Int. J. Electron. Commun. (AEÜ) xxx (2015) xxx–xxx

Contents lists available at ScienceDirect

International Journal of Electronics and Communications (AEÜ)

journal homepage: www.elsevier.com/locate/aeue

Feedback enhances the security of wiretap channel with states

B. Dai [a,b,*], A.J. Han Vinck [c], Y. Wang [d]

[a] School of Information Science and Technology, Southwest JiaoTong University, Chengdu, China
[b] The National Mobile Communications Research Laboratory, Southeast University, Nanjing, China
[c] Institute for Experimental Mathematics, Duisburg-Essen University, Ellernstr. 29, Essen, Germany
[d] China Information Technology Security Evaluation Center, Beijing, China

ARTICLE INFO

Article history:
Received 20 April 2013
Accepted 8 April 2015

Keywords:
Wiretap channel
Channel state information
Capacity-equivocation region
Noiseless feedback
Secrecy capacity

ABSTRACT

Wyner, in his well-known paper on the wiretap channel, studied the problem on 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. In this paper, the model of wiretap channel has been reconsidered for the case that the main channel is controlled by channel state information (CSI), and it is available at the transmitter in a noncausal manner (termed here noncausal channel state information) or causal manner (termed here causal channel state information). Moreover, there is a noiseless feedback from the legitimate receiver to the transmitter. Measuring the uncertainty of the wiretapper by equivocation, the capacity-equivocation regions for both manners (causal and noncausal) are determined. Furthermore, the secrecy capacities are formulated, which provide the best transmission rate with perfect secrecy. The results of this paper are further explained via binary and Gaussian examples, and we find that the noiseless feedback helps to enhance the security of wiretap channel with noncausal or causal CSI at the transmitter.

1. Introduction

The most important issues in communication are reliability and security. The reliability quantifies the maximum rate achievable with small probability of error. Security is an important issue when the transmitted information is confidential and needs to be kept as secret as possible from wiretapper. Communication of confidential messages has been studied in the literature for some classes of channel models, and the wiretap channel is the most important model of them.

The concept of the wiretap channel was first introduced by Wyner [1]. It is a kind of degraded broadcast channels. The wiretapper knows the encoding scheme used at the transmitter and the decoding scheme used at the legitimate receiver, see Fig. 1. 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. Furthermore, 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). In addition, Merhav [4] studied a variation of the 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.

In communication systems there is often a feedback link from the receiver to the transmitter. For example, the two-way channels for telephone connections. It is well known that feedback does not increase the capacity of discrete memoryless channel (DMC) [18, pp. 216–218]. However, does the feedback increase the capacity region of the wiretap channel? In order to solve this problem, Ahlswede and Cai studied the general wiretap channel (the wiretap channel does not need to be degraded) with noiseless feedback from the legitimate receiver to the transmitter [5] (see Fig. 2), and both the upper and lower bounds of the secrecy capacity were provided. Specifically, for the degraded case, they showed that the secrecy capacity is larger than that of Wyner's wiretap channel (without feedback). In the achievability proof, Ahlswede and Cai [5] used the noiseless feedback as a secret key shared by the

* Corresponding author at: School of Information Science and Technology, Southwest JiaoTong University, Chengdu, China.
E-mail address: daibin@home.swjtu.edu.cn (B. Dai).

http://dx.doi.org/10.1016/j.aeue.2015.04.005
1434-8411/

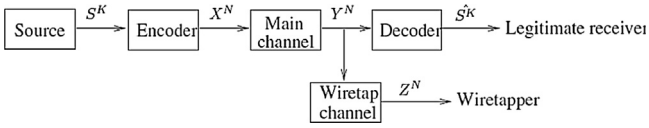

Fig. 1. Wiretap channel.

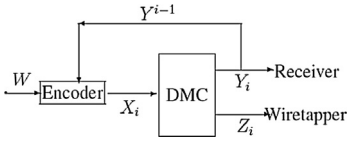

Fig. 2. The general wiretap channel with noiseless feedback.

transmitter and the legitimate receiver, while the wiretapper had no knowledge about the key except his own received symbols. Based on the work of [5], Dai et al. [6] studied a special case of the general wiretap channel with noiseless feedback, and found that the noiseless feedback enhances the secrecy capacity of the non-degraded wiretap channel. Besides Ahlswede and Cai's work, the wiretap channel with noisy feedback was studied in [7], and the wiretap channel with secure rate-limited feedback was studied in [8], and both of them focused on bounds of the secrecy capacity.

The coding for channels with causal (past and current) channel state information at the encoder was first investigated by Shannon [9] in 1958. After that, in order to solve the problem of coding for a computer memory with defective cells, Kuznetsov and Tsybakov [10] considered a channel in the presence of noncausal channel state information at the transmitter. They provided some coding techniques without determination of the capacity. The capacity was found in 1980 by Gel'fand and Pinsker [11]. Furthermore, Max H.M. Costa [12] 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. In order to introduce channel state information to the broadcast channels, Steinberg investigated the degraded broadcast channel with channel state information [13], where both causal and noncausal channel state information were considered in his paper. Specifically, inner and outer bounds on capacity region were provided for the degraded broadcast channel with noncausal channel state information [13], meanwhile, the capacity region of the degraded broadcast channel with causal channel state information was totally determined [13].

Inspired by the works of [12] and [1], Mitrpant et al. [14] studied transmission of confidential messages in the channels with channel state information (CSI). In [14], an inner bound on the capacity-equivocation region was provided for the Gaussian wiretap channel with CSI. Furthermore, Chen et al. [15] investigated the discrete memoryless wiretap channel with noncausal CSI (see Fig. 3), and also provided an inner bound on the capacity-equivocation region. Note that the coding scheme of [15] is a combination of those in [11,1]. Based on the work of [15], Dai [16] provided an outer bound on the wiretap channel with noncausal CSI, and determined the capacity-equivocation region for the model of wiretap channel with memoryless CSI, where the memoryless means that at the i-th time,

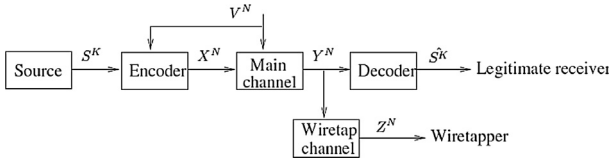

Fig. 3. Wiretap channel with noncausal channel state information.

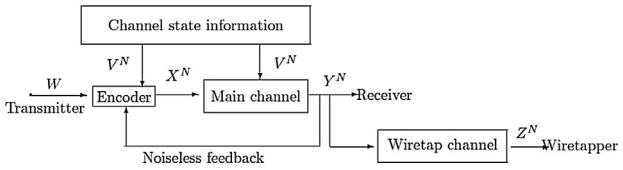

Fig. 4. Wiretap channel with channel state information and noiseless feedback.

the output of the channel encoder depends only on the i-th time CSI.

In this paper, we study the model of wiretap channel with channel state information and noiseless feedback, see Fig. 4. It is derived from the model of Fig. 2 and the model of Fig. 3. *The motivation of this work is to investigate how the feedback works in the mode of the wiretap channel with channel state information, and whether the achievable region of [15] can be enhanced by using the noiseless feedback.*

In the new model of Fig. 4, the conditional transition probability distribution of the main channel depends on a channel state information sequence V^N, which is available at the encoder in a noncausal or causal manner. In addition, there is a noiseless feedback from the output of the main channel to the transmitter. The wiretapper can get a degraded version of the symbols Y^N via a wiretap channel.

The capacity-equivocation region is determined for this new model in both causal and noncausal manners. Furthermore, the secrecy capacity is formulated, which provides the best transmission rate with perfect secrecy.

The organization of this paper is as follows. In Section 2, we present the basic definitions and the main results on the capacity-equivocation regions. Section 3 is for examples about the model of Fig. 4. Final conclusions are presented in Section 4.

2. Notations, definitions and the main results

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 product 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 $p_V(v)$ denote the probability mass function $Pr\{V = v\}$. Throughout the paper, the logarithmic function is to the base 2.

In this section, the model of Fig. 4 is considered into two parts. The model of Fig. 4 with noncausal CSI is described in Section 2.1, and the model of Fig. 4 with causal CSI is described in Section 2.2, see the followings.

2.1. The model of Fig. 4 with noncausal channel state information

In this subsection, a description of the model of Fig. 4 with noncausal CSI is given by Definition 1 to Definition 4. The capacity-equivocation region $\mathcal{R}^{(n)}$, which is composed of all achievable (R, R_e) pairs in the model of Fig. 4 with noncausal CSI, are characterized in Theorem 1. The achievable (R, R_e) pair is defined in Definition 5.

Definition 1. (**Channel encoder for the noncausal manner**) The message W is uniformly distributed over $\mathcal{W}$. The channel state information V^N is the output of a discrete memoryless source $P_V(\cdot)$, and it is available at the channel encoder in a noncausal manner. V^N is independent of W. The feedback Y^{i-1} (where $2 \le i \le N$ and Y^{i-1} takes values in $\mathcal{Y}^{i-1}$) is the previous $i-1$ time output of the main channel. At the i-th time, the inputs of the channel encoder

Please cite this article in press as: Dai B, et al. Feedback enhances the security of wiretap channel with states. Int J Electron Commun (AEÜ) (2015), http://dx.doi.org/10.1016/j.aeue.2015.04.005

are W, Y^{i-1} and V^N, while the output is X_i, i.e., the encoder is a (stochastic) mapping

$$f_i : \mathcal{W} \times \mathcal{Y}^{i-1} \times \mathcal{V}^N \to \mathcal{X}_i, \tag{2.1}$$

where $f_i(w, y^{i-1}, v^N) = x_i \in \mathcal{X}$, $w \in \mathcal{W}$, $y^{i-1} \in \mathcal{Y}^{i-1}$ and $v^N \in \mathcal{V}^N$.

The transmission rate of the message W is $\frac{\log \|\mathcal{W}\|}{N}$.

Definition 2. (**Main channel**) The main channel is a DMC with finite input alphabet $\mathcal{X} \times \mathcal{V}$, finite output alphabet $\mathcal{Y}$, and transition probability $Q_M(y|x, v)$, where $x \in \mathcal{X}$, $v \in \mathcal{V}$, $y \in \mathcal{Y}$. $Q_M(y^N|x^N, v^N) = \prod_{n=1}^{N} Q_M(y_n|x_n, v_n)$. The inputs of the main channel are X^N and V^N, while the output is Y^N.

Definition 3. (**Wiretap channel**) The wiretap channel is also a DMC with finite input alphabet $\mathcal{Y}$, finite output alphabet $\mathcal{Z}$, and transition probability $Q_W(z|y)$, where $y \in \mathcal{Y}$, $z \in \mathcal{Z}$. The input and output of the wiretap channel are Y^N and Z^N, respectively. The equivocation to the wiretapper is defined as

$$\Delta = \frac{1}{N} H(W|Z^N). \tag{2.2}$$

The cascade of the main channel and the wiretap channel is another DMC with transition probability

$$Q_{MW}(z|x, v) = \sum_{y \in \mathcal{Y}} Q_W(z|y) Q_M(y|x, v). \tag{2.3}$$

Definition 4. (**Decoder**)

The decoder is a mapping $f_D : \mathcal{Y}^N \to \mathcal{W}$, with input Y^N and output $\hat{W} = f_D(Y^N)$. Let P_e be the error probability, defined as $Pr\{W \neq \hat{W}\}$.

Definition 5. (**Achievable** (R, R_e) **pair in the model of Fig. 4 with noncausal channel state information**) A pair (R, R_e) (where R, $R_e > 0$) is called achievable if, for any $\epsilon > 0$, there exists an encoder–decoder (N, Δ, P_e) such that

$$\lim_{N\to\infty} \frac{\log \|\mathcal{W}\|}{N} = R, \ \lim_{N\to\infty} \Delta \geq R_e, P_e \leq \epsilon. \tag{2.4}$$

Theorem 1 gives a single-letter characterization of the capacity-equivocation region $\mathcal{R}^{(n)}$, which is composed of all achievable (R, R_e) pairs in the model of Fig. 4 with noncausal channel state information, and it is proved in Appendix A and B.

Theorem 1. *A single-letter characterization of the region* $\mathcal{R}^{(n)}$ *is as follows,*

$$\begin{aligned} \mathcal{R}^{(n)} = \{(R, R_e) : 0 \leq R_e \leq R, \\ 0 \leq R \leq I(K;Y) - I(K;V), \\ R_e \leq H(Y|Z)\}, \end{aligned}$$

for some distribution

$$\begin{aligned} & P_{KVXYZ}(k, v, x, y, z) \\ & = P_{Z|Y}(z|y) P_{Y|XV}(y|x, v) P_{X|KV}(x|k, v) P_{KV}(k, v), \end{aligned}$$

which implies the Markov chain $K \to (X, V) \to Y \to Z$. *Here note that the random variable* K *is an auxiliary random variable which is used to characterize the capacity-equivocation region of the wiretap channel with noncausal CSI and noiseless feedback.*

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

- The range of the random variable K satisfies

$$\|\mathcal{K}\| \leq \|\mathcal{X}\| \|\mathcal{V}\| + 1.$$

The proof is standard and easily obtained by using the support lemma (see [17, p. 310]), and thus, we omit the proof here.

- The capacity of the main channel $C_M^{(n)}$ is denoted byu

$$C_M^{(n)} = \max_{p_{KVXY}(k,v,x,y)} I(K;Y) - I(K;V), \tag{2.5}$$

which is coincident with the capacity of the channel with noncausal CSI at the transmitter [11].

- The points in $\mathcal{R}^{(n)}$ for which $R = R_e$ are of considerable interest.

Definition 6. (**The secrecy capacity** $C_s^{(nf)}$) The secrecy capacity $C_s^{(nf)}$ of the model of Fig. 4 with noncausal channel state information, is denoted by

$$C_s^{(nf)} = \max_{(R, R_e = R) \in \mathcal{R}^{(n)}} R. \tag{2.6}$$

Furthermore, the secrecy capacity $C_s^{(nf)}$ satisfies

$$\begin{aligned} C_s^{(nf)} = \max \min\{I(K;Y) - I(K;V), \\ H(Y|Z)\}. \end{aligned} \tag{2.7}$$

The formula in (2.7) is derived as follows. Substituting $R_e = R$ into the region $\mathcal{R}^{(n)}$ in Theorem 1, we have

$$R \leq I(K;Y) - I(K;V), \tag{2.8}$$

$$R \leq H(Y|Z), . \tag{2.9}$$

By using (2.6), (2.8) and (2.9), the formula (2.7) is achieved, thus the proof is completed.

- An achievable rate-equivocation region of the wiretap channel without feedback, but with noncausal CSI [15], is given by

$$\begin{aligned} \mathcal{R}_i^n = \{(R, R_e) : 0 \leq R_e \leq R, \\ 0 \leq R \leq I(K;Y) - I(K;V), \\ R_e \leq I(K;Y) - I(K;Z)\}, \end{aligned} \tag{2.10}$$

where $K \to (X, V) \to Y \to Z$.

Note that

$$\begin{aligned} & I(K;Y) - I(K;Z) \\ & = H(K) - H(K|Y) - H(K) + H(K|Z) \\ & \overset{(a)}{=} H(K|Z) - H(K|Y, Z) \\ & = I(K;Y|Z) \leq H(Y|Z), \end{aligned}$$

where (a) is from $K \to Y \to Z$. Therefore, the achievable rate-equivocation region in [15] is enhanced by using the noiseless feedback.

2.2. The model of Fig. 4 with causal channel state information

The model of Fig. 4 with causal CSI is similar to the model with noncausal CSI in Section 2.1, except that the V^N in Definition 1 is known to the encoder in a causal manner, i.e., at the i-th time $(1 \leq i \leq N)$, the output of the channel encoder is $x_i = f_i(w, y^{i-1}, v^i)$, where $v^i = (v_1, v_2, \ldots, v_i)$. Note that V_i is independent of W, Y^{i-1} and V_{i+1}^N, and V_{i+1}^N is independent of W, Y^i and Z^i.

Theorem 2 gives a single-letter characterization of the capacity-equivocation region $\mathcal{R}^{(c)}$, which is composed of all achievable (R, R_e) pairs in the model of Fig. 4 with causal channel state information, and it is proved in Appendix C and Appendix D.

Please cite this article in press as: Dai B, et al. Feedback enhances the security of wiretap channel with states. Int J Electron Commun (AEÜ) (2015), http://dx.doi.org/10.1016/j.aeue.2015.04.005

Theorem 2. *A single-letter characterization of the region $\mathcal{R}^{(c)}$ is as follows,*

$$\mathcal{R}^{(c)} = \{(R, R_e) : 0 \le R \le I(K;Y),$$
$$0 \le R_e \le R,$$
$$R_e \le H(Y|Z)\},$$

for some distribution

$$P_{KVXYZ}(k, v, x, y, z)$$
$$= P_{Z|Y}(z|y)P_{Y|XV}(y|x, v)P_{X|KV}(x|k, v)P_K(k)P_V(v),$$

which implies the Markov chain $K \to (X, V) \to Y \to Z$ and the fact that V is independent of K. Here note that the random variable K is an auxiliary random variable which is used to characterize the capacity-equivocation region of the wiretap channel with causal CSI and noiseless feedback.

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

- The range of the auxiliary random variable K satisfies

$$\|\mathcal{K}\| \le \|\mathcal{X}\|\|\mathcal{V}\|.$$

  The proof is standard and easily obtained by using the support lemma (see [17, p. 310]), and thus, we omit the proof here.
- The capacity of the main channel $C_M^{(c)}$ is defined as follows.

$$C_M^{(c)} = \max_{p_{KVXY}(k,v,x,y)} I(K;Y). \tag{2.11}$$

- The points in $\mathcal{R}^{(c)}$ for which $R = R_e$ are of considerable interest.

Definition 7. (**The secrecy capacity** $C_s^{(cf)}$) The secrecy capacity $C_s^{(cf)}$ of the model of Fig. 4, is denoted by

$$C_s^{(cf)} = \max_{(R,R_e=R)\in\mathcal{R}^{(c)}} R. \tag{2.12}$$

Furthermore, the secrecy capacity $C_s^{(cf)}$ satisfies

$$C_s^{(cf)} = \max_{p_{KVXYZ}(k,v,x,y,z)} \min\{I(K;Y), H(Y|Z)\}. \tag{2.13}$$

[Proof of (2.13)] Substituting $R = R_e$ into the region $\mathcal{R}^{(c)}$ in Theorem 2, we have

$$R \le I(K;Y), \tag{2.14}$$
$$R \le H(Y|Z). \tag{2.15}$$

By using (2.12), (2.14) and (2.15), the formula (2.13) is achieved, thus the proof is completed.

- An achievable rate-equivocation region of the wiretap channel without feedback, but with causal CSI [16], is given by

$$\mathcal{R}_i^c = \{(R, R_e) : 0 \le R_e \le R,$$
$$0 \le R \le I(K;Y), \tag{2.16}$$
$$R_e \le I(K;Y) - I(K;Z)\},$$

  where $K \to (X, V) \to Y \to Z$.
  Note that

$$I(K;Y) - I(K;Z)$$
$$= H(K) - H(K|Y) - H(K) + H(K|Z)$$
$$\overset{(a)}{=} H(K|Z) - H(K|Y, Z)$$
$$= I(K;Y|Z) \le H(Y|Z),$$

where (a) is from $K \to Y \to Z$. Therefore, the achievable rate-equivocation region in [16] is enhanced by using the noiseless feedback.

3. Examples

3.1. Gaussian case of Fig. 4 with noncausal CSI at the transmitter

For the Gaussian case of Fig. 4 with noncausal CSI at the transmitter, the i-th time ($1 \le i \le N$) channel inputs and outputs are given by

$$Y_i = X_i + V_i + Z_{1,i},$$
$$Z_i = X_i + V_i + Z_{1,i} + Z_{2,i}, \tag{3.1}$$

where $Z_{1,i} \sim \mathcal{N}(0, N_1)$, $Z_{2,i} \sim \mathcal{N}(0, N_2)$ and $V_i \sim \mathcal{N}(0, Q)$. Here note that $Z_{1,i}$ is independent of $Z_{2,i}$, and $\frac{1}{N}\sum_{i=1}^{N} E(X_i^2) \le P$. Similar to [12] and [15], substituting $U = X + \alpha V$ ($0 \le \alpha \le 1$), $X \sim \mathcal{N}(0, P)$ and $V \sim \mathcal{N}(0, Q)$ into Theorem 1, and using the fact that X is independent of V, we have the following Theorem 3 for the Gaussian case.

Theorem 3. *For the Gaussian case of Fig. 4 with noncausal CSI at the transmitter, the secrecy capacity C_s^{gf} is given by*

$$C_s^{gf} = \max_{0\le\alpha\le 1} \min\{\frac{1}{2}\log\frac{(P+N_1)(P+\alpha^2Q)}{\alpha^2Q(P+N_1)+N_1P}$$
$$-\frac{1}{2}\log\frac{P+\alpha^2Q}{P}, \frac{1}{2}\log\frac{2\pi e(P+N_1)N_2}{P+N_1+N_2}\}$$
$$\overset{(a)}{=} \min\{\frac{1}{2}\log(1+\frac{P}{N_1}), \frac{1}{2}\log\frac{2\pi e(P+N_1)N_2}{P+N_1+N_2}\},$$

where (a) is from the fact that the maximum of C_s^{gf} is achieved when $\alpha = 0$.

Recall that the maximum achievable secrecy rate of the Gaussian wiretap channel with noncausal CSI at the transmitter [15] is characterized by the following Theorem 4.

Theorem 4. *For the Gaussian non-feedback model of Fig. 4, an achievable secrecy rate C_s^{gi} is denoted by*

$$C_s^{gi} = \max_{0\le\alpha\le 1} \min\{\frac{1}{2}\log\frac{(P+N_1)(P+\alpha^2Q)}{\alpha^2Q(P+N_1)+N_1P}$$
$$-\frac{1}{2}\log\frac{P+\alpha^2Q}{P}, \frac{1}{2}\log\frac{(P+N_1)(P+\alpha^2Q)}{\alpha^2Q(P+N_1)+N_1P}$$
$$-\frac{1}{2}\log\frac{(P+N_1+N_2)(P+\alpha^2Q)}{\alpha^2QP+(N_1+N_2)(P+\alpha^2Q)}\}$$
$$\overset{(b)}{=} \min\{\frac{1}{2}\log\frac{(P+N_1)}{N_1},$$
$$\frac{1}{2}\log\frac{(P+N_1)}{N_1} - \frac{1}{2}\log\frac{(P+N_1+N_2)}{(N_1+N_2)}\},$$

where (b) is from the fact that both $\frac{1}{2}\log\frac{(P+N_1)(P+\alpha^2Q)}{\alpha^2Q(P+N_1)+N_1P} - \frac{1}{2}\log\frac{P+\alpha^2Q}{P}$ and $\frac{1}{2}\log\frac{(P+N_1)(P+\alpha^2Q)}{\alpha^2Q(P+N_1)+N_1P} - \frac{1}{2}\log\frac{(P+N_1+N_2)(P+\alpha^2Q)}{\alpha^2QP+(N_1+N_2)(P+\alpha^2Q)}$ are increasing while α is decreasing, and thus the maximum of C_s^{gi} is achieved when $\alpha = 0$. Here note that Theorem 4 is directly obtained from [15], and therefore, the proof is omitted here.

Fig. 5 plots $C_s^{gf}(\alpha)$ and $C_s^{gi}(\alpha)$ for $N_1 = 3$, $N_2 = 1$ and several values of P and Q. It is easy to see that $C_s^{gi}(\alpha)$ is enhanced by using the noiseless feedback. Moreover, we can see that both C_s^{gi} and C_s^{gf} are increasing while α is decreasing.

Please cite this article in press as: Dai B, et al. Feedback enhances the security of wiretap channel with states. Int J Electron Commun (AEÜ) (2015), http://dx.doi.org/10.1016/j.aeue.2015.04.005

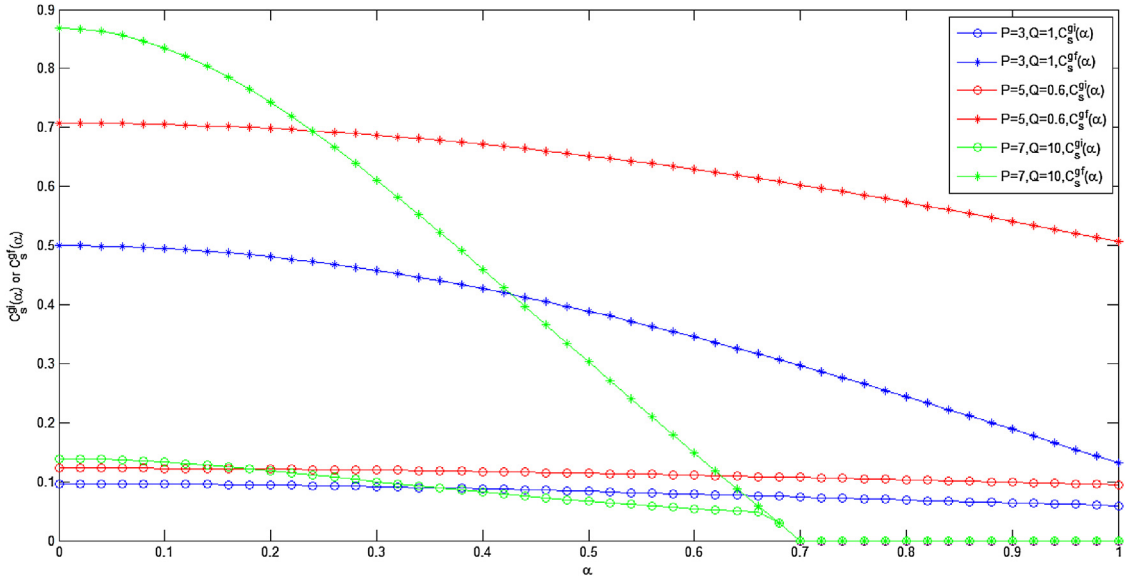

Fig. 5. The relations α-C_s^{gf} and α-C_s^{gi} for $N_1 = 3$, $N_2 = 1$, and several values of P and Q.

Fig. 6 plots the relationships $P - C_s^{gf}$ and $P - C_s^{gi}$ for several values of N_1, N_2 and Q. It is easy to see that C_s^{gi} is enhanced by using the noiseless feedback. Moreover, as we can see, when the power P tends to infinity, the secrecy rates C_s^{gi} and C_s^{gf} tend to be the constants. Here note that from Theorem 3 and Theorem 4, we can see that $C_s^{gi} = \frac{1}{2}\log\frac{N_1+N_2}{N_1}$ and $C_s^{gf} = \frac{1}{2}\log(2\pi e N_2)$ while P tends to infinity.

3.2. Binary case of Fig. 4 with noncausal or causal CSI at the transmitter

In this subsection, we calculate the secrecy capacity of a binary case of Fig. 4 with noncausal or causal CSI at the transmitter. Suppose that the random variable V is uniformly distributed over $\{0, 1\}$, i.e., $p_V(0) = p_V(1) = \frac{1}{2}$. Meanwhile, the random variables X, Y and Z take values in $\{0, 1\}$, and the wiretap channel is a BSC (binary symmetric channel) with crossover probability q. The transition probability of the main channel is defined as follows:

When $v = 0$,

$$p_{Y|X,V}(y|x, v=0) = \begin{cases} 1-p, & \text{if } y = x, \\ p, & \text{otherwise.} \end{cases} \tag{3.2}$$

When $v = 1$,

$$p_{Y|X,V}(y|x, v=1) = \begin{cases} p, & \text{if } y = x, \\ 1-p, & \text{otherwise.} \end{cases} \tag{3.3}$$

From Remark 1, we see that the secrecy capacity for the model of Fig. 4 with noncausal CSI at the transmitter is given by

$$C_s^{(nf)} = \max \min\{I(K;Y) - I(K;V), H(Y|Z)\}, \tag{3.4}$$

and the maximum achievable secrecy rate $C_s^{(ni)}$ of the wiretap channel with noncausal CSI [15] is given by

$$\begin{aligned} C_s^{(ni)} \quad = \quad & \max \min\{I(K;Y) - I(K;V), \\ & I(K;Y) - I(K;Z)\}, \end{aligned} \tag{3.5}$$

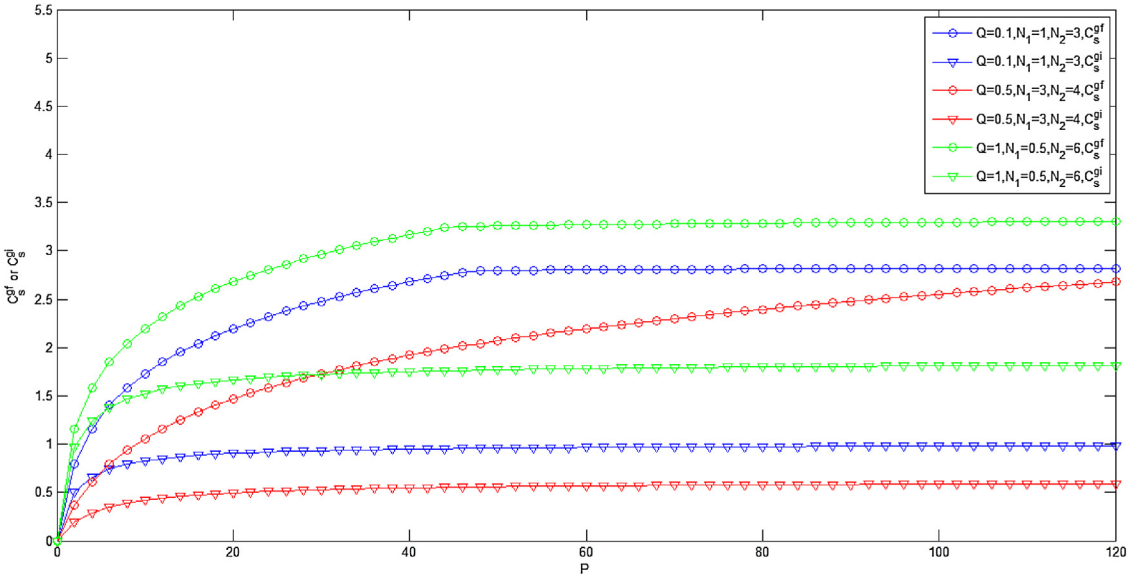

Fig. 6. The relationships $P - C_s^{gf}$ and $P - C_s^{gi}$ for several values of N_1, N_2 and Q.

Please cite this article in press as: Dai B, et al. Feedback enhances the security of wiretap channel with states. Int J Electron Commun (AEÜ) (2015), http://dx.doi.org/10.1016/j.aeue.2015.04.005

where (3.5) is from (2.10).

From Remark 2, we know that the secrecy capacity for the model of Fig. 4 with causal CSI at the transmitter is given by

$$C_s^{(cf)} = \max \min\{I(K;Y), H(Y|Z)\}, \tag{3.6}$$

and the maximum achievable secrecy rate $C_s^{(ci)}$ of the wiretap channel with causal CSI [16] is given by

$$C_s^{(ci)} = \max(I(K;Y) - I(K;Z)), \tag{3.7}$$

where (3.7) is from (2.16).

The remainder of this subsection is to calculate $C_s^{(nf)}$, $C_s^{(ni)}$, $C_s^{(cf)}$ and $C_s^{(ci)}$, see the followings.

The calculation of $C_s^{(cf)}$ and $C_s^{(ci)}$: For the causal case, the auxiliary random K is independent of V. Since $P_{Z|Y}(z|y)$, $P_{Y|X,V}(y|x,v)$ and $P_V(v)$ are fixed, from Theorem 2, we see that the joint probability $P_{KVXYZ}(k,v,x,y,z)$ depends only on the conditional probability $P_{X|K,V}$ and the probability $P_K(k)$, which implies that the characters $I(K;Y)$, $H(Y|Z)$ and $I(K;Y)-I(K;Z)$ are functions of $P_{X|K,V}$ and $P_K(k)$. Let K take values in $\{0,1\}$. The probability of K is defined as $p_K(0)=\alpha$ and $p_K(1)=1-\alpha$, where $0\le\alpha\le 1$. Define the conditional probability mass function $p_{X|K,V}(x|k,v)$ as follows.

$$\begin{aligned}
&p_{X|K,V}(0|0,0)=\beta_1, p_{X|K,V}(1|0,0)=1-\beta_1,\\
&p_{X|K,V}(0|0,1)=\beta_2, p_{X|K,V}(1|0,1)=1-\beta_2,\\
&p_{X|K,V}(0|1,0)=\beta_3, p_{X|K,V}(1|1,0)=1-\beta_3,\\
&p_{X|K,V}(0|1,1)=\beta_4, p_{X|K,V}(1|1,1)=1-\beta_4,
\end{aligned} \tag{3.8}$$

where $0\le\beta_1,\beta_2,\beta_3,\beta_4\le 1$.

The joint probability mass functions p_{KY} is calculated by

$$\begin{aligned}
p_{KY}(k,y) &= \sum_{x,v} p_{KYXV}(k,y,x,v)\\
&= \sum_{x,v} p_{Y|XV}(y|x,v)p_{X|K,V}(x|k,v)\\
&\quad p_K(k)p_V(v).
\end{aligned} \tag{3.9}$$

Then, we have

$$p_{KY}(0,0) = \frac{\alpha}{2}[1-(\beta_1-\beta_2)(1-2p)], \tag{3.10}$$

$$p_{KY}(0,1) = \frac{\alpha}{2}[1+(\beta_1-\beta_2)(1-2p)], \tag{3.11}$$

$$p_{KY}(1,0) = \frac{\alpha}{2}[1-(\beta_3-\beta_4)(1-2p)], \tag{3.12}$$

$$p_{KY}(1,1) = \frac{\alpha}{2}[1+(\beta_3-\beta_4)(1-2p)]. \tag{3.13}$$

By calculating, we have

$$C_s^{(cf)} = \min\{1-h(p), h(q)\}, \tag{3.14}$$

and

$$C_s^{(ci)} = h(p+q-2pq)-h(p), \tag{3.15}$$

where $h(x)=-x\log x-(1-x)\log(1-x)$ and $0\le x\le 1$.

The calculation of $C_s^{(nf)}$ and $C_s^{(ni)}$: For the noncausal case, the auxiliary random K is not independent of V in general. Since $P_{Z|Y}(z|y)$, $P_{Y|X,V}(y|x,v)$ and $P_V(v)$ are fixed, from Theorem 1, we see that the joint probability $P_{KVXYZ}(k,v,x,y,z)$ depends only on the conditional probabilities $P_{X|K,V}$ and $P_{K|V}(k|v)$, which implies that the characters $I(K;Y)-I(K;V)$, $H(Y|Z)$ and $I(K;Y)-I(K;Z)$ are functions of $P_{X|K,V}$ and $P_{K|V}(k|v)$. The conditional probability $P_{K|V}(k|v)$ is defined as $p_{K|V}(0|0)=\alpha_1$, $p_{K|V}(1|0)=1-\alpha_1$, $p_{K|V}(0|1)=\alpha_2$ and $p_{K|V}(1|1)=1-\alpha_2$, where $0\le\alpha_1,\alpha_2\le 1$. Define the conditional probability mass function $p_{X|K,V}(x|k,v)$ as (3.8).

Observing that

$$\begin{aligned}
C_s^{(nf)} &= \max \min\{I(K;Y)-I(K;V), H(Y|Z)\},\\
&\le \max \min\{I(K;Y), H(Y|Z)\},
\end{aligned} \tag{3.16}$$

and

$$\begin{aligned}
C_s^{(ni)} &= \max \min\{I(K;Y)-I(K;V),\\
&\quad I(K;Y)-I(K;Z)\},\\
&\le \max \min\{I(K;Y), I(K;Y)-I(K;Z)\},\\
&= \max I(K;Y)-I(K;Z),
\end{aligned} \tag{3.17}$$

it is easy to see that $C_s^{(nf)}\le C_s^{(cf)}$ and $C_s^{(ni)}\le C_s^{(ci)}$. Here note that the equalities of (3.16) and (3.17) hold if $I(K;V)=0$, which implies that K is independent of V. Hence, for the noncausal case, we can see that $C_s^{(nf)}$ and $C_s^{(ni)}$ are maximized if K is independent of V. From the definition of the probability $P_{K|V}(k|v)$, it is easy to see that K is independent of V if $\alpha_1=\alpha_2$. Hence, we can say that $C_s^{(nf)}$ and $C_s^{(ni)}$ are maximized if $\alpha_1=\alpha_2$. Furthermore, letting $\alpha_1=\alpha_2=\alpha$, the characters $I(K;Y)-I(K;V)$ (here $\alpha_1=\alpha_2=\alpha$ implies that $I(K;V)=0$), $H(Y|Z)$ and $I(K;Y)-I(K;Z)$ of $C_s^{(nf)}$ and $C_s^{(ni)}$ depend only on $P_{X|K,V}$ and $P_K(k)$, and the probabilities $P_{X|K,V}$ and $P_K(k)$ for the noncausal case are defined the same as those for the causal case. Thus, along the lines of the calculation of the characters $I(K;Y)$, $H(Y|Z)$ and $I(K;Y)-I(K;Z)$ in $C_s^{(cf)}$ and $C_s^{(ci)}$, we can conclude that

$$C_s^{(nf)} = C_s^{(cf)} = \min\{1-h(p), h(q)\}, \tag{3.18}$$

and

$$C_s^{(ni)} = C_s^{(ci)} = h(p+q-2pq)-h(p). \tag{3.19}$$

The following Figs. 7–9 show $C_s^{(nf)}$, $C_s^{(ni)}$, $C_s^{(cf)}$ and $C_s^{(ci)}$ for several values of q. Here note that the noise of the wiretap channel is increasing while q is increasing. It is easy to see that when $q<0.5$, $C_s^{(nf)}$ and $C_s^{(cf)}$ are always greater than $C_s^{(ni)}$ and $C_s^{(ci)}$, respectively. When $q=0.5$ (which implies that the wiretap channel is completely noisy), $C_s^{(nf)}=C_s^{(ni)}=C_s^{(cf)}=C_s^{(ci)}=1-h(p)$, i.e., the security of the wiretap channel with noncausal or causal CSI at the transmitter cannot be enhanced by using the noiseless feedback. This is due to the fact that when $q=0.5$, the wiretapper has no knowledge about the messages, and thus there is no need to do anything else to enhance the security. Moreover, we can see that the gap between $C_s^{(nf)}$ (or $C_s^{(cf)}$) and $C_s^{(ni)}$ (or $C_s^{(ci)}$) is decreasing while q is increasing.

4. Conclusion

In this paper, we study the wiretap channel with CSI and noiseless feedback. The capacity-equivocation regions for both manners (causal and noncausal) are determined. Furthermore, the secrecy capacities are formulated, which provide the best transmission rate with perfect secrecy. The results are further explained via binary and Gaussian examples, and we find that the noiseless feedback helps to enhance the security of the wiretap channel with noncausal or causal CSI at the transmitter.

Acknowledgements

The authors would like to thank Professor Ning Cai for his valuable suggestions to improve this paper. 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

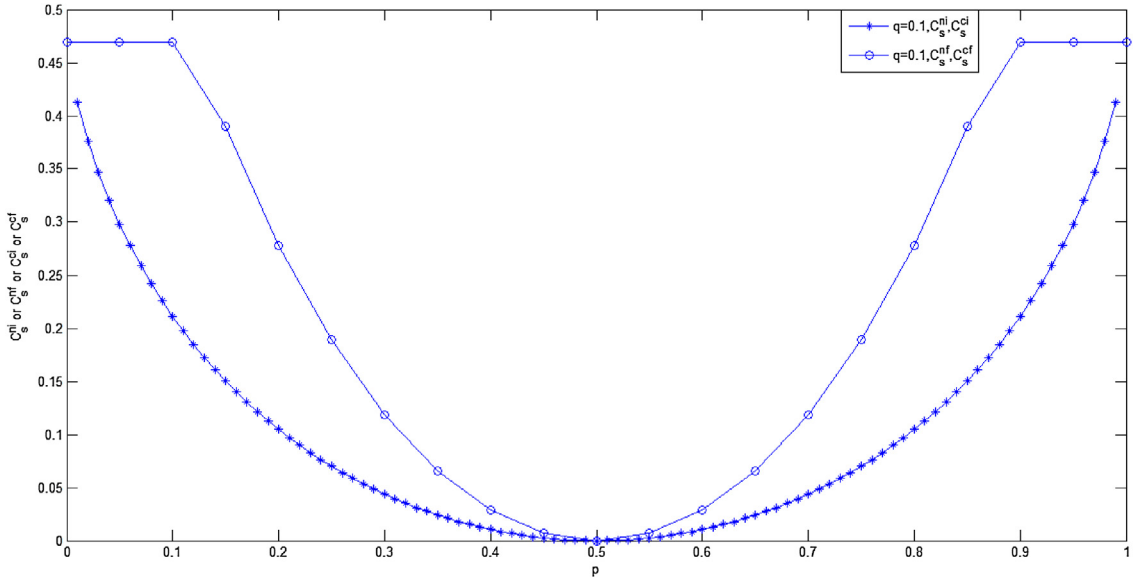

Fig. 7. The $C_s^{(nf)}$, $C_s^{(ni)}$, $C_s^{(cf)}$ and $C_s^{(ci)}$ for $q = 0.1$.

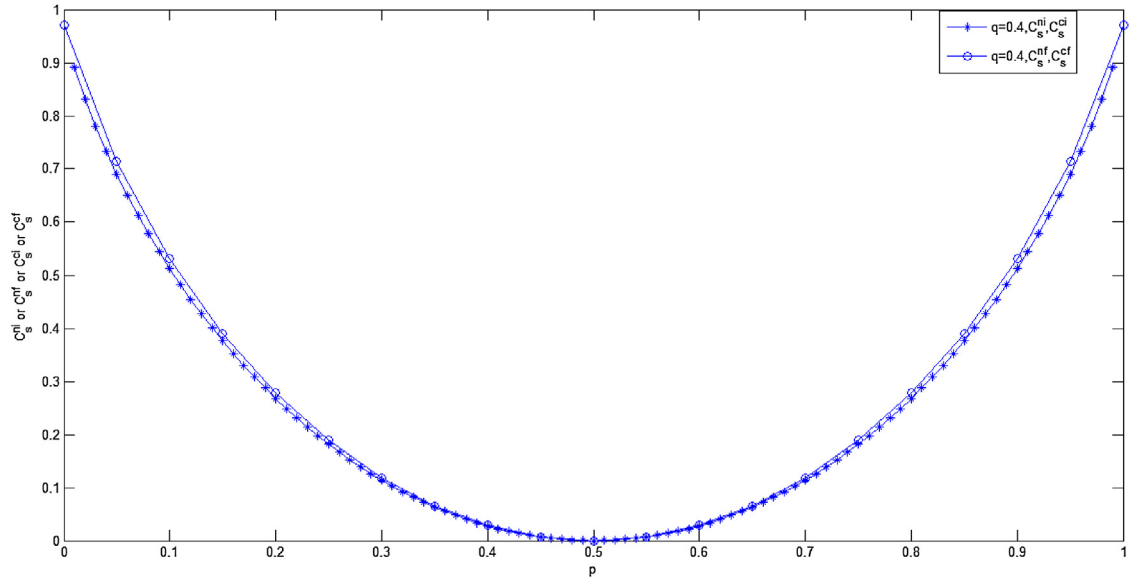

Fig. 8. The $C_s^{(nf)}$, $C_s^{(ni)}$, $C_s^{(cf)}$ and $C_s^{(ci)}$ for $q = 0.4$.

Research Fund of National Mobile Communications Research Laboratory, Southeast University (No. 2014D01).

Appendix A. Direct part of Theorem 1

In this section, we will show that any pair $(R, R_e) \in \mathcal{R}^n$ is achievable. Gel'fand-Pinsker's binning, block Markov coding and Ahlswede-Cai's secret key on feedback [5] are used in the construction of the code-book.

Now the remainder of this section is organized as follows. The code construction is in Section A.1. The proof of achievability is given in Section A.2.

A.1. Code construction

Given a pair (R, R_e), choose a joint probability mass function $p_{K,V,X,Y,Z}(k, v, x, y, z)$ such that $0 \le R_e \le R$, $R \le I(K;Y) - I(K;V)$ and $R_e \le H(Y|Z)$.

The message set $\mathcal{W}$ satisfies:

$$\lim_{N\to\infty} \frac{1}{N} \log \|\mathcal{W}\| = R = I(K;Y) - I(K;V) - \gamma_1, \tag{A.1}$$

where γ_1 is fixed positive real numbers. Let $\mathcal{W} = \{1, 2, \ldots, 2^{NR}\}$.

We use the block Markov coding method. The random vectors K^n, V^n, X^n, Y^n and Z^n consist of n blocks of length N. For example, $K^n = (k_1^{(1)}, k_2^{(1)}, \ldots, k_N^{(1)}, k_1^{(2)}, k_2^{(2)}, \ldots, k_N^{(2)}, \ldots, k_1^{(n)}, k_2^{(n)}, \ldots, k_N^{(n)})$. For simplicity, denote $(k_1^{(i)}, k_2^{(i)}, \ldots, k_N^{(i)})$ $(1 \le i \le n)$ by $\widetilde{K}_i$, and thus $K^n = (\widetilde{K}_1, \ldots, \widetilde{K}_n)$. Let K^j be $(\widetilde{K}_1, \ldots, \widetilde{K}_{j-1}, \widetilde{K}_{j+1}, \ldots, \widetilde{K}_n)$. Similar convention is applied to V^n, X^n, Y^n and Z^n. The specific values of the above random vectors are denoted by lower case letters.

The message for n blocks is $W^n = (W_2, W_3, \ldots, W_n)$, where W_i $(2 \le i \le n)$ are i.i.d. random variables uniformly distributed over $\mathcal{W}$. Note that in the first block, there is no W_1.

Code-book generation:

Please cite this article in press as: Dai B, et al. Feedback enhances the security of wiretap channel with states. Int J Electron Commun (AEÜ) (2015), http://dx.doi.org/10.1016/j.aeue.2015.04.005

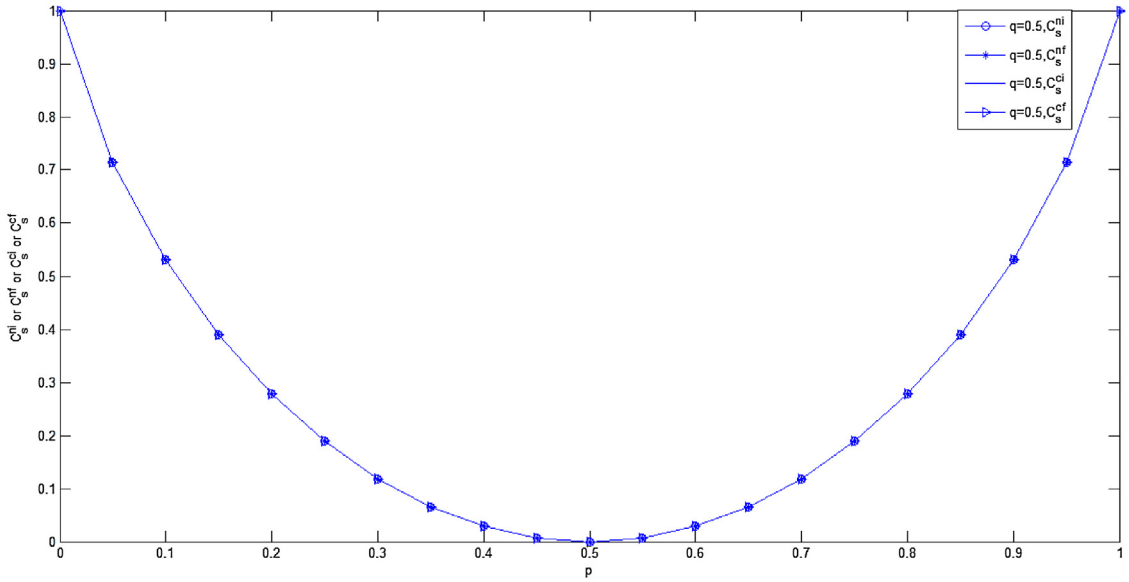

Fig. 9. The $C_s^{(nf)}$, $C_s^{(ni)}$, $C_s^{(cf)}$ and $C_s^{(ci)}$ for $q = 0.5$.

- **(Construction of K^N)**

  Gel'fand-Pinsker's binning, block Markov coding and Ahlswede-Cai's secret key on feedback [5] are used in the construction of K^N, see Fig. A.10.

  Generate $2^{N(I(K;Y)-\epsilon_{2,N})}$ ($\epsilon_{2,N} \to 0$ as $N \to \infty$) i.i.d. sequences k^N, according to the probability mass function $p_K(k)$. Distribute these sequences at random into $2^{NR} = 2^{N(I(K;Y)-I(K;V)-\gamma_1)}$ bins such that each bin contains $2^{N(I(K;V)+\gamma_1-\epsilon_{2,N})}$ sequences. Index each bin by $l \in \{1, 2, \ldots, 2^{NR}\}$.

  In the first block, for a given side information v^N, try to find a k^N such that $(k^N, v^N) \in T_{KV}^N(\epsilon)$. If multiple such sequences exist, randomly choose one for transmission. If no such sequence exists, declare an encoding error.

  For the i-th block ($2 \le i \le n$), firstly we generate a mapping $g_f : \mathcal{Y}^N \to \mathcal{W}$ (note that $\|\mathcal{Y}\|^N \ge \|\mathcal{W}\|$). Define a random variable $K_i^* = g_f(\widetilde{Y}_{i-1})$ ($2 \le i \le n$), which is uniformly distributed over $\mathcal{W}$, and K_i^* is independent of W_i. Reveal the mapping g_f to both receivers and the transmitter.

  Then, when the transmitter receives the output $\widetilde{y}_{i-1}$ of the i-1-th block, he computes $k_i^* = g_f(\widetilde{y}_{i-1}) \in \mathcal{W}$. For a given w_i, the transmitter chooses a sequence $k^N(w_i \oplus k_i^*, j^*)$ from the bin $w_i \oplus k_i^*$ (where $\oplus$ is the modulo addition over $\mathcal{W}$) such that $(k^N(w_i \oplus k_i^*, j^*), v^N) \in T_{KV}^N(\epsilon)$. If multiple such sequences in bin $w_i \oplus k_i^*$ exist, choose the one with the smallest index in the bin. If no such sequence exists, declare an encoding error.
- **(Construction of X^N)**

  For each block, the x^N is generated according to a new discrete memoryless channel (DMC) with inputs k^N, v^N, and output x^N.

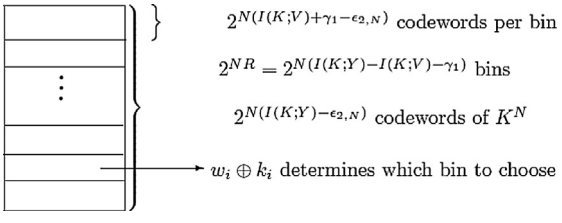

Fig. 10. Code-book construction for K^N in Theorem 1, where w_i and k_i^* are the message and the secret key for block i, respectively.

The transition probability of this new DMC is $p_{X|K,V}(x|k, v)$. The probability $p_{X^N|K^N,V^N}(x^N|k^N, v^N)$ is calculated as follows.

$$p_{X^N|K^N,V^N}(x^N|k^N, v^N) \tag{A.2}$$

$$= \prod_{i=1}^{N} p_{X|K,V}(x_i|k_i, v_i). \tag{A.3}$$

Decoding:

For block i ($2 \le i \le n$), given a vector $\widetilde{y}_i \in \mathcal{Y}^N$, try to find a sequence $k^N(\hat{w}_i, \hat{j})$ such that $(k^N(\hat{w}_i, \hat{j}), \widetilde{y}_i) \in T_{KY}^N(\epsilon_5)$. If there exist sequences with the same index of the bin $\hat{w}_i \oplus k_i^*$, put out the corresponding $\hat{w}_i \oplus k_i^*$. Otherwise, declare a decoding error. Finally, since the legitimate receiver knows k_i^* ($k_i^* = g_f(\widetilde{y}_{i-1})$), put out the corresponding $\hat{w}_i$ from $\hat{w}_i \oplus k_i^*$.

A.2. Proof of achievability

The rate of the message W^n is defined as

$$R^* = \lim_{N\to\infty} \lim_{n\to\infty} \frac{H(W^n)}{nN}, \tag{A.4}$$

and it satisfies

$$\begin{aligned} R^* &= \lim_{N\to\infty} \lim_{n\to\infty} \frac{H(W^n)}{nN} \\ &= \lim_{N\to\infty} \lim_{n\to\infty} \frac{\sum_{i=2}^{n} H(W_i)}{nN} \\ &= \lim_{N\to\infty} \lim_{n\to\infty} \frac{(n-1)H(W)}{nN} \\ &= R. \end{aligned} \tag{A.5}$$

In addition, note that the encoding and decoding scheme for Theorem 1 is similar to that in [11], except that the transmitted message for legitimate receiver is $w \oplus k^*$. Since legitimate receiver knows k^*, the decoding scheme for Theorem 1 is in fact the same as that in [11]. Hence, we omit the proof of $P_e \le \epsilon$ here.

It remains to show that $\lim_{N\to\infty} \Delta \ge R_e$, see the following. Since the confidential message W is encrypted by $W \oplus K^*$, the equivocation about W is equivalent to the equivocation about K^*. There are two ways for the wiretapper to obtain the secret key k^*. One way is that

Please cite this article in press as: Dai B, et al. Feedback enhances the security of wiretap channel with states. Int J Electron Commun (AEÜ) (2015), http://dx.doi.org/10.1016/j.aeue.2015.04.005

he tries to guess the k^* from its alphabet $\mathcal{W}$. The other way is that he tries to guess the feedback y^N (y^N is the output of the main channel for the previous block, and $k^* = g_f(y^N)$) from the conditional typical set $T^N_{[Y|Z]}(\delta)$, and this is because for a given z^N and sufficiently large N, $Pr\{(y^N \notin T^N_{[Y|Z]}(\delta)\} \to 0$. Note that there are $2^{NH(Y|Z)}$ sequences $y^N \in T^N_{[Y|Z]}(\delta)$ when $N \to \infty$ and $\delta \to 0$. Therefore, the equivocation about W is $\min\left\{\frac{\log\|\mathcal{W}\|}{N} = R, H(Y|Z)\right\}$, and note that $R \geq R_e$ and $H(Y|Z) \geq R_e$, then $\lim_{N\to\infty} \Delta \geq R_e$ is obtained.

The details about the proof are as follows.

First, we will show that $K_i^* \oplus W_i$ is independent of K_i^* and W_i, and this is used in the proof of $\lim_{N\to\infty} \Delta \geq R_e$.

Since K_i^* is independent of W_i ($2 \leq i \leq n$), and all of them are uniformly distributed over $\mathcal{W}$, the fact that $K^* \oplus W_i$ is independent of K^* and W_i is proved by the following (A.6) and (A.7).

$$\begin{aligned} &Pr\{K_i^* \oplus W_i = a\} \\ &= \sum_{k_i^* \in \mathcal{W}} Pr\{K_i^* \oplus W_i = a, K_i^* = k_i^*\} \\ &= \sum_{k_i^* \in \mathcal{W}} Pr\{W_i = a \ominus k_i^*, K_i^* = k_i^*\} \\ &= \sum_{k_i^* \in \mathcal{W}} Pr\{W_i = a \ominus k_i^*\} Pr\{K_i^* = k_i^*\} \\ &= \frac{1}{\|\mathcal{W}\|}. \end{aligned} \tag{A.6}$$

$$\begin{aligned} &Pr\{K_i^* \oplus W_i = a, K_i^* = k_i^*\} \\ &= Pr\{W_i = a \ominus k_i^*, K_i^* = k_i^*\} \\ &= Pr\{W_i = a \ominus k_i^*\} Pr\{K_i^* = k_i^*\} \\ &= \frac{1}{\|\mathcal{W}\|^2}. \end{aligned} \tag{A.7}$$

Then, $\lim_{N\to\infty} \Delta \geq R_e$ is proved by the following (A.8).

$$\begin{aligned} \lim_{N\to\infty} \Delta &= \lim_{N\to\infty} \lim_{n\to\infty} \frac{H(W^n|Z^n)}{nN} \\ &= \lim_{N\to\infty} \lim_{n\to\infty} \frac{\sum_{i=2}^n H(W_i|W^{i-1}, Z^n)}{nN} \\ &\overset{(a)}{=} \lim_{N\to\infty} \lim_{n\to\infty} \frac{\sum_{i=2}^n H(W_i|\widetilde{Z}_i, \widetilde{Z}_{i-1})}{nN} \\ &\geq \lim_{N\to\infty} \lim_{n\to\infty} \frac{\sum_{i=2}^n H(W_i|\widetilde{Z}_i, \widetilde{Z}_{i-1}, W_i \oplus K_i^*)}{nN} \\ &\overset{(b)}{=} \lim_{N\to\infty} \lim_{n\to\infty} \frac{\sum_{i=2}^n H(W_i|\widetilde{Z}_{i-1}, W_i \oplus K_i^*)}{nN} \\ &= \lim_{N\to\infty} \lim_{n\to\infty} \frac{\sum_{i=2}^n H(K_i^*|\widetilde{Z}_{i-1}, W_i \oplus K_i^*)}{nN} \\ &\overset{(c)}{=} \lim_{N\to\infty} \lim_{n\to\infty} \frac{\sum_{i=2}^n H(K_i^*|\widetilde{Z}_{i-1})}{nN} \\ &\overset{(d)}{=} \lim_{N\to\infty} \lim_{n\to\infty} \frac{\sum_{i=2}^n \min\{NH(Y|Z), NR\}}{nN} \\ &= \lim_{N\to\infty} \lim_{n\to\infty} \frac{(n-1)\min\{NR, NH(Y|Z)\}}{nN} \\ &= \min\{R, H(Y|Z)\} \\ &\geq R_e, \end{aligned} \tag{A.8}$$

where (a) is from $W_i \to (\widetilde{Z}_i, \widetilde{Z}_{i-1}) \to (W^{i-1}, \widetilde{Z}^{i-2}, \widetilde{Z}_{i+1}^n)$ is a Markov chain, (b) is from $W_i \to (W_i \oplus K_i^*, \widetilde{Z}_{i-1}) \to \widetilde{Z}_i$ is a Markov chain, (c) follows from the fact that $K_i^* \oplus W_i$ is independent of K_i^* and $\widetilde{Z}_{i-1}$, and (d) is from the fact that the wiretapper can guess the specific vector $\widetilde{Y}_{i-1}$ (corresponding to the key K_i^*) from the conditional typical set $T^N_{[Y|Z]}(\delta)$, and K_i^* is uniformly distributed over $\mathcal{W}$ (K_i^* is the key used in block i).

Thus, $\lim_{N\to\infty} \Delta \geq R_e$ is proved, and the direct part of Theorem 1 is completed.

Appendix B. Converse part of Theorem 1

In this section, we establish the converse part of Theorem 1: all the achievable (R, R_e) pairs are contained in the set $\mathcal{R}^{(n)}$. Suppose (R, R_e) is achievable, i.e., for any given $\epsilon > 0$, there exists a channel encoder-decoder (N, Δ, P_e) such that

$$\lim_{N\to\infty} \frac{\log\|\mathcal{W}\|}{N} = R, \lim_{N\to\infty} \Delta \geq R_e, P_e \leq \epsilon.$$

Then we will show the existence of random variables $K \to (X, V) \to Y \to Z$ such that

$$0 \leq R_e \leq R, \tag{B.1}$$

$$0 \leq R \leq I(K;Y) - I(K;V), \tag{B.2}$$

$$R_e \leq H(Y|Z). \tag{B.3}$$

B.1. Proof of (B.1)

$$R_e \leq \lim_{N\to\infty} \Delta = \lim_{N\to\infty} \frac{1}{N} H(W|Z^N) \leq \lim_{N\to\infty} \frac{1}{N} H(W) \overset{(a)}{=} R,$$

where (a) is from the fact that W is uniformly distributed over $\mathcal{W}$.

B.2. Proof of (B.2) and (B.3)

The formulas (B.2) and (B.3) are proved by Lemma 1, see the followings.

Lemma 1. *The random vectors Y^N, Z^N and the random variables W, K, Y, Z of Fig. 4 and Theorem 1, satisfy:*

$$\frac{1}{N} H(W) \leq I(K;Y) - I(K;V) + \delta(P_e), \tag{B.4}$$

$$\frac{1}{N} H(W|Z^N) \leq H(Y|Z) + \frac{1}{N}\delta(P_e), \tag{B.5}$$

where $\delta(P_e) = h(P_e) + P_e \log(|\mathcal{W}| - 1)$. *Note that* $h(P_e) = -P_e \log P_e - (1 - P_e)\log(1 - P_e)$.

Substituting $H(W) = \log\|\mathcal{W}\|$, $\frac{1}{N} H(W|Z^N) = \Delta$ and (2.4) into (B.4) and (B.5), it is easy to see that

$$R \leq I(K;Y) - I(K;V) + \delta(\epsilon), \tag{B.6}$$

$$R_e \leq H(Y|Z). \tag{B.7}$$

Letting $\epsilon \to 0$ and using the fact that $\delta(\epsilon) \to 0$ as $\epsilon \to 0$, the formulas (B.2) and (B.5) are obtained.

It remains to prove Lemma 1, see the followings. [Proof of Lemma 1] The formula (B.4) is from (B.8), (B.10) and (B.15). The formula (B.5) is proved by (B.9), (B.12) and (B.16).

<Part i> The left parts of the inequalities (B.4) and (B.5) are bounded by

$$\begin{aligned} \frac{1}{N} H(W) &= \frac{1}{N}(I(W;Y^N) + H(W|Y^N)) \\ &\overset{(1)}{\leq} \frac{1}{N}(I(W;Y^N) + \delta(P_e)), \end{aligned} \tag{B.8}$$

$$\begin{aligned}\frac{1}{N}H(W|Z^N) &\overset{(2)}{\leq} \frac{1}{N}H(W|Z^N)+\frac{1}{N}\delta(P_e)\\ &\quad -\frac{1}{N}H(W|Y^N,Z^N) \qquad (B.9)\\ &= \frac{1}{N}I(W;Y^N|Z^N)+\frac{1}{N}\delta(P_e),\end{aligned}$$

where (1) and (2) follow from the Fano's inequality.

<Part ii> The character $\frac{1}{N}I(W;Y^N)$ in formula (B.8) can be bounded by (B.10), see the followings.

$$\begin{aligned}&\frac{1}{N}I(W;Y^N)\overset{(a)}{=}\frac{1}{N}(I(W;Y^N)-I(W;V^N))\\ &\overset{(b)}{=}\frac{1}{N}\sum_{i=1}^{N}(I(Y_i;W,V_{i+1}^N|Y^{i-1})\\ &-I(V_i;W,Y^{i-1}|V_{i+1}^N))\\ &\overset{(c)}{\leq}\frac{1}{N}\sum_{i=1}^{N}(H(Y_i)-H(Y_i|Y^{i-1},W,V_{i+1}^N) \qquad (B.10)\\ &-H(V_i)+H(V_i|V_{i+1}^N,W,Y^{i-1}))\\ &=\frac{1}{N}\sum_{i=1}^{N}(I(Y_i;W,V_{i+1}^N,Y^{i-1})\\ &-I(V_i;W,Y^{i-1},V_{i+1}^N)).\end{aligned}$$

Formula (a) follows from the fact that W is independent of V^N.

Formula (b) is from the fact that

$$\begin{aligned}&\sum_{i=1}^{N}I(Y_i;V_{i+1}^N|Y^{i-1},W)\\ &=\sum_{i=1}^{N}I(V_i;Y^{i-1}|V_{i+1}^N,W). \qquad (B.11)\end{aligned}$$

Here note that the equality (B.11) is Csiszár's sum identity [2].

Formula (c) follows from that V^N is composed of N i.i.d. random variables.

<Part iii> The character $I(W;Y^N|Z^N)$ in formula (B.9) can be rewritten as follows,

$$\begin{aligned}\frac{1}{N}I(W;Y^N|Z^N) &\leq \frac{1}{N}H(Y^N|Z^N)\\ &\leq \frac{1}{N}\sum_{i=1}^{N}H(Y_i|Z_i). \qquad (B.12)\end{aligned}$$

<Part iv>(single letter) To complete the proof, we introduce an random variable J, which is independent of W, X^N, V^N, Y^N and Z^N. Furthermore, J is uniformly distributed over $\{1, 2, \ldots, N\}$. Define

$$K=(Y^{J-1},V_{J+1}^N,W,J), \qquad (B.13)$$

$$X=X_J, Y=Y_J, Z=Z_J, V=V_J. \qquad (B.14)$$

<Part v> Then (B.10) can be rewritten as

$$\begin{aligned}&\frac{1}{N}I(W;Y^N)\leq\frac{1}{N}\sum_{i=1}^{N}(I(Y_i;W,V_{i+1}^N,Y^{i-1})\\ &-I(V_i;W,Y^{i-1},V_{i+1}^N))\\ &=\frac{1}{N}\sum_{i=1}^{N}(I(Y_i;W,V_{i+1}^N,Y^{i-1}|J=i)\\ &-I(V_i;W,Y^{i-1},V_{i+1}^N|J=i)) \qquad (B.15)\\ &=I(Y_J;W,V_{J+1}^N,Y^{J-1}|J)-I(V_J;W,Y^{J-1},V_{J+1}^N|J)\\ &\overset{(a)}{\leq}I(Y_J;W,V_{J+1}^N,Y^{J-1},J)\\ &-I(V_J;W,Y^{J-1},V_{J+1}^N,J)\\ &\leq I(K;Y)-I(K;V),\end{aligned}$$

where (a) is from the fact that V_J is independent of J, i.e., $p(V_J=v,J=i)=p(V_J=v)p(J=i)$.

<Part vi> Similarly, (B.12) can be rewritten as follows,

$$\frac{1}{N}I(W;Y^N|Z^N)\leq H(Y|Z). \qquad (B.16)$$

Substituting (B.15) and (B.16) into (B.8) and (B.9), Lemma 1 is proved.

The Markov chain $K\to(X,V)\to Y\to Z$ is easy to be checked by using (B.13) and (B.14).

The proof of the converse part of Theorem 1 is completed.

Appendix C. Direct part of Theorem 2

In this section, we will show that any pair $(R, R_e)\in\mathcal{R}^c$ is achievable.

C.1. Code construction

Given a pair (R, R_e), choose a joint probability mass function $p_{K,V,X,Y,Z}(k,v,x,y,z)$ such that $0\leq R_e\leq R$, $R\leq I(K;Y)$ and $R_e\leq H(Y|Z)$.

The message set $\mathcal{W}$ satisfies:

$$\lim_{N\to\infty}\frac{1}{N}\log\|\mathcal{W}\|=R=I(K;Y)-\gamma_1, \qquad (C.1)$$

where γ and γ_1 are fixed positive numbers. Let $\mathcal{W}=\{1,2,\ldots,2^{NR}\}$.

We use the block Markov coding method. The random vectors K^N, V^N, X^N, Y^N and Z^N consist of n blocks of length N. The message for n blocks is $W^n=(W_2,W_3,\ldots,W_n)$, 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.

Let $\widetilde{Z}_i$ $(1\leq i\leq n)$ be the output of channel 2 for block i, $Z^n=(\widetilde{Z}_1,\ldots,\widetilde{Z}_n)$, $Z^j=(\widetilde{Z}_1,\ldots,\widetilde{Z}_{j-1},\widetilde{Z}_{j+1},\ldots,\widetilde{Z}_n)$ $(1\leq j\leq n)$. Similarly, $Y^n=(\widetilde{Y}_1,\ldots,\widetilde{Y}_n)$, and $\widetilde{Y}_i$ $(1\leq i\leq n)$ is the output of channel 1 for block i. The specific values of the above random vectors are denoted by lower case letters.

Code-book generation:

- **(Construction of K^N)**
  In the first block, generate a sequence k^N i.i.d. according to the probability mass function $p_K(k)$.
  In the i-th block $(2\leq i\leq n)$, firstly we generate a mapping $g_f:\mathcal{Y}^N\to\mathcal{W}$. Define a random variable $K_i^*=g_f(\widetilde{Y}_{i-1})$ $(2\leq i\leq n)$, which is uniformly distributed over $\mathcal{W}$, and K_i^* is independent of W_i. Reveal the mapping g_f to both receivers and the transmitter. Then, when the transmitter receives the output $\widetilde{y}_{i-1}$ of the i-1-th block, he computes $k_i^*=g_f(\widetilde{y}_{i-1})\in\mathcal{W}$.

Please cite this article in press as: Dai B, et al. Feedback enhances the security of wiretap channel with states. Int J Electron Commun (AEÜ) (2015), http://dx.doi.org/10.1016/j.aeue.2015.04.005

Given the encrypted message $w_i \oplus k_i^*$ (where $\oplus$ is the modulo addition over $\mathcal{W}$), generate a corresponding sequence k^N i.i.d. according to the probability mass function $p_K(k)$. Index k^N by $w_i \oplus k_i^* \in \mathcal{W}$.

- The construction of X^N is the same as that in Appendix A.

Decoding: For block i ($2 \le i \le n$), given a vector $\widetilde{y}_i \in \mathcal{Y}^N$, try to find a sequence $k^N(\hat{w}_i \oplus k_i^*)$ such that $(k^N(\hat{w}_i \oplus k_i^*), \widetilde{y}_i) \in T_{KY}^N(\epsilon_5)$. If there exists a sequence, put out the corresponding index $\hat{w}_i \oplus k_i^*$. Otherwise, declare a decoding error. Finally, since the legitimate receiver knows k_i^* ($k_i^* = g_f(\widetilde{y}_{i-1})$), put out the corresponding $\hat{w}_i$ from $\hat{w}_i \oplus k_i^*$.

C.2. Proof of achievability

Note that the encoding and decoding scheme for Theorem 2 is exactly the same as that in [9], except that the transmitted message for the legitimate receiver is $w \oplus k^*$. Since the legitimate receiver knows k^*, the decoding scheme for Theorem 2 is in fact the same as that in [9]. Hence, we omit the proof of $P_e \le \epsilon$ here. It remains to show that $\lim_{N\to\infty} \Delta \ge R_e$, see the following.

Since the message W is encrypted by $W \oplus K^*$, the equivocation about W is equivalent to the equivocation about K^*. There are two ways for the wiretapper to obtain the secret key k^*. One way is that he tries to guess the k^* from its alphabet $\mathcal{W}$. The other way is that he tries to guess the feedback y^N (y^N is the output of the main channel for the previous block, and $k^* = g_f(y^N)$) from the conditional typical set $T_{[Y|Z]}^N(\delta)$, and this is because for a given z^N and sufficiently large N, $Pr\{(y^N \notin T_{[Y|Z]}^N(\delta)\} \to 0$. Note that there are $2^{NH(Y|Z)}$ sequences $y^N \in T_{[Y|Z]}^N(\delta)$ when $N \to \infty$ and $\delta \to 0$. Therefore, the equivocation about W is $\min\{\frac{\log\|\mathcal{W}\|}{N} = R, H(Y|Z)\}$, and note that $R \ge R_e$ and $H(Y|Z) \ge R_e$, then $\lim_{N\to\infty} \Delta \ge R_e$ is obtained. The detail about the proof of $\lim_{N\to\infty} \Delta \ge R_e$ is exactly the same as (A.8), and it is omitted here.

Thus, $\lim_{N\to\infty} \Delta \ge R_e$ is proved, and the direct part of Theorem 2 is completed. The proof of Theorem 2 is completed.

Appendix D. Converse half of Theorem 2

Note that for the causal channel state information, V_i is independent of $K_i = (Y^{J-1}, V_{J+1}^N, W, J = i)$, and therefore, the character $I(K;V) = 0$ for the causal case. Thus the converse proof of Theorem 2 can be directly obtained from the converse proof of Theorem 1, and we omit it here. The proof of the converse part of Theorem 2 is completed.

References

[1] Wyner AD. The wire-tap channel. Bell Syst Tech J 1975;54:1355–87.
[2] Csiszár I, Körner J. Broadcast channels with confidential messages. IEEE Trans Inf Theory 1978;24:339–48.
[3] Leung-Yan-Cheong SK, Hellman ME. The Gaussian wire-tap channel. IEEE Trans Inf Theory 1978;24:451–6.
[4] Merhav N. Shannon's secrecy system with informed receivers and its application to systematic coding for wiretapped channels. IEEE Trans Inf Theory 2008;54:2723–34.
[5] Ahlswede R, Cai N. Transmission identification and common randomness capacities for wire-tap channels with secure feedback from the decoder. Gen Theory Inf Transf Comb 2006:258–75.
[6] Dai B, Han Vinck AJ, Luo Y, Zhuang Z. Capacity region of non-degraded wiretap channel with noiseless feedback. In: Proceedings of 2012 IEEE International Symposium on Information Theory. 2012.
[7] Lai L, El Gamal H, Poor V. The wiretap channel with feedback: encryption over the channel. IEEE Trans Inf Theory 2008;54:5059–67.
[8] Ardestanizadeh E, Franceschetti M, Javidi T, Kim Y. Wiretap channel with secure rate-limited feedback. IEEE Trans Inf Theory 2009;55:5353–61.
[9] Shannon CE. Channels with side information at the transmitter. IBM J Res Dev 1958;2:289–93.
[10] Kuznetsov NV, Tsybakov BS. Coding in memories with defective cells. Probl Peredachi Inform 1974;10:52–60.
[11] Gel'fand SI, Pinsker MS. Coding for channel with random parameters. Probl Control Inf Theory 1980;9:19–31.
[12] Costa MHM. Writing on dirty paper. IEEE Trans Inf Theory 1983;29:439–41.
[13] Steinberg Y. Coding for the degraded broadcast channel with random parameters, with causal and noncausal side information. IEEE Trans Inf Theory 2005;51:2867–77.
[14] Mitrpant C, Han Vinck AJ, Luo Y. An achievable region for the Gaussian wiretap channel with side information. IEEE Trans Inf Theory 2006;52:2181–90.
[15] Chen Y, Han Vinck AJ. Wiretap channel with side information. IEEE Trans Inf Theory 2008;54:395–402.
[16] Dai B, Luo Y. Some new results on wiretap channel with side information. Entropy 2012;14:1671–702.
[17] Csiszár I, Körner J. Information theory: coding theorems for discrete memoryless systems. London, UK: Academic; 1981. p. 123–4.
[18] Cover TM, Thomas JA. Elements of information theory. 2nd edition NJ: Willey-Interscience; 2006.

Please cite this article in press as: Dai B, et al. Feedback enhances the security of wiretap channel with states. Int J Electron Commun (AEÜ) (2015), http://dx.doi.org/10.1016/j.aeue.2015.04.005