Codes and Game Theory for Key Agreement with Untrusted Participants

Nebojsa Milosavljevic

Electrical Engineering and Computer Sciences
University of California at Berkeley

Technical Report No. UCB/EECS-2011-6
http://www.eecs.berkeley.edu/Pubs/TechRpts/2011/EECS-2011-6.html

January 22, 2011

Codes and Game Theory for Key Agreement with Untrusted Participants

Nebojsa Milosavljevic

December 17, 2010

Abstract

In this work we study the problem of confidential communication when different resources of randomness are available.

We start with the relay channel where source observations are available at each terminal. We study the scenario where the transmitter (Alice) sends a private message to the destination (Bob), which is confidential to the relay (Eve). Alice and Bob also want to agree on a secret key that is protected from Eve. We propose an achievable scheme and show that if the channel is degraded or reversely degraded, the secret message-secret key sum rate is optimal.

Then, we consider a scenario where three terminals, Alice, Bob and Charlie, observe memoryless correlated observations. Alice wants to agree with Bob on a key that is secured from Charlie. At the same time Alice wants to agree with Charlie on a key that is secured from Bob. We further assume that Alice has no knowledge on how the distributed sources are correlated, and that she is the one who constructs the codebooks for the key agreement. In order to construct the codebooks which would achieve a desired level of secrecy, Alice request some information from Bob and Charlie about their observations. Since Bob and Charlie act like eavesdroppers to each other, they may not be completely honest about what they observe. Therefore, their reports are based on some objective that is a function of the key rate and the amount of information they can learn about the other user's key, called the leakage rate. We approach this problem from a game-theoretic point of view. For a class of Bob and Charlie's objective functions that are linear in the key rate and the leakage rate, we characterize a Nash equilibrium. Then, we propose a strategy that Alice can apply in order to ensure that Bob and Charlie's honest reporting is always a Nash equilibrium. Finally, for the binary erasure source distributions we extend this concept to the multiple terminal case.

Contents

1 Introduction **5**

1.1 Overview of Thesis . . . 7

2 Secure Communication using an Untrusted Relay **8**

2.1 Introduction . . . 8

2.2 Problem Setup . . . 10

2.3 Results . . . 12

2.4 An Outer Bound . . . 17

2.5 Gaussian Relay Channel . . . 18

2.5.1 Reversely Degraded Gaussian Channel . . . 18

2.5.2 Degraded Gaussian Relay Channel . . . 19

3 The Role of Game Theory in Key Agreement Over a Public Channel **21**

3.1 Introduction . . . 21

3.2 Problem Statement . . . 24

3.3 An Achievable Key Agreement Scheme . . . 26

3.4 Binary Erasure Distribution . . . 28

3.4.1 Game 1 . . . 28

3.4.2 Game 2 . . . 30

3.5 Extension to More General Case . . . 33

3.5.1 Game 1 . . . 33

3.5.2 Game 2 . . . 35

3.6 Binary Symmetric Distribution . . . 38

3.6.1 Game 1 . . . 38

3.6.2 Game 2 . . . 38

3.7 Privacy Considerations . . . 41

3.7.1 Game 1 41

3.7.2 Game 2 42

3.7.3 Binary Erasure Distribution 43

3.8 Multiterminal Key Agreement 44

3.8.1 Binary Erasure Example 44

3.8.2 Simulations 48

3.8.3 Generalizations of Proposition 3.1 for arbitrary number of users 49

3.8.4 Game 2 52

4 Conclusions **53**

A Appendix 1 **54**

B Appendix 2 **63**

List of Figures

2.1 Relay channel model with correlated observations. Alice Bob and Eve have access to a memoryless source observations S_A^n, S_B^n and S_E^n. Alice uses the relay channel and the observed sequence S_A^n to send a private message M to Bob and to agree with him on a key K. Both M and K are perfectly protected from Eve. 10

2.2 Relay channel model with confidential and public messages. Alice uses the relay channel to transmit the secret message M_S to Bob that is perfectly protected from Eve. She also sends to Bob the public message M_P that is not protected from Eve . 12

2.3 Reversely degraded relay channel: (R_K, R_M) rate region. $P_A = P_E = 10$, $N_2 = 1$, $N_1 = 2$, $N_A = 1$, $N_B = 1$, $N_E \to \infty$. The figure shows the secret key-secret message sum rate optimality. 19

2.4 Degraded relay channel: (R_K, R_M) rate region. $P_A = P_E = 10$, $N_2 = 2$, $N_1 = 1$, $N_A = 1$, $N_B = 1$, $N_E \to \infty$. The figure shows the secret key-secret message sum rate optimality. 20

3.1 Key agreement over a noiseless public channel with unknown joint statistics. Alice agrees with Bob on a key K_{AB} that is perfectly protected from Charlie. Alice and Charlie agree on a key K_{AC} that is perfectly protected from Bob. To construct the codebooks for the key agreement Alice requests from Bob and Charlie to send her some sufficient information about their observations. Here we model these reports by having Bob and Charlie select discrete memoryless channels $P_{Y_r|Y}$ and $P_{Z_r|Z}$, respectively, and send sufficient information about Y_r and Z_r over the public channel. 22

3.2 Utility matrix: In each box, the left entry is Charlie's utility, and the right entry is Bob's utility. 30

3.3 Utility matrix when $\epsilon \leq \frac{\lambda}{\lambda+1}$, $\delta > \frac{\lambda}{\lambda+1}$. $\Gamma = \delta(\frac{1}{\lambda+1} - \alpha) + \lambda(\frac{\lambda}{\lambda+1} + \alpha - \epsilon)(1-\delta)$. Bob and Charlie have no incentive to unilaterally change their strategies and move from the upper left box of the utility matrix. 31

3.4 Utility matrix when $\epsilon > \frac{\lambda}{\lambda+1}$, $\delta \leq \frac{\lambda}{\lambda+1}$. $\Delta = \epsilon(\frac{1}{\lambda+1} - \alpha) + \lambda(\frac{\lambda}{\lambda+1} + \alpha - \delta)(1-\epsilon)$. Bob and Charlie have no incentive to unilaterally change their strategies and move from the upper left box of the utility matrix. 31

3.5 Utility matrix when $\epsilon \leq \frac{\lambda}{\lambda+1}$, $\delta \leq \frac{\lambda}{\lambda+1}$. $\Pi = (\frac{1}{\lambda+1} - \alpha)(\lambda(1-\epsilon) + \alpha(\lambda+1))$, $\Sigma = (\frac{1}{\lambda+1} - \alpha)(\lambda(1-\delta) + \alpha(\lambda+1))$. Bob and Charlie have no incentive to unilaterally change their strategies and move from the upper left box of the utility matrix. . . . 32

3.6 Binary erasure distribution: Region where honest reporting by all players is a Nash equilibrium. The figure shows the case $\lambda = \frac{1}{2}$ 49

3.7 Lower boundary of the region in Figure 3.6 shows that $\epsilon_i > \frac{\lambda}{\lambda+1}$ for $i = 1, 2, 3$ and $\lambda = \frac{1}{2}$ belongs to the region where honest reporting by all players is a Nash equilibrium. 50

3.8 Upper boundary of the region in Figure 3.6 shows that $\epsilon_i > \frac{\lambda}{\lambda+1}$ for $i = 1, 2$ and $\lambda = \frac{1}{2}$ belongs to the region where honest reporting by all players is a Nash equilibrium. 51

Chapter 1

Introduction

The fact that channel randomness can be used as a resource for secret communication was first observed by Wyner in [1]. He considered a point to point communication setup where Alice wants to send a secret message to Bob that is perfectly concealed from an eavesdropper (Eve) who observes some noisy version of that transmission. A perfectly secure message can be sent across such a channel as long as the channel from Alice to Bob is less noisy than the channel from Alice to Eve. Subsequent work in this area considered different channel problems: the broadcast channel [2], the multiple access channel [3], the relay channel [4], [5], [6], [7], [8], a broadcast channel with independent messages [9], the interference channel [9] etc.

On the other hand, correlated source observations can be viewed as another resource for secret communication. In the simplest model, two terminals, Alice and Bob, observe correlated sources, and want to agree on a secret key that is protected from an eavesdropper (Eve) who observes public communication between them. It is shown in [2] that using a Slepian-Wolf coding scheme [10], one can achieve the optimal key rate. This model was extended to the case when Eve, in addition to having access to the public communication between Alice and Bob, has access to observations that are correlated with Alice and Bob's observations. Csisz*á*r and Narayan proposed a coding scheme that is based on Slepian-Wolf coding and Wyner's wiretap channel code.

Further extensions of this model considered a multi-terminal key agreement, where a subset of the terminals, observing distinct components of a discrete memoryless multiple source (DMMS), want to agree on a key that is perfectly protected from an eavesdropper. To that end, terminals are allowed to use a public noiseless channel that can be observed by all terminals including the eavesdropper. These problems have been studied in [11] and [12].

The question that arises from the discussion is: what if we have both resources of randomness: channel and correlated source observations? In this type of problems, terminals have access to discrete memoryless source observations, and they communicate through a noisy channel. The goal is to find a tradeoff between the key rate and the secret message rate. For the special case of the broadcast channel, this problem was studied in [13] and [14]. Under some special conditions it is shown that a separation strategy for source and channel coding is optimal. In [15] and Chapter 2, we study this problem for the relay channel. We assumed that the relay node (Eve) is curious about the private communication between Alice to Bob, but not malicious in terms of altering the communication protocol. Under some special channel and source distributions we determine the optimal tradeoff between secret message-secret key sum rate.

The problem with all security related problems is that the legitimate users have to know how powerful the eavesdropper is. Based on that information, they know how much of their communication is protected from the eavesdropper. Let us assume that two remote communication nodes, say Alice and Bob, want to agree on a key by exploiting correlated observations at each node. They know that an eavesdropper (Eve) is present, but they do not know her eavesdropping capabilities or even how Eve, Alice and Bob's observations are correlated. What can Alice and Bob do to ensure some level of security? They can simply ask Eve to report how powerful she really is. But, Eve has no incentive to do so unless she gets something in return. But this means that Eve has to be a part of the system. In this thesis, we therefore consider a "symmetric" version of the classical eavesdropping problem. To this end we modify our problem by assuming that there are three legitimate points of communications: Alice, Bob and Charlie. Alice wants to agree on a key with Bob that is protected from Charlie. At the same time, she wants to agree on a key with Charlie that is protected from Bob. In this scenario we essentially have two eavesdroppers (Bob and Charlie). We assume that both Bob's and Charlie's capabilities are unknown to Alice, and it is up to them to report that to her. If their goal is to maximize the amount of information they can eavesdrop, then they will report nothing, just like in the previous scenario with the passive eavesdropper. The problem with this decision is that Bob and Charlie will end up with no secure key shared between them and Alice. On the other hand, if they honestly report their capabilities, they will use all of their resources to agree with Alice on the keys, and will end up with no information about the other user's key. Therefore, we approach this problem from a game-theoretic point of view, where Bob and Charlie base their reports on some utility functions. In [16] and Chapter 3, for a special class of the utility functions, we characterized a stable solution, also known as Nash equilibrium.

1.1 Overview of Thesis

Secure Communication using an Untrusted Relay

In Chapter 2 we investigate the problem where the transmitter (Alice) sends a private message to the destination (Bob), which is confidential from the relay (Eve). Alice, Bob and Eve have access to discrete memoryless source observations, which Alice and Bob can use to boost their security level. Alice and Bob also want to agree on a secret key that is a function of Alice's observations. We propose an achievable scheme based on a separation strategy [13], and Cover and El Gamal's scheme (see *Theorem 7* in [17]). We also show that if the channel is degraded or reversely degraded [17], the secret message-secret key sum rate is optimal.

The Role of Game Theory in Key Agreement Over a Public Channel

In Chapter 3 we study the problem when three users, Alice, Bob and Charlie, observe the distinct components of a discrete memoryless multiple source. For the purposes of key generation, Alice can communicate with Bob and Charlie over a public channel. Alice and Bob (resp. Alice and Charlie) want to agree on a key which is concealed from Charlie (resp. Bob). We assume that the joint distribution P_{XYZ} is unknown to Alice, and that her goal is to learn it. To that end she requests from Bob and Charlie to send her sufficient information about their observations over the public channel. In return, Alice constructs the codebooks for the key agreements. We also assume that Bob and Charlie, besides agreeing with Alice on the keys, want to learn as much as possible about the other user's key: we call this quantity the *leakage*. We model the reports by having Bob and Charlie select discrete memoryless channels and passing their true observations through them. We approach this problem from a game-theoretic point of view. For a class of Bob and Charlie's objective functions which are linear in the key rate and the leakage rate, we characterize a Nash equilibrium. Also, we propose a strategy that Alice can apply in order to ensure that Bob and Charlie's honest reporting is a Nash equilibrium.

Chapter 2

Secure Communication using an Untrusted Relay

2.1 Introduction

The problem of secret communication in relay channels was first studied by Oohama in [4]. He considered the model where the relay is an eavesdropper, while at the same time it helps transmission of the message to destination. He proposed an achievable scheme that is based on a partial decode and forward (PDF) strategy [17], and an outer bound which coincides with the inner bound in the case of a reversely degraded relay channel (defined in [17]). Yener and He in [5] suggested a new achievable strategy that is based on compress and forward [17], and in [6] proposed an outer bound for the relay channel with orthogonal components. Secrecy in relay channels with external eavesdropper is observed in [7] and [8]. In their recent work, Ekrem and Ulukus [18] studied relay broadcast channels where the relay and the receiver see each other as eavesdroppers.

The fact that dependent source observations at the terminals can be used as a resource for generating secret key (a uniform random variable shared by Alice and Bob which is oblivious to Eve) was recognized by Ahlswede and Csiszár [19] and Maurer [20]. In [21], the problem of secret key generation with a helper was studied where it is assumed that a noiseless rate constrained channel is available from Alice to Bob, while Eve can overhear any communication across that channel. The scenario where both secret communication and secret key agreement are desired in the presence of noisy one-way broadcast channel and correlated sources at each terminal, was studied by Prabhakaran, Eswaran and Ramchandran in [13].

We propose an achievable scheme based on a separation strategy [13], and Cover and El Gamal's scheme (see *Theorem 7* in [17]). We also show that if the channel is degraded or reversely degraded [17], the secret message-secret key sum rate is optimal.

2.2 Problem Setup

Notation: Random variables are denoted by upper-case letters, their realizations by lower-case letters, and the alphabets over which they take values by calligraphic letters. A vector $(X_1, X_2, ..., X_n)$ will be denoted as X^n.

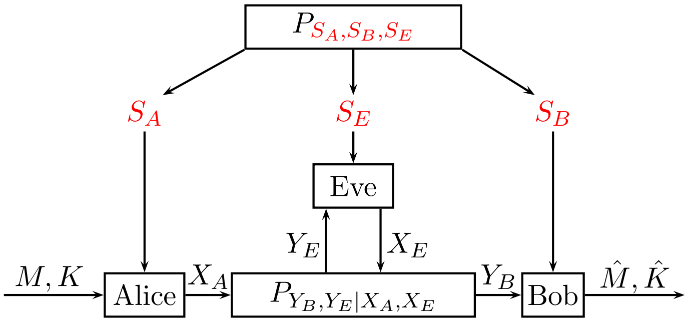

Figure 2.1: Relay channel model with correlated observations. Alice Bob and Eve have access to a memoryless source observations S_A^n, S_B^n and S_E^n. Alice uses the relay channel and the observed sequence S_A^n to send a private message M to Bob and to agree with him on a key K. Both M and K are perfectly protected from Eve.

The relay channel model (see Figure 2.1) consists of a message set $\mathcal{M}$, two input alphabets $\mathcal{X}_A$ and $\mathcal{X}_E$, and two output alphabets $\mathcal{Y}_E$ and $\mathcal{Y}_B$. The channel is assumed to be discrete memoryless with transition probability distribution $P_{Y_E,Y_B|X_A,X_E}$, where $X_A \in \mathcal{X}_A$, $X_E \in \mathcal{X}_E$, $Y_E \in \mathcal{Y}_E$ and $Y_B \in \mathcal{Y}_B$. We assume that the source observations S_A^n, S_B^n and S_E^n are memoryless, independent of the channel and have joint distribution p_{S_A,S_B,S_E} over the alphabet $\mathcal{S}_A \times \mathcal{S}_B \times \mathcal{S}_E$. The number of source observations is the same as the number of channel uses available. Let M and K be uniformly distributed random variables taking values in the alphabets $\mathcal{M} = \{1, ..., 2^{nR_M}\}$ and $k \in \mathcal{K} = \{1, ..., 2^{nR_K}\}$ respectively. The random variable M is a private message sent only to the receiver that contains information that needs to be kept secret from the relay. Suppose the parties make n observations of their sources.

Based on her side information S_A^n, Alice creates a secret key $K = g(S_A^n)$ for some g which has to satisfy the following properties

- Key K has to be ϵ-recoverable from (S_B^n, Y_B^n), meaning that there exists a function f such that $Pr(K \neq f(S_B^n, Y_B^n)) < \epsilon$.
- Both key K and message M have to satisfy secrecy condition:

$$\frac{1}{n} I(M, K; Y_B^n, S_E^n) < \epsilon$$

- K also has to satisfy uniformity condition:

$$\frac{1}{n}H(K) \geq \log|\mathcal{K}| - \epsilon$$

We say that the key K is ϵ-secret if it satisfies all these properties above. We define $(R_{K,\epsilon}, R_{M,\epsilon})$ to be an ϵ-achievable rate pair if there exists an ϵ-secret key K such that $\frac{1}{n}H(K) = R_{K,\epsilon}$, and the message M that is ϵ-recoverable from (Y_B^n, S_B^n) such that $\frac{1}{n}H(M) = R_{M,\epsilon}$. A rate pair (R_M, R_K) is said to be achievable if there is a sequence of ϵ_n such that $(R_{M,\epsilon_n}, R_{K,\epsilon_n})$ are ϵ_n-achievable rate pairs, and as $n \to \infty$,

$$\epsilon_n \to 0, \qquad R_{M,\epsilon_n} \to R_M, \qquad R_{K,\epsilon_n} \to R_K$$

2.3 Results

In order to provide an achievable scheme for the problem above, we first consider the scenario without correlated observations, where besides the secret message, here denoted by M_S, we have a public message M_P which can also be decoded by Bob, but it is not protected from Eve (see Figure 2.2). The Coding strategy is based on the Cover and El Gamal's scheme (see *Theorem 7* in [17]), random binning [1], and channel prefixing [2].

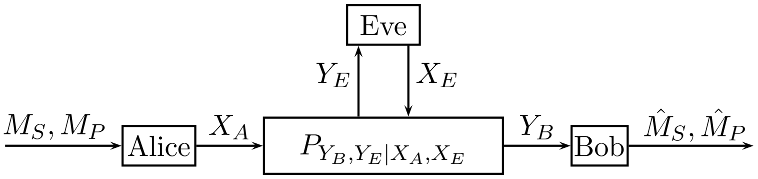

Figure 2.2: Relay channel model with confidential and public messages. Alice uses the relay channel to transmit the secret message M_S to Bob that is perfectly protected from Eve. She also sends to Bob the public message M_P that is not protected from Eve

Definition 2.1. An $(2^{nR_S}, 2^{nR_P}, n)$ code for the relay channel $(\mathcal{X}_A, \mathcal{X}_E, P_{Y_E,Y_B|X_A,X_E}, \mathcal{Y}_E, \mathcal{Y}_B)$ with confidential messages consists of the following

1. Sets of integers $\mathcal{M}_S = \{1, 2, ..., 2^{nR_S}\}$ and $\mathcal{M}_P = \{1, 2, ..., 2^{nR_P}\}$
2. An encoding function $X_A^n : \mathcal{M}_S \times \mathcal{M}_P \to \mathcal{X}_A^n$ and a set of relay functions $\{f_i\}_{i=1}^n$ such that

$$X_{2i} = f_i(Y_{E,1}, Y_{E,2}, ..., Y_{E,i-1}), \quad 1 \leq i \leq n$$

3. Decoding functions

$$g_1 : \mathcal{Y}_B \to \mathcal{M}_S$$
$$g_2 : \mathcal{Y}_B \to \mathcal{M}_P$$

Let M_S and M_P be uniformly distributed random variables taking values in the alphabets $\mathcal{M}_S$ and $\mathcal{M}_P$, respectively, then the rate pair (R_S, R_P) is said to be achievable if

$$\begin{aligned}
&Pr\{M_S \neq g_1(Y_B^n)\} \leq \epsilon \\
&Pr\{M_P \neq g_2(Y_B^n)\} \leq \epsilon \\
&\frac{1}{n}H(M_S) \geq R_S - \epsilon \\
&\frac{1}{n}H(M_P) \geq R_P - \epsilon \\
&\frac{1}{n}I(M_S; Y_E^n, X_E^n) \leq 4\epsilon
\end{aligned} \tag{2.1}$$

where $\lim_{n\to\infty} \epsilon = 0$.

We define $\tilde{\mathcal{R}}_c$ to be the set of all achievable rate pairs (R_S, R_P).

Let $\mathcal{P}_c$ denote the set of all joint distributions of random variables V, U, V_A, X_A, X_E, Y_E, $\hat{Y}_2$, Y_B satisfying

$$P_{V,U,V_A,X_A,X_E,Y_E,\hat{Y}_E,Y_B} = P_V P_{U|V} P_{V_A|U} P_{X_A|V_A} P_{X_E|V} P_{Y_E,Y_B|X_A,X_E} P_{\hat{Y}_E|X_E,Y_E,U}, \tag{2.2}$$

For $p \in \mathcal{P}_c$, let $\mathcal{R}_c(p)$ be the set of all non-negative rate pairs (R_S, R_P) which satisfy the following inequalities:

$$R_S \leq \{I(V_A; Y_B, \hat{Y}_2 | X_E, U) - I(V_A; Y_E | X_E, U)\}_+$$
$$R_S + R_P \leq \min\{I(V; Y_B) + I(U; Y_B | X_E, V), I(U; Y_E | X_E, V)\} + I(V_A; Y_B, \hat{Y}_E | X_E, U)$$

subject to constraint

$$I(X_E; Y_B | V) \geq I(\hat{Y}_2; Y_E | Y_B, X_E, U). \tag{2.3}$$

Theorem 2.1.

$$\tilde{\mathcal{R}}_c \supseteq \bigcup_{p \in \mathcal{P}_c} \mathcal{R}_c(p).$$

A complete proof of theorem 2.1 is provided in the Appendix A.

Remark 2.1. If we suppress the common message by setting $V = 0$, $U = 0$, the channel coding strategy reduces to compress and forward [5]

$$R_S \leq \{I(V_A; Y_B, \hat{Y}_E | X_E) - I(V_A; Y_E | X_E)\}_+$$

subject to

$$I(\hat{Y}_2; Y_E | X_E, Y_B) \leq I(X_E; Y_B), \tag{2.4}$$

for any joint distribution of the form

$$P_{V_A} P_{X_A|V_A} P_{X_E} P_{Y_E,Y_B|X_A,X_E} P_{\hat{Y}_E|X_E,Y_E} \tag{2.5}$$

Remark 2.2. If we disable cooperation between the relay and the destination by setting $V = 0$, $X_E = 0$, $\hat{Y}_E = 0$, the channel model reduces to the broadcast channel with the confidential messages [2].

$$R_S + R_P \leq I(V_A; Y_B | U) + \min\{I(U; Y_B), I(U; Y_E)\}$$
$$R_S \leq \{I(V_A; Y_B | U) - I(V_A; Y_E | U)\}_+, \tag{2.6}$$

for any joint distribution

$$P_U P_{V_A|U} P_{X_A|V_A} P_{Y_E,Y_B|X_A}, \tag{2.7}$$

which implies that the Markov chain $U - V_A - X_A - (Y_E, Y_B)$ holds.

Remark 2.3. By setting $\hat{Y}_2 = 0$ and $V = X_E$ we obtain Oohama's [4] partial decode and forward strategy when stochastic encoder is used.

$$\begin{aligned} R_S + R_P &\leq I(V_A; Y_B|U, X_E) + \min\{I(U, X_E), I(U; Y_E|X_E)\} \\ R_S &\leq \{I(V_A; Y_B|U, X_E) - I(V_A; Y_E|X_E, U)\}_+, \end{aligned}$$

for any joint distribution of the form

$$P_{X_E} P_{U|X_E} P_{V_A|U} P_{X_A|V_A} P_{Y_E,Y_B|X_A,X_E}. \tag{2.8}$$

Going back to our original problem, an achievable scheme is based on a separation strategy [13] which converts the relay channel into a public and private bit pipe. The public bit pipe delivers bits reliably to both Alice and Eve, while bits sent over the private bit pipe are reliably delivered to Bob and are perfectly secret form Eve. Then, the sources are used to generate a secret key shared by Alice and Bob, part of which is used to increase the secret message rate by one time padding the message sent over the public bit pipe with a key of equal size. We define $\tilde{\mathcal{R}}$ to be the set of all achievable rate pairs (R_M, R_K).

Let $\mathcal{P}$ denote the set of all joint distributions of random variables W, V, U, V_A, X_A, X_E, Y_E, $\hat{Y}_E$, Y_B, S_A, S_B, S_E satisfying

$$P_{V,U,V_A,X_A,X_E,Y_E\hat{Y}_E,Y_B} = P_V P_{U|V} P_{V_A|U} P_{X_A|V_A} P_{X_E|V} P_{Y_E,Y_B|X_A,X_E} P_{\hat{Y}_E|X_E,Y_E,U}, \tag{2.9}$$

$$P_{W,S_A,S_B,S_E} = P_W P_{S_A|W} P_{S_B,S_E|S_A} \tag{2.10}$$

such that W and (V, V_A) are independent.

For $p \in \mathcal{P}$, let $\mathcal{R}(p)$ be the set of all non-negative rate pairs (R_M, R_K) which satisfy the following inequalities:

$$\begin{aligned} R_K + R_M \leq\ & \{I(V_A; Y_B, \hat{Y}_E|X_E, U) - I(V_A; Y_E|X_E, U)\}_+ \\ & + \{I(W; S_B) - I(W; S_E)\}_+ \qquad (2.11) \\ R_M \leq\ & I(V_A; Y_B, \hat{Y}_E|X_E, U) \\ & + \min\{I(V; Y_B) + I(U; Y_B|X_E, V), I(U; Y_E|X_E, V)\} \\ & - I(W; S_A|S_B) \qquad (2.12) \end{aligned}$$

subject to constraint

$$I(X_E; Y_B|V) \geq I(\hat{Y}_E; Y_E|Y_B, X_E, U).$$

Theorem 2.2.

$$\tilde{\mathcal{R}} \supseteq \bigcup_{p \in \mathcal{P}} \mathcal{R}(p).$$

Sketch of Proof: Using similar strategy as in [13] and the results from Theorem 2.1, we create secret and public bit pipes of rates R_S and R_P respectively. Over the secret bit pipe we send a part of the secret message at rate R_{M1} and a part of the bin index from a Wyner-Ziv source coder to generate part of the key of rate R_{K1}. Then, we use the public bit pipe for the following purposes:

- Generate a secret key of rate $R_{K2} + R_{M2}$ by sending the remainder of the Wyner-Ziv bin index.
- Send the remaining part of the secret message at rate R_{M2} one-time padded by R_{M2} bits of the secret-key.

From the analysis above, the following has to be satisfied:

$$R_{K1} + R_{M1} \leq R_S = [I(V_A; Y_B, \hat{Y}_E | X_E, U) - I(V_A; Y_E | X_E, U)]_+ \tag{2.13}$$

Csiszar and Ahlswede showed in [19] that the achievable key rate we can derive from the source is $\{I(W; S_B) - I(W; S_E)\}_+$, where W, S_A, S_B, S_E satisfy $W - S_A - (S_B, S_E)$. Thus, we have

$$R_{K2} + R_{M2} \leq \{I(W; S_B) - I(W; S_E)\}_+ \tag{2.14}$$

The bin information should fit into its allocated bin budget:

$$R_{M1} + R_{M2} + I(W; S_A | S_B) \leq R_S + R_P \tag{2.15}$$

The one time padded part of the secret message is sent over the public bit pipe together with the common message, so they should not exceed the public bit pipe rate

$$R_{M2} \leq R_P \tag{2.16}$$

To get the achievable rate region, we write

$$\begin{aligned} R_K &= R_{K1} + R_{K2} && (2.17) \\ R_M &= R_{M1} + R_{M2}. && (2.18) \end{aligned}$$

By eliminating variables $R_{K1}, R_{K2}, R_{M1}, R_{M2}$ we obtain the results from Theorem 2.2. A complete proof of Theorem 2.2 is provided in the Appendix A.

Remark 2.4. If we disable cooperation between the relay and the destination by setting $X_E = 0$, $\hat{Y}_E = 0$, $U = V$, the channel model reduces to the broadcast channel observed in [13].

$$\begin{aligned} R_K + R_M &\leq [I(V_A; Y_B|U) - I(V_A; Y_E|U)]_+ \\ &\quad + [I(W; S_B) - I(W; S_E)]_+ \\ R_M &\leq I(V_A; Y_B) - I(W; S_A|S_B), \end{aligned} \tag{2.19}$$

for any joint distributions which satisfy

$$\begin{aligned} P_{U,V_A,X_A,Y_B,Y_E} &= P_U P_{V_A|U} P_{X_A|V_A} P_{Y_E,Y_B|X_A} \\ P_{W,S_A,S_B,S_E} &= P_W P_{S_A|W} P_{S_B,S_E|S_A}. \end{aligned}$$

2.4 An Outer Bound

An outer bound on the rate-equivocation region for the relay channel without correlated observations is derived in [4], and later improved in [6] for the relay channel with orthogonal components. Now, we provide an outer bound for the secret message-secret key rate region which is based on Oohama's [4] outer bound for the relay channel with confidential messages and an outer bound on the secret message-secret key rate region for the broadcast channel with correlated observations studied in [13].

Theorem 2.3. *The secret key-secret message rate region of the relay channel $P_{Y_E,Y_B|X_A,X_E}$ with correlated observations lies in the union of the following rate pairs,*

$$\begin{aligned} R_M &\le I(X_A, X_E; Y_E, Y_B) - I(W; S_A|S_B) \\ R_M + R_K &\le I(X_A; Y_B|X_E, Y_E) + I(W; S_B|S_E), \end{aligned}$$

where (W, S_A, S_B, S_E) form the Markov Chain $W - S_A - (S_B, S_E)$.

Proof of Theorem 2.3 can be found in the Appendix A.

Remark 2.5. If the relay channel is reversely degraded [17] *i.e.* $P_{Y_B,Y_E|X_A,X_E} = P_{Y_B|X_A,X_E}P_{Y_E|Y_B,X_E}$ and (W, S_A, S_B, S_E) form the Markov chain $W - S_A - S_B - S_E$, then inner and outer bound on the secret message-secret key sum rate coincide.

To show this, note that $I(W; S_B|S_E) = I(W; S_B) - I(W; S_E)$ and $I(X_A, Y_B|X_E, Y_E) = I(X_A; Y_B|X_E) - I(X_A; Y_E|X_E)$. Applying this to the Theorem 2.3, we have

$$\begin{aligned} R_M + R_K \le\ & I(X_A; Y_B|X_E) - I(X_A; Y_E|X_E) \\ & + I(W; S_B) - I(W; S_E), \end{aligned}$$

which is achieved by setting $V_A = X_A$, $U = V = 0$, $\hat{Y}_E = 0$ in the Theorem 2.2.

Remark 2.6. If the relay channel is degraded [17] *i.e.* $P_{Y_B,Y_E|X_A,X_E} = P_{Y_E|X_A,X_E}P_{Y_B|Y_E,X_E}$ and (W, S_A, S_B, S_E) form the same Markov chain as in the previous remark, we again have that the secret message-secret key sum rate is optimal.

It is immediately clear from the definition of the degraded relay channel that $I(X_A; Y_B|X_E, Y_E) = 0$. Therefore,

$$R_M + R_K \le I(W; S_B) - I(W; S_E),$$

which is always achievable according to the Theorem 2.2.

2.5 Gaussian Relay Channel

In this section we confirm our previously stated result about the sum rate optimality when the relay channel is degraded or reversely degraded, and the sources are distributed such that the Markov chain $S_A - S_B - S_E$ holds.

2.5.1 Reversely Degraded Gaussian Channel

Reversely degraded Gaussian channel can be defined as follows:

$$Y_B = X_A + X_E + Z_2 \tag{2.20}$$

$$Y_E = X_A + Z_1, \tag{2.21}$$

where $\mathbb{E}[X_A^2] \leq P_A$, $\mathbb{E}[X_E^2] \leq P_E$, $Z_2 \sim \mathcal{N}(0, N_2)$, $Z_1 = Z_2 + Z_{1|2}$, where $Z_{1|2} \sim \mathcal{N}(0, N_1 - N_2)$ is independent of Z_2, and $N_1 > N_2$. Rewriting (2.22) and (2.23) we obtain

$$\begin{aligned} Y_B &= X_A + X_E + Z_2 \\ Y_E &= X_A + Z_2 + Z_{1|2}, \end{aligned}$$

from which it is easy to verify that the Markov chain $X_A - (Y_B, X_E) - Y_E$ holds. For the source model, we assume that the observations at Alice, Eve and Bob are jointly Gaussian, where $S_B = S_A + Z_B$, $S_E = S_A + Z_E$ such that $S_A \sim \mathcal{N}(0, N_A)$, $Z_B \sim \mathcal{N}(0, N_B)$ and $Z_E \sim \mathcal{N}(0, N_E)$. Calculating the inner and the outer bound from the Theorems 2.2 and 2.3, for $\theta \in [0,1]$ and $\nu \in [0,1]$, we obtain:

$$\begin{aligned} R_M + R_K &\leq \frac{1}{2}\ln\left(1 + \frac{P_A(1-\theta^2)}{N_2}\right) - \frac{1}{2}\ln\left(1 + \frac{P_A(1-\theta^2)}{N_1}\right) \\ &\quad + \frac{1}{2}\ln\left(1 + \frac{\bar{\nu}N_A}{\nu N_A + N_B}\right) - \frac{1}{2}\ln\left(1 + \frac{\bar{\nu}N_A}{\nu N_A + N_E}\right) \\ R_M &\leq \frac{1}{2}\ln\left(1 + \frac{P_A(1-\theta^2)}{N_2}\right) - \frac{1}{2}\ln\left(1 + \frac{\bar{\nu}N_A}{\nu(N_A + N_B)}\right), \end{aligned}$$

for the inner bound, and

$$\begin{aligned} R_M + R_K &\leq \frac{1}{2}\ln\left(1 + \frac{P_A(1-\theta^2)}{N_2}\right) - \frac{1}{2}\ln\left(1 + \frac{P_A(1-\theta^2)}{N_1}\right) \\ &\quad + \frac{1}{2}\ln\left(1 + \frac{\bar{\nu}N_A}{\nu N_A + N_B}\right) - \frac{1}{2}\ln\left(1 + \frac{\bar{\nu}N_A}{\nu N_A + N_E}\right) \\ R_M &\leq \frac{1}{2}\ln\left(1 + \frac{P_A P_E(1-\theta^2) + P_A(N_1 - N_2) + P_E N_1 + 2(N_1 - N_2)\theta\sqrt{P_A P_E}}{N_2(N_1 - N_2)}\right) \\ &\quad - \frac{1}{2}\ln\left(1 + \frac{\bar{\nu}N_A}{\nu(N_A + N_B)}\right), \end{aligned}$$

for the outer bounder, where $\bar{x} = 1 - x$. Rate region in Figure 2.3 shows message-key sum rate optimality when the relay channel is reversely degraded.

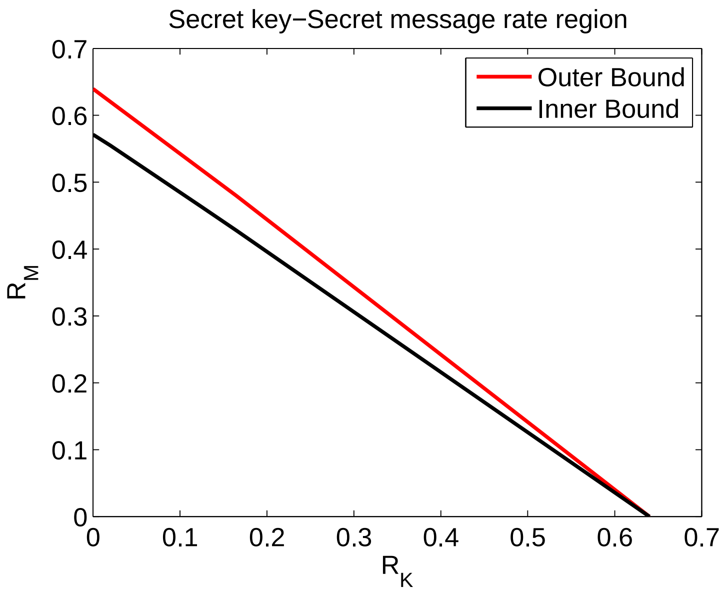

Figure 2.3: Reversely degraded relay channel: (R_K, R_M) rate region. $P_A = P_E = 10$, $N_2 = 1$, $N_1 = 2$, $N_A = 1$, $N_B = 1$, $N_E \to \infty$. The figure shows the secret key-secret message sum rate optimality.

2.5.2 Degraded Gaussian Relay Channel

Degraded Gaussian channel can be defined as follows:

$$Y_B = X_A + X_E + Z_2 \tag{2.22}$$

$$Y_E = X_A + Z_1, \tag{2.23}$$

where $\mathbb{E}[X_A^2] \leq P_A$, $\mathbb{E}[X_E^2] \leq P_E$, $Z_1 \sim \mathcal{N}(0, N_1)$, $Z_2 = Z_1 + Z_{2|1}$, where $Z_{2|1} \sim \mathcal{N}(0, N_2 - N_1)$ is independent of Z_1, and $N_2 > N_1$. Rewriting (2.22) and (2.23) we obtain

$$Y_B = X_A + X_E + Z_1 + Z_{2|1}$$

$$Y_E = X_A + Z_1,$$

from which it is easy to verify that the Markov chain $X_A - (Y_E, X_E) - Y_B$ holds. Calculating the inner and the outer bound from the Theorems 2.2 and 2.3, for $\theta \in [0,1]$ and $\nu \in [0,1]$, we obtain:

$$\begin{aligned} R_M + R_K &\leq \frac{1}{2}\ln\left(1+\frac{\bar{\nu}N_A}{\nu N_A + N_B}\right) - \frac{1}{2}\ln\left(1+\frac{\bar{\nu}N_A}{\nu N_A + N_E}\right) \\ R_M &\leq \frac{1}{2}\ln\left(1+\frac{P_A(1-\theta^2)}{N_2}\right) - \frac{1}{2}\ln\left(1+\frac{\bar{\nu}N_A}{\nu(N_A + N_B)}\right), \end{aligned}$$

for the inner bound, and

$$\begin{aligned} R_M + R_K &\leq \frac{1}{2}\ln\left(1+\frac{\bar{\nu}N_A}{\nu N_A + N_B}\right) - \frac{1}{2}\ln\left(1+\frac{\bar{\nu}N_A}{\nu N_A + N_E}\right) \\ R_M &\leq \frac{1}{2}\ln\left(1+\frac{P_AP_E(1-\theta^2)+P_A(N_2-N_1)+P_EN_2+2(N_2-N_1)\theta\sqrt{P_AP_E}}{N_1(N_2-N_1)}\right) \\ &\quad - \frac{1}{2}\ln\left(1+\frac{\bar{\nu}N_A}{\nu(N_A + N_B)}\right), \end{aligned}$$

for the outer bounder. Rate region in Figure 2.4 shows message-key sum rate optimality when the relay channel is degraded.

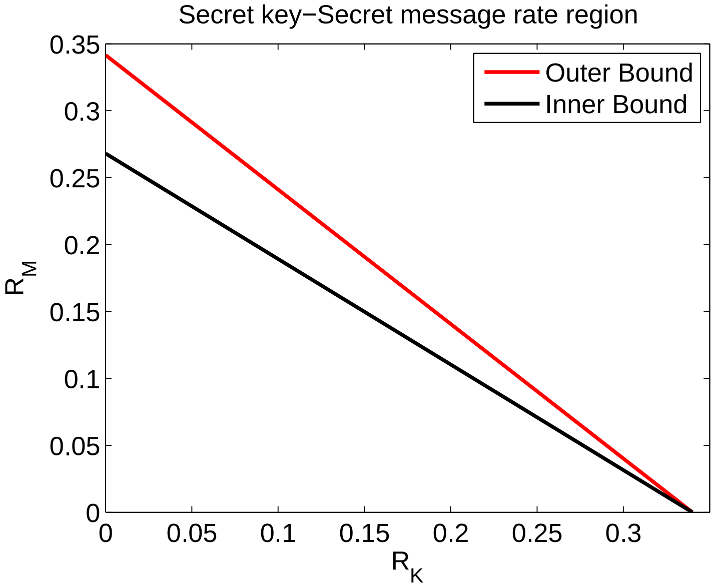

Figure 2.4: Degraded relay channel: (R_K, R_M) rate region. $P_A = P_E = 10$, $N_2 = 2$, $N_1 = 1$, $N_A = 1$, $N_B = 1$, $N_E \to \infty$. The figure shows the secret key-secret message sum rate optimality.

Chapter 3

The Role of Game Theory in Key Agreement Over a Public Channel

3.1 Introduction

The fact that dependent source observations at the terminals can be used as a resource for generating secret key was recognized by Ahlswede and Csiszar [19] and Maurer [20]. This work was later extended to multi terminal key agreement (see [22], [23], [11], [12]).

Connections between game theory and information theory were studied in [24] and [25], [26]. Also, the role of game theory in cryptography, especially in the problems of multiparty computation, where multiple terminals want to agree on some function of their private observations by transmitting them over a public channel, has been studied in [27], [28].

In this chapter we study the problem of key agreement over a public channel in the presence of distributed source observations available to each terminal, when only partial knowledge about their observations is available. We restrict our attention to the three-terminal problem in which Alice wants to agree with Bob and Charlie on keys K_{AB} and K_{AC}, which are perfectly secret from Charlie and Bob, respectively.

Alice observes $X^n = (X_1, ..., X_n)$, Bob observes $Y^n = (Y_1, ..., Y_n)$, and Charlie observes $Z^n = (Z_1, ..., Z_n)$, which are elements of $\mathcal{X}^n, \mathcal{Y}^n, \mathcal{Z}^n$. They can transmit any function of their observations over a public noiseless channel in order to construct the keys K_{AB} and K_{AC}.

We assume that Alice constructs the codebooks for both keys, and defines the protocol for the key agreement. To this end, she has to know how "powerful" Bob and Charlie are in terms of agreeing with her on a key, and in terms of eavesdropping on the other user's key. The notion of the capabilities of the three nodes is captured by the joint pmf P_{XYZ}, which is not available to Alice.

In order to learn this joint distribution, she requests from Bob and Charlie sufficient information about their observations over the public channel.

We model these reports by having Bob and Charlie select discrete memoryless channels $P_{Y_r|Y}$ and $P_{Z_r|Z}$, respectively, and essentially sending the information about Y_r and Z_r over the public channel (see Figure 3.1). After this, Alice gets access to $P_{XY_rZ_r}$, and Bob and Charlie both know $P_{XYY_rZZ_r}$. Based on the distribution $P_{XY_rZ_r}$, Alice constructs and sends to Bob and Charlie, the codebooks for the keys K_{AB} and K_{AC}.

Why do we consider the problem where Bob and Charlie may lie about their observations? To address this, let us investigate their incentives. Specifically, Bob, as an eavesdropper, is motivated to misreport his observations, because this gives him a chance to "snoop" more about the key K_{AC}. But Bob, as a legitimate user, wants to report honestly because this maximizes the key rate that he can agree with Alice. The same holds for Charlie. Alice, on the other hand, wants to keep both of them honest because she wants the keys K_{AB} and K_{AC} to be perfectly secret.

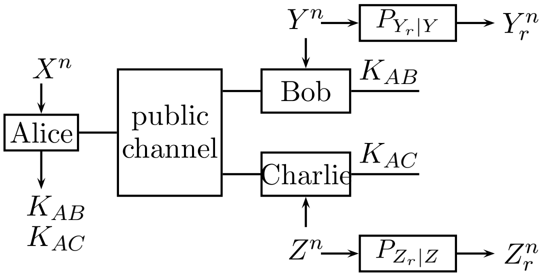

Figure 3.1: Key agreement over a noiseless public channel with unknown joint statistics. Alice agrees with Bob on a key K_{AB} that is perfectly protected from Charlie. Alice and Charlie agree on a key K_{AC} that is perfectly protected from Bob. To construct the codebooks for the key agreement Alice requests from Bob and Charlie to send her some sufficient information about their observations. Here we model these reports by having Bob and Charlie select discrete memoryless channels $P_{Y_r|Y}$ and $P_{Z_r|Z}$, respectively, and send sufficient information about Y_r and Z_r over the public channel.

We phrase this as a game-theoretic problem. Bob and Charlie select the channels $P_{Y_r|Y}$ and $P_{Z_r|Z}$, respectively, based on an objective that is a function of their key rates and the amount of information they can learn about each other's keys, called the leakage rates. Moreover, Alice's behavior is fully known to both Bob and Charlie.

For simplicity, we consider linear objectives:

$$\begin{aligned} U_{Bob} &= R_{AB} + \lambda R^L_{AC} \ \text{ for some } P_{Y_r|Y}, \\ U_{Charlie} &= R_{AC} + \lambda R^L_{AB} \ \text{ for some } P_{Z_r|Z}, \end{aligned} \tag{3.1}$$

where $\lambda \in [0,1]$, R_{AB} and R_{AC} are the rates of the keys K_{AB} and K_{AC}, respectively, and R^L_{AB} and R^L_{AC} denote the leakage rates of the keys K_{AB} and K_{AC}, respectively. Considering more general classes of utility functions is a part of ongoing and future research.

As mentioned above, Alice's strategy for the key agreement is fixed and known to everyone. In this work we analyze two games defined as follows:

Game 1

In this game Bob and Charlie choose their reports $P_{Y_r|Y}$ and $P_{Z_r|Z}$ by maximizing their utility functions (3.1). Alice maximizes both key rates R_{AB} and R_{AC} by constructing the codebooks based on the reported source distribution $P_{XY_rZ_r}$.

Game 2

In game 1 we assigned Alice a completely passive role, in which she just blindly accepts what Bob and Charlie report. However, one obvious goal for Alice is to keep Bob and Charlie honest, because Alice wants the keys K_{AB} and K_{AC} to be as protected as possible. Hence, in this game we study the scenario where Alice can modify the reports and construct the codebooks based on some function of Bob and Charlie's reported observations. Moreover, we assume that Bob and Charlie have access to the source distributions P_{XY} and P_{XZ}, respectively.

In Game 2 Alice intentionally reduces the key rate in order to lower the leakage rate and enforce honesty. It is important to point out that Alice has no access to the true joint source distribution P_{XYZ}. Hence, in Game 2, her protocol cannot depend on it.

3.2 Problem Statement

A pair of random variables (K_{AB}, K_{AC}) represents a pair of ϵ-keys if there exist two other pairs of random variables $(\hat{K}_{AB}, \hat{K}_{AC})$ and $(\tilde{K}_{AB}, \tilde{K}_{AC})$ satisfying

$$\begin{aligned}\hat{K}_{AB} &= \hat{K}_{AB}(g, X^n) \quad & \hat{K}_{AC} &= \hat{K}_{AC}(g, X^n),\\ \tilde{K}_{AB} &= \tilde{K}_{AB}(g, Y_r^n) \quad & \tilde{K}_{AC} &= \tilde{K}_{AC}(g, Z_r^n),\end{aligned}$$

where $\hat{K}_{AB}$ $(\hat{K}_{AC})$ and $\tilde{K}_{AB}$ $(\tilde{K}_{AC})$ take values in the same finite set $\mathcal{K}_{AB}$ $(\mathcal{K}_{AC})$, and g denotes all transmissions over the public channel such that

$$\begin{aligned}Pr\{K_{AB} \neq \hat{K}_{AB}\} \leq \epsilon, &\quad Pr\{K_{AC} \neq \hat{K}_{AC}\} \leq \epsilon,\\ Pr\{K_{AB} \neq \tilde{K}_{AB}\} \leq \epsilon, &\quad Pr\{K_{AC} \neq \tilde{K}_{AC}\} \leq \epsilon.\end{aligned}$$

In addition, the ϵ-keys generated between Alice and Bob, and Alice and Charlie, respectively, have to satisfy an independence condition: $I(K_{AB}; K_{AC}) \leq \epsilon$, a secrecy condition:

$$\frac{1}{n} I(K_{AB}; g, Z_r^n) \leq \epsilon, \quad \frac{1}{n} I(K_{AC}; g, Y_r^n) \leq \epsilon,$$

and a uniformity condition:

$$\begin{aligned}\frac{1}{n} H(K_{AB}) &= \frac{1}{n} \log |\mathcal{K}_{AB}| - \epsilon = R_{AB,\epsilon},\\ \frac{1}{n} H(K_{AC}) &= \frac{1}{n} \log |\mathcal{K}_{AC}| - \epsilon = R_{AC,\epsilon}.\end{aligned}$$

If all of the above conditions are satisfied, we say that the key rate pair $(R_{AB,\epsilon}, R_{AC,\epsilon})$ is ϵ-achievable.

A key rate pair (R_{AB}, R_{AC}) is said to be achievable if there is a sequence of ϵ_n such that $(R_{AB,\epsilon_n}, R_{AC,\epsilon_n})$ are ϵ_n-achievable key rate pairs, and as $n \to \infty$, $\epsilon_n \to 0$, $R_{AB,\epsilon_n} \to R_{AB}$ and $R_{AC,\epsilon_n} \to R_{AC}$. Since the agreement relies on, in general, a false joint source distribution $P_{XY_rZ_r}$, part of the keys K_{AB} and K_{AC} may leak to Charlie and Bob, respectively. We call this leakage rate and formally define it as follows:

Definition 3.1. The leakage rate R_{AB}^L for key K_{AB} is defined to be

$$R_{AB}^L = \frac{1}{n} I(K_{AB}; g, Z^n). \tag{3.2}$$

It models a part of the key K_{AB} that Charlie may be able to decode. Similarly, we define

$$R_{AC}^L = \frac{1}{n} I(K_{AC}; g, Y^n), \tag{3.3}$$

where Y^n and Z^n correspond to Bob and Charlie's actual observations, respectively.

We define $\tilde{\mathcal{R}}$ to be the set of all achievable rate tuples $(R_{AB}, R_{AB}^L, R_{AC}, R_{AC}^L)$.

Let us now formally define game 1 and game 2.

Definition 3.2. In Game 1 we define Alice, Bob and Charlie's utility functions as follows:

- $U_{Bob} = \max_{P_{Y_r|Y}} R_{AB} + \lambda R_{AC}^L$ for some $P_{Y_r|Y}$.
- $U_{Charlie} = \max_{P_{Z_r|Z}} R_{AC} + \lambda R_{AB}^L$ for some $P_{Z_r|Z}$.
- Upon receiving information about Y_r and Z_r from Bob and Charlie, respectively, Alice constructs the codebooks for key agreement based on the the joint source distribution $P_{XY_rZ_r}$ and objective function

$$U_{Alice} = \max R_{AB} + \max R_{AC}$$

Definition 3.3. In Game 2 we define Alice, Bob and Charlie's utility functions as follows:

- $U_{Bob} = \max_{P_{Y_r|Y}} R_{AB} + \lambda R_{AC}^L$ for some $P_{Y_r|Y}$ such that the Markov chain $(X, Z, Z_r) - Y - Y_r$ holds. This is equivalent to saying that Bob has no knowledge about the true joint source distribution P_{XYZ}.
- $U_{Charlie} = \max_{P_{Z_r|Z}} R_{AC} + \lambda R_{AB}^L$ for some $P_{Z_r|Z}$ such that the Markov chain $(X, Y, Y_r) - Z - Z_r$ holds. This is equivalent to saying that Charlie has no knowledge about the true joint source distribution P_{XYZ}.
- Upon receiving information about Y_r and Z_r from Bob and Charlie, respectively, Alice constructs the codebooks for key agreement based on the joint source distribution $P_{XY_rZ_r}$ such that $Y_r = Y$ and $Z_r = Z$ is Nash equilibrium.

3.3 An Achievable Key Agreement Scheme

Let $\mathcal{P}_1$ be the set of all joint distributions of random variables U, X, Y, Y_r, Z and Z_r that can be written as

$$P_{XYZ}P_{Y_r|Y}P_{U|Y_r}P_{Z_r|Z}. \tag{3.4}$$

Similarly, we define $\mathcal{P}_2$ to be the set of all joint distributions of random variables V, X, Y, Y_r, Z and Z_r that can be written as

$$P_{XYZ}P_{Z_r|Z}P_{V|Z_r}P_{Y_r|Y}. \tag{3.5}$$

For $p \in \mathcal{P}_1$, let $\mathcal{R}_1(p)$ be the set of all non-negative rate pairs $(R_{AB}, R^L_{AB}, R_{AC}, R^L_{AC})$ which satisfy the following inequalities:

$$\begin{aligned}
R_{AB} &\leq I(Y_r;X|U) - I(Y_r;Z_r|U),\\
R^L_{AB} &\leq I(Y_r;Z|U) - I(Y_r;Z_r|U),\\
R_{AC} &\leq I(X;Z_r|Y_r),\\
R^L_{AC} &\leq I(Z_r;Y) - I(Z_r;Y_r).
\end{aligned}$$

Similarly, for $p \in \mathcal{P}_2$, we define $\mathcal{R}_2(p)$ to be the set of all rate tuples which satisfy the following inequalities:

$$\begin{aligned}
R_{AB} &\leq I(X;Y_r|Z_r),\\
R^L_{AB} &\leq I(Y_r;Z) - I(Y_r;Z_r),\\
R_{AC} &\leq I(Z_r;X|V) - I(Z_r;Y_r|V),\\
R^L_{AC} &\leq I(Z_r;Y|V) - I(Z_r;Y_r|V),
\end{aligned}$$

where U and V take values in $\mathcal{U}$ and $\mathcal{V}$, respectively, such that $|\mathcal{U}| \leq |\mathcal{Y}| + 1$ and $|\mathcal{V}| \leq |\mathcal{Z}| + 1$.

Theorem 3.1.

$$\tilde{\mathcal{R}} \supseteq Co\,(\mathcal{R}_1(p) \cup \mathcal{R}_2(p)) \quad \textit{for some } p \in \mathcal{P}_1 \cup \mathcal{P}_2,$$

where Co *denotes the convex hull.*

Sketch of Proof: Here, we just show the achievability for the $\mathcal{R}_1$ region. The key agreement protocol is performed in two stages ([29], *Theorem 2.2*): First, Bob agrees with Alice on a key K_{AB} by treating Charlie as an eavesdropper. Applying the results from [19] $R_{AB} \leq I(Y_r;X|U) - I(Y_r;Z_r|U)$ for $U - Y_r - (X, Z_r)$. Charlie as an eavesdropper has access to the true observations z^n, and thus can reduce uncertainty about the key K_{AB}. Alice partitions the codebook in such a way that each bin has exactly one sequence y_r^n that is jointly typical with z_r^n. Since Charlie observes z^n, there will actually be approximately $2^{nR_{AB}^L} \leq 2^{n(I(Y_r;Z)-I(Y_r;Z_r))}$ bins which have exactly one sequence z^n that is jointly typical with y_r^n. In the second stage, Alice has access to Y_r, and Charlie agrees with her on a key K_{AC} at the rate $R_{AC} \leq I(Z_r;X,Y_r) - I(Z_r;Y_r) = I(X;Z_r|Y_r)$. It is straightforward to show, that the leakage rate for the key K_{AC} is $R_{AC}^L \leq I(Z_r;Y) - I(Z_r;Y_r)$. A complete proof of Theorem 3.1 is provided in the Appendix B.

3.4 Binary Erasure Distribution

In this example we consider an erasure source distribution: let $X \sim Ber(\frac{1}{2})$, and let Y and Z correspond to the output of an erasure channel with input X, and erasure probabilities ϵ and δ, respectively.

3.4.1 Game 1

As pointed out above, Bob and Charlie are ready to sacrifice their key rate in order to gain in leakage rate. We consider the following utility functions:

$$U_{Bob} = R_{AB} + \lambda R^L_{AC} \quad \text{for some } \epsilon_r \geq \epsilon, \tag{3.6}$$

$$U_{Charlie} = R_{AC} + \lambda R^L_{AB} \quad \text{for some } \delta_r \geq \delta. \tag{3.7}$$

Based on the utilities and their knowledge of the true joint distribution P_{XYZ}, they select conditional distributions $P_{Y_r|Y}$ and $P_{Z_r|Z}$, respectively. As pointed out in the introduction, $P_{Y_r|X}$ and $P_{Z_r|X}$ are also Binary Erasure Channels. It can be shown that Alice maximizes both key rates by setting $U = V = 0$ in Theorem 3.1.

Remark 3.1. For $U = V = 0$, if the Markov chain $Y - X - Z$ holds, then the following rate tuple $(R_{AB}, R^L_{AB}, R_{AC}, R^L_{AC})$ is achievable:

$$\begin{aligned} R_{AB} &\leq I(Y_r; X) - I(Y_r; Z_r), \\ R^L_{AB} &\leq I(Y_r; Z) - I(Y_r; Z_r), \\ R_{AC} &\leq I(Z_r; X) - I(Z_r; Y_r), \\ R^L_{AC} &\leq I(Z_r; Y) - I(Z_r; Y_r). \end{aligned}$$

This result directly follows from Theorem 3.1 by noticing that $\mathcal{R}_1$ and $\mathcal{R}_2$ provide the same rate region. From now on we restrict attention to those source distributions for which the Markov chain $Y - X - Z$ holds. It is easy to verify that the binary erasure source satisfies this Markov chain condition.

Before we continue with the analysis of this game, we state a formal definition of Nash equilibria.

Definition 3.4. Nash equilibria are stable states of a system that involves several interacting participants in which no participant can gain by a change of strategy as long as all the other participants remain unchanged.

As pointed out in Definition 3.2, Bob and Charlie have access to the true joint distribution P_{XYZ}. In this example this means that they both know ϵ and δ.

Claim 1. *For the binary erasure source distribution with parameters ϵ and δ, Nash equilibrium for Game 1, can be computed as follows:*

$$(\epsilon_r, \delta_r) = \begin{cases} (\epsilon, \delta) & \textit{if } \epsilon > \frac{\lambda}{\lambda+1} \textit{ and } \delta > \frac{\lambda}{\lambda+1} \\ (\epsilon, 1) & \textit{if } \epsilon < \frac{\lambda}{\lambda+1} \textit{ and } \delta > \frac{\lambda}{\lambda+1} \\ (1, \delta) & \textit{if } \epsilon > \frac{\lambda}{\lambda+1} \textit{ and } \delta < \frac{\lambda}{\lambda+1} \\ (\epsilon, 1) \textit{ and } (1, \delta) & \textit{if } \epsilon < \frac{\lambda}{\lambda+1} \textit{ and } \delta < \frac{\lambda}{\lambda+1} \end{cases}$$

Let us prove this claim: setting $U = V = 0$ in Theorem 3.1 we have:

$$R_{AB} = \delta_r(1-\epsilon_r), \quad R_{AB}^L = (\delta_r - \delta)(1-\epsilon_r),$$
$$R_{AC} = \epsilon_r(1-\delta_r), \quad R_{AC}^L = (\epsilon_r - \epsilon)(1-\delta_r).$$

Hence, Bob and Charlie's utilities is equal to

$$U_{Bob} = \delta_r(1-\epsilon_r) + \lambda(\epsilon_r - \epsilon)(1-\delta_r),$$
$$U_{Charlie} = \epsilon_r(1-\delta_r) + \lambda(\delta_r - \delta)(1-\epsilon_r),$$

respectively. Optimizing these utilities, we have

$$\arg\max_{\epsilon \le \epsilon_r \le 1} U_{Bob} = \arg\max_{\epsilon \le \epsilon_r \le 1} \epsilon_r(\lambda - \delta_r(\lambda+1)),$$
$$\arg\max_{\delta \le \delta_r \le 1} U_{Charlie} = \arg\max_{\delta \le \delta_r \le 1} \delta_r(\lambda - \epsilon_r(\lambda+1)).$$

Hence ϵ_r and δ_r are chosen in the following way:

$$\epsilon_r = \begin{cases} \epsilon & \text{if } \delta_r > \frac{\lambda}{\lambda+1} \\ 1 & \text{if } \delta_r < \frac{\lambda}{\lambda+1} \end{cases} \qquad \delta_r = \begin{cases} \delta & \text{if } \epsilon_r > \frac{\lambda}{\lambda+1} \\ 1 & \text{if } \epsilon_r < \frac{\lambda}{\lambda+1} \end{cases}$$

This analysis shows that the considered Nash equilibrium sits at the corner points *i.e.* $\epsilon_r = \{\epsilon, 1\}$, $\delta_r = \{\delta, 1\}$. Knowing this, the Nash equilibrium can be easily computed by observing the utility matrix in Figure 3.2: the entries of the matrix are the utilities evaluated at the points of interest (in each box, the left entry for Charlie and the right entry for Bob).

When $\epsilon > \frac{\lambda}{\lambda+1}$ and $\delta > \frac{\lambda}{\lambda+1}$, Bob and Charlie have no incentive to unilaterally change their strategies and move from the upper left box of the utility matrix. In other words if Bob changes his strategy from $\epsilon_r = \epsilon$ to $\epsilon_r = 1$ he will decrease his utility functions (upper right box of the utility matrix). Similarly, is Charlie changes his strategy from $\delta_r = \delta$ to $\delta_r = 1$ he will also decrease his utility function (lower left box of the utility matrix). When $\epsilon > \frac{\lambda}{\lambda+1}$ and $\delta < \frac{\lambda}{\lambda+1}$, Bob and Charlie have no incentive to unilaterally change their strategies and move from the upper right box of the

$U_{Charlie}$ \ U_{Bob}	$\epsilon_r = \epsilon$	$\epsilon_r = 1$
$\delta_r = \delta$	$\delta(1-\epsilon)$ $\epsilon(1-\delta)$	$\lambda(1-\epsilon)(1-\delta)$ $1-\delta$
$\delta_r = 1$	$1-\epsilon$ $\lambda(1-\epsilon)(1-\delta)$	0 0

Figure 3.2: Utility matrix: In each box, the left entry is Charlie's utility, and the right entry is Bob's utility.

utility matrix. When $\epsilon < \frac{\lambda}{\lambda+1}$ and $\delta > \frac{\lambda}{\lambda+1}$, Bob and Charlie have no incentive to unilaterally change their strategies and move from the lower left box of the utility matrix. When $\epsilon < \frac{\lambda}{\lambda+1}$ and $\delta < \frac{\lambda}{\lambda+1}$, Bob and Charlie have no incentive to unilaterally change their strategies and move from the upper right box of the utility matrix. They also have no incentive to unilaterally change their strategies and move from the lower left box of the utility matrix. Hence, for this case there exists two Nash equilibria.

3.4.2 Game 2

As we can see from the analysis above, the Nash equilibrium depends on the true distributions of both players. The question we ask is: what should Alice do in this game in order to ensure that honest reporting by both players is a Nash equilibrium. The answer to this is straightforward if Alice is ready to consciously leak a portion of the keys she agreed upon with Bob and Charlie. She generates both keys according to the following parameters:

$$\tilde{\epsilon} = \begin{cases} \epsilon_r & \text{if } \epsilon_r > \frac{\lambda}{\lambda+1} \\ \frac{\lambda}{\lambda+1} + \alpha & \text{if } \epsilon_r \leq \frac{\lambda}{\lambda+1} \end{cases} \qquad \tilde{\delta} = \begin{cases} \delta_r & \text{if } \delta_r > \frac{\lambda}{\lambda+1} \\ \frac{\lambda}{\lambda+1} + \alpha & \text{if } \delta_r \leq \frac{\lambda}{\lambda+1} \end{cases}$$

where $0 < \alpha \ll 1$. Notice that Alice is not any more just a passive observer who blindly follows some predetermined protocol. For this game, $\epsilon_r = \epsilon$ and $\delta_r = \delta$ is a Nash equilibrium. However, it is not the unique equilibrium because if $\epsilon \leq \frac{\lambda}{\lambda+1}$ ($\delta \leq \frac{\lambda}{\lambda+1}$), then every point in $\epsilon \leq \epsilon_r \leq \frac{\lambda}{\lambda+1}$ ($\delta \leq \delta_r \leq \frac{\lambda}{\lambda+1}$) is Nash equilibrium point. It is obvious that for all these equilibrium points, Bob and Charlie's utility functions are the same. Let us verify these results:

Case 1: If $\epsilon > \frac{\lambda}{\lambda+1}$ and $\delta > \frac{\lambda}{\lambda+1}$, then by the results of Claim 1, $\epsilon_r = \epsilon$, $\delta_r = \delta$ is the unique Nash equilibrium.

Case 2: $\epsilon \leq \frac{\lambda}{\lambda+1}$ and $\delta > \frac{\lambda}{\lambda+1}$.

U_{Bob} $U_{Charlie}$	$\epsilon \leq \epsilon_r \leq \frac{\lambda}{\lambda+1}$	$\epsilon_r = 1$
$\delta_r = \delta$	Γ $(\frac{\lambda}{\lambda+1} + \alpha)(1-\delta)$	$\lambda(1-\epsilon)(1-\delta)$ $1-\delta$
$\delta_r = 1$	$\frac{1}{\lambda+1} - \alpha$ $\lambda(\frac{1}{\lambda+1} - \alpha)(1-\delta)$	0 0

Figure 3.3: Utility matrix when $\epsilon \leq \frac{\lambda}{\lambda+1}$, $\delta > \frac{\lambda}{\lambda+1}$. $\Gamma = \delta(\frac{1}{\lambda+1} - \alpha) + \lambda(\frac{\lambda}{\lambda+1} + \alpha - \epsilon)(1-\delta)$. Bob and Charlie have no incentive to unilaterally change their strategies and move from the upper left box of the utility matrix.

The utility matrix (see Figure 3.3) indicates that Bob has no incentive to change his report from $\epsilon \leq \epsilon_r \leq \frac{\lambda}{\lambda+1}$ to $\epsilon_r = 1$ because

$$\delta(\frac{1}{\lambda+1} - \alpha) + \lambda(\frac{\lambda}{\lambda+1} + \alpha - \epsilon)(1-\delta) > \lambda(1-\epsilon)(1-\delta)$$

is equivalent to $\delta > \frac{\lambda}{\lambda+1}$ which is true by the assumption. It is only left to show that Charlie also has no incentive to change his strategy. This is true because

$$(\frac{\lambda}{\lambda+1} + \alpha)(1-\delta) > \lambda(\frac{1}{\lambda+1} - \alpha)(1-\delta) \Leftrightarrow \alpha(1+\lambda-\delta) > 0,$$

which is always true.

Case 3: $\epsilon > \frac{\lambda}{\lambda+1}$ and $\delta \leq \frac{\lambda}{\lambda+1}$.

U_{Bob} $U_{Charlie}$	$\epsilon_r = \epsilon$	$\epsilon_r = 1$
$\delta \leq \delta_r \leq \frac{\lambda}{\lambda+1}$	$(\frac{\lambda}{\lambda+1} + \alpha)(1-\epsilon)$ Δ	$\lambda(1-\epsilon)(\frac{1}{\lambda+1} - \alpha)$ $\frac{1}{\lambda+1} - \alpha$
$\delta_r = 1$	$1-\epsilon$ $\lambda(1-\epsilon)(1-\delta)$	0 0

Figure 3.4: Utility matrix when $\epsilon > \frac{\lambda}{\lambda+1}$, $\delta \leq \frac{\lambda}{\lambda+1}$. $\Delta = \epsilon(\frac{1}{\lambda+1} - \alpha) + \lambda(\frac{\lambda}{\lambda+1} + \alpha - \delta)(1-\epsilon)$. Bob and Charlie have no incentive to unilaterally change their strategies and move from the upper left box of the utility matrix.

The utility matrix (see Figure 3.4) indicates that Charlie has no incentive to change his report from $\delta \leq \delta_r \leq \frac{\lambda}{\lambda+1}$ to $\delta_r = 1$ because

$$\epsilon(\frac{1}{\lambda+1} - \alpha) + \lambda(\frac{\lambda}{\lambda+1} + \alpha - \delta)(1-\epsilon) > \lambda(1-\epsilon)(1-\delta)$$

is equivalent to $\epsilon > \frac{\lambda}{\lambda+1}$ which is true by the assumption. Bob has no incentive to change his strategy because

$$(\frac{\lambda}{\lambda+1} + \alpha)(1-\epsilon) > \lambda(\frac{1}{\lambda+1} - \alpha)(1-\epsilon) \Leftrightarrow \alpha(1+\lambda-\epsilon) > 0,$$

which is always true.

Case 4: $\epsilon \leq \frac{\lambda}{\lambda+1}$ and $\delta \leq \frac{\lambda}{\lambda+1}$.

U_{Bob} $U_{Charlie}$	$\epsilon \leq \epsilon_r \leq \frac{\lambda}{\lambda+1}$	$\epsilon_r = 1$
$\delta \leq \delta_r \leq \frac{\lambda}{\lambda+1}$	Π Σ	$\lambda(1-\epsilon)(\frac{1}{\lambda+1} - \alpha)$ $\frac{1}{\lambda+1} - \alpha$
$\delta_r = 1$	$\frac{1}{\lambda+1} - \alpha$ $\lambda(\frac{1}{\lambda+1} - \alpha)(1-\delta)$	0 0

Figure 3.5: Utility matrix when $\epsilon \leq \frac{\lambda}{\lambda+1}$, $\delta \leq \frac{\lambda}{\lambda+1}$. $\Pi = (\frac{1}{\lambda+1} - \alpha)(\lambda(1-\epsilon) + \alpha(\lambda+1))$, $\Sigma = (\frac{1}{\lambda+1} - \alpha)(\lambda(1-\delta) + \alpha(\lambda+1))$. Bob and Charlie have no incentive to unilaterally change their strategies and move from the upper left box of the utility matrix.

The utility matrix in Figure 3.5 indicates that both Bob and Charlie have no incentive to change their reports from $\epsilon \leq \epsilon_r \leq \frac{\lambda}{\lambda+1}$ and $\delta \leq \delta_r \leq \frac{\lambda}{\lambda+1}$ to $\epsilon_r = 1$ and $\delta_r = 1$, respectively. This follows from the fact that $\Pi > \lambda(1-\epsilon)(\frac{1}{\lambda+1} - \alpha)$ and $\Sigma > \lambda(1-\delta)(\frac{1}{\lambda+1} - \alpha)$ because $\alpha(\lambda+1) > 0$ always.

Since Alice's strategy in game 2 does not require knowledge of the true joint distributions, she can apply it when this information is not available to her. Now, Bob and Charlie also do not need to know the true erasure probabilities ϵ and δ, because their honest reporting is the Nash equilibrium, and they cannot gain anything by playing according to some other Nash equilibrium.

3.5 Extension to More General Case

In this section we generalize our result for a special class of discrete memoryless distributions. As pointed out before, we restrict attention to those distributions for which the Markov chain $Y-X-Z$ holds.

3.5.1 Game 1

Like in the binary erasure example, Bob and Charlie base their strategy on the best response: they maximize their utilities for every possible other player's response. From Remark 3.1, the optimizing distribution of Bob and Charlie's utility can be expressed as

$$\arg\max_{p(y_r|y)} U_{Bob} = \arg\max_{p(y_r|y)} I(Y_r;X) - (1+\lambda)I(Y_r;Z_r), \tag{3.8}$$

$$\arg\max_{p(z_r|z)} U_{Charlie} = \arg\max_{p(z_r|z)} I(Z_r;X) - (1+\lambda)I(Y_r;Z_r). \tag{3.9}$$

Based on (3.8) we define the function $\mathcal{R}_y$ as follows:

Definition 3.5. For a given distribution P_{XYZZ_r}, let $\mathcal{P}_{Y_r}$ be the set defined as follows

$$\mathcal{P}_{Y_r} = \{P_{Y_r} \mid \exists P_{Y_r|Y} \ s.t. \ \mathbb{E}_Y[P_{Y_r|Y}] = P_{Y_r}\}$$

We define the function $\mathcal{R}_y : \mathcal{P}_{Y_r} \mapsto \mathbb{R}$ given by

$$R_y(P_{Y_r}) = I(Y_r;X) - (1+\lambda)I(Y_r;Z_r), \tag{3.10}$$

and the set

$$\begin{aligned} S_y = \{(P_{Y_r}, t) \mid P_{Y_r} \in \mathcal{P}_{Y_r},\ t \leq R_y(P_{Y_r}) \text{ if } R_y(P_{Y_r}) \geq 0,\, t \geq 0,& \\ t \geq R_y(P_{Y_r}) \text{ if } R_y(P_{Y_r}) < 0,\, t < 0\}& \end{aligned} \tag{3.11}$$

Lemma 3.1. *If $(P_Y, \mathcal{R}_y(P_Y))$ is on the boundary of the convex hull of the set S_y, then Bob maximizes his utility by choosing:*

$$Y_r = \begin{cases} Y & \textit{if } I(X;Y) > (1+\lambda)I(Y;Z_r) \\ 0 & \textit{if } I(X;Y) < (1+\lambda)I(Y;Z_r) \end{cases}$$

where Y_r corresponds to $P_{Y_r|Y}$, and $Y_r = 0$ means that Bob's report to Alice contains no information.

Proof. Using the mutual information properties we can write

$$\begin{aligned} I(Y_r;X) - (1+\lambda)I(Y_r;Z_r) = I(Y;X) - (1+\lambda)I(Y;Z_r)& \\ - [I(Y;X|Y_r) - (1+\lambda)I(Y;Z_r|Y_r)].& \end{aligned} \tag{3.12}$$

Note that

$$\sup_{Y_r - Y - (X, Z_r)} I(Y; X|Y_r) - (1 + \lambda)I(Y; Z_r|Y_r)$$

computes the convex hull of the set S_y at the point $(P_Y, \mathcal{R}_y(P_Y))$. From the condition in Lemma 3.1 we have that

$$\begin{aligned} I(Y; X) - (1 + \lambda)I(Y; Z_r) &\geq I(Y; X|Y_r) - (1 + \lambda)I(Y; Z_r|Y_r) \;\text{ if } I(Y; X) - (1 + \lambda)I(Y; Z_r) \geq 0 \\ I(Y; X) - (1 + \lambda)I(Y; Z_r) &< I(Y; X|Y_r) - (1 + \lambda)I(Y; Z_r|Y_r) \;\text{ if } I(Y; X) - (1 + \lambda)I(Y; Z_r) < 0 \end{aligned} \tag{3.13}$$

From (3.12) and (3.13), we conclude that

$$I(Y; X) - (1 + \lambda)I(Y; Z_r) \geq 0 \Leftrightarrow I(Y_r; X) - (1 + \lambda)I(Y_r; Z_r) \geq 0. \tag{3.14}$$

If $I(Y; X) - (1+\lambda)I(Y; Z_r) \geq 0$ then it follows from (3.13) that $I(Y; X|Y_r) \geq (1+\lambda)I(Y; Z_r|Y_r)$. This shows that $Y_r = Y$ maximizes the expression (3.12).

If $I(Y; X) - (1 + \lambda)I(Y; Z_r) < 0$, then from (3.14) we have that $I(Y_r; X) < (1 + \lambda)I(Y_r; Z_r)$ for all Y_r such that the Markov chain $Y_r - Y - (X, Z_r)$ holds. Hence, (3.12) is maximized when $Y_r = 0$. □

Similarly, to optimize Charlie's utility, we define the function $\mathcal{R}_z$.

Definition 3.6. For a given distribution P_{XYY_rZ}, let $\mathcal{P}_{Z_r}$ be the set defined as follows

$$\mathcal{P}_{Z_r} = \{P_{Z_r} \mid \exists P_{Z_r|Z} \; s.t. \; \mathbb{E}_Z[P_{Z_r|Z}] = P_{Z_r}\}$$

We define the function $\mathcal{R}_z : \mathcal{P}_{Z_r} \mapsto \mathbb{R}$ given by

$$R_z(P_{Z_r}) = I(Z_r; X) - (1 + \lambda)I(Z_r; Y_r), \tag{3.15}$$

and the set

$$\begin{aligned} S_z = \{(P_{Z_r}, t) \mid P_{Z_r} \in \mathcal{P}_{Z_r}, \; t \leq R_z(P_{Z_r}) \text{ if } R_z(P_{Z_r}) \geq 0, \, t \geq 0, \\ t \geq R_z(P_{Z_r}) \text{ if } R_z(P_{Z_r}) < 0, \, t < 0\} \end{aligned} \tag{3.16}$$

Lemma 3.2. *If $(P_Z, \mathcal{R}_z(P_Z))$ is on the boundary of the convex hull of the set S_z, then Bob maximizes his utility by choosing:*

$$Z_r = \begin{cases} Z & \text{if } I(Z; X) > (1 + \lambda)I(Z; Y_r) \\ 0 & \text{if } I(Z; X) < (1 + \lambda)I(Z; Y_r) \end{cases}$$

where Z_r corresponds to $P_{Z_r|Z}$, and $Z_r = 0$ means that Bob's report to Alice contains no information.

From the results of the Lemmas 3.1 and 3.2, and the analysis of the binary erasure example, it is straightforward to characterize a Nash equilibrium for the special class of discrete memoryless source distributions.

Theorem 3.2. *For a given joint distribution $P_{XYZ} = P_X P_{Y|X} P_{Z|X}$, if the conditions of Lemmas 3.1 and 3.2 are satisfied for all $P_{Z_r|Z}$ and $P_{Y_r|Y}$, respectively, then a Nash equilibrium for the Game 1 can be characterized as follows:*

$$(Y_r, Z_r) = \begin{cases} (Y, Z) & \textit{if} \quad I(X;Y) > (1+\lambda)I(Y;Z) \textit{ and } I(Z;X) > (1+\lambda)I(Z;Y) \\ (Y, 0) & \textit{if} \quad I(X;Y) > (1+\lambda)I(Y;Z) \textit{ and } I(Z;X) < (1+\lambda)I(Z;Y) \\ (0, Z) & \textit{if} \quad I(X;Y) < (1+\lambda)I(Y;Z) \textit{ and } I(Z;X) > (1+\lambda)I(Z;Y) \\ (Y, 0), (0, Z) & \textit{if} \quad I(X;Y) < (1+\lambda)I(Y;Z) \textit{ and } I(Z;X) < (1+\lambda)I(Z;Y) \end{cases}$$

where Y_r and Z_r correspond to the distributions $P_{Y_r|Y}$ and $P_{Z_r|Z}$, respectively.

3.5.2 Game 2

Applying the same approach as in the binary erasure example, Alice enforces Bob and Charlie's honesty at the expense of constructing non-perfectly secret keys.

Let us define $\mathcal{B}_y$ and $\mathcal{B}_z$ as follows

$$\mathcal{B}_y = \{P_{Y_r|Y} \mid I(Z;X) > (1+\lambda)I(Z;Y_r)\},$$
$$\mathcal{B}_z = \{P_{Z_r|Z} \mid I(X;Y) > (1+\lambda)I(Y;Z_r)\}.$$

Definition 3.7. Let $Y^\star$ correspond to the distribution $P_{Y^\star|Y}$ such that

$$I(Z;X) = (1+\lambda)I(Z;Y^\star). \tag{3.17}$$

Similarly, $Z^\star$ correspond to the distribution $P_{Z^\star|Z}$ such that

$$I(X;Y) = (1+\lambda)I(Y;Z^\star). \tag{3.18}$$

Theorem 3.3. *If the joint distribution P_{XYZ} satisfies the conditions of Theorem 3.2, then Alice ensures that Bob and Charlie's honest reporting is a Nash equilibrium by constructing the keys K_{AB} and K_{AC} based on the following distributions:*

$$(P_{\tilde{Y}|Y}, P_{\tilde{Z}|Z}) = \begin{cases} (P_{Y_r|Y}, P_{Z_r|Z}) & \textit{if } P_{Y_r|Y} \in \mathcal{B}_y,\ P_{Z_r|Z} \in \mathcal{B}_z \\ (P_{Y_r|Y}, P_{Z^\star_+|Z}) & \textit{if } P_{Y_r|Y} \in \mathcal{B}_y,\ P_{Z_r|Z} \notin \mathcal{B}_z \\ (P_{Y^\star_+|Y}, P_{Z_r|Z}) & \textit{if } P_{Y_r|Y} \notin \mathcal{B}_y,\ P_{Z_r|Z} \in \mathcal{B}_z \\ (P_{Y^\star_+|Y}, P_{Z^\star_+|Z}) & \textit{if } P_{Y_r|Y} \notin \mathcal{B}_y,\ P_{Z_r|Z} \notin \mathcal{B}_z \end{cases}$$

where $P_{Y^\star_+|Y}$ and $P_{Z^\star_+|Z}$ are chosen such that $P_{Y^\star_+|Y} \in \mathcal{B}_y$ and $P_{Z^\star_+|Z} \in \mathcal{B}_z$.

Proof. Using the same analysis as in Lemma 3.1, it is straightforward to show that the possible conditional distributions which correspond to a Nash equilibrium are $P_{Y_r|Y} = \{P_{\tilde{Y}|Y}, 0\}$ and $P_{Z_r|Z} = \{P_{\tilde{Z}|Z}, 0\}$.

Case 1: If $I(Z;X) > (1+\lambda)I(Z;Y)$ and $I(X;Y) > (1+\lambda)I(Y;Z)$, then by the the results of Theorem 3.2, honest reporting is the Nash equilibrium.

Case 2: If $I(Z;X) \leq (1+\lambda)I(Z;Y)$ and $I(X;Y) > (1+\lambda)I(Y;Z)$, then $Z_r = Z$ is Charlie's best response for $\tilde{Y} = Y_+^\star$.

$$U_{Charlie}(Z_r = Z) = I(Z;X) - I(Z;Y_+^\star)$$
$$U_{Charlie}(Z_r = 0) = \lambda I(Z;Y_+^\star)$$

Since $I(Z;X) = (1+\lambda)I(Z;Y^\star) > (1+\lambda)I(Z;Y_+^\star)$, it follows that

$$U_{Charlie}(Z_r = Z) > U_{Charlie}(Z_r = 0)$$

It is only left to check that for $Z_r = Z$, $P_{Y_r|Y} \notin \mathcal{B}_y$ is Bob's best response. For such case Alice constructs the codebooks according to the distribution $P_{\tilde{Y}|Y}$. We have that

$$U_{Bob}(P_{Y_r|Y} \notin \mathcal{B}_y) = I(Y_+^\star;X) - (1+\lambda)I(Y_+^\star;Z) + \lambda I(Z;Y)$$
$$U_{Bob}(Y_r = 0) = \lambda I(Z;Y)$$

From (3.14) we have that $I(Y_+^\star;X) > (1+\lambda)I(Y_+^\star;Z)$. Hence,

$$U_{Bob}(P_{Y_r|Y} \notin \mathcal{B}_y) > U_{Bob}(Y_r = 0).$$

Case 3: If $I(Z;X) > (1+\lambda)I(Z;Y)$ and $I(X;Y) \leq (1+\lambda)I(Y;Z)$, then $Y_r = Y$ is Bob's best response for $\tilde{Z} = Z_+^\star$.

$$U_{Bob}(Y_r = Y) = I(Y;X) - I(Y;Z_+^\star)$$
$$U_{Bob}(Y_r = 0) = \lambda I(Y;Z_+^\star)$$

Since $I(Y;X) = (1+\lambda)I(Y;Z^\star) > (1+\lambda)I(Y;Z_+^\star)$, it follows that

$$U_{Bob}(Y_r = Y) > U_{Bob}(Y_r = 0)$$

It is only left to check that for $Y_r = Y$, $P_{Z_r|Z} \notin \mathcal{B}_z$ is Charlie's best response. For that case Alice constructs the codebooks according to the distribution $P_{\tilde{Z}|Z}$. We have that

$$U_{Charlie}(P_{Z_r|Z} \notin \mathcal{B}_z) = I(Z_+^\star;X) - (1+\lambda)I(Z_+^\star;Y) + \lambda I(Y;Z)$$
$$U_{Charlie}(Y_r = 0) = \lambda I(Y;Z)$$

From Lemma 3.2 we have that $I(Z_+^\star; X) > (1+\lambda)I(Z_+^\star; Y)$. Hence,

$$U_{Charlie}(P_{Z_r|Z} \notin \mathcal{B}_z) > U_{Charlie}(Z_r = 0).$$

Case 4: If $I(Z;X) \leq (1+\lambda)I(Z;Y)$ and $I(X;Y) \leq (1+\lambda)I(Y;Z)$, then $P_{Y_r|Y} \notin \mathcal{B}_y$ is Bob's best response for $\tilde{Z} = Z_+^\star$:

$$\begin{aligned} U_{Bob}(P_{Y_r|Y} \notin \mathcal{B}_y) &= I(Y_+^\star; X) - (1+\lambda)I(Y_+^\star; Z_+^\star) + \lambda I(Z_+^\star; Y) \\ U_{Bob}(Y_r = 0) &= \lambda I(Z_+^\star; Y) \end{aligned}$$

$U_{Bob}(P_{Y_r|Y} \notin \mathcal{B}_y) > U_{Bob}(Y_r = 0)$ because

$$I(Y;X) = (1+\lambda)I(Y;Z^\star) \Rightarrow I(Y;X) > (1+\lambda)I(Y;Z_+^\star) \Leftrightarrow I(Y_+^\star;X) > (1+\lambda)I(Y_+^\star;Z_+^\star).$$

The last inequality follows from (3.14). It is only left to check that $P_{Z_r|Z} \notin \mathcal{B}_z$ is Charlie's best response for $\tilde{Y} = Y_+^\star$:

$$\begin{aligned} U_{Charlie}(P_{Z_r|Z} \notin \mathcal{B}_z) &= I(Z_+^\star; X) - (1+\lambda)I(Z_+^\star; Y_+^\star) + \lambda I(Y_+^\star; Z) \\ U_{Charlie}(Z_r = 0) &= \lambda I(Y_+^\star; Z) \end{aligned}$$

$U_{Charlie}(P_{Z_r|Z} \notin \mathcal{B}_z) > U_{Charlie}(Z_r = 0)$ because

$$I(Z;X) = (1+\lambda)I(Z;Y^\star) \Rightarrow I(Z;X) > (1+\lambda)I(Z;Y_+^\star) \Leftrightarrow I(Z_+^\star;X) > (1+\lambda)I(Z_+^\star;Y_+^\star).$$

The last inequality follows from Lemma 3.2.

□

Let us verify that the binary erasure example indeed satisfies the conditions of Theorem 3.3. The function $I(X;Y) - (1+\lambda)I(Y;Z_r) = (1-\epsilon) - (1+\lambda)(1-\epsilon)(1-\delta_r)$ is linear in δ_r and thus satisfies the conditions of Theorem 3.2 for game 1. Furthermore, for game 2 we have

$$I(X;Y) > (1+\lambda)I(Y;Z_r) \Leftrightarrow \delta_r > \frac{\lambda}{\lambda+1}.$$

Hence, $\mathcal{B}_z = \{\delta_r \mid \delta_r > \frac{\lambda}{\lambda+1}\}$. Similarly, we can show that $\mathcal{B}_y = \{\epsilon_r \mid \epsilon_r > \frac{\lambda}{\lambda+1}\}$. Therefore, $\epsilon^\star = \delta^\star = \frac{\lambda}{\lambda+1}$. This allows as to pick $\epsilon_+^\star = \delta_+^\star = \frac{\lambda}{\lambda+1} + \alpha$, for α small, which is consistent with our previous analysis.

3.6 Binary Symmetric Distribution

Let $X \sim Ber(\frac{1}{2})$, $Y = X \oplus E$, $Z = X \oplus D$, where $E \sim Ber(\epsilon)$ and $D \sim Ber(\delta)$, respectively. We now evaluate Theorems 3.2 and 3.3 for this special case.

3.6.1 Game 1

As pointed out in the introduction, the conditional distributions $P_{Y_r|X}$ and $P_{Z_r|X}$ are modeled as binary symmetric channels: $Y_r = X \oplus E_r$ where $E_r \sim Ber(\epsilon_r)$ such that $\epsilon \leq \epsilon_r \leq \frac{1}{2}$, and $Z_r = X \oplus D_r$ where $D_r \sim Ber(\delta_r)$ such that $\delta \leq \delta_r \leq \frac{1}{2}$. Setting $U = V = 0$ in Theorem 3.1 we obtain

$$\begin{aligned}
R_{AB} &= h(\epsilon_r + \delta_r - 2\epsilon_r\delta_r) - h(\epsilon_r), \\
R_{AB}^L &= h(\epsilon_r + \delta_r - 2\epsilon_r\delta_r) - h(\epsilon_r + \delta - 2\epsilon_r\delta), \\
R_{AC} &= h(\epsilon_r + \delta_r - 2\epsilon_r\delta_r) - h(\delta_r), \\
R_{AC}^L &= h(\epsilon_r + \delta_r - 2\epsilon_r\delta_r) - h(\epsilon + \delta_r - 2\epsilon\delta_r),
\end{aligned}$$

where $h(x) = -(1-x)\log_2(1-x) - x\log_2 x$. To check that the conditions of the Lemmas 3.1 and 3.2 are met, we consider the function R_y:

$$R_y(\epsilon_r) = h(\epsilon_r + \delta_r - 2\epsilon_r\delta_r) - h(\epsilon_r) - \lambda, \quad \text{for } \epsilon \leq \epsilon_r \leq \frac{1}{2}.$$

It is easy to verify that $R_y(\epsilon)$ is on the boundary of the convex hull of S_y for all δ_r. Similarly, we can show that $R_z(\delta)$ is on the boundary of the convex hull of S_z for all ϵ_r. Applying the results of Theorem 3.2, we characterize the Nash equilibrium for this problem as follows

$$(\epsilon_r, \delta_r) = \begin{cases}
(\epsilon, \delta) & \text{if } \delta > \frac{h^{-1}(\frac{\lambda+h(\epsilon)}{\lambda+1})-\epsilon}{1-2\epsilon}, \; \epsilon > \frac{h^{-1}(\frac{\lambda+h(\delta)}{\lambda+1})-\delta}{1-2\delta} \\
(\epsilon, \frac{1}{2}) & \text{if } \delta < \frac{h^{-1}(\frac{\lambda+h(\epsilon)}{\lambda+1})-\epsilon}{1-2\epsilon}, \; \epsilon > \frac{h^{-1}(\frac{\lambda+h(\delta)}{\lambda+1})-\delta}{1-2\delta} \\
(\frac{1}{2}, \delta) & \text{if } \delta > \frac{h^{-1}(\frac{\lambda+h(\epsilon)}{\lambda+1})-\epsilon}{1-2\epsilon}, \; \epsilon < \frac{h^{-1}(\frac{\lambda+h(\delta)}{\lambda+1})-\delta}{1-2\delta} \\
(\epsilon, \frac{1}{2}) \text{ and } (\frac{1}{2}, \delta) & \text{if } \delta < \frac{h^{-1}(\frac{\lambda+h(\epsilon)}{\lambda+1})-\epsilon}{1-2\epsilon}, \; \epsilon < \frac{h^{-1}(\frac{\lambda+h(\delta)}{\lambda+1})-\delta}{1-2\delta}
\end{cases}$$

3.6.2 Game 2

In order to ensure that Bob and Charlie's honest reporting is a Nash equilibrium, it may be tempting to proceed by analogy to the BEC example and let Alice use the following:

$$(\tilde{\epsilon},\tilde{\delta}) = \begin{cases} (\epsilon_r,\delta_r) & \text{if } \epsilon_r > \epsilon^\star,\ \delta_r > \delta^\star \\ (\epsilon_r,\delta_+^\star) & \text{if } \epsilon_r > \epsilon^\star,\ \delta_r \le \delta^\star \\ (\epsilon_+^\star,\delta_r) & \text{if } \epsilon_r \le \epsilon^\star,\ \delta_r > \delta^\star \\ (\epsilon_+^\star,\delta_+^\star) & \text{if } \epsilon_r \le \epsilon^\star,\ \delta_r \le \delta^\star \end{cases}$$

where $\epsilon^\star$ and $\delta^\star$ are derived from the equations (3.31) and (3.32):

$$I(Z;X) = (1+\lambda)I(Z;Y^\star) \Leftrightarrow 1-h(\delta) = (1+\lambda)(1-h(\epsilon^\star+\delta-2\epsilon^\star\delta)) \tag{3.19}$$

$$I(Y;X) = (1+\lambda)I(Y;Z^\star) \Leftrightarrow 1-h(\epsilon) = (1+\lambda)(1-h(\delta^\star+\epsilon-2\delta^\star\epsilon)). \tag{3.20}$$

Hence,

$$\epsilon^\star = \frac{h^{-1}(\frac{\lambda+h(\delta)}{\lambda+1})-\delta}{1-2\delta}, \quad \delta^\star = \frac{h^{-1}(\frac{\lambda+h(\epsilon)}{\lambda+1})-\epsilon}{1-2\epsilon}. \tag{3.21}$$

This result directly follows from Theorem 3.3.

In the binary erasure example, we had that $\epsilon^\star = \frac{\lambda}{\lambda+1}$ and $\delta^\star = \frac{\lambda}{\lambda+1}$ do not depend on the true parameters ϵ and δ. However, this is not the case here (see (3.21)). Therefore, for the binary symmetric case, Alice's strategy depends on the true distributions which is not acceptable by the definition of Game 2.

To get around this problem, Alice can construct $\epsilon_+^\star$ and $\delta_+^\star$ such that they do not depend on the true parameters ϵ and δ. To that end, we propose a crude upper bound

$$1.4(1+\lambda)(1-h(\epsilon))(1-h(\delta)) > (1+\lambda)h(\epsilon+\delta-2\epsilon\delta).$$

Applying this inequality to (3.19) and (3.20) we obtain

$$1-h(\delta) > 1.4(1+\lambda)(1-h(\epsilon^\star))(1-h(\delta)) \Rightarrow 1-h(\delta) > (1+\lambda)h(\epsilon+\delta-2\epsilon\delta) \tag{3.22}$$

$$1-h(\epsilon) > 1.4(1+\lambda)(1-h(\delta^\star))(1-h(\epsilon)) \Rightarrow 1-h(\epsilon) > (1+\lambda)h(\epsilon+\delta-2\epsilon\delta) \tag{3.23}$$

From (3.22) and (3.23) it follows that

$$\epsilon^\star < h^{-1}\left(\frac{\lambda+\frac{2}{7}}{\lambda+1}\right), \quad \delta^\star < h^{-1}\left(\frac{\lambda+\frac{2}{7}}{\lambda+1}\right). \tag{3.24}$$

Therefore, we can set

$$\epsilon_+^\star = h^{-1}\left(\frac{\lambda+\frac{2}{7}}{\lambda+1}\right), \quad \delta_+^\star = h^{-1}\left(\frac{\lambda+\frac{2}{7}}{\lambda+1}\right). \tag{3.25}$$

Applying the results of Theorem 3.3, Alice constructs the codebooks using the following parameters:

$$(\tilde{\epsilon},\tilde{\delta}) = \begin{cases} (\epsilon_r,\delta_r) & \text{if } \epsilon_r > h^{-1}\left(\frac{\lambda+\frac{2}{7}}{\lambda+1}\right) \text{ and } \delta_r > h^{-1}\left(\frac{\lambda+\frac{2}{7}}{\lambda+1}\right) \\ (\epsilon_r, h^{-1}\left(\frac{\lambda+\frac{2}{7}}{\lambda+1}\right)) & \text{if } \epsilon_r > h^{-1}\left(\frac{\lambda+\frac{2}{7}}{\lambda+1}\right) \text{ and } \delta_r \leq h^{-1}\left(\frac{\lambda+\frac{2}{7}}{\lambda+1}\right) \\ (h^{-1}\left(\frac{\lambda+\frac{2}{7}}{\lambda+1}\right), \delta_r) & \text{if } \epsilon_r \leq h^{-1}\left(\frac{\lambda+\frac{2}{7}}{\lambda+1}\right) \text{ and } \delta_r > h^{-1}\left(\frac{\lambda+\frac{2}{7}}{\lambda+1}\right) \\ (h^{-1}\left(\frac{\lambda+\frac{2}{7}}{\lambda+1}\right), h^{-1}\left(\frac{\lambda+\frac{2}{7}}{\lambda+1}\right)) & \text{if } \epsilon_r \leq h^{-1}\left(\frac{\lambda+\frac{2}{7}}{\lambda+1}\right) \text{ and } \delta_r \leq h^{-1}\left(\frac{\lambda+\frac{2}{7}}{\lambda+1}\right) \end{cases}$$

Since we have selected such a crude bound, for $\lambda = 0$ or when Bob and Charlie are maximizing their key rates only, Alice's mechanism design will not accept Bob and Charlie's honest reporting when $\epsilon < h^{-1}(\frac{2}{7})$ or $\delta < h^{-1}(\frac{2}{7})$. Therefore, we incorporate this special case to Alice's strategy in Game 2:

$$(\tilde{\epsilon},\tilde{\delta}) = \begin{cases} (\epsilon_r,\delta_r) & \text{if } \epsilon_r > h^{-1}\left(\frac{\lambda+\frac{2}{7}}{\lambda+1}\right) \text{ and } \delta_r > h^{-1}\left(\frac{\lambda+\frac{2}{7}}{\lambda+1}\right) \text{ or } \lambda = 0 \\ (\epsilon_r, h^{-1}\left(\frac{\lambda+\frac{2}{7}}{\lambda+1}\right)) & \text{if } \epsilon_r > h^{-1}\left(\frac{\lambda+\frac{2}{7}}{\lambda+1}\right) \text{ and } \delta_r \leq h^{-1}\left(\frac{\lambda+\frac{2}{7}}{\lambda+1}\right) \text{ and } \lambda \neq 0 \\ (h^{-1}\left(\frac{\lambda+\frac{2}{7}}{\lambda+1}\right), \delta_r) & \text{if } \epsilon_r \leq h^{-1}\left(\frac{\lambda+\frac{2}{7}}{\lambda+1}\right) \text{ and } \delta_r > h^{-1}\left(\frac{\lambda+\frac{2}{7}}{\lambda+1}\right) \text{ and } \lambda \neq 0 \\ (h^{-1}\left(\frac{\lambda+\frac{2}{7}}{\lambda+1}\right), h^{-1}\left(\frac{\lambda+\frac{2}{7}}{\lambda+1}\right)) & \text{if } \epsilon_r \leq h^{-1}\left(\frac{\lambda+\frac{2}{7}}{\lambda+1}\right) \text{ and } \delta_r \leq h^{-1}\left(\frac{\lambda+\frac{2}{7}}{\lambda+1}\right) \text{ and } \lambda \neq 0 \end{cases}$$

Like in the binary erasure example, Alice's strategy does not depend any more on the true parameters ϵ and δ. Hence, it can be applied when that information is not available to anybody.

3.7 Privacy Considerations

So far we have assumed that Bob and Charlie's utility functions depend on their desire of being legitimate users or eavesdroppers. In this section we briefly analyze the setting where Bob and Charlie are concerned about how much of the key they agreed upon with Alice leaks to the other player. To address this, for both games, we consider the following utility functions for Bob and Charlie, respectively:

$$\begin{aligned} U_{Bob} &= R_{AB} + \lambda_1 R^L_{AC} - \lambda_2 R^L_{AB}, \quad \text{for some } P_{Y_r|Y} \\ U_{Charlie} &= R_{AC} + \lambda_1 R^L_{AB} - \lambda_2 R^L_{AC}, \quad \text{for some } P_{Z_r|Z}, \end{aligned} \tag{3.26}$$

where $\lambda_1 \geq 0,\ \lambda_2 \geq 0$. The analysis of Games 1 and 2 for the utility functions given in equation (3.26) proceeds along the same lines as the one given in Section 3.5.

3.7.1 Game 1

Using the same notation as in Section 3.5, we define the function $\mathcal{R}_y : \mathcal{P}_{Y_r} \mapsto \mathbb{R}$ given by

$$R_y(P_{Y_r}) = I(Y_r; X) - (1 + \lambda_1 - \lambda_2) I(Y_r; Z_r) - \lambda_2 I(Y_r; Z), \tag{3.27}$$

and the set

$$\begin{aligned} S_y = \{(P_{Y_r}, t) \mid P_{Y_r} \in \mathcal{P}_{Y_r},\ & t \leq R_y(P_{Y_r}) \text{ if } R_y(P_{Y_r}) \geq 0,\ t \geq 0, \\ & t \geq R_y(P_{Y_r}) \text{ if } R_y(P_{Y_r}) < 0,\ t < 0\} \end{aligned} \tag{3.28}$$

Similarly, we define the function $\mathcal{R}_z : \mathcal{P}_{Z_r} \mapsto \mathbb{R}$ given by

$$R_z(P_{Z_r}) = I(Z_r; X) - (1 + \lambda_1 - \lambda_2) I(Z_r; Y_r) - \lambda_2 I(Z_r; Y), \tag{3.29}$$

and the set

$$\begin{aligned} S_z = \{(P_{Z_r}, t) \mid P_{Z_r} \in \mathcal{P}_{Z_r},\ & t \leq R_z(P_{Z_r}) \text{ if } R_z(P_{Z_r}) \geq 0,\ t \geq 0, \\ & t \geq R_z(P_{Z_r}) \text{ if } R_z(P_{Z_r}) < 0,\ t < 0\} \end{aligned} \tag{3.30}$$

Based on the results from Section 3.5, we now characterize a Nash equilibrium for the special class of discrete memoryless source distributions for which the Markoc chain $Y - X - Z$ holds.

Theorem 3.4. *For a given joint distribution P_{XYZ}, if $(P_Y, \mathcal{R}_y(P_Y))$ and $(P_Z, \mathcal{R}_z(P_Z))$ are on the boundary of the convex hull of the sets S_y and S_z, respectively, then a Nash equilibrium for Game*

1 can be characterized as follows:

$$(Y_r, Z_r) = \begin{cases} (Y, Z) & \textit{if} \quad I(X;Y) > (1+\lambda_1)I(Y;Z) \textit{ and } I(Z;X) > (1+\lambda_1)I(Z;Y) \\ (Y, 0) & \textit{if} \quad I(X;Y) > (1+\lambda_1)I(Y;Z) \textit{ and } I(Z;X) < (1+\lambda_1)I(Z;Y) \\ (0, Z) & \textit{if} \quad I(X;Y) < (1+\lambda_1)I(Y;Z) \textit{ and } I(Z;X) > (1+\lambda_1)I(Z;Y) \\ (Y,0),(0,Z) & \textit{if} \quad I(X;Y) < (1+\lambda_1)I(Y;Z) \textit{ and } I(Z;X) < (1+\lambda_1)I(Z;Y) \end{cases}$$

where Y_r and Z_r correspond to the distributions $P_{Y_r|Y}$ and $P_{Z_r|Z}$, respectively.

Interestingly, the Nash equilibrium described in Theorem 3.4 is exactly the same as that described in Theorem 3.2 when the privacy of each key was not considered. However, for Game 2 this is not the case.

3.7.2 Game 2

Like in Section 3.5, we define $\mathcal{B}_y$ and $\mathcal{B}_z$ as follows

$$\mathcal{B}_y = \{P_{Y_r|Y} \mid I(Z;X) - \lambda_2 I(Z;Y) > (1+\lambda_1-\lambda_2)I(Z;Y_r)\},$$
$$\mathcal{B}_z = \{P_{Z_r|Z} \mid I(Y;X) - \lambda_2 I(Y;Z) > (1+\lambda_1-\lambda_2)I(Y;Z_r)\}.$$

Definition 3.8. Let $Y^\star$ correspond to distribution $P_{Y^\star|Y}$ such that

$$I(Z;X) - \lambda_2 I(Z;Y) = (1+\lambda_1-\lambda_2)I(Z;Y^\star). \tag{3.31}$$

Similarly, $Z^\star$ correspond to distribution $P_{Z^\star|Z}$ such that

$$I(Y;X) - \lambda_2 I(Y;Z) = (1+\lambda_1-\lambda_2)I(Y;Z^\star). \tag{3.32}$$

Theorem 3.5. *For a given joint distribution P_{XYZ}, if $(P_Y, \mathcal{R}_y(P_Y))$ and $(P_Z, \mathcal{R}_z(P_Z))$ are on the boundary of the convex hull of the sets S_y and S_z, respectively, then Alice ensures that Bob and Charlie's honest reporting is a Nash equilibrium by constructing the keys K_{AB} and K_{AC} based on the following distributions:*

$$(P_{\tilde{Y}|Y}, P_{\tilde{Z}|Z}) = \begin{cases} (P_{Y_r|Y}, P_{Z_r|Z}) & \textit{if } P_{Y_r|Y} \in \mathcal{B}_y,\ P_{Z_r|Z} \in \mathcal{B}_z \\ (P_{Y_r|Y}, P_{Z^\star_+|Z}) & \textit{if } P_{Y_r|Y} \in \mathcal{B}_y,\ P_{Z_r|Z} \notin \mathcal{B}_z \\ (P_{Y^\star_+|Y}, P_{Z_r|Z}) & \textit{if } P_{Y_r|Y} \notin \mathcal{B}_y,\ P_{Z_r|Z} \in \mathcal{B}_z \\ (P_{Y^\star_+|Y}, P_{Z^\star_+|Z}) & \textit{if } P_{Y_r|Y} \notin \mathcal{B}_y,\ P_{Z_r|Z} \notin \mathcal{B}_z \end{cases}$$

where $P_{Y^\star_+|Y}$ and $P_{Z^\star_+|Z}$ are chosen such that $P_{Y^\star_+|Y} \in \mathcal{B}_y$ and $P_{Z^\star_+|Z} \in \mathcal{B}_z$.

3.7.3 Binary Erasure Distribution

In Theorem 3.4 we showed equivalence between Nash equilibria for the utility functions defined in (3.1) and (3.26) when Bob and Charlie know distributions P_{XY} and P_{XZ}, respectively (Game 1). Therefore, here we only consider Game 2 setting when source observations are modeled as binary erasure channels. Applying Definition 3.8 we obtain $\epsilon^\star$ and $\delta^\star$ as follows:

$$\epsilon^\star = \frac{\lambda_1 - \lambda_2 \epsilon}{1 + \lambda_1 - \lambda_2}, \quad \delta^\star = \frac{\lambda_1 - \lambda_2 \delta}{1 + \lambda_1 - \lambda_2}. \tag{3.33}$$

Now, $\epsilon^\star$ and $\delta^\star$ depend on the true erasure probabilities ϵ and δ, which is not acceptable according to the definition of Game 2. Therefore, we construct upper bounds $\epsilon^\star_+$ and $\delta^\star_+$, which are not the functions of ϵ and δ, as follows:

$$\epsilon^\star_+ = \frac{\lambda_1}{1 + \lambda_1 - \lambda_2}, \quad \delta^\star_+ = \frac{\lambda_1}{1 + \lambda_1 - \lambda_2}. \tag{3.34}$$

Applying the results of Theorem 3.5, Alice constructs the codebooks using the following parameters:

$$(\tilde{\epsilon}, \tilde{\delta}) = \begin{cases} (\epsilon_r, \delta_r) & \text{if } \epsilon_r > \frac{\lambda_1}{1+\lambda_1-\lambda_2} \text{ and } \delta_r > \frac{\lambda_1}{1+\lambda_1-\lambda_2} \\ (\epsilon_r, \frac{\lambda_1}{1+\lambda_1-\lambda_2}) & \text{if } \epsilon_r > \frac{\lambda_1}{1+\lambda_1-\lambda_2} \text{ and } \delta_r \leq \frac{\lambda_1}{1+\lambda_1-\lambda_2} \\ (\frac{\lambda_1}{1+\lambda_1-\lambda_2}, \delta_r) & \text{if } \epsilon_r \leq \frac{\lambda_1}{1+\lambda_1-\lambda_2} \text{ and } \delta_r > \frac{\lambda_1}{1+\lambda_1-\lambda_2} \\ (\frac{\lambda_1}{1+\lambda_1-\lambda_2}, \frac{\lambda_1}{1+\lambda_1-\lambda_2}) & \text{if } \epsilon_r \leq \frac{\lambda_1}{1+\lambda_1-\lambda_2} \text{ and } \delta_r \leq \frac{\lambda_1}{1+\lambda_1-\lambda_2} \end{cases}$$

3.8 Multiterminal Key Agreement

In this section we consider the scenario in which Alice and m other users observe discrete memoryless sources X^n, Y_1^n, Y_2^n,...,Y_m^n generated according to

$$P_{X^nY_1^n...Y_m^n} = \prod_{i=1}^{n} P_{X_iY_{1,i}...Y_{m,i}}$$

Alice wants to agree with user i on a key K_i that is perfectly secret from the remaining $m-1$ users. We again consider the scenario where m users report sufficient information about their observations to Alice over a public channel. Alice estimates the joint pmf and constructs the codebooks for the key agreement. Like in the previous sections, the reports are modeled in the shape of fictitious memoryless channels $P_{Z_i|Y_i}$, where $i = 1, ..., m$.

Before we proceed with the analysis of this problem we define a multi-user version of the leakage rate.

Definition 3.9. The multi-user leakage rate $R_i^{L,l}$, $l = 1, ..., m$, $l \neq i$, for key K_i is defined to be

$$R_i^{L,l} = \frac{1}{n} I(K_i; g, Y^n) \tag{3.35}$$

where g corresponds to all transmissions over the public channel. It models a part of the key K_i that User l may be abe to decode.

For simplicity, we study the case where the Markov chain $Y_i - X - Y_j$, $i \neq j$ holds. Under this condition it is straightforward to show the following achievability result

Theorem 3.6. *The following key rate - multi-user leakage rate tuples are achievable:*

$$\begin{aligned} R_i &\leq I(Z_i; X) - \max_{j \neq i} I(Z_i; Z_j) \\ R_i^{L,l} &\leq \{I(Z_i; Y_l) - \max_{j \neq i} I(Z_i; Z_j)\}_+, \quad l = 1, ..., m, \ l \neq i \end{aligned}$$

for $i = 1, ..., m$.

We study the case where user i selects the channel $P_{Z_i|Y_i}$ based on a utility function

$$U_i = R_i + \lambda \sum_{j \neq i} R_j^{L,i}$$

3.8.1 Binary Erasure Example

In this example Alice observes $X \sim Ber(\frac{1}{2})$, while m users observe erased versions of Alice's observations with erasure probabilities ϵ_i, $i = 1, ..., m$. User i reports to Alice erasure probability δ_i, where $\epsilon_i \leq \delta_i \leq 1$.

Applying Theorem 3.6 we have that the following rates are achievable

$$\begin{aligned} R_i &= \min_{j\neq i} \delta_j(1-\delta_i) \\ R_i^{L,l} &= \min_{j\neq i}(\delta_j-\epsilon_l)(1-\delta_i), \quad l\neq i \end{aligned}$$

Therefore, player i chooses δ_i based on the utility function:

$$U_i = \min_{j\neq i} \delta_j(1-\delta_i) + \lambda \sum_{j\neq i} \{\min_{l\neq j}(\delta_l-\epsilon_i)(1-\delta_j)\}_+ \tag{3.36}$$

In this problem we restrict our attention to characterizing the region where honest reporting by all players is the unique Nash equilibrium. Then, applying the same strategy as in the Game 2, Alice can ensure that honest reporting by all players is the unique Nash equilibrium when the joint pmf is not available to anyone. To build our intuition for an arbitrary number of players, we start with $m = 3$.

Proposition 3.1. For $m = 3$, if

$$\epsilon_i > \begin{cases} \frac{\lambda}{\lambda+1} & \text{when } \lambda \in [0,1] \\ \frac{\lambda}{\lambda+\frac{1}{2}} & \text{when } \lambda > 1 \end{cases}$$

for $i = 1, 2, 3$, then honest reporting by all users is the unique Nash equilibrium.

Remark 3.2. The ϵ_i region, for $i = 1, 2, 3$ defined in Proposition 3.1 provides only sufficient condition for honesty to hold.

Proof. This proof contains two parts. First, we show that honest reporting by all players is a Nash equilibrium. In the second part of the proof we show the uniqueness of that equilibrium by analyzing all possible responses of the players. Without loss of generality let us assume $\epsilon_1 \leq \epsilon_2 \leq \epsilon_3$. The utility functions of users 1, 2 and 3 are:

$$U_1(\delta_1) = \min\{\delta_2,\delta_3\}(1-\delta_1) + \lambda(\min\{\delta_1,\delta_3\}-\epsilon_1)(1-\delta_2) + \lambda(\min\{\delta_1,\delta_2\}-\epsilon_1)(1-\delta_3) \tag{3.37}$$

$$U_2(\delta_2) = \min\{\delta_1,\delta_3\}(1-\delta_2) + \lambda(\min\{\delta_2,\delta_3\}-\epsilon_2)(1-\delta_1) + \lambda(\min\{\delta_1,\delta_2\}-\epsilon_2)(1-\delta_3) \tag{3.38}$$

$$U_3(\delta_3) = \min\{\delta_1,\delta_2\}(1-\delta_3) + \lambda(\min\{\delta_2,\delta_3\}-\epsilon_3)(1-\delta_1) + \lambda(\min\{\delta_1,\delta_3\}-\epsilon_3)(1-\delta_2) \tag{3.39}$$

Let us start by writing conditions for User 3 to be honest ($\delta_3 = \epsilon_3$) assuming that users 1 and 2 reported their erasure probabilities honestly, *i.e.* $\delta_1 = \epsilon_1$ and $\delta_2 = \epsilon_2$. Due to the linearity of $U_3(\delta_3)$, the only two candidates are $\delta_3 = \epsilon_3$ or $\delta_3 = 1$. Evaluating U_3 in (3.39) for $\delta_3 = \epsilon_3$ and

$\delta_3 = 1$, respectively, we find:

$$U_3(\delta_3 = \epsilon_3) = \epsilon_1(1 - \epsilon_3)$$
$$U_3(\delta_3 = 1) = 0$$

Therefore, User 3 has no incentive to switch from $\delta_3 = \epsilon_3$ to $\delta_3 = 1$.

For User 2, setting $\delta_1 = \epsilon_1$ and $\delta_3 = \epsilon_3$, the utility $U_2(\delta_2)$ can be evaluated at $\delta_2 = \epsilon_2$ and $\delta_2 = 1$ as:

$$U_2(\delta_2 = \epsilon_2) = \epsilon_1(1 - \epsilon_2) \tag{3.40}$$
$$U_2(\delta_2 = 1) = \lambda(\epsilon_3 - \epsilon_2)(1 - \epsilon_1) \tag{3.41}$$

In order for honest reporting by User 2 to be a Nash equilibrium the following inequality has to hold:

$$U_2(\delta_2 = \epsilon_2) \geq U_2(\delta_2 = 1) \tag{3.42}$$

Substituting for $U_2(\delta_2 = \epsilon_2)$ and $U_2(\delta_2 = 1)$ from (3.40) and (3.41) into (3.42) one obtains

$$U_2(\delta_2 = \epsilon_2) \geq U_2(\delta_2 = 1) \Leftrightarrow \epsilon_1 - \lambda\epsilon_3(1 - \epsilon_1) \geq \epsilon_2[\epsilon_1 - \lambda(1 - \epsilon_1)]$$

Since $\epsilon_1 - \lambda\epsilon_3(1-\epsilon_1) \geq \epsilon_1 - \lambda(1-\epsilon_1)$ is always true, User 2 will report his observations honestly if $\epsilon_1 > \frac{\lambda}{\lambda+1}$.

For User 1, setting $\delta_2 = \epsilon_2$ and $\delta_3 = \epsilon_3$, the utility $U_1(\delta_1)$ can be evaluated at $\delta_2 = \epsilon_2$ and $\delta_2 = 1$ as:

$$U_1(\delta_1 = \epsilon_1) = \epsilon_2(1 - \epsilon_1)$$
$$U_1(\delta_1 = 1) = \lambda(\epsilon_3 - \epsilon_1)(1 - \epsilon_2) + \lambda(\epsilon_2 - \epsilon_1)(1 - \epsilon_3)$$

Repeating the same analysis as for User 2, we obtain

$$U_1(\delta_1 = \epsilon_1) > U_1(\delta_1 = 1) \Leftrightarrow \epsilon_2 - \lambda[\epsilon_2 + \epsilon_3 - 2\epsilon_2\epsilon_3] \geq \epsilon_2 - \lambda(2 - \epsilon_2 - \epsilon_3) \tag{3.43}$$

Since $2 - \epsilon_2 - \epsilon_3 \geq \epsilon_2 + \epsilon_3 - 2\epsilon_2\epsilon_3$ is always true, it follows from (3.43) that User 1 will report his observations honestly if

$$\epsilon_2 > \frac{\lambda\epsilon_3}{1 - \lambda + 2\lambda\epsilon_3} \tag{3.44}$$

It is straightforward to show that $\frac{\lambda\epsilon_3}{1-\lambda+2\lambda\epsilon_3} < \frac{\lambda}{\lambda+1}$ when $\lambda \in [0, 1]$, and $\frac{\lambda\epsilon_3}{1-\lambda+2\lambda\epsilon_3} < \frac{\lambda}{\lambda+\frac{1}{2}}$ when $\lambda > 1$. Combining the last two inequalities with (3.44) one obtains that $\delta_1 = \epsilon_1$ when $\epsilon_2 > \Lambda$, where

$$\Lambda = \begin{cases} \frac{\lambda}{\lambda+1} & \text{if } \lambda \in [0,1] \\ \frac{\lambda}{\lambda+\frac{1}{2}} & \text{if } \lambda > 1 \end{cases}$$

In order for $\delta_i = \epsilon_i$, $i = 1, 2, 3$, to be the unique Nash equilibrium the following inequality has to be satisfied:

$$U_i(\delta_i = \epsilon_i) \geq U_i(\delta_i = 1) \tag{3.45}$$

no matter what the other players' responses are. We only need to check end points $\delta_i = \epsilon_i$ and $\delta_i = 1$, because $U_i(\delta_i)$ is linear.

For User 3 we already analyzed the case when users 1 and 2 are honest. It is also obvious that when $\delta_1 = \delta_2 = 1$ User 3 maximizes his utility by reporting $\delta_3 = \epsilon_3$. The remaining two cases can be analyzed as follows.

If $\delta_1 = \epsilon_1$, $\delta_2 = 1$ then

$$U_3(\delta_3 = \epsilon_3) = \epsilon_1(1-\epsilon_3) \tag{3.46}$$

$$U_3(\delta_3 = 1) = \lambda(1-\epsilon_3)(1-\epsilon_1) \tag{3.47}$$

From (3.45), (3.46) and (3.47) we have

$$U_3(\delta_3 = \epsilon_3) \geq U_3(\delta_3 = 1) \Leftrightarrow \epsilon_1(1-\epsilon_3) \geq \lambda(1-\epsilon_3)(1-\epsilon_1) \Leftrightarrow \epsilon_1 \geq \frac{\lambda}{\lambda+1}$$

If $\delta_1 = 1$, $\delta_2 = \epsilon_2$ then

$$U_3(\delta_3 = \epsilon_3) = \epsilon_2(1-\epsilon_3) \tag{3.48}$$

$$U_3(\delta_3 = 1) = \lambda(1-\epsilon_3)(1-\epsilon_2) \tag{3.49}$$

From (3.45), (3.48) and (3.49) we have

$$U_3(\delta_3 = \epsilon_3) \geq U_3(\delta_3 = 1) \Leftrightarrow \epsilon_2(1-\epsilon_3) \geq \lambda(1-\epsilon_3)(1-\epsilon_2) \Leftrightarrow \epsilon_2 \geq \frac{\lambda}{\lambda+1}$$

For User 2 we again have to check only two cases (since $U_2(\delta_2)$):

If $\delta_1 = \epsilon_1$, $\delta_3 = 1$ then

$$U_2(\delta_2 = \epsilon_2) = \epsilon_1(1-\epsilon_2) \tag{3.50}$$

$$U_2(\delta_2 = 1) = \lambda(1-\epsilon_2)(1-\epsilon_1) \tag{3.51}$$

From (3.45), (3.50) and (3.51) we have

$$U_2(\delta_2 = \epsilon_2) \geq U_2(\delta_2 = 1) \Leftrightarrow \epsilon_1(1-\epsilon_2) \geq \lambda(1-\epsilon_2)(1-\epsilon_1) \Leftrightarrow \epsilon_1 \geq \frac{\lambda}{\lambda+1}$$

If $\delta_1 = 1$, $\delta_3 = \epsilon_3$ then

$$U_2(\delta_2 = \epsilon_2) = \epsilon_3(1 - \epsilon_2) \tag{3.52}$$

$$U_2(\delta_2 = 1) = \lambda(1 - \epsilon_2)(1 - \epsilon_3) \tag{3.53}$$

From (3.45), (3.52) and (3.53) we have

$$U_2(\delta_2 = \epsilon_2) \geq U_2(\delta_2 = 1) \Leftrightarrow \epsilon_3(1 - \epsilon_2) \geq \lambda(1 - \epsilon_2)(1 - \epsilon_3) \Leftrightarrow \epsilon_3 \geq \frac{\lambda}{\lambda + 1}$$

For User 1 we have:

If $\delta_2 = \epsilon_2$, $\delta_3 = 1$ then

$$U_1(\delta_1 = \epsilon_1) = \epsilon_2(1 - \epsilon_1) \tag{3.54}$$

$$U_1(\delta_1 = 1) = \lambda(1 - \epsilon_1)(1 - \epsilon_2) \tag{3.55}$$

From (3.45), (3.54) and (3.55) we have

$$U_1(\delta_1 = \epsilon_1) \geq U_1(\delta_1 = 1) \Leftrightarrow \epsilon_2(1 - \epsilon_1) \geq \lambda(1 - \epsilon_1)(1 - \epsilon_2) \Leftrightarrow \epsilon_2 \geq \frac{\lambda}{\lambda + 1}$$

If $\delta_2 = 1$, $\delta_3 = \epsilon_3$ then

$$U_1(\delta_1 = \epsilon_1) = \epsilon_3(1 - \epsilon_1) \tag{3.56}$$

$$U_1(\delta_1 = 1) = \lambda(1 - \epsilon_1)(1 - \epsilon_3) \tag{3.57}$$

From (3.45), (3.56) and (3.57) we have

$$U_1(\delta_1 = \epsilon_1) \geq U_1(\delta_1 = 1) \Leftrightarrow \epsilon_3(1 - \epsilon_1) \geq \lambda(1 - \epsilon_1)(1 - \epsilon_3) \Leftrightarrow \epsilon_3 \geq \frac{\lambda}{\lambda + 1}$$

This completes the proof. □

3.8.2 Simulations

For the three player game, the region where honest reporting by all players is a Nash equilibrium is provided in Figure 3.6; axes in this figure correspond to the true erasure probabilities. Comparing this with the results of Proposition 3.1 we can confirm that $\epsilon_i > \frac{\lambda}{\lambda+1}$ for $\lambda = \frac{1}{2}$, is indeed contained in the region shown in Figure 3.6. To see this, we break the boundaries of the region in Figure 3.6 into two parts from which it is visible that $\epsilon_i > \frac{\lambda}{\lambda+1}$ belongs to that region (see Figures 3.7 and 3.8).

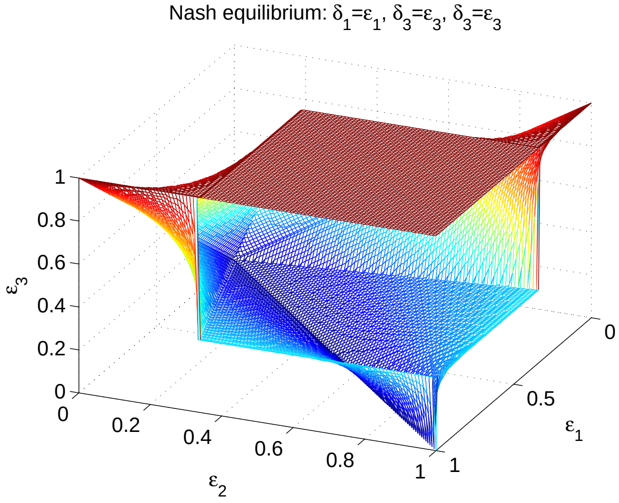

Figure 3.6: Binary erasure distribution: Region where honest reporting by all players is a Nash equilibrium. The figure shows the case $\lambda = \frac{1}{2}$

3.8.3 Generalizations of Proposition 3.1 for arbitrary number of users

Proposition 3.2. For an arbitrary number of users m, if

$$\epsilon_i > \begin{cases} \frac{\lambda}{\lambda+\frac{1}{m-2}} & \text{when } \lambda \in [0, \frac{1}{m-2}] \\ \frac{\lambda}{\lambda+\frac{1}{m-1}} & \text{when } \lambda > \frac{1}{m-2} \end{cases}$$

for $i = 1, 2, ..., m$, then honest reporting by all users is the unique Nash equilibrium.

Remark 3.3. The ϵ_i region, for $i = 1, ..., m$ defined in Proposition 3.2 provides only sufficient condition for honesty to hold.

Proof. Like in the three player game we break our proof in two parts. First, we show that honest reporting by all players is a Nash equilibrium. Without loss of generality let us assume $\epsilon_1 \leq \epsilon_2 \leq \cdots \leq \epsilon_m$. We start by writing conditions for users 3 through m to be honest assuming that all the remaining users are honest. From (3.36) we have the following

$$U_i(\delta_i = \epsilon_i) = \epsilon_1(1 - \epsilon_i)$$
$$U_i(\delta_i = 1) = 0$$

for $i = 3, 4, ..., m$. Hence, users 3 through m have no incentive to switch from $\delta_i = \epsilon_i$ to $\delta_i = 1$ where $i = 3, 4...m$.

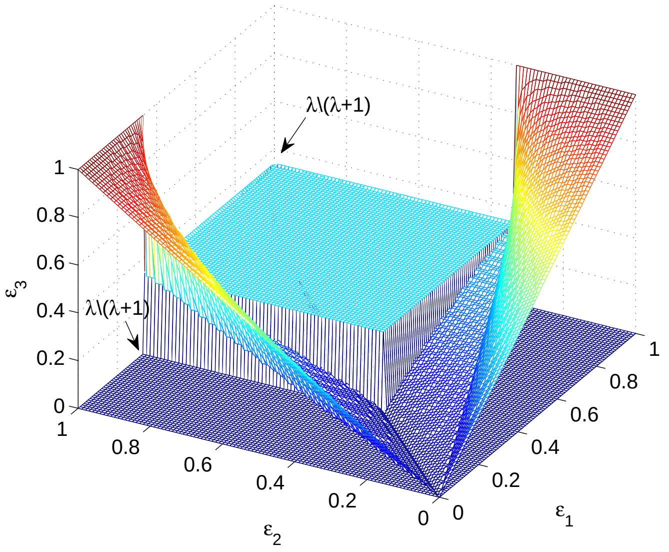

Figure 3.7: Lower boundary of the region in Figure 3.6 shows that $\epsilon_i > \frac{\lambda}{\lambda+1}$ for $i = 1, 2, 3$ and $\lambda = \frac{1}{2}$ belongs to the region where honest reporting by all players is a Nash equilibrium.

For User 2, setting $\delta_i = \epsilon_i$ where $i = 1, 3, 4, ..., m$ we have

$$U_2(\delta_2 = \epsilon_2) = \epsilon_1(1 - \epsilon_2)$$

$$U_2(\delta_2 = 1) = \lambda(\epsilon_3 - \epsilon_2)(1 - \epsilon_1)$$

Notice that $U_2(\delta_2 = \epsilon_2)$ and $U_2(\delta_2 = 1)$ are exactly the same as in proof of Proposition 3.1. Hence, in order for honest reporting by User 2 to be a Nash equilibrium $\epsilon_1 > \frac{\lambda}{\lambda+1}$ has to hold.

For User 1, setting $\delta_i = \epsilon_i$ where $i = 2, 3, ..., m$ we have

$$U_1(\delta_1 = \epsilon_1) = \epsilon_2(1 - \epsilon_1)$$

$$\begin{aligned} U_1(\delta_1 = 1) &= \lambda(\epsilon_3 - \epsilon_1)(1 - \epsilon_2) + \lambda(\epsilon_2 - \epsilon_1)(1 - \epsilon_3) + \lambda(\epsilon_2 - \epsilon_1)(1 - \epsilon_4) + \cdots + \lambda(\epsilon_2 - \epsilon_1)(1 - \epsilon_m) \\ &= \lambda(\epsilon_3 - \epsilon_1)(1 - \epsilon_2) + \lambda(\epsilon_2 - \epsilon_1)(m - 2 - s) \qquad (3.58) \end{aligned}$$

where $s = \sum_{i=3}^{m} \epsilon_i$. In order for honest reporting by User 1 to be a Nash equilibrium $U_1(\delta_1 = \epsilon_1) \geq U_1(\delta_1 = 1)$ has to hold. This condition is satisfied if

$$\epsilon_2 - \lambda\epsilon_3(1 - \epsilon_2) - \lambda\epsilon_2(m - 2 - s) \geq \epsilon_1[\epsilon_2 - \lambda(1 - \epsilon_2) - \lambda(m - 2 - s)] \qquad (3.59)$$

Since $\epsilon_2 - \lambda\epsilon_3(1 - \epsilon_2) - \lambda\epsilon_2(m - 2 - s) \geq \epsilon_2 - \lambda(1 - \epsilon_2) - \lambda(m - 2 - s)$ is always true, we have that

$$\epsilon_2 - \lambda(1 - \epsilon_2) - \lambda(m - 2 - s) \geq 0 \Rightarrow \epsilon_2 - \lambda\epsilon_3(1 - \epsilon_2) - \lambda\epsilon_2(m - 2 - s) \geq 0 \qquad (3.60)$$

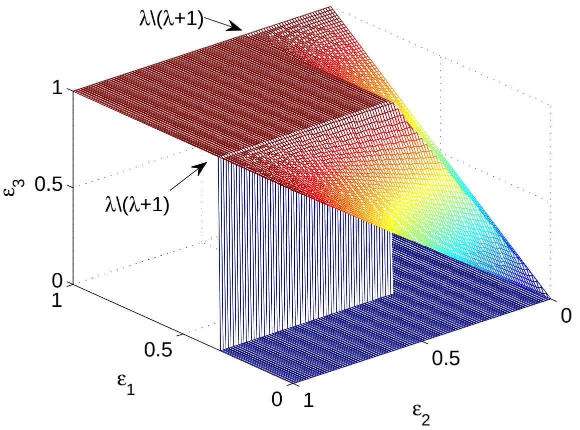

Figure 3.8: Upper boundary of the region in Figure 3.6 shows that $\epsilon_i > \frac{\lambda}{\lambda+1}$ for $i = 1, 2$ and $\lambda = \frac{1}{2}$ belongs to the region where honest reporting by all players is a Nash equilibrium.

Since $m - 2 - s \leq m - 2 - (m-2)\epsilon_2 = (m-2)(1-\epsilon_2)$ it follows that

$$\epsilon_2 - \lambda(1-\epsilon_2) - \lambda(1-\epsilon_2)(m-2) \geq 0 \Rightarrow \epsilon_2 - \lambda(1-\epsilon_2) - \lambda(m-2-s) \geq 0 \tag{3.61}$$

From (3.59), (3.60) and (3.61) it follows that if $\epsilon_2 - \lambda(1-\epsilon_2) - \lambda(1-\epsilon_2)(m-2) \geq 0$ then $\delta_1 = \epsilon_1$. The last inequality is equivalent to $\epsilon_2 > \frac{\lambda}{\lambda + \frac{1}{m-1}}$.

However from (3.59) we have that if $\epsilon_2 \geq \frac{\lambda\epsilon_3}{1+\lambda\epsilon_3-\lambda(m-2-s)}$ then $\delta_1 = \epsilon_1$. In order to prove Proposition 3.2 we need to check under which conditions

$$\frac{\lambda\epsilon_3}{1+\lambda\epsilon_3-\lambda(m-2-s)} \leq \frac{\lambda(m-2)}{\lambda(m-2)+1} \tag{3.62}$$

holds. This means that if $\epsilon_2 \geq \frac{\lambda(m-2)}{\lambda(m-2)+1}$ then $\delta_1 = \epsilon_1$. Inequality (3.62) reduces to

$$\epsilon_3(1-\lambda(m-2)^2) \leq m-2-\lambda(m-2)^2,$$

which is true whenever $m - 2 - \lambda(m-2)^2 \geq 0 \Leftrightarrow \lambda \leq \frac{1}{m-2}$. This completes the first part of the proof.

To show that honest reporting by all players is the only equilibrium under the conditions given in Proposition 3.2, we break our analysis into two cases. Let us consider User i. First we assume that at least one of the users 1 through $i-1$ is honest *i.e.* $\delta_1 = \epsilon_1$ or $\delta_2 = \epsilon_2$ or $\cdots$ or $\delta_{i-1} = \epsilon_{i-1}$ In this case utility U_i can be evaluated at $\delta_i = \epsilon_i$ and $\delta_i = 1$ as

$$U_i(\delta_i = \epsilon_i) = \min_{j=1,\dots,i-1} \delta_j(1-\epsilon_i)$$
$$U_i(\delta_i = 1) = 0$$

Hence, honest reporting by player i is his best strategy. Now, we analyze the case when $\delta_1 = \delta_2 = \cdots = \delta_{i-1} = 1$. Users $i+1$ through m can either be honest or completely lie due to the linearity of utility functions. Assuming that among these $m-i$ users, k of them are telling the truth, let us define $\epsilon_{(j)}$, $j = 1, ..., k+1$ in the following way: $\epsilon_{(1)} = \epsilon_i$, $\epsilon_{(2)}$ through $\epsilon_{(k+1)}$ are equal to the honest reports from users $i+1$ through m such that $\epsilon_{(1)} \leq \epsilon_{(2)} \leq \cdots \leq \epsilon_{(k+1)}$. Now, we have

$$\begin{aligned} U_i(\delta_i = \epsilon_i) &= \epsilon_{(2)}(1-\epsilon_{(1)}) \\ U_i(\delta_i = 1) &= \lambda(\epsilon_{(3)} - \epsilon_{(1)})(1-\epsilon_{(2)}) + \lambda(\epsilon_{(2)} - \epsilon_{(1)})(1-\epsilon_{(3)}) + \cdots + \lambda(\epsilon_{(2)} - \epsilon_{(1)})(1-\epsilon_{(k+1)}) \\ &= \lambda(\epsilon_{(3)} - \epsilon_{(1)})(1-\epsilon_{(2)}) + \lambda(\epsilon_{(2)} - \epsilon_{(1)})(k-1-r) \end{aligned} \tag{3.63}$$

where $r = \sum_{i=3}^{k+1} \epsilon_{(i)}$. Using the same analysis as in the first part of this proof, we conclude that payer i best strategy is to be honest *i.e.* $\delta_i = \epsilon_i$ if

$$\epsilon_{(2)} > \begin{cases} \frac{\lambda}{\lambda + \frac{1}{k-1}} & \text{when } \lambda \in [0, \frac{1}{k-1}] \\ \frac{\lambda}{\lambda + \frac{1}{k}} & \text{when } \lambda > \frac{1}{k-1} \end{cases}$$

for $2 \leq k \leq m-i$, $i = 1, ..., m-2$, and $\epsilon_{(2)} > \frac{\lambda}{\lambda+1}$ for $k = 1$. Upper-bounding this region we have that $\delta_i = \epsilon_i$ is the best strategy if

$$\epsilon_{(2)} > \begin{cases} \frac{\lambda}{\lambda + \frac{1}{m-2}} & \text{when } \lambda \in [0, \frac{1}{m-2}] \\ \frac{\lambda}{\lambda + \frac{1}{m-1}} & \text{when } \lambda > \frac{1}{m-2} \end{cases}$$

no matter what the remaining players' responses are. This completes the proof. □

3.8.4 Game 2

As we can see from the analysis above, the Nash equilibrium depends on the true erasure probabilities of all players. Using exactly the same approach as in Game 2 of the original problem, Alice can enforce honesty of all players, by using the following erasure probabilities to construct codebooks for key agreement:

$$\tilde{\epsilon}_i = \begin{cases} \delta_i & \text{if } \delta_i > \frac{\lambda}{\lambda + \frac{1}{m-2}} \text{ and } \lambda \in [0, \frac{1}{m-2}] \\ \frac{\lambda}{\lambda + \frac{1}{m-2}} + \alpha & \text{if } \delta_i \leq \frac{\lambda}{\lambda + \frac{1}{m-2}} \text{ and } \lambda \in [0, \frac{1}{m-2}] \end{cases}$$

$$\tilde{\epsilon}_i = \begin{cases} \delta_i & \text{if } \delta_i > \frac{\lambda}{\lambda + \frac{1}{m-1}} \text{ and } \lambda > \frac{1}{m-2} \\ \frac{\lambda}{\lambda + \frac{1}{m-1}} + \alpha & \text{if } \delta_i \leq \frac{\lambda}{\lambda + \frac{1}{m-1}} \text{ and } \lambda > \frac{1}{m-2} \end{cases}$$

for $i = 1, 2, ..., m$ and $0 < \alpha \ll 1$. It is easy to show that $(\delta_1, \delta_2, ..., \delta_m) = (\epsilon_1, \epsilon_2, ..., \epsilon_m)$ is the unique Nash equilibrium. The proof of this claim is straightforward extension of the analysis of Game 2 provided in section 3.4.2.

Chapter 4

Conclusions

In this work we studied the problem of confidential communication when different resources of randomness were available.

In Chapter 2 we observed the problem where two resources of randomness were given: the relay channel, and the source observations available at each terminal. We studied the scenario where transmitter (Alice) sends a private message to the destination (Bob), which was confidential to the relay (Eve). Alice and Bob also want to agree on a secret key that is also protected from Eve. We proposed an achievable scheme based on a separation strategy and showed that if the channel was degraded or reversely degraded [17], the secret message-secret key sum rate would be optimal.

In Chapter 3 we considered the key agreement scenario where the joint distribution of Alice, Bob and Charlie's observations was not known to Alice who constructs the codebooks for the key agreement. We studied the problem where Alice and Bob want to agree on a key that is protected from Charlie. At the same time, Alice and Charlie want to agree on a key that is protected from Bob. We further assumed that it was up to Bob and Charlie to report a sufficient information about their observations to Alice using a public channel. We modeled these reports by having Bob and Charlie select discrete memoryless channels with true observations as their inputs, and reporting a sufficient information about the outputs to Alice. Bob and Charlie picked those channels according to some objective that was a function of a key rate and the amount of information they could learn about the other user's key, called the leakage rate. We approached this problem from a game-theoretic point of view. For a class of Bob and Charlie's objective functions which were linear in the key rate and the leakage rate, we characterized a Nash equilibrium. Then, we proposed a strategy that Alice can apply in order to ensure that Bob and Charlie's honest reporting is always a Nash equilibrium. For the binary erasure source distributions we extended this concept to the multiple terminal case.

Appendix A

Appendix 1

Proof of Theorem 2.1

Proof. If $I(V_A;Y_B,\hat{Y}_E|X_E,U)-I(V_A;Y_E|X_E,U)<0$, the claim follows from theorem 7 in [17]. Therefore, we will focus on the case when $I(V_A;Y_B,\hat{Y}_E|X_E,U)-I(V_A;Y_E|X_E,U)>0$. Let us divide M_P into two parts $M_{P,a}$ and $M_{P,b}$ such that they are random variables distributed over the sets $\{1,2,...,2^{nR_{P,a}}\}$ and $\{1,2,...,2^{nR_{P,b}}\}$, where $R_{P,a}$ and $R_{P,b}$ are non-negative satisfying

$$R_P=R_{P,a}+R_{P,b}. \tag{A.1}$$

Random Coding

1. Generate $2^{n(I(V;Y_B)-\epsilon)}$ i.i.d. $\mathbf{v}$ sequences, each with probability

   $$P_{\mathbf{V}}(\mathbf{v})=\prod_{i=1}^{n}P_V(v_i).$$

   Label these $\mathbf{v}(m)$, $m\in[1,2^{n(I(V;Y_B)-\epsilon)}]$.

2. For every $\mathbf{v}(m)$ generate $2^{n(I(X_E;Y_B|V)-\epsilon)}$ i.i.d. $\mathbf{x}_E$ sequences, each with probability

   $$P_{\mathbf{X}_E|\mathbf{V}}(\mathbf{x}_E|\mathbf{v}(m))=\prod_{i=1}^{n}P_{X_E|V}(x_{Ei}|v_i(m)).$$

   Label these $\mathbf{x}_E(s|m)$, $s\in[1,2^{n(I(X_E;Y_B|V)-\epsilon)}]$.

3. For every $\mathbf{v}(m)$ generate $2^{nR_{P,a}}$ i.i.d. $\mathbf{u}$ sequences, each with probability

   $$P_{\mathbf{U}|\mathbf{V}}(\mathbf{u}|\mathbf{v}(m))=\prod_{i=1}^{n}P_{U|V}(u_i|v_i(m)).$$

   Label these $\mathbf{u}(w'|m)$, $w'\in[1,2^{nR_{P,a}}]$.

4. For every $\mathbf{u}(w'|m)$ generate $2^{n(R_S+R_{P,b})}$ i.i.d. $\mathbf{v}_A$ sequences, each with probability

$$P_{\mathbf{V}_A|\mathbf{U}}(\mathbf{v}_A|\mathbf{u}(w'|m)) = \prod_{i=1}^{n} P_{V_A|U}(v_{Ai}|u_i(w'|m)).$$

Label these $\mathbf{v}_A(j,l|m,w')$, where $j \in [1, 2^{nR_{P,b}}]$, $l \in [1, 2^{nR_S}]$. Let

$$R_{P,b} = I(V_A;Y_E|X_E,U) - \epsilon \tag{A.2}$$

5. For every $(\mathbf{x}_E(s|m), \mathbf{v}(m))$, generate $2^{n(I(\hat{Y}_E;Y_E|X_E,U)+\epsilon)}$ i.i.d. $\hat{\mathbf{y}}_E$ sequences, each with probability

$$P_{\hat{\mathbf{Y}}_E|\mathbf{X}_E,\mathbf{U}}(\hat{\mathbf{y}}_E|\mathbf{x}_E(s|m),\mathbf{u}(w'|m)) = \prod_{i=1}^{n} P_{\hat{Y}_E|X_E,U}(\hat{y}_{Ei}|x_{Ei}(s|m),u_i(w'|m)).$$

Label these $\hat{\mathbf{y}}_E(z|w',s,m)$, $z \in [1, 2^{n(I(\hat{Y}_E;Y_E|X_E,U)+\epsilon)}]$.

Random Partitions

1. Randomly partition the set $\{1,...,2^{nR_{P,a}}\}$ into $2^{n(I(V;Y_B)-\epsilon)}$ cells S_{1m}, where $m \in [1, 2^{nI(V;Y_B)}]$.

2. Randomly partition the set $\{1,...,2^{n(I(\hat{Y}_E;Y_E|X_E,U)+\epsilon)}\}$ into $2^{n(I(X_E;Y_B|V)-\epsilon)}$ cells S_{2s}, where $s \in [1, 2^{n(I(X_E;Y_B|V)-\epsilon)}]$.

Encoding

Let $w_i = (w'_i, j_i, l_i)$ be the message to be sent in block i, and assume that $(\hat{\mathbf{y}}_E(z_{i-1}|w'_{i-1}, s_{i-1}, m_{i-1}), \mathbf{y}_E(i-1), u(w'_{i-1}|m_{i-1}), \mathbf{x}_E(s_{i-1}|m_{i-1}))$ are jointly ϵ-typical and that $w'_{i-1} \in S_{1m_i}$ and $z_{i-1} \in S_{2s_i}$. Then the codeword pair $(\mathbf{x}_A(j_i,l_i|m_i,w'_i), \mathbf{x}_E(s_i|m_i))$ will be transmitted in block i, where the channel input sequence is generated from the mapping $P_{\mathbf{X}_A|\mathbf{V}_A}$.

Decoding

At the end of block i we have the following.

1. The receiver estimates m_i and s_i, by first looking for the unique ϵ-typical $\mathbf{v}(m_i)$ with $\mathbf{y}_B(i)$, then for the unique ϵ-typical $\mathbf{x}_E(s_i|m_i)$ with $(\mathbf{y}_B(i), \mathbf{v}(m_i))$. For sufficiently large n this decoding step can be done with arbitrarily small probability of error. Let the estimates of s_i and m_i be $\hat{s}_i$, $\hat{m}_i$ respectively.

2. The receiver calculates a set $L_1(\mathbf{y}_B(i-1))$ of w' such that $w' \in L_1(Y_B(i-1))$ if $(\mathbf{u}(w'|m_{i-1}), \mathbf{y}_B(i-1))$ are jointly ϵ-typical. The receiver then declares that $\hat{w}'_{i-1}$ was sent in block $i-1$ if

$\hat{w}'_{i-1} \in S_{1m_i} \cap L_1(\mathbf{y}_B(i-1))$. For sufficiently large n, $\hat{w}'_{i-1} = w'_{i-1}$ with probability arbitrarily close to one if

$$R_{P,a} \leq I(V;Y_B) + I(U;Y_B|X_E,V) - \epsilon \tag{A.3}$$

3. The receiver calculates a set $L_2(\mathbf{y}_B(i-1))$ of z such that $z \in L_2(\mathbf{y}_B(i-1))$ if $(\hat{\mathbf{y}}_E(z|\hat{w}'_{i-1}, \hat{s}_{i-1}, \hat{m}_{i-1}), \mathbf{x}_E(\hat{s}_{i-1}|\hat{m}_{i-1}), \mathbf{y}_B(i-1))$ are jointly ϵ-typical. The receiver declares that $\hat{z}_{i-1}$ was sent in block $i-1$ if $\hat{z}_{i-1} \in S_{2s_i} \cap L_2(\mathbf{y}_B(i-1))$. For sufficiently large n, $\hat{z}_{i-1} = z_{i-1}$ with probability arbitrarily close to one if

$$I(\hat{Y}_E;Y_E|X_E,U) + \epsilon < I(\hat{Y}_E;Y_B|X_E,U) + I(X_E;Y_B|V) - \epsilon.$$

Since $I(\hat{Y}_E;Y_E,Y_B|X_E,U) = I(\hat{Y}_E;Y_E|X_E,U)$ the above inequality becomes

$$I(X_E;Y_B|V) > I(\hat{Y}_E;Y_E|Y_B,X_E,U) + 2\epsilon$$

4. Using both $\hat{\mathbf{y}}_E(\hat{z}_{i-1}|\hat{w}'_{i-1}, \hat{s}_{i-1}, \hat{m}_{i-1})$ and $\mathbf{y}_B(i-1)$ the receiver declares that $(\hat{j}_{i-1}, \hat{l}_{i-1})$ was sent in block $i-1$ if $(\mathbf{v}_A(\hat{j}_{i-1}, \hat{l}_{i-1}|\hat{m}_{i-1}, \hat{w}'_{i-1}), \hat{\mathbf{y}}_E(\hat{z}_{i-1}|\hat{w}'_{i-1}, \hat{s}_{i-1}, \hat{m}_{i-1}), \mathbf{y}_B(i-1))$ are jointly ϵ-typical. $(\hat{j}_{i-1}, \hat{l}_{i-1}) = (j_{i-1}, l_{i-1})$ with probability arbitrarily close to one if

$$R_S + R_{P,b} < I(V_A;Y_B,\hat{Y}_E|X_E,U) - \epsilon \tag{A.4}$$

5. The relay upon receiving $\mathbf{y}_E(i)$ declares that $\hat{w}'_i$ was received if $(u(\hat{w}'_i|m_i), \mathbf{y}_E(i), \mathbf{x}_E(s_i|m_i))$ are jointly ϵ-typical. For sufficiently large n, $\hat{w}'_i = w'_i$ with probability arbitrarily close to one if

$$R_{P,a} < I(U;Y_E|X_E,V) \tag{A.5}$$

6. The relay also finds a z_i such that $(\hat{\mathbf{y}}_E(z_i|w'_i, s_i, m_i), \mathbf{y}_E(i), \mathbf{x}_E(s_i|m_i))$ are jointly ϵ-typical. Such z_i will exist with high probability for large n, therefore the relay knows that $z_i \in S_{2s_{i+1}}$.

Computation of Security Level

Suppose that $M_S(k)$, $W_{public,a}(k)$ and $W_{public,b}(k)$ are random variables corresponding to the transmitted messages at block k. For each block, we now establish a lower bound on $H(M_S(k)|Y_E^n(k), X_E^n(k))$.

$$\begin{aligned}
H(M_S(k)|X_E^n(k), Y_E^n(k)) &\geq H(M_S(k)|X_E^n(k), Y_E^n(k), U^n(k)) \\
&= H(M_S(k), Y_E^n(k)|X_E^n(k), U^n(k)) - H(Y_E^n(k)|X_E^n(k), U^n(k)) \\
&= H(M_S(k), Y_E^n(k), V_A^n(k)|X_E^n(k), U^n(k)) \\
&\quad - H(V_A^n(k)|X_E^n(k), M_S(k), Y_E^n(k), U^n(k)) - H(Y_E^n(k)|X_E^n(k), U^n(k)) \\
&= H(M_S(k), V_A^n(k)|X_E^n(k), U^n(k)) \\
&\quad + H(Y_E^n(k)|M_S(k), V_A^n(k), X_E^n(k), U^n(k)) \\
&\quad - H(V_A^n(k)|X_E^n(k), M_S(k), Y_E^n(k), U^n(k)) - H(Y_E^n(k)|X_E^n(k), U^n(k)) \\
&\geq H(V_A^n(k)|X_E^n(k), U^n(k)) + H(Y_E^n(k)|V_A^n(k), X_E^n(k), U^n(k)) \\
&\quad - H(V_A^n(k)|X_E^n(k), M_S(k), Y_E^n(k), U^n(k)) \\
&\quad - H(Y_E^n(k)|X_E^n(k), U^n(k)) \qquad \text{(A.6)}
\end{aligned}$$

We proceed to bound each of four terms in (A.6).

1. $H(V_A^n(k)|X_E^n(k), U^n(k)) = H(V_A^n(k)) = n(R_S + R_{P,b}) + n\epsilon$. The first equality comes from the fact that $X_E^n(k)$ is computed from the blocks received before k and therefore is independent of $V_A^n(k)$.

2. $H(Y_E^n(k)|V_A^n(k), X_E^n(k), U^n(k)) = nH(Y_E|V_A, X_E, U) + n\epsilon$, follows from the fact that channel is memoryless.

3. $H(V_A^n(k)|X_E^n(k), M_S(k), Y_E^n(k), U^n(k)) \leq n\epsilon$, follows from Fano's inequality.

4. $H(Y_E^n(k)|X_E^n(k), U^n(k)) = nH(Y_E|X_E, U) + n\epsilon$, follows from the fact that the channel is memoryless.

Substituting these results into (A.6), we get

$$\begin{aligned}
H(M_S(k)|X_E^n(k), Y_E^n(k)) &\geq n(R_S + R_{P,b}) \\
&\quad + nH(Y_E|V_A, X_E, U) - nH(Y_E|X_E, U) - 4n\epsilon \\
&= n(R_S + R_{P,b} - I(V_A; Y_E|X_E, U)) - 4n\epsilon. \qquad \text{(A.7)}
\end{aligned}$$

Therefore, using (A.2), we can write (A.7) as

$$R_S - \frac{1}{n} H(M_S(k)|X_E^n(k), Y_E^n(k)) \leq 4\epsilon \qquad \text{(A.8)}$$

and, thus, the security condition (2.1) is satisfied. Based on (A.4) it follows that

$$R_S \leq I(V_A; Y_B, \hat{Y}_E | X_E, U) - I(V_A; Y_E | X_E, U)$$

Combining (A.1), (A.2), (A.3) and (A.5) we obtain

$$R_P \leq \min\{I(V; Y_B) + I(U; Y_B | X_E, V), I(U; Y_E | X_E, V)\} + I(V_A; Y_E | X_E, U).$$

□

The following lemma is exactly the same as Lemma 2 in [13]. For the sake of completeness, we will state it here without proof.

We consider a discrete memoryless multiple source with three components with alphabets $(\mathcal{S}_A, \mathcal{S}_B, \mathcal{S}_E)$, respectively, and corresponding generic random variables (S_A, S_B, S_E), observed by Alice, Bob and Eve, respectively. We are given a noiseless public channel of capacity R. The goal is to design a key shared by Alice and Bob that is perfectly secret from Eve.

Lemma A.1. *Consider any joint distribution P_{W,S_A,S_B,S_E} satisfying the Markov chain $W - S_A - (S_B, S_E)$ such that $I(W; S_B) > I(W; S_E)$. If $R \geq I(W; S_A | S_B)$, the following secret key rate is achievable*

$$I(W; S_B) - I(W; S_E). \tag{A.9}$$

Specifically, for all $\delta > 0$ and sufficiently large n, there exists an encoding function $\psi : \mathcal{S}_A^n \to \{1, ..., 2^{nR}\}$ and decoding function $K_A : \{1, ..., 2^{nR}\} \times \mathcal{S}_A^n \to \{1, ..., 2^{n((W;S_B)-I(W;S_E)-\delta)}\}$, $K_B : \{1, ..., 2^{nR}\} \times \mathcal{S}_B^n \to \{1, ..., 2^{n((W;S_B)-I(W;S_E)-\delta)}\}$ such that

$$Pr\{K_A(\psi(S_A^n), S_A^n) \neq K_B(\psi(S_A^n), S_B^n)\} \leq \delta \tag{A.10}$$

and the following conditions are satisfied:

$$\frac{1}{n} I(K_A(\psi(S_A^n), S_A^n); \psi(S_A^n), S_E^n) \leq \delta \tag{A.11}$$

$$\frac{1}{n} I(\psi(S_A^n); S_E^n) \leq \delta \tag{A.12}$$

$$\frac{1}{n} H(K_A(\psi(S_A^n), S_A^n)) \geq I(W; S_B) - I(W; S_E) - 2\delta \tag{A.13}$$

$$\frac{1}{n} H(\psi(S_A^n)) \geq I(W; S_A | S_B) - \delta \tag{A.14}$$

Proof of Theorem 2.2

Proof. We will now use Theorem 2.1 and Lemma A.1 to prove our achievability result. We consider two cases depending on whether R_M is larger than R_S in Theorem 2.1.

Case 1. If $R_M \geq R_S$, we split the secret message into two independent parts $M = (M_{SBP}, M_{PBP})$ of rates $R_{SBP} - \delta$ and $R'_M - \delta = R_M - R_{PBP} - \delta$, respectively. Let us denote the key generated by Alice by K_A. Let us split this key into two independent parts $K = (K_1, K_2)$ of alphabet sizes 2^{nR_K} and $2^{nR'_M}$, respectively. Now, we can write

$$\begin{aligned} R_K + R'_M &= R_K + R_M - R_{SBP} \\ &= \{I(W;S_B) - I(W;S_E)\}_+ \end{aligned}$$

Now, we can set

$$\begin{aligned} M_S &= M_{SBP} \\ M_P &= (\psi(S_A^n), K_2 \oplus M_{PBP}) \end{aligned}$$

where $\oplus$ is a bit-wise XOR. In choosing M_P as above, we have to make sure that

$$\begin{aligned} R_{PBP} - I(W;S_A|S_B) - R'_{SM} &= R_{PBP} + R_{SBP} - I(W;S_A|S_B) - R_S M \\ &= \min\{I(V;Y_B) + I(U;Y_B|X_E,V), I(U;Y_E|X_E,V)\} + I(V_A;Y_B,\hat{Y}_E|X_E,U) \\ &\quad - I(W;S_A|S_B) - R_{SM} \\ &\geq 0 \end{aligned}$$

where inequality follows from (2.12). With high probability, Bob can recover (M_S, M_P) (by Theorem 2.1) and $K_A = (K_1, K_2)$ (by Lemma A.1). Bob declares K_1 to be the secret key. He also recovers M_{PBP} by undoing the bit-wise XOR and thus can output M. It is straightforward to show that the key satisfies uniformity conditions and that the secrecy constraints are met (see [13]).

Case 2. If $R_M < R_S$ and $I(W;S_A|S_B) \geq R_S - R_M$, we split $\psi(S_A^n)$ into two parts $\psi(S_A^n) = (\psi_{SBP}, \psi_{PBP})$ such that their alphabets are $\{1, 2, ..., 2^{n(R_S - R_M)}\}$ and $\{1, 2, ..., 2^{n(I(W;S_A|S_B) - R_S + R_M)}\}$, respectively. In doing this, we made use of Theorem 2.1 which implies that

$$\begin{aligned} R_P + R_S - I(W;S_A|S_B) - R_M = \min\{&I(V;Y_B) + I(U;Y_B|X_E,V), I(U;Y_E|X_E,V)\} \\ &+ I(V_A;Y_B,\hat{Y}_E|X_E,U) - I(W;S_A|S_B) - R_M \geq 0 \end{aligned}$$

If $I(W;S_A|S_B) \leq R_S - R_M$, we define $\psi_{SBP} = \psi(S_A^n)$ and $\psi_{PBP} = 0$. Now, we make the following choice

$$\begin{aligned} M_S &= (M, \psi_{SBP}) \\ M_P &= \psi_{PBP} \end{aligned}$$

By Theorem 2.1, Bob recovers the secret message M and the pair (ψ_{SBP}, ψ_{PBP}), and therefore K_A with high probability. In this case, we define secret key as $K = (\psi_{SBP}, K_A)$. Following the similar steps as in [13] uniformity and secrecy conditions are easily verifiable. Since the key is defined as above, we have

$$R_K = \{I(W;S_B) - I(W;S_E)\}_+ + R_S - R_M.$$

In other words

$$R_K = \{I(W;S_B) - I(W;S_E)\}_+ + \{I(V_A;Y_B,\hat{Y}_E|X_E,U) - I(V_A;Y_E|X_E,U)\}_+ - R_M.$$

□

Proof of Theorem 2.3

Proof. Let Q be uniformly distributed over $\{1,2,...,n\}$ and independent of all other random variables. Then, we have

$$\begin{aligned}
&nI(X_{A,Q},X_{E,Q};Y_{E,Q},Y_{B,Q}|Q)\\
&\geq I(X_A^n,X_E^n;Y_E^n,Y_B^n)\\
&= I(M,K,S_A^n,X_A^n,X_E^n;Y_E^n,Y_B^n)\\
&\geq I(M,K,S_A^n,X_E^n;Y_E^n,Y_B^n)\\
&\geq I(M,K,S_A^n,X_E^n;Y_E^n,Y_B^n) - I(S_B^n,S_E^n;Y_E^n,Y_B^n)\\
&= I(M,K,S_A^n,S_B^n,S_E^n,X_E^n;Y_E^n,Y_B^n) - I(S_B^n,S_E^n;Y_E^n,Y_B^n) && \text{(A.15)}\\
&= I(M,K,S_A^n,X_E^n;Y_E^n,Y_B^n|S_B^n,S_E^n)\\
&= I(M;Y_E^n,Y_B^n|S_B^n,S_E^n)\\
&\quad + I(K,S_A^n,X_E^n;Y_E^n,Y_B^n|S_B^n,S_E^n,M)\\
&= H(M|S_B^n,S_E^n) + I(K,S_A^n,X_E^n;Y_E^n,Y_B^n|S_B^n,S_E^n,M) && \text{(A.16)}\\
&= H(M) + I(K,S_A^n,X_E^n;Y_E^n,Y_B^n|S_B^n,S_E^n,M)\\
&= R_M + I(K,S_A^n,X_E^n;Y_E^n,Y_B^n|S_B^n,S_E^n,M), && \text{(A.17)}
\end{aligned}$$

where (A.15) is true because $(S_B^n,S_E^n) - S_A^n - (M,K,X_A^n,X_E^n,Y_E^n,Y_B^n)$ is a Markov chain, and (A.16) follows from Fano's inequality which gives $H(M|Y_E^n,S_E^n) = o(n)$. To bound the second term in (A.17), we write

$$
\begin{aligned}
&I(K, S_A^n, X_E^n; Y_E^n, Y_B^n|S_B^n, S_E^n, M)\\
&= H(Y_E^n, Y_B^n|S_B^n, S_E^n, M)\\
&\quad - H(Y_E^n, Y_B^n|K, S_A^n, S_B^n, S_E^n, X_E^n, M)\\
&= H(Y_E^n, Y_B^n|S_B^n, S_E^n, M) + H(K, X_E^n|Y_E^n, Y_B^n, S_B^n, S_E^n, M)\\
&\quad - H(Y_E^n, Y_B^n|K, S_A^n, S_B^n, S_E^n, X_E^n, M) \qquad \text{(A.18)}\\
&\geq H(K, X_E^n, Y_E^n, Y_B^n|S_B^n, S_E^n, M)\\
&\quad - H(K, X_E^n, Y_E^n, Y_B^n|S_A^n, S_B^n, S_E^n, M)\\
&= I(K, X_E^n, Y_E^n, Y_B^n; S_A^n|S_B^n, S_E^n, M)\\
&= I(K, X_E^n, Y_E^n, Y_B^n; S_A^n|S_B^n, S_E^n, M) + I(M; S_A^n|S_B^n, S_E^n)\\
&= I(M, K, X_E^n, Y_E^n, Y_B^n; S_A^n|S_B^n, S_E^n)\\
&= \sum_{i=1}^{n} I(M, K, X_E^n, Y_E^n, Y_B^n; S_{A,i}|S_A^{i-1}, S_B^n, S_E^n)\\
&= \sum_{i=1}^{n} I(M, K, X_E^n, Y_E^n, Y_B^n; S_{A,i}|S_B^n, S_E^n)\\
&= \sum_{i=1}^{n} I(M, K, X_E^n, Y_E^n, Y_B^n, S_{B,\tilde{i}}, S_{E,\tilde{i}}; S_{A,i}|S_{B,i}, S_{E,i})\\
&= nI(W; S_{A,Q'}|S_{B,Q'}, S_{E,Q'}), \qquad \text{(A.19)}
\end{aligned}
$$

where (A.18) follows from Fano's inequality which implies that $H(K|Y_B^n, S_B^n) = o(n)$ and the fact that $X_E^n = g_n(Y_E^{n-1})$. We define $S_{B,\tilde{i}} = (S_B^{i-1}, S_{B,i+1}^n)$ and $S_{E,\tilde{i}} = (S_E^{i-1}, S_{E,i+1}^n)$, and $W = (M, K, X_E^n, Y_E^n, Y_B^n, S_{B,\tilde{i}}, S_{E,\tilde{i}}, Q')$. Note that W does indeed satisfy the condition $W - S_{A,Q'} - (S_{B,Q'}, S_{E,Q'})$.

$$
\begin{aligned}
&n(R_M + R_K)\\
&\leq I(M, K; Y_E^n, Y_B^n, S_B^n, S_E^n|X_E^n)\\
&= I(M, K; Y_E^n, Y_B^n, S_B^n, S_E^n|X_E^n) - I(M, K; Y_E^n, S_E^n|X_E^n) \qquad \text{(A.20)}\\
&= I(M, K; Y_B^n, S_B^n|Y_E^n, X_E^n, S_E^n)\\
&= I(M, K; Y_B^n|Y_E^n, X_E^n, S_E^n)\\
&\quad + I(M, K; S_B^n|Y_E^n, Y_B^n, X_E^n, S_E^n)\\
&\leq I(M, K, S_A^n, S_E^n, X_A^n; Y_B^n|Y_E^n, X_E^n)\\
&\quad + I(M, K; S_B^n|Y_E^n, Y_B^n, X_E^n, S_E^n)
\end{aligned}
$$

$$\begin{aligned}
&= I(X_A^n; Y_B^n | X_E^n, Y_E^n) \\
&\quad + \sum_{i=1}^{n} I(M, K; S_{B,i} | S_B^{i-1}, Y_E^n, Y_B^n, X_E^n, S_E^n) \\
&= \sum_{i=1}^{n} H(Y_{B,i} | Y_B^{i-1}, X_E^n, Y_E^n) - H(Y_{B,i} | Y_B^{i-1}, X_A^n, X_E^n, Y_E^n) \\
&\quad + \sum_{i=1}^{n} I(M, K; S_{B,i} | S_B^{i-1}, Y_E^n, Y_B^n, X_E^n, S_E^n) \\
&\leq \sum_{i=1}^{n} H(Y_{B,i} | X_{E,i}, Y_{E,i}) - H(Y_{B,i} | X_{A,i}, X_{E,i}, Y_{E,i}) \\
&\quad + \sum_{i=1}^{n} I(M, K, Y_E^n, Y_B^n, X_E^n S_{B,\tilde{i}}, S_{E,\tilde{i}}; S_{B,i} | S_{E,i}) \\
&= \sum_{i=1}^{n} I(X_{A,i}; Y_{B,i} | X_{E,i}, Y_{E,i}) \\
&\quad + \sum_{i=1}^{n} I(M, K, Y_E^n, Y_B^n, X_E^n, S_{B,\tilde{i}}, S_{E,\tilde{i}}; S_{B,i} | S_{E,i}) \\
&= nI(X_{A,Q}; Y_{B,Q} | X_{E,Q}, Y_{E,Q}, Q) + nI(W; S_{B,Q'} | S_{E,Q'}), \qquad \text{(A.21)}
\end{aligned}$$

where (A.20) follows from the secrecy assumption $I(M, K; Y_E^n, S_E^n | X_E^n) = o(n)$. □

Appendix B

Appendix 2

Proof of Theorem 3.1

Proof. To avoid complicated notation, we just show the achievability for the $\mathcal{R}_1$ region. Key agreement protocol is performed in two stages (see [29], *Theorem 2.2*). First, Bob uses the public channel to agree on a key K_{AB} with Alice. Given the random variables X, Y, Z, Y_r, Z_r and U satisfying (3.4)

- Generate randomly a typical sequence U^n with probability

  $$P_{U^n}(U^n) = \prod_{i=1}^{n} P_U(u_i)$$

  We assume that Alice, Bob and Charlie know the sequence U^n.

- Generate $2^{n(H(Y_r|U)+\epsilon)}$ i.i.d. $\mathbf{y}_r$ sequences, each with probability

  $$P_{Y_r^n|U^n}(Y_r^n|U^n) = \prod_{i=1}^{n} P_{Y_r|U}(y_{r,i}|u_i)$$

  and label each of them $\mathbf{y}_r(b,k,j)$, where $1 \leq b \leq 2^{nR_b}$, $1 \leq k \leq 2^{nR_{AB}}$, $1 \leq j \leq 2^{nR'}$. Hence,

  $$R_b + R_{AB} + R' = H(Y_r|U) + \epsilon \tag{B.1}$$

  This random codebook is generated such that all the codewords

  $$C_b = \{Y_r^n(b,k,j) \mid 1 \leq k \leq 2^{nR_{AB}},\ 1 \leq j \leq 2^{nR'}\}$$

  constitutes a Discrete Memoryless Channel (DMC) codebook for the channel $P_{X|Y_r}$. Therefore, if $R_{AB} + R' = I(Y_r;X|U) - \epsilon'$ then with high probability, there is the unique sequence $\mathbf{y}_r$ that is jointly typical with $\mathbf{x}$ given U^n.

- Bob partitions the codebooks C_b, $1 \leq b \leq 2^{nR_b}$ by randomly assigning the codewords $\mathbf{y}_r \in C_b$ to $2^{nR_{AB}}$ bins. Each bin, denoted by $k \in [1, 2^{nR_{AB}}]$, corresponds to a DMC codebook for the channel $P_{Z_r|Y_r}$. For $R' = I(Y_r; Z_r) - \epsilon'$, with high probability, within each bin there will be the unique sequence $\mathbf{z}_r$ that is jointly typical with $\mathbf{y}_r \in C_b$. Key K_{AB} is defined to be the index k in the codeword $\mathbf{y}_r$.

- Observing a typical source sequence $\mathbf{y}_r(b, k, j)$, Bob sends the bin index b to Alice over the public channel.

- Alice looks for a codeword $\mathbf{y}_r(b, k, j)$ such that

  $$(\mathbf{y}_r(b, k, j), \mathbf{x}) \in A_\epsilon^{*(n)}(X, Y_r|U).$$

  As pointed out above, since $\mathbf{y}_r \in C_b$, Alice can find the unique $\mathbf{y}_r$ that is jointly typical with $\mathbf{x}$ given $\mathbf{u}$.

- As an eavesdropper, Charlie has access to the sequence $\mathbf{z}$. He can reduce uncertainty about the key K_{AB} by assigning all sequences $\mathbf{y}_r \in C_b$ to $2^{n(I(Y_r;X|U)-I(Y_r;Z|U)-\delta')}$ bins of size $2^{n(I(Y_r;Z|U)-\delta')}$. Each such bin represents a DMC codebook for the channel $P_{Z|Y_r}$, so with high probability, within each bin, there will be the unique sequence $\mathbf{y}_r \in C_b$. By doing this Charlie is able to reduce uncertainty about K_{AB} from $2^{n(I(Y_r;Z_r|U)-\epsilon')}$ to $2^{n(I(Y_r;Z|U)-\epsilon')}$ possible key outcomes. This key rate uncertainty reduction is the leakage rate R_{AB}^L. Hence,

  $$R_{AB}^L \leq I(Y_r; Z|U) - I(Y_r; Z_r|U)$$

After this stage, Alice has access to $\mathbf{y}_r$, and her own observations $\mathbf{x}$. To construct the key K_{AC} we repeat the same approach as above by considering Bob as an eavesdropper. The assumption is that Charlie has access to the noisy observations $\mathbf{z}_r$ (generated from $P_{Z_r|Z}$), while Alice observes $(\mathbf{x}, \mathbf{y}_r)$. Hence,

$$R_{AC} = I(Z_r; X, Y_r) - I(Z_r; Y_r) = I(Z_r; X|Y_r) - \epsilon' \tag{B.2}$$

$$R_{AC}^L = I(Z; Y_r) - I(Z_r; Y_r) - \epsilon', \tag{B.3}$$

where (B.2) is true because the Markov chain $Z_r - (X, Y_r) - Y_r$ holds.

Computation of Security Level

Charlie's uncertainty about the key K_{AB} can be bounded as follows

$$\begin{aligned}
H(K_{AB}|b,Z^n) &\geq H(K_{AB}|b,Z^n,U^n) \\
&= H(K_{AB},Z^n|b,U^n) - H(Z^n|b,U^n) \\
&= H(K_{AB},Z^n,Y_r^n|b,U^n) - H(Y_r^n|K_{AB},Z^n,b,U^n) - H(Z^n|b,U^n) \\
&= H(K_{AB},Y_r^n|b,U^n) + H(Z^n|K_{AB},Y_r^n,b,U^n) \\
&\quad - H(Y_r^n|K_{AB},Z^n,b,U^n) - H(Z^n|b,U^n) \\
&\geq H(Y_r^n|b,U^n) + H(Z^n|Y_r^n,U^n) \\
&\quad - H(Y_r^n|K_{AB},Z^n,b,U^n) - H(Z^n|b,U^n) \\
&\overset{(a)}{\geq} H(Y_r^n|b,U^n) + H(Z^n|Y_r^n,U^n) + n\delta_1 - H(Z^n|U^n) \\
&= H(Y_r^n|b,U^n) - I(Y_r^n;Z^n|U^n) + n\delta_1 \qquad \text{(B.4)}
\end{aligned}$$

where (a) follows from Fano's inequality and the fact that conditioning reduces entropy.

We now bound each of these terms:

$$\begin{aligned}
H(Y_r^n|b,U^n) &= H(Y_r^n,b|U^n) - H(b|U^n) \\
&\overset{(b)}{=} H(Y_r^n|U^n) - H(b|U^n) \\
&\overset{(c)}{\geq} n[H(Y_r|U)+\epsilon] - n[H(Y_r|X,U)+\epsilon''] \\
&\geq nI(Y_r;X|U) + n\epsilon
\end{aligned}$$

where (b) holds because b is a component of Y_r^n, and (c) follows from the fact that given U^n, Y_r^n and b have $I(Y_r;X|U)+\epsilon$ and $H(Y_r|X,U)+\epsilon''$ possible values, respectively.

To bound $I(Y_r^n;Z^n|U^n)$ in (B.4), let L be an indicator random variable which takes on the value 1 when $(Y_r^n, Z^n) \in A_\epsilon^{*(n)}(Y_r, Z|U)$ and 0 otherwise.

$$\begin{aligned} I(Y_r^n; Z^n|U^n) &\leq I(Y_r^n, L; Z^n|U^n) \\ &= I(Y_r^n; Z^n|L, U^n) + I(L; Z^n|U^n) \\ &= \sum_{j=0}^{1} Pr(L = j) I(Y_r^n; Z^n|U^n, L = j) + I(L; Z^n|U^n) \\ &\leq \sum_{j=0}^{1} \Pr(L = j) I(Y_r^n; Z^n|U^n, L = j) + H(L) \\ &\leq \sum_{j=0}^{1} \Pr(L = j) I(Y_r^n; Z^n|U^n, L = j) + 1 \\ &\leq \Pr(L = 1) I(Y_r^n; Z^n|U^n, L = 1) + n \log|\mathcal{Y}| \Pr(L = 0) + 1 \\ &\leq \Pr(L = 1) I(Y_r^n; Z^n|U^n, L = 1) + n\delta' + 1 \qquad \text{(B.5)} \end{aligned}$$

From the joint typicality properties, we have

$$\begin{aligned} &\Pr(T = L) I(Y_r^n; Z^n|U^n, L = 1) \leq I(Y_r^n; Z^n|U^n, L = 1) \\ &= \sum_{(\mathbf{y}_r, \mathbf{z}) \in A_\epsilon^{*(n)}(Y_r, Z|U)} \Pr(\mathbf{y}_r, \mathbf{z}|\mathbf{u})[\log \Pr(\mathbf{y}_r, \mathbf{z}|\mathbf{u}) - \log \Pr(\mathbf{y}_r|\mathbf{u}) - \log \Pr(\mathbf{z}|\mathbf{u})] \\ &\leq n[H(Y_r|U) + H(Z|U) - H(Y_r, Z|U) + \delta''] \\ &= n[I(Y_r; Z|U) + \delta''] \end{aligned}$$

Combing the last step with (B.5) we get

$$\begin{aligned} I(Y_r^n; Z^n|U^n) &\leq nI(Y_r; Z|U) + n[\frac{1}{n} + \delta' + \delta''] \\ &\leq n[I(Y_r; Z|U) + \delta] \qquad \text{(B.6)} \end{aligned}$$

From (B.4), (B.5) and (B.6) we have

$$\frac{1}{n} H(K_{AB}|b, Z^n) \geq I(Y_r; X|U) - I(Y_r; Z|U)$$

Similarly, we can show

$$\frac{1}{n} H(K_{AB}|b, Z_r^n) \geq I(Y_r; X|U) - I(Y_r; Z_r|U)$$

It is only left to calculate an upper bound on the leakage rate R_{AB}^L. From Definition 3.1 we have

$$\begin{aligned} R_{AB}^L &= \frac{1}{n} I(K_{AB}; b, Z^n) \\ &= \frac{1}{n} \left(H(K_{AB}) - H(K_{AB}|b, Z^n) \right) \\ &\leq I(Y_r; Z|U) - I(Y_r; Z_r|U). \end{aligned}$$

Now we bound Bob's uncertainty about the key K_{AC}. Let c be the bin index of the codeword $\mathbf{z}_r$, which Charlie sends to Alice over the public channel.

$$\begin{aligned} H(K_{AC}|c, Y^n) &\geq H(K_{AC}|c, Y^n) \\ &= H(K_{AC}, Y^n|c) - H(Y^n|c) \\ &= H(K_{AC}, Y^n, Z_r^n|c) - H(Z_r^n|K_{AC}, Y^n, c) - H(Y^n|c) \\ &= H(K_{AC}, Z_r^n|c) + H(Y^n|K_{AC}, Z_r^n, c) \\ &\quad - H(Z_r^n|K_{AC}, Y^n, c) - H(Y^n|c) \\ &\geq H(Z_r^n|c) + H(Y^n|Z_r^n) - H(Z_r^n|K_{AC}, Y^n, c) - H(Y^n|c) \\ &\overset{(d)}{\geq} H(Z_r^n|c) + H(Y^n|Z_r^n) + n\delta_2 - H(Y^n) \\ &= H(Z_r^n|c) - I(Z_r^n; Y^n) + n\delta_2 \end{aligned} \tag{B.7}$$

where (d) follows from Fano's inequality and the fact that conditioning reduces entropy. Using the same approach as we did for the key K_{AB}, we can show that

$$H(Z_r^n|c) = I(Z_r; X, Y_r) - \delta' \tag{B.8}$$

$$I(Z_r^n; Y^n) \leq nI(Z_r; Y) \tag{B.9}$$

Hence,

$$\frac{1}{n}H(K_{AC}|c, Y^n) \geq I(Z_r; X, Y_r) - I(Z_r; Y_r)$$

Similarly, we can show

$$\frac{1}{n}H(K_{AC}|c, Y_r^n) \geq I(Z_r; X, Y_r) - I(Z_r; Y_r)$$

It is only left to calculate an upper bound on the leakage rate R_{AC}^L. From Definition 3.1 we have

$$\begin{aligned} R_{AC}^L &= \frac{1}{n}I(K_{AC}; c, Y^n) \\ &= \frac{1}{n}\left(H(K_{AC}) - H(K_{AC}|c, Y^n)\right) \\ &\leq I(Z_r; Y) - I(Z_r; Y_r). \end{aligned}$$

□

Bibliography

[1] A. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[3] L. Yingbin and H. Poor, "Multiple-Access Channels With Confidential Messages ," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, 2008.

[4] Y. Oohama, "Relay channels with confidential messages," *Arxiv preprint cs/0611125*, 2006.

[5] X. He and A. Yener, "On the equivocation region of relay channels with orthogonal components," in *41th Asilomar Conf. Signals, Syst. and Comp*, 2007.

[6] ——, "The role of an untrusted relay in secret communication," in *IEEE International Symposium on Information Theory*, 2008, pp. 2212–2216.

[7] M. Yuksel and E. Erkip, "The relay channel with a wire-tapper," in *41st Annual Conf. on Inf. Sciences and Syst.* Citeseer, 2007.

[8] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, 2008.

[9] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete Memoryless Interference and Broadcast Channels with Confidential Messages: ecrecy Rate Regions," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2493–2507, 2008.

[10] D. Slepian and J. Wolf, "Noiseless coding of correlated information sources," *IEEE Transactions on Information Theory*, vol. 19, no. 4, pp. 471–480, 1973.

[11] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 3047–3061, 2004.

[12] A. Gohari and V. Anantharam, “Information-theoretic key agreement of multiple terminals–Part I: Source model,” *Preprint*, 2007.

[13] V. M. Prabhakaran, K. Eswaran, and K. Ramchandran, “Secrecy via Sources and Channels-A Secret Key-Secret Message Rate Tradeoff Region,” in *Proceedings of the IEEE International Symposium on Information Theory, Toronto, Canada*, July 2008, pp. 1010 – 1014.

[14] V. Prabhakaran and K. Ramchandran, “A separation result for secure communication,” in *talk presented at the 45th Allerton Conf. Commun., Contr., Computing*, 2007.

[15] N. Milosavljevic, M. Gastpar, and K. Ramchandran, “Secure communication using an untrusted relay via sources and channels,” in *Proceedings of the 2009 IEEE international conference on Symposium on Information Theory*, 2009, pp. 2457–2461.

[16] ——, “The Role of Game Theory in Key Agreement Over a Public Channel,” in *Proceedings of the 2010 IEEE international conference on Symposium on Information Theory*, 2010.

[17] T. Cover and A. Gamal, “Capacity theorems for the relay channel,” *IEEE Transactions on Information Theory*, vol. 25, no. 5, pp. 572–584, 1979.

[18] E. Ekrem and S. Ulukus, “Secrecy in cooperative relay broadcast channels,” in *IEEE International Symposium on Information Theory*, 2008.

[19] R. Ahlswede, “Common randomness in information theory and cryptography–Part I: Secret sharing,” *IEEE Trans. Inform. Theory*, 1993.

[20] U. Maurer, “Secret key agreement by public discussion from common information,” *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, 1993.

[21] R. Csiszar and P. Narayan, “Common randomness and secret key generation with a hepler,” *IEEE Trans. Inform. Theory*, vol. 46, no. 2, pp. 344–366.

[22] C. Ye and P. Narayan, “The private key capacity region for three terminals,” in *Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on.*

[23] ——, “The secret key-private key capacity region for three terminals,” *Arxiv preprint cs/0511047*, 2005.

[24] R. A. Berry and D. N. C. Tse, “The role of an untrusted relay in secret communication,” in *ITW*, 2009.

[25] S. Chung, S. Kim, J. Lee, and J. Cioffi, “A game-theoretic approach to power allocation in frequency-selective Gaussian interference channels,” in *IEEE International Symposium on Information Theory*, 2003, pp. 316–316.

[26] M. Yuksel, X. Liu, and E. Erkip, “A Secure Communication Game with a Relay Helping the Eavesdropper,” pp. 110–114.

[27] S. Gordon and J. Katz, “Rational secret sharing, revisited,” *Lecture Notes in Computer Science*, vol. 4116, 2006.

[28] I. Abraham, D. Dolev, R. Gonen, and J. Halpern, “Distributed computing meets game theory: Robust mechanisms for rational secret sharing and multiparty computation,” in *Proceedings of the twenty-fifth annual ACM symposium on Principles of distributed computing.* ACM, 2006, pp. 53–62.

[29] C. Ye, “Information Theoretic Generation of Multiple Secret Keys,” *PHD Thesis, University of Maryland, College Park*, 2005.