho_1'' < H(X_1|U), \tag{3.177}$$

$$R_2 + \rho_2' + \rho_2'' < H(X_2|U), \tag{3.178}$$

$$R_1 + \rho_1' + \rho_1'' + R_2 + \rho_2' + \rho_2'' < I(X_1, X_2; Y). \tag{3.179}$$

Secrecy analysis: Let $\bar{P}$ be the probability induced when both encoders use $(M_0^{(b)}, M_0'^{(b)}, M_0''^{(b)})$. Let P be the probability when Encoder 1 uses the estimate $(\tilde{M}_0^{(b)}, \tilde{M}_0'^{(b)}, \tilde{M}_0''^{(b)})$ and Encoder 2 uses the estimate $(\hat{M}_0^{(b)}, \hat{M}_0'^{(b)}, \hat{M}_0''^{(b)})$. For the secrecy analysis, we find conditions so that $I(M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)}, M_2^{(b)}, M_2'^{(b)}, M_2''^{(b)}, M_0^{(b)}, \tilde{M}_0^{(b)}, \hat{M}_0^{(b)}, \tilde{M}_0'^{(b)}, \hat{M}_0'^{(b)}; Z_b^r)$ vanishes exponentially with r. This is motivated by:

- $(M_1^{(b)}, M_2^{(b)}, M_0^{(b)}, \tilde{M}_0^{(b)}, \hat{M}_0^{(b)})$ are the Encoder 1 and Encoder 2 secret messages in the present, the past and the estimates of the latter (at Encoder 1 and Encoder 2 respectively), which must be kept secret from Z_b^r.
- $(M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)})$ and $(M_2^{(b)}, M_2'^{(b)}, M_2''^{(b)})$ must be kept independent of Z_b^r according to the functional dependence graph (Figure 3.13) to ensure the distribution of Z remains i.i.d. across blocks
- $\tilde{M}_0'^{(b)}$ and $\hat{M}_0'^{(b)}$ are kept independent from Z_b^r to allow Encoder 1 and Encoder 2 to possess a *local* randomness that is separate from the common randomness shared with between each other: Resolvability analysis showed us that having a local randomness at both encoders can be beneficial for achievable rates.

Let $\bar{I}(\cdot;\cdot)$ be the mutual information according to $\bar{P}$

$$\begin{aligned}
&\bar{I}(M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)}, M_2^{(b)}, M_2'^{(b)}, M_2''^{(b)}, M_0^{(b)}, \tilde{M}_0^{(b)}, \hat{M}_0^{(b)}, \tilde{M}_0'^{(b)}, \hat{M}_0'^{(b)}; Z_b^r) \\
&\quad = \mathbb{D}(\bar{P}_{M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)}, M_2^{(b)}, M_2'^{(b)}, M_2''^{(b)}, M_0^{(b)}, \tilde{M}_0^{(b)}, \hat{M}_0^{(b)}, \tilde{M}_0'^{(b)}, \hat{M}_0'^{(b)} Z_b^r} || \\
&\qquad\qquad\qquad \bar{P}_{M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)}, M_2^{(b)}, M_2'^{(b)}, M_2''^{(b)}, M_0^{(b)}, \tilde{M}_0^{(b)}, \hat{M}_0^{(b)}, \tilde{M}_0'^{(b)}, \hat{M}_0'^{(b)}} \bar{P}_{Z_b^r}) \\
&\quad \leq \mathbb{D}(\bar{P}_{M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)}, M_2^{(b)}, M_2'^{(b)}, M_2''^{(b)}, M_0^{(b)}, \tilde{M}_0^{(b)}, \hat{M}_0^{(b)}, \tilde{M}_0'^{(b)}, \hat{M}_0'^{(b)} Z_b^r} || \\
&\qquad\qquad\qquad \bar{P}_{M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)}, M_2^{(b)}, M_2'^{(b)}, M_2''^{(b)}, M_0^{(b)}, \tilde{M}_0^{(b)}, \hat{M}_0^{(b)}, \tilde{M}_0'^{(b)}, \hat{M}_0'^{(b)}} Q_Z^{\otimes r})
\end{aligned} \tag{3.180}$$

Similar to Section 3.4.11, the divergence in (3.180) can be shown to vanish exponentially with r if:

$$\rho_1'' + \rho_2'' > I(U;Z), \tag{3.181}$$

$$\rho_1' + \rho_1'' + \rho_2'' > I(U,X_1;Z), \tag{3.182}$$

$$\rho_2' + \rho_1'' + \rho_2'' > I(U,X_2;Z), \tag{3.183}$$

$$\rho_1' + \rho_2' + \rho_1'' + \rho_2'' > I(X_1,X_2;Z). \tag{3.184}$$

Define $M_1^{(a:b)} = \{M_1^{(a)}, \ldots, M_1^{(b)}\}$, $M_2^{(a:b)} = \{M_2^{(a)}, \ldots, M_2^{(b)}\}$ and $Z^{(1:b),r} = \{Z_1^r, \ldots, Z_b^r\}$.

$$\begin{aligned}
&\bar{I}(M_1^{(a:b)}, M_2^{(a:b)}; Z^{(1:b),r})\\
&\leq \bar{I}(M_1^{(1:b)}, M_1'^{(b)}, M_1''^{(b)}, M_2^{(1:b)}, M_2'^{(b)}, M_2''^{(b)}, M_0^{(b)}, \tilde{M}_0^{(b)}, \hat{M}_0^{(b)}, \tilde{M}_0'^{(b)}, \hat{M}_0'^{(b)}; Z^{(1:b),r}) \qquad (3.185)\\
&= \bar{I}(M_1^{(1:b)}, M_1'^{(b)}, M_1''^{(b)}, M_2^{(1:b)}, M_2'^{(b)}, M_2''^{(b)}, M_0^{(b)}, \tilde{M}_0^{(b)}, \hat{M}_0^{(b)}, \tilde{M}_0'^{(b)}, \hat{M}_0'^{(b)}; Z_b^r)\\
&\quad + \bar{I}(M_1^{(1:b)}, M_1'^{(b)}, M_1''^{(b)}, M_2^{(1:b)}, M_2'^{(b)}, M_2''^{(b)}, M_0^{(b)}, \tilde{M}_0^{(b)}, \hat{M}_0^{(b)}, \tilde{M}_0'^{(b)}, \hat{M}_0'^{(b)}; Z^{(1:b-1),r}|Z_b^r)\\
&\qquad (3.186)\\
&= \bar{I}(M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)}, M_2^{(b)}, M_2'^{(b)}, M_2''^{(b)}, M_0^{(b)}, \tilde{M}_0^{(b)}, \hat{M}_0^{(b)}, \tilde{M}_0'^{(b)}, \hat{M}_0'^{(b)}; Z_b^r)\\
&\quad + \bar{I}(M_1^{(1:b-1)}, M_2^{(1:b-1)}; Z_b^r|M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)}, M_2^{(b)}, M_2'^{(b)}, M_2''^{(b)}, M_0^{(b)}, \tilde{M}_0^{(b)}, \hat{M}_0^{(b)}, \tilde{M}_0'^{(b)}, \hat{M}_0'^{(b)})\\
&\quad + \bar{I}(M_1^{(1:b)}, M_1'^{(b)}, M_1''^{(b)}, M_2^{(1:b)}, M_2'^{(b)}, M_2''^{(b)}, M_0^{(b)}, \tilde{M}_0^{(b)}, \hat{M}_0^{(b)}, \tilde{M}_0'^{(b)}, \hat{M}_0'^{(b)}; Z^{(1:b-1),r}|Z_b^r)\\
&\qquad (3.187)\\
&\leq \bar{I}(M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)}, M_2^{(b)}, M_2'^{(b)}, M_2''^{(b)}, M_0^{(b)}, \tilde{M}_0^{(b)}, \hat{M}_0^{(b)}, \tilde{M}_0'^{(b)}, \hat{M}_0'^{(b)}; Z_b^r)\\
&\quad + \bar{I}(M_1^{(1:b-1)}, M_2^{(1:b-1)}; M_1''^{(b-1)}, M_2''^{(b-1)}, Z_b^r|M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)}, M_2^{(b)}, M_2'^{(b)}, M_2''^{(b)},\\
&\qquad\qquad M_0^{(b)}, \tilde{M}_0^{(b)}, \hat{M}_0^{(b)}, \tilde{M}_0'^{(b)}, \hat{M}_0'^{(b)})\\
&\quad + \bar{I}(M_1^{(1:b)}, M_1'^{(b)}, M_1''^{(b)}, M_2^{(1:b)}, M_2'^{(b)}, M_2''^{(b)}, M_0^{(b)}, \tilde{M}_0^{(b)}, \hat{M}_0^{(b)}, \tilde{M}_0'^{(b)}, \hat{M}_0'^{(b)}; Z^{(1:b-1),r}|Z_b^r)\\
&\qquad (3.188)\\
&\overset{(a)}{=} \bar{I}(M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)}, M_2^{(b)}, M_2'^{(b)}, M_2''^{(b)}, M_0^{(b)}, \tilde{M}_0^{(b)}, \hat{M}_0^{(b)}, \tilde{M}_0'^{(b)}, \hat{M}_0'^{(b)}; Z_b^r)\\
&\quad + \bar{I}(M_1^{(1:b-1)}, M_2^{(1:b-1)}; Z_b^r|M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)}, M_2^{(b)}, M_2'^{(b)}, M_2''^{(b)}, M_0^{(b)}, \tilde{M}_0^{(b)}, \hat{M}_0^{(b)},\\
&\qquad\qquad \tilde{M}_0'^{(b)}, \hat{M}_0'^{(b)}, M_1^{(b-1)}, M_1'^{(b-1)}, M_1''^{(b-1)}, M_2^{(b-1)}, M_2'^{(b-1)}, M_2''^{(b-1)})
\end{aligned}$$

$$+\,\bar{I}(M_1^{(1:b)}, M_1'^{(b)}, M_1''^{(b)}, M_2^{(1:b)}, M_2'^{(b)}, M_2''^{(b)}, M_0^{(b)}, \tilde{M}_0^{(b)}, \hat{M}_0^{(b)}, \tilde{M}_0'^{(b)}, \hat{M}_0'^{(b)}; Z^{(1:b-1),r}|Z_b^r) \tag{3.189}$$

$$\overset{(b)}{\leq} 2^{-\alpha r}$$

$$+\,\bar{I}(M_1^{(1:b)}, M_1'^{(b)}, M_1''^{(b)}, M_2^{(1:b)}, M_2'^{(b)}, M_2''^{(b)}, M_0^{(b)}, \tilde{M}_0^{(b)}, \hat{M}_0^{(b)}, \tilde{M}_0'^{(b)}, \hat{M}_0'^{(b)}; Z^{(1:b-1),r}|Z_b^r) \tag{3.190}$$

$$\leq 2^{-\alpha r} + \bar{I}(M_1^{(1:b)}, M_1'^{(b)}, M_1''^{(b)}, M_2^{(1:b)}, M_2'^{(b)}, M_2''^{(b)}, M_0^{(b)}, \tilde{M}_0^{(b)}, \hat{M}_0^{(b)}, \tilde{M}_0'^{(b)}, \hat{M}_0'^{(b)}, M_0^{(b-1)}, \tilde{M}_0^{(b-1)}, \hat{M}_0^{(b-1)}, \tilde{M}_0'^{(b-1)}, \hat{M}_0'^{(b-1)}, M_1''^{(b-1)}, M_2''^{(b-1)}, Z_b^r; Z^{(1:b-1),r}) \tag{3.191}$$

$$\overset{(c)}{=} 2^{-\alpha r} + \bar{I}(M_1^{(1:b-1)}, M_1'^{(b-1)}, M_1''^{(b-1)}, M_2^{(1:b-1)}, M_2'^{(b-1)}, M_2''^{(b-1)}, M_0^{(b-1)}, \tilde{M}_0^{(b-1)}, \hat{M}_0^{(b-1)}, \tilde{M}_0'^{(b-1)}, \hat{M}_0'^{(b-1)}; Z^{(1:b-1),r}) \tag{3.192}$$

$$\overset{(d)}{\leq} b \times 2^{-\alpha r}$$

Therefore $\bar{I}(M_1, M_2; Z^n) \leq B \times 2^{-\alpha r}$ where,

(a) holds because $M_0^{(b)} = \tilde{M}_0^{(b)} = \hat{M}_0^{(b)} = M_1^{(b-1)}$, $\tilde{M}_0'^{(b)} = \hat{M}_0'^{(b)} = M_1'^{(b-1)}$ and $(M_1''^{(b-1),}M_2''^{(b-1)})$ is independent of $(M_1^{(1:b-1)}, M_2^{(1:b-1)})$ by construction;

(b) holds because $\bar{I}(M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)}, M_2^{(b)}, M_2'^{(b)}, M_2''^{(b)}, M_0^{(b)}, \tilde{M}_0^{(b)}, \hat{M}_0^{(b)}, \tilde{M}_0'^{(b)}, \hat{M}_0'^{(b)}; Z_b^r) \leq 2^{-\alpha r}$ by (3.180)-(3.184) and $M_1^{(1:b-1)}, M_2^{(1:b-1)} \to M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)}, M_2^{(b)}, M_2'^{(b)}, M_2''^{(b)}, M_0^{(b)}, \tilde{M}_0^{(b)}, \hat{M}_0^{(b)}, \tilde{M}_0'^{(b)}\hat{M}_0'^{(b)}, M_1^{(b-1)}, M_1'^{(b-1)}, M_1''^{(b-1)}, M_2^{(b-1)}, M_2'^{(b-1)}, M_2''^{(b-1)} \to Z_b^r$ (see Figure 3.13);

(c) holds because $M_1^{(1:b)}, M_1'^{(b)}, M_1''^{(b)}, M_2^{(1:b)}, M_2'^{(b)}, M_2''^{(b)}, M_0^{(b)}, \tilde{M}_0^{(b)}, \hat{M}_0^{(b)}, \tilde{M}_0'^{(b)}, \hat{M}_0'^{(b)}, Z_b^r \to M_0^{(b-1)}, \tilde{M}_0^{(b-1)}, \hat{M}_0^{(b-1)}, \tilde{M}_0'^{(b-1)}, \hat{M}_0'^{(b-1)}, M_1''^{(b-1)}, M_2''^{(b-1)}; Z^{(1:b-1),r}$ (see Figure 3.13).

(d) holds by repeating (3.185)-(3.192) $b-1$ times.

Next we show that $I(M_1^{(1:b)}, M_2^{(1:b)}; Z^{(1:b),r})$ is not too different from $\bar{I}(M_1^{(1:b)}, M_2^{(1:b)}; Z^{(1:b),r})$.

$$
\begin{aligned}
&I(M_1^{(1:b)}, M_2^{(1:b)}; Z^{(1:b),r}) \\
&\quad = \mathbb{D}(P_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}} || P_{M_1^{(1:b)} M_2^{(1:b)}} P_{Z^{(1:b),r}}) \\
&\quad \overset{(a)}{\leq} \mathbb{D}(P_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}} || P_{M_1^{(1:b)} M_2^{(1:b)}} Q_Z^{\otimes br}) \\
&\quad = \sum_{m_1^{(1:b)}, m_2^{(1:b)}, z^{(1:b),r}} P(m_1^{(1:b)}, m_2^{(1:b)}, z^{(1:b),r}) \log \frac{P(m_1^{(1:b)}, m_2^{(1:b)}, z^{(1:b),r})}{\bar{P}(m_1^{(1:b)}, m_2^{(1:b)}, z^{(1:b),r})} \\
&\qquad + \sum_{m_1^{(1:b)}, m_2^{(1:b)}, z^{(1:b),r}} P(m_1^{(1:b)}, m_2^{(1:b)}, z^{(1:b),r}) \log \frac{\bar{P}(m_1^{(1:b)}, m_2^{(1:b)}, z^{(1:b),r})}{P(m_1^{(1:b)}, m_2^{(1:b)}) Q_Z^{\otimes br}} \\
&\qquad + \mathbb{D}(\bar{P}_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b,r)}} || P_{M_1^{(1:b)} M_2^{(1:b)}} Q_Z^{\otimes br}) - \mathbb{D}(\bar{P}_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}} || P_{M_1^{(1:b)} M_2^{(1:b)}} Q_Z^{\otimes br}) \\
&\quad = \mathbb{D}(P_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}} || \bar{P}_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}}) + \mathbb{D}(\bar{P}_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}} || P_{M_1^{(1:b)} M_2^{(1:b)}} Q_Z^{\otimes br}) \\
&\qquad + \sum_{m_1^{(1:b)}, m_2^{(1:b)}, z^{(1:b),r}} (P_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}} - \bar{P}_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}}) \log \frac{\bar{P}(m_1^{(1:b)}, m_2^{(1:b)}, z^{(1:b),r})}{P(m_1^{(1:b)}, m_2^{(1:b)}) Q_Z^{\otimes br}} \\
&\quad \overset{(b)}{\leq} \mathbb{D}(P_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}} || \bar{P}_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}}) + \mathbb{D}(\bar{P}_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}} || \bar{P}_{M_1^{(1:b)} M_2^{(1:b)}} Q_Z^{\otimes br}) \\
&\qquad + \log \frac{1}{\mu} \mathbb{V}(P_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}}, \bar{P}_{M_1^{(1:b)} M_2^{(1:b)} Z^{b,r}}) \\
&\quad \overset{(c)}{\leq} 2 \log \frac{1}{\mu} \mathbb{V}(P_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}}, \bar{P}_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}}) + \mathbb{D}(\bar{P}_{M_1^{(1:b)} M_2^{(1:b)} Z^{b,r}} || \bar{P}_{M_1^{(1:b)} M_2^{(1:b)}} \bar{P}_{Z^{(1:b),r}}) \\
&\qquad + \mathbb{D}(\bar{P}_{Z^{(1:b),r}} || Q_Z^{\otimes br}) \\
&\quad = 2 \log \frac{1}{\mu} \mathbb{V}(P_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}}, \bar{P}_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}}) + \bar{I}(M_1^{(1:b)}, M_2^{(1:b)}; Z^{(1:b),r}) \\
&\qquad + \mathbb{D}(\bar{P}_{Z^{(1:b),r}} || Q_Z^{\otimes br})
\end{aligned}
\tag{3.193}
$$

where

(a) follows by adding $\mathbb{D}(P_{Z^{b,r}} || Q_Z^{\otimes br})$;

(b) follows because $\bar{P}_{M_1^{(1:b)}, M_2^{(1:b)}} = P_{M_1^{(1:b)}, M_2^{(1:b)}}$, $(P_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}} - \bar{P}_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}}) \leq |P_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}} - \bar{P}_{M_1^{(1:b)} M_2^{(1:b)} Z^{(1:b),r}}|$ and by defining $\mu \triangleq \min_{z^{b,r}} Q_Z^{\otimes br}(z^{b,r})$;

(c) follows by Lemma 2 and because $\mathbb{D}(\bar{P}_{M_1^{(1:b)}M_2^{(1:b)}Z^{(1:b),r}}||\bar{P}_{M_1^{(1:b)}M_2^{(1:b)}}Q_Z^{\otimes br}) = \mathbb{D}(\bar{P}_{M_1^{(1:b)}M_2^{(1:b)}Z^{b,r}}||\bar{P}_{M_1^{(1:b)}M_2^{(1:b)}}\bar{P}_{Z^{(1:b),r}}) + \mathbb{D}(\bar{P}_{Z^{(1:b),r}}||Q_Z^{\otimes br})$.

The first and third terms of (3.193) vanish exponentially with br similar to Section 3.4.1.

We now derive an achievable rate region by choosing values for ρ_1', ρ_1'', ρ_2', ρ_2'', R_1 and R_2 that satisfy the constraints for secrecy and probability of error. We find it more convenient to separately derive achievable rate regions under the two conditions $H(X_1|U)+H(X_2|U) \lesseqgtr I(X_1,X_2;Y)$, and then merge them.

When $H(X_1|U) + H(X_2|U) > I(X_1,X_2;Y)$, The following rates satisfy all error and secrecy constraints:

$$\begin{aligned}
\rho_1'' &= \epsilon,\\
\rho_1' &= \epsilon,\\
\rho_2'' &= I(U,X_1;Z) + \epsilon,\\
\rho_2' &= I(X_2;Z|X_1,U) + \epsilon,\\
R_1 &= H(X_1|U) - 2\epsilon,\\
R_2 &= I(X_1,X_2;Y) - H(X_1|U) - I(X_1,X_2;Z) - \epsilon,
\end{aligned}$$

and the same is true for the following rates:

$$\begin{aligned}
\rho_1'' &= I(U,X_2;Z) + \epsilon,\\
\rho_1' &= I(X_1;Z|X_2,U) + \epsilon,\\
\rho_2' &= \epsilon,\\
\rho_2'' &= \epsilon,\\
R_1 &= I(X_1,X_2;Y) - H(X_2|U) - I(X_1,X_2;Z) - 2\epsilon,\\
R_2 &= H(X_2|U) - \epsilon.
\end{aligned}$$

Considering the above two corner points, the following rate region is achievable.

$$R_1 \leq H(X_1|U)$$

$$R_2 \leq H(X_2|U)$$

$$R_1 + R_2 \leq I(X_1, X_2; Y) - I(X_1, X_2; Z)$$

When $H(X_1|U) + H(X_2|U) \leq I(X_1, X_2; Y)$, the following rates satisfy all error and secrecy constraints:

$$\rho_1'' = \epsilon,$$

$$\rho_1' = \epsilon,$$

$$\rho_2'' = I(U, X_1; Z) + \epsilon,$$

$$\rho_2' = I(X_2; Z|X_1, U) + \epsilon,$$

$$R_1 = H(X_1|U) - 2\epsilon,$$

$$R_2 = (X_2|U) - I(X_1, X_2; Z) - \epsilon,$$

and the same is true for the following rates:

$$\rho_1'' = I(U, X_2; Z) + \epsilon,$$

$$\rho_1' = I(X_1; Z|X_2, U) + \epsilon,$$

$$\rho_2' = \epsilon,$$

$$\rho_2'' = \epsilon,$$

$$R_1 = H(X_1|U) - I(X_1, X_2; Z) - 2\epsilon,$$

$$R_2 = H(X_2|U) - \epsilon.$$

Considering the above two corner points, the following rate region is achievable.

$$R_1 \leq H(X_1|U)$$

$$R_2 \leq H(X_2|U)$$

$$R_1 + R_2 \leq H(X_1|U) + H(X_2|U) - I(X_1, X_2; Z)$$

Thus far, we have two achievable rate regions for the two conditions $H(X_1|U) + H(X_2|U) \lesseqgtr I(X_1, X_2; Y)$, and the overall achievable rate region is usually specified as the union of the two. It then follows that the smaller of the two derived sum rate constraints is always active. Therefore we can simplify the expression of the achievable region by using the intersection of the two sum rate constraints.

This concludes the proof of Proposition 11.

3.4.9 Convexity proof of channel resolvability of MAC with one-sided strictly-causal cribbing

To prove the convexity of the inner bound, assume that $(R_1^{(1)}, R_2^{(1)})$ and $(R_1^{(2)}, R_2^{(2)})$ are achievable, which implies the existence of two distributions $P^{(1)}_{U,X_1,X_2,Z} = P^{(1)}_U P^{(1)}_{X_1|U} P^{(1)}_{X_2|U} W_{Z|X_1,X_2}$ and $P^{(2)}_{U,X_1,X_2,Z} = P^{(2)}_U P^{(2)}_{X_1|U} P^{(2)}_{X_2|U} W_{Z|X_1,X_2}$ with marginal Q_Z such that,

$$\begin{aligned}
R_1^{(1)} &\geq I(U^{(1)}, X_1^{(1)}; Z^{(1)}),\\
R_2^{(1)} &\geq I(X_1^{(1)}, X_2^{(1)}; Z^{(1)}) - H(X_1^{(1)}|U^{(1)}),\\
R_1^{(1)} + R_2^{(1)} &\geq I(X_1^{(1)}, X_2^{(1)}; Z^{(1)}),\\
&\text{with } H(X_1^{(1)}|U^{(1)}) > I(U^{(1)}, X_1^{(1)}; Z^{(1)}),\\
&\qquad \text{and}\\
R_1^{(2)} &\geq I(U^{(2)}, X_1^{(2)}; Z^{(2)}),\\
R_2^{(1)} &\geq I(X_1^{(2)}, X_2^{(2)}; Z^{(2)}) - H(X_1^{(2)}|U^{(2)}),\\
R_1^{(2)} + R_2^{(2)} &\geq I(X_1^{(2)}, X_2^{(2)}; Z^{(2)}),\\
&\text{with } H(X_1^{(2)}|U^{(2)}) > I(U^{(2)}, X_1^{(2)}; Z^{(2)}).
\end{aligned}$$

For $\lambda \in [\![0,1]\!]$, let $Q \in \{1,2\}$ with $\Pr(Q=1)=\lambda$ and $\Pr(Q=2)=1-\lambda$. Define $U^{(3)} \triangleq (U^{(Q)},Q)$, $X_1^{(3)} \triangleq X_1^{(Q)}$, $X_2^{(3)} \triangleq X_2^{(Q)}$ and $Z^{(3)} \triangleq Z^{(Q)}$. Let Q, $(U^{(1)},X_1^{(1)},X_2^{(1)},Z^{(1)})$ and $(U^{(2)},X_1^{(2)},X_2^{(2)},Z^{(2)})$ be independent so that $P^{(3)}_{U,X_1,X_2,Z} = \lambda P^{(1)}_{U,X_1,X_2,Z} + (1-\lambda)P^{(2)}_{U,X_1,X_2,Z}$ can be written as $P^{(3)}_{U,X_1,X_2,Z} = P^{(3)}_U P^{(3)}_{X_1|U} P^{(3)}_{X_2|U} W_{Z|X_1,X_2}$. From the definition of the random variables:

$$H(X_1^{(3)}|U^{(3)}) = \lambda H(X_1^{(1)}|U^{(1)}) + (1-\lambda)H(X_1^{(2)}|U^{(2)}).$$

For a fixed Q_Z, we have $P^{(3)}_{X_1,X_2|Z} = \lambda P^{(1)}_{X_1,X_2|Z} + (1-\lambda)P^{(2)}_{X_1,X_2|Z}$ and $P^{(3)}_{U,X_1|Z} = \lambda P^{(1)}_{U,X_1|Z} + (1-\lambda)P^{(2)}_{U,X_1|Z}$. From the convexity of $I(U,X_1;Z)$ with respect to $P_{U,X_1|Z}$ and the convexity of $I(X_1,X_2;Z)$ with respect to $P_{X_1,X_2|Z}$:

$$\begin{aligned}
I(U^{(3)},X_1^{(3)};Z^{(3)}) &\leq \lambda I(U^{(1)},X_1^{(1)};Z^{(1)}) + (1-\lambda)I(U^{(2)}X_1^{(2)};Z^{(2)}),\\
I(X_1^{(3)},X_2^{(3)};Z^{(3)}) &\leq \lambda I(X_1^{(1)},X_2^{(1)};Z^{(1)}) + (1-\lambda)I(X_1^{(2)},X_2^{(2)};Z^{(2)}).
\end{aligned}$$

Therefore we have

$$\begin{aligned}
I(U^{(3)},X_1^{(3)};Z^{(3)}) &\leq \lambda R_1^{(1)} + (1-\lambda)R_1^{(2)},\\
I(X_1^{(3)},X_2^{(3)};Z^{(3)}) - H(X_1^{(3)}|U^{(3)}) &\leq \lambda R_2^{(1)} + (1-\lambda)R_2^{(2)},\\
I(X_1^{(3)},X_2^{(3)};Z^{(3)}) &\leq \lambda(R_1^{(1)}+R_2^{(1)}) + (1-\lambda)(R_1^{(2)}+R_2^{(2)}).
\end{aligned}$$

and

$$\begin{aligned}
H(X_1^{(3)}|U^{(3)}) &= \lambda H(X_1^{(1)}|U^{(1)}) + (1-\lambda)H(X_1^{(2)}|U^{(2)})\\
&> \lambda I(U^{(1)},X_1^{(1)};Z^{(1)}) + (1-\lambda)I(U^{(2)}X_1^{(2)};Z^{(2)})\\
&\geq I(U^{(3)},X_1^{(3)};Z^{(3)}),
\end{aligned}$$

which implies that $\left(\lambda R_1^{(1)} + (1-\lambda)R_1^{(2)}, \lambda R_2^{(1)} + (1-\lambda)R_2^{(2)}\right)$ is inside the achievable region defined by $P^{(3)}_{U,X_1,X_2,Z}$. The convexity of the outer bound is proven similarly but without the entropy constraint $H(X_1|U) > I(U,X_1;Z)$.

3.4.10 Convexity proof of channel resolvability of MAC with one-sided causal/non-causal cribbing

Assume that $(R_1^{(1)}, R_2^{(1)})$ and $(R_1^{(2)}, R_2^{(2)})$ are achievable, which implies the existence of two distributions $P^{(1)}_{X_1,X_2,Z}$ and $P^{(2)}_{X_1,X_2,Z}$ with marginal Q_Z such that,

$$\begin{aligned} R_1^{(1)} &\geq I(X_1^{(1)}; Z^{(1)}), \\ R_2^{(1)} &\geq I(X_1^{(1)}, X_2^{(1)}; Z^{(1)}) - H(X_1^{(1)}), \\ R_1^{(1)} + R_2^{(1)} &\geq I(X_1^{(1)}, X_2^{(1)}; Z^{(1)}), \\ &\text{and} \\ R_1^{(2)} &\geq I(X_1^{(2)}; Z^{(2)}), \\ R_2^{(1)} &\geq I(X_1^{(2)}, X_2^{(2)}; Z^{(2)}) - H(X_1^{(2)}), \\ R_1^{(2)} + R_2^{(2)} &\geq I(X_1^{(2)}, X_2^{(2)}; Z^{(2)}). \end{aligned}$$

Let $P^{(3)}_{X_1,X_2|Z} = \lambda P^{(1)}_{X_1,X_2|Z} + (1-\lambda) P^{(2)}_{X_1,X_2|Z}$ for $\lambda \in [\![0,1]\!]$. Then $P^{(3)}_{X_1|Z} = \lambda P^{(1)}_{X_1|Z} + (1-\lambda) P^{(2)}_{X_1|Z}$ and $P^{(3)}_{X_1} = \lambda P^{(1)}_{X_1} + (1-\lambda) P^{(2)}_{X_1}$.

From the convexity of $I(X_1, X_2; Z)$ with respect to $P_{X_1,X_2|Z}$, the convexity of $I(X_1; Z)$ with respect to $P_{X_1|Z}$ for a fixed Q_Z and the concavity of $H(X_1)$ with respect to P_{X_1}:

$$\begin{aligned} I(X_1^{(3)}; Z^{(3)}) &\leq \lambda I(X_1^{(1)}; Z^{(1)}) + (1-\lambda) I(X_1^{(2)}; Z^{(2)}), \\ H(X_1^{(3)}) &\geq \lambda H(X_1^{(1)}) + (1-\lambda) H(X_1^{(2)}), \\ I(X_1^{(3)}, X_2^{(3)}; Z^{(3)}) &\leq \lambda I(X_1^{(1)}, X_2^{(1)}; Z^{(1)}) + (1-\lambda) I(X_1^{(2)}, X_2^{(2)}; Z^{(2)}). \end{aligned}$$

Therefore we have

$$\begin{aligned} I(X_1^{(3)}; Z^{(3)}) &\leq \lambda R_1^{(1)} + (1-\lambda) R_1^{(2)}, \\ I(X_1^{(3)}, X_2^{(3)}; Z^{(3)}) - H(X_1^{(3)}) &\leq \lambda R_2^{(1)} + (1-\lambda) R_2^{(2)}, \\ I(X_1^{(3)}, X_2^{(3)}; Z^{(3)}) &\leq \lambda (R_1^{(1)} + R_2^{(1)}) + (1-\lambda)(R_1^{(2)} + R_2^{(2)}), \end{aligned}$$

which implies that $\left(\lambda R_1^{(1)} + (1-\lambda) R_1^{(2)}, \lambda R_2^{(1)} + (1-\lambda) R_2^{(2)}\right)$ is inside the achievable region defined by $P^{(3)}_{X_1,X_2,Z}$.

3.4.11 Proof of Equations (3.24)-(3.27)

Before we proceed to the proof, we recall some definitions. The random codebook for MAC with strictly-causal cribbing in block b is denoted by

$$\begin{aligned}\mathfrak{C}_r = \{U^r(m_0^{(b)}), X_1^r(m_0^{(b)}, m_1^{\prime(b)}, m_1^{\prime\prime(b)}), X_2^r(m_0^{(b)}, m_2^{(b)}), m_0^{(b)} \in [\![1, 2^{r\rho_0}]\!], m_1^{\prime(b)} \in [\![1, 2^{r\rho_1'}]\!],\\ m_1^{\prime\prime(b)} \in [\![1, 2^{r\rho_1''}]\!], m_2 \in [\![1, 2^{r\rho_2}]\!]\}\end{aligned}$$

We use $\bar{P}$ to denote the probability distribution induced when both encoders use $M_0^{(b)}$ as defined in (3.23)

$$\bar{P}_{Z_b^r} = \sum_{\substack{m_0^{(b)}, m_1^{\prime(b)},\\ m_1^{\prime\prime(b)}, m_2^{(b)}}} 2^{-r(\rho_0+\rho_1'+\rho_1''+\rho_2)} W^{\otimes r}(z_b^r | u^r(m_0^{(b)}), x_1^r(m_0^{(b)}, m_1^{\prime(b)}, m_1^{\prime\prime(b)}), x_2^r(m_0^{(b)}, m_2^{(b))}))$$

The average KL divergence is:

$$\begin{aligned}
&\mathbb{E}_{\mathfrak{C}_r}(\mathbb{D}(\bar{P}_{Z_b^r, M_1^{\prime\prime(b)}} || Q_Z^{\otimes r} \bar{P}_{M_1^{\prime\prime(b)}}))\\
&= \mathbb{E}_{\mathfrak{C}_r} \sum_{m_1^{\prime\prime(b)}, z_b^r} \bar{P}(m_1^{\prime\prime(b)}, z_b^r) \log \frac{\bar{P}(m_1^{\prime\prime(b)}, z_b^r)}{\bar{P}_{M_1^{\prime\prime(b)}}(m_1^{\prime\prime(b)}) Q_Z^{\otimes r}(z^r)}\\
&= \mathbb{E}_{\mathfrak{C}_r} \sum_{m_1^{\prime\prime(b)}} \bar{P}(m_1^{\prime\prime(b)}) \sum_{z_b^r} \bar{P}(z_b^r | m_1^{\prime\prime(b)}) \log \frac{\bar{P}(z_b^r | m_1^{\prime\prime(b)})}{Q_Z^{\otimes r}(z^r)}\\
&= \mathbb{E}_{\mathfrak{C}_r} \sum_{m_1^{\prime\prime(b)}} \bar{P}(m_1^{\prime\prime(b)}) \sum_{z_b^r} \sum_{i,j,k} \frac{W^{\otimes r}(z_b^r | U^r(i), X_1^r(i, j, m_1^{\prime\prime(b)}), X_2^r(i, k))}{2^{r(\rho_0+\rho_1'+\rho_2)}}\\
&\qquad\qquad \log \sum_{i',j',k'} \frac{W^{\otimes r}(z_b^r | U^r(i'), X_1^r(i', j', m_1^{\prime\prime(b)}), X_2^r(i', k'))}{2^{r(\rho_0+\rho_1'+\rho_2)} Q_Z^{\otimes r}(z^r)}\\
&= \sum_{u^r(1)} \sum_{x_1^r(1,1,1)} \sum_{x_2^r(1,1)} \cdots \sum_{u^r(2^{r\rho_0})} \sum_{x_1^r(2^{r\rho_0}, 2^{r\rho_1'}, 2^{r\rho_1''})} \sum_{x_2^n(2^{r\rho_0}, 2^{r\rho_2})}\\
&\qquad\qquad \prod_{(k_1,k_2,k3,k4)=(1,1,1,1)}^{(2^{r\rho_0}, 2^{r\rho_1'}, 2^{r\rho_1''}, 2^{r\rho_2})} \bar{P}(u^r(k_1), x_1^r(k_1, k_2, k_3), x_2^r(k_1, k_4))\\
&\qquad\qquad \sum_{m_1^{\prime\prime(b)}} \bar{P}(m_1^{\prime\prime(b)}) \sum_{z_b^r} \sum_{i,j,k} \frac{W^{\otimes r}(z_b^r | u^r(i), x_1^r(i, j, m_1^{\prime\prime(b)}), x_2^r(i, k))}{2^{r(\rho_0+\rho_1'+\rho_2)}}
\end{aligned}$$

$$
\begin{aligned}
&\log \sum_{i',j',k'} \frac{W^{\otimes r}(z_b^r|u^r(i'), x_1^r(i',j',m_1''^{(b)}), x_2^r(i',k'))}{2^{r(\rho_0+\rho_1'+\rho_2)} Q_Z^{\otimes r}(z^r)} \\
\overset{(a)}{=}\ & \frac{1}{2^{r(\rho_0+\rho_1'+\rho_2)}} \sum_{m_1''^{(b)}} \bar{P}(m_1''^{(b)}) \sum_{i,j,k} \sum_{z_b^r} \sum_{u^r(i)} \sum_{x_1^r(i,j,m_1''^{(b)})} \sum_{x_2^r(i,k)} \bar{P}(u^r(i), x_1^r(i,j,m_1''^{(b)}), x_2^r(i,k), z_b^r) \\
& \qquad \mathbb{E}_{\setminus(i,j,k)} \log \sum_{i',j',k'} \frac{W^{\otimes r}(z_b^r|U^r(i'), X_1^r(i',j',m_1''^{(b)}), X_2^r(i',k'))}{2^{r(\rho_0+\rho_1'+\rho_2)} Q_Z^{\otimes r}(z^r)} \\
\overset{(b)}{\leq}\ & \frac{1}{2^{r(\rho_0+\rho_1'+\rho_2)}} \sum_{m_1''^{(b)}} \bar{P}(m_1''^{(b)}) \sum_{i,j,k} \sum_{z_b^r} \sum_{u^r(i)} \sum_{x_1^r(i,j,m_1''^{(b)})} \sum_{x_2^r(i,k)} \bar{P}(u^r(i), x_1^r(i,j,m_1''^{(b)}), x_2^r(i,k), z_b^r) \\
& \qquad \log \mathbb{E}_{\setminus(i,j,k)} \sum_{i',j',k'} \frac{W^{\otimes r}(z_b^r|U^r(i'), X_1^r(i',j',m_1''^{(b)}), X_2^r(i',k'))}{2^{r(\rho_0+\rho_1'+\rho_2)} Q_Z^{\otimes r}(z^r)} \\
\leq\ & \frac{1}{2^{r(\rho_0+\rho_1'+\rho_2)}} \sum_{m_1''^{(b)}} \bar{P}(m_1''^{(b)}) \sum_{i,j,k} \sum_{z_b^r} \sum_{u^r(i)} \sum_{x_1^r(i,j,m_1''^{(b)})} \sum_{x_2^r(i,k)} \bar{P}(u^r(i), x_1^r(i,j,m_1''^{(b)}), x_2^r(i,k), z_b^r) \\
& \qquad \log \mathbb{E}_{\setminus(i,j,k)} \frac{1}{2^{r(\rho_0+\rho_1'+\rho_2)} Q_Z^{\otimes r}(z^r)} \Bigg(W^{\otimes r}(z_b^r|u^r(i), x_1^r(i,j,m_1''^{(b)}), x_2^r(i,k)) \\
& \qquad + \sum_{\substack{j'\neq j\\ k'\neq k}} W^{\otimes r}(z_b^r|u^r(i), X_1^r(i,j',m_1''^{(b)}), X_2^r(i,k')) \\
& \qquad + \sum_{k'\neq k} W^{\otimes r}(z_b^r|u^r(i), x_1^r(i,j,m_1''^{(b)}), X_2^r(i,k')) \\
& \qquad + \sum_{j'\neq j} W^{\otimes r}(z_b^r|u^r(i), X_1^r(i,j',m_1''^{(b)}), x_2^r(i,k)) \\
& \qquad + \sum_{\substack{i'\neq i\\ j',k'}} W^{\otimes r}(z_b^r|U^r(i'), X_1^r(i',j',m_1''^{(b)}), X_2^r(i',k')) \Bigg) \\
\overset{(c)}{\leq}\ & \frac{1}{2^{r(\rho_0+\rho_1'+\rho_2)}} \sum_{m_1''^{(b)}} \bar{P}(m_1''^{(b)}) \sum_{i,j,k} \sum_{z_b^r} \sum_{u^r(i)} \sum_{x_1^r(i,j,m_1''^{(b)})} \sum_{x_2^r(i,k)} \bar{P}(u^r(i), x_1^r(i,j,m_1''^{(b)}), x_2^r(i,k), z_b^r) \\
& \qquad \log \frac{1}{2^{r(\rho_0+\rho_1'+\rho_2)} Q_Z^{\otimes r}(z^r)} \Bigg(W^{\otimes r}(z_b^r|u^r(i), x_1^r(i,j,m_1''^{(b)}), x_2^r(i,k)) \\
& \qquad + \sum_{\substack{j'\neq j\\ k'\neq k}} \bar{P}^{\otimes r}(z_b^r|u^r(i)) + \sum_{k'\neq k} \bar{P}^{\otimes r}(z_b^r|u^r(i), x_1^r(i,j,m_1''^{(b)})) \\
& \qquad + \sum_{j'\neq j} \bar{P}^{\otimes r}(z_b^r|u^r(i), x_2^r(i,k)) + 1 \Bigg)
\end{aligned}
$$

$$= \Psi_1 + \Psi_2$$

where

(a) follows since $\mathbb{E}_X \mathbb{E}_Y\big(f(X)f(X,Y)\big) = \mathbb{E}_X\big(f(X)\mathbb{E}_Y f(X,Y)\big)$. Recall $\mathbb{E}_{\setminus(i,j,k)}(\cdot)$ is the expectation over $U^r(i')$, $X_1^r(i',j',m_1''^{(b)})$ and $X_2^r(i',k')$ for $(i',j',k') \neq (i,j,k)$;

(b) follows by Jensen's inequality where $\mathbb{E}\log(\cdot) \leq \log\mathbb{E}(\cdot)$;

(c) follows by applying the expectation $\mathbb{E}_{\setminus(i,j,k)}$ to each term inside the bracket.

$$\begin{aligned}
\Psi_1 \triangleq\ & \frac{1}{2^{r(\rho_0+\rho_1'+\rho_2)}} \sum_{m_1''^{(b)}} \bar{P}(m_1''^{(b)}) \sum_{i,j,k} \sum_{(u^r(i),x_1^r(i,j,m_1''^{(b)}),x_2^r(i,k),z_b^r)\in\mathcal{T}_\epsilon^r(P_{U,X_1,X_2,Z})} \\
& \bar{P}(u^r(i),x_1^r(i,j,m_1''^{(b)}),x_2^r(i,k),z_b^r) \log \frac{1}{2^{r(\rho_0+\rho_1'+\rho_2)} Q_Z^{\otimes r}(z^r)} \\
& \Bigg(W^{\otimes r}(z_b^r|u^r(i),x_1^r(i,j,m_1''^{(b)}),x_2^r(i,k)) + \sum_{\substack{j'\neq j \\ k'\neq k}} \bar{P}^{\otimes r}(z_b^r|u^r(i)) \\
& + \sum_{k'\neq k} \bar{P}^{\otimes r}(z_b^r|u^r(i),x_1^r(i,j,m_1''^{(b)})) + \sum_{j'\neq j} \bar{P}^{\otimes r}(z_b^r|u^r(i),x_2^r(i,k)) + 1 \Bigg) \\
\leq\ & \log\Bigg(\frac{2^{-r(1-\epsilon)H(Z|X_1,X_2)}}{2^{r(\rho_0+\rho_1'+\rho_2)}2^{-r(1+\epsilon)H(Z)}} + \frac{2^{-r(1-\epsilon)H(Z|U)}}{2^{r\rho_0}2^{-r(1+\epsilon)H(Z)}} + \frac{2^{-r(1-\epsilon)H(Z|U,X_1)}}{2^{r(\rho_0+\rho_1')}2^{-r(1+\epsilon)H(Z)}} \\
& + \frac{2^{-r(1-\epsilon)H(Z|U,X_2)}}{2^{r(\rho_0+\rho_2)}2^{-r(1+\epsilon)H(Z)}} + 1 \Bigg) \\
\leq\ & \log\Big(2^{-r(\rho_0+\rho_1'+\rho_2-I(X_1,X_2;Z)-2\epsilon H(Z))} + 2^{-r(\rho_0-I(U;Z)-2\epsilon H(Z))} + 2^{-r(\rho_0+\rho_1'-I(U,X_1;Z)-2\epsilon H(Z))} \\
& + 2^{-r(\rho_0+\rho_2-I(U,X_2;Z)-2\epsilon H(Z))} + 1 \Big)
\end{aligned}$$

$$\begin{aligned}
\Psi_2 \triangleq\ & \sum_{m_1''^{(b)}} \bar{P}(m_1''^{(b)}) \sum_i \sum_j \sum_k \sum_{(u^r(i),x_1^r(i,j,m_1''^{(b)}),x_2^r(i,k),z_b^r)\notin\mathcal{T}_\epsilon^r(P_{U,X_1,X_2,Z})} \\
& \bar{P}(u^r(i),x_1^r(i,j,m_1''^{(b)}),x_2^r(i,k),z_b^r) \log \frac{1}{2^{r(\rho_0+\rho_1'+\rho_2)} Q_Z^{\otimes r}(z^r)}
\end{aligned}$$

$$\Big(W^{\otimes r}(z_b^r|u^r(i), x_1^r(i,j,m_1''^{(b)}), x_2^r(i,k)) + \sum_{\substack{j'\neq j\\ k'\neq k}} \bar{P}^{\otimes r}(z_b^r|u^r(i))$$

$$+ \sum_{k'\neq k} \bar{P}^{\otimes r}(z_b^r|u^r(i), x_1^r(i,j,m_1''^{(b)})) + \sum_{j'\neq j} \bar{P}^{\otimes r}(z_b^r|u^r(i), x_2^r(i,k)) + 1\Big)$$

$$\leq 2|\mathcal{U}||\mathcal{X}_1||\mathcal{X}_2||\mathcal{Z}|e^{-r\epsilon^2\mu_{UX_1X_2Z}} r\log(\frac{4}{\mu_Z}+1)$$

where

$$\mu_Z = \min_{z\in\mathcal{Z}} Q(z)$$

$$\mu_{UX_1X_2Z} = \min_{(u,x_1,x_2,z)\in(\mathcal{U},\mathcal{X}_1,\mathcal{X}_2,\mathcal{Z})} Q(u,x_1,x_2,z)$$

Combining the bounds on Ψ_1 and Ψ_2, $\mathbb{E}(\mathbb{D}(\bar{P}_{Z_b^r, M_1''^{(b)}}||Q_Z^{\otimes r}\bar{P}_{M_1''^{(b)}})) \xrightarrow{r\to\infty} 0$ when (3.24)-(3.27) are satisfied.

CHAPTER 4

MAC WITH FEEDBACK AND MAC WITH GENERALIZED FEEDBACK [1] [2]

The MAC models studied so far involve cooperation via pre-shared information or noiseless information exchange between the two encoders.

We start by a MAC model with (noise-free) feedback. we show that feedback does not improve channel resolvability, but still can improve the secrecy rates. We then study MAC with generalized feedback. For the channel resolvability, we introduce two achievable resolvability regions. The first inner bound is constructed by using a decoding strategy, where each encoder decodes the other encoder's message. The second inner bound is constructed by randomness extraction; this approach is motivated to improve resolvability rates when the feedback is very noisy and therefore decoding is not helpful. We then provide inner bounds for the strong secrecy regions building on the results of channel resolvability.

4.1 MAC with Feedback

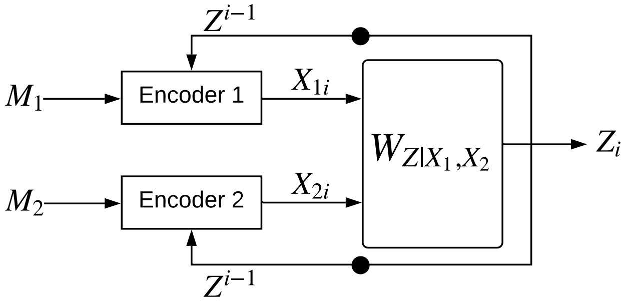

Figure 4.1. The multiple access channel with feedback.

[1] © N. Helal and M. Bloch and A. Nosratinia, "Channel Resolvability with a Full-Duplex Decode-and-Forward Relay," 2019 Information Theory Workshop (ITW), pp. 1-5, 2019.

[2] © N. Helal and M. Bloch and A. Nosratinia, "Resolvability of the Multiple Access Channel with Two-Sided Cooperation," 2020 IEEE International Symposium on Information Theory (ISIT).

The discrete memoryless MAC with feedback (Figure 4.1) consists of finite input alphabets $\mathcal{X}_1$ and $\mathcal{X}_2$, and finite output alphabet Z with a channel transition probability $W_{Z|X_1,X_2}$. For a joint distribution P_{X_1,X_2} on $\mathcal{X}_1 \times \mathcal{X}_2$, the output is distributed according to $Q_Z(z) = \sum_{x_1,x_2} P_{X_1,X_2}(x_1,x_2)W_{Z|X_1,X_2}(z|x_1,x_2)$. A $(2^{nR_1}, 2^{nR_2}, n)$ channel resolvability code consists of two encoders f_1 and f_2 with inputs $M_1 \in [\![1, 2^{nR_1}]\!]$ and $M_2 \in [\![1, 2^{nR_2}]\!]$. The encoding functions are defined as follows:

$$f_{1i} : \mathcal{M}_1 \times \mathcal{Z}^{i-1} \to \mathcal{X}_{1i} \qquad f_{2i} : \mathcal{M}_2 \times \mathcal{Z}^{i-1} \to \mathcal{X}_{2i}. \tag{4.1}$$

Definition 9. *A rate pair (R_1, R_2) is said to be achievable for the discrete memoryless MAC with feedback $(\mathcal{X}_1 \times \mathcal{X}_2, W_{Z|X_1,X_2}, \mathcal{Z})$ if for a given Q_Z there exists a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes with increasing block length such that $\lim_{n\to\infty} \mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) = 0$. The MAC resolvability region is the closure of the set of achievable rate pairs (R_1, R_2).*

Theorem 8. *The resolvability of MAC with feedback is the set of rate pairs (R_1, R_2) such that:*

$$R_1 \geq I(X_1; Z|U)$$

$$R_2 \geq I(X_2; Z|U)$$

$$R_1 + R_2 \geq I(X_1, X_2; Z|U)$$

for some joint distribution $P_{U,X_1,X_2,Z} \triangleq P_U P_{X_1|U} P_{X_2|U} W_{Z|X_1,X_2}$ with marginal Q_Z.

Proof. See Section 4.4.1. □

We provide a converse proof and show that feedback does not improve the resolvability of the multiple access channel.

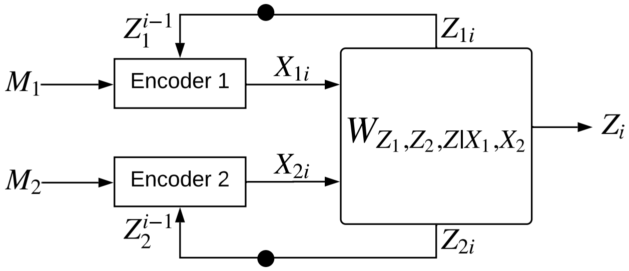

Figure 4.2. The multiple access channel with generalized feedback.

4.2 MAC with Generalized Feedback

The discrete memoryless MAC with generalized feedback (Figure 4.2) consists of finite input alphabets $\mathcal{X}_1$ and $\mathcal{X}_2$, and finite output alphabets Z_1, Z_2 and Z with a channel transition probability $W_{Z,Z_1,Z_2|X_1,X_2}$. For a joint distribution P_{X_1,X_2} on $\mathcal{X}_1 \times \mathcal{X}_2$, the output is distributed according to $Q_Z(z) = \sum_{x_1,x_2,z_1,z_2} P_{X_1,X_2}(x_1,x_2)W_{Z,Z_1,Z_2|X_1,X_2}(z,z_1,z_2|x_1,x_2)$. A $(2^{nR_1}, 2^{nR_2}, n)$ channel resolvability code consists of two encoders f_1 and f_2 with inputs $M_1 \in [\![1, 2^{nR_1}]\!]$ and $M_2 \in [\![1, 2^{nR_2}]\!]$. The encoding functions are defined as follows:

$$f_{1i} : \mathcal{M}_1 \times \mathcal{Z}_1^{i-1} \to \mathcal{X}_{1i} \qquad f_{2i} : \mathcal{M}_2 \times \mathcal{Z}_2^{i-1} \to \mathcal{X}_{2i}. \tag{4.2}$$

Definition 10. *A rate pair (R_1, R_2) is said to be achievable for the discrete memoryless MAC with generalized feedback $(\mathcal{X}_1 \times \mathcal{X}_2, W_{Z_1,Z_2,Z|X_1,X_2}, \mathcal{Z}_1 \times \mathcal{Z}_2 \times \mathcal{Z})$ if for a given Q_Z there exists a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes with increasing block length such that $\lim_{n\to\infty} \mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) = 0$. The MAC resolvability region is the closure of the set of achievable rate pairs (R_1, R_2).*

Proposition 12. *For the discrete memoryless MAC channel with generalized feedback, the following region is achievable via decode-and-forward if there exists a joint distribution $P_{U,X_1,X_2,Z,Z_1,Z_2} = P_U P_{X_1|U} P_{X_2|U} W_{Z,Z_1,Z_2|X_1,X_2}$ with marginal Q_Z satisfying $I(X_1; Z_1|X_2, U) + I(X_2; Z_2|X_1, U) > I(X_1, X_2; Z)$ for which:*

$$R_1 \geq I(X_1, X_2; Z) - I(X_2; Z_1|X_1, U)$$

$$R_2 \geq I(X_1, X_2; Z) - I(X_1; Z_2 | X_2, U)$$

$$R_1 + R_2 \geq I(X_1, X_2; Z)$$

Proof. See Section 4.4.3. We present here a sketch of the proof. This achievable bound on the channel resolvability is constructed by allowing the two encoders to cooperate over multiple blocks. Each encoder recovers the other's message over a secure channel, i.e., the two encoders exchange information in such a way so that the output Z is oblivious to it. This is accomplished through two mechanisms: first, the feedback outputs Z_1 and Z_2 are different from the output Z, which creates a virtual wiretap channel allowing the feedback to carry information that is not accessible to Z. Second, the resolution of information available at each encoder is better than the output, because each encoder knows its own transmission and can somewhat clean up the feedback to get access to the communication from the other user.

It is interesting to note that this second mechanism was not helpful in the case of simple output feedback, also called Shannon feedback, since it was shown that feedback does not improve the resolvability rate. In the case of generalized feedback, conditioning on each encoder's own message, while decoding the feedback, seems to improve the resolvability rates.

The information exchanged during each time block is used in the next block to coordinate transmissions by the two users to facilitate obfuscation at Z. In the achievability proof, the security of the exchange of messages (mentioned in the previous paragraph) is used to demonstrate, via a chaining argument, the breaking of the dependence across blocks. □

Remark 11. *The resolvability of the relay channel via decode-and-forward [36] can be retrieved from Proposition 12 by setting $R_2 = 0$ and $U = X_2$.*

Proposition 13. *For the discrete memoryless MAC channel with generalized feedback, the following region is achievable via randomness extraction if there exists a joint distribution* $P_{X_1,X_2,Z,Z_1,Z_2} = P_{X_1}P_{X_2}W_{Z,Z_1,Z_2|X_1,X_2}$ *with marginal* Q_Z *for which:*

$$\begin{aligned} R_1 &\geq I(X_1;Z) - H(Z_1|X_1,Z) \\ R_2 &\geq I(X_2;Z) - H(Z_2|X_2,Z) \\ R_1 + R_2 &\geq I(X_1,X_2;Z) - H(Z_1,Z_2|X_1,X_2,Z) \end{aligned}$$

Proof. See Section 4.4.3. We provide here a sketch of the proof. We divide the transmission into multiple blocks. In every block, each encoder independently generates randomness that stems from channel noise via a random binning argument. This fresh randomness is re-injected into the channel in the next block to assist in the approximation of output distribution. □

Remark 12. *Proposition 13 shows a* third *way in which generalized feedback improves the resolvability rate of MAC, and that is in providing* fresh *randomness to the inputs that are* independent of each other and of Z. *Our understanding of this mechanism is refined and focused via the earlier result that Shannon feedback does not improve the resolvability rate: we therefore conclude that only the fresh randomness that is independent of* Z *is useful in improving resolvability rates. This insight is not obvious because this recycled randomness is used only in the following time block and is re-processed through the channel.*

Remark 13. *The resolvability of the relay channel via randomness extraction [36] can be retrieved from Proposition 13 by setting* $R_2 = 0$ *and* $Z_1 =$ *constant.*

Remark 14. *The achievable resolvability of MAC can be retrieved from Proposition 13 by setting* $Z_1 = Z_2 =$ *constant.*

Proposition 14. *For the discrete memoryless MAC channel with generalized feedback, the following region is achievable via decode-and-forward with randomness extraction if there exists a joint distribution* $P_{U,X_1,X_2,Z_1,Z_2,Z} = P_U P_{X_1|U} P_{X_2|U} W_{Z_1,Z_2,Z|X_1,X_2}$ *with marginal* Q_Z *satisfying* $I(X_1; Z_2|X_2, U) + I(X_2; Z_1|X_1, U) > I(X_1, X_2; Z)$ *for which:*

$$\begin{aligned} R_1 &\geq I(X_1, X_2; Z) - I(X_2; Z_1|X_1, U) - H(Z_1, Z_2|X_1, X_2, Z), \\ R_2 &\geq I(X_1, X_2; Z) - I(X_1; Z_2|X_2, U) - H(Z_1, Z_2|X_1, X_2, Z), \\ R_1 + R_2 &\geq I(X_1, X_2; Z) - H(Z_1, Z_2|X_1, X_2, Z). \end{aligned}$$

Proof. The proof follows by combining the proofs of Proposition 12 and Proposition 13. □

4.3 Strong Secrecy from Channel Resolvability

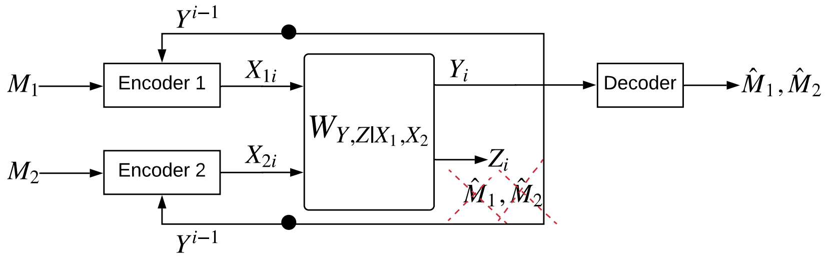

Figure 4.3. The multiple access wiretap channel with feedback.

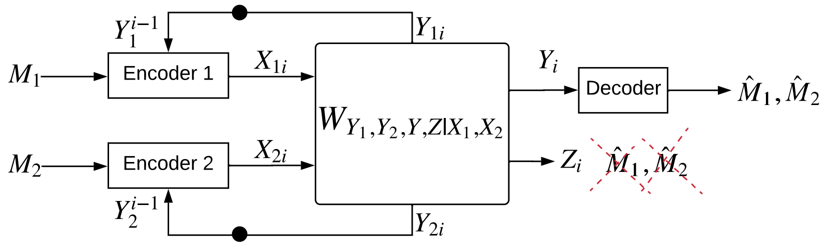

Figure 4.4. The multiple access wiretap channel with generalized feedback.

The multiple-access wiretap channel with feedback or the multiple-access wiretap channel with generalized feedback consists of two encoders f_1 and f_2 and a decoder g. The encoders are defined similar to definitions presented in (4.1) and (4.2), but the functions f_{1i} and f_{2i} are now stochastic and not deterministic. The decoding function at the legitimate receiver is defined as:

$$g : \mathcal{Y}^n \to \hat{\mathcal{M}}_1 \times \hat{\mathcal{M}}_2. \tag{4.3}$$

The probability of error at the legitimate receiver is defined as $P_e^{(n)} = \mathbb{P}\Big((\hat{M}_1, \hat{M}_2) \neq (M_1, M_2)\Big)$. The total amount of leaked confidential information per codeword is defined as $L^{(n)} = I(M_1, M_2; Z^n)$.

Definition 11. *A strong secrecy rate pair (R_1, R_2) is said to be achievable for the discrete memoryless wiretap MAC if there exists a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes such that $P_e^{(n)}$ and $L^{(n)}$ vanish as $n \to \infty$.*

Proposition 15. *For the multiple-access wiretap channel with feedback, the following strong-secrecy rate region is achievable via decode-and-forward:*

$$(R_1, R_2) = \bigcup_{P_U P_{X_1|U} P_{X_2|U} W_{YZ|X_1X_2}} \mathcal{R}^{(\text{in})}_{\text{FB-DF}},$$

$$\mathcal{R}^{(\text{in})}_{\text{FB-DF}} = \left\{ \begin{array}{l} R_1, R_2 \geq 0 \\ R_1 \leq I(X_1; Y|X_2, U) \\ R_2 \leq I(X_2; Y|X_1, U) \\ R_1 + R_2 \leq I(X_1; Y|X_2, U) + I(X_2; Y|X_1, U) - I(X_1, X_2; Z) \\ R_1 + R_2 \leq I(X_1, X_2; Y) - I(X_1, X_2; Z) \end{array} \right\}. \tag{4.4}$$

Proof. See Section 4.4.2. □

Proposition 16. *For the multiple-access wiretap channel with feedback, the following strong-secrecy rate region is achievable via randomness extraction:*

$$(R_1, R_2) = \bigcup_{P_{X_1} P_{X_2} W_{YZ|X_1X_2}} \mathcal{R}^{(\text{in})}_{\text{FB-RE}},$$

$$\mathcal{R}^{(\text{in})}_{\text{FB-RE}} = \left\{ \begin{array}{l} R_1, R_2 \geq 0 \\ R_1 \leq I(X_1; Y|X_2) \\ R_2 \leq I(X_2; Y|X_1) \\ R_1 + R_2 \leq I(X_1, X_2; Y) - [I(X_1, X_2; Z) - H(Y|X_1, X_2, Z)]^+ \end{array} \right\}. \tag{4.5}$$

Proof. See Section 4.4.2. □

Proposition 17. *For the multiple-access wiretap channel with feedback, the following strong-secrecy rate region is achievable via decode-and-forward with randomness extraction:*

$$(R_1, R_2) = \bigcup_{P_U P_{X_1|U} P_{X_2|U} W_{YZ|X_1X_2}} \mathcal{R}^{(\text{in})}_{\text{FB-DF-RE}},$$

$$\mathcal{R}^{(\text{in})}_{\text{FB-DF-RE}} = \left\{ \begin{array}{l} R_1, R_2 \geq 0 \\ R_1 \leq I(X_1; Y|X_2, U) \\ R_2 \leq I(X_2; Y|X_1, U) \\ R_1 + R_2 \leq I(X_1; Y|X_2, U) + I(X_2; Y|X_1, U) \\ \qquad\qquad\qquad\qquad -[I(X_1, X_2; Z) - H(Y|X_1, X_2, Z)]^+ \\ R_1 + R_2 \leq I(X_1, X_2; Y) - [I(X_1, X_2; Z) - H(Y|X_1, X_2, Z)]^+ \end{array} \right\}. \tag{4.6}$$

Proof. The proof follows by combining the proofs of Proposition 15 and Proposition 16. □

Proposition 18. *For the multiple-access wiretap channel with generalized feedback, the following strong-secrecy rate region is achievable via decode-and-forward:*

$$(R_1, R_2) = \bigcup_{P_U P_{X_1|U} P_{X_2|U} W_{Y_1Y_2YZ|X_1X_2}} \mathcal{R}^{(\text{in})}_{\text{GFB-DF}},$$

$$\mathcal{R}^{(\text{in})}_{\text{GFB-DF}} = \left\{ \begin{array}{l} R_1, R_2 \geq 0 \\ R_1 \leq I(X_1; Y_2 | X_2, U) \\ R_2 \leq I(X_2; Y_1 | X_1, U) \\ R_1 + R_2 \leq I(X_1; Y_2 | X_2, U) + I(X_2; Y_1 | X_1, U) - I(X_1, X_2; Z) \\ R_1 + R_2 \leq I(X_1, X_2; Y) - I(X_1, X_2; Z) \end{array} \right\}. \tag{4.7}$$

Proof. The proof follows by steps similar to Proposition 15. □

Remark 15. *The achievable strong secrecy rate region of the relay wiretap channel via decode-and-forward can be obtained from Proposition 18 by setting $R_2 = 0$, $Y_1 =$ constant and $U = X_2$.*

Proposition 19. *For the multiple-access wiretap channel with generalized feedback, the following strong-secrecy rate region is achievable via randomness extraction:*

$$(R_1, R_2) = \bigcup_{P_{X_1} P_{X_2} W_{Y_1 Y_2 Y Z | X_1 X_2}} \mathcal{R}^{(\text{in})}_{\text{GFB-RE}},$$

$$\mathcal{R}^{(\text{in})}_{\text{GFB-RE}} = \left\{ \begin{array}{l} R_1, R_2 \geq 0 \\ R_1 \leq I(X_1; Y | X_2) \\ R_2 \leq I(X_2; Y | X_1) \\ R_1 + R_2 \leq I(X_1, X_2; Y) - [I(X_1, X_2; Z) - H(Y_1, Y_2 | X_1, X_2, Z)]^+ \end{array} \right\}. \tag{4.8}$$

Proof. The proof follows by steps similar to Proposition 16. □

Proposition 20. *For the multiple-access wiretap channel with generalized feedback, the following strong-secrecy rate region is achievable via decode-and-forward with randomness extraction:*

$$(R_1, R_2) = \bigcup_{P_U P_{X_1|U} P_{X_2|U} W_{Y_1, Y_2, Y, Z | X_1 X_2}} \mathcal{R}^{(\text{in})}_{\text{GFB-DF-RE}},$$

$$\mathcal{R}^{(\text{in})}_{\text{GFB-DF-RE}} = \left\{ \begin{array}{l} R_1, R_2 \geq 0 \\ R_1 \leq I(X_1; Y_2|X_2, U) \\ R_2 \leq I(X_2; Y_1|X_1, U) \\ R_1 + R_2 \leq I(X_1; Y_2|X_2, U) + I(X_2; Y_1|X_1, U) \\ \qquad\qquad\qquad -[I(X_1, X_2; Z) - H(Y_1, Y_2|X_1, X_2, Z)]^+ \\ R_1 + R_2 \leq I(X_1, X_2; Y) - [I(X_1, X_2; Z) - H(Y_1, Y_2|X_1, X_2, Z)]^+ \end{array} \right\}. \tag{4.9}$$

Proof. The proof follows by combining the proofs of Proposition 18 and Proposition 19. □

4.4 Proofs

4.4.1 Channel resolvability of MAC with feedback

Converse:

By assumption,

$$\begin{aligned} \epsilon &\geq \mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) \\ &= \mathbb{D}(P_{Z_1 \dots Z_n}||Q_Z^{\otimes n}) \\ &= \sum_{i=1}^{n} \mathbb{D}(P_{Z_i|Z^{i-1}}||Q_Z|P_{Z^{i-1}}) && (4.10) \\ &= \sum_{i=1}^{n} \mathbb{D}(P_{Z_i}||Q_Z) + \sum_{i=1}^{n} I(Z_i; Z^{i-1}) && (4.11) \end{aligned}$$

$$\begin{aligned} nR_1 &= H(M_1) && (4.12) \\ &\geq I(M_1; Z^n) && (4.13) \\ &= \sum_i I(M_1; Z_i|Z^{i-1}) && (4.14) \\ &\overset{(a)}{=} I(M_1, X_{1i}; Z_i|Z^{i-1}) && (4.15) \end{aligned}$$

$$\geq I(X_{1i}; Z_i|Z^{i-1}) \tag{4.16}$$

$$= \sum_i I(Z^{i-1}, X_{1i}; Z_i) - \sum_i I(Z^{i-1}; Z_i) \tag{4.17}$$

$$\overset{(b)}{\geq} \sum_i I(U_i, X_{1i}; Z_i) - \epsilon \tag{4.18}$$

$$= \sum_i \mathbb{D}(P_{U_i,X_{1i},Z_i}||P_{U_i,X_{1i}}P_{Z_i}) - \epsilon \tag{4.19}$$

$$= \sum_i \mathbb{D}(P_{U_i,X_{1i},Z_i}||P_{U_i,X_{1i}}Q_{Z_i}) - \sum_i \mathbb{D}(P_{Z_i}||Q_{Z_i}) - \epsilon \tag{4.20}$$

$$\overset{(c)}{\geq} \sum_i \mathbb{D}(P_{U_i,X_{1i},Z_i}||P_{U_i,X_{1i}}Q_{Z_i}) - \epsilon' \tag{4.21}$$

$$\overset{(d)}{\geq} n\mathbb{D}\left(\frac{\sum_i P_{P_{U_i,X_{1i},Z_i}}}{n}\middle|\middle|\frac{\sum_i P_{U_i,X_{1i}}}{n}Q_{Z_i}\right) - \epsilon' \tag{4.22}$$

$$= n\mathbb{D}(\tilde{P}_{U,X_1,Z}||\tilde{P}_{U,X_1}Q_Z) - \epsilon' \tag{4.23}$$

$$\overset{(e)}{\geq} n\mathbb{D}(\tilde{P}_{U,X_1,Z}||\tilde{P}_{U,X_1}\tilde{P}_Z) - \epsilon' \tag{4.24}$$

$$= nI(\tilde{U}, \tilde{X}_1; \tilde{Z}) - \epsilon' \tag{4.25}$$

$$\geq nI(\tilde{X}_1; \tilde{Z}|\tilde{U}) \tag{4.26}$$

where

(a) follows by the encoding function;

(b) follows since $\sum_i I(Z^{i-1}; Z_i) \leq \mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) \leq \epsilon$ and by setting $U_i \triangleq Z^{i-1}$;

(c) follows since $\sum_i \mathbb{D}(P_{Z_i}||Q_{Z_i}) \leq \epsilon$;

(d) follows by Jensen's inequality and convexity of $\mathbb{D}(\cdot||\cdot)$;

(e) follows since $\mathbb{D}(\tilde{P}_{U,X_1,Z}||\tilde{P}_{U,X_1}Q_Z) = \mathbb{D}(\tilde{P}_{U,X_1,Z}||\tilde{P}_{U,X_1}\tilde{P}_Z) + \mathbb{D}(\tilde{P}_Z||Q_Z)$;

Similarly we obtain,

$$nR_2 \geq nI(\tilde{X}_2; \tilde{Z}|\tilde{U}) - \epsilon' \tag{4.27}$$

and

$$n(R_1 + R_2) \geq nI(\tilde{X}_1, \tilde{X}_2; \tilde{Z}|\tilde{U}) - \epsilon' \tag{4.28}$$

The following steps proves $P_{U,X_1,X_2,Z} = P_U P_{X_1|U} P_{X_2|U} W_{Z|X_1,X_2}$.

$$\begin{aligned}
&P(z^{i-1}|m_1, m_2)P(z^{i-1}|m_1', m_2') \\
&= \prod_{j=1}^{i-1} P(z_j|m_1, m_2, z^{j-1}) \times \prod_{j=1}^{i-1} P(z_j|m_1', m_2', z^{j-1}) && (4.29) \\
&= \prod_{j=1}^{i-1} \sum_{\tilde{x}_{1j}, \tilde{x}_{2j}} P(\tilde{x}_{1j}, \tilde{x}_{2j}, z_j|m_1, m_2, z^{j-1}) \times \prod_{j=1}^{i-1} \sum_{x_{1j}, x_{2j}} P(x_{1j}, x_{2j}, z_j|m_1', m_2', z^{j-1}) && (4.30) \\
&= \prod_{j=1}^{i-1} \sum_{\tilde{x}_{1j}, \tilde{x}_{2j}} P(\tilde{x}_{1j}|m_1, m_2, z^{j-1}) P(\tilde{x}_{2j}|m_1, m_2, z^{j-1}, \tilde{x}_{1j}) P(z_j|m_1, m_2, z^{j-1}, \tilde{x}_{1j}, \tilde{x}_{2j}) \\
&\quad \times \prod_{j=1}^{i-1} \sum_{x_{1j}, x_{2j}} P(x_{1j}|m_1', m_2', z^{j-1}) P(x_{2j}|m_1', m_2', z^{j-1}, x_{1j}) P(z_j|m_1', m_2', z^{j-1}, x_{1j}, x_{2j}) && (4.31) \\
&\overset{(a)}{=} \prod_{j=1}^{i-1} \sum_{\tilde{x}_{1j}, \tilde{x}_{2j}} P(\tilde{x}_{1j}|m_1, z^{j-1}) P(\tilde{x}_{2j}|m_2, z^{j-1}) W(z_j|\tilde{x}_{1j}, \tilde{x}_{2j}) \\
&\quad \times \prod_{j=1}^{i-1} \sum_{x_{1j}, x_{2j}} P(x_{1j}|m_1', z^{j-1}) P(x_{2j}|m_2', z^{j-1}) W(z_j|x_{1j}, x_{2j}) && (4.32) \\
&\overset{(b)}{=} \prod_{j=1}^{i-1} \sum_{\tilde{x}_{1j}, x_{2j}} P(\tilde{x}_{1j}|m_1, z^{j-1}) P(x_{2j}|m_2', z^{j-1}) W(z_j|\tilde{x}_{1j}, x_{2j}) \\
&\quad \times \prod_{j=1}^{i-1} \sum_{x_{1j}, \tilde{x}_{2j}} P(x_{1j}|m_1', z^{j-1}) P(\tilde{x}_{2j}|m_2, z^{j-1}) W(z_j|x_{1j}, \tilde{x}_{2j}) && (4.33) \\
&= P(z^{i-1}|m_1, m_2') P(z^{i-1}|m_1', m_2) && (4.34)
\end{aligned}$$

where

(a) follows from the encoding functions and the discrete memoryless nature of the channel;

(b) follows from the discrete memoryless nature of the channel.

$$
\begin{aligned}
&P(m_1, m_2|z^{i-1}) \\
&= \frac{P(m_1, m_2, z^{i-1})}{P(z^{i-1})} && (4.35) \\
&= \frac{\sum_{m_1', m_2'} P(m_1, m_2, z^{i-1}) P(m_1', m_2', z^{i-1})}{P(z^{i-1}) P(z^{i-1})} && (4.36) \\
&= \frac{\sum_{m_1', m_2'} P(m_1) P(m_2) P(z^{i-1}|m_1, m_2) P(m_1') P(m_2') P(z^{i-1}|m_1', m_2')}{P(z^{i-1}) P(z^{i-1})} && (4.37) \\
&\overset{(a)}{=} \frac{\sum_{m_2'} P(m_1) P(m_2') P(z^{i-1}|m_1, m_2') \sum_{m_1'} P(m_1') P(m_2) P(z^{i-1}|m_1', m_2)}{P(z^{i-1}) P(z^{i-1})} && (4.38) \\
&= P(m_1|z^{i-1}) P(m_2|z^{i-1}) && (4.39)
\end{aligned}
$$

where

(a) follows from (4.34).

$$
\begin{aligned}
&P(x_{1i}, x_{2i}|z^{i-1}) \\
&= \sum_{m_1, m_2} P(m_1, m_2, x_{1i}, x_{2i}|z^{i-1}) && (4.40) \\
&= \sum_{m_1, m_2} P(m_1, m_2|z^{i-1}) P(x_{1i}, x_{2i}|m_1, m_2, z^{i-1}) && (4.41) \\
&\overset{(a)}{=} \sum_{m_1, m_2} P(m_1|z^{i-1}) P(m_2|z^{i-1}) P(x_{1i}|m_1, z^{i-1}) P(x_{2i}|m_2, z^{i-1}) && (4.42) \\
&= P(x_{1i}|z^{i-1}) P(x_{2i}|z^{i-1}) && (4.43)
\end{aligned}
$$

(a) follows from the encoding functions and (4.39).

4.4.2 Strong secrecy of MAC with feedback

Achievability via decode-and-forward:

We use a combination of block-Markov encoding and backward decoding. Independently and uniformly distributed messages $m_1^{(b)} \in [\![1, 2^{rR_1}]\!]$ and $m_2^{(b)} \in [\![1, 2^{rR_2}]\!]$ will be sent over

B blocks. Each block consists of r transmissions so that $n = rB$. Consider a distribution $P(u, x_1, x_2) = P(u)P(x_1|u)P(x_2|u)$ such that $\sum_{u,x_1,x_2} P(u, x_1, x_2)W(z|x_1, x_2) = Q_Z(z)$.

Code Construction: In each block $b \in [\![1, B]\!]$:

- Independently generate $2^{r(R_1+\rho'_1+\rho''_1+R_2+\rho'_2+\rho''_2)}$ codewords u^r_b each with probability $P(u^r) = P_U^{\otimes r}(u^r)$. Label them $u^r(m_0^{(b)}, m_0'^{(b)}, m_0''^{(b)})$, $m_0^{(b)} \in [\![1, 2^{r(R_1+R_2)}]\!]$, $m_0'^{(b)} \in [\![1, 2^{r(\rho'_1+\rho'_2)}]\!]$ and $m_0''^{(b)} \in [\![1, 2^{r(\rho''_1+\rho''_2)}]\!]$.

- For every $u^r(m_0^{(b)}, m_0'^{(b)}, m_0''^{(b)})$, independently generate $2^{r(R_1+\rho'_1+\rho''_1)}$ codewords x^r_{1b} each with probability $P(x^r_1|u^r(m_0^{(b)}, m_0'^{(b)}, m_0''^{(b)})) = P^{\otimes r}_{X_1|U}(x^r_1|u^r(m_0^{(b)}, m_0'^{(b)}, m_0''^{(b)}))$. Label them $x^r_1(m_0^{(b)}, m_0'^{(b)}, m_0''^{(b)}, m_1^{(b)}, m_1'^{(b)}, m_1''^{(b)})$, $m_1^{(b)} \in [\![1, 2^{rR_1}]\!]$, $m_1'^{(b)} \in [\![1, 2^{r\rho'_1}]\!]$ and $m_1''^{(b)} \in [\![1, 2^{r\rho''_1}]\!]$.

- For every $u^r(m_0^{(b)}, m_0'^{(b)}, m_0''^{(b)})$, independently generate $2^{r(R_2+\rho'_2+\rho''_2)}$ codewords x^r_{2b} each with probability $P(x^r_2|u^r(m_0^{(b)}, m_0'^{(b)}, m_0''^{(b)})) = P^{\otimes r}_{X_2|U}(x^r_2|u^r(m_0^{(b)}, m_0'^{(b)}, m_0''^{(b)}))$. Label them $x^r_2(m_0^{(b)}, m_0'^{(b)}, m_0''^{(b)}, m_2^{(b)}, m_2'^{(b)}, m_2''^{(b)})$, $m_2^{(b)} \in [\![1, 2^{rR_2}]\!]$, $m_2'^{(b)} \in [\![1, 2^{r\rho'_2}]\!]$ and $m_2''^{(b)} \in [\![1, 2^{r\rho''_2}]\!]$.

We intend to use these codebooks in the following manner:

1. Block Markov encoding via $M_0^{(b)} = (M_1^{(b-1)}, M_2^{(b-1)})$, $M_0'^{(b)} = (M_1'^{(b-1)}, M_2'^{(b-1)})$ and $M_0''^{(b)} = (M_1''^{(b-1)}, M_2''^{(b-1)})$;

2. $M_1^{(b)}$, $M_1'^{(b)}$ and $M_1''^{(b)}$ can be decoded (at Encoder 2) from Y^r_b knowing $(M_0^{(b)}, M_0'^{(b)}, M_0''^{(b)}, M_2^{(b)}, M_2'^{(b)}, M_2''^{(b)})$;

3. $M_2^{(b)}$, $M_2'^{(b)}$ and $M_2''^{(b)}$ can be decoded (at Encoder 1) from Y^r_b knowing $(M_0^{(b)}, M_0'^{(b)}, M_0''^{(b)}, M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)})$;

4. $\{M_1^{(1)}, \ldots, M_1^{(B)}\}$ and $\{M_2^{(1)}, \ldots, M_2^{(B)}\}$ are secret from $\{Z^r_1, \ldots, Z^r_B\}$;

5. $M_1''^{(b)}$ and $M_2''^{(b)}$ are the common randomness to be used by both encoders in block $b+1$;

6. $M_1'^{(b)}$ is local randomness used by Encoder 1 and $M_2'^{(b)}$ is local randomness used by Encoder 2;

7. The messages $M_0^{(b)}$, $M_0'^{(b)}$, $M_0''^{(b)}$, $M_1^{(b)}$, $M_1'^{(b)}$, $M_1''^{(b)}$, $M_2^{(b)}$, $M_2'^{(b)}$ and $M_2''^{(b)}$ can be decoded at the receiver from Y_b^r and the messages decoded in future blocks $b+1$ to B (backward decoding).

As a result of cribbing, after block b, Encoder 2 finds estimates $(\hat{m}_1^{(b)}, \hat{m}_1'^{(b)}, \hat{m}_1''^{(b)})$ for $(m_1^{(b)}, m_1'^{(b)}, m_1''^{(b)})$ such that

$$\begin{aligned}(u^r(\hat{m}_0^{(b)}, \hat{m}_0'^{(b)}, \hat{m}_0''^{(b)}), x_1^r(\hat{m}_0^{(b)}, \hat{m}_0'^{(b)}, \hat{m}_0''^{(b)}, \hat{m}_1^{(b)}, \hat{m}_1'^{(b)}, \hat{m}_1''^{(b)}),&\\ x_2^r(\hat{m}_0^{(b)}, \hat{m}_0'^{(b)}, \hat{m}_0''^{(b)}, m_2^{(b)}, m_2'^{(b)}, m_2''^{(b)}), y_b^r) \in \mathcal{T}_\epsilon^{(r)}(P_{U,X_1,X_2,Y}).& \qquad (4.44)\end{aligned}$$

where $(\hat{m}_0^{(b)}, \hat{m}_0'^{(b)}, \hat{m}_0''^{(b)}) = (\hat{m}_1^{(b-1)}, m_2^{(b-1)}, \hat{m}_1'^{(b-1)}, m_2'^{(b-1)}, \hat{m}_1''^{(b-1)}, m_2''^{(b-1)})$. Also, Encoder 1 finds estimates $(\tilde{M}_2^{(b)}, \tilde{M}_2'^{(b)}, \tilde{M}_2''^{(b)})$ for $(m_2^{(b)}, m_2'^{(b)}, m_2''^{(b)})$ such that

$$\begin{aligned}(u^r(\tilde{M}_0^{(b)}, \tilde{M}_0'^{(b)}, \tilde{M}_0''^{(b)}), x_1^r(\tilde{M}_0^{(b)}, \tilde{M}_0'^{(b)}, \tilde{M}_0''^{(b)}, M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)}),&\\ x_2^r(\tilde{M}_0^{(b)}, \tilde{M}_0'^{(b)}, \tilde{M}_0''^{(b)}, \tilde{M}_2^{(b)}, \tilde{M}_2'^{(b)}, \tilde{M}_2''^{(b)}), y_b^r) \in \mathcal{T}_\epsilon^{(r)}(P_{U,X_1,X_2,Y}).& \qquad (4.45)\end{aligned}$$

where $(\tilde{m}_0^{(b)}, \tilde{m}_0'^{(b)}, \tilde{m}_0''^{(b)}) = (m_1^{(b-1)}, \tilde{m}_2^{(b-1)}, m_1'^{(b-1)}, \tilde{m}_2'^{(b-1)}, m_1''^{(b-1)}, \tilde{m}_2''^{(b-1)})$.

Encoding: We apply block-Markov encoding as follows. In block b, the encoders send:

$$\begin{aligned}x_{1b}^r &= x_1^r(m_0^{(b)}, m_0'^{(b)}, m_0''^{(b)}, m_1^{(b)}, m_1'^{(b)}, m_1''^{(b)})\\ x_{2b}^r &= x_2^r(\hat{m}_0^{(b)}, \hat{m}_0'^{(b)}, \hat{m}_0''^{(b)}, m_2^{(b)}, m_2'^{(b)}, m_2''^{(b)})\end{aligned}$$

We also assume that the encoders and decoder have access to $(M_0^{(1)}, M_0'^{(1)}, M_0''^{(1)}, M_1^{(B)}, M_1'^{(B)}, M_1''^{(B)}, M_2^{(B)}, M_2'^{(B)})$ through private common randomness.

Decoding at the receiver: The legitimate receiver waits until all B blocks are transmitted and then performs backward decoding. The decoder first finds $(\hat{\hat{m}}_0^{(B)}, \hat{\hat{m}}_0'^{(B)}, \hat{\hat{m}}_0''^{(B)})$ such that

$$(u^r(\hat{\hat{m}}_0^{(B)}, \hat{\hat{m}}_0'^{(B)}, \hat{\hat{m}}_0''^{(B)}), x_1^r(\hat{\hat{m}}_0^{(B)}, \hat{\hat{m}}_0'^{(B)}, \hat{\hat{m}}_0''^{(B)}, \hat{\hat{m}}_1^{(B)}, \hat{\hat{m}}_1'^{(B)}, \hat{\hat{m}}_1''^{(B)}),$$
$$x_2^r(\hat{\hat{m}}_0^{(B)}, \hat{\hat{m}}_0'^{(B)}, \hat{\hat{m}}_0''^{(B)}, \hat{\hat{m}}_2^{(B)}, \hat{\hat{m}}_2'^{(B)}, \hat{\hat{m}}_2''^{(B)}), y_B^r) \in \mathcal{T}_\epsilon^{(r)}(P_{U,X_1,X_2,Y}).$$

Assuming that $(m_0^{(B)}, m_0'^{(B)}, m_0''^{(B)})$, $(m_0^{(B-1)}, m_0'^{(B-1)}, m_0''^{(B-1)})$, $\ldots$, $(m_0^{(b+1)}, m_0'^{(b+1)}, m_0''^{(b+1)})$ have been decoded, the decoder sets $(\hat{\hat{m}}_1^{(b)}, \hat{\hat{m}}_1'^{(b)}, \hat{\hat{m}}_1''^{(b)}) = (\hat{\hat{m}}_0^{(b+1)}, \hat{\hat{m}}_0'^{(b+1)}, \hat{\hat{m}}_0''^{(b+1)})$ and finds $(\hat{\hat{m}}_0^{(b)}, \hat{\hat{m}}_0'^{(b)}, \hat{\hat{m}}_0''^{(b)})$ and $(\hat{\hat{m}}_2^{(b)}, \hat{\hat{m}}_2'^{(b)})$ such that

$$(u^r(\hat{\hat{m}}_0^{(b)}, \hat{\hat{m}}_0'^{(b)}, \hat{\hat{m}}_0''^{(b)}), x_1^r(\hat{\hat{m}}_0^{(b)}, \hat{\hat{m}}_0'^{(b)}, \hat{\hat{m}}_0''^{(b)}, \hat{\hat{m}}_1^{(b)}, \hat{\hat{m}}_1'^{(b)}, \hat{\hat{m}}_1''^{(b)}),$$
$$x_2^r(\hat{\hat{m}}_0^{(b)}, \hat{\hat{m}}_0'^{(b)}, \hat{\hat{m}}_0''^{(b)}, \hat{\hat{m}}_2^{(b)}, \hat{\hat{m}}_2'^{(b)}, \hat{\hat{m}}_2''^{(b)}), y_b^r) \in \mathcal{T}_\epsilon^{(r)}(P_{U,X_1,X_2,Y}).$$

Probability of error analysis: Using the arguments for error analysis from [35, Lemma 4], the probability of error of each block vanishes exponentially with r and in turn vanishes across blocks if

$$R_1 + \rho_1' + \rho_1'' < I(X_1; Y|X_2, U), \tag{4.46}$$

$$R_2 + \rho_2' + \rho_2'' < I(X_2; Y|X_1, U), \tag{4.47}$$

$$R_1 + \rho_1' + \rho_1'' + R_2 + \rho_2' + \rho_2'' < I(X_1, X_2; Y). \tag{4.48}$$

Secrecy analysis: Let $\bar{P}$ be the probability induced when both encoders use $(M_0^{(b)}, M_0'^{(b)}, M_0''^{(b)})$. Let P be the probability when Encoder 1 uses the estimate $(\tilde{M}_0^{(b)}, \tilde{M}_0'^{(b)}, \tilde{M}_0''^{(b)})$ and Encoder 2 uses the estimate $(\hat{M}_0^{(b)}, \hat{M}_0'^{(b)}, \hat{M}_0''^{(b)})$. For the secrecy analysis, we find conditions so that $I(M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)}, M_2^{(b)}, M_2'^{(b)}, M_2''^{(b)}, M_0^{(b)}, \tilde{M}_0^{(b)}, \hat{M}_0^{(b)}, \tilde{M}_0'^{(b)}, \hat{M}_0'^{(b)}; Z_b^r)$ vanishes exponentially with r. This is motivated by:

- $(M_1^{(b)}, M_2^{(b)}, M_0^{(b)}, \tilde{M}_0^{(b)}, \hat{M}_0^{(b)})$ are the Encoder 1 and Encoder 2 secret messages in the present, the past and the estimates of the latter (at Encoder 1 and Encoder 2 respectively), which must be kept secret from Z_b^r.
- $(M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)})$ and $(M_2^{(b)}, M_2'^{(b)}, M_2''^{(b)})$ must be kept independent of Z_b^r according to the functional dependence graph (it can be shown by a figure similar to Figure 3.13) to ensure the distribution of Z remains i.i.d. across blocks.
- $\tilde{M}_0'^{(b)}$ and $\hat{M}_0'^{(b)}$ are kept independent from Z_b^r to allow Encoder 1 and Encoder 2 to possess a *local* randomness that is separate from the common randomness shared with between each other: Resolvability analysis showed us that having a local randomness at both encoders can be beneficial for achievable rates.

It can be shown, similar to Section 3.4.11, that $I(M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)}, M_2^{(b)}, M_2'^{(b)}, M_2''^{(b)}, M_0^{(b)}, \tilde{M}_0^{(b)}, \hat{M}_0^{(b)}, \tilde{M}_0'^{(b)}, \hat{M}_0'^{(b)}; Z_b^r) \to 0$ as $r \to \infty$ if:

$$\rho_1'' + \rho_2'' > I(U; Z), \tag{4.49}$$

$$\rho_1' + \rho_1'' + \rho_2'' > I(U, X_1; Z), \tag{4.50}$$

$$\rho_2' + \rho_1'' + \rho_2'' > I(U, X_2; Z), \tag{4.51}$$

$$\rho_1' + \rho_2' + \rho_1'' + \rho_2'' > I(X_1, X_2; Z). \tag{4.52}$$

Similar to Section 3.4.8, it can be shown that $I(M_1^{(b)}, M_1'^{(b)}, M_1''^{(b)}, M_2^{(b)}, M_2'^{(b)}, M_2''^{(b)}, M_0^{(b)}, \tilde{M}_0^{(b)}, \hat{M}_0^{(b)}, \tilde{M}_0'^{(b)}, \hat{M}_0'^{(b)}; Z_b^r) \xrightarrow{r\to\infty} 0$ for all b implies $I(M_1, M_2; Z^n) \xrightarrow{n\to\infty} 0$.

We now derive an achievable rate region by choosing values for ρ_1', ρ_1'', ρ_2', ρ_2'', R_1 and R_2 that satisfy the constraints for secrecy and probability of error. We find it more convenient to separately derive achievable rate regions under the two conditions $I(X_1; Y|X_2, U) + I(X_2; Y|X_1, U) \lessgtr I(X_1, X_2; Y)$, and then merge them.

When $I(X_1;Y|X_2,U) + I(X_2;Y|X_1,U) > I(X_1,X_2;Y)$, The following rates satisfy all error and secrecy constraints:

$$\begin{aligned}
&\rho_1'' = \epsilon,\\
&\rho_1' = \epsilon,\\
&\rho_2'' = I(U,X_1;Z) + \epsilon,\\
&\rho_2' = I(X_2;Z|X_1,U) + \epsilon,\\
&R_1 = I(X_1;Y|X_2,U) - 2\epsilon,\\
&R_2 = I(U,X_2;Y) - I(X_1,X_2;Z) - \epsilon,
\end{aligned}$$

and the same is true for the following rates:

$$\begin{aligned}
&\rho_1'' = I(U,X_2;Z) + \epsilon,\\
&\rho_1' = I(X_1;Z|X_2,U) + \epsilon,\\
&\rho_2' = \epsilon,\\
&\rho_2'' = \epsilon,\\
&R_1 = I(U,X_1;Y) - I(X_1,X_2;Z) - 2\epsilon,\\
&R_2 = I(X_2;Y|X_1,U) - \epsilon.
\end{aligned}$$

Considering the above two corner points, the following rate region is achievable.

$$\begin{aligned}
R_1 &\leq I(X_1;Y|X_2,U)\\
R_2 &\leq I(X_2;Y|X_1,U)\\
R_1 + R_2 &\leq I(X_1,X_2;Y) - I(X_1,X_2;Z)
\end{aligned}$$

When $I(X_1;Y|X_2,U) + I(X_2;Y|X_1,U) \leq I(X_1,X_2;Y)$, the following rates satisfy all error and secrecy constraints:

$$\rho_1'' = \epsilon,$$

$$\begin{aligned}
\rho'_1 &= \epsilon,\\
\rho''_2 &= I(U, X_1; Z) + \epsilon,\\
\rho'_2 &= I(X_2; Z|X_1, U) + \epsilon,\\
R_1 &= I(X_1; Y|X_2, U) - 2\epsilon,\\
R_2 &= I(X_2; Y|X_1, U) - I(X_1, X_2; Z) - \epsilon,
\end{aligned}$$

and the same is true for the following rates:

$$\begin{aligned}
\rho''_1 &= I(U, X_2; Z) + \epsilon,\\
\rho'_1 &= I(X_1; Z|X_2, U) + \epsilon,\\
\rho'_2 &= \epsilon,\\
\rho''_2 &= \epsilon,\\
R_1 &= I(X_1; Y|X_2, U) - I(X_1, X_2; Z) - 2\epsilon,\\
R_2 &= I(X_2; Y|X_1, U) - \epsilon.
\end{aligned}$$

Considering the above two corner points, the following rate region is achievable.

$$\begin{aligned}
R_1 &\leq I(X_1; Y|X_2, U)\\
R_2 &\leq I(X_2; Y|X_1, U)\\
R_1 + R_2 &\leq I(X_1; Y|X_2, U) + I(X_2; Y|X_1, U) - I(X_1, X_2; Z)
\end{aligned}$$

Thus far, we have two achievable rate regions for the two conditions $I(X_1; Y|X_2, U) + I(X_2; Y|X_1, U) \lesseqgtr I(X_1, X_2; Y)$, and the overall achievable rate region is usually specified as the union of the two. It then follows that the smaller of the two derived sum rate constraints is always active. Therefore we can simplify the expression of the achievable region by using the intersection of the two sum rate constraints.

This concludes the proof of Proposition 15.

Achievability via randomness extraction:

We divide the transmission into B blocks. Independently and uniformly distributed messages $m_1^{(b)} \in [\![1, 2^{rR_1}]\!]$ and $m_2^{(b)} \in [\![1, 2^{rR_2}]\!]$ will be sent over B blocks. Each block consists of r transmissions so that $n = rB$. Consider a distribution $P_{X_1,X_2,Y,Z} \triangleq P_{X_1}P_{X_2}W_{Y,Z|X_1,X_2}$ with marginal Q_Z.

Code Construction: For block $b = 1$,

- Independently generate $2^{r(\rho_1+\rho_1')}$ codewords according to $P_{X_1}^{\otimes r}$ and label them $x_1^r(m_1^{(1)}, m_1'^{(1)})$, where $m_1^{(1)} \in [\![1, 2^{r\rho_1}]\!]$ and $m_1'^{(1)} \in [\![1, 2^{r\rho_1'}]\!]$.

- Independently generate $2^{r(\rho_2+\rho_2')}$ codewords according to $P_{X_2}^{\otimes r}$ and label them $x_2^r(m_2^{(1)}, m_2'^{(1)})$, where $m_2^{(1)} \in [\![1, 2^{r\rho_2}]\!]$ and $m_2'^{(1)} \in [\![1, 2^{r\rho_2'}]\!]$.

For $b \in [\![1, B-1]\!]$, we perform random binning as follows:

- For each y_b^r, assign uniformly and independently two random bin indices $k_1^{(b)} \in [\![1, 2^{r\rho_{k1}}]\!]$ and $k_2^{(b)} \in [\![1, 2^{r\rho_{k2}}]\!]$. We denote $k_1^{(b)} = \phi_1(y_b^r)$ and $k_2^{(b)} = \phi_2(y_b^r)$.

$K_1^{(b)}$ is recycled by Encoder 1 towards the generation of $M_1'^{(b+1)}$. $K_2^{(b)}$ is recycled by Encoder 2 towards the generation of $M_2'^{(b+1)}$. Therefore the effective secret rate at Encoder 1 is $R_1 = \rho_1 + \rho_{k1}$. Similarly, the effective secret rate at Encoder 2 is $R_2 = \rho_2 + \rho_{k2}$.

For blocks $b \in [\![2, B]\!]$:

- Independently generate $2^{r(\rho_1+\rho_1')}$ codewords according to $P_{X_1}^{\otimes r}$ and label them $x_1^r(m_1^{(b)}, m_1'^{(b)})$, where $m_1^{(b)} \in [\![1, 2^{r\rho_1}]\!]$ and $m_1'^{(b)} \in [\![1, 2^{r\rho_1'}]\!]$.

- Independently generate $2^{r(\rho_2+\rho_2')}$ codewords according to $P_{X_2}^{\otimes r}$ and label them $x_2^r(m_2^{(b)}, m_2'^{(b)})$, where $m_2^{(b)} \in [\![1, 2^{r\rho_2}]\!]$ and $m_2'^{(b)} \in [\![1, 2^{r\rho_2'}]\!]$.

We intend to use these codebooks in the following manner:

1. $\{M_1^{(1)}, \ldots, M_1^{(B)}\}$ and $\{M_2^{(1)}, \ldots, M_2^{(B)}\}$ are secret from $\{Z_1^r, \ldots, Z_B^r\}$;

2. $M_1'^{(b)}$ is local randomness used by Encoder 1 and $M_2'^{(b)}$ is local randomness used by Encoder 2;

3. $K_1^{(b)}$ and $K_1^{(b)}$ are randomness extracted from the channel independent from each other and independent from Z_b^r. They are recycled towards the creation of $M_1'^{(b+1)}$ and $M_2'^{(b+1)}$ respectively;

4. The messages $M_1^{(b)}$, $M_1'^{(b)}$, $M_2^{(b)}$ and $M_2'^{(b)}$ can be decoded at the receiver from Y_b^r.

Encoding: In block b, the encoders send:

$$x_{1b}^r = x_1^r(m_1^{(b)}, m_1'^{(b)})$$
$$x_{2b}^r = x_2^r(m_2^{(b)}, m_2'^{(b)})$$

Decoding at the receiver: In block b, the legitimate receiver finds $\hat{m}_1$, $\hat{m}_1'$, $\hat{m}_2$ and $\hat{m}_2'$ such that

$$(x_1^r(\hat{m}_1, \hat{m}_1'), x_2^r(\hat{m}_2, \hat{m}_2'), y_b^r) \in \mathcal{T}_\epsilon^{(r)}(P_{X_1,X_2,Y})$$

Probability of error analysis: Using the arguments for error analysis from [35, Lemma 4], the probability of error of each block vanishes exponentially with r and in turn vanishes across blocks if

$$\rho_1 + \rho_1' < I(X_1; Y|X_2), \tag{4.53}$$

$$\rho_2 + \rho_2' < I(X_2; Y|X_1), \tag{4.54}$$

$$\rho_1 + \rho_1' + \rho_2 + \rho_2' < I(X_1, X_2; Y). \tag{4.55}$$

Secrecy analysis: It can be shown, similar to Section 3.4.11, that $I(M_1^{(b)}, M_2^{(b)}, K_1^{(b)}, K_2^{(b)}; Z_b^r) \to 0$ as $r \to \infty$ if:

$$\rho_1' + \rho_2' - \rho_{k1} - \rho_{k2} \geq I(X_1, X_2; Z) - H(Y|X_1, X_2, Z) \tag{4.56}$$

$$\rho_2' - \rho_{k1} - \rho_{k2} \geq I(X_2; Z) - H(Y|X_2, Z) \tag{4.57}$$

$$\rho_1' - \rho_{k1} - \rho_{k2} \geq I(X_1; Z) - H(Y|X_1, Z) \tag{4.58}$$

$$\rho_1' + \rho_2' \geq I(X_1, X_2; Z) \tag{4.59}$$

$$-\rho_{k1} - \rho_{k2} \geq H(Z) - H(Y, Z) \tag{4.60}$$

$$\rho_1' \geq I(X_1; Z) \tag{4.61}$$

$$\rho_2' \geq I(X_2; Z) \tag{4.62}$$

Similar to Section 3.4.8, it can be shown that $I(M_1^{(b)}, M_2^{(b)}, K_1^{(b)}, K_2^{(b)}; Z_b^r) \xrightarrow{r\to\infty} 0$ for all b implies $I(M_1, M_2; Z^n) \xrightarrow{n\to\infty} 0$.

We now derive an achievable rate region by choosing values for ρ_1, ρ_1', ρ_{k1}, ρ_2, ρ_2' and ρ_{k2} that satisfy the constraints for secrecy and probability of error.

The following rates satisfy all error and secrecy constraints:

$$\begin{aligned}
\rho_1' - \rho_{k1} &= \epsilon, \\
\rho_2' - \rho_{k2} &= [I(X_1, X_2; Z) - H(Y|X_1, X_2, Z) - \epsilon]^+, \\
R_1 &= I(X_1; Y|X_2) - \epsilon, \\
R_2 &= I(X_1, X_2; Y) - I(X_1; Y|X_2) - [I(X_1, X_2; Z) - H(Y|X_1, X_2, Z) - \epsilon]^+ + \epsilon,
\end{aligned}$$

and the same is true for the following rates:

$$\begin{aligned}
\rho_2' - \rho_{k2} &= \epsilon, \\
\rho_1' - \rho_{k1} &= [I(X_1, X_2; Z) - H(Y|X_1, X_2, Z) - \epsilon]^+, \\
R_2 &= I(X_2; Y|X_1) - \epsilon, \\
R_1 &= I(X_1, X_2; Y) - I(X_2; Y|X_1) - [I(X_1, X_2; Z) - H(Y|X_1, X_2, Z) - \epsilon]^+ + \epsilon.
\end{aligned}$$

Considering the above two corner points, the following rate region is achievable.

$$R_1 \leq I(X_1; Y|X_2)$$

$$R_2 \leq I(X_2;Y|X_1)$$

$$R_1 + R_2 \leq I(X_1,X_2;Y) - [I(X_1,X_2;Z) - H(Y|X_1,X_2,Z)]^+$$

4.4.3 Channel resolvability of MAC with generalized feedback

Achievability: Decode-and-forward

To handle the strict causality constraint, we adopt a block-Markov encoding scheme over $B > 0$ consecutive and dependent blocks, each consisting of r transmissions such that $n = rB$. The vector of n channel outputs Z^n at the channel output may then be described as $Z^n \triangleq (Z_1^r, \cdots, Z_B^r)$, where each Z_b^r for $b \in [\![1, B]\!]$ describes the observations in block b. The distribution induced by the coding scheme is the joint distribution $P_Z^n \triangleq P_{Z_1^r,\cdots,P_{Z_B^r}}$, while the target output distribution is a product distribution of product distributions $Q_Z^{\otimes n} \triangleq \prod_{j=1}^{B} Q_Z^{\otimes r}$.

Codebook Construction:

Consider a distribution $P_{U,X_1,X_2} = P_U P_{X_1|U} P_{X_2|U}$ such that $\sum_{u,x_1,x_2,Z_1,Z_2} P_{U,X_1,X_2} W_{Z_1,Z_2,Z|X_1,X_2} = Q_Z$ that satisfies $I(X_1;Z_2|X_2,U) + I(X_2;Z_1|X_1,U) > I(X_1,X_2;Z)$. For every $b \in [\![1, B]\!]$:

- Independently generate $2^{r\rho_0}$ codewords $u^r(m_0^{(b)})$ each with probability $P_{U^r} = P_U^{\otimes r}$. Label them $u^r(m_0^{(b)})$, $m_0^{(b)} \in [\![1, 2^{r\rho_0}]\!]$.
- For every $u^r(m_0^{(b)})$, independently generate $2^{r(\rho_1' + \rho_1'')}$ codewords $x_1^r(m_0^{(b)}, m_1^{\prime(b)}, m_1^{\prime\prime(b)})$ each with probability $P_{X_1^r|U^r} = P_{X_1^r|U^r}^{\otimes r}$. Label them $x_1^r(m_0^{(b)}, m_1^{\prime(b)}, m_1^{\prime\prime(b)})$, $m_1^{\prime(b)} \in [\![1, 2^{r\rho_1'}]\!]$ and $m_1^{\prime\prime(b)} \in [\![1, 2^{r\rho_1''}]\!]$.
- For every $u^r(m_0^{(b)})$, independently generate $2^{r(\rho_2' + \rho_2'')}$ codewords $x_2^r(m_0^{(b)}, m_2^{\prime(b)}, m_2^{\prime\prime(b)})$ each with probability $P_{X_2^r|U^r} = P_{X_2^r|U^r}^{\otimes r}$. Label them $x_2^r(m_0^{(b)}, m_2^{\prime(b)}, m_2^{\prime\prime(b)})$, $m_2^{\prime(b)} \in [\![1, 2^{r\rho_2'}]\!]$ and $m_2^{\prime\prime(b)} \in [\![1, 2^{r\rho_2''}]\!]$.

This defines the codebook in block b

$$\mathcal{C}_r = \{u^r(m_0^{(b)}), x_1^r(m_0^{(b)}, m_1'^{(b)}, m_1''^{(b)}), x_2^r(m_0^{(b)}, m_2'^{(b)}, m_2''^{(b)}), m_0^{(b)} \in [\![1, 2^{r\rho_0}]\!],$$
$$m_1'^{(b)} \in [\![1, 2^{r\rho_1'}]\!], m_1''^{(b)} \in [\![1, 2^{r\rho_1''}]\!], m_2'^{(b)} \in [\![1, 2^{r\rho_2'}]\!], m_2''^{(b)} \in [\![1, 2^{r\rho_2''}]\!]\} \quad (4.63)$$

and we denote the random codebook in block b by

$$\mathfrak{C}_r = \{U^r(m_0^{(b)}), X_1^r(m_0^{(b)}, m_1'^{(b)}, m_1''^{(b)}), X_2^r(m_0^{(b)}, m_2'^{(b)}, m_2''^{(b)}), m_0^{(b)} \in [\![1, 2^{r\rho_0}]\!],$$
$$m_1'^{(b)} \in [\![1, 2^{r\rho_1'}]\!], m_1''^{(b)} \in [\![1, 2^{r\rho_1''}]\!], m_2'^{(b)} \in [\![1, 2^{r\rho_2'}]\!], m_2''^{(b)} \in [\![1, 2^{r\rho_2''}]\!]\} \quad (4.64)$$

The messages $M_1'^{(b)}$ and $M_2'^{(b)}$ are part of $M_1^{(b)}$ and $M_2^{(b)}$ respectively and represent the local randomness at each encoder. The messages $M_1''^{(b)}$ and $M_2''^{(b)}$ are part of $M_1^{(b)}$ and $M_2^{(b)}$ respectively that are used by both encoders toward the creation of $M_0^{(b+1)}$, assuming $\rho_1'' + \rho_2'' > \rho_0$. Furthermore, for $\gamma \in [\![0, 1]\!]$, an amount $\gamma(\rho_1'' + \rho_2'' - \rho_0)$ is recycled towards the creation of $M_1'^{(b+1)}$ and an amount $(1 - \gamma)(\rho_1'' + \rho_2'' - \rho_0)$ is recycled towards the creation of $M_2'^{(b+1)}$.

Next we bound $\mathbb{D}(P_{Z^n}||Q_Z^{\otimes n})$ and show that dependencies across blocks created by block-Markov encoding can be eliminated by appropriately recycling randomness from one block to the next.

$$\begin{aligned}
&\mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) \\
&\quad = \mathbb{D}(P_{Z_1^r \ldots Z_B^r}||Q_Z^{\otimes rB}) \\
&\quad = \sum_{b=1}^{B} \mathbb{D}(P_{Z_j^r|Z_{b+1}^{B,r}}||Q_Z^{\otimes r}|P_{Z_{b+1}^{B,r}}) && (4.65) \\
&\quad = \sum_{b=1}^{B} \mathbb{D}(P_{Z_j^r}||Q_Z^{\otimes r}) + \sum_{b=1}^{B} \mathbb{D}(P_{Z_j^r|Z_{b+1}^{B,r}}||P_{Z_j^r}|P_{Z_{b+1}^{B,r}}) && (4.66) \\
&\quad = \sum_{b=1}^{B} \mathbb{D}(P_{Z_b^r}||Q_Z^{\otimes r}) + \sum_{b=1}^{B} I(Z_b^r; Z_{b+1}^{B,r}) && (4.67)
\end{aligned}$$

$$\overset{(a)}{\leq} \sum_{b=1}^{B} \mathbb{D}(P_{M_1''^{(b)},M_2''^{(b)},Z_b^r}||P_{M_1''^{(b)},M_2''^{(b)}}Q_Z^{\otimes r}) + \sum_{b=1}^{B} I(Z_b^r; M_1''^{(b)}, \hat{M}_1''^{(b)}, M_2''^{(b)}, \hat{M}_2''^{(b)}, Z_{b+1}^B) \tag{4.68}$$

$$\overset{(b)}{=} \sum_{b=1}^{B} \mathbb{D}(P_{M_1''^{(b)},M_2''^{(b)},Z_b^r}||P_{M_1''^{(b)},M_2''^{(b)}}Q_Z^{\otimes r}) + \sum_{b=1}^{B} I(Z_b^r; M_1''^{(b)}, \hat{M}_1''^{(b)}, M_2''^{(b)}, \hat{M}_2''^{(b)}) \tag{4.69}$$

$$\overset{(c)}{\leq} \sum_{b=1}^{B} 2 \times \mathbb{D}(P_{M_1''^{(b)},M_2''^{(b)},Z_b^r}||P_{M_1''^{(b)},M_2''^{(b)}}Q_Z^{\otimes r}) + \sum_{b=1}^{B} H(\hat{M}_1''^{(b)}, \hat{M}_2''^{(b)}|M_1''^{(b)}, M_2''^{(b)}) \tag{4.70}$$

where

(a) follows since $\mathbb{D}(P_{Z_b^r}||Q_Z^{\otimes r}) = \mathbb{D}(P_{Z_b^r,M_1''^{(b)},M_2''^{(b)}}||P_{M_1''^{(b)},M_2''^{(b)}}Q_Z^{\otimes r}) - \mathbb{D}(P_{Z_b^r,M_1''^{(b)},M_2''^{(b)}}||P_{M_1''^{(b)},M_2''^{(b)}}P_{Z_b^r})$;

(b) follows since $Z_b^r \to M_1''^{(b)}, \hat{M}_1''^{(b)}, M_2''^{(b)}, \hat{M}_2''^{(b)} \to Z_{b+1}^{B,r}$ holds; follows since $I(Z_b^r; M_1''^{(b)}, M_2''^{(b)}) = \mathbb{D}(P_{Z_b^r,M_1''^{(b)},M_2''^{(b)}}||P_{M_1''^{(b)},M_2''^{(b)}}P_{Z_b^r}) \leq \mathbb{D}(P_{Z_b^r,M_1''^{(b)},M_2''^{(b)}}||P_{M_1''^{(b)},M_2''^{(b)}}Q_Z^{\otimes r})$.

Let $P_e^{(b)}$ be the average error probability of both encoders decoding the other encoder's message. From Fano's inequality, we can write $H(\hat{M}_1''^{(b)}, \hat{M}_2''^{(b)}|M_1''^{(b)}, M_2''^{(b)}) \leq H(\hat{M}_1''^{(b)}|M_1''^{(b)}) + H(\hat{M}_2''^{(b)}|M_2''^{(b)}) \leq 2H(P_e^{(b)}) + r(\rho_1'' + \rho_2'')P_e^{(b)}$. By random coding we know that $\mathbb{E}_{\mathfrak{C}_r}\left(P_e^{(b)}\right) < 2^{-\alpha r}$ for some $\alpha > 0$ and all r large enough if $\rho_1' + \rho_1'' < I(X_1; Z_2|X_2, U)$ and $\rho_2' + \rho_2'' < I(X_2; Z_1|X_1, U)$.

Let $\bar{P}$ be the probability distribution induced when both encoders are using the same $M_0^{(b)}$, i.e., $(\hat{M}_1''^{(b-1)}, \hat{M}_2''^{(b-1)}) = (M_1''^{(b-1)}, M_2''^{(b-1)})$.

$$\mathbb{E}_{\mathfrak{C}_r}\big(\mathbb{D}(\bar{P}_{Z_b^r,M_1''^{(b)},M_2''^{(b)}}||\bar{P}_{M_1''^{(b)},M_2''^{(b)}}Q_Z^{\otimes r})\big)$$

$$= \mathbb{E}_{\mathfrak{C}_r} \sum_{m_1''^{(b)},m_2''^{(b)},z_b^r} \bar{P}_{Z_b^r,M_1''^{(b)},M_2''^{(b)}} \log \frac{\bar{P}_{Z_b^r|M_1''^{(b)},M_2''^{(b)}}}{Q_Z^{\otimes r}} \tag{4.71}$$

$$= \mathbb{E}_{\mathfrak{C}_r} \sum_{m_1''^{(b)},m_2''^{(b)},z_b^r} 2^{-r(\rho_1''+\rho_2'')} \sum_{m_0^{(b)},m_1'^{(b)},m_2'^{(b)}} 2^{-r(\rho_0+\rho_1'+\rho_2')}$$

$$\bar{P}^{\otimes r}(z_b^r|U^r(m_0^{(b)}), X_1^r(m_0^{(b)}, m_1'^{(b)}, m_1''^{(b)}), X_2^r(m_0^{(b)}, m_2'^{(b)}, m_2''^{(b)}))$$

$$\times \log \sum_{i,j,k} \frac{P^{\otimes r}(z_b^r|U^r(i), X_1^r(i,j,m_1''^{(b)}), X_2^r(i,k,m_2''^{(b)}))}{2^{r(\rho_0+\rho_1'+\rho_2')}Q_Z^{\otimes r}} \tag{4.72}$$

$$\overset{(a)}{\leq} \sum_{m_1''^{(b)}, m_2''^{(b)}, z_b^r} 2^{-n(\rho_1''+\rho_2'')} \sum_{m_0^{(b)}, m_1'^{(b)}, m_2'^{(b)}} 2^{-r(\rho_0+\rho_1'+\rho_2')} \sum_{u^r(m_0^{(b)}), x_1^r(m_0^{(b)}, m_1'^{(b)}, m_1''^{(b)}), x_2^r(m_0^{(b)}, m_2'^{(b)}, m_2''^{(b)})}$$

$$\bar{P}^{\otimes r}(u^r(m_0^{(b)}), x_1^r(m_0^{(b)}, m_1'^{(b)}, m_1''^{(b)}), x_2^r(m_0^{(b)}, m_2'^{(b)}, m_2''^{(b)}), z_b^r)$$

$$\times \log \mathbb{E}_{\setminus(m_0^{(b)}, m_1'^{(b)}, m_2'^{(b)})} \sum_{i,j,k} \frac{P^{\otimes r}(z_b^r|U^r(i), X_1^r(i,j,m_1''^{(b)}), X_2^r(i,k,m_2''^{(b)}))}{2^{r(\rho_0+\rho_1'+\rho_2')}Q_Z^{\otimes r}} \tag{4.73}$$

$$= \sum_{m_1''^{(b)}, m_2''^{(b)}, z_b^r} 2^{-n(\rho_1''+\rho_2'')} \sum_{m_0^{(b)}, m_1'^{(b)}, m_2'^{(b)}} 2^{-r(\rho_0+\rho_1'+\rho_2')} \sum_{u^r(m_0^{(b)}), x_1^r(m_0^{(b)}, m_1'^{(b)}, m_1''^{(b)}), x_2^r(m_0^{(b)}, m_2'^{(b)}, m_2''^{(b)})}$$

$$\bar{P}^{\otimes r}(u^r(m_0^{(b)}), x_1^r(m_0^{(b)}, m_1'^{(b)}, m_1''^{(b)}), x_2^r(m_0^{(b)}, m_2'^{(b)}, m_2''^{(b)}), z_b^r)$$

$$\times \log \mathbb{E}_{\setminus(m_0^{(b)}, m_1'^{(b)}, m_2'^{(b)})} \frac{1}{2^{r(\rho_0+\rho_1'+\rho_2')}Q_Z^{\otimes r}}$$

$$\Bigg[P^{\otimes r}(z_b^r|u^r(m_0^{(b)}), x_1^r(m_0^{(b)}, m_1'^{(b)}, m_1''^{(b)}), x_2^r(m_0^{(b)}, m_2'^{(b)}, m_2''^{(b)}))$$

$$+ \sum_{j \neq m_1'^{(b)}} P^{\otimes r}(z_b^r|u^r(m_0^{(b)}), X_1^r(m_0^{(b)}, j, m_1''^{(b)}), x_2^r(m_0^{(b)}, m_2'^{(b)}, m_2''^{(b)}))$$

$$+ \sum_{k \neq m_2'^{(b)}} W^{\otimes r}(z_b^r|u^r(m_0^{(b)}), x_1^r(m_0^{(b)}, m_1'^{(b)}, m_1''^{(b)}), X_2^r(m_0^{(b)}k, m_2''^{(b)}))$$

$$+ \sum_{\substack{j \neq m_1'^{(b)} \\ k \neq m_2'^{(b)}}} W^{\otimes r}(z_b^r|u^r(m_0^{(b)}), X_1^r(m_0^{(b)}, j, m_1''^{(b)}), X_2^r(m_0^{(b)}, k, m_2''^{(b)}))$$

$$+ \sum_{\substack{i \neq m_0^{(b)} \\ j,k}} W^{\otimes r}(z_b^r|U^r(i), X_1^r(i,j,m_1''^{(b)}), X_2^r(i,k,m_2''^{(b)}))\Bigg] \tag{4.74}$$

$$\overset{(b)}{\leq} \sum_{m_1''^{(b)}, m_2''^{(b)}, z_b^r} 2^{-n(\rho_1''+\rho_2'')} \sum_{m_0^{(b)}, m_1'^{(b)}, m_2'^{(b)}} 2^{-r(\rho_0+\rho_1'+\rho_2')} \sum_{u^r(m_0^{(b)}), x_1^r(m_0^{(b)}, m_1'^{(b)}, m_1''^{(b)}), x_2^r(m_0^{(b)}, m_2'^{(b)}, m_2''^{(b)})}$$

$$\bar{P}^{\otimes r}(u^r(m_0^{(b)}), x_1^r(m_0^{(b)}, m_1'^{(b)}, m_1''^{(b)}), x_2^r(m_0^{(b)}, m_2'^{(b)}, m_2''^{(b)}), z_b^r)$$

$$\times \log \frac{1}{2^{r(\rho_0+\rho_1'+\rho_2')}Q_Z^{\otimes r}}$$

$$\begin{aligned}
&\Bigg[P^{\otimes r}(z_b^r|u^r(m_0^{(b)}), x_1^r(m_0^{(b)}, m_1'^{(b)}, m_1''^{(b)}), x_2^r(m_0^{(b)}, m_2'^{(b)}, m_2''^{(b)})) \\
&+ \sum_{j \neq m_1'^{(b)}} \bar{P}^{\otimes r}(z_b^r|u^r(m_0^{(b)}), x_2^r(m_0^{(b)}, m_2'^{(b)}, m_2''^{(b)})) \\
&+ \sum_{k \neq m_2'^{(b)}} \bar{P}^{\otimes r}(z_b^r|u^r(m_0^{(b)}), x_1^r(m_0^{(b)}, m_1'^{(b)}, m_1''^{(b)})) \\
&+ \sum_{\substack{j \neq m_1'^{(b)} \\ k \neq m_2'^{(b)}}} \bar{P}^{\otimes r}(z_b^r|u^r(m_0^{(b)})) \\
&+ \sum_{\substack{i \neq m_0^{(b)} \\ j,k}} \bar{P}^{\otimes r}(z_b^r)\Bigg] \qquad (4.75) \\
&\overset{(c)}{=} \Psi_1 + \Psi_2 \qquad (4.76)
\end{aligned}$$

where

(a) follows by Jensen's Inequality;

(b) follows by taking the expectation inside the log of the previous step;

(c) Ψ_1 is found by restricting the sum in the previous step over $(u^r, x_1^r, x_2^r, z_b^r) \in \mathcal{T}_\epsilon^r(P_{U,X_1,X_2,Y,Z})$ and Ψ_2 is found by restricting that sum over $(u^r, x_1^r, x_2^r, z_b^r) \notin \mathcal{T}_\epsilon^r(P_{U,X_1,X_2,Z})$.

Solving Ψ_1 and Ψ_2 like in previous sections we find that $\mathbb{D}(\bar{P}_{Z_b^r, M_1''^{(b)}, M_2''^{(b)}} || \bar{P}_{M_1''^{(b)}, M_2''^{(b)}} Q_Z^{\otimes r}) \xrightarrow{r\to\infty} 0$ if:

$$\rho_0 + \rho_1' + \rho_2' > I(X_1, X_2; Z) \qquad (4.77)$$

$$\rho_0 + \rho_2' > I(U, X_2; Z) \qquad (4.78)$$

$$\rho_0 + \rho_1' > I(U, X_1; Z) \qquad (4.79)$$

$$\rho_0 > I(U; Z) \qquad (4.80)$$

Let $\epsilon > 0$, set

$$\rho_0 = I(U; Z) + \epsilon \tag{4.81}$$

$$\rho_1' = I(X_1; Z|U) + \epsilon \tag{4.82}$$

$$\rho_1'' = I(X_1; Z_2|X_2, U) - I(X_1; Z|U) - 2\epsilon \tag{4.83}$$

$$\rho_2' = I(X_2; Z|X_1, U) + \epsilon \tag{4.84}$$

$$\rho_2'' = I(X_2; Z_1|X_1, U) - I(X_2; Z|X_1, U) - 2\epsilon \tag{4.85}$$

We can write the effective rates of new randomness at both encoders as:

$$R_1 \triangleq \rho_1' + \rho_1'' - \gamma(\rho_1'' + \rho_2'' - \rho_0) \tag{4.86}$$

$$R_2 \triangleq \rho_2' + \rho_2'' - (1 - \gamma)(\rho_1'' + \rho_2'' - \rho_0) \tag{4.87}$$

$$R_1 + R_2 \triangleq \rho_1' + \rho_2' + \rho_0 \tag{4.88}$$

Using the values of ρ_0, ρ_1', ρ_1'', ρ_2' and ρ_2'' chosen above, we obtain the rate region as follows:

$$R_1 \geq I(X_1, X_2; Z) - I(X_2; Z_1|X_2, U) + 2\epsilon \tag{4.89}$$

$$R_2 \geq I(X_1, X_2; Z) - I(X_1; Z_2|X_1, U) + 2\epsilon \tag{4.90}$$

$$R_1 + R_2 \geq I(X_1, X_2; Z) + 3\epsilon \tag{4.91}$$

Finally, we note that $\mathbb{E}_{\mathfrak{C}_r}\big(\mathbb{D}(\bar{P}_{Z_b^r, M_1''^{(b)}, M_2''^{(b)}} || \bar{P}_{M_1''^{(b)}, M_2''^{(b)}} Q_Z^{\otimes r})\big) \xrightarrow{r\to\infty} 0$ implies $\mathbb{E}_{\mathfrak{C}_r}\big(\mathbb{D}(P_{Z_b^r, M_1''^{(b)}, M_2''^{(b)}} || P_{M_1''^{(b)}, M_2''^{(b)}} Q_Z^{\otimes r})\big) \xrightarrow{r\to\infty} 0$ (see discussion in Section 3.4.1) if

$$\rho_1' + \rho_1'' < I(X_1; Z_2|X_2, U) \tag{4.92}$$

$$\rho_2' + \rho_2'' < I(X_2; Z_1|X_1, U) \tag{4.93}$$

Achievability: Randomness Extraction

We adopt a block-Markov encoding scheme over $B > 0$ consecutive and dependent blocks, each consisting of r transmissions such that $n = rB$. The vector of n channel outputs Z^n

at the channel output may then be described as $Z^n \triangleq (Z_1^r, \cdots, Z_B^r)$, where each Z_b^r for $b \in \llbracket 1, B \rrbracket$ describes the observations in block b. The distribution induced by the coding scheme is the joint distribution $P_Z^n \triangleq P_{Z_1^r, \cdots, P_{Z_B^r}}$, while the target output distribution is a product distribution of product distributions $Q_Z^{\otimes n} \triangleq \prod_{j=1}^{B} Q_Z^{\otimes r}$.

Codebook Construction:

Consider a distribution $P_{X_1,X_2} = P_{X_1} P_{X_2}$ such that $\sum_{x_1,x_2,Z_1,Z_2} P_{X_1,X_2} W_{Z_1,Z_2,Z|X_1,X_2} = Q_Z$. For every $b \in \llbracket 1, B \rrbracket$:

- Independently generate $2^{r\rho_1}$ codewords $x_1^r(m_1^{(b)})$ each with probability $P_{X_1^r} = P_{X_1^r}^{\otimes r}$. Label them $x_1^r(m_1^{(b)})$, $m_1^{(b)} \in \llbracket 1, 2^{r\rho_1} \rrbracket$.

- Independently generate $2^{r\rho_2}$ codewords $x_1^r(m_2^{(b)})$ each with probability $P_{X_2^r} = P_{X_2^r}^{\otimes r}$. Label them $x_2^r(m_2^{(b)})$, $m_2^{(b)} \in \llbracket 1, 2^{r\rho_2} \rrbracket$.

Random binning at each encoder:

- For each $(x_1^r(m_1^{(b)}), z_{1b}^r)$, assign uniformly and independently a random bin index $k_1^{(b)} \in \llbracket 1, 2^{r\rho_{k1}} \rrbracket$. We denote $k_1^{(b)} = \phi_{1b}(x_1^r(m_1^{(b)}), z_{1b}^r)$.

- For each $(x_2^r(m_2^{(b)}), z_{2b}^r)$, assign uniformly and independently a random bin index $k_2^{(b)} \in \llbracket 1, 2^{r\rho_{k2}} \rrbracket$. We denote $k_2^{(b)} = \phi_{2b}(x_2^r(m_2^{(b)}), z_{2b}^r)$.

This defines the codebook in block b

$$\mathcal{C}_r = \{x_1^r(m_1^{(b)}), x_2^r(m_2^{(b)}), m_1^{(b)} \in \llbracket 1, 2^{r\rho_1} \rrbracket, m_2^{(b)} \in \llbracket 1, 2^{r\rho_2} \rrbracket\} \tag{4.94}$$

and we denote the random codebook in block b by

$$\mathfrak{C}_r = \{X_1^r(m_1^{(b)}), X_2^r(m_2^{(b)}), m_1^{(b)} \in \llbracket 1, 2^{r\rho_1} \rrbracket, m_2^{(b)} \in \llbracket 1, 2^{r\rho_2} \rrbracket\} \tag{4.95}$$

$K_1^{(b)}$ and $K_1^{(b)}$ are random variables representing the randomness that stems from channel noise and are used towards the creation of $M_1^{(b+1)}$ and $M_2^{(b+1)}$ respectively. For every

$(X_1^r(m_1^{(b)}), z_{1b}^r)$, let $\Phi_{1b}(X_1^r(m_1^{(b)}), z_{1b}^r)$ be the random variables representing the index associated to $(X_1^r(m_1^{(b)}), z_{1b}^r)$. For every $(X_2^r(m_2^{(b)}), z_{2b}^r)$, let $\Phi_{2b}(X_2^r(m_2^{(b)}), z_{2b}^r)$ be the random variables representing the index associated to $(X_2^r(m_2^{(b)}), z_{2b}^r)$.

Next we bound $\mathbb{D}(P_{Z^n}||Q_Z^{\otimes n})$ and show that the dependencies across blocks created by block-Markov coding can be eliminated by suitably recycling the extracted randomness from one block to the next.

$$\begin{aligned}
&\mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) = \mathbb{D}(P_{Z_1^r \dots Z_B^r}||Q_Z^{\otimes rB}) \\
&\overset{(a)}{=} \sum_{b=1}^{B} \mathbb{D}(P_{Z_b^r}||Q_Z^{\otimes r}) + \sum_{b=1}^{B} \mathbb{D}(P_{Z_b^r|Z_{b+1}^{B,r}}||P_{Z_b^r}|P_{Z_{b+1}^{B,r}}) \\
&= \sum_{b=1}^{B} \mathbb{D}(P_{Z_b^r}||Q_Z^{\otimes r}) + \sum_{b=1}^{B} I(Z_b^r; Z_{b+1}^{B,r}) \\
&\overset{(b)}{\leq} \sum_{b=1}^{B} \mathbb{D}(P_{Z_b^r, K_1^{(b)}, K_2^{(b)}}||Q_Z^{\otimes r} Q_{K_1^{(b)}} Q_{K_2^{(b)}}) + \sum_{b=1}^{B} I(Z_b^r; K_1^{(b)}, K_2^{(b)}, Z_{b+1}^{B,r}) \\
&\overset{(c)}{=} \sum_{b=1}^{B} \mathbb{D}(P_{Z_b^r, K_1^{(b)}, K_2^{(b)}}||Q_Z^{\otimes r} Q_{K_1^{(b)}} Q_{K_2^{(b)}}) + \sum_{b=1}^{B} I(Z_b^r; K_1^{(b)}, K_2^{(b)}) \\
&\overset{(d)}{\leq} 2 \sum_{b=1}^{B} \mathbb{D}(P_{Z_b^r, K_1^{(b)}, K_2^{(b)}}||Q_Z^{\otimes r} Q_{K_1^{(b)}} Q_{K_2^{(b)}})
\end{aligned}$$

where

(a) follows from the definition $Z_{b+1}^{B,r} = \{Z_{b+1}^r, \dots Z_B^r\}$;

(b) follows since $\mathbb{D}(P_{Z_b^r}||Q_Z^{\otimes r}) = \mathbb{D}(P_{Z_b^r, K_1^{(b)}, K_2^{(b)}}||Q_Z^{\otimes r} Q_{K_1^{(b)}} Q_{K_2^{(b)}}) - \mathbb{D}(P_{Z_b^r, K_1^{(b)}, K_2^{(b)}}||P_{Z_b^r} Q_{K_1^{(b)}} Q_{K_2^{(b)}})$. $Q_{K_1^{(b)}}$ is the uniform distribution over $[\![1, 2^{r\rho_{k1}}]\!]$ and $Q_{K_2^{(b)}}$ is the uniform distribution over $[\![1, 2^{r\rho_{k2}}]\!]$;

(c) follows since $Z_b^r \to K_1^{(b)}, K_2^{(b)} \to Z_{b+1}^{B,r}$ holds;

(d) follows since $I(Z_b^r; K_1^{(b)}, K_2^{(b)}) = \mathbb{D}(P_{Z_b^r, K_1^{(b)}, K_2^{(b)}}||P_{Z_b^r} P_{K_1^{(b)}, K_2^{(b)}}) \leq \mathbb{D}(P_{Z_b^r, K_1^{(b)}, K_2^{(b)}}||Q_Z^{\otimes r} Q_{K_1^{(b)}} Q_{K_2^{(b)}})$.

$$
\begin{aligned}
&\mathbb{E}_{\mathfrak{C}_r,\Phi_{1b},\Phi_{2b}}\big(\mathbb{D}(P_{Z_b^r,K_1^{(b)},K_2^{(b)}}||Q_{K_1^{(b)}}Q_{K_2^{(b)}}Q_Z^{\otimes r})\big)\\
&= \mathbb{E}_{\mathfrak{C}_r,\Phi_{1b},\Phi_{2b}} \sum_{k_1^{(b)},k_2^{(b)},z_b^r} P_{Z_b^r,K_1^{(b)},K_2^{(b)}} \log \frac{P_{Z_b^r,K_1^{(b)},K_2^{(b)}}}{Q_{K_1^{(b)}}Q_{K_2^{(b)}}Q_Z^{\otimes r}} \qquad (4.96)\\
&= \mathbb{E}_{\mathfrak{C}_r,\Phi_{1b},\Phi_{2b}} \sum_{k_1^{(b)},k_2^{(b)},z_b^r} \sum_{m_1^{(b)},m_2^{(b)}} \sum_{z_{1b}^r,z_{2b}^r} 2^{-r(\rho_1+\rho_2)}\\
&\quad W^{\otimes r}(z_{1b}^r,z_{2b}^r,z_b^r|X_1^r(m_1^{(b)}),X_2^r(m_2^{(b)}))\mathbb{1}\{\Phi_{1b}(x_1^r(m_1^{(b)}),z_{1b}^r)=k_1^{(b)}\}\mathbb{1}\{\Phi_{2b}(x_2^r(m_2^{(b)}),z_{2b}^r)=k_2^{(b)}\}\\
&\quad \times \log \sum_{i,j,\bar{z}_1,\bar{z}_2} \frac{W^{\otimes r}(\bar{z}_1,\bar{z}_2,z_b^r|X_1^r(i),X_2^r(j)\mathbb{1}\{\Phi_{1b}(x_1^r(i),\bar{z}_1)=k_1^{(b)}\}\mathbb{1}\{\Phi_{2b}(x_2^r(j),\bar{z}_2)=k_2^{(b)}\}}{2^{r(\rho_1+\rho_2-\rho_{k1}-\rho_{k2})}Q_Z^{\otimes r}}\\
&\qquad (4.97)\\
&\overset{(a)}{\leq} \sum_{k_1^{(b)},k_2^{(b)},z_b^r} \sum_{m_1^{(b)},m_2^{(b)}} \sum_{z_{1b}^r,z_{2b}^r} 2^{-r(\rho_1+\rho_2)}2^{-r(\rho_{k1}+\rho_{k2})} \sum_{x_1^r(m_1^{(b)}),x_2^r(m_2^{(b)})}\\
&\quad P^{\otimes r}(x_1^r(m_1^{(b)}),x_2^r(m_2^{(b)}),z_{1b}^r,z_{2b}^r,z_b^r) \times \log \mathbb{E}_{\backslash(m_1^{(b)},m_2^{(b)},z_{1b}^r,z_{2b}^r)}\\
&\quad \sum_{i,j,\bar{z}_1,\bar{z}_2} \frac{W^{\otimes r}(\bar{z}_1,\bar{z}_2,z_b^r|X_1^r(i),X_2^r(j))\mathbb{1}\{\Phi_{1b}(x_1^r(i),\bar{z}_1)=k_1^{(b)}\}\mathbb{1}\{\Phi_{2b}(x_2^r(j),\bar{z}_2)=k_2^{(b)}\}}{2^{r(\rho_1+\rho_2-\rho_{k1}-\rho_{k2})}Q_Z^{\otimes r}}\\
&\qquad (4.98)\\
&= \sum_{k_1^{(b)},k_2^{(b)},z_b^r} \sum_{m_1^{(b)},m_2^{(b)}} \sum_{z_{1b}^r,z_{2b}^r} 2^{-r(\rho_1+\rho_2)}2^{-r(\rho_{k1}+\rho_{k2})} \sum_{x_1^r(m_1^{(b)}),x_2^r(m_2^{(b)})}\\
&\quad P^{\otimes r}(x_1^r(m_1^{(b)}),x_2^r(m_2^{(b)}),z_{1b}^r,z_{2b}^r,z_b^r) \times \log \mathbb{E}_{\backslash(m_1^{(b)},m_2^{(b)},z_{1b}^r,z_{2b}^r)} \frac{1}{2^{r(\rho_1+\rho_2-\rho_{k1}-\rho_{k2})}Q_Z^{\otimes r}}\\
&\quad \Big[W^{\otimes r}(z_{1b}^r,z_{2b}^r,z_b^r|x_1^r(m_1^{(b)}),x_2^r(m_2^{(b)}))\mathbb{1}\{\phi_{1b}(x_1^r(m_1^{(b)}),z_{1b}^r)=k_1^{(b)}\}\mathbb{1}\{\phi_{2b}(x_2^r(m_1^{(b)}),z_{2b}^r)=k_2^{(b)}\}\\
&\quad + \sum_{i\neq m_1^{(b)}} W^{\otimes r}(z_{1b}^r,z_{2b}^r,z_b^r|X_1^r(i),x_2^r(m_2^{(b)}))\mathbb{1}\{\Phi_{1b}(x_1^r(i),z_{1b}^r)=k_1^{(b)}\}\mathbb{1}\{\phi_{2b}(x_2^r(m_2^{(b)}),z_{2b}^r)=k_2^{(b)}\}\\
&\quad + \sum_{j\neq m_2^{(b)}} W^{\otimes r}(z_{1b}^r,z_{2b}^r,z_b^r|x_1^r(m_1^{(b)}),X_2^r(j))\mathbb{1}\{\phi_{1b}(x_1^r(m_1^{(b)}),z_{1b}^r)=k_1^{(b)}\}\mathbb{1}\{\Phi_{2b}(x_2^r(j),z_{2b}^r)=k_2^{(b)}\}\\
&\quad + \sum_{\bar{z}_1\neq z_{1b}^r} W^{\otimes r}(\bar{z}_1,z_{2b}^r,z_b^r|x_1^r(m_1^{(b)}),x_2^r(m_2^{(b)}))\mathbb{1}\{\Phi_{1b}(x_1^r(m_1^{(b)}),\bar{z}_1)=k_1^{(b)}\}
\end{aligned}
$$

$$\mathbb{1}\{\phi_{2b}(x_2^r(m_2^{(b)}), z_{2b}^r) = k_2^{(b)}\}$$

$$+ \sum_{\bar{z}_2 \neq z_{2b}^r} W^{\otimes r}(z_{1b}^r, \bar{z}_2, z_b^r | x_1^r(m_1^{(b)}), x_2^r(m_2^{(b)})) \mathbb{1}\{\phi_{1b}(x_1^r(m_1^{(b)}), z_{1b}^r) = k_1^{(b)}\}$$

$$\mathbb{1}\{\Phi_{2b}(x_2^r(m_2^{(b)}), \bar{z}_2) = k_2^{(b)}\}$$

$$+ \sum_{\substack{i \neq m_1^{(b)} \\ j \neq m_2^{(b)}}} W^{\otimes r}(z_1^{(b)}, z_2^{(b)}, z_b^r | X_1^r(i), X_2^r(j)) \mathbb{1}\{\Phi_{1b}(x_1^r(i), z_1^{(b)}) = k_1^{(b)}\}$$

$$\mathbb{1}\{\Phi_{2b}(x_2^r(j), z_2^{(b)}) = k_2^{(b)}\}$$

$$+ \sum_{\substack{\bar{Z}_1 \neq z_1^{(b)} \\ \bar{z}_2 \neq z_{2b}^r}} W^{\otimes r}(\bar{z}_1, \bar{z}_2, z_b^r | x_1^r(m_1^{(b)}), x_2^r(m_2^{(b)})) \mathbb{1}\{\Phi_{1b}(x_1^r(m_1^{(b)}), \bar{z}_1) = k_1^{(b)}\}$$

$$\mathbb{1}\{\Phi_{2b}(x_2^r(m_2^{(b)}), \bar{z}_2) = k_2^{(b)}\}$$

$$+ \sum_{\substack{i \neq m_1^{(b)} \\ \bar{z}_1 \neq z_{1b}^r}} W^{\otimes r}(\bar{z}_1, z_{2b}^r, z_b^r | X_1^r(i), x_2^r(m_2^{(b)})) \mathbb{1}\{\Phi_{1b}(x_1^r(i), \bar{z}_1) = k_1^{(b)}\} \mathbb{1}\{\phi_{2b}(x_2^r(m_2^{(b)}), z_{2b}^r) = k_2^{(b)}\}$$

$$+ \sum_{\substack{i \neq m_1^{(b)} \\ \bar{z}_2 \neq z_{2b}^r}} W^{\otimes r}(z_{1b}^r, \bar{z}_2, z_b^r | X_1^r(i), x_2^r(m_2^{(b)})) \mathbb{1}\{\Phi_{1b}(x_1^r(i), z_{1b}^r) = k_1^{(b)}\} \mathbb{1}\{\Phi_{2b}(x_2^r(m_2^{(b)}), \bar{z}_2) = k_2^{(b)}\}$$

$$+ \sum_{\substack{j \neq m_2^{(b)} \\ \bar{z}_1 \neq z_{1b}^r}} W^{\otimes r}(\bar{z}_1, z_{2b}^r, z_b^r | x_1^r(m_1^{(b)}), X_2^r(j)) \mathbb{1}\{\Phi_{1b}(x_1^r(m_1^{(b)}), \bar{z}_1) = k_1^{(b)}\} \mathbb{1}\{\Phi_{2b}(x_2^r(j), z_{2b}^r) = k_2^{(b)}\}$$

$$+ \sum_{\substack{j \neq m_2^{(b)} \\ \bar{z}_2 \neq z_{2b}^r}} W^{\otimes r}(z_{1b}^r, \bar{z}_2, z_b^r | x_1^r(m_1^{(b)}), X_2^r(j)) \mathbb{1}\{\phi_{1b}(x_1^r(m_1^{(b)}), z_{1b}^r) = k_1^{(b)}\} \mathbb{1}\{\Phi_{2b}(x_2^r(j), \bar{z}_2) = k_2^{(b)}\}$$

$$+ \sum_{\substack{i \neq m_1^{(b)} \\ j \neq m_2^{(b)} \\ \bar{z}_1 \neq z_{1b}^r}} W^{\otimes r}(\bar{z}_1, z_{2b}^r, z_b^r | X_1^r(i), X_2^r(j)) \mathbb{1}\{\Phi_{1b}(x_1^r(i), \bar{z}_1) = k_1^{(b)}\} \mathbb{1}\{\Phi_{2b}(x_2^r(j), z_{2b}^r) = k_2^{(b)}\}$$

$$+ \sum_{\substack{i \neq m_1^{(b)} \\ j \neq m_2^{(b)} \\ \bar{z}_2 \neq z_{2b}^r}} W^{\otimes r}(z_{1b}^r, \bar{z}_2, z_b^r | X_1^r(i), X_2^r(j)) \mathbb{1}\{\Phi_{1b}(x_1^r(i), z_{1b}^r) = k_1^{(b)}\} \mathbb{1}\{\Phi_{2b}(x_2^r(j), \bar{z}_2) = k_2^{(b)}\}$$

$$+ \sum_{\substack{i\neq m_1^{(b)}\\ \bar{z}_1\neq z_{1b}^r\\ \bar{z}_2\neq z_{2b}^r}} W^{\otimes r}(\bar{z}_1,\bar{z}_2,z_b^r|X_1^r(i),x_2^r(m_2^{(b)}))\mathbb{1}\{\Phi_{1b}(x_1^r(i),\bar{z}_1)=k_1^{(b)}\}\mathbb{1}\{\Phi_{2b}(x_2^r(m_2^{(b)}),\bar{z}_2)=k_2^{(b)}\}$$

$$+ \sum_{\substack{j\neq m_2^{(b)}\\ \bar{z}_1\neq z_{1b}^r\\ \bar{z}_2\neq z_{2b}^r}} W^{\otimes r}(\bar{z}_1,\bar{z}_2,z_b^r|x_1^r(m_1^{(b)}),X_2^r(j))\mathbb{1}\{\Phi_{1b}(x_1^r(m_1^{(b)}),\bar{z}_1)=k_1^{(b)}\}\mathbb{1}\{\Phi_{2b}(x_2^r(j),\bar{z}_2)=k_2^{(b)}\}$$

$$+ \sum_{\substack{i\neq m_1^{(b)}\\ j\neq m_2^{(b)}\\ \bar{z}_1\neq z_{1b}^r\\ \bar{z}_2\neq z_{2b}^r}} W^{\otimes r}(\bar{z}_1,\bar{z}_2,z_b^r|X_1^r(i),X_2^r(j))\mathbb{1}\{\Phi_{1b}(x_1^r(i),\bar{z}_1)=k_1^{(b)}\}\mathbb{1}\{\Phi_{2b}(x_2^r(j),\bar{z}_2)=k_2^{(b)}\}\Bigg] \tag{4.99}$$

$$\leq \sum_{k_1^{(b)},k_2^{(b)},z_b^r}\ \sum_{m_1^{(b)},m_2^{(b)}}\ \sum_{z_{1b}^r,z_{2b}^r} 2^{-r(\rho_1+\rho_2)}2^{-r(\rho_{k1}+\rho_{k2})} \sum_{x_1^r(m_1^{(b)}),x_2^r(m_2^{(b)})}$$

$$P^{\otimes r}(x_1^r(m_1^{(b)}),x_2^r(m_2^{(b)}),z_{1b}^r,z_{2b}^r,z_b^r)\times\log\frac{1}{2^{r(\rho_1+\rho_2-\rho_{k1}-\rho_{k2})}Q_Z^{\otimes r}}$$

$$\Bigg[W^{\otimes r}(z_{1b}^r,z_{2b}^r,z_b^r|x_1^r(m_1^{(b)}),x_2^r(m_2^{(b)}))$$

$$+\sum_{i\neq m_1^{(b)}} 2^{-r\rho_{k1}}P^{\otimes r}(z_{1b}^r,z_{2b}^r,z_b^r|x_2^r(m_2^{(b)}))$$

$$+\sum_{j\neq m_2^{(b)}} 2^{-r\rho_{k2}}P^{\otimes r}(z_{1b}^r,z_{2b}^r,z_b^r|x_1^r(m_1^{(b)}))\}$$

$$+2^{-r\rho_{k1}}P^{\otimes r}(z_{2b}^r,z_b^r|x_1^r(m_1^{(b)}),x_2^r(m_2^{(b)}))$$

$$+2^{-r\rho_{k2}}P^{\otimes r}(z_{1b}^r,z_b^r|x_1^r(m_1^{(b)}),x_2^r(m_2^{(b)}))$$

$$+\sum_{\substack{i\neq m_1^{(b)}\\ j\neq m_2^{(b)}}} 2^{-r(\rho_{k1}+\rho_{k2})}P^{\otimes r}(z_{1b}^r,z_{2b}^r,z_b^r)$$

$$+2^{r(\rho_{k1}+\rho_{k2})}P^{\otimes r}(z_b^r|x_1^r(m_1^{(b)}),x_2^r(m_2^{(b)}))$$

$$+\sum_{i\neq m_1^{(b)}} 2^{-r\rho_{k1}}P^{\otimes r}(z_{2b}^r,z_b^r|x_2^r(m_2^{(b)}))$$

$$+ \sum_{i \neq m_1^{(b)}} 2^{-r(\rho_{k1}+\rho_{k2})} P^{\otimes r}(z_{1b}^r, z_b^r | x_2^r(m_2^{(b)}))$$

$$+ \sum_{j \neq m_2^{(b)}} 2^{-r(\rho_{k1}+\rho_{k2})} P^{\otimes r}(z_{2b}^r, z_b^r | x_1^r(m_1^{(b)}))$$

$$+ \sum_{j \neq m_2^{(b)}} 2^{-r\rho_{k2}} P^{\otimes r}(z_{1b}^r, z_b^r | x_1^r(m_1^{(b)}))$$

$$+ \sum_{\substack{i \neq m_1^{(b)} \\ j \neq m_2^{(b)}}} 2^{-r(\rho_{k1}+\rho_{k1})} P^{\otimes r}(z_{2b}^r, z_b^r)$$

$$+ \sum_{\substack{i \neq m_1^{(b)} \\ j \neq m_2^{(b)}}} 2^{-r(\rho_{k1}+\rho_{k1})} P^{\otimes r}(z_{1b}^r, z_b^r)$$

$$+ \sum_{i \neq m_1^{(b)}} 2^{-r(\rho_{k1}+\rho_{k1})} P^{\otimes r}(z_b^r | x_2^r(m_2^{(b)}))$$

$$+ \sum_{j \neq m_2^{(b)}} 2^{-r(\rho_{k1}+\rho_{k1})} P^{\otimes r}(z_b^r | x_1^r(m_1^{(b)}))$$

$$+ \sum_{\substack{i \neq m_1^{(b)} \\ j \neq m_2^{(b)}}} 2^{-r(\rho_{k1}+\rho_{k1})} P^{\otimes r}(z_b^r) \Bigg] \tag{4.100}$$

$$= \Psi_1 + \Psi_2 \tag{4.101}$$

where

(a) follows by taking the expectation over $X_1^r(m_1^{(b)})$, $X_2^r(m_2^{(b)})$, $\Phi_{1b}(X_1^r(m_1^{(b)}), z_{1b}^r)$ and $\Phi_{2b}(X_2^r(m_2^{(b)}), z_{2b}^r)$

Solving Ψ_1 and Ψ_2 like in previous sections we find that $\mathbb{D}(P_{Z_b^r, K_1^{(b)}, K_2^{(b)}} || Q_{K_1^{(b)}} Q_{K_2^{(b)}} Q_Z^{\otimes r}) \xrightarrow{r \to \infty} 0$ if:

$$\rho_1 + \rho_2 - \rho_{k1} - \rho_{k2} > I(X_1, X_2; Z) - H(Z_1, Z_2 | X_1, X_2, Z) \tag{4.102}$$

$$\rho_2 - \rho_{k2} > I(X_2; Z) - H(Z_1, Z_2 | X_2, Z) \tag{4.103}$$

$$\rho_1 - \rho_{k1} > I(X_1; Z) - H(Z_1, Z_2 | X_1, Z) \tag{4.104}$$

$$\rho_1 + \rho_2 - \rho_{k2} > I(X_1, X_2; Z) - H(Z_2 | X_1, X_2, Z) \tag{4.105}$$

$$\rho_1 + \rho_2 - \rho_{k1} > I(X_1, X_2; Z) - H(Z_1 | X_1, X_2, Z) \tag{4.106}$$

$$H(Z_1, Z_2, Z) > H(Z) \tag{4.107}$$

$$\rho_1 + \rho_2 > I(X_1, X_2; Z) \tag{4.108}$$

$$\rho_2 - \rho_{k2} > I(X_2; Z) - H(Z_2 | X_2, Z) \tag{4.109}$$

$$\rho_2 > I(X_2; Z) - H(Z_1 | X_2, Z) \tag{4.110}$$

$$\rho_1 > I(X_1; Z) - H(Z_2 | X_1, Z) \tag{4.111}$$

$$\rho_1 - \rho_{k1} > I(X_1; Z) - H(Z_1 | X_1, Z) \tag{4.112}$$

$$H(Z_2, Z) > H(Z) \tag{4.113}$$

$$H(Z_1, Z) > H(Z) \tag{4.114}$$

$$\rho_2 > I(X_2; Z) \tag{4.115}$$

$$\rho_1 > I(X_1; Z) \tag{4.116}$$

Defining the effective rates of new randomness at each encoder as $R_1 \triangleq \rho_1 - \rho_{k1}$ and $R_2 \triangleq \rho_2 - \rho_{k2}$ and performing Fourier-Motzkin elimination completes the proof.

CHAPTER 5

CONCLUSION

This dissertation develops inner and outer bounds for the resolvability rates of the multiple-access channel with several cooperation strategies: (i) degraded message sets, (ii) a common message, (iii) conferencing, (iv) cribbing, (v) feedback, and (vi) generalized feedback. For the multiple access channel with cribbing, we investigate the following cases: (a) one-sided strictly-causal cribbing, (b) one-sided causal cribbing, (c) one-sided non-causal cribbing and (d) two-sided strictly-causal cribbing.

The derived inner and outer bounds are tight for the cases of the multiple access channel with degraded message sets, a common message, conferencing, one-sided causal cribbing, one-sided non-causal cribbing, and feedback.

The key insights of this dissertation are as follows. First, feedback does not improve the resolvability of the MAC, which we show by providing a converse that is tight against the results of [7]. Resolvability may be improved by the other cooperation schemes. Second, the encoding schemes involve the hiding of the encoder cooperation, so that the dependencies created by cooperation are undetectable at the channel output. This is made possible because the cooperation mechanism creates an effective wiretap channel and allows the exchange of secret information. In the context of channel resolvability, this secret information plays the role of randomness that can be reused for cooperation without impacting the desired output approximation. Third, we develop two achievability approaches investigating the roles of decoding and randomness extraction. The first approach is constructed by using decode-and-forward strategy, where each encoder decodes the other encoder's message. The second approach is constructed by a randomness extraction mechanism which can be motivated by a case when each encoder's observation is very noisy, allowing cooperation without decoding.

Then, deriving secrecy from channel resolvability, achievable strong secrecy rates were derived for MAC wiretap channel for all the previously mentioned cooperation schemes.

REFERENCES

[1] A. Wyner, “The wire-tap channel,” *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[2] ——, “The common information of two dependent random variables,” *IEEE Trans. Inform. Theory*, vol. 21, no. 2, pp. 163–179, Mar. 1975.

[3] T. S. Han and S. Verdú, “Approximation theory of output statistics,” *IEEE Trans. Inform. Theory*, vol. 39, no. 3, pp. 752–772, May 1993.

[4] P. Cuff, “Distributed channel synthesis,” *IEEE Trans. Inform. Theory*, vol. 59, no. 11, pp. 7071–7096, Nov. 2013.

[5] J. Hou and G. Kramer, “Informational divergence approximations to product distributions,” in *13th Canadian Workshop on Information Theory*, Toronto, ON, Canada, Jun. 2013, pp. 76–81.

[6] Y. Steinberg, “Resolvability theory for the multiple-access channel,” *IEEE Trans. Inform. Theory*, vol. 44, no. 2, pp. 472–487, Mar. 1998.

[7] M. Frey, I. Bjelaković, and S. Stańczak, “The MAC resolvability region, semantic security and its operational implications,” arXiv preprint: 1710.02342, 2017.

[8] M. H. Yassaee and M. R. Aref, “Multiple access wiretap channels with strong secrecy,” in *IEEE Information Theory Workshop (ITW)*, 2010, pp. 1–5.

[9] 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.

[10] T. Cover and C. Leung, “An achievable rate region for the multiple-access channel with feedback,” *IEEE Transactions on Information Theory*, vol. 27, no. 3, pp. 292–298, 1981.

[11] F. Willems, “The feedback capacity region of a class of discrete memoryless multiple access channels (corresp.),” *IEEE Trans. Inform. Theory*, vol. 28, no. 1, pp. 93–95, 1982.

[12] M. Bloch, “Channel intrinsic randomness,” in *IEEE International Symposium on Information Theory (ISIT)*, Jun. 2010, pp. 2607–2611.

[13] I. Csiszár, “Almost independence and secrecy capacity,” in *Problems of Information Transmission*, vol. 32, no. 1, 1996, p. 40–47.

[14] U. Maurer and S. Wolf, “Information-theoretic key agreement: From weak to strong secrecy for free,” in *Advances in Cryptology — EUROCRYPT 2000*, B. Preneel, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 351–368.

[15] O. Simeone and A. Yener, "The cognitive multiple access wire-tap channel," in *43rd Annual Conference on Information Sciences and Systems (CISS)*, Mar. 2009, pp. 158–163.

[16] P. Xu, Z. Ding, and X. Dai, "Rate regions for multiple access channel with conference and secrecy constraints," *IEEE Trans. Inf. Forensics Security.*, vol. 8, no. 12, pp. 1961–1974, Dec. 2013.

[17] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Multiple access channels with generalized feedback and confidential messages," in *IEEE Information Theory Workshop (ITW)*. IEEE, 2007, pp. 608–613.

[18] Z. H. Awan, A. Zaidi, and L. Vandendorpe, "Multiaccess channel with partially cooperating encoders and security constraints," *IEEE Trans. Inf. Forensics Security.*, vol. 8, no. 7, pp. 1243–1254, Jul. 2013.

[19] S. I. Bross, "The discrete memoryless interference channel with one-sided generalized feedback and secrecy," *IEEE Trans. Inform. Theory*, vol. 63, no. 5, pp. 2710–2725, May 2017.

[20] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai, and S. Verdú, "Capacity of cognitive interference channels with and without secrecy," *IEEE Trans. Inform. Theory*, vol. 55, no. 2, pp. 604–619, Feb. 2009.

[21] R. K. Farsani and R. Ebrahimpour, "Capacity theorems for the cognitive radio channel with confidential messages," in *IEEE International Symposium on Information Theory (ISIT)*, Jun. 2014, pp. 1416–1420.

[22] L. Lai and H. E. Gamal, "The relay eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inform. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[23] M. Yuksel and E. Erkip, "The relay channel with a wire-tapper," in *41st Annual Conference on Information Sciences and Systems*, Mar. 2007, pp. 13–18.

[24] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," *IEEE Trans. Inform. Theory*, vol. 57, no. 1, pp. 137–155, Jan. 2011.

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

[26] Z. Goldfeld, G. Kramer, H. H. Permuter, and P. Cuff, "Strong secrecy for cooperative broadcast channels," *IEEE Trans. Inform. Theory*, vol. 63, no. 1, pp. 469–495, Jan. 2017.

[27] S. Watanabe and Y. Oohama, “Cognitive interference channels with confidential messages under randomness constraint,” *IEEE Trans. Inform. Theory*, vol. 60, no. 12, pp. 7698–7707, Dec. 2014.

[28] R. A. Chou and A. Yener, “Polar coding for the multiple access wiretap channel via rate-splitting and cooperative jamming,” in *IEEE International Symposium on Information Theory (ISIT)*, Jul. 2016, pp. 983–987.

[29] I. Sason and S. Verdú, “f -divergence inequalities,” *IEEE Trans. Inform. Theory*, vol. 62, no. 11, pp. 5973–6006, Nov. 2016.

[30] N. Helal, M. Bloch, and A. Nosratinia, “Multiple-access channel resolvability with cribbing,” in *IEEE International Symposium on Information Theory (ISIT)*, Jun. 2018, pp. 2052–2056.

[31] ——, “Cooperative resolvability and secrecy in the cribbing multiple-access channel,” arXiv preprint: 1811.11649, 2018.

[32] F. Willems and E. van der Meulen, “The discrete memoryless multiple-access channel with cribbing encoders,” *IEEE Trans. Inform. Theory*, vol. 31, no. 3, pp. 313–327, May 1985.

[33] M. R. Bloch and J. Kliewer, “Strong coordination over a line network,” in *IEEE International Symposium on Information Theory (ISIT)*, Istanbul, Turkey, Jul. 2013, pp. 2319–2323.

[34] T. Cover and A. Gamal, “Capacity theorems for the relay channel,” *IEEE Trans. Inform. Theory*, vol. 25, no. 5, pp. 572–584, Sep. 1979.

[35] H. Asnani and H. H. Permuter, “Multiple-access channel with partial and controlled cribbing encoders,” *IEEE Trans. Inform. Theory*, vol. 59, no. 4, pp. 2252–2266, Apr. 2013.

[36] N. Helal, M. Bloch, and A. Nosratinia, “Channel resolvability with a full-duplex decode-and-forward relay,” in *IEEE Information Theory Workshop (ITW)*, Aug. 2019.

BIOGRAPHICAL SKETCH

Noha Helal received her BS degree in electrical engineering from the Faculty of Engineering, Alexandria University, Alexandria, Egypt, and her MS degree in electrical engineering from the Nile University, Giza, Egypt. She is currently working toward her PhD in electrical engineering at The University of Texas at Dallas, Richardson, TX, USA. Her research interests include information theory and its applications in physical layer security. She received the Erik Jonsson Graduate Fellowship in 2014 from The University of Texas at Dallas.

CURRICULUM VITAE

Noha Helal

Summary

An electrical engineer with 7+ years of combined research and industrial experience in information theory and wireless communications.

Key Skills

- Solid background in mathematics: Information theory, Statistics and Random Processes.
- Theoretical performance analysis of communication systems.
- Technical Skills: Python, MATLAB, C, NS-2 and WARPLab.

Professional Experience

The University of Texas at Dallas (UTD), Dallas, Texas
Research Assistant/ Teaching Assistant ***S*****eptember 2014 - March 2020**

- Conducting research on Information theory and its applications in physical layer security.
- Understanding and analyzing the role of cooperation in improving the system security.
- Teaching assistant to multiple undergraduate courses.

Nile University with Cooperation from Qatar University
Research Assistant ***September 2010-July 2012***

- Analyzing the performance of wireless networks in presence of cooperation.

Orascom Telecom, Cairo, Egypt
IT engineer intern ***June - August 2007***

- Implementing and troubleshooting all technology interfaces in a new construction.

Publications

Journals

1. **N. Helal**, M. Bloch and A. Nosratinia, "Resolvability and Secrecy of the Multiple-Access Channel with Two-Sided Cooperation," In preparation.

2. K. S. Subramani, **N. Helal**, A. Antonopoulos, A. Nosratinia and Y. Makris,"Amplitude-Modulating Analog/RF Hardware Trojans in Wireless Networks: Risks and Remedies," accepted for IEEE Transactions on Information Forensics and Security.

3. **N. Helal**, M. Bloch and A. Nosratinia, "Cooperative Resolvability and Secrecy in the Cribbing Multiple-Access Channel," accepted for IEEE Transactions on Information Theory.

Conference Papers

1. **N. Helal**, M. Bloch and A. Nosratinia, "Resolvability of the Multiple Access Channel with Two-Sided Cooperation," IEEE International Symposium on Information Theory (ISIT), Los Angelos, CA, Jun. 2020.

2. **N. Helal**, M. Bloch and A. Nosratinia, "Channel Resolvability with a Full-Duplex Decode-and-Forward Relay," IEEE Information Theory Workshop (ITW), Visby, Gotland, Sweden, Aug. 2019.

3. **N. Helal**, M. Bloch and A. Nosratinia, "Multiple-Access Channel Resolvability with Cribbing," IEEE International Symposium on Information Theory (ISIT), Vail, CO, Jun. 2018, pp. 2052-2056.

4. **N. Helal** and A. Nosratinia, "Multiple access wiretap channel with cribbing," IEEE International Symposium on Information Theory (ISIT), Aachen, Jun. 2017, pp. 739-743.

5. **N. Helal**, K. G. Seddik, A. El-Keyi and T. El Batt, "A feedback-based access scheme for cognitive-relaying networks," IEEE Wireless Communications and Networking Conference (WCNC), Shanghai, April 2012, pp. 1287-1292.

Education

The University of Texas at Dallas, Dallas, Tx
P.hD. in Electrical Engineering, ***August 2014 - Current***
Advisor: Prof. Aria Nosratinia.
Research: Physical layer security in the multiple access channel with cooperation

Nile University, Egypt
M.Sc. in Electrical Engineering, ***September 2010 - July 2012***
Advisor: Karim Seddik.
Research: Wireless communication with focus on cooperative relaying in cognitive radio networks

Alexandria University, Alexandria, Egypt
B.Sc. in Electrical Engineering, ***September 2005 - July 2010***