entropy

MDPI

Article

Feedback Schemes for the Action-Dependent Wiretap Channel with Noncausal State at the Transmitter

Haonan Zhang [1,†], Linman Yu [2,†] and Bin Dai [1,*,†]

1 School of Information Science and Technology, Southwest Jiaotong University, Chengdu 611756, China; cq@my.swjtu.edu.cn
2 School of Economics and Management, Chengdu Textile College, Chengdu 611731, China; yulinman1991@gmail.com
* Correspondence: daibin@home.swjtu.edu.cn; Tel.: +86-135-480-53724
† These authors contributed equally to this work.

Received: 29 December 2018; Accepted: 9 March 2019; Published: 13 March 2019

Abstract: In this paper, we propose two feedback coding schemes for the action-dependent wiretap channel with noncausal state at the transmitter. The first scheme follows from the already existing secret key based feedback coding scheme for the wiretap channel. The second one follows from our recently proposed hybrid feedback scheme for the wiretap channel. We show that, for the action-dependent wiretap channel with noncausal state at the transmitter, the second feedback scheme performs better than the first one, and the capacity results of this paper are further explained via a Gaussian example, which we call the action-dependent dirty paper wiretap channel with noiseless feedback.

Keywords: action-dependent channel; dirty paper channel; noiseless feedback; secrecy capacity; wiretap channel

1. Introduction

Using channel feedback to enhance the physical layer security (PLS) of a communication system was first proposed by Ahlswede and Cai [1], who re-visited the foundation of the PLS—the wiretap channel model [2]—by considering a noiseless feedback channel from the legitimate receiver to the transmitter. Ahlswede et al. [1] showed that, since the eavesdropper does not know the feedback, the legitimate receiver's feedbackcan be used to generate secret keys shared between the transmitter and the legitimate receiver, and these keys can be used to encrypt the transmitted message. Using the feedback scheme in [1], it has been shown that the secrecy capacity (channel capacity with perfect secrecy constraint) of the wiretap channel can be enhanced. Furthermore, Ahlswede et al. [1] showed that this usage of feedback is optimal (achieving the secrecy capacity of the wiretap channel with noiseless feedback) if the channel is physically degraded (the eavesdropper's received signal is a degraded version of the legitimate receiver's). In recognition of this, Ardestanizadeh et al. [3] further pointed out that, if the noiseless feedback channel can be used to transmit anything the legitimate parties wish, the best choice of the legitimate parties is to send pure random bits (secret key) over the feedback channel. Subsequently, Schaefer et al. [4] extended the work of [3] to a broadcast situation, where two legitimate receivers of the broadcast channel independently send their secret keys to the transmitter via two noiseless feedback channels, and these keys help to enhance the achievable secrecy rate region of the broadcast wiretap channel [5]. Other related works in the PLS of the feedback channels include those by [6–8], who introduced channel state information (CSI) into various feedback channel models. Recently, Dai et al. [9] showed that, for the general wiretap channel (without physically degraded assumption), a better usage of the feedback is to generate not only key but also

cooperative message from it, and this cooperative message helps the legitimate receiver to improve his decoding performance. Dai et al. [9] showed that this new feedback scheme achieves a larger achievable secrecy rate than the already existing secret key based feedback scheme [1] does.

Channel with noncausal state at the transmitter was first investigated by [10], and the capacity of this channel model was found by [11]. Subsequently, Costa et al. [12] studied the Gaussian case in [11], which is known as the dirty paper channel, and showed that the capacity of the dirty paper channel equals the capacity of the Gaussian channel without the state (also called interference). Here, note that the channel state in [10–12] is assumed to be independent of the transmitted message. In [13], the channel with noncausal or causal state available at the transmitter is revisited by considering the case that the transmitter can take actions on the channel state, i.e., the state is no longer independent of the transmitted message. This model is known as the action-dependent channel with states, and the capacity of this model is determined for both the noncausal and causal cases. Moreover, for the Gaussian case of the action-dependent channel with states (also called action-dependent dirty paper channel), it is shown that the actions on the state enhance the capacity of the dirty paper channel. Recently, a natural extension of the channel with noncausal state at the transmitter to the secrecy communication setting receives a lot of attention.Specifically, the authors of [14–16] studied the discrete memoryless wiretap channel with noncausal state at the transmitter, and proposed lower and upper bounds on its secrecy capacity. Mitrpant et al. [17] studied the Gaussian case in [14] (also called the dirty paper wiretap channel), and showed that the state (interference) non-causally known by the transmitter helps to enhance the secrecy capacity of the Gaussian wiretap channel [18]. Dai et al. [19] extended the state-dependent wiretap channel [14] to a broadcast situation, and proposed inner and outer bounds on the secrecy capacity region of this model. Dai et al. [20] studied the physically degraded action-dependent wiretap channel with noncausal state, and proposed lower and upper bounds on its secrecy capacity. Here, note that the action encoder in [20] is assumed to be deterministic, which implies that the output of the action encoder is a deterministic function of the transmitted message, and this leads to additional information leakage to the eavesdropper. Based on the work of [20,21] studied the feedback effect on the model proposed in [20]. A secret key based feedback scheme is provided in [21], and it is shown to be optimal for the physically degraded case.

In this paper, we study the action-dependent wiretap channel with noncausal state and noiseless feedback (the model of this paper can be viewed as the model of [21] without physically degraded assumption and with stochastic action encoder) (see Figure 1), and try to answer the following two fundamental questions:

(1) How should the feedback scheme in [9] be extended to the action-dependent wiretap channel with noncausal state?
(2) For the action-dependent wiretap channel with noncausal state, does the hybrid feedback scheme in [9] still gain advantages over the traditional one used in [1–8]?

The main contribution of this paper includes:

(1) We propose a new lower bound on the secrecy capacity of the action-dependent wiretap channel with noncausal state and noiseless feedback, which is constructed according to a hybrid feedback scheme similar to that in [9].
(2) From a Gaussian example, which is also called the action-dependent dirty paper wiretap channel with noiseless feedback, we show that our new lower bound on the secrecy capacity is larger than the secret key based lower bound. Moreover, we find that our new lower bound achieves the secrecy capacity for some special cases.

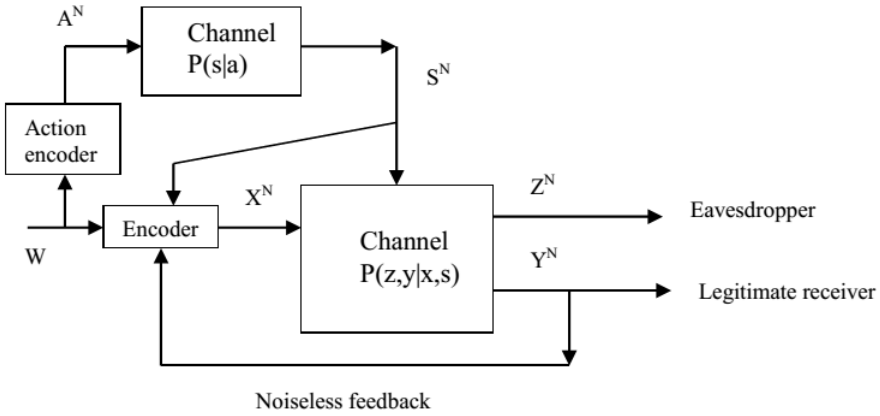

Figure 1. The action-dependent wiretap channel with noncausal state and noiseless feedback.

The remainder of this paper is organized as follows. Section 2 is about the problem formulation and the main result of this paper. The achievability proof of our new lower bound on the secrecy capacity of the action-dependent wiretap channel with noncausal state and noiseless feedback is provided in Section 3. A Gaussian example and numerical results are provided in Section 4. Final conclusions are presented in Section 5.

2. Problem Formulation and New Result

Notations: For the rest of this manuscript, the random variables (RVs), values and alphabets are written in uppercase letters, lowercase letters and calligraphic letters, respectively. The random vectors and their values are denoted by a similar convention. For example, Y represents a RV, and y represents a value in the alphabet $\mathcal{Y}$. Similarly, Y^N represents a random N-vector $(Y_1, ..., Y_N)$, and $y^N = (y_1, ..., y_N)$ represents a vector value in $\mathcal{Y}^N$ (the Nth Cartesian power of $\mathcal{Y}$). In addition, for an event $X = x$, its probability is denoted by $P(x)$. In the remainder of this manuscript, the base of the log function is 2.

Model description: In Figure 1, the channel is discrete memoryless, i.e., the overall channel transition probability is given by

$$P(y^N, z^N|x^N, s^N) = \prod_{i=1}^{N} P(z_i, y_i|x_i, s_i), \tag{1}$$

where $s_i \in \mathcal{S}$, $x_i \in \mathcal{X}$, $y_i \in \mathcal{Y}$ and $z_i \in \mathcal{Z}$. The message W is uniformly distributed in its alphabet $\mathcal{W} = \{1, 2, ..., |\mathcal{W}|\}$, and a stochastic action encoder encodes W into an action sequence A^N. The channel state sequence S^N is generated through a discrete memoryless channel (DMC) $A^N \to S^N$ with transition probability $P(s|a)$. Since S^N is non-causally known by the channel encoder and the legitimate receiver's channel output is sent back to the transmitter, the ith ($i \in \{1, 2, ..., N\}$) channel input $X_i = f_i(W, S^N, Y^{i-1})$, where f_i is a stochastic encoding function. The legitimate receiver produces an estimation $\hat{W} = \psi(Y^N)$ (ψ is the legitimate receiver's decoding function), and the average decoding error probability equals

$$P_e = \frac{1}{|\mathcal{W}|} \sum_{i \in \mathcal{W}} Pr\{\psi(y^N) \neq i | i \text{ sent}\}. \tag{2}$$

The eavesdropper's equivocation rate of the message W is formulated as

$$\Delta = \frac{1}{N} H(W|Z^N). \tag{3}$$

Given a positive number R, if for arbitrarily small ϵ and sufficiently large N, there exist a pair of channel encoder and decoder described above such that

$$\frac{\log|\mathcal{W}|}{N} \geq R-\epsilon,\ \Delta \geq R-\epsilon,\ P_e \leq \epsilon, \tag{4}$$

we say R is achievable with weak perfect secrecy. The secrecy capacity $\mathcal{C}_{sa}^{f}$ consists of all achievable weak secrecy rates, and bounds on $\mathcal{C}_{sa}^{f}$ are given in the following theorems and corollary.

Theorem 1. *$\mathcal{C}_{sa}^{f} \geq R_{sa}^{f*}$, where*

$$R_{sa}^{f*} = \max\min\{I(U;Y)-I(U;S|A), [I(U;V,Y)-I(U;Z)]^{+}+H(Y|U,Z)\}, \tag{5}$$

$[x]^{+} = x$ for $x \geq 0$, else $[x]^{+} = 0$, and the joint distribution is denoted by

$$P(u,v,a,s,x,y,z) = P(v|u,y)P(y,z|x,s)P(x|u,s)P(u|a,s)P(a,s). \tag{6}$$

Proof. The lower bound R_{sa}^{f*} is achieved by combining the binning scheme in [13] with the hybrid coding scheme in [9], and the details about the proof are in Section 3. □

The following lower bound R_{sa}^{f**} in Corollary 1 can be directly obtained from Theorem 1 by letting V be constant, and this lower bound can be viewed as a secret key based lower bound (application of the secret key based feedback strategy [1] to the model of Figure 1) on $\mathcal{C}_{sa}^{f}$.

Corollary 1. *$\mathcal{C}_{sa}^{f} \geq R_{sa}^{f**}$, where*

$$R_{sa}^{f**} = \max\min\{I(U;Y)-I(U;S|A), [I(U;Y)-I(U;Z)]^{+}+H(Y|U,Z)\}, \tag{7}$$

and the joint distribution is denoted by

$$P(u,a,s,x,y,z) = P(y,z|x,s)P(x|u,s)P(u|a,s)P(a,s). \tag{8}$$

Remark 1. *Note that [21] also proposed a secret key based lower bound on the secrecy capacity of the physically degraded action-dependent wiretap channel with noncausal state and noiseless feedback. However, we should point out that the model studied in [21] assumes the action encoder is a deterministic encoder, i.e., if the eavesdropper knows A^N, he also knows the message W. Hence, our lower bound R_{sa}^{f**} generalizes that in [21] as the deterministic action encoder is a special case of the stochastic one studied in this paper and there is no physically degraded assumption in this paper.*

Besides the above lower bounds on $\mathcal{C}_{sa}^{f}$, the following theorem shows a simple upper bound on $\mathcal{C}_{sa}^{f}$.

Theorem 2. *$\mathcal{C}_{sa}^{f} \leq \mathcal{C}_{sa}^{f-out}$, where*

$$\mathcal{C}_{sa}^{f-out} = \max(I(U;Y)-I(U;S|A)), \tag{9}$$

and the joint distribution is denoted by Equation (8).

Proof. Since $\mathcal{C}_{sa}^{f}$ cannot exceed the capacity of the model in Figure 1 without eavesdropper, we know that $\mathcal{C}_{sa}^{f}$ is upper bounded by the capacity of the action-dependent channel with feedback. In [13], it has been shown that feedback does not increase the capacity of the action-dependent channel ($\max(I(U;Y)-I(U;S|A))$), hence Theorem 2 is proved. The proof of Theorem 2 is completed. □

In Section 4, the above proposed hybrid lower bound R_{sa}^{f*} ise compared with the secret key based lower bound R_{sa}^{f**} via a Gaussian example, and we show which feedback strategy performs better.

3. Proof of Theorem 1

In this section, the hybrid feedback strategy for the wiretap channel [9] and the binning scheme for the action-dependent channel with noncausal state at the transmitter [13] are combined to show the achievability of Theorem 1. The rest of this section is organized as follows. The code-book construction and the transmission scheme are described in Section 3.1, and the equivocation analysis of the proposed scheme is shown in Section 3.2.

3.1. Code-Book Construction and Transmission Scheme

Definitions and notations:

- Similar to the coding scheme in [9], suppose that the overall transmission consists of B blocks, and the codeword length in each block is N.
- The overall message W is composed of B components ($W = (W_1, ..., W_B)$), and each component W_b ($b \in \{1, 2, ..., B\}$) is the message transmitted in block b. The value of W_b belongs to the set $\{1, ..., 2^{NR}\}$. Next, split W_b into two parts $W_b = (W_{b,1}, W_{b,2})$, and the values of $W_{b,1}$ and $W_{b,2}$, respectively, belong to the sets $\{1, ..., 2^{NR_1}\}$ and $\{1, ..., 2^{NR_2}\}$. Note that $R_1 + R_2 = R$.
- Analogously, the randomly produced dummy messages $W^{'}$ and $W^{''}$, which are used to confuse the wiretapper, also consist of B components ($W^{'} = (W_1^{'}, ..., W_B^{'})$ and $W^{''} = (W_1^{''}, ..., W_B^{''})$), and the components $W_b^{'}$ and $W_b^{''}$ ($b \in \{1, 2, ..., B\}$) are transmitted in block b. Here, note that $W_b^{'}$ and $W_b^{''}$ are uniformly drawn from the sets $\{1, ..., 2^{NR^{'}}\}$ and $\{1, ..., 2^{NR^{''}}\}$, respectively.
- The auxiliary message W^*, which is used to cooperate with the channel state, consists of B components ($W^* = (W_1^*, ..., W_B^*)$), and the value of W_b^* ($b \in \{1, 2, ..., B\}$) belongs to the set $\{1, ..., 2^{NR^*}\}$.
- The help information W^{**} and W^{***}, which is used to ameliorate the legitimate receiver's decoding performance, consists of B components ($W^{**} = (W_1^{**}, ..., W_B^{**})$ and $W^{***} = (W_1^{***}, ..., W_B^{***})$), and the value of W_b^{**} and W_b^{***} ($b \in \{1, 2, ..., B\}$), respectively, belongs to the sets $\{1, ..., 2^{NR^{**}}\}$ and $\{1, ..., 2^{NR^{***}}\}$.
- In block b ($1 \leq b \leq B$), the random vectors A^N, X^N, Y^N, Z^N, S^N, U^N and V^N are denoted by $\bar{A}_b$, $\bar{X}_b$, $\bar{Y}_b$, $\bar{Z}_b$, $\bar{S}_b$, $\bar{U}_b$ and $\bar{V}_b$, respectively. In addition, let $X^B = (\bar{X}_1, ..., \bar{X}_B)$ be a collection of the random vectors X^N for all blocks. Analogously, we have $A^B = (\bar{A}_1, ..., \bar{A}_B)$, $Y^B = (\bar{Y}_1, ..., \bar{Y}_B)$, $Z^B = (\bar{Z}_1, ..., \bar{Z}_B)$, $S^B = (\bar{S}_1, ..., \bar{S}_B)$, $U^B = (\bar{U}_1, ..., \bar{U}_B)$ and $V^B = (\bar{V}_1, ..., \bar{V}_B)$. The vector value is written in lower case letter.

Code-book generation:

- In block b ($1 \leq b \leq B$), randomly produce $2^{N(R_1+R_2+R^{''})}$ i.i.d. codewords $\bar{a}_b$ with respect to (w.r.t.) $P(a)$, and label them as $\bar{a}_b(w_{b,1}, w_{b,2}, w_b^{''})$, where $w_{b,1} \in \{1, 2, ..., 2^{NR_1}\}$, $w_{b,2} \in \{1, 2, ..., 2^{NR_2}\}$ and $w_b^{''} \in \{1, 2, ..., 2^{NR^{''}}\}$.
- In block b ($1 \leq b \leq B$), randomly produce $2^{N(R_1+R_2+R^{'}+R^*+R^{**})}$ i.i.d. codewords $\bar{u}_b$ w.r.t. $P(u|a, s)$, and label them as $\bar{u}_b(w_{b,1}, w_{b,2}, w_b^{'}, w_b^*, w_{b-1}^{**})$, where $w_{b,1} \in \{1, 2, ..., 2^{NR_1}\}$, $w_{b,2} \in \{1, 2, ..., 2^{NR_2}\}$, $w_b^{'} \in \{1, 2, ..., 2^{NR^{'}}\}$, $w_b^* \in \{1, 2, ..., 2^{NR^*}\}$ and $w_{b-1}^{**} \in \{1, 2, ..., 2^{NR^{**}}\}$.
- For each possible value of $\bar{u}_b(w_{b,1}, w_{b,2}, w_b^{'}, w_b^*, w_{b-1}^{**})$ and $\bar{y}_b$, randomly produce $2^{N(R^{**}+R^{***})}$ i.i.d. codewords $\bar{v}_b$ on the basis of $P(v|u, y)$. Then, label these $\bar{v}_b$ as $\bar{v}_b(w_b^{**}, w_b^{***})$, where $w_b^{**} \in \{1, 2, ..., 2^{NR^{**}}\}$ and $w_b^{***} \in \{1, 2, ..., 2^{NR^{***}}\}$.
- For given $\bar{u}_b$ and $\bar{s}_b$, the transmitted sequence $\bar{x}_b$ is i.i.d. produced on the basis of the probability $P(x|u, s)$.

Encoding scheme:

- For block 1, the transmitter chooses $\bar{a}_1(w_{1,1}, w_{1,2} = 1, w_1^{''})$. Next, define $w_0^{**} = 1$, for given $\bar{a}_1(w_{1,1}, w_{1,2} = 1, w_1^{''})$ and the state sequence $\bar{s}_1$, the transmitter selects an index w_1^* such that $(\bar{u}_1(w_{1,1}, w_{1,2} = 1, w_1^{'}, w_1^*, w_0^{**} = 1), \bar{a}_1(w_{1,1}, w_{1,2} = 1, w_1^{''}), \bar{s}_1)$ are jointly typical. If no such w_1^* exists, declare an encoding error. If multiple w_1^* exist, randomly pick out one. Based on the Covering Lemma [22], the encoding error tends to zero if

$$R^* > I(U; S|A). \tag{10}$$

- For block b ($i \in \{2, 3, ..., B-1\}$), before transmission, produce a mapping $g_b : \bar{y}_{b-1} \to \{1, 2, ..., 2^{NR_2}\}$ (this mapping is generated exactly the same as that in [1]). Based on this mapping, generate a random variable (RV) $K_b = g_b(\bar{Y}_{b-1})$ taking values in $\{1, 2, ..., 2^{NR_2}\}$, and $Pr\{K_b = j\} = 2^{-NR_2}$ for $j \in \{1, 2, ..., 2^{NR_2}\}$. The RV K_b is used as a secret key and it is not known to the eavesdropper, and K_b is independent of the real transmitted messages $W_{b,1}$ and $W_{b,2}$ for block b. Notice that $k_b = g_b(\bar{y}_{b-1}) \in \{1, 2, ..., 2^{NR_2}\}$ is a realization of K_b. The mapping g_b is revealed to all parties. First, since the transmitter knows its own $\bar{u}_{b-1}(w_{b-1,1}, w_{b-1,2} \oplus k_{b-1}, w_{b-1}^{'}, w_{b-1}^*, w_{b-2}^{**})$, $\bar{a}_{b-1}(w_{b-1,1}, w_{b-1,2}, w_{b-1}^{''})$, $\bar{s}_{b-1}$ and $\bar{y}_{b-1}$, he tries to find a $\bar{v}_{b-1}(w_{b-1}^{**}, w_{b-1}^{***})$ such that $(\bar{v}_{b-1}, \bar{u}_{b-1}, \bar{y}_{b-1}, \bar{s}_{b-1}, \bar{a}_{b-1})$ are jointly typical. For the case that more than one $\bar{v}_{b-1}$ exist, randomly pick one; if no such $\bar{v}_{b-1}$ exists, declare an encoding error. According to the Covering Lemma [22], the encoding error approaches to zero if

$$R^{**} + R^{***} \geq I(V; U, Y, A, S) \overset{(1)}{=} I(V; U, Y), \tag{11}$$

where (1) is from the definition in Equation (6), which implies that $V \to (U, Y) \to (A, S)$. Next, the transmitter chooses $\bar{a}_b(w_{b,1}, w_{b,2}, w_b^{''})$. Finally, since the transmitter obtains $\bar{v}_{b-1}(w_{b-1}^{**}, w_{b-1}^{***})$, he extracts w_{b-1}^{**} and tries to find a w_b^* such that $(\bar{u}_b(w_{b,1}, w_{b,2} \oplus k_b, w_b^{'}, w_b^*, w_{b-1}^{**}), \bar{a}_b(w_{b,1}, w_{b,2}, w_b^{''}), \bar{s}_b)$ are jointly typical. If no such w_b^* exists, declare an encoding error. If multiple w_b^* exist, randomly pick out one. Based on the Covering Lemma [22], the encoding error tends to zero if Equation (10) holds. The codeword $\bar{u}_b(w_{b,1}, w_{b,2} \oplus k_b, w_b^{'}, w_b^*, w_{b-1}^{**})$ is picked for transmission.
- At block B, first, the transmitter chooses $\bar{a}_B(1, 1, 1)$. Next, after receiving the feedback $\bar{y}_{B-1}$, the transmitter tries to find a $\bar{v}_{B-1}(w_{B-1}^{**}, w_{B-1}^{***})$ such that $(\bar{v}_{B-1}(w_{B-1}^{**}, w_{B-1}^{***}), \bar{u}_{B-1}, \bar{y}_{B-1}, \bar{s}_{B-1}, \bar{a}_{B-1})$ are jointly typical. After decoding such $\bar{v}_{B-1}(w_{B-1}^{**}, w_{B-1}^{***})$, the transmitter extracts w_{B-1}^{**} and tries to find a w_B^* such that $(\bar{u}_B(1, 1, 1, w_B^*, w_{B-1}^{**}), \bar{a}_B(1, 1, 1), \bar{s}_B)$ are jointly typical. If no such w_B^* exists, declare an encoding error. If multiple w_B^* exist, randomly pick out one. The codeword $\bar{u}_B(1, 1, 1, w_B^*, w_{B-1}^{**})$ is picked for transmission.

Decoding scheme:

The decoding procedure starts from block B. At block B, the legitimate receiver chooses a $\bar{u}_B(1, 1, 1, w_B^*, w_{B-1}^{**})$ which is jointly typical with $\bar{y}_B$ and $\bar{a}_B(1, 1, 1)$. For the case that more than one or no such $\bar{u}_B$ exists, declare a decoding error. Based on the Packing Lemma [22] and a similar argument in [13], this kind of decoding error approaches to zero when

$$R^* + R^{**} \leq I(U; Y). \tag{12}$$

After decoding $\bar{u}_B$, the legitimate receiver extracts w_{B-1}^{**} from it. Then, he tries to select only one $\bar{v}_{B-1}(w_{B-1}^{**}, w_{B-1}^{***})$ such that given w_{B-1}^{**}, $\bar{v}_{B-1}$ is jointly typical with $\bar{y}_{B-1}$. For the case that more than one or no such $\bar{v}_{B-1}$ exist, declare a decoding error. Based on the Packing Lemma [22], this kind of decoding error approaches to zero when

$$R^{***} \leq I(V; Y). \tag{13}$$

After obtaining such unique $\bar{v}_{B-1}$, the legitimate receiver tries to find only one pair of $(\bar{u}_{B-1}, \bar{a}_{B-1})$ such that $(\bar{y}_{B-1}, \bar{a}_{B-1}, \bar{v}_{B-1}, \bar{u}_{B-1})$ are jointly typical. Based on the Packing Lemma [22] and a similar argument in [13], this kind of decoding error approaches to zero when

$$R_1 + R_2 + R^{'} + R^{*} + R^{**} + R^{''} \leq I(U; V, Y). \tag{14}$$

After decoding $\bar{u}_{B-1}$, the legitimate receiver picks out $w_{B-1,1}$, $w_{B-1,2} \oplus k_{B-1}$, w^{**}_{B-2} from it. Note that the legitimate receiver has full knowledge of $k_{B-1} = g_{B-1}(\bar{y}_{B-2})$, and hence he obtains the message $w_{B-1} = (w_{B-1,1}, w_{B-1,2})$. Analogously, the legitimate receiver decodes the messages $w_{B-2}, w_{B-3}, \ldots, w_1$, and the decoding procedure is completed. For convenience, the encoding and decoding schemes are explained by the following Figures 2 and 3, respectively.

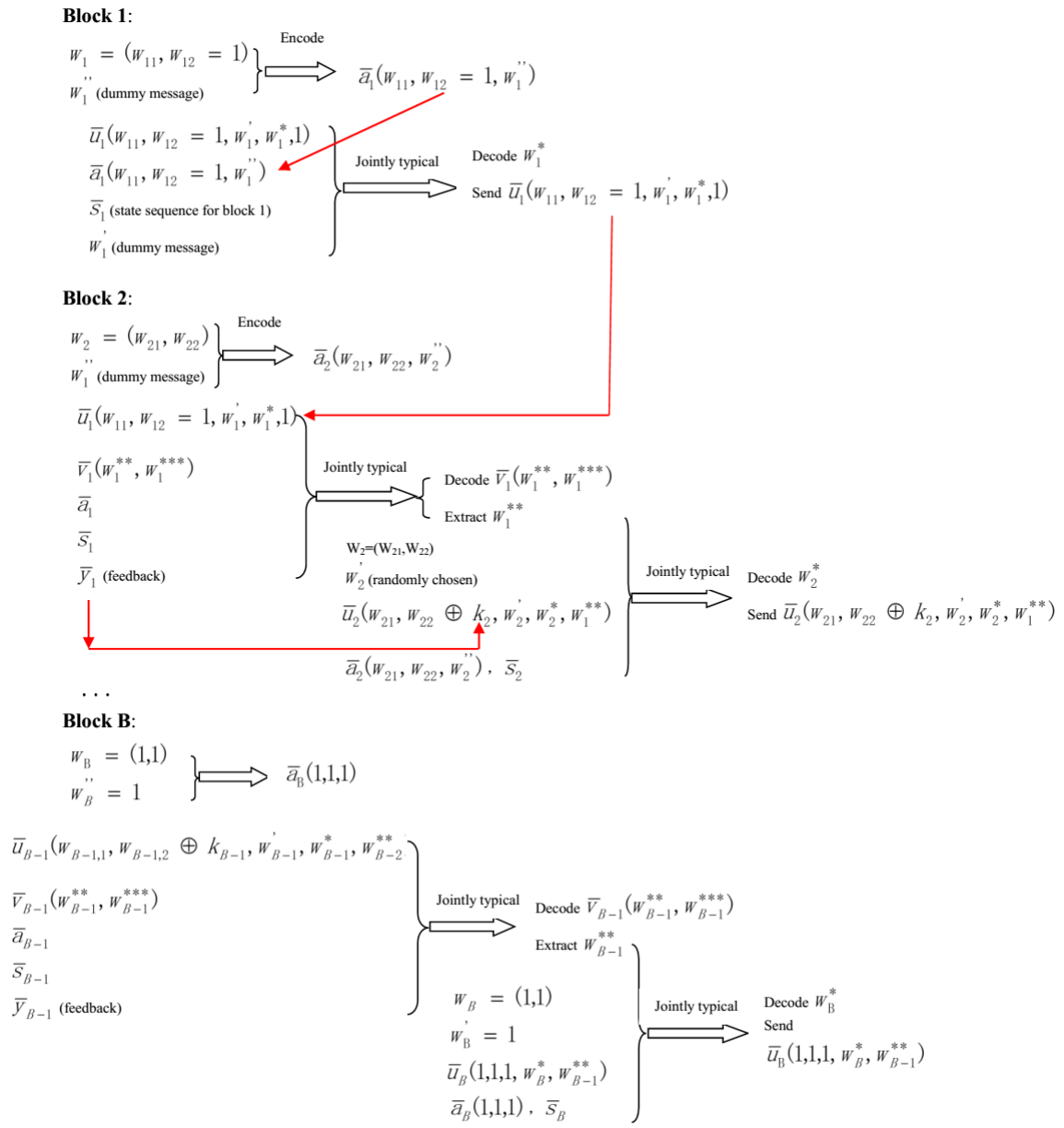

Figure 2. The encoding procedure for all blocks.

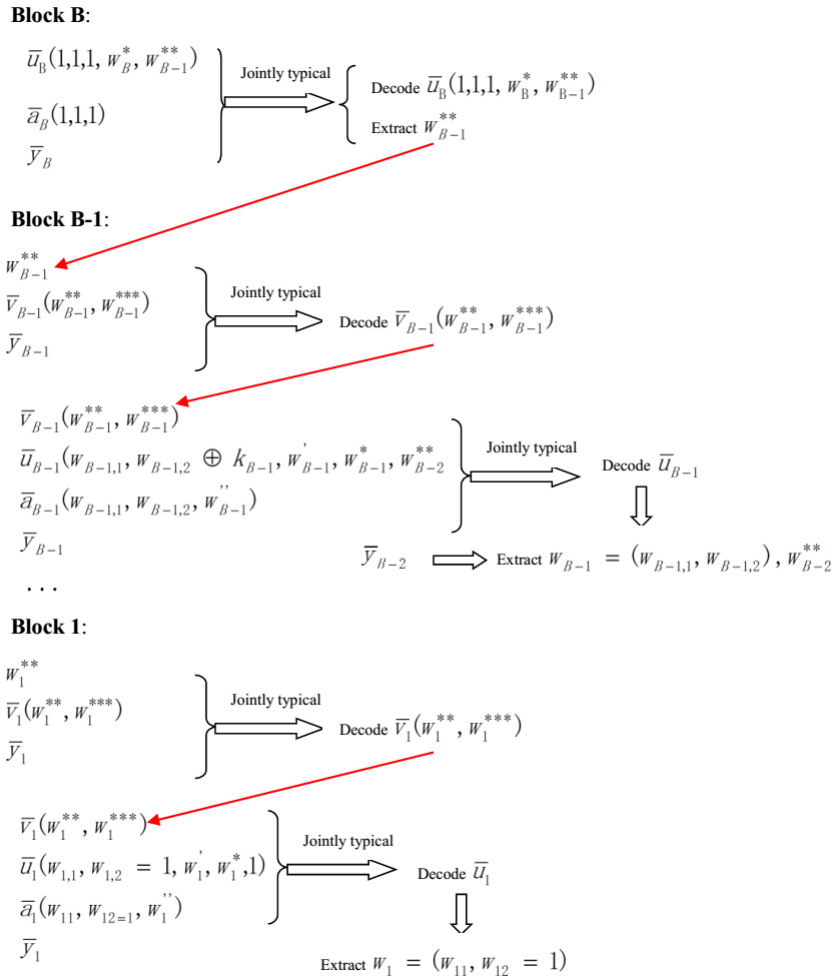

Figure 3. The decoding procedure for all blocks.

3.2. Equivocation Analysis

The overall equivocation Δ, which is denoted by $\Delta = \frac{1}{BN} H(W|Z^B)$, is given by

$$\Delta \overset{(a)}{=} \frac{1}{BN}(H(\tilde{W}_1|Z^B) + H(\tilde{W}_2|Z^B, \tilde{W}_1)), \tag{15}$$

where (a) is due to the definitions $\tilde{W}_1 = (W_{1,1}, ..., W_{B,1})$ and $\tilde{W}_2 = (W_{1,2}, ..., W_{B,2})$.

The term $H(\tilde{W}_1|Z^B)$ in Equation (15) can be bounded by

$$\begin{aligned}
&H(\tilde{W}_1|Z^B) = H(\tilde{W}_1, Z^B) - H(Z^B) \\
&= H(\tilde{W}_1, Z^B, U^B) - H(U^B|\tilde{W}_1, Z^B) - H(Z^B) \\
&\overset{(b)}{=} H(U^B) - H(U^B|\tilde{W}_1, Z^B) - I(U^B; Z^B) \\
&\overset{(c)}{=} (B-1)NR_1 + (B-2)NR_2 + (B-1)NR^{'} + BNR^* + (B-1)NR^{**} - BNI(U;Z) - H(U^B|\tilde{W}_1, Z^B) \\
&\overset{(d)}{\geq} (B-1)NR_1 + (B-2)NR_2 + (B-1)NR^{'} + BNR^* + (B-1)NR^{**} - BNI(U;Z) - BN\epsilon_3,
\end{aligned} \tag{16}$$

where (b) is implied by $H(\tilde{W}_1|U^B) = 0$, (c) is due to the construction of U^B and the channel is memoryless, and (d) is due to that given $\tilde{w}_1$ and z^B, the eavesdropper attempts to find a unique u^B that is jointly typical with his own received signals z^B, and according to the Packing Lemma [22], we can conclude that the eavesdropper's decoding error tends to zero if

$$R_2 + R^{'} + R^* + R^{**} \leq I(U;Z), \tag{17}$$

then applying Fano's inequality, $\frac{1}{BN}H(U^B|\tilde{W}_1, Z^B) \leq \epsilon_3$ is obtained, where $\epsilon_3 \to 0$ while $B, N \to \infty$.

Moreover, the term $H(\tilde{W}_2|Z^B, \tilde{W}_1)$ in Equation (15) can be bounded by

$$\begin{aligned}
&H(\tilde{W}_2|Z^B, \tilde{W}_1)\\
&\geq \sum_{i=2}^{B-1} H(W_{i,2}|Z^B, \tilde{W}_1, W_{1,2} = 1, ..., W_{i-1,2}, W_{i,2} \oplus K_i)\\
&\overset{(e)}{=} \sum_{i=2}^{B-1} H(W_{i,2}|\bar{Z}_{i-1}, W_{i,2} \oplus K_i)\\
&\geq \sum_{i=2}^{B-1} H(W_{i,2}|\bar{Z}_{i-1}, \bar{U}_{i-1}, W_{i,2} \oplus K_i)\\
&= \sum_{i=2}^{B-1} H(K_i|\bar{Z}_{i-1}, \bar{U}_{i-1}, W_{i,2} \oplus K_i)\\
&\overset{(f)}{=} \sum_{i=2}^{B-1} H(K_i|\bar{Z}_{i-1}, \bar{U}_{i-1})\\
&\overset{(g)}{\geq} (B-2)(\log \frac{1-\epsilon_1}{1+\delta} + N(1-\epsilon_2)H(Y|U, Z)),
\end{aligned} \tag{18}$$

where (e) is due to the Markov chain $W_{i,2} \to (\bar{Z}_{i-1}, W_{i,2} \oplus K_i) \to (\tilde{W}_1, W_{1,2}, ..., W_{i-1,2}, \bar{Z}_1, ..., \bar{Z}_{i-2}, \bar{Z}_i, ..., \bar{Z}_B)$, (f) follows by $K_i \to (\bar{Z}_{i-1}, \bar{U}_{i-1}) \to W_{i,2} \oplus K_i$, and (g) is from the balanced coloring Lemma [9] (p. 264), i.e., given $\bar{z}_{i-1}$ and $\bar{u}_{i-1}$, there are at least $\frac{\gamma}{1+\delta}$ colors, which implies that

$$H(K_i|\bar{Z}_{i-1}, \bar{U}_{i-1}) \geq \log \frac{1-\epsilon_1}{1+\delta} + N(1-\epsilon_2)H(Y|U, Z), \tag{19}$$

where ϵ_1, ϵ_2 and δ approach to 0 as N goes to infinity.

Substituting Equations (16) and (18) into Equation (15), we have

$$\begin{aligned}
\Delta \geq\ & R^* + \frac{B-1}{B}(R_1 + R^{'} + R^{**}) + \frac{B-2}{B}R_2 - I(U; Z) - \epsilon_3\\
&+ \frac{B-2}{BN}\log \frac{1-\epsilon_1}{1+\delta} + \frac{B-2}{B}(1-\epsilon_2)H(Y|U, Z).
\end{aligned} \tag{20}$$

The bound in Equation (20) indicates that if

$$R^{'} + R^* + R^{**} \geq I(U; Z) - H(Y|U, Z), \tag{21}$$

$\Delta \geq R_1 + R_2 - \epsilon$ can be proved by choosing sufficiently large B and N.

Now combining Equation (11) with Equation (13), we have

$$R^{**} \geq I(U, Y; V) - I(Y; V) = I(V; U|Y). \tag{22}$$

Next, from Equations (22), (10) and (14), we can conclude that

$$R_1 + R_2 + R^{'} + R^{''} \leq I(Y, V; U) - I(V; U|Y) - I(U; S|A) = I(U; Y) - I(U; S|A). \tag{23}$$

Then, implied by Equations (21) and (14), we have

$$R_1 + R_2 + R^{''} \leq I(Y, V; U) - I(U; Z) + H(Y|U, Z). \tag{24}$$

Finally, applying Fourier–Motzkin elimination to remove R_1, R_2 ($R = R_1 + R_2$), $R^{'}$, $R^{''}$, R^* and R^{**} from Equations (22), (23), (24), (12), (14), (17) and (21), Theorem 1 is proved.

4. The Action-Dependent Dirty Paper Wiretap Channel with Noiseless Feedback

The Gaussian case of the action-dependent wiretap channel with noncausal state at the transmitter and feedback, which we also call the action-dependent dirty paper wiretap channel with noiseless feedback, is depicted in Figure 4. At time i ($i \in \{1, 2, ..., N\}$), the inputs and outputs of this Gaussian model satisfy

$$S_i = A_i + W_i,\ Y_i = X_i + S_i + \eta_{1,i},\ Z_i = X_i + tS_i + \eta_{2,i}, \tag{25}$$

where X_i is the channel input subject to an average power constraint P, A_i is the output of the action encoder subject to an average power constraint P_A, t is a constant, and W_i, $\eta_{1,i}$, $\eta_{2,i}$ are independent Gaussian noises and are i.i.d. across the time index i. Here, note that $W_i \sim \mathcal{N}(0, \sigma_w^2)$, $\eta_{1,i} \sim \mathcal{N}(0, \sigma_1^2)$ and $\eta_{2,i} \sim \mathcal{N}(0, \sigma_2^2)$. The secrecy capacity of the action-dependent dirty paper wiretap channel with feedback is denoted by $\mathcal{C}_{sag}^f$, and the lower and upper bounds on $\mathcal{C}_{sag}^f$ will be given in the remainder of this section.

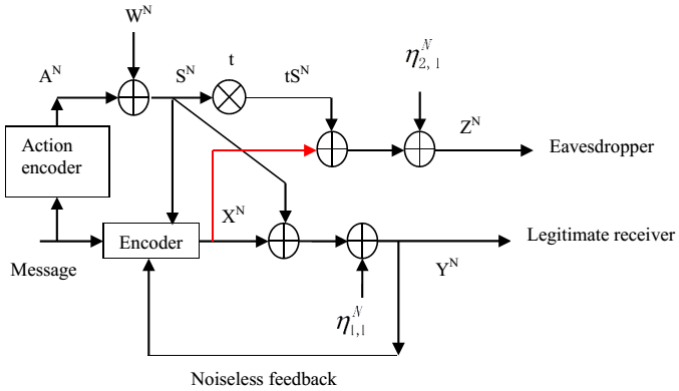

Figure 4. The action-dependent dirty paper wiretap channel with noiseless feedback.

Before we show the bounds on $\mathcal{C}_{sag}^f$, define

$$A \sim \mathcal{N}(0, P_A),\ X = \alpha A + \gamma W + G,\ U = \delta X + A + \beta W, \tag{26}$$

where $\alpha^2 P_A + \gamma^2 \sigma_w^2 \leq P$, $G \sim \mathcal{N}(0, P - \alpha^2 P_A - \gamma^2 \sigma_w^2)$ and G, A, W, η_1, η_2 are independent of each other. Note that the definitions in Equation (26) are exactly the same as those in the action-dependent dirty paper channel [13]. Further, define

$$D = P - \alpha^2 P_A - \gamma^2 \sigma_w^2, \tag{27}$$

$$E(U^2) = (1 + \delta\alpha)^2 P_A + (\delta\gamma + \beta)^2 \sigma_w^2 + \delta^2 D, \tag{28}$$

$$E(Y^2) = (\alpha + 1)^2 P_A + (\gamma + 1)^2 \sigma_w^2 + D + \sigma_1^2, \tag{29}$$

$$E(Z^2) = (\alpha + t)^2 P_A + (\gamma + t)^2 \sigma_w^2 + D + \sigma_2^2, \tag{30}$$

$$E(UY) = (1 + \delta\alpha)(1 + \alpha) P_A + (\delta\gamma + \beta)(1 + \gamma) \sigma_w^2 + \delta D, \tag{31}$$

$$E(UZ) = (1 + \delta\alpha)(t + \alpha) P_A + (\delta\gamma + \beta)(t + \gamma) \sigma_w^2 + \delta D, \tag{32}$$

$$E(YZ) = (1+\alpha)(t+\alpha)P_A + (\gamma+1)(\gamma+t)\sigma_w^2 + D, \tag{33}$$

$$L = det\begin{pmatrix} E(U^2) & E(UY) & E(UZ) \\ E(UY) & E(Y^2) & E(YZ) \\ E(UZ) & E(YZ) & E(Z^2) \end{pmatrix}. \tag{34}$$

First, substituting Equations (26) and (25) into Equation (5), our new lower bound R_{sag}^{f*} on $\mathcal{C}_{sag}^{f}$ is given by the following Theorem 3.

Theorem 3. *$\mathcal{C}_{sag}^{f} \geq R_{sag}^{f*}$, where*

$$\begin{aligned} R_{sag}^{f*} = \max_{\alpha,\gamma,\delta,\beta} \min\{&\frac{1}{2}\log(\frac{E(Y^2)E(U^2)}{E(Y^2)E(U^2)-(E(UY))^2}) - \frac{1}{2}\log(\frac{(\gamma\delta+\beta)^2\sigma_w^2+\delta^2 D}{\delta^2 D}), \\ &[\frac{1}{2}\log(2\pi e E(U^2)) - \frac{1}{2}\log(\frac{E(Z^2)E(U^2)}{E(Z^2)E(U^2)-(E(UZ))^2})]^+ + \frac{1}{2}\log(\frac{2\pi e L}{E(Z^2)E(U^2)-(E(UZ))^2})\}, \end{aligned} \tag{35}$$

and $[x]^+ = x$ for $x \geq 0$, else $[x]^+ = 0$.

Second, substituting Equations (26) and (25) into Equation (7), the secret key based lower bound R_{sag}^{f**} on $\mathcal{C}_{sag}^{f}$ is given by the following Theorem 4.

Theorem 4. *$\mathcal{C}_{sag}^{f} \geq R_{sag}^{f**}$, where*

$$\begin{aligned} R_{sag}^{f**} = \max_{\alpha,\gamma,\delta,\beta} \min\{&\frac{1}{2}\log(\frac{E(Y^2)E(U^2)}{E(Y^2)E(U^2)-(E(UY))^2}) - \frac{1}{2}\log(\frac{(\gamma\delta+\beta)^2\sigma_w^2+\delta^2 D}{\delta^2 D}), \\ &[\frac{1}{2}\log(\frac{E(Y^2)E(U^2)}{E(Y^2)E(U^2)-(E(UY))^2}) - \frac{1}{2}\log(\frac{E(Z^2)E(U^2)}{E(Z^2)E(U^2)-(E(UZ))^2})]^+ + \frac{1}{2}\log(\frac{2\pi e L}{E(Z^2)E(U^2)-(E(UZ))^2})\}, \end{aligned} \tag{36}$$

and $[x]^+ = x$ for $x \geq 0$, else $[x]^+ = 0$.

Third, substituting Equations (26) and (25) into Equation (9), the upper bound $\mathcal{C}_{sag}^{f-out}$ on $\mathcal{C}_{sag}^{f}$ is given by Theorem 5.

Theorem 5. *$\mathcal{C}_{sag}^{f} \leq \mathcal{C}_{sag}^{f-out}$, where*

$$\mathcal{C}_{sag}^{f-out} = \frac{1}{2}\log(\max_{(\alpha,\gamma):\alpha^2 P_A+\gamma^2\sigma_w^2 \leq P} \frac{\sigma_1^2+D}{\sigma_1^2} \cdot \frac{D+\sigma_w^2(\gamma+1)^2+\sigma_1^2+P_A(\alpha+1)^2}{D+\sigma_w^2(\gamma+1)^2+\sigma_1^2}). \tag{37}$$

Proof. Here note that Equation (9) is also the capacity of the action-dependent channel with noncausal state at the transmitter, and the capacity formula of its Gaussian case is be given in [13] by substituting Equations (26) and (25) into Equation (9) and maximizing the parameters δ and β. Now, directly using the Gaussian capacity formula in [13], we have Equation (37). The proof is completed. □

Finally, to show the feedback gain, we also provide a lower bound $\mathcal{C}_{sag}^{in}$ on the secrecy capacity $\mathcal{C}_{sag}$ of the action-dependent dirty paper wiretap channel (see Theorem 6).

Theorem 6. *$\mathcal{C}_{sag} \geq \mathcal{C}_{sag}^{in}$, where*

$$\begin{aligned} \mathcal{C}_{sag}^{in} = \max_{\alpha,\gamma,\delta,\beta} \min\{&\frac{1}{2}\log(\frac{E(Y^2)E(U^2)}{E(Y^2)E(U^2)-(E(UY))^2}) - \frac{1}{2}\log(\frac{(\gamma\delta+\beta)^2\sigma_w^2+\delta^2 D}{\delta^2 D}), \\ &\frac{1}{2}\log(\frac{E(Y^2)E(U^2)}{E(Y^2)E(U^2)-(E(UY))^2}) - \frac{1}{2}\log(\frac{E(Z^2)E(U^2)}{E(Z^2)E(U^2)-(E(UZ))^2})\}, \end{aligned} \tag{38}$$

Proof. In [20], a lower bound $\mathcal{C}_{sa}^{in}$ on the secrecy capacity $\mathcal{C}_{sa}$ of the discrete memoryless action-dependent wiretap channel with noncausal state at the transmitter is provided, and it is given by

$$\mathcal{C}_{sa}^{in} = \max \min\{I(U;Y) - I(U;S|A), I(U;Y) - I(U;Z), H(A|Z)\}. \tag{39}$$

Here, note that the term $H(A|Z)$ in Equation (39) holds due to the assumption that the action encoder is a deterministic function of the transmitted message. Specifically, once the eavesdropper obtains the action sequence A^N, he knows the transmitted message, hence the achievable secrecy rate cannot exceed the eavesdropper's uncertainty about A^N, i.e., $H(A|Z)$.

In this paper, we use a stochastic action encoder instead of the deterministic one in [20], which indicates that, even if the eavesdropper obtains A^N, he does not know the transmitted message due to the randomness assumption of the action encoder. Hence. the term $H(A|Z)$ no longer holds in this paper, i.e., for the action-dependent wiretap channel with noncausal state at the transmitter and stochastic action encoder, a lower bound $\mathcal{C}_{sa}^{in*}$ is given by

$$\mathcal{C}_{sa}^{in*} = \max \min\{I(U;Y) - I(U;S|A), I(U;Y) - I(U;Z)\}. \tag{40}$$

Finally, substituting Equations (26) and (25) into Equations (40), Equation (38) is obtained. The proof is completed. □

Figure 5 depicts the bounds on $\mathcal{C}_{sag}^{f}$ and the lower bound $\mathcal{C}_{sag}^{in}$ on the secrecy capacity of the action-dependent dirty paper wiretap channel for $\sigma_w^2 = P_A = 1$, $\sigma_1^2 = 1$, $\sigma_2^2 = 0.1$, $t = 0.9$ and several values of P. For this case, we see that there is no positive achievable secrecy rate $\mathcal{C}_{sag}^{in}$ of the action-dependent dirty paper wiretap channel, and feedback enhances $\mathcal{C}_{sag}^{in}$. Moreover, we see that the hybrid feedback scheme performs better than the secret key based feedback scheme, and there exists a gap between the lower and upper bounds on $\mathcal{C}_{sag}^{f}$ when P is sufficiently large.

Figure 6 depicts the bounds on $\mathcal{C}_{sag}^{f}$ and the lower bound $\mathcal{C}_{sag}^{in}$ on the secrecy capacity of the action-dependent dirty paper wiretap channel for $\sigma_w^2 = P_A = 1$, $\sigma_1^2 = 0.1$, $\sigma_2^2 = 0.1$, $t = 0.6$ and P taking values in $[0, 0.5]$. For this case, we see that feedback enhances $\mathcal{C}_{sag}^{in}$, and the hybrid feedback scheme performs better than the secret key based feedback scheme. Moreover, we see that, when P is small, the hybrid feedback scheme is optimal, i.e., its corresponding lower bound meets the upper bound, which implies that the secrecy capacity $\mathcal{C}_{sag}^{f}$ is determined for this case. Figure 7 is an extension of Figure 6 with P taking values in $[0, 50]$. We see that, when P is sufficiently large, there exists a gap between the lower and upper bounds on $\mathcal{C}_{sag}^{f}$, and eliminating this gap still has a long way to go.

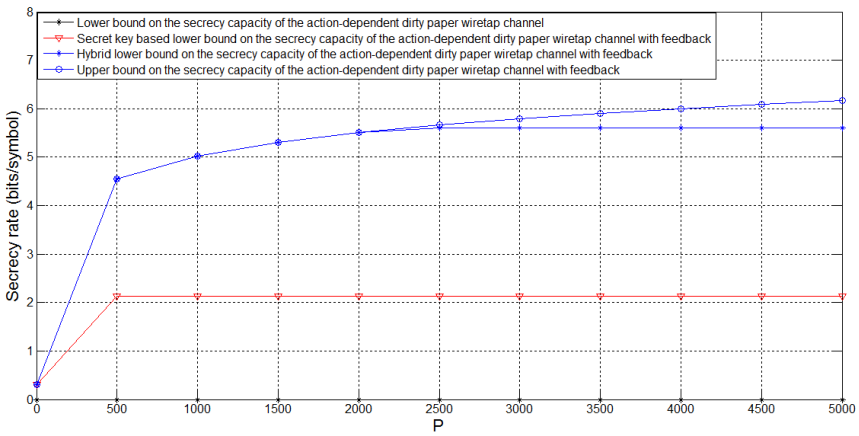

Figure 5. Comparison of the bounds on $\mathcal{C}_{sag}^{f}$ for $P_A = 1$, $\sigma_w^2 = 1$, $\sigma_1^2 = 1$, $\sigma_2^2 = 0.1$, $t = 0.9$ and P taking values in $[0, 5000]$.

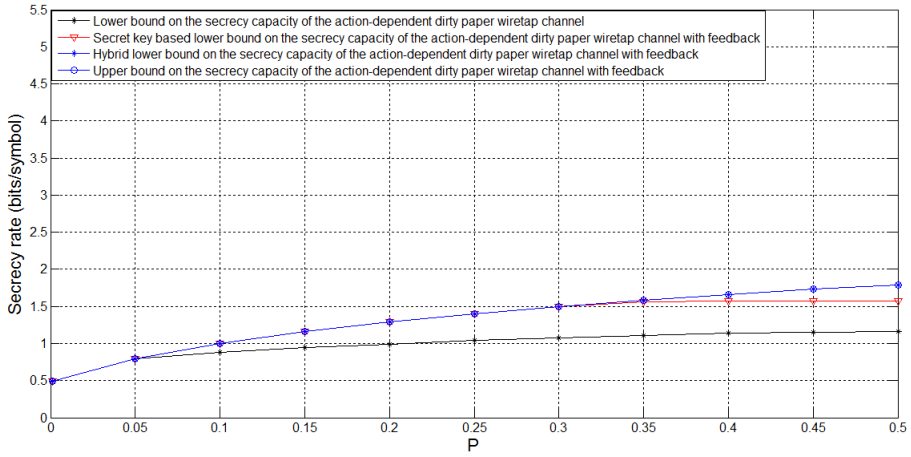

Figure 6. Comparison of the bounds on $\mathcal{C}_{sag}^{f}$ for $P_A = 1$, $\sigma_w^2 = 1$, $\sigma_1^2 = 0.1$, $\sigma_2^2 = 0.1$, $t = 0.6$ and P taking values in $[0, 0.5]$.

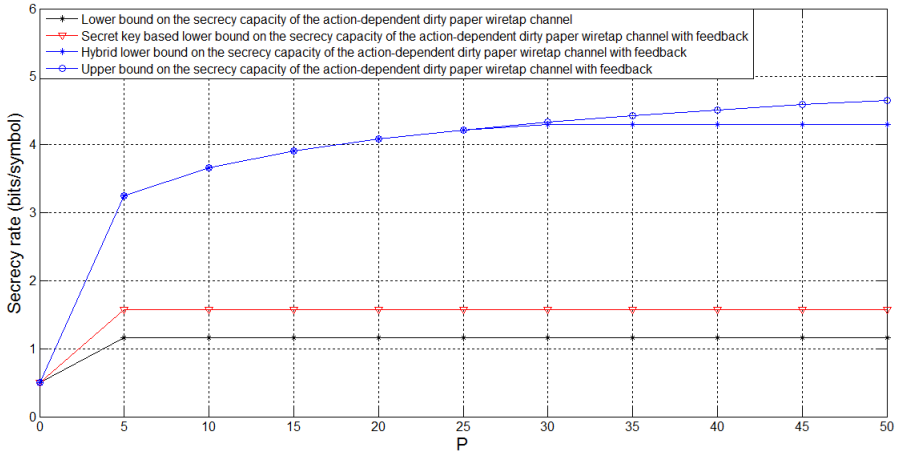

Figure 7. Comparison of the bounds on $\mathcal{C}_{sag}^{f}$ for $P_A = 1$, $\sigma_w^2 = 1$, $\sigma_1^2 = 0.1$, $\sigma_2^2 = 0.1$, $t = 0.6$ and P taking values in $[0, 50]$.

5. Conclusions

In this paper, we propose two achievable secrecy rates for the action-dependent wiretap channel with noncausal state at the transmitter and feedback, where one rate is achieved by using the already existing secret key based feedback strategy, and the other is achieved by using a hybrid feedback strategy. From a Gaussian example (also called the action-dependent dirty paper wiretap channel with feedback), we show that both feedback strategies proposed in this paper enhance the achievable secrecy rate of the action-dependent dirty paper wiretap channel, and the hybrid feedback strategy performs better than the secret key based feedback strategy. Moreover, we show that the hybrid feedback strategy is optimal for some special cases.

Author Contributions: H.Z. did the theoretical work, performed the experiments, analyzed the data and drafted the work; B.D. designed the work, performed the theoretical work, analyzed the data, interpreted the data for the work and revised the work; and L.Y. performed the theoretical work, interpreted the data for the work and revised the work. All authors approved the version to be published and agreed to be accountable for all aspects of the work in ensuring that questions related to the accuracy or integrity of any part of the work are appropriately investigated and resolved.

Acknowledgments: This work was supported by the National Natural Science Foundation of China (Grants 61671391 and U1734209), the China Scholarship Council (file No. 201807005013), and the 111 Project No. 111-2-14.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

MDPI	Multidisciplinary Digital Publishing Institute
DOAJ	Directory of open access journals
TLA	Three letter acronym
LD	linear dichroism

References

1. Ahlswede, R.; Cai, N. Transmission, identification and common randomness capacities for wire-tap channels with secure feedback from the decoder. In *General Theory of Information Transfer and Combinatorics*; Springer: Berlin/Heidelberg, Germany, 2006; pp. 258–275.
2. Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
3. Ardestanizadeh, E.; Franceschetti, M.; Javidi, T.; Kim, Y. Wiretap channel with secure rate-limited feedback. *IEEE Trans. Inf. Theory* **2009**, *55*, 5353–5361. [CrossRef]
4. Schaefer, R.F.; Khisti, A.; Poor, H.V. Secure broadcasting using independent secret keys. *IEEE Trans. Commun.* **2018**, *66*, 644–661. [CrossRef]
5. Ekrem, E.; Ulukus, S. Secrecy capacity of a class of broadcast channels with an eavesdropper. *EURASIP J. Wirel. Commun. Netw.* **2009**, *2009*, 1–29. [CrossRef]
6. Cohen, A.; Cohen, A. Wiretap channel with causal state information and secure rate-limited feedback. *IEEE Trans. Commun.* **2016**, *64*, 1192–1203. [CrossRef]
7. Dai, B.; Ma, Z.; Luo, Y. Finite state Markov wiretap channel with delayed feedback. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 746–760. [CrossRef]
8. Dai, B.; Ma, Z.; Xiao, M.; Tang, X.; Fan, P. Secure communication over finite state multiple-access wiretap channel with delayed feedback. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 723–736. [CrossRef]
9. Dai, B.; Luo, Y. An improved feedback coding scheme for the wiretap channel. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 262–271. [CrossRef]
10. Kuznetsov, N.V.; Tsybakov, B.S. Coding in memories with defective cells. *Probl. Control Inf. Theory* **1974**, *10*, 52–60.
11. Gel'fand, S.I.; Pinsker, M.S. Coding for channel with random parameters. *Probl. Control Inf. Theory* **1980**, *9*, 19–31.
12. Costa, M.H.M. Writing on dirty paper. *IEEE Trans. Inf. Theory* **1983**, *29*, 439–441. [CrossRef]
13. Weissman, T. Capacity of channels with action-dependent states. *IEEE Trans. Inf. Theory* **2010**, *56*, 5396–5411. [CrossRef]
14. Chen, Y.; Han Vinck, A.J. Wiretap channel with side information. *IEEE Trans. Inf. Theory* **2008**, *54*, 395–402. [CrossRef]
15. Dai, B.; Luo, Y. Some new results on wiretap channel with side information. *Entropy* **2012**, *14*, 1671–1702. [CrossRef]
16. El-Halabi, M.; Liu, T.; Georghiades, C.N.; Shamai, S. Secret writing on dirty paper: A deterministic view. *IEEE Trans. Inf. Theory* **2012**, *58*, 3419–3429. [CrossRef]
17. Mitrpant, C.; Han Vinck, A.J.; Luo, Y. An achievable region for the gaussian wiretap channel with side information. *IEEE Trans. Inf. Theory* **2006**, *52*, 2181–2190. [CrossRef]
18. Leung-Yan-Cheong, S.K.; Hellman, M.E. The Gaussian wire-tap channel. *IEEE Trans. Inf. Theory* **1978**, *24*, 451–456. [CrossRef]
19. Dai, B.; Ma, Z.; Fang, X. Feedback enhances the security of state-dependent degraded broadcast channels with confidential messages. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 1529–1542. [CrossRef]
20. Dai, B.; Han Vinck, A.J.; Luo, Y.; Tang, X. Wiretap channel with action-dependent channel state information. *Entropy* **2013**, *15*, 445–473. [CrossRef]

21. Dai, B.; Han Vinck, A.J.; Luo, Y. Wiretap channel in the presence of action-dependent states and noiseless feedback. *J. Appl. Math.* **2013**, *2013*, 1–17. [CrossRef]
22. El Gamal, A.; Kim, Y.H. Information measures and typicality. In *Network Information Theory*; Cambridge University Press: Cambridge, UK, 2011; pp. 17–37, ISBN 978-1-107-00873-1.