Capacity-Equivocation Region of a Special Case of Wiretap Channel with Noiseless Feedback

Bin Dai, A. J. Han Vinck, Yuan Luo, and Zheng Ma

Abstract: **The general wiretap channel with noiseless feedback is first investigated by Ahlswede and Cai, where lower and upper bounds on the secrecy capacity are provided in their work. The upper bound is met with equality only in some special cases. In this paper, we study a special case of the general wiretap channel with noiseless feedback (called non-degraded wiretap channel with noiseless feedback). Inner and outer bounds on the capacity-equivocation region of this special model are provided. The outer bound is achievable if the main channel is more capable than the wiretap channel. The inner bound is constructed especially for the case that the wiretap channel is more capable than the main channel. The results of this paper are further explained via binary and Gaussian examples. Compared with the capacity results for the non-degraded wiretap channel, we find that the security is enhanced by using the noiseless feedback.**

Index Terms: **Capacity-equivocation region, noiseless feedback, secrecy capacity, wiretap channel.**

I. INTRODUCTION

THE concept of the wiretap channel was first introduced by Wyner [1]. It is a kind of degraded broadcast channel. The wiretapper knows the encoding scheme used at the transmitter and the decoding scheme used at the legitimate receiver. The object is to describe the rate of reliable communication from the transmitter to the legitimate receiver, subject to a constraint of the equivocation to the wiretapper. After the publication of Wyner's work, Csiszár and Körner [2] investigated a more general situation: The broadcast channels with confidential messages. It is clear that Wyner's wiretap channel is a special case of the model of Csiszár and Körner, in a manner that the main channel is less noisy than the wiretap channel. In addition, the secrecy capacity of the non-degraded wiretap channel was also formulated in [2], which provides the best transmission rate with perfect secrecy. Based on Wyner's work, Leung-Yan-Cheong and Hellman studied the Gaussian wiretap channel (GWC) [3], and showed that its secrecy capacity was the difference between the main channel capacity and the overall wiretap channel capacity (the cascade of main channel and wiretap channel). Recently, Mitrpant *et al.* [4] and Chen *et al.* [5] studied wiretap channel with noncausal channel state information, where both of them focused on achievable regions. Based on the work of [5], Dai [6] provided an outer bound on the wiretap channel with noncausal channel state information (CSI), and determined the capacity-equivocation region for the model of wiretap channel 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. In addition, Merhav [7] studied a specific wiretap channel, and obtained the capacity region, where both the legitimate receiver and the wiretapper have access to some leaked symbols from the source, but the channels for the wiretapper are more noisy than the legitimate receiver, which shares a secret key with the encoder.

It is a well-known fact that the feedback does not increase the capacity of a discrete memoryless channel (DMC). However, does the feedback increase the secrecy capacity of the wiretap channel? To solve this problem, Ahlswede and Cai [8] studied the general wiretap channels with noiseless feedback, see Fig. 1. The upper and lower bounds on the secrecy capacity were provided. The lower bound is proved to be tight, while the upper bound is only tight for some special cases. Specifically, for the degraded wiretap channel with noiseless feedback, the secrecy capacity satisfies

$$\begin{aligned} C_s &= \max_{p(x)} \min\{I(X;Y), \\ &\qquad I(X;Y) - I(X;Z) + H(Y|X,Z)\} \end{aligned} \tag{1.1}$$

where X, Y, and Z are input of the main channel, output of the main channel, and output of the wiretap channel, respectively. Recall that the secrecy capacity C_{s1} of the degraded wiretap channel is determined by Wyner [1], and it is given by

$$C_{s1} = \max_{p(x)} \min\{I(X;Y), I(X;Y) - I(X;Z)\}. \tag{1.2}$$

From the above definitions of C_s and C_{s1}, it is easy to see that the noiseless feedback increases the secrecy capacity of the wiretap channel.

Here note that in [8], the legitimate receiver just sends back the previous received symbols to the transmitter, and it is natural to ask: is it better for the legitimate receiver to send back pure randomness secret keys to the transmitter? Ardestanizadeh *et al.* [9] answered this question by considering the model of wiretap channel with secure rate-limited feedback. Ardestanizadeh *et al.*

Manuscript received June 14, 2013; approved for publication by Emanuele Viterbo, Division I Editor, December 13, 2014.

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, the Fundamental Research Funds for the Central Universities under Grant 2682014CX099, and the Open Research Fund of National Mobile Communications Research Laboratory, Southeast University (No. 2014D01).

B. Dai is with the School of Information Science and Technology, Southwest JiaoTong University, Chengdu 610031, China, and with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China, email: daibin@home.swjtu.edu.cn.

A. J. Han Vinck is with the Institute for Experimental Mathematics, Duisburg-Essen University, Ellernstr. 29, 45326 Essen, Germany, email: vinck@iem.uni-due.de.

Y. Luo is with the Computer Science and Engineering Department, Shanghai Jiao Tong University, Shanghai 200240, China, email: yuanluo@sjtu.edu.cn.

Z. Ma is with the School of Information Science and Technology, Southwest JiaoTong University, Chengdu 610031, China, email: zma@home.swjtu.edu.cn.

Digital object identifier 10.1109/JCN.2015.000005

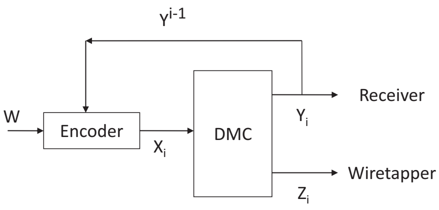


Fig. 1. The general wiretap channel with noiseless feedback.

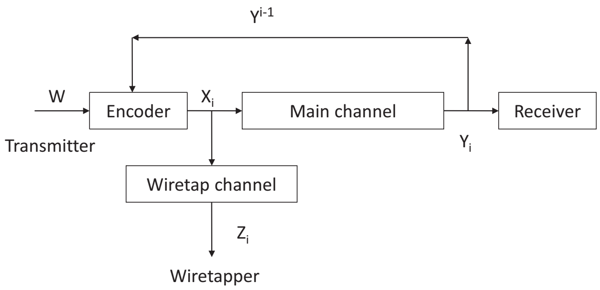


Fig. 2. The non-degraded wiretap channel with noiseless feedback.

[9] showed that if the limits (capacity) of the feedback channel is denoted by R_f, the secrecy capacity of the physically degraded wiretap channel ($X \rightarrow Y \rightarrow Z$) with secure rate-limited feedback is given by

$$C_{sf} = \max_{p(x)} \min\{I(X;Y), \; I(X;Y) - I(X;Z) + R_f\}. \quad (1.3)$$

Compared with C_s, it is easy to see that if $R_f \leq H(Y|X,Z)$, sending pure randomness secret keys is no better than sending Y^{i-1} back. If $R_f > H(Y|X,Z)$, sending pure randomness secret keys is better than sending Y^{i-1} back.

In this paper, we study the model of non-degraded wiretap channel with noiseless feedback, see Fig. 2. In this model, the ith time input of the main channel X_i depends not only on the message W, but also on the previous outputs of the main channel Y^{i-1}. The wiretapper can observe X_i via a wiretap channel, see Fig. 2. Note that in Fig. 2, given X_i, Y_i is independent of Z_i, i.e., $X_i \rightarrow Z_i \rightarrow Y_i$. Therefore, the model of Fig. 2 is a special case of Fig. 1. Inner and outer bounds on the capacity-equivocation region of Fig. 2 are provided. The results are further explained via binary and Gaussian examples.

The reminder of this paper is organized as follows. In Section II, we present the basic definitions and the main results on the capacity-equivocation region (including the secrecy capacity). In Section III, we give the capacity-equivocation regions of the binary and Gaussian examples. Final conclusions are presented in Section IV.

II. DEFINITIONS AND THE MAIN RESULTS

In this paper, random variab1es, sample values, and alphabets are denoted by capital letters, lower case letters, and calligraphic letters, respectively. Let $P_V(v)$ denote the probability mass function $Pr\{V = v\}$. Let $T_V^N(\eta)$ be the strong typical set with respect to $P_V(v)$. Throughout the paper, the logarithmic function is to the base 2.

Definition 1: (**Channel encoder**) The message W is uniformly distributed over $\mathcal{W}$. The feedback Y^{i-1} (where $2 \leq i \leq N$) is the previous $i-1$ time output of the main channel. At the ith time, the inputs of the channel encoder are W and Y^{i-1}, while the output is X_i. The ith time channel encoder is a stochastic encoder with the conditional probability distribution $P_{X|W,Y_1,\cdots,Y_{i-1}}(x_i|w, y_1, \cdots, y_{i-1})$.

Definition 2: (**Channels**) The main channel is a DMC with finite input alphabet $\mathcal{X}$, finite output alphabet $\mathcal{Y}$, and transition probability $P_{Y|X}(y|x)$, where $x \in \mathcal{X}$, and $y \in \mathcal{Y}$. $P_{Y^N|X^N}(y^N|x^N) = \Pi_{i=1}^N P_{Y|X}(y_i|x_i)$. The input of the main channel is X^N, while the output is Y^N.

The wiretap channel is also a DMC with finite input alphabet $\mathcal{X}$, finite output alphabet $\mathcal{Z}$, and transition probability $P_{Z|X}(z|x)$, where $x \in \mathcal{X}$, $z \in \mathcal{Z}$. The input and output of the wiretap channel are X^N and Z^N, respectively. The equivocation to the wiretapper is defined as

$$\Delta = \frac{1}{N} H(W|Z^N). \quad (2.1)$$

The perfect secrecy is achieved when $H(W|Z^N) = H(W)$. Note that given the input X^N, the output Z^N of the wiretap channel and the output Y^N of the main channel are conditionally independent.

Definition 3: (**The relation of the main channel and the wiretap channel**) Similar to the definitions in [2], "the main channel is more capable than the wiretap channel" is characterized by $I(X;Y) \geq I(X;Z)$ for every input $P_X(x)$, and "the wiretap channel is more capable than the main channel" is characterized by $I(X;Y) \leq I(X;Z)$ for every input $P_X(x)$.

Definition 4: (**Decoder**) The Decoder for the receiver is a mapping $f_D : \mathcal{Y}^{\mathcal{N}} \rightarrow \mathcal{W}$, with input Y^N and output $\hat{W}$. Let P_e be the error probability of the receiver, and it is defined as $Pr\{W \neq \hat{W}\}$.

A rate pair (R, R_e) (where $R, R_e > 0$) is called achievable if, for any $\epsilon > 0$, there exists a channel encoder-decoder (N, Δ, P_e) such that

$$\lim_{N \rightarrow \infty} \frac{\log |\mathcal{W}|}{N} = R, \lim_{N \rightarrow \infty} \Delta \geq R_e, P_e \leq \epsilon. \quad (2.2)$$

The capacity-equivocation region $\mathcal{R}$ is the set composed of all achievable (R, R_e) pairs in the model of Fig. 2.

Define $\mathcal{R}^{\mathcal{A}}$ to be the set of all pairs (R_1, R_e) such that

$$\mathcal{R}^{\mathcal{A}} = \bigcup_{P_X(x):} \left\{ \begin{array}{l} (R, R_e) : R_e \leq R, \\ R \leq I(X;Y), \\ R_e \leq H(Y|Z). \end{array} \right\},$$

for some distribution

$$P_{X,Y,Z}(x,y,z) = P_{Z|X}(z|x) P_{Y|X}(y|x) P_X(x),$$

which implies the Markov chain $Y \rightarrow X \rightarrow Z$.

As stated in the next theorem, the set $\mathcal{R}^{\mathcal{A}}$ is an outer bound on the capacity-equivocation region $\mathcal{R}$ of the model of Fig. 2.

Theorem 1: The capacity-equivocation region $\mathcal{R}$ of Fig. 2 satisfies

$$\mathcal{R} \subseteq \mathcal{R}^{\mathcal{A}}.$$

Proof: See Appendix I. □

Remark 1: There are some notes on Theorem 1, see the followings.

1) The outer bound $\mathcal{R}^{\mathcal{A}}$ is achievable if the main channel is more capable than the wiretap channel, i.e., if $I(X;Y) \geq I(X;Z)$ for every input $P_X(x)$, the capacity-equivocation region of Fig. 2 is denoted by

$$\mathcal{R} = \mathcal{R}^{\mathcal{A}} = \bigcup_{\substack{P_X(x): \\ I(X;Y) \geq I(X;Z)}} \left\{ \begin{array}{l} (R, R_e) : R_e \leq R, \\ R \leq I(X;Y), \\ R_e \leq H(Y|Z). \end{array} \right\}.$$

Proof: See Appendix I and Appendix II. □

2) The secrecy capacity $C_s^{'}$ of the model of Fig. 2 is denoted by

$$C_s^{'} = \max_{(R, R_e = R) \in \mathcal{R}} R. \tag{2.3}$$

Substituting $R_e = R$ into Theorem 1, it is easy to see that

$$C_s^{'} \leq \max_{P_X(x)} \min\{I(X;Y), H(Y|Z)\}, \tag{2.4}$$

and "=" is achieved if $I(X;Y) \geq I(X;Z)$ for every input $P_X(x)$.

The inner bound is stated next. Define $\mathcal{R}^{\mathcal{B}}$ to be the set of all pairs (R, R_e) such that

$$\mathcal{R}^{\mathcal{B}} = \bigcup_{\substack{P_X(x): \\ I(X;Y) \leq I(X;Z)}} \left\{ \begin{array}{l} (R, R_e) : R_e \leq R, \\ R \leq I(X;Y), \\ R_e \leq H(Y|X). \end{array} \right\},$$

for some distribution

$$P_{X,Y,Z}(x,y,z) = P_{Z|X}(z|x) P_{Y|X}(y|x) P_X(x),$$

which implies the Markov chain $Y \rightarrow X \rightarrow Z$.

Theorem 2: The capacity-equivocation region $\mathcal{R}$ of Fig. 2 satisfies

$$\mathcal{R}^{\mathcal{B}} \subseteq \mathcal{R}.$$

Remark 2: There are some notes on Theorem 2, see the followings.

1) Note that the inequality $R_e \leq H(Y|X)$ of $\mathcal{R}^{\mathcal{B}}$ implies that $R_e \leq H(Y|X) = H(Y|X,Z) \leq H(Y|Z)$. Since the secrecy rate $R = \max_{P_X(x)} \min\{I(X;Y), H(Y|Z)\}$ is achievable if the main channel is more capable than the wiretap channel, the secrecy rate $\max_{P_X(x)} \min\{I(X;Y), H(Y|X)\}$ is also achievable for this case. To prove the achievability of $\mathcal{R}^{\mathcal{B}}$, it remains to show that $\mathcal{R}^{\mathcal{B}}$ is achievable if the wiretap channel is more capable than the main channel, see Appendix II.
2) The secrecy capacity $C_s^{'}$ of the model of Fig. 2 satisfies

$$C_s^{'} \geq \max_{P_X(x)} \min\{I(X;Y), H(Y|X)\}. \tag{2.5}$$

3) If the wiretap channel is more capable than the main channel, the secrecy capacity of the non-degraded wiretap channel without feedback reduces to zero. However, for the feedback model, the rate $\max_{P_X(x)} \min\{I(X;Y), H(Y|X)\}$ is also an achievable secrecy rate, and this is because the noiseless feedback is used as a secret key shared by the transmitter and the legitimate receiver, while the wiretapper does not know the key. Therefore, by using feedback, the security is enhanced.

III. BINARY AND GAUSSIAN EXAMPLES OF FIGURE 2

A. The Binary Case of the Model of Figure 2

In this subsection, we study the following binary case of Fig. 2. Throughout this subsection, the logarithmic function is to the base 2.

Assume that all channels inputs and outputs take values in $\{0, 1\}$, and the channels are discrete memoryless. The input-output relationship of the channels at each time instant satisfies

$$Y_i = X_i \oplus Z_{1,i}, \quad Z_i = X_i \oplus Z_{2,i}, \tag{3.1}$$

where $1 \leq i \leq N$, and Z_1^N, Z_2^N are composed of N i.i.d. random variables with distributions $Pr\{Z_{1,i} = 1\} = p$, $Pr\{Z_{1,i} = 0\} = 1 - p$, $Pr\{Z_{2,i} = 1\} = q$, and $Pr\{Z_{2,i} = 0\} = 1 - q$, respectively. Let $0 \leq p, q \leq 0.5$. The following Theorem 3 provides the secrecy capacity of the binary case of Fig. 2.

Theorem 3: For the binary non-degraded wiretap channel with noiseless feedback (Fig. 2), the achievable secrecy rate C_s^{fbi} is given by

$$C_s^{\text{fbi}} = \begin{cases} \min\{1 - h(p), h(p + q - 2pq)\}, & \text{if } q \geq p, \\ \min\{1 - h(p), h(p)\}, & \text{otherwise.} \end{cases} \tag{3.2}$$

Proof: Let $P_X(0) = \alpha$ and $P_X(1) = 1 - \alpha$. By calculating and maximizing (the maximum is achieved when $\alpha = 0.5$) the terms in Theorem 1 and 2, we have Theorem 3. Thus, the proof of Theorem 3 is completed. □

Moreover, the secrecy capacity of the binary non-degraded wiretap channel (Fig. 2 without feedback) is given by the following Theorem 4.

Theorem 4: For the binary non-degraded wiretap channel, the secrecy capacity C_s^b is given by

$$C_s^b = \begin{cases} h(q) - h(p), & \text{if } q \geq p, \\ 0, & \text{otherwise.} \end{cases} \tag{3.3}$$

Proof: The proof of Theorem 4 is directly obtained by calculating and maximizing $I(X;Y) - I(X;Z)$, and thus, the proof is omitted here. □

By using $0 \leq h(p + q - 2pq) \leq 0.5$ and $h(p + q - 2pq) = h(q + p(1 - 2q)) \geq h(q) \geq h(q) - h(p)$, it is easy to see that C_s^{fbi} is larger than C_s^b, i.e., feedback enhances the security of this binary model.

B. The Gaussian Case of the Model of Figure 2

In this subsection, we study the Gaussian case of Fig. 2. The channel input-output relationships at each time instant i ($1 \leq i \leq N$) are given by

$$Y_i = X_i + Z_{1,i}, \quad Z_i = X_i + Z_{2,i} \tag{3.4}$$

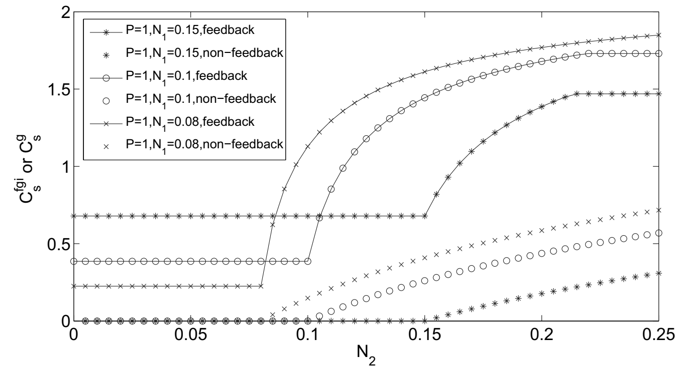


Fig. 3. The secrecy rates of the Gaussian non-degraded wiretap channel with or without noiseless feedback.

where $Z_{1,i} \sim \mathcal{N}(0, N_1)$ and $Z_{2,i} \sim \mathcal{N}(0, N_2)$. The random vectors Z_1^N and Z_2^N are independent with i.i.d. components. The channel input X^N is subject to the average power constraint P.

The following Theorem 5 provides the secrecy capacity of the Gaussian case of Fig. 2.

Theorem 5: For the Gaussian non-degraded wiretap channel with noiseless feedback (Fig. 2), the secrecy rate C_s^{fgi} is given by

$$C_s^{\text{fgi}} = \min\left\{\frac{1}{2}\log\left(1+\frac{P}{N_1}\right), \frac{1}{2}\log(2\pi e N_1)\right\} \tag{3.5}$$

if $N_1 \geq N_2$, and

$$C_s^{\text{fgi}} = \min\left\{\frac{1}{2}\log\left(1+\frac{P}{N_1}\right), \frac{1}{2}\log\left(2\pi e\left(N_1+\frac{(N_2-N_1)P}{N_2}\right)\right)\right\} \tag{3.6}$$

if $N_1 < N_2$.

Proof: The proof of Theorem 5 is directly obtained by calculating and maximizing the terms in Theorem 1, and thus, the proof is omitted here. □

Moreover, the secrecy capacity of the Gaussian non-degraded wiretap channel (Fig. 2 without feedback) is given by the following Theorem 6.

Theorem 6: For the Gaussian non-degraded wiretap channel, the secrecy capacity C_s^g is given by

$$C_s^g = \begin{cases} 0, & \text{if } N_1 \geq N_2, \\ \frac{1}{2}\log\left(\frac{N_2(N_1+P)}{N_1(N_2+P)}\right), & \text{otherwise.}\end{cases} \tag{3.7}$$

Proof: The result is directly obtained from [3], and therefore, the proof is omitted here. □

Fig. 3 plots the secrecy rates of the Gaussian case of Fig. 2 with or without feedback. It is easy to see that for fixed P and N_1, the feedback enhances the security of the Gaussian non-degraded wiretap channel Moreover, when P is fixed, the secrecy capacity of the Gaussian non-degraded wiretap channel is increasing while N_1 is decreasing.

IV. CONCLUSION

In this paper, we study the model of non-degraded wiretap channel with noiseless feedback. Inner and outer bounds on the capacity-equivocation region of the model of Fig. 2 are provided. We show that if X, Y, and Z satisfy the Markov chain $Y \rightarrow X \rightarrow Z$ and $I(X;Y) \geq I(X;Z)$ for every input $p_X(x)$, the outer bound is achievable. Moreover, if X, Y, and Z satisfy the Markov chain $Y \rightarrow X \rightarrow Z$ and $I(X;Y) \leq I(X;Z)$ for every input $p_X(x)$, we provide an inner bound for this case, and it is different from that of [8, Theorem 1]. Compared with the capacity results for the non-degraded wiretap channel, we find that the security is enhanced by using this noiseless feedback.

ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers for their valuable suggestions on improving this paper.

APPENDICES

I. PROOF OF THEOREM 1

In this section, we prove all the achievable pairs (R, R_e) of the model of Fig. 2 are contained in the set $\mathcal{R}^{\mathcal{A}}$. We will prove the inequalities of $\mathcal{R}^{\mathcal{A}}$ in the remainder of this section. The proof of $R \leq I(X;Y)$ and $R_e \leq R$ are obvious, and it is omitted here. Therefore, it only needs to prove that $R_e \leq H(Y|Z)$, see the following.

$$\begin{aligned} \frac{1}{N}H(W|Z^N) &\stackrel{(1)}{\leq} \frac{1}{N}(I(W;Y^N|Z^N)+\delta(P_e)) \\ &\leq \frac{1}{N}\sum_{i=1}^{N} H(Y_i|Z_i) + \frac{\delta(P_e)}{N} \\ &\stackrel{(2)}{\leq} H(Y_J|Z_J) + \frac{\delta(P_e)}{N} \\ &\stackrel{(3)}{=} H(Y|Z) + \frac{\delta(P_e)}{N} \end{aligned} \tag{A1}$$

where (1) is from Fano's inequality, (2) is from J is a random variable (uniformly distributed over $\{1, 2, \cdots, N\}$), and it is independent of Y^N and Z^N, and (3) is from the definitions that $Y \triangleq Y_J$ and $Z \triangleq Z_J$.

By using $P_e \leq \epsilon$, $\epsilon \rightarrow 0$ as $N \rightarrow \infty$, $\lim_{N\rightarrow\infty} \frac{H(W|Z^N)}{N} \geq R_e$ and (A1), it is easy to see that $R_e \leq H(Y|Z)$.

The proof of Theorem 1 is completed.

II. ACHIEVABILITY PROOF OF $\mathcal{R}^{\mathcal{A}}$ AND $\mathcal{R}^{\mathcal{B}}$

A. Achievability Proof of $\mathcal{R}^{\mathcal{A}}$

In this subsection, we will show that if $I(X;Y) \geq I(X;Z)$ for every input $P_X(x)$, any pair $(R, R_e) \in \mathcal{R}^{\mathcal{A}}$ is achievable. Block Markov coding and Ahlswede-Cai's secret key on feedback [8] are used in the construction of the code-book. Since $R_e \leq H(Y|Z)$ and $R_e \leq R \leq I(X;Y)$, the achievability proof of $\mathcal{R}^{\mathcal{A}}$ is considered into two cases.

- **Case 1:** If $I(X;Y) \geq H(Y|Z)$, it is sufficient to show that the pair $(R = I(X;Y) - \epsilon, R_e = H(Y|Z))$ is achievable, where ϵ is a fixed small positive real numbers, and $\epsilon \rightarrow 0$.

- **Case 2:** If $I(X;Y) \leq H(Y|Z)$, it is sufficient to show that the pair $(R = I(X;Y) - \epsilon, R_e = R = I(X;Y) - \epsilon)$ is achievable.

Lemma 1: (Balanced coloring lemma) For all ϵ_1, ϵ_2, ϵ_3, $\delta > 0$, sufficiently large N and all N-type $P_Y(y)$, there exists a γ- coloring c: $T_Y^N(\epsilon_1) \rightarrow \{1, 2, \cdots, \gamma\}$ of $T_Y^N(\epsilon_1)$ such that for all joint N-type $P_{YZ}(y,z)$ with marginal distribution $P_Z(z)$ and $\frac{|T^N_{Y|Z}(z^N)|}{\gamma} > 2^{N\epsilon_2}$, $z^N \in T_Z^N(\epsilon_3)$,

$$|c^{-1}(k)| \leq \frac{|T^N_{Y|Z}(z^N)|(1+\delta)}{\gamma}, \tag{A2}$$

for $k = 1, 2, \cdots, \gamma$, where c^{-1} is the inverse image of c.

Proof: Letting $U = \text{const}$, Lemma 1 is directly from [8, p. 259], and thus we omit it here. □

Lemma 1 shows that if y^N and z^N are joint typical, for given z^N, the number of $y^N \in T^N_{Y|Z}(z^N)$ for a certain color k ($k = 1, 2, \cdots, \gamma$), which is denoted as $|c^{-1}(k)|$, is upper bounded by $\frac{|T^N_{Y|Z}(z^N)|(1+\delta)}{\gamma}$. By using Lemma 1, it is easy to see that the typical set $T^N_{Y|Z}(z^N)$ maps into at least

$$\frac{|T^N_{Y|Z}(z^N)|}{\frac{|T^N_{Y|Z}(z^N)|(1+\delta)}{\gamma}} = \frac{\gamma}{1+\delta} \tag{A3}$$

colors. On the other hand, the typical set $T^N_{Y|Z}(z^N)$ maps into at most γ colors.

Code construction: Fix the joint probability mass function $P_{Z|Y}(z|y)P_{Y|X}(y|x)P_X(x)$. The message set $\mathcal{W}$ satisfies $\frac{\log \|\mathcal{W}\|}{N} = R = I(X;Y) - \epsilon$, where ϵ is a fixed small positive real numbers.

We use the block Markov coding method. The random vectors X^N, Y^N and Z^N consist of n blocks of length N. Let $\tilde{Y}_i$ and $\tilde{Z}_i$ ($1 \leq i \leq n$) are the outputs of the main channel and the wiretap channel, respectively. Define $Y^n = (\tilde{Y}_1, \tilde{Y}_2, \cdots, \tilde{Y}_n)$ and $Z^n = (\tilde{Z}_1, \tilde{Z}_2, \cdots, \tilde{Z}_n)$. The message for n blocks is $W^n = (W_1, W_2, \cdots, W_n)$, where W_i ($2 \leq i \leq n$) are i.i.d. random variables uniformly distributed over $\mathcal{W}$. Note that in the first block, there is no w_1.

- **Construction of X^N for case 1:** Generate 2^{NR} i.i.d. sequences x^N, according to the probability mass function $P_X(x)$. Denote the message w_i ($2 \leq i \leq n$) by $w_i = (w_{i1}, w_{i2})$, where $w_{i1} \in \{1, 2, \cdots, 2^{NH(Y|Z)}\}$ and $w_{i2} \in \{1, 2, \cdots, 2^{N(R-H(Y|Z))}\}$. In the first block, randomly choose a codeword $x^N(a_1)$ ($a_1 \in \{1, 2, \cdots, 2^{NR}\}$) to transmit. For the ith block ($2 \leq i \leq n$), when the transmitter receives the output $\tilde{Y}_{i-1}$ of the $(i-1)$th block, he gives up if $\tilde{Y}_{i-1} \notin T_Y^N(\epsilon_2)$ ($\epsilon_2 \rightarrow 0$ as $N \rightarrow \infty$). It is easy to see that the probability for giving up at the $(i-1)$th block tends to 0 as $N \rightarrow \infty$. In the case $\tilde{Y}_{i-1} \in T_Y^N(\epsilon_2)$, generate a mapping g_f: $T_Y^N(\epsilon_2) \rightarrow \{1, 2, \cdots, 2^{NH(Y|Z)}\}$. Define a random variable $K_i^* = g_f(\tilde{Y}_{i-1})$ ($2 \leq i \leq n$), which is uniformly distributed over $\{1, 2, \cdots, 2^{NH(Y|Z)}\}$, and K_i^* is independent of W_i. Reveal the mapping g_f to the legitimate receiver, the wiretapper and the transmitter. Then, since the transmitter receives the output $\tilde{Y}_{i-1}$ of the $(i-1)$th block, he computes $k_i^* = g_f(\tilde{y}_{i-1}) \in \{1, 2, \cdots, 2^{NH(Y|Z)}\}$. For a given $w_i = (w_{i1}, w_{i2})$ ($2 \leq i \leq n$), the transmitter chooses a sequence $x^N(w_{i1} \oplus k_i^*, w_{i2})$ to transmit (note that here $\oplus$ is the modulo addition over $\{1, 2, \cdots, 2^{NH(Y|Z)}\}$).
- **Construction of X^N for case 2:** The construction of X^N for case 2 is similar to that of case 1, except that there is no need to divide w_i into two parts. The detail is as follows. For the ith block ($2 \leq i \leq n$), if $\tilde{Y}_{i-1} \in T_Y^N(\epsilon_2)$, generate a mapping g_f: $T_Y^N(\epsilon_2) \rightarrow \mathcal{W}$ (note that $|T_Y^N(\epsilon_2)| \geq |\mathcal{W}|$). Define a random variable $K_i^* = g_f(\tilde{Y}_{i-1})$ ($2 \leq i \leq n$), which is uniformly distributed over $\mathcal{W}$, and K_i^* is independent of W_i. Reveal the mapping g_f to the legitimate receiver, the wiretapper and the transmitter. Then when the transmitter receives the output $\tilde{Y}_{i-1}$ of the $(i-1)$th block, he computes $k_i^* = g_f(\tilde{y}_{i-1}) \in \mathcal{W}$. For a given w_i ($2 \leq i \leq n$), the transmitter chooses a sequence $x^N(w_i \oplus k_i^*)$ to transmit (note that here $\oplus$ is the modulo addition over $\mathcal{W}$).

Decoding: For block i ($2 \leq i \leq n$), given a vector $\tilde{y}_i \in \mathcal{Y}^{\mathcal{N}}$, try to find a sequence $x^N(\hat{w}_{i1} \oplus k_i^*, \hat{w}_{i2})$ (case 1) or $x^N(\hat{w}_i \oplus k_i^*)$ (case 2) such that x^N and $\tilde{y}_i$ are joint typical. If there exists such a sequence, put out the corresponding $(\hat{w}_{i1} \oplus k_i^*, \hat{w}_{i2})$ or $\hat{w}_i \oplus k_i^*$. Otherwise, declare a decoding error. Since the legitimate receiver knows k_i^*, put out the corresponding $\hat{w}_i$ from $(\hat{w}_{i1} \oplus k_i^*, \hat{w}_{i2})$ or $\hat{w}_i \oplus k_i^*$.

Proof of achievability: The rate of the message W^n is defined as R^*, and it satisfies

$$\begin{aligned} R^* &= \lim_{N\rightarrow\infty} \lim_{n\rightarrow\infty} \frac{H(W^n)}{nN} = \lim_{N\rightarrow\infty} \lim_{n\rightarrow\infty} \frac{\sum_{i=2}^n H(W_i)}{nN} \\ &= \lim_{N\rightarrow\infty} \lim_{n\rightarrow\infty} \frac{(n-1)NR}{nN} = R. \end{aligned} \tag{A4}$$

Since the legitimate receiver knows k_i^*, the decoding scheme for Theorem 1 is in fact the same as that in [1]. Hence, we omit the proof of $P_e \leq \epsilon$ here. It remains to show that $\lim_{N\rightarrow\infty} \Delta \geq R_e$, see the following.

- For the case 1, part of the message w_i is encrypted by k_i^*. In the analysis of the equivocation, we drop w_{i2} from w_i. Then, the equivocation about w_i is equivalent to the equivocation about k_i^*. Since $k_i^* = g_f(\tilde{y}_{i-1})$, the wiretapper tries to guess k_i^* from $\tilde{y}_{i-1}$. Note that for a given $\tilde{z}_{i-1}$ and sufficiently large N, $Pr\{\tilde{y}_{i-1} \in T^N_{Y|Z}(\tilde{z}_{i-1})\} \rightarrow 1$. Thus, the wiretapper can guess $\tilde{y}_{i-1}$ from the conditional typical set $T^N_{Y|Z}(\tilde{z}_{i-1})$. By using the above Lemma 1 and (A3), the set $T^N_{Y|Z}(\tilde{z}_{i-1})$ maps into at least $\frac{2^{NH(Y|Z)}}{1+\delta}$ (here $\gamma = 2^{NH(Y|Z)}$) k_i^* (colors). Thus, in the ith block, the uncertainty about K_i^* is bounded by

$$\frac{1}{N} H(K_i^*|\tilde{Z}_{i-1}) \geq H(Y|Z) - \frac{\log(1+\delta)}{N}, \tag{A5}$$

here note that K_i^* is uniformly distributed.
- For the case 2, the alphabet of the secret key k_i^* equals to the alphabet of w_i, and the encrypted message is denoted by $w_i \oplus k_i^*$. Then, by using the above Lemma 1 and (A3), the set $T^N_{Y|Z}(\tilde{z}_{i-1})$ maps into at least $\frac{2^{NR}}{1+\delta}$ (here $\gamma = 2^{NR}$) k_i^* (colors). Thus, in the ith block, the uncertainty about K_i^* is bounded by

$$\frac{1}{N} H(K_i^*|\tilde{Z}_{i-1}) \geq R - \frac{\log(1+\delta)}{N}. \tag{A6}$$

Proof of $\lim_{N\to\infty}\Delta \geq R_e$ for case 1: Here Δ is bounded by

$$\begin{aligned}\Delta &= \frac{H(W^n|Z^n)}{nN} \stackrel{(a)}{=} \frac{\sum_{i=2}^{n} H(W_i|\tilde{Z}_i, \tilde{Z}_{i-1})}{nN} \\ &\stackrel{(b)}{\geq} \frac{\sum_{i=2}^{n} H(W_{i1}|\tilde{Z}_{i-1}, W_{i1}\oplus K_i^*)}{nN} \\ &\stackrel{(c)}{=} \frac{\sum_{i=2}^{n} H(K_i^*|\tilde{Z}_{i-1})}{nN} \\ &\stackrel{(d)}{\geq} \frac{(n-1)(NH(Y|Z) - \log(1+\delta))}{nN} \end{aligned} \tag{A7}$$

where (a) is from $W_i \rightarrow (\tilde{Z}_i, \tilde{Z}_{i-1}) \rightarrow (W^{i-1}, \tilde{Z}^{i-2}, \tilde{Z}_{i+1}^n)$, (b) is from $W_{i1} \rightarrow (W_{i1}\oplus K_i^*, \tilde{Z}_{i-1}) \rightarrow \tilde{Z}_i$, (c) follows from the fact that $W_{i1}\oplus K_i^*$ is independent of K_i^*, W_{i1} and $\tilde{Z}_{i-1}$, and (d) is from (A5). Letting $N\rightarrow\infty$ and $n\rightarrow\infty$, we have $\lim_{N\to\infty}\Delta \geq H(Y|Z) = R_e$.

Proof of $\lim_{N\to\infty}\Delta \geq R_e$ for case 2: Analogously, we have

$$\begin{aligned}\Delta &\geq \frac{\sum_{i=2}^{n} H(K_i^*|\tilde{Z}_{i-1})}{nN} \stackrel{(1)}{\geq} \frac{\sum_{i=2}^{n}(NR - \log(1+\delta))}{nN} \\ &= \frac{(n-1)(NR - \log(1+\delta))}{nN}, \end{aligned} \tag{A8}$$

where (1) is from (A6). Letting $N\rightarrow\infty$ and $n\rightarrow\infty$, we have $\lim_{N\to\infty}\Delta \geq R = R_e$.

Thus, the achievability proof of $\mathcal{R}^{\mathcal{A}}$ is completed.

B. Achievability Proof of $\mathcal{R}^{\mathcal{B}}$ for the Case that the Wiretap Channel is More Capable than the Main Channel

Since the wiretap channel is more capable than the main channel, the wiretapper also can decode the codeword x^N. By using Lemma 1 and the definitions that $\gamma = 2^{NH(Y|X,Z)}$ for the case $I(X;Y) \geq H(Y|X,Z)$, $\gamma = 2^{NR}$ for the case $I(X;Y) \leq H(Y|X,Z)$, the achievability proof of $\mathcal{R}^{\mathcal{B}}$ is along the lines of that of $\mathcal{R}^{\mathcal{A}}$, and thus we omit it here.

Thus, the achievability proof of $\mathcal{R}^{\mathcal{A}}$ and $\mathcal{R}^{\mathcal{B}}$ is completed.

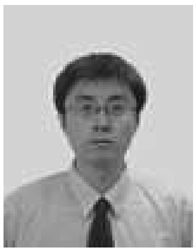
REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.
[2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
[3] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, July 1978.
[4] C. Mitrpant, A. J. Han Vinck, and Y. Luo, "An Achievable Region for the Gaussian Wiretap Channel with Side Information," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2181–2190, 2006.
[5] Y. Chen and A. J. Han Vinck, "Wiretap channel with side information," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 395–402, Jan. 2008.
[6] B. Dai and Y. Luo, "Some new results on wiretap channel with side information," *Entropy*, vol. 14, pp. 1671–1702, 2012.
[7] N. Merhav, "Shannon's secrecy system with informed receivers and its application to systematic coding for wiretapped channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2723–2734, June 2008.
[8] R. Ahlswede and N. Cai, "Transmission, Identification and Common Randomness Capacities for Wire-Tap Channels with Secure Feedback from the Decoder," book chapter in *General Theory of Information Transfer and Combinatorics*, LNCS 4123, pp. 258–275, Berlin: Springer-Verlag, 2006.
[9] E. Ardestanizadeh *et al.*,"Wiretap channel with secure rate-limited feedback," *IEEE Trans. Inf. Theory*, vol. 55, no. 12, pp. 5353–5361, Dec. 2009.

Bin Dai received the B.Sc. degree in communications and information systems from University of Electronic Science and Technology of China, Chengdu, China, in 2004. He received the M.Sc. and Ph.D. degrees in computer science and technology from Shanghai Jiaotong University, Shanghai, China in 2007 and 2012, respectively. In 2011 and 2012, he was a Visiting Scholar with the Institute for Experimental Mathematics, Duisburg-Essen University, Essen, Germany. He is currently a Lecturer with the Southwest Jiaotong University. His research interests include information-theoretic security, network information theory, and coding.

A. J. Han Vinck received the Ph.D. degree in electrical engineering from the University of Eindhoven, Eindhoven, The Netherlands, in 1980. He has been a Full Professor of Digital Communications at the University of Duisburg-Essen, Duisburg, Germany, since 1990. He studied electrical engineering at the University of Eindhoven, the Netherlands, where he obtained his Ph.D. in 1980. In 2003, he was an Adjunct Professor at the Sun Yat-Sen University, Kaohsiung, Taiwan. His interest is in information and communication theory, coding, and network aspects in digital communications. Dr. Vinck was elected a Fellow by the IEEE for his "Contributions to Coding Techniques." He has served on the Board of Governors of the IEEE Information Theory Society since 1997 (until 2006). In 2003, he was elected President of the IEEE Information Theory Society. In 1997, he was a Co-Chairman for the 1997 IEEE Information Theory Symposium, Ulm, Germany. He is the initiator of the Japan-Benelux Workshops on Information Theory (now Asia-Europe) and the International Winter Meeting on Coding, Cryptography, and Information Theory.

Yuan Luo received the B.S., M.S., and Ph.D. degrees in applied mathematics from Nankai University, Tianjin, China, in 1993, 1996, and 1999, respectively. From July 1999 to April 2001, he held a postdoctoral position at the Institute of Systems Science, Chinese Academy of Sciences, Beijing, China. From May 2001 to April 2003, he held a postdoctoral position at the Institute for Experimental Mathematics, University of Duisburg-Essen, Essen, Germany. Since June 2003, he has been with the Computer Science and Engineering Department, Shanghai Jiao Tong University, Shanghai, China. He held his present position as a Full Professor since 2006. His current research interests include coding theory and information theory.



Zheng Ma received the B.Sc. and Ph.D. degrees in communications and information systems from Southwest Jiaotong University, Chengdu, China, in 2000 and 2006, respectively. He was a Visiting Scholar with the University of Leeds, Leeds, U.K. in 2003. In 2003 and 2005, he was a Visiting Scholar with Hong Kong University of Science and Technology, Kowloon, Hong Kong. From 2008 to 2009, he was a Visiting Research Fellow with the Department of Communication Systems, Lancaster University, Lancaster, U.K. He is currently a Professor with the Southwest Jiaotong University. His research interests include information theory and coding, communication systems, signal design and processing, field-programmable gate array/digital signal processor implementation, and professional mobile radio. Dr. Ma has been the Vice-Chairman of the IT Chapter of the IEEE Chengdu Section since 2009.