Published in IET Communications
Received on 30th April 2013
Revised on 10th October 2013
Accepted on 20th November 2013
doi: 10.1049/iet-com.2013.0630

ISSN 1751-8628

Multiple-access wiretap channel with common channel state information at the encoders

Bin Dai[1], *Yongtao Wang*[2], *Zhuojun Zhuang*[3]

[1]School of Information Science and Technology, Southwest JiaoTong University, Northbound Section Second Ring Road 111, Chengdu 610031, People's Republic of China
[2]China Information Technology Security Evaluation Center, Beijing 100085, People's Republic of China
[3]Computer Science and Engineering Department, Shanghai Jiao Tong University, Shanghai 200240, People's Republic of China
E-mail: daibinsjtu@gmail.com

Abstract: The multiple-access wiretap channel (MAC-WTC) with common channel state information (CSI) at the encoders is studied, where two transmitters wish to send their confidential messages (no common message) to a legitimate receiver, while keeping a wiretapper as ignorant of the confidential messages as possible. Meanwhile, the channel is controlled by CSI, and it is available at the transmitters in a non-causal manner or causal manner. This model can be viewed as a MAC extension of the WTC with CSI. Both the situation that the encoders can cooperate with each other and the situation that cooperation is not allowed between the encoders are investigated. More specifically, first, the cooperative MAC-WTC with common CSI at the encoders is investigated, inner bounds on the secrecy capacity regions are provided for both non-causal and causal manners. Secondly, the non-cooperative MAC-WTC with common CSI at the encoders is investigated, and also provide inner bounds on the secrecy capacity regions for both non-causal and causal manners. Finally, by calculating the binary examples, the authors find that the cooperation between the encoders helps to obtain a larger secrecy rate region, that is, cooperation enhances the security of the MAC-WTC with common CSI at the encoders.

1 Introduction

The coding for channels with channel state information (CSI) at the transmitter was first investigated by Shannon [1] in 1958, where the CSI is available to the transmitter in a causal manner. The capacity of this model was totally determined by Shannon [1]. After that, in order to solve the problem of coding for a computer memory with defective cells, Kuznetsov and Tsybakov [2] considered a channel in the presence of non-causal CSI at the transmitter. They provided some coding techniques without determination of the capacity. The capacity was found in 1980 by Gelfand and Pinsker [3]. Based on Gelfand and Pinsker's work, Costa [4] investigated a power constrained additive noise channel, where part of the noise is known at the transmitter as side information. This channel is also called dirty paper channel. By using the capacity formula of Gelfand–Pinsker's channel [3], Costa showed that the capacity of the dirty paper channel is the same as that of the standard Gaussian channel (no side information to the transmitter). In addition, based on Shannon's model [1], Salehi [5] investigated the situation that the channel encoder and decoder have access to noisy versions of the CSI, and the channel capacity of this model was determined. However, Caire and Shamai [6] showed that the capacity formula given by Salehi [5] can be obtained from Shannon's result [1].

Recently, a few works on multiple user communication systems with CSI have been studied. Das and Narayan [7] characterised the capacity region of time-varying multiple-access channel (MAC) with causal CSI at the encoders. After that, Cemal and Steinberg [8] investigated the MAC with full CSI at the decoder, and partial, rate-limited CSI at the encoders. Inner and outer bounds were derived on the capacity region of this new model. In addition, the capacity region was determined for a special case, where the CSI available at one of the encoders is a subset of the CSI available at the other encoder. Moreover, Jafar [9] studied the MAC with CSI in a manner that there are three different kinds of CSI, and they are available to the two encoders and the decoder, respectively. An achievable region was provided in [9]. In 2013, Lapidoth and Steinberg [10, 11] studied the MAC with causal CSI, where both the case where two independent states are respectively available to the corresponding encoders and the case where a common state is available to the encoders are considered. Inner and outer bounds on the capacity regions are provided for these models. Note that in [10, 11], both the causal CSI and strictly causal CSI are studied, and the strictly causal CSI is a special case of the causal CSI. Other

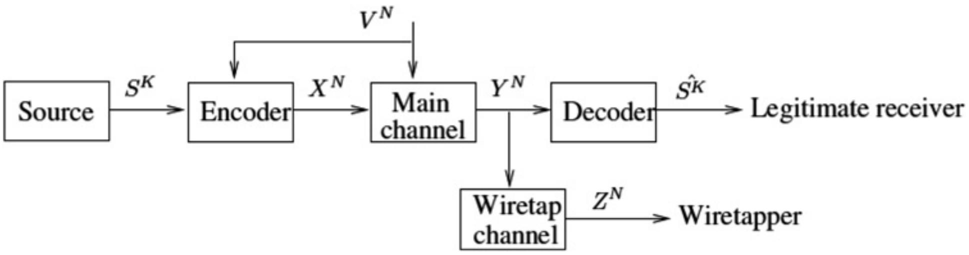

Fig. 1 *Wiretap channel with non-causal CSI*

related works are in [12–15]. Besides these works on the MAC with CSI, Steinberg investigated the degraded broadcast channel with CSI [16], where both causal and non-causal manners were considered in his paper. Specifically, inner and outer bounds on capacity region were provided for the degraded broadcast channel with non-causal CSI [16], meanwhile, the capacity region of the degraded broadcast channel with causal CSI was totally determined [16].

Transmission of confidential messages has been studied in the literature of several classes of channels. Wyner, in his well-known paper on the wiretap channel (WTC) [17], studied the problem that how to transmit the confidential messages to the legitimate receiver via a degraded broadcast channel, while keeping the wiretapper as ignorant of the messages as possible. Measuring the uncertainty of the wiretapper by equivocation, the capacity-equivocation region was established. Furthermore, the secrecy capacity was also established, which provided the maximum transmission rate with perfect secrecy. After the publication of Wyner's work, Csiszár and Körner [18] investigated a more general situation: the broadcast channels with confidential messages (BCC). In this model, a common message and a confidential message were sent through a general broadcast channel. The common message was assumed to be decoded correctly by the legitimate receiver and the wiretapper, whereas the confidential message was only allowed to be obtained by the legitimate receiver. This model is also a generalisation of [19], where no confidentiality condition is imposed. The capacity-equivocation region and the secrecy capacity region of BCC [18] were totally determined, and the results were also a generalisation of those in [17]. Based on Wyner's work, Leung-Yan-Cheong and Hellman studied the Gaussian wiretap channel (GWC) [20], and showed that its secrecy capacity was the difference between the main channel capacity and the overall WTC capacity (the cascade of main channel and WTC).

Inspired by the works of [3, 4, 17], Mitrpant *et al.* [21] studied transmission of confidential messages in the channels with CSI. In [21], an inner bound on the capacity-equivocation region was provided for the GWC with CSI. Furthermore, Chen *et al.* [22] investigated the discrete memoryless WTC with non-causal CSI (see Fig. 1), and also provided an inner bound on the capacity-equivocation region. Note that the coding scheme of [22] is a combination of those in [3, 17]. Based on the work of [22], Dai [23] provided an outer bound on the WTC with non-causal CSI, and determined the capacity-equivocation region for the model of WTC with memoryless CSI, where the memoryless means that at the ith time, the output of the channel encoder depends only on the ith time CSI. Some other related works on the WTC (including feedback and secret key) can be found in [24–31].

Recently, the information-theoretical security for other multi-user communication systems has been investigated. The relay channel with confidential messages was studied in [32], and the interference channel with confidential messages was studied in [33]. The multiple-access channel with confidential messages was studied in [34–38].

In this paper, first, we study the cooperative MAC-WTC with common CSI at the encoders, see Fig. 2. For the cooperative case, both the messages W_1 and W_2 are known by Encoder 1 and Encoder 2. The transition probability of the channel depends on the CSI S^N, and S^N is available to the channel encoders in a causal or non-causal manner. The wiretapper wishes to obtain the confidential messages. Inner bounds (achievable regions) on the secrecy capacity regions of Fig. 2 are provided for both causal and non-causal manners.

Second, the non-cooperative MAC-WTC with common CSI at the encoders is investigated, see Fig. 3. The only difference between Figs. 2 and 3 is that the messages W_1 and W_2 of Fig. 3 are known by Encoder 1 and Encoder 2, respectively. In other words, W_1 is not known by Encoder 2, and W_2 is not known by Encoder 1. Inner bounds on the secrecy capacity regions of Fig. 3 are also provided for both causal and non-causal manners.

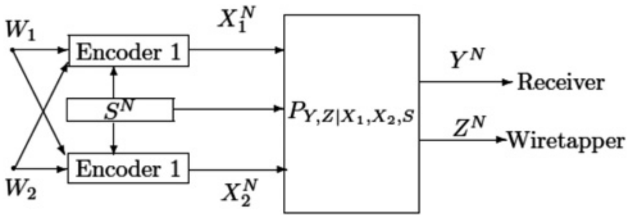

Fig. 2 *Cooperative MAC-WTC with common CSI at the encoders*

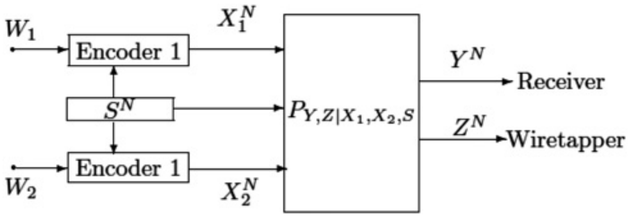

Fig. 3 *Non-cooperative MAC-WTC with common CSI at the encoders*

Finally, the results of this paper are further explained via binary examples. The main contribution of this paper is as follows:

- Several encoding–decoding schemes for the models of Figs. 2 and 3 are constructed.
- The gap between the cooperative encoders and the non-cooperative encoders is shown by the binary examples of Figs. 2 and 3.

In this paper, random variables, sample values and alphabets are denoted by capital letters, lower case letters and calligraphic letters, respectively. A similar convention is applied to the random vectors and their sample values. For example, U^N denotes a random N-vector $(U_1, \ldots, U_N)$, and $u^N = (u_1, \ldots, u_N)$ is a specific vector value in $\mathcal{U}^N$ that is the Nth Cartesian power of $\mathcal{U}$. U_i^N denotes a random $N-i+1$-vector $(U_i, \ldots, U_N)$, and $u_i^N = (u_i, \ldots, u_N)$ is a specific vector value in $\mathcal{U}_i^N$. Let $p_V(v)$ denotes the probability mass function $\Pr\{V=v\}$. Throughout the paper, the logarithmic function is to the base 2.

The organisation of this paper is as follows: In Section 2, the inner bounds on the secrecy capacity regions of the model of Fig. 2 for both causal and non-causal manners are provided. In Section 3, the inner bounds on the secrecy capacity regions of the model of Fig. 3 are provided. In Section 4, we will show the binary examples about the models of Figs. 2 and 3. Final conclusions are provided in Section 5.

2 Cooperative MAC-WTC with common CSI at the encoders

2.1 Model of Fig. 2 with non-causal CSI

In this subsection, a description of the model of Fig. 2 with non-causal CSI is given by Definitions 1–3. The inner bound on the secrecy capacity region $\mathcal{C}_s^{cn}$, which is composed of all achievable secrecy pairs (R_1, R_2) in the model of Fig. 2 with non-causal CSI, is characterised in Theorem 1, where the achievable secrecy pair (R_1, R_2) is defined in Definition 4.

Definition 1: (Encoder 1 and Encoder 2): Encoder 1 and Encoder 2 of the model of Fig. 2 with non-causal CSI are stochastic encoders. The inputs of the two encoders are W_1, W_2 and S^N, while the outputs are X_1^N and X_2^N, respectively. The message W_1 takes the value in $\mathcal{W}_1$, and the message W_2 takes value in $\mathcal{W}_2$. W_1 and W_2 are independent and uniformly distributed over their ranges W_1 and W_2. S^N is the CSI sequence, and it is the output of a discrete memoryless source $p_S(s)$.

Definition 2: (channels): The channel is a DMC with finite input alphabet $\mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{S}$, finite output alphabet $\mathcal{Y} \times \mathcal{Z}$ and transition probability $Q_M(y, z|x_1, x_2, s)$, where $x_1 \in \mathcal{X}_1$, $x_2 \in \mathcal{X}_2$, $s \in \mathcal{S}$, $y \in \mathcal{Y}$ and $z \in \mathcal{Z}$. The inputs of the channel are X_1^N, X_2^N and S^N, while the outputs are Y^N and Z^N. Note that $(W_1, W_2) \rightarrow (X_1^N, X_2^N, S^N) \rightarrow (Y^N, Z^N)$ is a Markov chain. The equivocation rate to the wiretapper is defined as

$$\Delta = \frac{H(W_1, W_2|Z^N)}{N} \tag{1}$$

Note that $\Delta = ((H(W_1, W_2))/N)$ implies that the wiretapper has no knowledge of the messages, that is, the perfect secrecy is achieved.

Definition 3: (decoder): The decoder is a mapping $f_D{:}\mathcal{Y}^N \rightarrow \mathcal{W}_1 \times \mathcal{W}_2$, with input Y^N and output $(\hat{W}_1, \hat{W}_2) = f_D(Y^N)$. Let P_e be the error probability, and it is defined as $\Pr\{(W_1, W_2) \neq (\hat{W}_1, \hat{W}_2)\}$.

Definition 4: (achievable secrecy pair (R$_1$, R$_2$) in the model of Fig. 2 with non-causal CSI): A pair (R_1, R_2) (where $R_1, R_2 > 0$) is called an achievable secrecy pair if, for any given $\epsilon > 0$ and sufficiently large N, there exists a code (N, Δ, P_e) with two message sets $\mathcal{W}_1$ and $\mathcal{W}_2$, such that

$$\begin{aligned} &\frac{log \parallel \mathcal{W}_1 \parallel}{N} \geq R_1 - \epsilon, \quad \frac{log \parallel \mathcal{W}_2 \parallel}{N} \geq R_2 - \epsilon, \\ &\Delta \geq R_1 + R_2 - \epsilon, \quad P_e \leq \epsilon \end{aligned} \tag{2}$$

The inner bound on the secrecy capacity region $\mathcal{C}_s^{cn}$ (composed of all achievable secrecy pairs) of the model of Fig. 2 with non-causal CSI is provided in Theorem 1.

Theorem 1: (Inner bound): A single-letter characterisation of the region $\mathcal{C}_s^{cni}$ is as follows

$$\mathcal{C}_s^{cni} = \bigcup_{p_{U S X_1 X_2 Y Z}} \left\{ \begin{array}{c} (R_1, R_2): \\ R_1 + R_2 \leq I(U;Y) - I(U;S) \\ R_1 + R_2 \leq I(U;Y) - I(U;Z) \end{array} \right\}$$

Here, note that

$$\begin{aligned} &p_{U X_1 X_2 S Y Z}(u, x_1, x_2, s, y, z) \\ &\quad = p_{Y,Z|X_1 X_2 S}(y, z|x_1, x_2, s) p_{U X_1 X_2 S}(u, x_1, x_2, s) \end{aligned}$$

and $\mathcal{C}_s^{cni}$ satisfies that $\mathcal{C}_s^{cni} \subseteq \mathcal{C}_s^{cn}$.

Remark 1: Since the encoders can cooperate with each other, the model of Fig. 2 reduces to the WTC with CSI [22] by considering the two cooperative encoders into one new encoder. From [22], we know that $R = \min\{I(U;Y) - I(U;S), I(U;Y) - I(U;Z)\}$ is an achievable secrecy rate of the WTC with CSI. Thus, replacing R by$R_1 + R_2$, we obtain the achievable secrecy rate region $\mathcal{C}_s^{cni}$ in Theorem 1.

2.2 Model of Fig. 2 with causal CSI

The model of Fig. 2 with causal CSI is similar to the model with non-causal CSI in Section 2.1, except that the S^N in Definition 1 is known to be the encoders in a causal manner, that is, at the ith time $(1 \leq i \leq N)$, the outputs of Encoder 1 and Encoder 2 are $x_{1,i} = f_{1,i}(w_1, w_2, s^i)$ and $x_{2,i} = f_{2,i}(w_1, w_2, s^i)$, respectively, where $s^i = (s_1, s_2, \ldots, s_i)$, $f_{1,i}$ is denoted as Encoder 1 at time i and $f_{2,i}$ is denoted as Encoder 2 at time i. Note that S_i is independent with W_1, W_2, Y^{i-1}, Z^{i-1} and S_{i+1}^N, and $f_{1,i}$, $f_{2,i}$ are stochastic encoders.

The inner bound on the secrecy capacity region $\mathcal{C}_s^{cc}$ of the model of Fig. 2 with causal CSI is provided in Theorem 2, and it is directly obtained from Theorem 1 by using the fact that S is independent of U. Thus the proof is omitted here.

Theorem 2: (Inner bound): A single-letter characterisation of the region $\mathcal{C}_s^{cci}$ is as follows

$$\mathcal{C}_s^{cci} = \bigcup_{p_{U\,S\,X_1\,X_2\,YZ}} \left\{ \begin{array}{l} (R_1, R_2) \\ R_1 + R_2 \le I(U; Y) - I(U; Z) \end{array} \right\}$$

Here, note that

$$\begin{aligned} & p_{UX_1X_2SYZ}(u, x_1, x_2, s, y, z) \\ & = p_{Y,Z|X_1X_2S}(y, z|x_1, x_2, s)\, p_{UX_1X_2S}(u, x_1, x_2, s) \end{aligned}$$

and $\mathcal{C}_s^{cci}$ satisfies that $\mathcal{C}_s^{cci} \subseteq \mathcal{C}_s^{cc}$.

3 Non-cooperative MAC-WTC with common CSI at the encoders

3.1 Model of Fig. 3 with non-causal CSI

The model of Fig. 3 with non-causal CSI is similar to Section 2.1, except the fact that the message W_2 is not known by Encoder 1, and the message W_1 is not known by Encoder 2, that is, the cooperation between the encoders is not allowed. The inner bound on the secrecy capacity region $\mathcal{C}_s^{nn}$ of the model of Fig. 3 with non-causal CSI is provided in Theorem 3, and it is proved in Appendix 1.

Theorem 3: (Inner bound): A single-letter characterisation of the region $\mathcal{C}_s^{nni}$ is as follows

$$\mathcal{C}_s^{nni} = \mathcal{A} \cup \mathcal{B}$$

where

$$\mathcal{A} = \bigcup_{p_{U_1X_1|S}p_{U_2X_2|S}} \left\{ \begin{array}{c} (R_1, R_2): \\ R_1 \le I(U_1; Y) - I(U_1; S) \\ R_1 \le I(U_1; Y) - I(U_1; Z) \\ R_2 \le I(U_2; Y|U_1) - I(U_2; S) \\ R_2 \le I(U_2; Y|U_1) - I(U_2; Z|U_1) \end{array} \right\}$$

and

$$\mathcal{B} = \bigcup_{p_{U_1X_1|S}p_{U_2X_2|S}} \left\{ \begin{array}{c} (R_1, R_2): \\ R_1 \le I(U_1; Y|U_2) - I(U_1; S) \\ R_1 \le I(U_1; Y|U_2) - I(U_1; Z|U_2) \\ R_2 \le I(U_2; Y) - I(U_2; S) \\ R_2 \le I(U_2; Y) - I(U_2; Z) \end{array} \right\}$$

Here, note that

$$\begin{aligned} & p_{U_1X_1U_2X_2SYZ}(u_1, x_1, u_2, x_2, s, y) \\ & = p_{Y,Z|X_1X_2S}(y, z|x_1, x_2, s) p_{U_1X_1|S} \\ & (u_1, x_1|s) p_{U_2X_2|S}(u_2, x_2|s) p_S(s) \end{aligned}$$

U_1 is independent of U_2, and $U_1 \to S \to U_2.\mathcal{C}_s^{nni}$ satisfies that $\mathcal{C}_s^{nni} \subseteq \mathcal{C}_s^{nn}$.

Remark 2: There are some notes on Theorem 3, which are as follows:

- The ranges of the random variables U_1 and U_2 satisfy

$$\| \mathcal{U}_1 \| \le \| \mathcal{X}_1 \| \| \mathcal{X}_2 \| \| \mathcal{S} \| + 2$$

$$\| \mathcal{U}_2 \| \le (\| \mathcal{X}_1 \| \| \mathcal{X}_2 \| \| \mathcal{S} \| + 2)^2$$

- Without the secrecy constraint, an achievable region $\mathcal{R}^*$ of the MAC with non-causal CSI at the non-cooperative encoders [12] is given by

$$\mathcal{R}^* = \bigcup_{p_{U_1X_1|S}p_{U_2X_2|S}} \left\{ \begin{array}{c} (R_1, R_2): \\ R_1 \le I(U_1; Y|U_2) - I(U_1; S) \\ R_2 \le I(U_2; Y|U_1) - I(U_2; S) \\ R_1 + R_2 \le I(U_1, U_2; Y) - I(U_1, U_2; S) \end{array} \right\}$$

Note that the inequality $R_1 + R_2 \le I(U_1, U_2;Y) - I(U_1, U_2;S)$ can be obtained from $R_1 \le I(U_1;Y|U_2) - I(U_1;S)$, $R_2 \le I(U_2;Y) - I(U_2;S)$ and $U_1 \to S \to U_2$. Therefore, compared with Theorem 3, it is easy to see that $\mathcal{C}_s^{nni} \subseteq \mathcal{R}^*$, that is, the secrecy constraint reduces the achievable region $\mathcal{R}^*$.

3.2 Model of Fig. 3 with causal CSI

The model of Fig. 3 with causal CSI is similar to the model with non-causal CSI in Section 3.1, except that the S^N in Definition 1 is known to be the encoders in a causal manner, that is, at the ith time $(1 \le i \le N)$, the outputs of Encoder 1 and Encoder 2 are $x_{1,\ i} = f_{1,\ i}(w_1, s^i)$ and $x_{2,\ i} = f_{2,\ i}(w_2, s^i)$, respectively, where $s^i = (s_1, s_2, \ldots, s_i)$, $f_{1,i}$ is denoted as Encoder 1 at time i and $f_{2,\ i}$ is denoted as Encoder 2 at time i. Note that S_i is independent with W_1, W_2, Y^{i-1}, Z^{i-1} and S_{i+1}^N, and $f_{1,\ i}$, $f_{2,\ i}$ are stochastic encoders.

The inner bound on the secrecy capacity region $\mathcal{C}_s^{nc}$ of the model of Fig. 3 with causal CSI is provided in Theorem 4, and it is directly obtained from Theorem 3 by using the fact that S is independent of U_1 and U_2. Thus, the proof is omitted here.

Theorem 4: (Inner bound): A single-letter characterisation of the region $\mathcal{C}_s^{nci}$ is as follows

$$\mathcal{C}_s^{nci} = \mathcal{C} \cup \mathcal{D}$$

where

$$\mathcal{C} = \bigcup_{p_{U_1X_1|S}p_{U_2X_2|S}} \left\{ \begin{array}{c} (R_1, R_2): \\ R_1 \le I(U_1; Y) - I(U_1; Z) \\ R_2 \le I(U_2; Y|U_1) - I(U_2; Z|U_1) \end{array} \right\}$$

and

$$\mathcal{D} = \bigcup_{p_{U_1X_1|S}p_{U_2X_2|S}} \left\{ \begin{array}{c} (R_1, R_2): \\ R_1 \le I(U_1; Y|U_2) - I(U_1; Z|U_2) \\ R_2 \le I(U_2; Y) - I(U_2; Z) \end{array} \right\}$$

Here, note that

$$\begin{aligned} & p_{U_1X_1U_2X_2SYZ}(u_1, x_1, u_2, x_2, s, y) \\ & = p_{Y,Z|X_1X_2S}(y, z|x_1, x_2, s) p_{U_1X_1|S}(u_1, x_1|s) \\ & p_{U_2X_2|S}(u_2, x_2|s) p_S(s) \end{aligned}$$

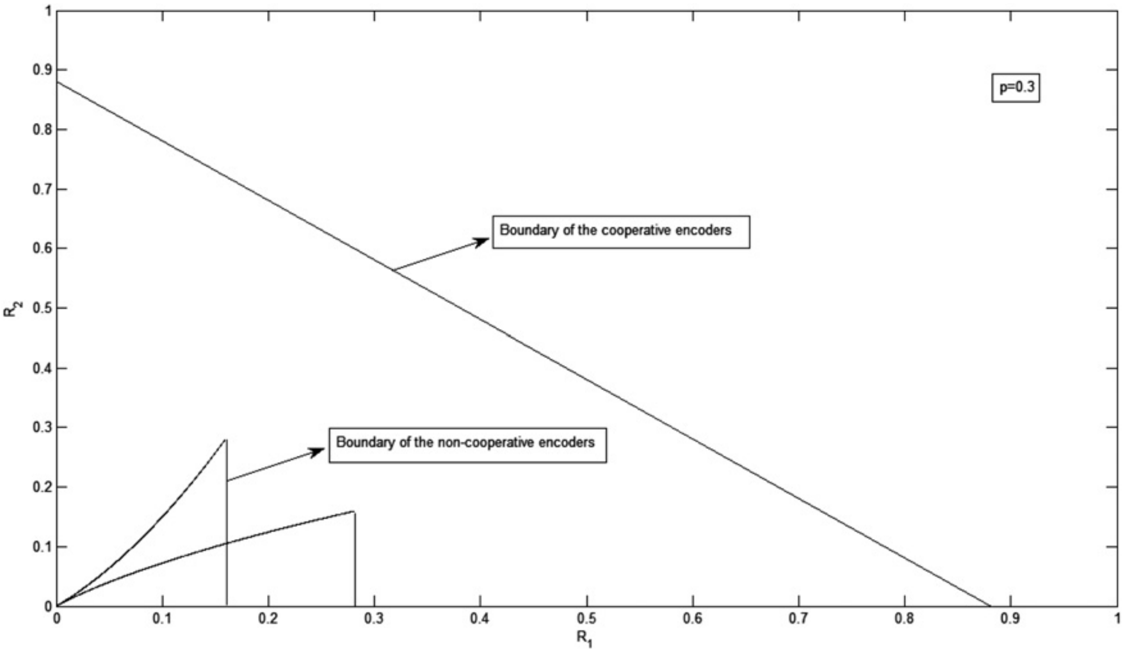

Fig. 4 *Binary case of the cooperative and non-cooperative encoders for p = 0.3*

U_1 is independent of U_2, and $U_1 \to S \to U_2.\mathcal{C}_s^{nci}$ satisfies that $\mathcal{C}_s^{nci} \subseteq \mathcal{C}_s^{nc}$.

4 Binary examples of MAC with causal CSI and with or without secrecy

In this section, we will calculate binary cases of Theorems 2 and 4, see the followings.

4.1 Definition

Let $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{Y} = \{0, 1\}$. Define $\mathcal{S} = \{0, 1\}, p_S(0) = p_S(1) = (1/2)$. The transition probability of the channel is defined as follows.

When $s = 0$

$$p_{Y|X_1,X_2,S}(y|x_1, x_2, s = 0) = \begin{cases} 1, & \text{if } y = x_1 \\ 0, & \text{otherwise} \end{cases} \tag{3}$$

When $s = 1$

$$p_{Y|X_1,X_2,S}(y|x_1, x_2, s = 1) = \begin{cases} 1, & \text{if } y = x_2 \\ 0, & \text{otherwise} \end{cases} \tag{4}$$

For convenience, we assume that the WTC is degraded, that is, the transition probability of the channel is given by

$$p_{Y,Z|X_1X_2S}(y, z|x_1, x_2, s) = p_{Z|Y}(z|y)p_{Y|X_1X_2S}(y|x_1, x_2, s)$$

The probability distribution $p_{Z/Y}(z|y)$ is defined as follows

$$p_{Z|Y}(z|y) = \begin{cases} 1 - p, & \text{if } y = z \\ p, & \text{otherwise} \end{cases} \tag{5}$$

Here, $0 \le p \le (1/2)$.

- For the cooperative case (Theorem 2), let $\mathcal{U} = \{0, 1\}$. The probability mass function of U is defined as: $p_U(0) = \alpha, p_U(1) = 1 - \alpha$, where $0 \le \alpha \le 1$.

In addition, define the conditional probability mass functions $p_{X_1|U,S}$ and $p_{X_2|U,S}$ as follows (see equation at the bottom of the page)

By substituting the above definitions into $R_1 + R_2 \le I(U;Y)–I(U;Z)$, we have $R_1 + R_2 \le h(p)$, where $h(p) = −p\log(p)–(1–p)\log(1–p)$. Note that $R_1 + R_2 = h(p)$ if $\alpha = 0.5$, $\beta_1 = \beta_4 = 1$, $\beta_2 = \beta_3 = 0$, $\gamma_1 = \gamma_2 = \gamma_3 = 1$ and $\gamma_4 = 0$.

- For the non-cooperative case (Theorem 4), let $\mathcal{U}_1 = \mathcal{U}_2 = \{0, 1\}$. The probability mass function of U_1 is defined as: $p_{U_1}(0) = \alpha$, $p_{U_1}(1) = 1 - \alpha$, $p_{U_2}(0) = \beta$, $p_{U_2}(1) = 1 - \beta$, where $0 \le \alpha$, $\beta \le 1$. By calculating, the

$$\begin{aligned}
&p_{X_1|U,S}(0|0, 0) = \beta_1, \quad p_{X_1|U,S}(1|0, 0) = 1 - \beta_1, \quad p_{X_1|U,S}(0|0, 1) = \beta_2, \quad p_{X_1|U,S}(1|0, 1) = 1 - \beta_2 \\
&p_{X_1|U,S}(0|1, 0) = \beta_3, \quad p_{X_1|U,S}(1|1, 0) = 1 - \beta_3, \quad p_{X_1|U,S}(0|1, 1) = \beta_4, \quad p_{X_1|U,S}(1|1, 1) = 1 - \beta_4 \\
&p_{X_2|U,S}(0|0, 0) = \gamma_1, \quad p_{X_2|U,S}(1|0, 0) = 1 - \gamma_1, \quad p_{X_2|U,S}(0|0, 1) = \gamma_2, \quad p_{X_2|U,S}(1|0, 1) = 1 - \gamma_2 \\
&p_{X_2|U,S}(0|1, 0) = \gamma_3, \quad p_{X_2|U,S}(1|1, 0) = 1 - \gamma_3, \quad p_{X_2|U,S}(0|1, 1) = \gamma_4, \quad p_{X_2|U,S}(1|1, 1) = 1 - \gamma_4
\end{aligned}$$

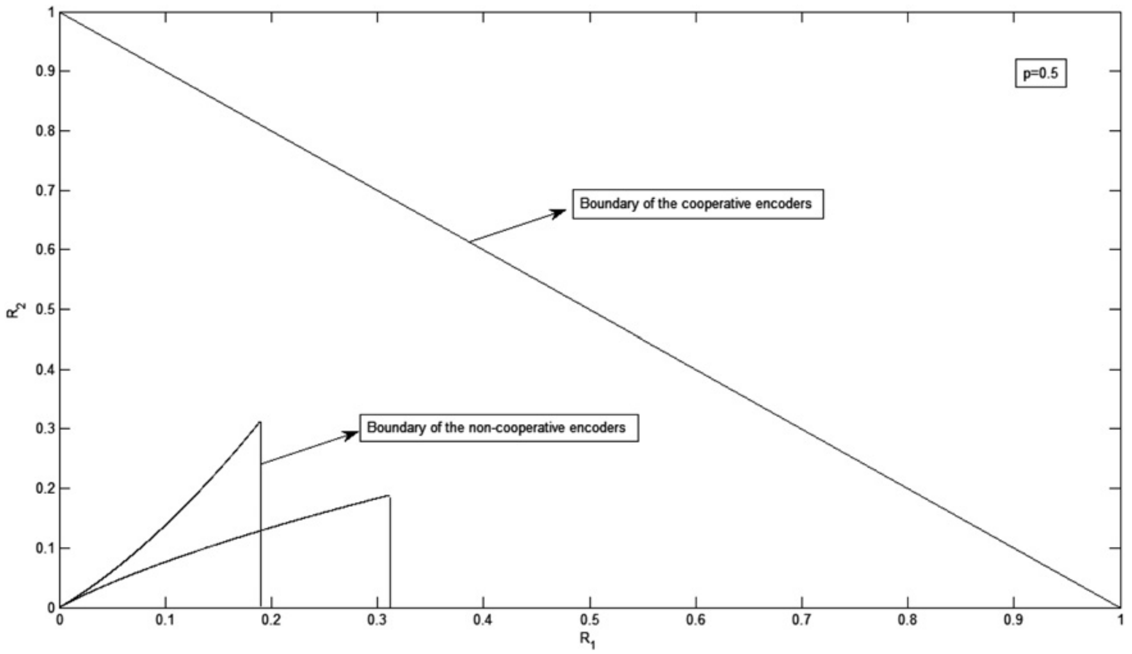

Fig. 5 *Binary case of the cooperative and non-cooperative encoders for p = 0.5*

secrecy rate region $\mathcal{C}_s^{nci}$ of this non-cooperative binary case is given by

$$\mathcal{C}_s^{nci} = \mathcal{C} \cup \mathcal{D}$$

where (see equation at the bottom of the page)

where $\alpha + \beta = 1$.

The following Figs. 4 and 5 plot the binary cases of Theorems 2 and 4 for several values of p. It is easy to see that the cooperation between the encoders enhances the secrecy rate region of the MAC-WTC with common CSI at the encoders.

5 Conclusion

In this paper, first, we investigate the cooperative MAC-WTC with common CSI at the encoders, inner bounds on the secrecy capacity regions are provided both for the case where the channel encoders are allowed to depend non-causally on the channel state sequence and the case where they are restricted to causal dependence. Second, we investigate the non-cooperative MAC-WTC with common CSI at the encoders, and also we provide inner bounds on the secrecy capacity regions for both non-causal and causal manners. Finally, by calculating the binary examples of the cooperative MAC-WTC with causal CSI and the non-cooperative MAC-WTC with causal CSI, we find that the cooperation between the encoders helps to obtain a larger secrecy rate region, that is, cooperation between the encoders enhances the security of the MAC-WTC with common CSI at the encoders.

6 Acknowledgment

This work was supported by a sub-project in National Basic Research Program of China under grant 2012CB316100 on Broadband Mobile Communications at High Speeds, the National Natural Science Foundation of China under grant 61301121, and the Program for New Century Excellent Talents in University under grant NECT-10-0705.

7 References

1 Shannon, C.E.: 'Channels with side information at the transmitter', *IBM J. Res. Dev.*, 1958, **2**, pp. 289–293

$$\mathcal{C}_s^{nci} = \left\{ \begin{array}{c} (R_1, R_2): \\ R_1 \leq (1-\beta)\left(h\left(\frac{1+\beta-2p\beta}{2}\right) - h\left(\frac{1-\beta}{2}\right) + \beta\left(h\left(\frac{\beta}{2} + p - p\beta\right) - h\left(\frac{\beta}{2}\right)\right)\right) \\ R_2 \leq 2\alpha\beta h(p) - (1-\beta)\left(h\left(\frac{1+\beta-2p\beta}{2}\right) - \beta\left(h\left(\frac{\beta}{2} + p - p\beta\right) - h\left(\frac{\beta}{2}\right)\right)\right) \end{array} \right\}$$

$$\cup \left\{ \begin{array}{c} (R_1, R_2): \\ R_1 \leq 2\alpha\beta h(p) - (1-\beta)\left(h\left(\frac{1+\beta-2p\beta}{2}\right) - \beta\left(h\left(\frac{\beta}{2} + p - p\beta\right) - h\left(\frac{\beta}{2}\right)\right)\right) \\ R_2 \leq (1-\beta)\left(h\left(\frac{1+\beta-2p\beta}{2}\right) - h\left(\frac{1-\beta}{2}\right) + \beta\left(h\left(\frac{\beta}{2} + p - p\beta\right) - h\left(\frac{\beta}{2}\right)\right)\right) \end{array} \right\}$$

2 Kuznetsov, N.V., Tsybakov, B.S.: 'Coding in memories with defective cells', *Problemy peredachi informatsii*, 1974, **10**, (2), pp. 52–60

3 Gelfand, S.I., Pinsker, M.S.: 'Coding for channel with random parameters', *Probl. Control Inf. Theory*, 1980, **9**, (1), pp. 19–31

4 Costa, M.H.M.: 'Writing on dirty paper', *IEEE Trans. Inf. Theory*, 1983, **IT-29**, (3), pp. 439–441

5 Salehi, M.: 'Capacity and coding for memories with real-time noisy defect information at encoder and decoder', *Proc. Inst. Electr. Engr – Pt. I*, 1992, **139**, (2), pp. 113–117

6 Caire, G., Shamai (Shitz), S.: 'On the capacity of some channels with channel state information', *IEEE Trans. Inf. Theory*, 1999, **IT-45**, (6), pp. 2007–2019

7 Das, A., Narayan, P.: 'Capacities of time-varying multiple-access channels with side information', *IEEE Trans. Inf. Theory*, 2002, **IT-48**, (1), pp. 4–25

8 Cemal, Y., Steinberg, Y.: 'The multiple-access channel with partial state information at the encoders', *IEEE Trans. Inf. Theory*, 2005, **IT-51**, (11), pp. 3992–4003

9 Jafar, S.: 'Capacity with causal and noncausal side information: a unified view', *IEEE Trans. Inf. Theory*, 2006, **IT-52**, (12), pp. 5468–5474

10 Lapidoth, A., Steinberg, Y.: 'The multiple-access channel with causal side information: common state', *IEEE Trans. Inf. Theory*, 2013, **IT-59**, pp. 32–50

11 Lapidoth, A., Steinberg, Y.: 'The multiple-access channel with causal side information: independent states', *IEEE Trans. Inf. Theory*, 2013, **IT-59**, (3), pp. 5468–5474

12 Farsani, R.K., Marvasti, F.: 'Capacity bounds for multiuser channels with noncausal channel state information at the transmitters', http://www.arxiv.org/pdf/1102.3410

13 Zhang, H., Shi, Y., Liu, M.: 'H step tracking control for networked discrete-time nonlinear systems with integral and predictive actions', *IEEE Trans. Ind. Inf.*, 2013, **9**, (1), pp. 337C345

14 Zhang, H., Shi, Y., Mehr, A.S.: 'Robust H PID control for multivariable networked control systems with disturbance/noise attenuation', *Int. J. Robust Nonlinear Control*, 2012, **22**, (2), pp. 183–204

15 Zhang, H., Shi, Y., Mehr, A.S.: 'Robust static output feedback control and remote PID design for networked motor systems', *IEEE Trans. Ind. Electron.*, 2011, **58**, (2), pp. 5396–5405

16 Steinberg, Y.: 'Coding for the degraded broadcast channel with random parameters, with causal and noncausal side information', *IEEE Trans. Inf. Theory*, 2005, **IT-51**, (8), pp. 2867–2877

17 Wyner, A.D.: 'The wire-tap channel', *The Bell Syst. Tech. J.*, 1975, **54**, (8), pp. 1355–1387

18 Csiszár, I., Körner, J.: 'Broadcast channels with confidential messages', *IEEE Trans. Inf. Theory*, 1978, **IT-24**, (3), pp. 339–348

19 Körner, J., Marton, K.: 'General broadcast channels with degraded message sets', *IEEE Trans. Inf. Theory*, 1977, **IT-23**, (1), pp. 60–64

20 Leung-Yan-Cheong, S.K., Hellman, M.E.: 'The Gaussian wire-tap channel', *IEEE Trans. Inf. Theory*, 1978, **IT-24**, (4), pp. 451–456

21 Mitrpant, C., Han Vinck, A.J., Luo, Y.: 'An achievable region for the Gaussian wiretap channel with side information', *IEEE Trans. Inf. Theory*, 2006, **IT-52**, (5), pp. 2181–2190

22 Chen, Y., Han Vinck, A.J.: 'Wiretap channel with side information', *IEEE Trans. Inf. Theory*, 2008, **IT-54**, (1), pp. 395–402

23 Dai, B., Luo, Y.: 'Some new results on wiretap channel with side information', *Entropy*, 2012, **14**, pp. 1671–1702

24 Ahlswede, R., Cai, N.: 'Transmission, identification and common randomness capacities for wire-tap channels with secure feedback from the decoder'. 'General Theory of Information Transfer and Combinatorics' (Springer, Berlin, 2006), *LNCS* **4123**, pp. 258–275

25 Ardestanizadeh, E., Franceschetti, M., Javidi, T., Kim, Y.: 'Wiretap channel with secure rate-limited feedback', *IEEE Trans. Inf. Theory*, 2009, **IT-55**, (12), pp. 5353–5361

26 Lai, L., El Gamal, H., Poor, V.: 'The wiretap channel with feedback: encryption over the channel', *IEEE Trans. Inf. Theory*, 2008, **IT-54**, pp. 5059–5067

27 Merhav, N.: 'Shannon's secrecy system with informed receivers and its application to systematic coding for wiretapped channels', *IEEE Trans. Inf. Theory*, 2008, **IT-54**, (6), pp. 2723–2734, Special Issue on Information-Theoretic Security

28 Dai, B., Han Vinck, A.J., Luo, Y., Zhuang, Z.: 'Capacity region of non-degraded wiretap channel with noiseless feedback'. Proc. 2012 IEEE Int. Symposium on Information Theory, 2012

29 Khodakarami, H., Lahouti, F.: 'Link adaptation for physical layer security over wireless fading channels', *IET Commun.*, 2012, **6**, (3), pp. 353–362

30 Bagherikaram, G., Plataniotis, K.N.: 'Secure joint source channel coding with interference known at the transmitter', *IET Commun.*, 2012, **6**, (17), pp. 2796–2808

31 Salimi, S., Salmasizadeh, M., Aref, M.R.: 'Rate regions of secret key sharing in a new source model', *IET Commun.*, 2011, **5**, (4), pp. 443–455

32 Lai, L., El Gamal, H.: 'The relay-eavesdropper channel: cooperation for secrecy', *IEEE Trans. Inf. Theory*, 2008, **IT-54**, (9), p. 4005C4019

33 Liu, R., Maric, I., Spasojevic, P., Yates, R.D.: 'Discrete memoryless interference and broadcast channels with confidential messages: secrecy rate regions', *IEEE Trans. Inf. Theory*, 2008, **IT-54**, (6), pp. 2493–2507

34 Liang, Y., Poor, H.V.: 'Multiple-access channels with confidential messages', *IEEE Trans. Inf. Theory*, 2008, **IT-54**, (3), pp. 976–1002

35 Tekin, E., Yener, A.: 'The Gaussian multiple access wire-tap channel', *IEEE Trans. Inf. Theory*, 2008, **IT-54**, (12), pp. 5747–5755

36 Tekin, E., Yener, A.: 'The general Gaussian multiple access and two-way wire-tap channels: achievable rates and cooperative jamming', *IEEE Trans. Inf. Theory*, 2008, **IT-54**, (6), pp. 2735–2751

37 Ekrem, E., Ulukus, S.: 'On the secrecy of multiple access wiretap channel'. Proc. Annual Allerton Conf. Communications, Control and Computing, Monticello, IL, September 2008

38 Wiese, M., Boche, H.: 'An achievable region for the wiretap multiple-access channel with common message'. Proc. 2012 IEEE Int. Symposium on Information Theory, 2012

8 Appendix: Proof of Theorem 3

In this section, we prove Theorem 3. Suppose $(R_1, R_2) \in \mathcal{C}_s^{nni}$, then we will show that (R_1, R_2) is achievable, that is, for any given $\epsilon > 0$ and sufficiently large N, there exists a code (N, Δ, P_e) with two message sets $\mathcal{W}_1$ and $\mathcal{W}_2$, such that

$$\frac{log \parallel \mathcal{W}_1 \parallel}{N} \geq R_1 - \epsilon, \quad \frac{log \parallel \mathcal{W}_2 \parallel}{N} \geq R_2 - \epsilon,$$
$$\Delta \geq R_1 + R_2 - \epsilon, \quad P_e \leq \epsilon$$

8.1.1 Code construction: Without loss of generality, we only prove that the region $\mathcal{A}$ is achievable.

Given a pair $(R_1, R_2) \in \mathcal{A}$, choose a joint probability mass function

$$p_{U_1X_1U_2X_2SYZ}(u_1, x_1, u_2, x_2, s, y)$$
$$= p_{Z|Y}(z|y)p_{Y|X_1X_2S}(y|x_1, x_2, s)p_{U_1X_1|S}(u_1, x_1|s)$$
$$\times p_{U_2X_2|S}(u_2, x_2|s)p_S(s)$$

such that

$$R_1 = I(U_1; Y) - \max\{I(U_1; S), \quad I(U_1; Z)\} \tag{6}$$

and

$$R_2 = I(U_2; Y|U_1) - \max\{I(U_2; S), \quad I(U_2; Z|U_1)\} \tag{7}$$

Let $\mathcal{W}_1$ and $\mathcal{W}_2$ satisfy

$$\parallel \mathcal{W}_1 \parallel = 2^{NR_1} \tag{8}$$

$$\parallel \mathcal{W}_2 \parallel = 2^{NR_2} \tag{9}$$

The following paragraphs are organised as follows. Step (i) and Step (ii) are about the realisations of the auxiliary random vectors U_1^N and U_2^N according to the probability mass functions of U_1 and U_2, respectively. Step (iii) is the determination of the outputs x_1^N and x_2^N of the channel encoders according to u_1^N, u_2^N and s^N. Step (iv) is to decode the received vector y^N.

- (Step i) (A realisation of U_1^N)

Generate $2^{N(I(U_1;Y)-\epsilon_{1,N})}(\epsilon_{1,N} \to 0 \text{ as } N \to \infty)$ i.i.d. sequences u_1^N, according to the probability mass function $p_{U_1}(u_1)$. Distribute these sequences at random into $2^{NR_1} = 2^{N(I(U_1;Y)-\max(I(U_1;S),I(U_1;Z)))}$ bins such that each bin contains $2^{N(\max(I(U_1;S),I(U_1;Z))-\epsilon_{1,N})}$ sequences. Index each bin by $i \in \{1, 2, \ldots, 2^{NR_1}\}$. Then place the $2^{N(\max(I(U_1;S),I(U_1;Z))-\epsilon_{1,N})}$ sequences in every bin randomly into $2^{N(\max(I(U_1;S),I(U_1;Z))-I(U_1;Z)+\epsilon_{2,N})}(\epsilon_{2,N} \to 0 \text{ as } N \to \infty)$ sub-bins such that every sub-bin contains $2^{N(\max(I(U_1;Z)-\epsilon_{1,N}-\epsilon_{2,N})}$ sequences. Let J be the random variable to represent the index of the sub-bin. Index each sub-bin by

$$j \in \{1, 2, \ldots, 2^{N(\max(I(U_1;S),I(U_1;Z))-I(U_1;Z)+\epsilon_{2,N})}\}, \text{ that is}$$

$$\begin{aligned} &log \parallel \mathcal{J} \parallel \\ &\quad = N(\max(I(U_1; S), I(U_1; Z)) - I(U_1; Z) + \epsilon_{2,N}) \end{aligned} \tag{10}$$

Here, note that the number of sequences in every sub-bin is $2^{N(\max(I(U_1;Z)-\epsilon_{1,N}-\epsilon_{2,N})}$. This implies that

$$\frac{1}{N} H(U_1^N | W_1, J, Z^N) \leq \delta(\epsilon) \tag{11}$$

where $\delta(\epsilon) \to 0$ as $\epsilon \to 0$. Note that (11) can be proved by using Fano's inequality.

For a given message $w_1 \big(w_1 \in \mathcal{W}_1\big)$ and channel state s^N, try to find a sequence $u_1^N(w_1, i^*)$ in bin w_1 such that $(u_1^N(w_1, i^*), s^N) \in T_{U_1S}^N(\epsilon_2)$. If such multiple sequences in bin w_1 exist, choose the one with the smallest index in the bin. If no such sequence exists, declare an encoding error.

Fig. 6 shows the code-book construction of U_1^N for Theorem 1.

- (Step ii) (A realisation of U_2^N)

Generate $2^{N(I(U_2;Y|U_1)-\epsilon_{3,N})}(\epsilon_{3,N} \to 0 \text{ as } N \to \infty)$ i.i.d. sequences u_2^N, according to the probability mass function $p_{U_2}(u_2)$. Distribute these sequences at random into $2^{NR_2} = 2^{N(I(U_2;Y|U_1)-\max(I(U_2;S),I(U_2;Z|U_1)))}$ bins such that each bin contains $2^{N(\max(I(U_2;S),I(U_2;Z|U_1))-\epsilon_{3,N})}$ sequences. Index each bin by $i \in \{1, 2, \ldots, 2^{NR_2}\}$. Then place the $2^{N(\max(I(U_2;S),I(U_2;Z|U_1))-\epsilon_{3,N})}$ sequences in every bin randomly into $2^{N(\max(I(U_2;S),I(U_2;Z|U_1))-I(U_2;Z|U_1)+\epsilon_{4,N})}$ $(\epsilon_{4,N} \to 0 \text{ as } N \to \infty)$ sub-bins such that every sub-bin contains $2^{N(\max(I(U_2;Z|U_1)-\epsilon_{3,N}-\epsilon_{4,N})}$ sequences. Let K be a random variable to represent the index of the sub-bin. Index each sub-bin by $k \in \{1, 2, \ldots, 2^{N(\max(I(U_2;S),I(U_2;Z|U_1))-}$ $I(U_2;Z|U_1) + \epsilon_{4,N})\}$, that is

$$\begin{aligned} \log \parallel \mathcal{K} \parallel = N(&\max(I(U_2; S), \\ &I(U_2; Z|U_1)) - I(U_2; Z|U_1) + \epsilon_{4,N}) \end{aligned} \tag{12}$$

Here, note that the number of sequences in every sub-bin is $2^{N(\max(I(U_2;Z|U_1)-\epsilon_{3,N}-\epsilon_{4,N})}$. This implies that

$$\frac{1}{N} H(U_2^N | W_2, K, U_1^N, Z^N) \leq \delta_1(\epsilon) \tag{13}$$

where $\delta_1(\epsilon) \to 0$ as $\epsilon \to 0$. Note that (13) can be proved by using Fano's inequality.

For a given message $w_2 (w_2 \in \mathcal{W}_2)$ and channel state s^N, try to find a sequence $u_2^N(w_2, i^{**})$ in bin w_2 such that $(u_2^N(w_2, i^{**}), s^N) \in T_{U_2S}^N(\epsilon_3)$. If such multiple sequences in bin w_2 exist, choose the one with the smallest index in the bin. If no such sequence exists, declare an encoding error.

Fig. 7 shows the code-book construction of U_2^N for Theorem 1.

- (Step iii) (A realisation of X_1^N and X_2^N)

The x_1^N is generated according to a new discrete memoryless channel (DMC) with inputs u_1^N, s^N, and output x_1^N. The transition probability of this new DMC is $p_{X_1|U_1,S}(x_1|u_1, s)$, which is obtained from the joint probability mass function $p_{U_1X_1U_2X_2SY}(u_1, x_1, u_2, x_2, s, y)$. The probability $p_{X_1^N|U_1^N,S^N}(x_1^N|u_1^N, s^N)$ is calculated as follows

$$p_{X_1^N|U_1^N,S^N}(x_1^N|u_1^N, s^N) = \prod_{i=1}^{N} p_{X_1|U_1,S}(x_{1,i}|u_{1,i}, s_i) \tag{14}$$

Analogously, the x_2^N is generated according to a new DMC with inputs u_2^N, s^N, and output x_2^N. The transition probability of this new DMC is $p_{X_2|U_2,S}(x_2|u_2, s)$, which is obtained from the joint probability mass function $p_{U_1X_1U_2X_2SY}(u_1,$

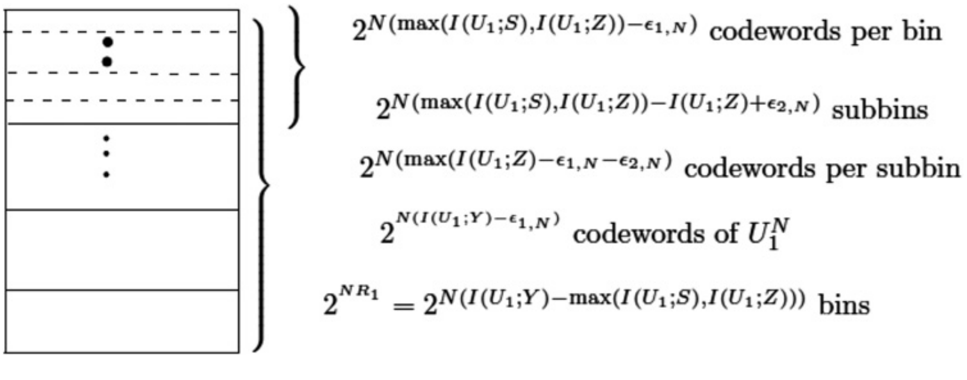
$2^{N(\max(I(U_1;S),I(U_1;Z))-\epsilon_{1,N})}$ codewords per bin
$2^{N(\max(I(U_1;S),I(U_1;Z))-I(U_1;Z)+\epsilon_{2,N})}$ subbins
$2^{N(\max(I(U_1;Z)-\epsilon_{1,N}-\epsilon_{2,N})}$ codewords per subbin
$2^{N(I(U_1;Y)-\epsilon_{1,N})}$ codewords of U_1^N
$2^{NR_1} = 2^{N(I(U_1;Y)-\max(I(U_1;S),I(U_1;Z)))}$ bins

Fig. 6 *Code-book construction of U_1^N for Theorem 3*

doi: 10.1049/iet-com.2013.0630

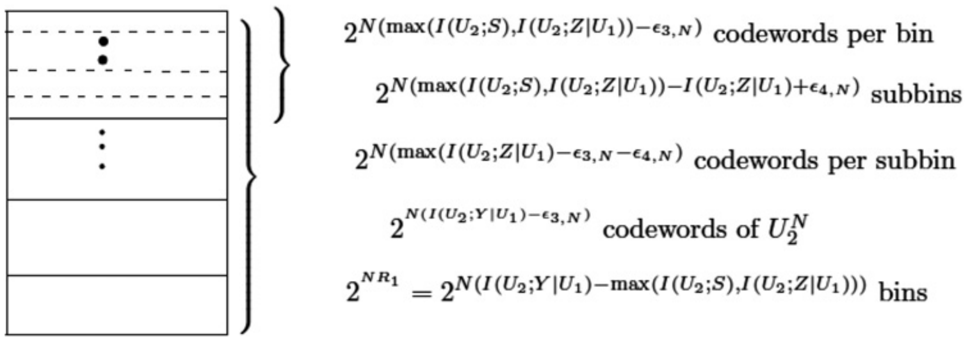
$2^{N(\max(I(U_2;S),I(U_2;Z|U_1))-\epsilon_{3,N})}$ codewords per bin
$2^{N(\max(I(U_2;S),I(U_2;Z|U_1))-I(U_2;Z|U_1)+\epsilon_{4,N})}$ subbins
$2^{N(\max(I(U_2;Z|U_1)-\epsilon_{3,N}-\epsilon_{4,N})}$ codewords per subbin
$2^{N(I(U_2;Y|U_1)-\epsilon_{3,N})}$ codewords of U_2^N
$2^{NR_1} = 2^{N(I(U_2;Y|U_1)-\max(I(U_2;S),I(U_2;Z|U_1)))}$ bins

Fig. 7 *Code-book construction of U_2^N for Theorem 3*

x_1, u_2, x_2, s, y). The probability $p_{X_2^N|U_2^N,S^N}(x_2^N|u_2^N, s^N)$ is calculated as follows

$$p_{X_2^N|U_2^N,S^N}(x_2^N|u_2^N, s^N) = \prod_{i=1}^{N} p_{X_2|U_2,S}(x_{2,i}|u_{2,i}, s_i) \qquad (15)$$

- (Step iv) (Decoding scheme of receiver): The inputs of the MAC are x_1^N, x_2^N and s^N, while the output is y^N. In the decoding scheme, for given y^N, try to find a pair of sequences $u_1^N(\hat{w}_1, \hat{i})$ and $u_2^N(\hat{w}_2, \hat{j})$ such that $(u_1^N(\hat{w}_1, \hat{i}), u_2^N(\hat{w}_2, \hat{j}), y^N) \in T^N_{U_1U_2Y}(\epsilon)$. If there exists a pair of such sequences, put out the corresponding $\hat{w}_1$ and $\hat{w}_2$ as the outputs of the decoder, else declare a decoding error.

8.1.2 Proof of achievability:

By using the above definitions, it is easy to verify that $(log \parallel \mathcal{W}_1 \parallel /N) \geq R_1 - \epsilon$ and $(log \parallel \mathcal{W}_2 \parallel /N) \geq R_2 - \epsilon$.

Then, note that $P_e \leq \epsilon$ holds if

$$R_1 \leq I(U_1; Y|U_2) - I(U_1; S) \qquad (16)$$

$$R_2 \leq I(U_2; Y|U_1) - I(U_2; S) \qquad (17)$$

and

$$R_1 + R_2 \leq I(U_1, U_2; Y) - I(U_1; S) - I(U_2; S) \qquad (18)$$

Observing that $R_1 = I(U_1;Y) - \max I(U_1;S)$, $I(U_1;Z)$ and $R_2 = I(U_2;Y|U_1) - \max I(U_2;S)$, $I(U_2;Z|U_1)$, then it is easy to see that (16), (17) and (18) are satisfied. Thus, $P_e \leq \epsilon$ is proved, and the details are omitted here.

It remains to show that $\Delta \geq R_1 + R_2 - \epsilon$, see the following.

The equivocation Δ can be rewritten as

$$\begin{aligned}\Delta &= \frac{1}{N}H(W_1, W_2|Z^N)\\ &= \frac{1}{N}(H(W_1|Z^N) + H(W_2|Z^N, W_1))\end{aligned} \qquad (19)$$

Then, the conditional entropies $H(W_1/Z^N)$ and $H(W_2/Z^N, W_1)$ are bounded as follows

$$\begin{aligned}\frac{1}{N}H(W_1|Z^N) &= \frac{1}{N}(H(W_1, Z^N) - H(Z^N))\\ &= \frac{1}{N}(H(W_1, Z^N, J, U_1^N) - H\\ &\quad \times (J, U_1^N|W_1, Z^N) - H(Z^N))\\ &=^{(1)} \frac{1}{N}(H(Z^N|U_1^N) + H(W_1, J, U_1^N)\\ &\quad - H(J|W_1, Z^N) - H(U_1^N|W_1, Z^N, J)\\ &\quad - H(Z^N))\\ &=^{(2)} \frac{1}{N}(H(Z^N|U_1^N) + H(U_1^N) - H(J|W_1, Z^N)\\ &\quad - H(U_1^N|W_1, Z^N, J) - H(Z^N))\\ &\geq^{(3)} \frac{1}{N}(H(Z^N|U_1^N) + H(U_1^N) - log|J|\\ &\quad - H(U_1^N|W_1, Z^N, J) - H(Z^N))\\ &\geq^{(4)} \frac{1}{N}(H(Z^N|U_1^N) + H(U_1^N) - log|J|\\ &\quad - H(Z^N)) - \delta(\epsilon)\\ &\geq \frac{1}{N}(H(Z^N|U_1^N) + H(U_1^N) - H(U_1^N|Y^N)\\ &\quad - log|J| - H(Z^N)) - \delta(\epsilon)\\ &=^{(5)} \frac{1}{N}(NI(U_1; Y) - NI(U_1; Z) - N\\ &\quad \times (\max(I(U_1; S), I(U_1; Z))\\ &\quad - I(U_1; Z) + \epsilon_{2,N})) - \delta(\epsilon)\\ &= I(U_1; Y) - \max(I(U_1; S),\\ &\quad \times I(U_1; Z)) - \epsilon_{2,N} - \delta(\epsilon)\\ &=^{(6)} R_1 - \epsilon_{2,N} - \delta(\epsilon)\end{aligned} \qquad (20)$$

where (1) is from the Markov chain $(J, W_1) \rightarrow U_1^N \rightarrow Z^N$, (2) is from the fact that $H(W_1, J|U_1^N) = 0$, (3) is from $H(J) \leq \log|J|$, (4) is from (11), (5) is from (10) and the fact that S^N, U_1^N, X_1^N and X_2^N are i.i.d. generated random vectors, and the channels are discrete memoryless, and (6) is from $R_1 = I(U_1;Y) - \max(I(U_1;S), I(U_1;Z))$.

where (a) is from $H(W_1|U_1^N) = 0$, (b) is from the Markov chain $(K, W_2) \rightarrow (U_1^N, U_2^N) \rightarrow Z^N$, (c) is from the fact that $H(W_2, K|U_1^N, U_2^N) = 0$, (d) is from (13), (e) is from (12) and the fact that S^N, U_1^N, U_2^N, X_1^N and X_2^N are i.i.d. generated random vectors, and the channels are discrete memoryless, and (f) is from $R_2 = I(U_2;Y|U_1) - \max(I(U_2;S), I(U_2;Z|U_1))$.

Substituting (20) and (21) into (19), and choosing sufficiently large N, $\Delta \geq R_1 + R_2 - \epsilon$ is proved.

The proof of Theorem 3 is completed.

$$
\begin{aligned}
\frac{1}{N}H(W_2|Z^N, W_1) &\geq H(W_2|Z^N, W_1, U_1^N)\\
&=^{(a)} H(W_2|Z^N, U_1^N)\\
&= \frac{1}{N}(H(W_2, Z^N, U_1^N) - H(Z^N, U_1^N))\\
&= \frac{1}{N}(H(W_2, Z^N, K, U_2^N, U_1^N) - H(K, U_2^N|W_2, Z^N, U_1^N) - H(Z^N, U_1^N))\\
&=^{(b)} \frac{1}{N}(H(Z^N|U_1^N, U_2^N) + H(W_2, K, U_1^N, U_2^N) - H(K|W_2, Z^N, U_1^N) - H(U_2^N|W_2, Z^N, K, U_1^N) - H(Z^N, U_1^N))\\
&\geq^{(c)} \frac{1}{N}(H(Z^N|U_1^N, U_2^N) + H(U_1^N, U_2^N) - log|K| - H(U_2^N|W_2, Z^N, K, U_1^N) - H(Z^N, U_1^N))\\
&\geq^{(d)} \frac{1}{N}(H(Z^N|U_1^N, U_2^N) + H(U_2^N|U_1^N) + H(U_1^N) - log|K| - H(Z^N, U_1^N)) - \delta_1(\epsilon)\\
&\geq \frac{1}{N}(H(Z^N|U_1^N, U_2^N) + H(U_2^N|U_1^N) - H(U_2^N|U_1^N, Y^N) + H(U_1^N) - log|K| - H(Z^N, U_1^N)) - \delta_1(\epsilon)\\
&=^{(e)} I(U_2; Y|U_1) - I(U_2; Z|U_1) - (\max(I(U_2; S), I(U_2; Z|U_1)) - I(U_2; Z|U_1) + \epsilon_{4,N}) - \delta_1(\epsilon)\\
&= I(U_2; Y|U_1) - \max(I(U_2; S), I(U_2; Z|U_1)) - \epsilon_{4,N} - \delta_1(\epsilon)\\
&=^{(f)} R_2 - \epsilon_{4,N} - \delta_1(\epsilon)
\end{aligned}
\tag{21}
$$