The Dirty Paper Wiretap Feedback Channel with or without Action on the State

Bin Dai*, Chong Li†, Yingbin Liang‡, Zheng Ma*, Shlomo Shamai (Shitz)§
* School of Information Science and Technology, Southwest Jiaotong University, Chengdu, 610031, China.
† Nakamoto & Turing Labs, New York, 10018, USA.
‡ Department of Electrical and Computer Engineering, The Ohio State University, Columbus, 43220, USA.
§ Department of Electrical Engineering, Technion-Israel Institute of Technology, Technion City, 32000, Israel.
daibin@home.swjtu.edu.cn, chongl@ntlabs.io, liang.889@osu.edu, zma@home.swjtu.edu.cn, sshlomo@ee.technion.ac.il.

***Abstract*—The dirty paper wiretap channel, also referred to as the Gaussian wiretap channel with noncausal state at the transmitter, is revisited. First, we determine the secrecy capacity of the dirty paper wiretap channel with noiseless feedback, where the feedback channel is from the legitimate receiver to the transmitter. Next, we obtain lower and upper bounds on the secrecy capacity of the action-dependent dirty paper wiretap channel with noiseless feedback, and show that these bounds meet for a special case. Unlike the fact that action on the state helps to enhance the capacity of the dirty paper channel with feedback, numerical results of this paper indicate that it may not help to enhance the secrecy capacity of the dirty paper wiretap channel with feedback.**

***Index Terms*—Action-dependent channel, dirty paper channel, feedback, secrecy capacity, wiretap channel.**

I. Introduction

[1] The effect of channel feedback on the physical layer security (PLS) of communication systems was initially studied in [1], where the pioneering work on the wiretap channel [2] has been re-visited by considering a noiseless feedback channel from the legitimate receiver to the transmitter. Since the transmitter also knows the legitimate receiver's channel output via the feedback channel, [1] showed that generating keys from this shared channel output and using them to encrypt the transmitted message help to increase the secrecy capacity (i.e., channel capacity with weak perfect secrecy constraint [2]) of the original channel model. Furthermore, [1] showed that this usage of feedback is optimal if the channel is physically degraded. Very recently, [3] showed that for feedback communication systems, a better usage of the feedback is to generate not only a key but also a cooperative message from it, and such a cooperative message helps the legitimate receiver to improve the decoding performance. Moreover, [4]-[5] showed that the well-known Schalkwijk-Kailath (SK) feedback scheme for the Gaussian channel [6] achieves the secrecy capacity of the Gaussian wiretap channel with noiseless feedback, which equals the capacity of the Gaussian channel without the eavesdropper.

In this paper, we revisit the Gaussian wiretap channel with noncausal state information at the transmitter [7]-[8] (which is also referred to as the dirty paper wiretap channel), and would like to answer the following three open questions:

1) In [4]-[5], it has been shown that the secrecy capacity of the Gaussian wiretap channel with feedback equals the capacity of the Gaussian channel without secrecy constraint. Does this still hold if the Gaussian wiretap channel with feedback is further corrupted by a state which is noncausally known at the transmitter, i.e., for the dirty paper wiretap channel with feedback?

2) Furthermore, does the same nature of result hold if the state is controlled by action. Namely, the secrecy capacity of the action-dependent dirty paper wiretap channel with feedback equals the capacity of the same channel model without secrecy constraint?

3) In [11], it has been shown that an action on the state helps to enhance the capacity of the dirty paper channel with noiseless feedback. Does such an action on the state also enhance the secrecy capacity of the dirty paper wiretap channel with feedback?

This paper provides the answers to the aforementioned questions. Our main contributions are summarized as follows:

1) We prove that the secrecy capacity of the dirty paper wiretap channel with feedback equals the capacity of the dirty paper channel with feedback, i.e., the secrecy requirement does not reduce the capacity. Here note that if the same channel model is not state dependent, then [4]-[5] showed that the original SK scheme achieves the secrecy capacity, which transmits the original message only at the first step, and then the transmissions after the first step combine only channel noises in the previous transmission steps. Since the information leakage occurs only in the first step of the transmission, the leakage rate vanishes as the codeword length tends to infinity. In this paper, since the channel is state-dependent, we need to adopt a modified SK scheme. Differently from the classical SK scheme, such a modified scheme transmits the original message through all transmission steps, i.e., the information leakage occurs in all transmission steps. Here the key step to show that secrecy still holds is our proof that the

[1] Acknowledgment: The work of B. Dai was supported by the National Natural Science Foundation of China under Grants 61671391, the China Scholarship Council (file No. 201807005013), and the 111 Project No.111-2-14. The work of Y. Liang was supported by U.S. NSF CCF-1801846. The work of Z. Ma was supported by U1734209. The work of S. Shamai was supported by the European Union's Horizon 2020 Research And Innovation Programme under Grant 694630.

amount of such leakage information is shrinking exponentially, and hence the information leakage rate still vanishes as the codeword length tends to infinity.

2) We prove that the secrecy capacity of the action-dependent dirty paper wiretap channel with feedback equals the capacity of the same channel under no secrecy constraint for a special case, i.e., the secrecy constraint does not reduce the capacity if the feedback channel has action-dependent state. Here note that the modified SK scheme used in 1) does not work well when the state is controlled by action. However, we find that since the state and the action are known by the transmitter, the channel input can be designed to be linear combination of the state and the action, and this leads to the equivalence of the action-dependent dirty paper wiretap channel with feedback and the Gaussian wiretap channel with feedback. Then applying the original SK scheme as used in [4]-[5] and choosing appropriate parameters of the state and the action (similar to the choice of the parameter in the dirty paper channel [10]), we obtain a lower bound on the secrecy capacity of the action-dependent dirty paper wiretap channel with feedback. Somewhat surprisingly, we find that such a scheme for the state-independent channel achieves the capacity of the action-dependent state corrupted channel for a special case.

II. Preliminaries

A. SK scheme for Gaussian wiretap channel with feedback

For the Gaussian channel with noiseless feedback, the i-th ($i \in \{1, 2, ..., N\}$) channel input and output satisfy

$$Y_i = X_i + \eta_i, \tag{2.1}$$

where X_i is the channel input subject to an average power constraint P, Y_i is the channel output, and $\eta_i \sim \mathcal{N}(0, \sigma^2)$ is the channel noise and is independent identically distributed (i.i.d.) across the time index i. The i-th time channel input X_i is a function of the message M and the channel feedback Y^{i-1}. It is well known that the capacity $\mathcal{C}^{gf}$ of the Gaussian channel with feedback equals to the capacity of the Gaussian channel, i.e.,

$$\mathcal{C}_{gf} = \frac{1}{2}\log(1 + \frac{P}{\sigma^2}). \tag{2.2}$$

It has been shown that the classical SK feedback scheme [6] achieves $\mathcal{C}_{gf}$, which is described below.

The message M takes values in the set $\mathcal{M} = \{1, 2, ..., 2^{NR}\}$. Divide the overall interval $[0.5, 0.5]$ into 2^{NR} equally spaced sub-intervals, and the center of each sub-interval is mapped to a message value in $\mathcal{M}$. Let θ be the center of the sub-interval with respect to (w.r.t.) the choosing message M. At time 1,

$$X_1 = \theta\alpha \tag{2.3}$$

is sent by the transmitter, where $\alpha = \sqrt{\frac{P+\sigma^2}{\sigma^2}}$. Upon receiving the output $Y_1 = X_1 + \eta_1$, the receiver computes

$$\hat{\theta}_1 = \frac{Y_1}{\alpha} = \theta + \frac{\eta_1}{\alpha} \tag{2.4}$$

as an estimation of θ at time 1. At time i ($i \in \{2, 3, ..., N\}$),

$$X_i = \alpha_i(\theta - \hat{\theta}_{i-1}) = -\alpha_i \frac{\sum_{j=1}^{i-1} \alpha_j \eta_j}{\sum_{j=1}^{i-1} \alpha_j^2} \tag{2.5}$$

is sent by the transmitter, where $\alpha_i = \sqrt{\frac{P}{\sigma^2}}\alpha^{i-1}$ for $i \in \{2, 3, ..., N\}$. Then the receiver receives $Y_i = X_i + \eta_i$ and computes

$$\hat{X}_i = \hat{\theta}_{i-1} + \frac{Y_i}{\alpha_i}, \tag{2.6}$$

$$\hat{\theta}_i = \frac{\sum_{j=1}^{i} \alpha_j^2 \hat{X}_j}{\sum_{j=1}^{i} \alpha_j^2} = \theta + \frac{\sum_{j=1}^{i} \alpha_j \eta_j}{\sum_{j=1}^{i} \alpha_j^2} \tag{2.7}$$

as an estimation of θ at time i. In [6], it has been shown that the decoding error probability P_e (the probability of $\hat{\theta}_N$ not belonging to the sub-interval of the choosing message M) of this proposed scheme *doubly exponentially decays to zero* for sufficiently large N and $R \leq \frac{1}{2}\log(1 + \frac{P}{\sigma^2})$.

For the Gaussian wiretap channel with noiseless feedback, the i-th ($i \in \{1, 2, ..., N\}$) channel input and outputs satisfy

$$Y_i = X_i + \eta_{1,i}, \ Z_i = X_i + \eta_{1,i} + \eta_{2,i}, \tag{2.8}$$

where X_i and Y_i are defined in the same way as those in (2.1), Z_i is the channel output at the eavesdropper, and $\eta_{1,i} \sim \mathcal{N}(0, \sigma_1^2)$, $\eta_{2,i} \sim \mathcal{N}(0, \sigma_2^2)$ are independent channel noises and are i.i.d. across the time index i. In [5], it has been shown that the above introduced SK scheme [6] also achieves the secrecy capacity of the Gaussian wiretap channel with noiseless feedback (i.e., its secrecy capacity equals $\mathcal{C}_{gf}$ in (2.2)), and the reason is given below. Since the transmitter sends the message only at time 1 (see (2.3) and (2.5)), the information leakage rate $\frac{1}{N}I(M; Z^N)$ depends only on $\frac{1}{N}I(M; Z_1)$, and it vanishes as N goes to infinity. In Section IV, we show that the SK scheme also achieves the secrecy capacity of the action-dependent dirty paper wiretap channel with feedback for a special case.

B. Dirty paper channel with noiseless feedback

For the dirty paper channel with noiseless feedback, the i-th channel input and output satisfy

$$Y_i = X_i + S_i + \eta_i, \tag{2.9}$$

where X_i is the channel input subject to an average power constraint P, and $S_i \sim \mathcal{N}(0, Q)$, $\eta_i \sim \mathcal{N}(0, \sigma^2)$ are independent Gaussian state interference and noise and are i.i.d. across the time index i ($1 \leq i \leq N$). Moreover, X_i is a function of the transmitted message M, the noncausal interference S^N and the channel feedback Y^{i-1}. It has already been shown that the feedback does not increase the capacity of the channel with noncausal state at the transmitter [13], and hence the capacity $\mathcal{C}_f$ of the dirty paper channel with noiseless feedback equals the capacity $\mathcal{C}_d$ of the dirty paper channel [10], i.e.,

$$\mathcal{C}_f = \mathcal{C}_d = \frac{1}{2}\log(1 + \frac{P}{\sigma^2}). \tag{2.10}$$

In this subsection, we introduce a feedback scheme [9] that achieves the capacity (2.10) of the dirty paper channel with noiseless feedback, which can be viewed as a variation of the SK scheme [6] introduced in the preceding subsection. The scheme is described below.

Without loss of generality, assume that the number of channel uses N equals $K+1$ and the time instant $k \in \{0, 1, ..., K\}$. At time k, the output X_k of the encoder is given by

$$X_k = aX_{k-1} - L(Y_{k-1} - S_{k-1}), \qquad (2.11)$$

where

$$a = \sqrt{1 + \frac{P}{\sigma^2}},\ L = a - \frac{1}{a}. \qquad (2.12)$$

Moreover, the k-th channel output Y_k is given by

$$Y_k = X_k + S_k + \eta_k, \qquad (2.13)$$

and at time k, the output $\hat{X}_{0,k}$ of the decoder is given by

$$\hat{X}_{0,k} = \hat{X}_{0,k-1} + a^{-k-1}LY_k. \qquad (2.14)$$

The transmitted message M is uniformly drawn from the alphabet set

$$\mathcal{M} = \{1, 2, ..., a^{(K+1)(1-\epsilon)}\}, \qquad (2.15)$$

where ϵ is an arbitrary small positive number. Similarly to the definition of the transmitted message in the SK scheme, we equally divide the overall interval

$$[-\sqrt{P}(1 + \frac{1}{a^{K+1}-1}),\ \sqrt{P}(1 + \frac{1}{a^{K+1}-1})] \qquad (2.16)$$

into $a^{(K+1)(1-\epsilon)}$ sub-intervals, and the center of each sub-interval corresponds to a specific value in $\{1, 2, ..., a^{(K+1)(1-\epsilon)}\}$. To start the encoding procedure, define $s_{-1} = y_{-1} = \hat{x}_{0,-1} = 0$ (s_{-1}, y_{-1} and $\hat{x}_{0,-1}$ are the values of S_{-1}, Y_{-1} and $\hat{X}_{0,-1}$, respectively), and define $x_{-1} = \frac{M+M^*}{a}$, where M^* is given by

$$M^* = -\frac{\sum_{j=0}^{K} a^{-j-1}Ls_j}{1 - a^{-K-2}}, \qquad (2.17)$$

and s_j is the value of S_j. For the decoder, at the end of time K, an estimation $\bar{M}_K$ defined by

$$\bar{M}_K = \frac{\hat{X}_{0,K}}{1 - a^{-2K-2}} \qquad (2.18)$$

is obtained, and then the receiver finds the closest sub-interval center to $\bar{M}_K$ and obtains the decoded message $\hat{M}$. The decoding error is defined as $Pr\{\hat{M} \neq M\}$.

Let W_M be the center of the sub-interval with respect to (w.r.t.) the choosing message M. The above definitions imply that the k-th channel input X_k can be expressed as

$$X_k = a^{-k}(W_M + M^*) - \sum_{j=0}^{k-1} a^{-k+1+j}L\eta_j. \qquad (2.19)$$

Finally, by combining (2.19) and the above definitions, [9] proves that the average channel input power of X_k tends to P as k tends to infinity, the transmission rate $R = \frac{\log|\mathcal{M}|}{K+1}$ tends to $\mathcal{C}_f = \frac{1}{2}\log(1 + \frac{P}{\sigma^2})$ as ϵ tends to zero, and the decoding error $Pr\{\hat{M} \neq M\}$ *doubly exponentially decays to zero* as K tends to infinity.

III. The dirty paper wiretap channel with noiseless feedback

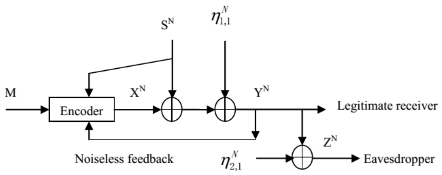

Fig. 1: The dirty paper wiretap channel with feedback.

In this section, we study the dirty paper wiretap channel with noiseless feedback, see Figure 1. The i-th channel inputs and outputs satisfy

$$Y_i = X_i + S_i + \eta_{1,i},\ Z_i = Y_i + \eta_{2,i}, \qquad (3.20)$$

where X_i, S_i are defined in the same way as those in Subsection II-B, Y_i and Z_i are channel outputs respectively at the legitimate receiver and the eavesdropper, and $\eta_{1,i} \sim \mathcal{N}(0, \sigma_1^2)$, $\eta_{2,i} \sim \mathcal{N}(0, \sigma_2^2)$ are the channel noises. The following Theorem 1 shows the secrecy capacity $\mathcal{C}_{sf}$ of the model of Figure 1 equals $\mathcal{C}_f$ (the capacity of the dirty paper channel with noiseless feedback).

Theorem 1: The secrecy capacity $\mathcal{C}_{sf}$ of the dirty paper wiretap channel with noiseless feedback is given by $\mathcal{C}_{sf} = \frac{1}{2}\log(1 + \frac{P}{\sigma_1^2})$.

Proof: First, note that the secrecy capacity $\mathcal{C}_{sf}$ cannot exceed the capacity of the model of Figure 1 without the eavesdropper. Hence, we have $\mathcal{C}_{sf} \leq \mathcal{C}_f = \frac{1}{2}\log(1 + \frac{P}{\sigma_1^2})$. Next, we show that the secrecy rate $\frac{1}{2}\log(1 + \frac{P}{\sigma_1^2})$ can be achieved by the previously proposed feedback coding scheme for the dirty paper channel with feedback, and the detail is given below.

In Subsection II-B, we have shown that the proposed feedback scheme achieves the rate $\frac{1}{2}\log(1+\frac{P}{\sigma_1^2})$ with decoding error probability doubly exponentially decaying to zero as codeword length tending to infinity. Now it remains to show that the eavesdropper's equivocation rate $\Delta = \frac{1}{N}H(M|Z^N) \geq \frac{1}{2}\log(1 + \frac{P}{\sigma_1^2}) - \epsilon^{'}$, where $\epsilon^{'}$ is an arbitrary small positive number. Since

$$\begin{aligned}
\Delta = \frac{1}{N}H(M|Z^N) &\overset{(1)}{=} \frac{1}{K+1}H(W_M|Z_0, ..., Z_K) \\
&\overset{(2)}{=} \frac{1}{K+1}H(W_M|W_M + M^* + S_0 + \eta_{1,0} + \eta_{2,0}, ..., \\
&a^{-K}(W_M + M^*) - \sum_{j=0}^{K-1}(a^{-K+1+j}L\eta_{1,j}) + S_K \\
&+\eta_{1,K} + \eta_{2,K}) \\
&\overset{(3)}{\geq} \frac{1}{K+1}H(W_M|W_M + \eta_{2,0}, a^{-1}M + \eta_{2,1}, ...,
\end{aligned}$$

$$
\begin{aligned}
&a^{-K}W_M+\eta_{2,K},S_0,...,S_K,\eta_{1,0},...,\eta_{1,K})\\
&\overset{(4)}{=}\frac{1}{K+1}H(W_M|W_M+\eta_{2,0},a^{-1}W_M+\eta_{2,1},...,\\
&a^{-K}W_M+\eta_{2,K})\\
&=\frac{1}{K+1}(h(W_M,\eta_{2,0},\eta_{2,1},...,\eta_{2,K})-h(W_M\\
&+\eta_{2,0},a^{-1}W_M+\eta_{2,1},...,a^{-K}W_M+\eta_{2,K}))\\
&\overset{(5)}{\geq}\frac{1}{K+1}(H(W_M)+\sum_{i=0}^{K}h(\eta_{2,i})\\
&-\sum_{i=0}^{K}h(a^{-i}W_M+\eta_{2,i}))\\
&\overset{(6)}{\geq}(1-\epsilon)\log(a)+\frac{1}{2(K+1)}\log(2\pi e\sigma_2^2)^{K+1}\\
&-\frac{1}{2(K+1)}\sum_{i=0}^{K}\log(2\pi e(\frac{P}{3}a^{-2i}+\sigma_2^2))\\
&=(1-\epsilon)\log(a)+\frac{1}{2(K+1)}\log(2\pi e\sigma_2^2)^{K+1}\\
&-\frac{1}{2(K+1)}\log((2\pi e)^{K+1}\prod_{i=0}^{K}(\frac{P}{3}a^{-2i}+\sigma_2^2))\\
&=(1-\epsilon)\log(a)+\frac{1}{2(K+1)}\log\left(\frac{1}{\prod_{i=0}^{K}(1+\frac{P}{3}\frac{a^{-2i}}{\sigma_2^2})}\right)\\
&=(1-\epsilon)\log(a)-\frac{1}{2(K+1)}\sum_{i=0}^{K}\log(1+\frac{P}{3}\frac{a^{-2i}}{\sigma_2^2})\\
&\overset{(7)}{\geq}(1-\epsilon)\log(a)-\frac{1}{2(K+1)}\frac{1}{\ln 2}\sum_{i=0}^{K}\frac{P}{3}\frac{a^{-2i}}{\sigma_2^2}\\
&=(1-\epsilon)\log(a)-\frac{1}{2(K+1)\ln 2}\frac{P}{3\sigma_2^2}\frac{1-a^{-2K-2}}{1-a^{-2}}\\
&\overset{(8)}{=}(1-\epsilon)\frac{1}{2}\log(1+\frac{P}{\sigma_1^2})-\frac{1}{2(K+1)\ln 2}\frac{P}{3\sigma_2^2}\cdot\\
&\frac{1-a^{-2K-2}}{1-a^{-2}},
\end{aligned}
\tag{3.21}
$$

where (1) follows from the fact that M can be denoted by W_M, and the definition $Z^N=(Z_0,...,Z_K)$, (2) follows from (3.20), (2.19) and (2.17), (3) follows from conditions reduce entropy and the fact that M^* is determined by $(S_0,...,S_K)$ (see (2.17)), (4) follows from the fact that S_0,...,S_K, $\eta_{1,0}$,...,$\eta_{1,K}$ are independent of W_M, $W_M+\eta_{2,0}$, $a^{-1}W_M+\eta_{2,1}$,...,$a^{-K}W_M+\eta_{2,K}$, (5) follows from the fact that $\eta_{2,0}$, $\eta_{2,1}$,...,$\eta_{2,K}$ are i.i.d. random variables, (6) follows from (2.15), $\eta_{2,i}\sim\mathcal{N}(0,\sigma_2^2)$, the fact that the variance of W_M equals $\frac{P}{3}$ as K tends to infinity, and the fact that W_M is independent of $\eta_{2,i}$, which implies

$$h(a^{-i}W_M+\eta_{2,i})\leq\frac{1}{2}\log(2\pi e(\frac{P}{3}a^{-2i}+\sigma_2^2)),\tag{3.22}$$

(7) follows from the inequality $\ln(1+x)\leq x$ for $x\geq 0$, and (8) follows from (2.12). Finally, note that when K tends to infinity, $\frac{1}{2(K+1)\ln 2}\frac{P}{3\sigma_2^2}\frac{1-a^{-2K-2}}{1-a^{-2}}$ in (3.21) tends to zero. Hence choosing sufficiently large K, we have $\Delta\geq\frac{1}{2}\log(1+\frac{P}{\sigma_1^2})-\epsilon^{'}$. The proof of Theorem 1 is completed. ■

Remark 1: From (2.19), we see that the original message is sent through all time instants, which leads to the information leakage occurs in all transmission steps. However, (3.21) shows that such an information leakage vanishes as the number of channel uses tends to infinity, which finally leads to the fact that the secrecy requirement does not reduce the channel capacity.

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

In this section, we study the action-dependent dirty paper wiretap channel with noiseless feedback, see Figure 2. This feedback model is defined the same as that introduced in Section III, except that the i-th ($i\in\{1,2,...,N\}$) channel state $S_i=A_i+W_i$, where A_i is the output of an action encoder subject to an average power constraint P_A, and W_i, $\eta_{1,i}$, $\eta_{2,i}$ are independent Gaussian noises and are i.i.d. across the time index i. The secrecy capacity of the action-dependent dirty paper wiretap channel with noiseless feedback is denoted by $\mathcal{C}_{sag}^{f}$. In the remainder of this section, we will show $\mathcal{C}_{sag}^{f}$ is upper bounded by the capacity $\mathcal{C}_{ag}$ of the action-dependent dirty paper channel without feedback [12], and the upper bound $\mathcal{C}_{ag}$ is capacity-achieving for a special case.

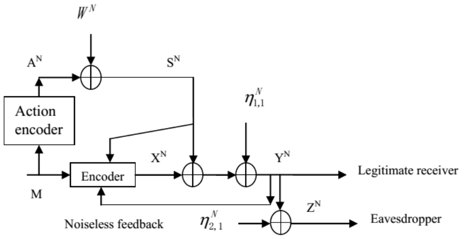

Fig. 2: The action-dependent dirty paper wiretap channel with noiseless feedback.

First, recall that the capacity $\mathcal{C}_{ag}$ of the action-dependent dirty paper channel is given by

$$
\begin{aligned}
\mathcal{C}_{ag}=&\max_{(\rho_1,\rho_2):\rho_1^2+\rho_2^2\leq 1}\frac{1}{2}\log\left(1+\frac{P(1-\rho_1^2-\rho_2^2)}{\sigma_1^2}\right)\\
&+\frac{1}{2}\log\left(1+\frac{(\sqrt{P_A}+\rho_2\sqrt{P})^2}{P(1-\rho_1^2-\rho_2^2)+(\sigma_w+\rho_1\sqrt{P})^2+\sigma_1^2}\right),
\end{aligned}
\tag{4.23}
$$

where $-1\leq\rho_1\leq 0$ and $0\leq\rho_2\leq 1$. The following Theorem 2 characterizes the secrecy capacity $\mathcal{C}_{sag}^{f}$ for one regime and the bounds on $\mathcal{C}_{sag}^{f}$ for the remaining parameter regime based on (4.23).

Theorem 2: Suppose that the pair (ρ_1^*,ρ_2^*) achieves $\mathcal{C}_{ag}$, and define $L=\frac{1}{2}\log\left(1+\frac{(\sqrt{P_A}+\rho_2^*\sqrt{P})^2}{P(1-\rho_1^{*2}-\rho_2^{*2})+(\sigma_w+\rho_1^*\sqrt{P})^2+\sigma_1^2}\right)$. If $\rho_1^{*2}+\rho_2^{*2}=1$, then $\mathcal{C}_{sag}^{f}=\mathcal{C}_{ag}=L$. Otherwise, if $\rho_1^{*2}+\rho_2^{*2}<1$, then $L\leq\mathcal{C}_{sag}^{f}\leq\mathcal{C}_{ag}=L+\frac{1}{2}\log\left(1+\frac{P(1-\rho_1^{*2}-\rho_2^{*2})}{\sigma_1^2}\right)$.

Remark 2: From Theorem 2, we conclude that if $\mathcal{C}_{ag}$ is achieved at the boundary of the constraint condition, i.e., $\rho_1^{*2} + \rho_2^{*2} = 1$, then $\mathcal{C}_{sag}^f$ equals $\mathcal{C}_{ag}$, and this implies that the secrecy constraint does not reduce the capacity if the feedback channel model has action-dependent state. Otherwise, if $\mathcal{C}_{ag}$ is achieved with $\rho_1^{*2} + \rho_2^{*2} < 1$, then $\mathcal{C}_{ag}$ serves as an upper bound on $\mathcal{C}_{sag}^f$, and part of $\mathcal{C}_{ag}$ (i.e.,$\frac{1}{2}\log\left(1+\frac{(\sqrt{P_A}+\rho_2^*\sqrt{P})^2}{P(1-\rho_1^{*2}-\rho_2^{*2})+(\sigma_w+\rho_1^*\sqrt{P})^2+\sigma_1^2}\right)$) serves as a lower bound on $\mathcal{C}_{sag}^f$.

Proof: Since feedback does not increase the capacity $\mathcal{C}_{ag}$ of the action-dependent dirty paper channel [11], and $\mathcal{C}_{sag}^f$ cannot exceed the capacity of the action-dependent dirty paper channel with feedback, we have $\mathcal{C}_{sag}^f \leq \mathcal{C}_{ag}$. Next, for the case that $\rho_1^{*2} + \rho_2^{*2} = 1$, construct $X = \frac{\rho_2^*\sqrt{P}}{\sqrt{P_A}}A + \frac{\rho_1^*\sqrt{P}}{\sigma_w}W$. Substituting the above definition of X and $S = A + W$ into $Y = X + S + \eta_1$ and $Z = X + S + \eta_1 + \eta_2$, we have $Y = (1+\frac{\rho_2^*\sqrt{P}}{\sqrt{P_A}})A + (1+\frac{\rho_1^*\sqrt{P}}{\sigma_w})W + \eta_1$, and $Z = Y + \eta_2$, which indicates that the action-dependent GWTC-N-CSIT with feedback is equivalent to the Gaussian wiretap channel with feedback shown in Subsection II-A. To be specific, the equivalent model has input $X^{'} = (1+\frac{\rho_2^*\sqrt{P}}{\sqrt{P_A}})A$ with power constraint $P^{'} = (1+\frac{\rho_2^*\sqrt{P}}{\sqrt{P_A}})^2 P_A$, has legitimate receiver's channel noise $\eta_1^{'} = (1+\frac{\rho_1^*\sqrt{P}}{\sigma_w})W + \eta_1$ satisfying $\eta_1^{'} \sim \mathcal{N}(0, \sigma_1^{'2} = (1+\frac{\rho_1^*\sqrt{P}}{\sigma_w})^2\sigma_w^2 + \sigma_1^2)$, and has eavesdropper's channel noise $\eta_2^{'} = \eta_2$ satisfying $\eta_2^{'} \sim \mathcal{N}(0, \sigma_2^2)$. Defining $\alpha = \sqrt{\frac{P' + \sigma_1^{'2}}{\sigma_1^{'2}}}$ and $\alpha_i = \sqrt{\frac{P'}{\sigma_1^{'2}}}\alpha^{i-1}$ for $i \in \{2, 3, ..., N\}$, and along the lines of the SK scheme introduced in Subsection II-A, the rate $R = \frac{1}{2}\log\left(1+\frac{P^{'}}{\sigma_1^{'2}}\right) = \frac{1}{2}\log\left(1+\frac{(\sqrt{P_A}+\rho_2^*\sqrt{P})^2}{(\sigma_w+\rho_1^*\sqrt{P})^2+\sigma_1^2}\right) = \mathcal{C}_{ag}$ is achievable with weak perfect secrecy.

Similarly, if $\mathcal{C}_{ag}$ is achieved with $\rho_1^{*2} + \rho_2^{*2} < 1$, construct $X = \frac{\rho_2^*\sqrt{P}}{\sqrt{P_A}}A + \frac{\rho_1^*\sqrt{P}}{\sigma_w}W + G$, where G is randomly generated according to $G \sim \mathcal{N}(0, P(1-\rho_1^{*2}-\rho_2^{*2}))$ and it is independent of A and W. Substituting $X = \frac{\rho_2^*\sqrt{P}}{\sqrt{P_A}}A + \frac{\rho_1^*\sqrt{P}}{\sigma_w}W + G$ and $S = A + W$ into $Y = X + S + \eta_1$ and $Z = X + S + \eta_1 + \eta_2$, we have $Y = (1+\frac{\rho_2^*\sqrt{P}}{\sqrt{P_A}})A + (1+\frac{\rho_1^*\sqrt{P}}{\sigma_w})W + G + \eta_1$, and $Z = Y + \eta_2$, which implies that the action-dependent GWTC-N-CSIT with feedback is equivalent to the Gaussian wiretap channel with feedback. The equivalent model has input $X^{''} = (1+\frac{\rho_2^*\sqrt{P}}{\sqrt{P_A}})A$ with power constraint $P^{''} = (1+\frac{\rho_2^*\sqrt{P}}{\sqrt{P_A}})^2 P_A$, has legitimate receiver's channel noise $\eta_1^{''} = (1+\frac{\rho_1^*\sqrt{P}}{\sigma_w})W + G + \eta_1$ satisfying $\eta_1^{''} \sim \mathcal{N}(0, \sigma_1^{''2} = (1+\frac{\rho_1^*\sqrt{P}}{\sigma_w})^2\sigma_w^2 + P(1-\rho_1^{*2}-\rho_2^{*2}) + \sigma_1^2)$, and has eavesdropper's channel noise $\eta_2^{''} = \eta_2$ satisfying $\eta_2^{''} \sim \mathcal{N}(0, \sigma_2^2)$. Defining $\alpha = \sqrt{\frac{P'' + \sigma_1^{''2}}{\sigma_1^{''2}}}$ and $\alpha_i = \sqrt{\frac{P''}{\sigma_1^{''2}}}\alpha^{i-1}$ for $i \in \{2, 3, ..., N\}$, and along the lines of the SK scheme introduced in Subsection II-A, the rate $R = \frac{1}{2}\log(1+\frac{P^{''}}{\sigma_1^{''2}}) = \frac{1}{2}\log\left(1+\frac{(\sqrt{P_A}+\rho_2^*\sqrt{P})^2}{P(1-\rho_1^{*2}-\rho_2^{*2})+(\sigma_w+\rho_1^*\sqrt{P})^2+\sigma_1^2}\right)$ is achievable with weak perfect secrecy. The proof is completed. ■

The following Figure 3 plots the bounds on $\mathcal{C}_{sag}^f$, the secrecy capacity of the dirty paper wiretap channel with noiseless feedback and the already existing lower bound on the secrecy capacity of the dirty paper wiretap channel [7]. From Figure 3, we see that the achievable secrecy rate for the dirty paper wiretap channel is enhanced by action on the state and channel feedback. Moreover, as we see, when the power P is small, action on the state further increases the secrecy capacity of the dirty paper wiretap channel with feedback. However, this may not hold in general.

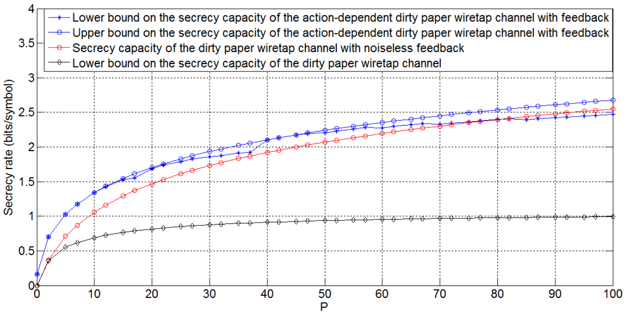

Fig. 3: Action versus non-action for $P_A = 1$, $\sigma_w^2 = 1$, $Q = P_A + \sigma_w^2 = 2$, $\sigma_1^2 = 3$, $\sigma_2^2 = 10$ and P taking values in $[0, 100]$.

REFERENCES

[1] R. Ahlswede, N. Cai, "Transmission, identification and common randomness capacities for wire-tap channels with secure feedback from the decoder," book chapter in *General Theory of Information Transfer and Combinatorics*, LNCS 4123, pp. 258-275, Berlin: Springer-Verlag, 2006.

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

[3] B. Dai, Y. Luo, "An improved feedback coding scheme for the wiretap channel," *IEEE Trans. Inf. Forensics and Security*, vol. 14, No. 1, pp. 262-271, 2019.

[4] C. Li, Y. Liang, H. V. Poor, S. Shamai, "A coding scheme for colored Gaussian wiretap channels with feedback," *IEEE International Symposium on Information Theory (ISIT)*, pp. 131-135, 2018.

[5] D. Gunduz, D. R. Brown and H. V. Poor, "Secret communication with feedback," *International Symposium on Information Theory and Its Applications, ISITA 2008*, pp. 1-6, 2008.

[6] J. P. M. Schalkwijk and T. Kailath, "A coding scheme for additive noise channels with feedback. part I: No bandwidth constraint," *IEEE Trans. Inf. Theory*, vol. 12, pp. 172-182, 1966.

[7] C. Mitrpant, A. J. Han Vinck and Y. Luo, "An achievable region for the Gaussian wiretap channel with side information," *IEEE Trans. Inf. Theory*, vol. IT-52, no. 5, pp. 2181-2190, 2006.

[8] M. El-Halabi, T. Liu , C. N. Georghiades, S. Shamai, " Secret writing on dirty paper: A deterministic view," *IEEE Trans. Inf. Theory*, vol. 58, no. 6, pp. 3419-3429, 2012.

[9] J. Liu, N. Elia, "Writing on dirty paper with feedback," *Communications in Information and Systems*, vol. 5, no. 4, pp. 401-422, 2005.

[10] M. H. M. Costa, "Writing on dirty paper," *IEEE Trans. Inf. Theory*, vol. 29, no. 3, pp. 439-441, 1983.

[11] T. Weissman, "Capacity of channels with action-dependent states," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5396-5411, 2010.

[12] L. Dikstein, H. H. Permuter, S. Shamai, "MAC with action-dependent state information at one encoder," *IEEE Trans. Inf. Theory*, vol. 61, no. 1, pp. 173-188, 2015.

[13] G. Keshet, Y. Steinberg and N. Merhav, "Channel coding in the presence of side information," *Foundations and Trends in Communications and Information Theory*, vol. 4, no. 6, 2007.