Impact of Action-Dependent State and Channel Feedback on Gaussian Wiretap Channels

Bin Dai, Chong Li, *Member, IEEE*, Yingbin Liang, *Senior Member, IEEE*, Zheng Ma, *Member, IEEE*, and Shlomo Shamai (Shitz), *Life Fellow, IEEE*

***Abstract*— We investigate the state-dependent Gaussian wiretap channel with noncausal channel state information at the transmitter (GWTC-N-CSIT), and explore whether three strategies (i.e., taking action on the state, legitimate receiver's channel output feedback, and combining the former two strategies together) help to enhance the secrecy capacity of the GWTC-N-CSIT. To be specific, we first determine the secrecy capacity of the GWTC-N-CSIT with noiseless feedback. Next, we derive lower and upper bounds on the secrecy capacity of the GWTC-N-CSIT with action-dependent state. Finally, we derive lower and upper bounds on the secrecy capacity of the GWTC-N-CSIT with both action-dependent state and noiseless feedback, and show that these bounds meet for a special case. Numerical results of this paper indicate that all three strategies enhance the secrecy capacity of the GWTC-N-CSIT. The study of this paper offers new options for enhancing the secrecy rates of the state-dependent wiretap channel models.**

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

I. Introduction

SHANNON first investigated the capacity of the channel in the presence of state by considering a state-dependent discrete memoryless channel (DMC) with causal state information available at the transmitter, and fully determined the capacity of such a channel model in [1]. Subsequently, [2] studied the state-dependent channel with noncausal state information at the transmitter (also referred to as the C-N-CSIT), and the capacity was established in [3]. [4] further pointed out that noiseless channel feedback does not increase the capacities of [1] and [3].

The Gaussian case of the model in [3], which is known as the dirty paper channel, was studied in [5], and was shown that the capacity of the dirty paper channel equals the capacity of the same channel model without the state interference. [6] further pointed out that the noiseless channel feedback does not increase the capacity of the dirty paper channel [5]. Moreover, the Gaussian case of the model in [1], which is known as the dirty tape channel, was studied in [7]–[9]. The capacity of the dirty tape channel remains open and is only known for some special cases. In all the aforementioned work [1]–[9], the channel state was assumed to be independent of the transmitted message. In [10], the models of [1] and [3] were revisited by considering the case that the transmitter can take action on the channel state (i.e., the state is correlated with the transmitted message). Such models are known as the action-dependent channel with noncausal or causal states, and their capacities were determined in [10]. Furthermore, [10] showed that for the Gaussian case of the action-dependent channel with noncausal states (also referred to as the action-dependent dirty paper channel), taking action on the state increases the capacity compared to the action-independent channel, i.e., the dirty paper channel. The capacity of the action-dependent dirty paper channel was fully determined in [11].

As a natural extension of the above work, the study of the state-dependent channel under additional secrecy requirements receives much attention recently. Specifically, [14] and [15] studied the discrete memoryless state-dependent wiretap channel with noncausal state at the transmitter (also referred to as the WTC-N-CSIT), and proposed lower and upper bounds on its secrecy capacity (i.e., channel capacity with the perfect secrecy constraint). [16]–[18] proposed lower and upper bounds on secrecy capacities of the discrete memoryless state-dependent wiretap channel with causal state at the transmitter (or at both the transmitter and the legitimate receiver), and showed that these bounds meet for the case that the eavesdropper's received signal is a degraded version

Manuscript received May 4, 2019; revised November 26, 2019; accepted January 2, 2020. Date of publication January 20, 2020; date of current version May 20, 2020. The work of Bin Dai was supported in part by the National Natural Science Foundation of China under Grant 61671391, in part by the China Scholarship Council under Grant 201807005013, and in part by the 111 Project under Grant 111-2-14. The work of Yingbin Liang was supported by U.S. NSF under Grant CCF-1801846. The work of Zheng Ma was supported in part by the National Natural Science Foundation of China under Grant U1734209 and Grant U1709219, in part by the Key Project of Sichuan Province under Grant 2017SZYZF0002, and in part by the Marie Curie Fellowship under Grant 796426. The work of Shlomo Shamai (Shitz) was supported by the European Union's Horizon 2020 Research and Innovation Programme under Grant 694630. This article was presented in part at the 2019 IEEE International Symposium on Information Theory (ISIT) and in part at the 2019 IEEE International Conference on Communications (ICC).

Bin Dai and Zheng Ma are with the School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, China (e-mail: daibin@home.swjtu.edu.cn; zma@home.swjtu.edu.cn).

Chong Li is with Nakamoto & Turing Labs, New York, NY 10018 USA (e-mail: chongl@ntlabs.io).

Yingbin Liang is with the Department of Electrical and Computer Engineering, The Ohio State University, Columbus, OH 43220 USA (e-mail: liang.889@osu.edu).

Shlomo Shamai (Shitz) is with the Department of Electrical Engineering, Technion-Israel Institute of Technology, Technion 32000, Israel (e-mail: sshlomo@ee.technion.ac.il).

Communicated by S. Watanabe, Associate Editor for Shannon Theory.

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2020.2967757

0018-9448 © 2020 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: Technion Israel Institute of Technology. Downloaded on May 24,2020 at 05:32:54 UTC from IEEE Xplore. Restrictions apply.

of the legitimate receiver's. For the Gaussian case of [14] (also referred to as the GWTC-N-CSIT), [19] showed that the state interference non-causally known by the transmitter helps to increase the secrecy capacity of the Gaussian wiretap channel [20]. Furthermore, [21] extended the models of [14] and [19] to a broadcast situation, and proposed inner and outer bounds on the secrecy capacity region of such models.

The above works mainly adopted the framework and tools in [12], [13] for establishing the secrecy rate/capacity. More recently, there has been a lot of attention on developing communication schemes to enhance the secrecy rates (i.e., reliable transmission rates subject to the perfect secrecy constraint). Artificial noise aided cooperative jamming [22]–[24] and channel feedback have been proven to be useful tools to enhance the secrecy rates of various channel models with eavesdropper(s). However, note that in some circumstances, such as Internet of Things (IoT), the artificial noise aided cooperative jamming is not a good choice due to the energy constraint of the devices [25], and hence the channel feedback is of particular interest for such circumstances. The effect of channel feedback on the physical layer security (PLS) of communication systems was initially studied in [26], where the pioneering work on the wiretap channel [12] was 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, [26] showed that generating keys from this shared channel output and using them to encrypt the transmitted messages help to increase the secrecy capacity of the original channel model. Furthermore, [26] showed that such a secret key based feedback scheme is optimal if the channel is physically degraded. In recognition of this, [27] further pointed out that if the noiseless feedback channel can be used to transmit anything as the legitimate parties wish, the best choice of the legitimate parties is to send pure random bits (secret key) over the feedback channel. Subsequently, [28] extended the work of [27] 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 increase the achievable secrecy rate region of the broadcast wiretap channel [29], [30]. Other related works in the PLS of feedback communication systems include [31]–[34] and [35], where channel state information (CSI) are introduced into various feedback channel models in the presence of an eavesdropper.

Very recently, [36] 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. Later, [37] and [38] further applied the feedback scheme of [36] to the state-dependent wiretap channel with and without action encoder, respectively. Moreover, [39] and [44] showed that the secrecy capacity of the Gaussian wiretap channel with noiseless feedback equals the capacity of the same channel model without the secrecy constraint, and it can be achieved by the classical Schalkwijk-Kailath (SK) feedback scheme for the Gaussian channel [40]. Furthermore, [41] provided a generalized SK feedback scheme for the colored Gaussian wiretap channel, and showed that this scheme also achieves the capacity of the same channel model without the secrecy constraint.

In this paper, we study the Gaussian wiretap channel that is both state-dependent with noncausal state information at the transmitter and with feedback, and would like to answer the following three open questions:

1) In [39], 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 GWTC-N-CSIT with feedback?

2) Furthermore, does the same nature of result hold if the state is further controlled by action. Namely, whether the secrecy capacity of the action-dependent GWTC-N-CSIT with feedback equals the capacity of the same channel model without secrecy constraint?

3) In [10] and [11], it has been shown that an action on the state helps to enhance the capacity of the dirty paper channel. Does such an action on the state also enhance the already existing achievable secrecy rate of the GWTC-N-CSIT [19]?

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

1) We prove that the secrecy capacity of the GWTC-N-CSIT 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 [39] showed that the original SK scheme achieves the secrecy capacity, which transmits the original message only at the first transmission, and then the transmissions after the first one combine only channel noises in the previous transmissions. Since the information leakage occurs only in the first 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 transmissions so that the information leakage occurs in all transmissions. Here the major technical step to show that the secrecy still holds lies in establishing that the amount of 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 GWTC-N-CSIT with feedback equals the capacity of the same channel under no secrecy constraint for a special case, in which case 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 perform well when the state is controlled by action. Alternatively, 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 GWTC-N-CSIT with feedback and the Gaussian wiretap channel with feedback. Then applying the original SK

Authorized licensed use limited to: Technion Israel Institute of Technology. Downloaded on May 24,2020 at 05:32:54 UTC from IEEE Xplore. Restrictions apply.

scheme as used in [39] and choosing appropriate parameters of the state and the action (similar to the choice of the parameter in the dirty paper channel [5]), we obtain a lower bound on the secrecy capacity of the action-dependent GWTC-N-CSIT 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. Moreover, we show that our new lower bound is tighter than the already existing secret key based lower bound [37] when the eavesdropper's channel noise variance is sufficiently small.

3) We provide lower and upper bounds on the secrecy capacity of the action-dependent GWTC-N-CSIT. To be specific, first, we derive bounds on the secrecy capacity of the discrete memoryless action-dependent wiretap channel with noncausal state information at the transmitter, where the lower bound is constructed by combining the coding scheme of [10] with the random binning scheme of the wiretap channel [12], and the upper bounds are constructed by applying the degradedness assumption and the standard converse derivation of [13] into the converse of [10]. Next, we further derive two lower bounds on the secrecy capacity of the action-dependent GWTC-N-CSIT by respectively introducing two different ways of choosing the distributions of the random variables to the corresponding discrete memoryless lower bound (see [10] and [11]), where one way only obtains a lower bound on the capacity of the action-dependent dirty paper channel [10], and the other way achieves the capacity of the action-dependent dirty paper channel [11]. Somewhat surprisingly, numerical results show that the former way may help to obtain a tighter lower bound on the secrecy capacity of the action-dependent GWTC-N-CSIT than the latter one. Moreover, numerical results indicate that the lower bounds for the action-dependent GWTC-N-CSIT meet the upper bound when the transmitting power is sufficiently large, and action on the state increases the secrecy capacity of the GWTC-N-CSIT [19].

To get a better understanding of the contribution of this paper and the related works studied in the literature, the following Table I summarizes the capacity results on the channels with noncausal state information at the transmitter, and with or without action, feedback and eavesdropping.

For the rest of this paper, the random variables (RVs), values and alphabets are denoted by 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 N-dimensional random vector $(Y_1, \ldots, Y_N)$, and $y^N = (y_1, \ldots, y_N)$ represents a vector value in $\mathcal{Y}^N$ (the N-th Cartesian power of $\mathcal{Y}$). In addition, for an event $\{X = x\}$, its probability is denoted by $P(x)$. Throughout this paper, the base of the $\log$ function is 2.

This paper is organized as follows. Section II gives formal definition of the models studied in this paper. Section III shows that an already existing modified SK scheme also achieves the secrecy capacity of the GWTC-N-CSIT with feedback. Section IV shows the capacity results on the discrete memoryless action-dependent wiretap channel with noncausal state information at the transmitter and its Gaussian case (the action-dependent GWTC-N-CSIT). Section V introduces a feedback coding scheme for the action-dependent GWTC-N-CSIT, and shows that this scheme achieves the secrecy capacity of the action-dependent GWTC-N-CSIT with feedback for a special case. Section VI includes final conclusion and future work.

TABLE I

SUMMARIZING ALL RESULTS ON THE CHANNELS WITH NONCAUSAL/CAUSAL STATE AT THE TRANSMITTER, AND WITH OR WITHOUT ACTION, FEEDBACK AND EAVESDROPPER

DMC / Gaussian	State	Action	Feedback	Secrecy	Capacity
DMC	Noncausal/Causal	No	No	No	Known, in [3]/[1]
DMC	Noncausal/Causal	No	Yes	No	Known, both in [4]
DMC	Noncausal/Causal	Yes	No	No	Known, both in [10]
DMC	Noncausal/Causal	Yes	Yes	No	Known, both in [10]
DMC	Noncausal/Causal	No	No	Yes	Not known, bounds in [14, 15]/[16,17,18]
DMC	Noncausal/Causal	No	Yes	Yes	Not known, bounds in [21,38]/[21,31]
DMC	Noncausal/Causal	Yes	No	Yes	Not known, bounds in [43] and **this paper**/[43]
DMC	Noncausal/Causal	Yes	Yes	Yes	Not known, bounds in [33,37]/[33]
Gaussian	Noncausal/Causal	No	No	No	Known, in [5]/Not known, bounds in [7,8,9]
Gaussian	Noncausal/Causal	No	Yes	No	Known, in [6]/Not known
Gaussian	Noncausal/Causal	Yes	No	No	Known, in [10,11]/Not known
Gaussian	Noncausal/Causal	Yes	Yes	No	Known, in [10,11]/Not known
Gaussian	Noncausal/Causal	No	No	Yes	Not known, bounds in [19]/Not known
Gaussian	Noncausal/Causal	No	Yes	Yes	Known, determined in **this paper**/Not known
Gaussian	Noncausal/Causal	Yes	No	Yes	Not known, **this paper** derives lower and upper bounds/Not known
Gaussian	Noncausal/Causal	Yes	Yes	Yes	Not known, bounds in [37] and **this paper**/Not known

II. MODEL FORMULATION

In this section, we give formal definitions of the GWTC-N-CSIT with feedback, and the action-dependent GWTC-N-CSIT with or without feedback. For convenience, the following Table II provides notations about capacities of various channel models introduced in the remainder of this paper.

A. Model I: The GWTC-N-CSIT With Noiseless Feedback

In this subsection, we describe the Gaussian state-dependent wiretap channel with noncausal state information at the transmitter and noiseless feedback (the GWTC-N-CSIT with noiseless feedback), see Figure 1. In Figure 1, the message M is uniformly distributed over its alphabet set $\mathcal{M} = \{1, 2, \ldots, |\mathcal{M}|\}$, and the state sequence S^N is independent identically distributed (i.i.d.), which is generated according to $\mathcal{N}(0, Q)$.

Authorized licensed use limited to: Technion Israel Institute of Technology. Downloaded on May 24,2020 at 05:32:54 UTC from IEEE Xplore. Restrictions apply.

TABLE II

NOTATIONS ON CAPACITIES OF VARIOUS CHANNEL MODELS INTRODUCED IN THIS PAPER

Notation	Meaning
$\mathcal{C}_g$	Capacity of the Gaussian channel
$\mathcal{C}_g^f$	Capacity of the Gaussian channel with feedback
$\mathcal{C}_{dpc}$	Capacity of the dirty paper channel
$\mathcal{C}_{dpc}^f$	Capacity of the dirty paper channel with feedback
$\mathcal{C}_a$	Capacity of the action-dependent C-N-CSIT
$\mathcal{C}_{ag}$	Capacity of the action-dependent dirty paper channel
$\mathcal{C}_{g-wtc}^f$	Secrecy capacity of the Gaussian wiretap channel with feedback
$\mathcal{C}_s^f$	Secrecy capacity of the WTC-N-CSIT with feedback
$\mathcal{C}_{sg}$	Secrecy capacity of the GWTC-N-CSIT
$\mathcal{C}_{sg}^f$	Secrecy capacity of the GWTC-N-CSIT with feedback
$\mathcal{C}_{sa}$	Secrecy capacity of the action-dependent WTC-N-CSIT
$\mathcal{C}_{sa}^f$	Secrecy capacity of the action-dependent WTC-N-CSIT with feedback
$\mathcal{C}_{sag}$	Secrecy capacity of the action-dependent GWTC-N-CSIT
$\mathcal{C}_{sag}^f$	Secrecy capacity of the action-dependent GWTC-N-CSIT with feedback

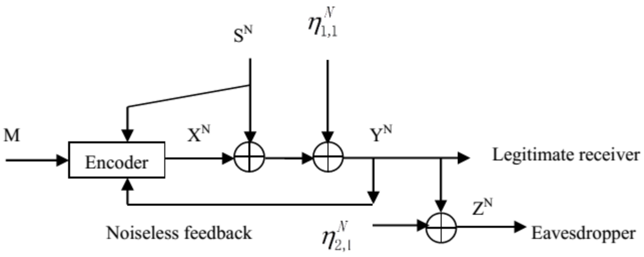

Fig. 1. The GWTC-N-CSIT with noiseless feedback.

At each time i ($i \in \{1, 2, \ldots, N\}$), the inputs and outputs of this Gaussian model satisfy

$$Y_i = X_i + S_i + \eta_{1,i}, \quad Z_i = X_i + S_i + \eta_{1,i} + \eta_{2,i}, \quad (2.1)$$

where X_i is the channel input at time i subject to an average power constraint P, and it is a (stochastic) function of the transmitted message M, the noncausal interference S^N and the channel feedback Y^{i-1}, Y_i and Z_i are channel outputs respectively at the legitimate receiver and the eavesdropper, and S_i, $\eta_{1,i}$, $\eta_{2,i}$ are independent Gaussian state interference and noises and are i.i.d. across the time index i. Here note that $S_i \sim \mathcal{N}(0, Q)$, $\eta_{1,i} \sim \mathcal{N}(0, \sigma_1^2)$ and $\eta_{2,i} \sim \mathcal{N}(0, \sigma_2^2)$.

The legitimate receiver produces an estimation $\hat{M} = \psi(Y^N)$, where ψ is the legitimate receiver's decoding function, and the average decoding error probability equals

$$P_e = \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} Pr\{\psi(y^N) \neq m | m \text{ sent}\}. \quad (2.2)$$

The eavesdropper's equivocation rate of the message M is defined as

$$\Delta = \frac{1}{N} H(M|Z^N). \quad (2.3)$$

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

$$\frac{\log |\mathcal{M}|}{N} \geq R - \epsilon, \ \Delta \geq R - \epsilon, \ P_e \leq \epsilon, \quad (2.4)$$

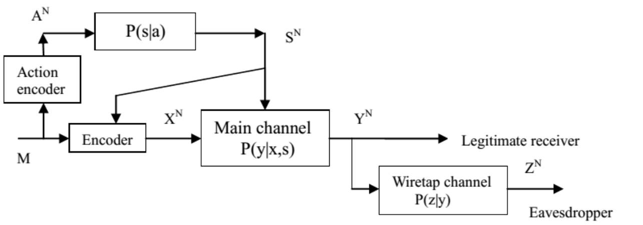

Fig. 2. The action-dependent wiretap channel with noncausal state information at the transmitter.

we say that R is achievable with perfect weak secrecy. The secrecy capacity $\mathcal{C}_{sg}^f$ is the supremum over all achievable weak secrecy rates, and it will be given in Section III.

B. Model II: The Action-Dependent GWTC-N-CSIT With or Without Noiseless Feedback

In this subsection, first, we study the action-dependent wiretap channel with noncausal state information at the transmitter and its Gaussian case (the action-dependent GWTC-N-CSIT). Then, we study the action-dependent GWTC-N-CSIT with noiseless feedback.

1) The Action-Dependent Wiretap Channel With Noncausal State Information at the Transmitter: The action-dependent wiretap channel with noncausal state at the transmitter is shown in Figure 2, where the overall channel transition probability is given by

$$P(y^N, z^N | x^N, s^N) = \prod_{i=1}^{N} P(z_i|y_i) P(y_i|x_i, s_i), \quad (2.5)$$

where $s_i \in \mathcal{S}$, $x_i \in \mathcal{X}$, $y_i \in \mathcal{Y}$ and $z_i \in \mathcal{Z}$.

The message M is uniformly distributed in its alphabet set $\mathcal{M} = \{1, 2, \ldots, |\mathcal{M}|\}$, and a stochastic action encoder encodes M into an action sequence A^N. The channel state sequence S^N is generated through a DMC $A^N \rightarrow S^N$ with transition probability $P(s|a)$. Since S^N is non-causally known by the channel encoder, the i-th ($i \in \{1, 2, \ldots, N\}$) channel input $X_i = f_i(M, S^N)$, where f_i is a stochastic encoding function. The legitimate receiver's decoding error and the eavesdropper's equivocation rate are defined in the same way as those in Subsection II-A (see (2.2) and (2.3)). The secrecy capacity $\mathcal{C}_{sa}$ of the model of Figure 2, is the supremum over all achievable weak secrecy rates defined in Subsection II-A. Bounds on $\mathcal{C}_{sa}$ will be given in Section IV.

Now we turn to the Gaussian case of the model of Figure 2 (the action-dependent GWTC-N-CSIT), see Figure 3. At time i ($i \in \{1, 2, \ldots, N\}$), the inputs and outputs of this Gaussian model satisfy

$$\begin{aligned} &S_i = A_i + W_i, \ Y_i = X_i + S_i + \eta_{1,i}, \\ &Z_i = X_i + S_i + \eta_{1,i} + \eta_{2,i}, \end{aligned} \quad (2.6)$$

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, Y_i and Z_i are channel outputs respectively at the legitimate receiver and the eavesdropper, and W_i, $\eta_{1,i}$, $\eta_{2,i}$ are independent Gaussian noises and are

Authorized licensed use limited to: Technion Israel Institute of Technology. Downloaded on May 24,2020 at 05:32:54 UTC from IEEE Xplore. Restrictions apply.

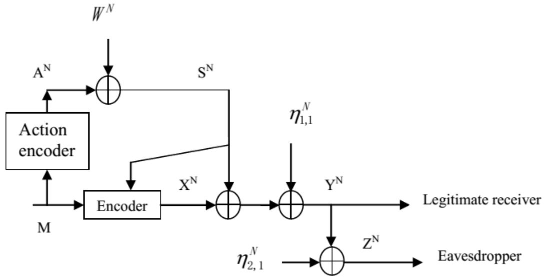

Fig. 3. The action-dependent GWTC-N-CSIT.

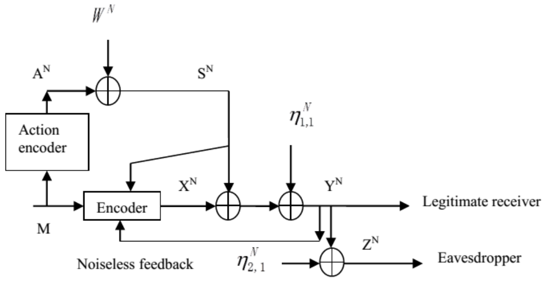

Fig. 4. The action-dependent GWTC-N-CSIT with noiseless feedback.

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 GWTC-N-CSIT is denoted by $\mathcal{C}_{sag}$, and bounds on $\mathcal{C}_{sag}$ will be given in Section IV.

2) The Action-Dependent GWTC-N-CSIT With Noiseless Feedback: The action-dependent GWTC-N-CSIT with noiseless feedback is shown in Figure 4. This feedback model is defined in the same way as the non-feedback model, except that the i-th ($i \in \{1, 2, \ldots, N\}$) channel encoder is a stochastic function of the message M, the interference S^N and the channel feedback Y^{i-1}. The secrecy capacity of the action-dependent GWTC-N-CSIT with noiseless feedback is denoted by $\mathcal{C}_{sag}^f$, and bounds on $\mathcal{C}_{sag}^f$ will be given in Section V.

III. The GWTC-N-CSIT With Noiseless Feedback

In this section, first, in order to show the advantage of using channel feedback, we review the capacity results on the GWTC-N-CSIT, see Subsection III-A. Next, we introduce a modified SK scheme [6] achieving the capacity of the dirty paper channel with feedback, see Subsection III-B. Finally, in Subsection III-C, we show that the introduced modified SK scheme in Subsection III-B also achieves the secrecy capacity of the GWTC-N-CSIT with noiseless feedback.

A. Capacity Results on the GWTC-N-CSIT

In this subsection, we review the GWTC-N-CSIT(see Figure 5). At each time i ($i \in \{1, 2, \ldots, N\}$), the inputs and outputs of this Gaussian model satisfy

$$Y_i = X_i + S_i + \eta_{1,i}, \quad Z_i = X_i + S_i + \eta_{1,i} + \eta_{2,i}, \qquad (3.1)$$

where X_i is the channel input subject to an average power constraint P, Y_i and Z_i are channel outputs respectively at the legitimate receiver and the eavesdropper, and S_i, $\eta_{1,i}$, $\eta_{2,i}$ are respectively independent Gaussian state interference and noises, and are i.i.d. across the time index i. Here note that $S_i \sim \mathcal{N}(0, Q)$, $\eta_{1,i} \sim \mathcal{N}(0, \sigma_1^2)$ and $\eta_{2,i} \sim \mathcal{N}(0, \sigma_2^2)$. The secrecy capacity of the GWTC-N-CSIT is denoted by $\mathcal{C}_{sg}$.

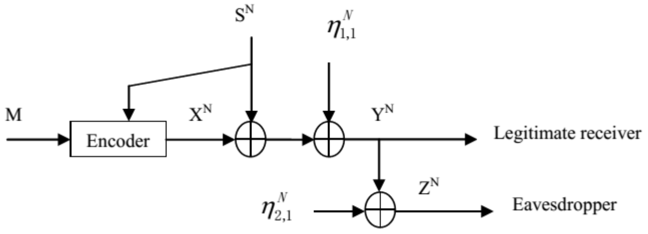

Fig. 5. The GWTC-N-CSIT.

A lower bound on $\mathcal{C}_{sg}$ has been obtained in [19], and is given by

$$\begin{aligned}
&\mathcal{C}_{sg} \geq R_{sg}^* \\
&= \max_{\alpha} \min \left\{ \frac{1}{2} \log \frac{(P+\alpha^2 Q)(P+Q+\sigma_1^2)}{(P+\alpha^2 Q)(P+Q+\sigma_1^2)-(P+\alpha Q)^2} \right. \\
&-\frac{1}{2} \log \frac{P+\alpha^2 Q}{P}, \\
&\frac{1}{2} \log \frac{(P+\alpha^2 Q)(P+Q+\sigma_1^2)}{(P+\alpha^2 Q)(P+Q+\sigma_1^2)-(P+\alpha Q)^2} \\
&\left. -\frac{1}{2} \log \frac{(P+\alpha^2 Q)(P+Q+\sigma_1^2+\sigma_2^2)}{(P+\alpha^2 Q)(P+Q+\sigma_1^2+\sigma_2^2)-(P+\alpha Q)^2} \right\}.
\end{aligned} \qquad (3.2)$$

Next, we present two upper bounds on $\mathcal{C}_{sg}$. The first upper bound $\mathcal{C}_{sg}^{upper-1}$ (see [19]) is obtained by letting the interference S be part of the channel input, i.e., the channel input has power constraint $P + Q$ and the main channel has no interference. Hence, following from the secrecy capacity of the Gaussian wiretap channel [20], we have

$$\begin{aligned}
&\mathcal{C}_{sg} \leq \mathcal{C}_{sg}^{upper-1} \\
&= \min \left\{ \frac{1}{2} \log \left(1 + \frac{P}{\sigma_1^2}\right), \right. \\
&\left. \frac{1}{2} \log \left(1 + \frac{P+Q}{\sigma_1^2}\right) - \frac{1}{2} \log \left(1 + \frac{P+Q}{\sigma_1^2 + \sigma_2^2}\right) \right\}.
\end{aligned} \qquad (3.3)$$

The second upper bound $\mathcal{C}_{sg}^{upper-2}$ has been obtained in [15], and is given by

$$\begin{aligned}
&\mathcal{C}_{sg} \leq \mathcal{C}_{sg}^{upper-2} \\
&= \min \left\{ \frac{1}{2} \log\left(1+\frac{P}{\sigma_1^2}\right), \frac{1}{2} \log\left(1+\frac{P+Q+2\sqrt{PQ}}{\sigma_1^2}\right) \right. \\
&\left. -\frac{1}{2} \log \left(1 + \frac{P+Q+2\sqrt{PQ}}{\sigma_1^2+\sigma_2^2}\right) \right\}.
\end{aligned} \qquad (3.4)$$

Since $f(x) = \log\left(1 + \frac{x}{\sigma_1^2}\right) - \log\left(1 + \frac{x}{(\sigma_1^2+\sigma_2^2)}\right)$ ($x \geq 0$) is monotonically increasing in x, the first upper bound is always tighter than the second one.

In the remainder of this paper, the capacity results on the GWTC-N-CSIT will be compared with those results on the GWTC-N-CSIT with feedback and the action-dependent GWTC-N-CSIT with or without feedback.

Authorized licensed use limited to: Technion Israel Institute of Technology. Downloaded on May 24,2020 at 05:32:54 UTC from IEEE Xplore. Restrictions apply.

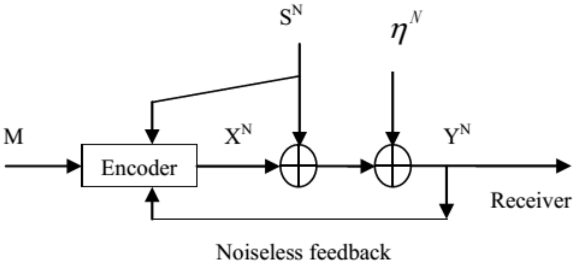

Fig. 6. The dirty paper channel with noiseless feedback.

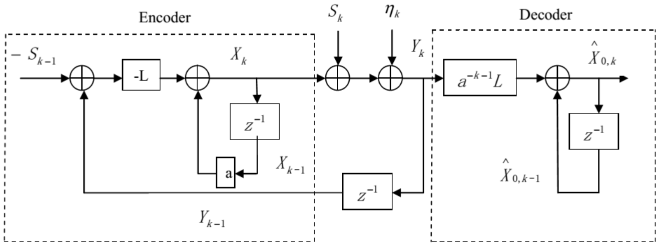

Fig. 7. The capacity achieving scheme for the dirty paper channel with noiseless feedback.

B. Capacity Achieving Scheme for the Dirty Paper Channel With Noiseless Feedback

For the dirty paper channel with noiseless feedback (see Figure 6), the i-th channel input and output satisfy

$$Y_i = X_i + S_i + \eta_i, \tag{3.5}$$

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, due to the channel feedback, the channel input X_i at time 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 information at the transmitter [42], and hence the capacity $\mathcal{C}^f_{dpc}$ of the dirty paper channel with noiseless feedback equals the capacity $\mathcal{C}_{dpc}$ of the dirty paper channel, i.e.,

$$\mathcal{C}^f_{dpc} = \mathcal{C}_{dpc} = \frac{1}{2}\log\left(1 + \frac{P}{\sigma^2}\right). \tag{3.6}$$

In this subsection, we introduce a feedback scheme [6] achieving the capacity (3.6) of the dirty paper channel with noiseless feedback, which can be viewed as a variation of the SK scheme [40]. The scheme is described below.

Without loss of generality, assume that the number of channel uses N equals $K + 1$ and the time instant $k \in \{0, 1, \ldots, K\}$. At time k, the encoder of the proposed scheme [6] is shown in Figure 7, and the output X_k of the encoder is given by

$$X_k = aX_{k-1} - L(Y_{k-1} - S_{k-1}), \tag{3.7}$$

where

$$a = \sqrt{1 + \frac{P}{\sigma^2}}, \tag{3.8}$$

and

$$L = a - \frac{1}{a}. \tag{3.9}$$

Moreover, from Figure 7, we see that the k-th channel output Y_k is given by

$$Y_k = X_k + S_k + \eta_k, \tag{3.10}$$

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

$$\hat{X}_{0,k} = \hat{X}_{0,k-1} + a^{-k-1}LY_k. \tag{3.11}$$

The transmitted message M is uniformly drawn from the alphabet set

$$\mathcal{M} = \{1, 2, \ldots, a^{(K+1)(1-\epsilon)}\}, \tag{3.12}$$

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

$$[-\sqrt{P}(1 + \frac{1}{a^{K+1} - 1}),\ \sqrt{P}(1 + \frac{1}{a^{K+1} - 1})], \tag{3.13}$$

into $a^{(K+1)(1-\epsilon)}$ sub-intervals, and the center of each sub-interval corresponds to a specific value in $\{1, 2, \ldots, a^{(K+1)(1-\epsilon)}\}$.

To start the encoding procedure, define $s_{-1} = y_{-1} = \hat{x}_{0,-1} = 0$ (where 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

$$M^* = -\frac{\sum_{j=0}^{K} a^{-j-1}Ls_j}{1 - a^{-K-2}}, \tag{3.14}$$

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

$$\bar{M}_K = \frac{\hat{X}_{0,K}}{1 - a^{-2K-2}} \tag{3.15}$$

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 w.r.t. the choosing message M. The above definitions imply that the k-th channel input X_k can be expressed as

$$X_k = a^{-k}(W_M + M^*) - \sum_{j=0}^{k-1} a^{-k+1+j}L\eta_j, \tag{3.16}$$

and the K-th output of the decoder $\hat{X}_{0,K}$ can be expressed as

$$\hat{X}_{0,K} = (1 - a^{-2K-2})M + a^{-2K-2}\sum_{j=0}^{K} a^{j+1}L\eta_j. \tag{3.17}$$

Finally, by combining (3.16), (3.17) and the above definitions, [6] 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.

Authorized licensed use limited to: Technion Israel Institute of Technology. Downloaded on May 24,2020 at 05:32:54 UTC from IEEE Xplore. Restrictions apply.

In the next subsection, we will show that the modified SK scheme introduced in this subsection also achieves the secrecy capacity of the GWTC-N-CSIT with feedback.

C. The Secrecy Capacity of the GWTC-N-CSIT With Noiseless Feedback

In this subsection, we show that the secrecy capacity $\mathcal{C}_{sg}^{f}$ of the GWTC-N-CSIT with noiseless feedback (see Subsection II-A) equals the capacity $\mathcal{C}_{dpc}^{f}$ of the same channel without secrecy constraints.

Theorem 1: The secrecy capacity $\mathcal{C}_{sg}^{f}$ of the GWTC-N-CSIT with noiseless feedback is given by

$$\mathcal{C}_{sg}^{f}=\mathcal{C}_{dpc}^{f}=\frac{1}{2}\log\left(1+\frac{P}{\sigma_1^2}\right). \tag{3.18}$$

Remark 1: From (3.16), we see that the original message is sent over all time instants, so that the information leakage occurs in all transmission steps. Hence the major step of the proof lies in showing 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.

Proof: First, note that the secrecy capacity $\mathcal{C}_{sg}^{f}$ cannot exceed the capacity of the model of Figure 1 without the eavesdropper. Hence, we have $\mathcal{C}_{sf}\leq\mathcal{C}_{dpc}^{f}=\frac{1}{2}\log(1+\frac{P}{\sigma_1^2})$. 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 (see Subsection III-B), and the detail is given below.

In Subsection III-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 while 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,\ldots,Z_K)\\
&\overset{(2)}{=} \frac{1}{K+1}H(W_M|W_M+M^*+S_0+\eta_{1,0}+\eta_{2,0},\\
&\quad a^{-1}(W_M+M^*)-L\eta_{1,0}+S_1+\eta_{1,1}+\eta_{2,1},\\
&\quad \ldots,a^{-K}(W_M+M^*)\\
&\quad -\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+M^*+S_0+\eta_{1,0}+\eta_{2,0},\\
&\quad a^{-1}(W_M+M^*)-L\eta_{1,0}+S_1+\eta_{1,1}+\eta_{2,1},\\
&\quad \ldots,a^{-K}(W_M+M^*)-\sum_{j=0}^{K-1}(a^{-K+1+j}L\eta_{1,j})\\
&\quad +S_K+\eta_{1,K}+\eta_{2,K},S_0,\ldots,S_K,\eta_{1,0},\ldots,\eta_{1,K})\\
&\overset{(4)}{=} \frac{1}{K+1}H(W_M|W_M+\eta_{2,0},a^{-1}W_M+\eta_{2,1},\ldots,\\
&\quad a^{-K}W_M+\eta_{2,K},S_0,\ldots,S_K,\eta_{1,0},\ldots,\eta_{1,K})\\
&\overset{(5)}{=} \frac{1}{K+1}H(W_M|W_M+\eta_{2,0},a^{-1}W_M+\eta_{2,1},\ldots,\\
&\quad a^{-K}W_M+\eta_{2,K})\\
&\overset{(6)}{=} \frac{1}{K+1}(H(W_M)\\
&\quad -I(W_M;W_M+\eta_{2,0},a^{-1}W_M+\eta_{2,1},\ldots,a^{-K}W_M+\eta_{2,K}))\\
&\overset{(7)}{=} \frac{1}{K+1}(H(W_M)\\
&\quad -h(W_M+\eta_{2,0},a^{-1}W_M+\eta_{2,1},\ldots,a^{-K}W_M+\eta_{2,K})\\
&\quad +h(W_M+\eta_{2,0},a^{-1}W_M+\eta_{2,1},\ldots,a^{-K}W_M+\eta_{2,K}|W_M))\\
&= \frac{1}{K+1}(H(W_M)\\
&\quad -h(W_M+\eta_{2,0},a^{-1}W_M+\eta_{2,1},\ldots,a^{-K}W_M+\eta_{2,K})\\
&\quad +h(\eta_{2,0},\eta_{2,1},\ldots,\eta_{2,K}|W_M))\\
&\overset{(8)}{=} \frac{1}{K+1}(H(W_M)\\
&\quad -h(W_M+\eta_{2,0},a^{-1}W_M+\eta_{2,1},\ldots,a^{-K}W_M+\eta_{2,K})\\
&\quad +h(\eta_{2,0},\eta_{2,1},\ldots,\eta_{2,K}))\\
&\overset{(9)}{=} \frac{1}{K+1}(H(W_M)+\sum_{i=0}^{K}h(\eta_{2,i})\\
&\quad -h(W_M+\eta_{2,0},a^{-1}W_M+\eta_{2,1},\ldots,a^{-K}W_M+\eta_{2,K}))\\
&\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{(10)}{=} (1-\epsilon)\log(a)+\frac{1}{2(K+1)}\log(2\pi e\sigma_2^2)^{K+1}\\
&\quad -\frac{1}{K+1}\sum_{i=0}^{K}h(a^{-i}W_M+\eta_{2,i})\\
&\overset{(11)}{\geq} (1-\epsilon)\log(a)+\frac{1}{2(K+1)}\log(2\pi e\sigma_2^2)^{K+1}\\
&\quad -\frac{1}{2(K+1)}\sum_{i=0}^{K}\log\left(2\pi e(\frac{P}{3}a^{-2i}+\sigma_2^2)\right)\\
&= (1-\epsilon)\log(a)+\frac{1}{2(K+1)}\log(2\pi e\sigma_2^2)^{K+1}\\
&\quad -\frac{1}{2(K+1)}\log\left((2\pi e)^{K+1}\prod_{i=0}^{K}(\frac{P}{3}a^{-2i}+\sigma_2^2)\right)\\
&= (1-\epsilon)\log(a)+\frac{1}{2(K+1)}\log\left(\frac{(\sigma_2^2)^{K+1}}{\prod_{i=0}^{K}(\frac{P}{3}a^{-2i}+\sigma_2^2)}\right)\\
&= (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\left(1+\frac{P}{3}\frac{a^{-2i}}{\sigma_2^2}\right)\\
&\overset{(12)}{\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}}
\end{aligned}$$

Authorized licensed use limited to: Technion Israel Institute of Technology. Downloaded on May 24,2020 at 05:32:54 UTC from IEEE Xplore. Restrictions apply.

$$\overset{(13)}{=} (1-\epsilon)\frac{1}{2}\log\left(1+\frac{P}{\sigma_1^2}\right) - \frac{1}{2(K+1)\ln 2}\frac{P}{3\sigma_2^2}\frac{1-a^{-2K-2}}{1-a^{-2}}, \tag{3.19}$$

where (1) follows from the fact that M can be denoted by W_M, and the definition $Z^N = (Z_0, \ldots, Z_K)$, (2) follows from (2.1), (3.16) and (3.14), (3) and (4) follow from conditions reduce entropy and the fact that M^* is determined by $(S_0, \ldots, S_K)$ (see (3.14)), (5) follows from the fact that S_0, ..., S_K, $\eta_{1,0}$,...,$\eta_{1,K}$ are independent of W_M, $W_M + \eta_{2,0}$, $a^{-1}W_M + \eta_{2,1}$,...,$a^{-K}W_M + \eta_{2,K}$, (6) follows from the fact that for a discrete RV A and a continuous RV B, $H(A|B) = H(A) - I(A;B)$ (see Definition 10.28 in [48]), (7) follows from the fact that for a discrete RV A and a continuous RV B, $I(A;B) = h(B) - h(B|A)$ (see Proposition 10.29 in [48]), (8) follows from the fact that W_M is independent of $\eta_{2,0}$, $\eta_{2,1}$,...,$\eta_{2,K}$, (9) follows from the fact that $\eta_{2,0}$, $\eta_{2,1}$,...,$\eta_{2,K}$ are i.i.d. random variables, (10) follows from (3.12) and $\eta_{2,i} \sim \mathcal{N}(0, \sigma_2^2)$, (11) follows from 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 $\eta_{2,i}$, hence we have

$$h(a^{-i}W_M + \eta_{2,i}) \leq \frac{1}{2}\log\left(2\pi e(\frac{P}{3}a^{-2i} + \sigma_2^2)\right), \tag{3.20}$$

(12) follows from the inequality $\ln(1+x) \leq x$ for $x \geq 0$, and (13) follows from (3.8).

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 (3.19) satisfies

$$\lim_{K\to\infty} \frac{1}{2(K+1)\ln 2}\frac{P}{3\sigma_2^2}\frac{1-a^{-2K-2}}{1-a^{-2}} = 0. \tag{3.21}$$

Hence choosing sufficiently large K, we have

$$\Delta \geq \frac{1}{2}\log(1+\frac{P}{\sigma_1^2}) - \epsilon^{'}. \tag{3.22}$$

The proof of Theorem 1 is completed. ■

The following Corollary 1 provides an already existing secret key based lower bound R_{sg}^{f*} on $\mathcal{C}_{sg}^f$.

Corollary 1: A lower bound R_{sg}^{f*} on the secrecy capacity $\mathcal{C}_{sg}^f$ of the GWTC-N-CSIT with noiseless feedback is given by

$$R_{sg}^{f*} = \min\left\{\frac{1}{2}\log\left(1+\frac{P}{\sigma_1^2}\right), \frac{1}{2}\log\left(\frac{2\pi e\sigma_2^2(P+\sigma_1^2)}{P+\sigma_1^2+\sigma_2^2}\right)\right\}. \tag{3.23}$$

Proof: In [38], the WTC-N-CSIT with noiseless feedback, i.e., the physically degraded state-dependent wiretap channel with channel feedback and noncausal state information at the transmitter, was studied. It has been shown that the secrecy capacity of this discrete memoryless model can be achieved by using the secret key based feedback strategy, and the secrecy capacity $\mathcal{C}_s^f$ is given by

$$\mathcal{C}_s^f = \max_{P(x|u,s),P(u|s)} \min\{I(U;Y) - I(U;S), H(Y|Z)\}, \tag{3.24}$$

where the joint distribution satisfies

$$P(u,s,x,y,z) = P(z|y)P(y|x,s)P(x|u,s)P(u|s)P(s). \tag{3.25}$$

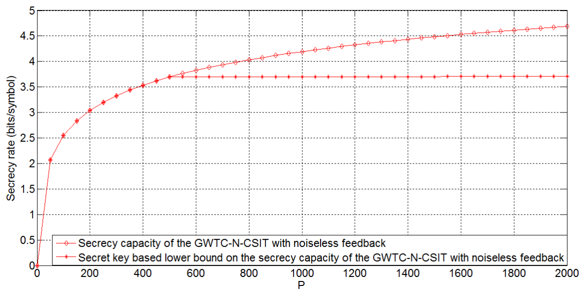

Fig. 8. The capacity results on the GWTC-N-CSIT with feedback for $Q = 2$, $\sigma_1^2 = 3$, $\sigma_2^2 = 10$ and P taking values in $[0, 2000]$.

However, we should note that the capacity formula in (3.24) is only an achievable secrecy rate for the GWTC-N-CSIT with noiseless feedback, and this is because the converse of $H(Y|Z)$ in (3.24) does not hold for the Gaussian case. To be specific, first, note that the term $H(Y|Z)$ in (3.24) follows from

$$\begin{aligned}
R - \epsilon &\leq \frac{1}{N}H(M|Z^N) \\
&\leq \frac{1}{N}(I(M;Y^N|Z^N) + \delta(\epsilon)) \\
&\overset{(a)}{\leq} \frac{1}{N}(H(Y^N|Z^N) + \delta(\epsilon)) \\
&\leq \frac{1}{N}(\sum_{i=1}^N H(Y_i|Z_i) + \delta(\epsilon)) \\
&\overset{(b)}{=} H(Y_J|Z_J, J) + \frac{1}{N}\delta(\epsilon) \\
&\overset{(c)}{\leq} H(Y|Z) + \frac{1}{N}\delta(\epsilon),
\end{aligned} \tag{3.26}$$

and letting $\epsilon \to 0$, where (a) follows from $I(M;Y^N|Z^N) \leq H(Y^N|Z^N)$, (b) follows from J is uniformly distributed over $\{1, 2, \ldots, N\}$ and it is independent of Y^N and Z^N, and (c) follows from the definitions $Y \triangleq Y_J$ and $Z \triangleq Z_J$. Next, from (3.26), we can check that for the Gaussian case, step (a) of (3.26) does not hold due to the fact that the differential conditional entropy $h(Y^N|Z^N, M)$ may be a negative number. Finally, substituting $U = X + \alpha S$, $X \sim \mathcal{N}(0, P)$ and (2.1) into (3.24), and maximizing α, the lower bound R_{sg}^{f*} on the secrecy capacity $\mathcal{C}_{sg}^f$ is obtained. The proof of Corollary 1 is completed. ■

The following Figure 8 shows the gap between the lower bound R_{sg}^{f*} and the secrecy capacity $\mathcal{C}_{sg}^f$ for $Q = 2$, $\sigma_1^2 = 3$, $\sigma_2^2 = 10$ and P taking values in $[0, 2000]$. It is easy to see that the gap is increasing while the power P is increasing.

The following Figure 9 compares the capacity results on the GWTC-N-CSIT with or without feedback for $Q = 2$, $\sigma_1^2 = 3$, $\sigma_2^2 = 10$ and P taking values in $[0, 20]$. From this figure, we see that the feedback enhances the secrecy capacity of the GWTC-N-CSIT.

Authorized licensed use limited to: Technion Israel Institute of Technology. Downloaded on May 24,2020 at 05:32:54 UTC from IEEE Xplore. Restrictions apply.

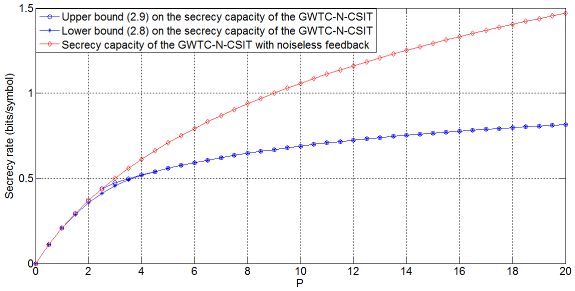

Fig. 9. The comparison of the capacity results on the GWTC-N-CSIT with or without feedback for $Q = 2$, $\sigma_1^2 = 3$, $\sigma_2^2 = 10$ and P taking values in $[0, 20]$.

IV. The Action-Dependent GWTC-N-CSIT

In this section, first, we introduce the capacity results on the action-dependent dirty paper channel, see Subsection IV-A. Next, we derive lower and upper bounds on the secrecy capacity of the discrete memoryless action-dependent wiretap channel with noncausal state information at the transmitter, see Subsection IV-B. Finally, we derive bounds on the secrecy capacity of the action-dependent GWTC-N-CSIT by using the bounds shown in the preceding subsections, see Subsection IV-C.

A. Capacity Results on the Action-Dependent Dirty Paper Channel

In this subsection, we review the capacity results on the action-dependent dirty paper channel (see Figure 10). At time i ($i \in \{1, 2, \ldots, N\}$), the inputs and output satisfy

$$S_i = A_i + W_i, \quad Y_i = X_i + S_i + \eta_{1,i}, \tag{4.1}$$

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, Y_i is the channel output at the receiver, and W_i, $\eta_{1,i}$ are independent Gaussian noises and are i.i.d. across the time index i. Here note that $W_i \sim \mathcal{N}(0, \sigma_w^2)$ and $\eta_{1,i} \sim \mathcal{N}(0, \sigma_1^2)$. The capacity of the action-dependent dirty paper channel is denoted by $\mathcal{C}_{ag}$.

A lower bound on $\mathcal{C}_{ag}$ has been obtained in [10], and is given by

$$\begin{aligned}\mathcal{C}_{ag} \;&\geq\; R_{ag}^{*}\\ &= \max_{(\alpha,\gamma):\alpha^2 P_A+\gamma^2\sigma_w^2\leq P}\left(\frac{1}{2}\log\left(1+\frac{D(\alpha,\gamma)}{\sigma_1^2}\right)\right.\\ &\quad\left.+\frac{1}{2}\log\left(1+\frac{P_A(\alpha+1)^2}{D(\alpha,\gamma)+\sigma_w^2(\gamma+1)^2+\sigma_1^2}\right)\right),\end{aligned} \tag{4.2}$$

where $D(\alpha, \gamma) = P - \alpha^2 P_A - \gamma^2 \sigma_w^2$.

Proof sketch of R_{ag}^*:

First, note that in [10], the capacity of the discrete memoryless action-dependent channel with noncausal state information at the transmitter has been obtained and is given by

$$\mathcal{C}_a = \max_{P(a),P(u|a,s),P(x|u,s)} (I(U;Y) - I(U;S|A)), \tag{4.3}$$

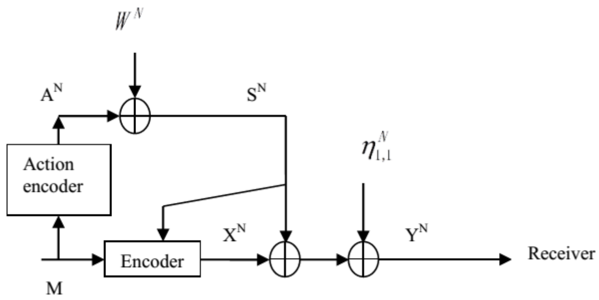

Fig. 10. The action-dependent dirty paper channel.

where the maximization is over all joint distribution

$$P(u, a, s, x, y) = P(a)P(s|a)P(u|a, s)P(x|u, s)P(y|x, s). \tag{4.4}$$

Then, letting $G \sim \mathcal{N}(0, P - \alpha^2 P_A - \gamma^2 \sigma_w^2)$, and $\alpha^2 P_A + \gamma^2 \sigma_w^2 \leq P$, where G, A, W, η_1 are independent of each other. Substituting

$$A \sim \mathcal{N}(0, P_A), \; X = \alpha A + \gamma W + G, \; U = \delta X + A + \beta W, \tag{4.5}$$

into the term $I(U;Y) - I(U;S|A)$ of (4.3) and maximizing it, the lower bound R_{ag}^* is obtained. The details of the proof is in [10].

However, we should notice that in general, R_{ag}^* is not tight. Recently, it has been shown in [11] that the capacity $\mathcal{C}_{ag}$ is given by

$$\begin{aligned}\mathcal{C}_{ag} \;&=\; \max_{(\rho_1,\rho_2):\rho_1^2+\rho_2^2\leq 1} \frac{1}{2}\log\left(1+\frac{P(1-\rho_1^2-\rho_2^2)}{\sigma_1^2}\right)\\ &\quad+\frac{1}{2}\log\left(1+\frac{(\sqrt{P_A}+\rho_2\sqrt{P})^2}{P(1-\rho_1^2-\rho_2^2)+(\sigma_w+\rho_1\sqrt{P})^2+\sigma_1^2}\right),\end{aligned} \tag{4.6}$$

where $-1 \leq \rho_1 \leq 0$ and $0 \leq \rho_2 \leq 1$.

Proof sketch of $\mathcal{C}_{ag}$:

- The converse part consists of the following three key steps: First, note that the term $I(U;Y) - I(U;S|A)$ of (4.3) can be further upper bounded by

  $$I(U;Y) - I(U;S|A) \leq I(A;Y) + I(X;Y|A, W). \tag{4.7}$$

  Second, it has been shown that (4.7) is maximized by taking (X, A, W, Z, Y) to be jointly Gaussian. Third, define $\rho_1 = \frac{E[XW]}{\sqrt{P\sigma_w^2}}$, $\rho_2 = \frac{E[XA]}{\sqrt{P}\sqrt{P_A}}$, and note that the power constraints of X and A respectively indicate that $E[X^2] = \sigma_X^2 \leq P$ and $E[A^2] = \sigma_A^2 \leq P_A$. Then it has been shown that respectively replacing σ_X^2 and σ_A^2 by P and P_A further increases the upper bound to $\mathcal{C}_{ag}$. Finally, note that the constraints of ρ_1 and ρ_2 follow from the fact the covariance matrix of (X, A, W) should satisfy the nonnegative-definiteness condition.
- For the direct part, $\mathcal{C}_{ag}$ is achieved by substituting $A \sim \mathcal{N}(0, P_A)$, $X \sim \mathcal{N}(0, P)$, $U = X + \beta S$ and (4.1)

Authorized licensed use limited to: Technion Israel Institute of Technology. Downloaded on May 24,2020 at 05:32:54 UTC from IEEE Xplore. Restrictions apply.

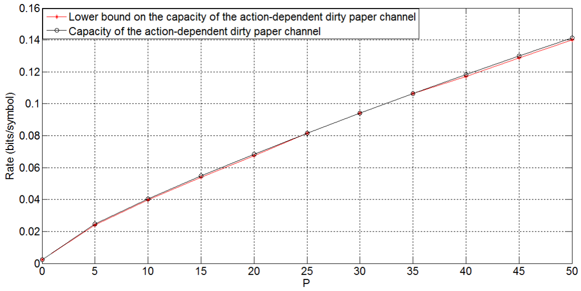

Fig. 11. Comparison of the already existing capacity results on the action-dependent dirty paper channel.

into $I(U;Y)-I(U;S|A)$ and using linear MMSE estimation to re-write the corresponding equality. The details of the converse and direct proof are in [11].

The following Figure 11 shows the gap between the lower bound R_{ag}^* and the capacity $\mathcal{C}_{ag}$ for $P_A=1$, $\sigma_w^2=1$, $\sigma_1^2=300$ and P taking values in $[0,50]$.

In the remainder of this paper, the capacity results of this subsection will play a role to derive lower and upper bounds on the secrecy capacities of the action-dependent GWTC-N-CSIT with or without feedback.

B. The Discrete Memoryless Action-Dependent Wiretap Channel With Noncausal State Information at the Transmitter

In this subsection, we propose one lower and two upper bounds on the secrecy capacity $\mathcal{C}_{sa}$ of the discrete memoryless action-dependent wiretap channel with noncausal state information at the transmitter (see Subsection II-B).

Theorem 2 (Lower Bound): $\mathcal{C}_{sa}\geq R_{sa}^*$, where

$$R_{sa}^*=\max_{P(a),P(u|a,s),P(x|u,s)}\min\{I(U;Y)-I(U;S|A),\\ I(U;Y)-I(U;Z)\}, \tag{4.8}$$

and the maximization is over all joint distributions taking the following form

$$P(u,a,s,x,y,z)\\ =P(a)P(s|a)P(u|a,s)P(x|u,s)P(y|x,s)P(z|y). \tag{4.9}$$

Proof: The lower bound R_{sa}^* is achieved by combining the coding scheme in [10] with the random binning scheme in [12]. The full detail of the proof is provided in Appendix A. ■

Remark 2: Note that [43] also proposes a lower bound on the secrecy capacity of the discrete memoryless action-dependent wiretap channel with noncausal state information at the transmitter. However, we should point out that the model studied in [43] assumes that the action encoder is a deterministic encoder, i.e., if the eavesdropper knows A^N, the message M is also known. Hence the lower bound R_{sa}^* generalizes that in [43] due to the reason that the deterministic action encoder is a special case of the stochastic one studied in this paper.

Besides the above lower bound on $\mathcal{C}_{sa}$, the following theorems provide two upper bounds on $\mathcal{C}_{sa}$.

Theorem 3 (Upper bound 1): $\mathcal{C}_{sa}\leq\mathcal{C}_{sa}^{upper-1}$, where

$$\mathcal{C}_{sa}^{upper-1}=\max_{P(a),P(u|a,s),P(x|u,s)}\min\{I(U;Y)-I(U;S|A),\\ I(X,S;Y)-I(X,S;Z)\}, \tag{4.10}$$

and the maximization is over the joint distributions described by (4.9).

Proof: See Appendix B. ■

Theorem 4: (Upper Bound 2): $\mathcal{C}_{sa}\leq\mathcal{C}_{sa}^{upper-2}$, where

$$\mathcal{C}_{sa}^{upper-2}=\max_{P(u,k|a,s),P(x|u,k,s),P(a)}\min\{I(U,K;Y)\\ -I(U,K;S|A),I(U,K;Y)-I(U,K;S|A)-I(U;Z)\\ +I(U;S|A)\}, \tag{4.11}$$

and the maximization is over the joint distributions given by

$$P(u,k,a,s,x,y,z)\\ =P(a)P(s|a)P(u,k|a,s)P(x|u,k,s)P(y|x,s)P(z|y). \tag{4.12}$$

Proof: See Appendix C. ■

In the next subsection, we further specialize the above proposed lower bound R_{sa}^* and the first upper bound $\mathcal{C}_{sa}^{upper-1}$ by the Gaussian channel, [1] which is also referred to as the action-dependent GWTC-N-CSIT.

C. The Action-Dependent GWTC-N-CSIT

In Subsection IV-A, it has been shown that for the action-dependent dirty paper channel, different ways of choosing distributions of (U,A,X) lead to different lower bounds on the capacity $\mathcal{C}_{ag}$. To be specific, [10] provides a lower bound R_{ag}^* on $\mathcal{C}_{ag}$ by the definition in (4.5), i.e.,

$$A\sim\mathcal{N}(0,P_A),\ X=\alpha A+\gamma W+G,\\ U=\delta X+A+\beta W, \tag{4.13}$$

where $\alpha^2P_A+\gamma^2\sigma_w^2\leq P$, $G\sim\mathcal{N}(0,P-\alpha^2P_A-\gamma^2\sigma_w^2)$ and G, A, W, η_1 are independent of each other. Here note that in general, R_{ag}^* is not tight. Moreover, [11] provides a tight lower bound (i.e., achieving $\mathcal{C}_{ag}$) by the definition $U=X+\beta(A+W)$. It is easy to see that for the channel model without secrecy constraints, the definition $U=X+\beta(A+W)$ is better than that in (4.5).

In this subsection, we provide two lower and one upper bounds on the secrecy capacity $\mathcal{C}_{sag}$ of the action-dependent GWTC-N-CSIT (see Subsection II-B), where the two lower bounds are respectively obtained by the above definitions (4.5) and $U=X+\beta(A+W)$, and the upper bound is obtained by applying entropy power inequality to $\mathcal{C}_{sa}^{upper-1}$. Somewhat surprisingly, numerical results indicate that the definition in (4.5) may achieve a tighter lower bound than $U=X+\beta(A+W)$ does. The detail about these bounds is given in the remainder of this subsection.

[1] Here note that further specializing the second upper bound $\mathcal{C}_{sa}^{upper-2}$ by the Gaussian channel is difficult and it remains open.

Authorized licensed use limited to: Technion Israel Institute of Technology. Downloaded on May 24,2020 at 05:32:54 UTC from IEEE Xplore. Restrictions apply.

First, we provide the following two lower bounds on $\mathcal{C}_{sag}$.

Theorem 5 (Lower Bound 1): $\mathcal{C}_{sag} \geq R^{*}_{sag}$, as shown in (4.14)–(4.19), at the bottom of the next page.

Proof: The lower bound R^{*}_{sag} is obtained by substituting (4.13) and (2.6) into (4.8), and the detail about the calculation is omitted. ■

Theorem 6 (Lower Bound 2): $\mathcal{C}_{sag} \geq R^{**}_{sag}$, where

$$\begin{aligned}R^{**}_{sag} = &\max_{(\rho_1,\rho_2):\rho_1^2+\rho_2^2\leq 1}\left(\frac{1}{2}\log\left(1+\frac{P(1-\rho_1^2-\rho_2^2)}{\sigma_1^2}\right)\right.\\ &-\frac{1}{2}\log\left(1+\frac{P(1-\rho_1^2-\rho_2^2)}{\sigma_1^2+\sigma_2^2}\right)\\ &+\frac{1}{2}\log\left(1+\frac{(\sqrt{P_A}+\rho_2\sqrt{P})^2}{P(1-\rho_1^2-\rho_2^2)+(\sigma_w+\rho_1\sqrt{P})^2+\sigma_1^2}\right)\\ &-\frac{1}{2}\log\,(1+\\ &\left.\left.\frac{(\sqrt{P_A}+\rho_2\sqrt{P})^2}{P(1-\rho_1^2-\rho_2^2)+(\sigma_w+\rho_1\sqrt{P})^2+\sigma_1^2+\sigma_2^2}\right)\right),\end{aligned} \tag{4.20}$$

$-1 \leq \rho_1 \leq 0$ and $0 \leq \rho_2 \leq 1$.

Proof: First, define $\rho_1 = \frac{E[XW]}{\sqrt{P\sigma_w^2}}$, $\rho_2 = \frac{E[XA]}{\sqrt{P}\sqrt{P_A}}$, and ρ_1, ρ_2 satisfy the constraints that $-1 \leq \rho_1 \leq 0$, $0 \leq \rho_2 \leq 1$ and $\rho_1^2+\rho_2^2 \leq 1$. Then it has been shown in [11] that substituting $A \sim \mathcal{N}(0, P_A)$, $X \sim \mathcal{N}(0, P)$, $U = X + \beta(A+W)$, $S = A+W$ and $Y = X+S+\eta_1$ (see (2.6)) into $I(U;Y) - I(U;S|A)$ and using linear MMSE estimation to re-write the corresponding equality, we have

$$\begin{aligned}&I(U;Y)-I(U;S|A)\\ &=\frac{1}{2}\log\left(1+\frac{P(1-\rho_1^2-\rho_2^2)}{\sigma_1^2}\right)\\ &+\frac{1}{2}\log\left(1+\frac{(\sqrt{P_A}+\rho_2\sqrt{P})^2}{P(1-\rho_1^2-\rho_2^2)+(\sigma_w+\rho_1\sqrt{P})^2+\sigma_1^2}\right).\end{aligned} \tag{4.21}$$

Analogously, substituting $A \sim \mathcal{N}(0, P_A)$, $X \sim \mathcal{N}(0, P)$, $U = X+\beta(A+W)$, $S = A+W$ and $Z = X+S+\eta_1+\eta_2$ (see (2.6)) into $I(U;Z) - I(U;S|A)$ and using linear MMSE estimation to re-write the corresponding equality, we have

$$\begin{aligned}&I(U;Z)-I(U;S|A)\\ &=\frac{1}{2}\log\left(1+\frac{P(1-\rho_1^2-\rho_2^2)}{\sigma_1^2+\sigma_2^2}\right)\\ &+\frac{1}{2}\log\left(1+\frac{(\sqrt{P_A}+\rho_2\sqrt{P})^2}{P(1-\rho_1^2-\rho_2^2)+(\sigma_w+\rho_1\sqrt{P})^2+\sigma_1^2+\sigma_2^2}\right).\end{aligned} \tag{4.22}$$

From (4.22), we know that $I(U;Z) - I(U;S|A) \geq 0$, which indicates that

$$\begin{aligned}&I(U;Y)-I(U;Z)\\ &=I(U;Y)-I(U;S|A)-(I(U;Z)-I(U;S|A))\\ &\leq I(U;Y)-I(U;S|A).\end{aligned} \tag{4.23}$$

Finally, substituting (4.21) and (4.22) into Theorem 2 and using the inequality (4.23), Theorem 6 is proved. ■

Next, we derive the following upper bound on $\mathcal{C}_{sag}$.

Theorem 7: $\mathcal{C}_{sag} \leq \mathcal{C}^{upper}_{sag} = \min\{L_1, L_2\}$, where

$$\begin{aligned}L_1 \ = \ &\max_{(\rho_1,\rho_2):\rho_1^2+\rho_2^2\leq 1}\frac{1}{2}\log\left(1+\frac{P(1-\rho_1^2-\rho_2^2)}{\sigma_1^2}\right)\\ &+\frac{1}{2}\log\left(1+\frac{(\sqrt{P_A}+\rho_2\sqrt{P})^2}{P(1-\rho_1^2-\rho_2^2)+(\sigma_w+\rho_1\sqrt{P})^2+\sigma_1^2}\right),\end{aligned} \tag{4.24}$$

$-1 \leq \rho_1 \leq 0$, $0 \leq \rho_2 \leq 1$ and

$$\begin{aligned}L_2 = &\frac{1}{2}\log\left(1+\frac{(\sqrt{P}+\sqrt{P_A+\sigma_w^2})^2}{\sigma_1^2}\right)\\ &-\frac{1}{2}\log\left(1+\frac{(\sqrt{P}+\sqrt{P_A+\sigma_w^2})^2}{\sigma_1^2+\sigma_2^2}\right).\end{aligned} \tag{4.25}$$

Proof: From (4.10), we have

$$\begin{aligned}&\mathcal{C}_{sag} \leq \max\min\{I(U;Y)-I(U;S|A),\\ &I(X,S;Y)-I(X,S;Z)\}\\ &\leq \min\{\max(I(U;Y)-I(U;S|A)),\\ &\max(I(X,S;Y)-I(X,S;Z))\}.\end{aligned} \tag{4.26}$$

Next, from [11], we know that

$$\max(I(U;Y)-I(U;S|A)) = L_1. \tag{4.27}$$

Now it remains to further upper bound $\max(I(X,S;Y) - I(X,S;Z))$ in (4.26).

$$\begin{aligned}&I(X,S;Y)-I(X,S;Z)\\ &=h(Y)-h(Y|X,S)-h(Z)+h(Z|X,S)\\ &\overset{(a)}{=} h(X+S+\eta_1)-h(\eta_1)-h(X+S+\eta_1+\eta_2)\\ &+h(\eta_1+\eta_2)\\ &\overset{(b)}{\leq} h(X+S+\eta_1)-h(\eta_1)\\ &-\frac{1}{2}\log(2^{2h(X+S+\eta_1)}+2^{2h(\eta_2)})+h(\eta_1+\eta_2),\end{aligned} \tag{4.28}$$

where (a) follows from (2.6), and (b) follows from the entropy power inequality. The differential entropy $h(X+S+\eta_1)$ in (4.28) can be further bounded by

$$\begin{aligned}&h(X+S+\eta_1) \ ^{(c)}\\ &\leq \frac{1}{2}\log(2\pi e(Var(X+S)+\sigma_1^2))\\ &\overset{(d)}{\leq} \frac{1}{2}\log(2\pi e((\sqrt{P}+\sqrt{P_A+\sigma_w^2})^2+\sigma_1^2)),\end{aligned} \tag{4.29}$$

where (c) follows from the fact that η_1 is independent of $X+S$, and (d) follows because

$$\begin{aligned}&Var(X+S)\\ &\leq Var(X)+Var(S)+2\sqrt{Var(X)}\sqrt{Var(S)}\\ &=(\sqrt{P}+\sqrt{P_A+\sigma_w^2})^2.\end{aligned} \tag{4.30}$$

Authorized licensed use limited to: Technion Israel Institute of Technology. Downloaded on May 24,2020 at 05:32:54 UTC from IEEE Xplore. Restrictions apply.

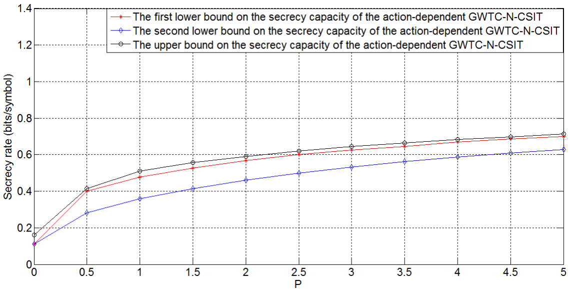

Fig. 12. Bounds on the secrecy capacity of the action-dependent GWTC-N-CSIT for $P_A = 1$, $\sigma_w^2 = 1$, $\sigma_1^2 = 3$, $\sigma_2^2 = 10$ and P taking values in $[0, 5]$.

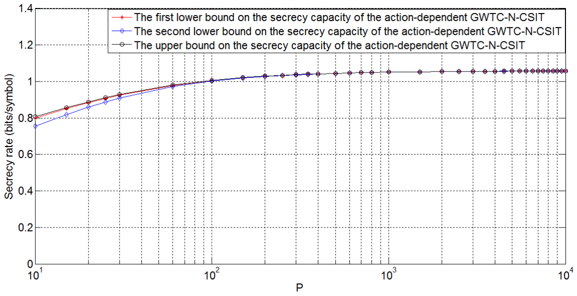

Fig. 13. Bounds on the secrecy capacity of the action-dependent GWTC-N-CSIT for $P_A = 1$, $\sigma_w^2 = 1$, $\sigma_1^2 = 3$, $\sigma_2^2 = 10$ and P taking values in $[10, 10000]$.

Since $h(X+S+\eta_1) - h(\eta_1) - \frac{1}{2}\log(2^{2h(X+S+\eta_1)} + 2^{2h(\eta_2)}) + h(\eta_1+\eta_2)$ in (4.28) is increasing while $h(X+S+\eta_1)$ is increasing, substituting (4.29) into (4.28), we obtain $\max(I(X,S;Y) - I(X,S;Z)) = L_2$. The proof is completed. ■

The following Figures 12 and 13 plot the bounds on $\mathcal{C}_{sag}$ for $P_A = 1$, $\sigma_w^2 = 1$, $\sigma_1^2 = 3$ and $\sigma_2^2 = 10$. It is easy to see that the first lower bound is tighter than the second one. Moreover, from Figure 13, we see that the lower bounds on $\mathcal{C}_{sag}$ meet the corresponding upper bound when the power P is sufficiently large, and this is because the upper and lower bounds on $\mathcal{C}_{sag}$ approaches the same limit $\frac{1}{2}\log\frac{\sigma_1^2+\sigma_2^2}{\sigma_1^2}$ when the power P goes to infinity, see Corollary 2.

In addition, the following Figure 14 plots the bounds on $\mathcal{C}_{sag}$ for $P_A = 5$, $\sigma_w^2 = 0$, $\sigma_1^2 = 3$, $\sigma_2^2 = 3$ and P taking values in $[0, 0.1]$. For this case, it is easy to see that the second lower bound is tighter than the first one.

The following Corollaries 2-4 show that for some special cases, the gap between the above lower and upper bounds on $\mathcal{C}_{sag}$ can be eliminated or be bounded by a constant value.

Corollary 2: For $P \to \infty$, we have

$$\lim_{P\to\infty} R_{sag}^{*} = \lim_{P\to\infty} R_{sag}^{**} = \lim_{P\to\infty} \mathcal{C}_{sag}^{upper} = \frac{1}{2}\log\frac{\sigma_1^2+\sigma_2^2}{\sigma_1^2}, \tag{4.31}$$

which indicates that the secrecy capacity $\mathcal{C}_{sag}$ tends to $\frac{1}{2}\log\frac{\sigma_1^2+\sigma_2^2}{\sigma_1^2}$ as $P \to \infty$.

Proof: This result follows by calculating the bounds R_{sag}^{*}, R_{sag}^{**} and $\mathcal{C}_{sag}^{upper}$ for $P \to \infty$. ■

Corollary 3: For $P = 0$, the first lower bound R_{sag}^{*} is invalid since it equals $-\infty$, and the gap between the second lower bound R_{sag}^{**} and the upper bound $\mathcal{C}_{sag}^{upper}$ is a constant value and it is given by

$$\mathcal{C}_{sag}^{upper} - R_{sag}^{**} = \begin{cases} \frac{1}{2}\log\left(1 + \frac{P_A}{\sigma_w^2+\sigma_1^2+\sigma_2^2}\right), & 0 \le P_A \le \frac{\sigma_2^2\sigma_w^2}{\sigma_1^2}, \\ \frac{1}{2}\log\left(1 + \frac{\sigma_2^2\sigma_w^2}{\sigma_1^2(\sigma_w^2+\sigma_1^2+\sigma_2^2)}\right), & P_A \ge \frac{\sigma_2^2\sigma_w^2}{\sigma_1^2}. \end{cases} \tag{4.32}$$

$$R_{sag}^{*} = \max_{\alpha,\gamma,\delta,\beta} \min\left\{\frac{1}{2}\log\frac{P_A\delta^2(P-\alpha^2P_A-\gamma^2\sigma_w^2)}{L_{A|Y}L_{U|A,Y}}, \frac{1}{2}\log\frac{L_{A|Z}L_{U|A,Z}}{L_{A|Y}L_{U|A,Y}}\right\}, \tag{4.14}$$

$$L_{A|Y} = P_A - \frac{(1+\alpha)^2(P_A)^2}{(1+2\alpha)P_A + (1+2\gamma)\sigma_w^2 + P + \sigma_1^2}, \tag{4.15}$$

$$L_{A|Z} = P_A - \frac{(1+\alpha)^2(P_A)^2}{(1+2\alpha)P_A + (1+2\gamma)\sigma_w^2 + P + \sigma_1^2 + \sigma_2^2}, \tag{4.16}$$

$$\begin{aligned} L_{U|A,Y} = {} & (1+\alpha\delta)^2P_A + (\gamma\delta+\beta)^2\sigma_w^2 + \delta^2(P-\alpha^2P_A-\gamma^2\sigma_w^2) \\ & - \frac{(1+\alpha\delta)^2P_A((1+2\alpha)P_A + (1+2\gamma)\sigma_w^2 + P + \sigma_1^2) + B^2 - 2(1+\alpha)(1+\alpha\delta)P_AB}{P-\alpha^2P_A+(1+2\gamma)\sigma_w^2+\sigma_1^2}, \end{aligned} \tag{4.17}$$

$$\begin{aligned} L_{U|A,Z} = {} & (1+\alpha\delta)^2P_A + (\gamma\delta+\beta)^2\sigma_w^2 + \delta^2(P-\alpha^2P_A-\gamma^2\sigma_w^2) \\ & - \frac{(1+\alpha\delta)^2P_A((1+2\alpha)P_A + (1+2\gamma)\sigma_w^2 + P + \sigma_1^2 + \sigma_2^2) + B^2 - 2(1+\alpha)(1+\alpha\delta)P_AB}{P-\alpha^2P_A+(1+2\gamma)\sigma_w^2+\sigma_1^2+\sigma_2^2}, \end{aligned} \tag{4.18}$$

$$B = (1+\alpha)(1+\alpha\delta)P_A + (1+\gamma)(\beta+\gamma\delta)\sigma_w^2 + \delta(P-\alpha^2P_A-\gamma^2\sigma_w^2). \tag{4.19}$$

Authorized licensed use limited to: Technion Israel Institute of Technology. Downloaded on May 24,2020 at 05:32:54 UTC from IEEE Xplore. Restrictions apply.

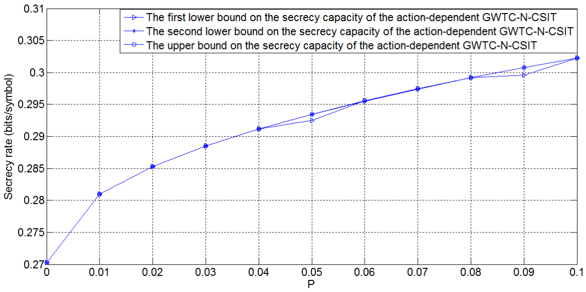

Fig. 14. Bounds on the secrecy capacity of the action-dependent GWTC-N-CSIT for $P_A = 5$, $\sigma_w^2 = 0$, $\sigma_1^2 = 3$, $\sigma_2^2 = 3$ and P taking values in $[0, 0.1]$.

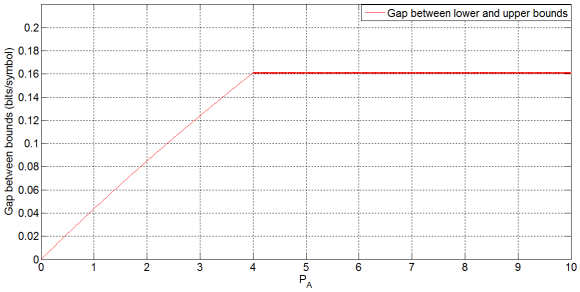

Fig. 15. The gap between the second lower bound R_{sag}^{**} and the upper bound $\mathcal{C}_{sag}^{upper}$ for $P = 0$, $\sigma_w^2 = 1$, $\sigma_1^2 = 3$, $\sigma_2^2 = 12$ and P_A taking values in $[0, 10]$.

Proof: Substituting $P = 0$ into R_{sag}^{**} and $\mathcal{C}_{sag}^{upper}$, we obtain

$$R_{sag}^{**} = \frac{1}{2}\log\left(1 + \frac{P_A}{\sigma_w^2 + \sigma_1^2}\right) - \frac{1}{2}\log\left(1 + \frac{P_A}{\sigma_w^2 + \sigma_1^2 + \sigma_2^2}\right), \tag{4.33}$$

From (4.33) and (4.34), shown at the bottom of the next page, we obtain the gap shown in (4.32), and the proof is completed. ■

The following Figure 15 plots the gap shown in Corollary 3 for $P = 0$, $\sigma_w^2 = 1$, $\sigma_1^2 = 3$, $\sigma_2^2 = 12$ and several values of P_A. It is easy to see that the gap increases as P_A increases. However, if P_A is larger than $\frac{\sigma_2^2\sigma_w^2}{\sigma_1^2}$, the gap is bounded by a constant value $\frac{1}{2}\log\left(1 + \frac{\sigma_2^2\sigma_w^2}{\sigma_1^2(\sigma_w^2+\sigma_1^2+\sigma_2^2)}\right)$.

Corollary 4: For $\sigma_w^2 = 0$, the second lower bound R_{sag}^{**} meets the upper bound $\mathcal{C}_{sag}^{upper}$, i.e., the secrecy capacity $\mathcal{C}_{sag}$ is determined and it is given by

$$\mathcal{C}_{sag} = \frac{1}{2}\log\left(1 + \frac{(\sqrt{P}+\sqrt{P_A})^2}{\sigma_1^2}\right) - \frac{1}{2}\log\left(1 + \frac{(\sqrt{P}+\sqrt{P_A})^2}{\sigma_1^2 + \sigma_2^2}\right). \tag{4.35}$$

Proof: First, substituting $\sigma_w^2 = 0$ into the upper bound $\mathcal{C}_{sag}^{upper}$, we have $\mathcal{C}_{sag}^{upper} = \min\{L_1, L_2\}$, where

$$\begin{aligned} L_1 = &\max_{(\rho_1,\rho_2):\rho_1^2+\rho_2^2\le 1} \frac{1}{2}\log\left(1 + \frac{P(1-\rho_1^2-\rho_2^2)}{\sigma_1^2}\right) \\ &+ \frac{1}{2}\log\left(1 + \frac{(\sqrt{P_A}+\rho_2\sqrt{P})^2}{P(1-\rho_1^2-\rho_2^2)+\rho_1^2P+\sigma_1^2}\right), \\ = &\max_{(\rho_1,\rho_2):\rho_1^2+\rho_2^2\le 1} \frac{1}{2}\log\left(\frac{P(1-\rho_1^2-\rho_2^2)+\sigma_1^2}{\sigma_1^2}\cdot\right. \\ &\left.\frac{P_A + 2\sqrt{P_A}\sqrt{P}\rho_2 + P + \sigma_1^2}{P(1-\rho_2^2)+\sigma_1^2}\right), \end{aligned} \tag{4.36}$$

for $-1 \le \rho_1 \le 0$, $0 \le \rho_2 \le 1$, and

$$L_2 = \frac{1}{2}\log\left(1 + \frac{(\sqrt{P}+\sqrt{P_A})^2}{\sigma_1^2}\right) - \frac{1}{2}\log\left(1 + \frac{(\sqrt{P}+\sqrt{P_A})^2}{\sigma_1^2 + \sigma_2^2}\right). \tag{4.37}$$

It is easy to see that L_1 in (4.36) achieves its maximum when $\rho_1 = 0$ and $\rho_2 = 1$, and hence we have

$$L_1 = \frac{1}{2}\log\left(1 + \frac{(\sqrt{P}+\sqrt{P_A})^2}{\sigma_1^2}\right). \tag{4.38}$$

Comparing L_1 with L_2, we can conclude that for $\sigma_w^2 = 0$, and we have

$$\mathcal{C}_{sag}^{upper} = \frac{1}{2}\log\left(1 + \frac{(\sqrt{P}+\sqrt{P_A})^2}{\sigma_1^2}\right) - \frac{1}{2}\log\left(1 + \frac{(\sqrt{P}+\sqrt{P_A})^2}{\sigma_1^2 + \sigma_2^2}\right). \tag{4.39}$$

Next, substituting $\sigma_w^2 = 0$ into the second lower bound R_{sag}^{**}, we have It is easy to see that R_{sag}^{**} in (4.40), shown at the bottom of the next page, achieves its maximum when $\rho_1 = 0$, and hence (4.40) can be re-written as (4.41), shown at the bottom of the next page, where (a) follows from the fact that R_{sag}^{**} achieves its maximum when $\rho_2 = 1$. Finally, comparing (4.41) with (4.39), we conclude that the secrecy capacity $\mathcal{C}_{sag}$ is determined, and the proof of Corollary 4 is completed. ■

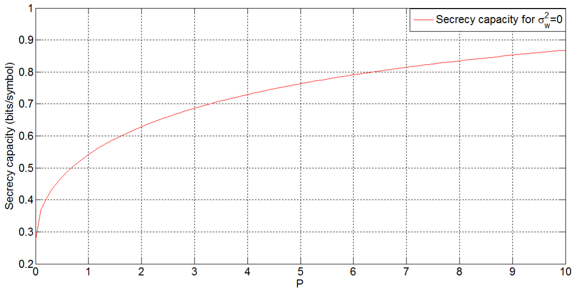

Fig. 16. The secrecy capacity $\mathcal{C}_{sag}$ for $\sigma_w^2 = 0$, $P_A = 2$, $\sigma_1^2 = 3$, $\sigma_2^2 = 12$ and P taking values in $[0, 10]$.

The following Figure 16 plots the secrecy capacity $\mathcal{C}_{sag}$ shown in Corollary 4 for $\sigma_w^2 = 0$, $P_A = 2$, $\sigma_1^2 = 3$, $\sigma_2^2 = 12$ and several values of P. It is easy to see that $\mathcal{C}_{sag}$ increases as the power P increases. However, we also note that as shown in Corollary 2, $\mathcal{C}_{sag}$ tends to $\frac{1}{2}\log\frac{\sigma_1^2+\sigma_2^2}{\sigma_1^2}$ as P approaches infinity.

Authorized licensed use limited to: Technion Israel Institute of Technology. Downloaded on May 24,2020 at 05:32:54 UTC from IEEE Xplore. Restrictions apply.

V. The Action-Dependent GWTC-N-CSIT With Noiseless Feedback

In this section, first, we introduce the classical SK feedback scheme [40] for the Gaussian channel, see Subsection V-A. Next, we show that the classical SK feedback scheme introduced in the preceding subsection may also achieve the secrecy capacity of the action-dependent GWTC-N-CSIT with noiseless feedback, see Subsection V-B.

A. The SK Scheme for the Gaussian Wiretap Channel With Noiseless Feedback

In this subsection, we first introduce the classical SK feedback scheme [40] for the Gaussian channel. Then, we show that such a feedback scheme also achieves the secrecy capacity of the Gaussian wiretap channel with noiseless feedback.

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

$$Y_i = X_i + \eta_i, \tag{5.1}$$

where X_i is the channel input subject to an average power constraint P, and $\eta_i \sim \mathcal{N}(0, \sigma^2)$ is the channel noise and is i.i.d. across the time index i. The i-th 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 $\mathcal{C}_g^f$ of the Gaussian channel with feedback equals the capacity of the Gaussian channel $\mathcal{C}_g$, i.e.,

$$\mathcal{C}_g^f = \mathcal{C}_g = \frac{1}{2}\log\left(1 + \frac{P}{\sigma^2}\right). \tag{5.2}$$

It has been shown that the classical SK scheme [40] achieves $\mathcal{C}_g^f$, which is described below.

The message M takes values in the set $\mathcal{M} = \{1, 2, \ldots, 2^{NR}\}$. 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,

$$X_1 = \theta\alpha \tag{5.3}$$

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

$$\hat{\theta}_1 = \frac{Y_1}{\alpha} = \theta + \frac{\eta_1}{\alpha} \tag{5.4}$$

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

$$X_i = \alpha_i(\theta - \hat{\theta}_{i-1}) = -\alpha_i \frac{\sum_{j=1}^{i-1} \alpha_j \eta_j}{\sum_{j=1}^{i-1} \alpha_j^2} \tag{5.5}$$

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

$$\hat{X}_i = \hat{\theta}_{i-1} + \frac{Y_i}{\alpha_i}, \tag{5.6}$$

$$\hat{\theta}_i = \frac{\sum_{j=1}^{i} \alpha_j^2 \hat{X}_j}{\sum_{j=1}^{i} \alpha_j^2} = \theta + \frac{\sum_{j=1}^{i} \alpha_j \eta_j}{\sum_{j=1}^{i} \alpha_j^2} \tag{5.7}$$

$$\mathcal{C}_{sag}^{upper} = \begin{cases} \frac{1}{2}\log\left(1 + \frac{P_A}{\sigma_w^2+\sigma_1^2}\right), & 0 \leq P_A \leq \frac{\sigma_2^2\sigma_w^2}{\sigma_1^2}, \\ \frac{1}{2}\log\left(1 + \frac{P_A+\sigma_w^2}{\sigma_1^2}\right) - \frac{1}{2}\log\left(1 + \frac{(P_A+\sigma_w^2}{\sigma_1^2+\sigma_2^2}\right), & P_A \geq \frac{\sigma_2^2\sigma_w^2}{\sigma_1^2}. \end{cases} \tag{4.34}$$

$$\begin{aligned} R_{sag}^{**} = & \max_{(\rho_1,\rho_2):\rho_1^2+\rho_2^2\leq 1} \frac{1}{2}\log\left(\frac{P(1-\rho_1^2-\rho_2^2)+\sigma_1^2}{\sigma_1^2} \cdot \frac{\sigma_1^2+\sigma_2^2}{P(1-\rho_1^2-\rho_2^2)+\sigma_1^2+\sigma_2^2}\right) \\ & + \frac{1}{2}\log\left(\frac{P+P_A+2\rho_2\sqrt{P}\sqrt{P_A}+\sigma_1^2}{P(1-\rho_2^2)+\sigma_1^2} \cdot \frac{P(1-\rho_2^2)+\sigma_1^2+\sigma_2^2}{P+P_A+2\rho_2\sqrt{P}\sqrt{P_A}+\sigma_1^2+\sigma_2^2}\right). \end{aligned} \tag{4.40}$$

$$\begin{aligned} R_{sag}^{**} &= \max_{0\leq\rho_2\leq 1} \frac{1}{2}\log\left(\frac{P(1-\rho_2^2)+\sigma_1^2}{\sigma_1^2} \cdot \frac{\sigma_1^2+\sigma_2^2}{P(1-\rho_2^2)+\sigma_1^2+\sigma_2^2}\right) \\ &\quad + \frac{1}{2}\log\left(\frac{P+P_A+2\rho_2\sqrt{P}\sqrt{P_A}+\sigma_1^2}{P(1-\rho_2^2)+\sigma_1^2} \cdot \frac{P(1-\rho_2^2)+\sigma_1^2+\sigma_2^2}{P+P_A+2\rho_2\sqrt{P}\sqrt{P_A}+\sigma_1^2+\sigma_2^2}\right) \\ &= \max_{0\leq\rho_2\leq 1} \frac{1}{2}\log\left(\frac{\sigma_1^2+\sigma_2^2}{\sigma_1^2} \cdot \frac{P+P_A+2\rho_2\sqrt{P}\sqrt{P_A}+\sigma_1^2}{P+P_A+2\rho_2\sqrt{P}\sqrt{P_A}+\sigma_1^2+\sigma_2^2}\right) \\ &\overset{(a)}{=} \frac{1}{2}\log\left(\frac{\sigma_1^2+\sigma_2^2}{\sigma_1^2} \cdot \frac{P+P_A+2\sqrt{P}\sqrt{P_A}+\sigma_1^2}{P+P_A+2\sqrt{P}\sqrt{P_A}+\sigma_1^2+\sigma_2^2}\right) \\ &= \frac{1}{2}\log\left(1 + \frac{(\sqrt{P}+\sqrt{P_A})^2}{\sigma_1^2}\right) - \frac{1}{2}\log\left(1 + \frac{(\sqrt{P}+\sqrt{P_A})^2}{\sigma_1^2+\sigma_2^2}\right), \end{aligned} \tag{4.41}$$

Authorized licensed use limited to: Technion Israel Institute of Technology. Downloaded on May 24,2020 at 05:32:54 UTC from IEEE Xplore. Restrictions apply.

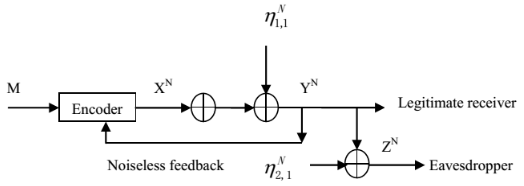

Fig. 17. The Gaussian wiretap channel with noiseless feedback.

as an estimation of θ at time i. In [40], it has been shown that the decoding error probability P_e (i.e., the probability that $\hat{\theta}_N$ does not belong to the sub-interval of the choosing message M) of this proposed scheme *doubly exponentially decays to zero* for sufficiently large N and $R \leq \frac{1}{2}\log(1+\frac{P}{\sigma^2})$.

The Gaussian wiretap channel with noiseless feedback is shown in Figure 17. At time i ($i \in \{1, 2, \ldots, N\}$), the channel input and outputs satisfy

$$Y_i = X_i + \eta_{1,i}, \quad Z_i = X_i + \eta_{1,i} + \eta_{2,i}, \qquad (5.8)$$

where X_i is the channel input with the power constraint P, Y_i and Z_i are the 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 independent channel noises and are i.i.d. across the time index i. The i-th channel input X_i is a stochastic function of the message M and the channel feedback Y^{i-1}. The following Theorem 8 [39] shows that the above proposed scheme also achieves the secrecy capacity $\mathcal{C}_{g-wtc}^f$ of the Gaussian wiretap channel with noiseless feedback.

Theorem 8 ([39]): The secrecy capacity $\mathcal{C}_{g-wtc}^f$ of the Gaussian wiretap channel with noiseless feedback is given by

$$\mathcal{C}_{g-wtc}^f = \frac{1}{2}\log\left(1 + \frac{P}{\sigma_1^2}\right). \qquad (5.9)$$

The converse is obvious since $\mathcal{C}_{g-wtc}^f$ can not exceed the capacity $\mathcal{C}_g^f$ of the Gaussian channel with feedback. For the direct part, it has been shown that the above proposed SK scheme achieves $\mathcal{C}_{g-wtc}^f$, and this is because the information leakage occurs only in the first transmission (see (5.3) and (5.5)), which leads to the leakage rate vanishes as the codeword length tends to infinity.

In the next subsection, we show that the SK scheme introduced in this subsection may also achieve the secrecy capacity of the action-dependent GWTC-N-CSIT with noiseless feedback.

B. Capacity Results on the Action-Dependent GWTC-N-CSIT With Noiseless Feedback

In this subsection, we derive lower and upper bounds on the secrecy capacity $\mathcal{C}_{sag}^f$ of the action-dependent GWTC-N-CSIT with noiseless feedback (see Subsection II-B), and show that the corresponding upper bound is capacity-achieving for a special case. The detail about these capacity results is given in the remainder of this subsection.

First, recall that in Subsection IV-A, it has been shown that the capacity $\mathcal{C}_{ag}$ of the action-dependent dirty paper channel is given by

$$\begin{aligned}\mathcal{C}_{ag} \;&=\; \max_{(\rho_1,\rho_2):\rho_1^2+\rho_2^2\leq 1} \frac{1}{2}\log\left(1 + \frac{P(1-\rho_1^2-\rho_2^2)}{\sigma_1^2}\right) \\ &\quad + \frac{1}{2}\log\left(1 + \frac{(\sqrt{P_A}+\rho_2\sqrt{P})^2}{P(1-\rho_1^2-\rho_2^2)+(\sigma_w+\rho_1\sqrt{P})^2+\sigma_1^2}\right), \end{aligned} \qquad (5.10)$$

where $-1 \leq \rho_1 \leq 0$ and $0 \leq \rho_2 \leq 1$. The following Theorem 9 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 (5.10).

Theorem 9: Suppose that the pair (ρ_1^*, ρ_2^*) achieves $\mathcal{C}_{ag}$, and define

$$L = \frac{1}{2}\log\left(1 + \frac{(\sqrt{P_A}+\rho_2^*\sqrt{P})^2}{P(1-\rho_1^{*2}-\rho_2^{*2})+(\sigma_w+\rho_1^*\sqrt{P})^2+\sigma_1^2}\right). \qquad (5.11)$$

If $\rho_1^{*2}+\rho_2^{*2} = 1$, then

$$\mathcal{C}_{sag}^f = \mathcal{C}_{ag} = L = \frac{1}{2}\log\left(1 + \frac{(\sqrt{P_A}+\rho_2^*\sqrt{P})^2}{(\sigma_w+\rho_1^*\sqrt{P})^2+\sigma_1^2}\right). \qquad (5.12)$$

Otherwise, if $\rho_1^{*2}+\rho_2^{*2} < 1$, then

$$L \leq \mathcal{C}_{sag}^f \leq \mathcal{C}_{ag} = L + \frac{1}{2}\log\left(1 + \frac{P(1-\rho_1^{*2}-\rho_2^{*2})}{\sigma_1^2}\right). \qquad (5.13)$$

Remark 3: From Theorem 9, 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 $\mathcal{C}_{ag} = \frac{1}{2}\log\left(1+\frac{(\sqrt{P_A}+\rho_2^*\sqrt{P})^2}{(\sigma_w+\rho_1^*\sqrt{P})^2+\sigma_1^2}\right)$, 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 $\mathcal{C}_{ag} = \frac{1}{2}\log\left(1+\frac{P(1-\rho_1^{*2}-\rho_2^{*2})}{\sigma_1^2}\right) + \frac{1}{2}\log\left(1+\frac{(\sqrt{P_A}+\rho_2^*\sqrt{P})^2}{P(1-\rho_1^{*2}-\rho_2^{*2})+(\sigma_w+\rho_1^*\sqrt{P})^2+\sigma_1^2}\right)$ 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 [10], 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

$$X = \frac{\rho_2^*\sqrt{P}}{\sqrt{P_A}}A + \frac{\rho_1^*\sqrt{P}}{\sigma_w}W. \qquad (5.14)$$

Substituting (5.14) and $S = A + W$ into $Y = X + S + \eta_1$ and $Z = X + S + \eta_1 + \eta_2$, we have

$$\begin{aligned} Y &= X + S + \eta_1 \\ &= (1 + \frac{\rho_2^*\sqrt{P}}{\sqrt{P_A}})A + (1 + \frac{\rho_1^*\sqrt{P}}{\sigma_w})W + \eta_1, \end{aligned} \qquad (5.15)$$

Authorized licensed use limited to: Technion Israel Institute of Technology. Downloaded on May 24,2020 at 05:32:54 UTC from IEEE Xplore. Restrictions apply.

and

$$Z = (1 + \frac{\rho_2^* \sqrt{P}}{\sqrt{P_A}})A + (1 + \frac{\rho_1^* \sqrt{P}}{\sigma_w})W + \eta_1 + \eta_2. \quad (5.16)$$

The equations (5.15) and (5.16) indicate that the action-dependent GWTC-N-CSIT with feedback is equivalent to the Gaussian wiretap channel with feedback shown in Subsection V-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 $i \in \{2, 3, \ldots, N\}$, and along the lines of the SK scheme introduced in Subsection V-A, the rate

$$\begin{aligned} R &= \frac{1}{2}\log\left(1 + \frac{P^{'}}{\sigma_1^{'2}}\right) \\ &= \frac{1}{2}\log\left(1 + \frac{(\sqrt{P_A} + \rho_2^* \sqrt{P})^2}{(\sigma_w + \rho_1^* \sqrt{P})^2 + \sigma_1^2}\right) \\ &= \mathcal{C}_{ag} \end{aligned} \quad (5.17)$$

is achievable with weak perfect secrecy.

On the other hand, 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

$$Y = (1 + \frac{\rho_2^* \sqrt{P}}{\sqrt{P_A}})A + (1 + \frac{\rho_1^* \sqrt{P}}{\sigma_w})W + G + \eta_1, \quad (5.18)$$

and

$$Z = (1 + \frac{\rho_2^* \sqrt{P}}{\sqrt{P_A}})A + (1 + \frac{\rho_1^* \sqrt{P}}{\sigma_w})W + G + \eta_1 + \eta_2. \quad (5.19)$$

Similarly, (5.18) and (5.19) imply 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 $i \in \{2, 3, \ldots, N\}$, and along the lines of the SK scheme introduced in Subsection V-A, the rate

$$\begin{aligned} R &= \frac{1}{2}\log(1 + \frac{P^{''}}{\sigma_1^{''2}}) \\ &= \frac{1}{2}\log\left(1 + \frac{(\sqrt{P_A} + \rho_2^* \sqrt{P})^2}{P(1 - \rho_1^{*2} - \rho_2^{*2}) + (\sigma_w + \rho_1^* \sqrt{P})^2 + \sigma_1^2}\right) \end{aligned} \quad (5.20)$$

is achievable with weak perfect secrecy. The proof is completed. ■

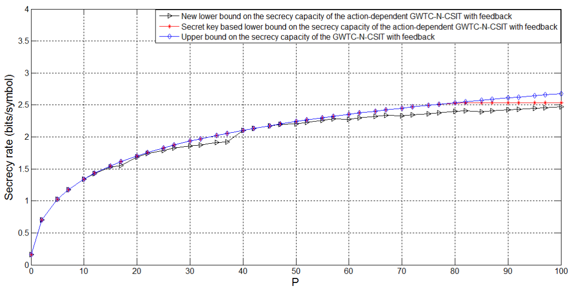

Fig. 18. Bounds on $\mathcal{C}_{sag}^f$ for $P_A = 1$, $\sigma_w^2 = 1$, $\sigma_1^2 = 3$, $\sigma_2^2 = 2$ and P taking values in $[0, 100]$.

The following Corollary 5 provides an already existing secret key based lower bound R_{sag}^{*f} on $\mathcal{C}_{sag}^f$.

Corollary 5: A lower bound R_{sag}^{*f} on the secrecy capacity $\mathcal{C}_{sag}^f$ of the action-dependent GWTC-N-CSIT with noiseless feedback is given by

$$R_{sag}^{*f} = \min\left\{\mathcal{C}_{ag}, \frac{1}{2}\log\left(\frac{2\pi e \sigma_2^2 (P + P_A + \sigma_w^2 + \sigma_1^2)}{P + P_A + \sigma_w^2 + \sigma_1^2 + \sigma_2^2}\right)\right\}. \quad (5.21)$$

Proof: In [33], [37], the discrete memoryless case of the action-dependent GWTC-N-CSIT with noiseless feedback, i.e., the physically degraded action-dependent wiretap channel with channel feedback and noncausal state information at the transmitter, was studied. It has been shown that the secrecy capacity of this discrete memoryless model can be achieved by using the secret key based feedback strategy, and the secrecy capacity $\mathcal{C}_{sa}^f$ is given by

$$\begin{aligned} &\mathcal{C}_{sa}^f \\ &= \max_{P(x|u,s), P(u|a,s), P(a)} \min\{I(U;Y) - I(U;S|A), H(Y|Z)\}, \end{aligned} \quad (5.22)$$

where the joint distribution satisfies

$$\begin{aligned} &P(u, a, s, x, y, z) \\ &= P(z|y)P(y|x, s)P(x|u, s)P(u|a, s)P(s|a)P(a). \end{aligned} \quad (5.23)$$

However, we should note that the capacity formula in (5.22) is only an achievable secrecy rate for the action-dependent GWTC-N-CSIT with noiseless feedback, and the reason is exactly the same as that in the proof of Corollary 1. Now substituting $A \sim \mathcal{N}(0, P_A)$, $X \sim \mathcal{N}(0, P)$, $U = X + \beta(A + W)$, $S = A + W$, $Y = X + S + \eta_1$ and $Z = X + S + \eta_1 + \eta_2$ (see (2.6)) into (5.22) and maximizing β, the lower bound

Authorized licensed use limited to: Technion Israel Institute of Technology. Downloaded on May 24,2020 at 05:32:54 UTC from IEEE Xplore. Restrictions apply.

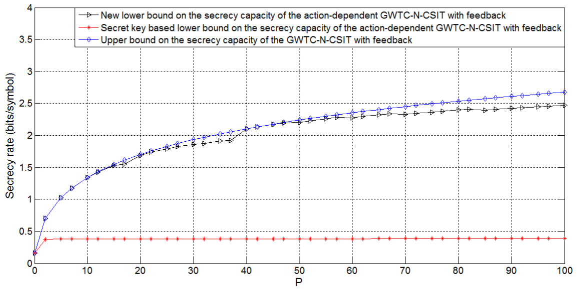

Fig. 19. Bounds on $\mathcal{C}_{sag}^{f}$ for $P_A = 1$, $\sigma_w^2 = 1$, $\sigma_1^2 = 3$, $\sigma_2^2 = 0.1$ and P taking values in $[0, 100]$.

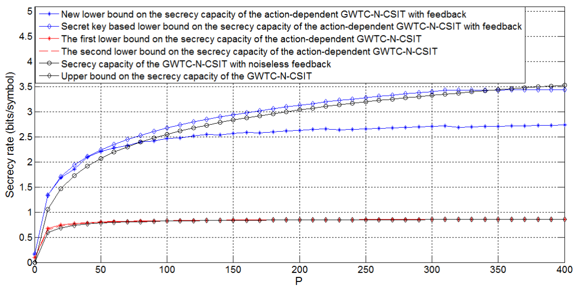

Fig. 20. Comparison of the lower bounds on the secrecy capacities of the GWTC-N-CSIT with or without action-dependent state and channel feedback for $P_A = 1$, $\sigma_w^2 = 1$, $Q = P_A + \sigma_w^2 = 2$, $\sigma_1^2 = 3$, $\sigma_2^2 = 7$ and P taking values in $[0, 400]$.

R_{sag}^{*f} on the secrecy capacity $\mathcal{C}_{sag}^{f}$ is obtained. The proof of Corollary 5 is completed. ■

For $P_A = 1$, $\sigma_w^2 = 1$, $\sigma_1^2 = 3$ and P taking values in $[0, 100]$, the following Figures 18 and 19 plot the lower and upper bounds on $\mathcal{C}_{sag}^{f}$ with $\sigma_2^2 = 2$ and $\sigma_2^2 = 0.1$, respectively. It is easy to see that our new lower bound is tighter than the secret key based lower bound when σ_2^2 is sufficiently small.

Figure 20 plots the lower bounds on $\mathcal{C}_{sag}^{f}$, lower bounds on the secrecy capacity of the action-dependent GWTC-N-CSIT, the secrecy capacity of the GWTC-N-CSIT with noiseless feedback and the upper bound on the secrecy capacity of the GWTC-N-CSIT for $P_A = 1$, $\sigma_w^2 = 1$, $Q = P_A + \sigma_w^2 = 2$, $\sigma_1^2 = 3$, $\sigma_2^2 = 7$ and P taking values in $[0, 400]$. From Figure 20, we see that the secrecy capacity of the GWTC-N-CSIT is enhanced by all three strategies, i.e., action on the state, channel feedback and a combination of the two. Note that a combination of action on the state and channel feedback (with more resources available to the encoder) should perform always better than either of them. However, from Figure 20, we see that the lower bounds on $\mathcal{C}_{sag}^{f}$ are not always larger than the lower bounds on the secrecy capacity of the action-dependent GWTC-N-CSIT and the secrecy capacity of the GWTC-N-CSIT with noiseless feedback, which indicates that the lower bounds on $\mathcal{C}_{sag}^{f}$ are not tight. Moreover, note that when P is sufficiently large, the lower bounds on the secrecy capacity of the action-dependent GWTC-N-CSIT meets the upper bound on the secrecy capacity of the GWTC-N-CSIT, and this is because all of them tend to $\frac{1}{2}\log\frac{\sigma_1^2+\sigma_2^2}{\sigma_1^2}$ when the power P tends to infinity.

VI. Conclusion

This paper focuses on studying the impact of action-dependent state and channel feedback on the GWTC-N-CSIT. Three strategies including action on the state, channel feedback and a combination of the two are shown to be useful in enhancing the secrecy capacity of the GWTC-N-CSIT. The highlight of this work includes two aspects: First, we determine the secrecy capacity of the GWTC-N-CSIT with noiseless feedback. Second, we propose a capacity-achieving scheme for a special case of the action-dependent GWTC-N-CSIT with noiseless feedback. However, we should notice that all the capacity results given in this paper only work well under the perfect weak secrecy condition, and how to design the corresponding encoding-decoding schemes under the strong perfect secrecy condition is of further interest to us. Another possible future work of this paper is to investigate the impact of fading on the GWTC-N-CSIT with or without action-dependent state and channel feedback. To be specific, [46], [47] studied the fading dirty paper channel with fading process perfectly known at the receiver, but either partially or completely not known at the transmitter. Using Costa's dirty paper coding (DPC) [5], [46], [47] determined the channel capacities for some special cases. However, we note that for the GWTC-N-CSIT (the dirty paper channel with an eavesdropper), [19] showed that the DPC is not optimal. Hence directly applying the DPC to fading cases of GWTC-N-CSIT with or without action-dependent state may not be optimal, and exploiting the optimal coding schemes is a challenging future work. Moreover, for the fading cases of GWTC-N-CSIT with channel feedback, it is worth exploring whether the modified SK scheme proposed in [6] is still optimal. If not, how to design the optimal feedback scheme involved with fading process is another challenging future work.

Appendix A
Proof of Theorem 2

The achievability of R_{sa}^{*} is proved by combining the binning scheme for the action-dependent channel [10] and the classical random binning scheme for the wiretap channel [12], and the detail of the proof is given below.

- The message M takes values in $\{1, 2, \ldots, 2^{NR}\}$.
- Randomly generate $2^{N(R+R^{''})}$ i.i.d. action sequences A^N w.r.t. $P(a)$, and index them as $a^N(m, m^{''})$, where $m \in \{1, 2, \ldots, 2^{NR}\}$ and $m^{''} \in \{1, 2, \ldots, 2^{NR^{''}}\}$.
- Randomly generate $2^{N(R+R^{*}+R^{'})}$ i.i.d. codewords U^N w.r.t. $P(u|a, s)$, and index them as $u^N(m, m^{*}, m^{'})$, where $m \in \{1, 2, \ldots, 2^{NR}\}$, $m^{*} \in \{1, 2, \ldots, 2^{NR^{*}}\}$ and $m^{'} \in \{1, 2, \ldots, 2^{NR^{'}}\}$.
- *Encoding procedure*:
  - Suppose that the message m is intended for transmission. Randomly choose an index $m^{''}$ in its alphabet set $\{1, 2, \ldots, 2^{NR^{''}}\}$ and select $a^N(m, m^{''})$ as the corresponding action sequence.
  - Let s^N be the state sequence produced by the DMC $A^N \rightarrow S^N$ with channel input $a^N(m, m^{''})$.

Authorized licensed use limited to: Technion Israel Institute of Technology. Downloaded on May 24,2020 at 05:32:54 UTC from IEEE Xplore. Restrictions apply.

  - Uniformly choose an index $m^{'}$, and for given $a^N(m,m^{''})$ and s^N, select an index m^* such that $(u^N(m,m^*,m^{'}),a^N(m,m^{''}),s^N)$ are jointly typical. If no such m^* exists, declare an encoding error. If multiple m^* exist, randomly pick out one. Based on the Covering Lemma [45], the encoding error tends to zero if

$$R^* > I(U;S|A). \tag{A1}$$

  - For given u^N and s^N, the channel input x^N is i.i.d. generated w.r.t. $P(x|u,s)$.

- *Decoding procedure*: once the legitimate receiver receives y^N, he seeks unique $a^N(\hat{m},\hat{m}^{''})$ and $u^N(\hat{m},\hat{m}^*,\hat{m}^{'})$ jointly typical with y^N. If there is more than one or no such a^N and u^N, a decoding error occurs. Based on the Packing Lemma [45] and a similar argument in [10], the decoding error tends to zero if

$$R+R^*+R^{'}+R^{''} < I(U;Y). \tag{A2}$$

Equivocation analysis:

$$\begin{aligned}
\Delta &= \frac{1}{N}H(M|Z^N) = \frac{1}{N}(H(M,Z^N)-H(Z^N))\\
&= \frac{1}{N}(H(M,Z^N,U^N)-H(U^N|M,Z^N)-H(Z^N))\\
&\overset{(1)}{=} \frac{1}{N}(H(Z^N|U^N)+H(U^N)\\
&\quad -H(U^N|M,Z^N)-H(Z^N))\\
&\overset{(2)}{\geq} R+R^*+R^{'}-\epsilon_1-I(U;Z)-\epsilon_2\\
&\quad -\frac{1}{N}H(U^N|M,Z^N)\\
&\overset{(3)}{\geq} R+R^*+R^{'}-I(U;Z)-\epsilon_1-\epsilon_2-\epsilon_3,
\end{aligned} \tag{A3}$$

where (1) follows from the Markov chain $M \rightarrow U^N \rightarrow Z^N$, (2) follows from a similar argument in [13, equations (16) and (23)], i.e., $\frac{1}{N}H(U^N) \geq R+R^*+R^{'}-\epsilon_1$ ($\epsilon_1 \rightarrow 0$ as $N \rightarrow \infty$) and follows from a similar argument in [49, Lemma 3], i.e., $\frac{1}{N}I(U^N;Z^N) \leq I(U;Z)+\epsilon_2$ ($\epsilon_2 \rightarrow 0$ as $N \rightarrow \infty$), and (3) follows from the fact that given M and Z^N, the eavesdropper seeks a unique U^N jointly typical with Z^N, and from Packing Lemma [45], we know that the eavesdropper's decoding error tends to zero if

$$R^*+R^{'} \leq I(U;Z), \tag{A4}$$

then applying Fano's inequality, $\frac{1}{N}H(U^N|M,Z^N) \leq \epsilon_3$ is obtained, where $\epsilon_3 \rightarrow 0$ as $N \rightarrow \infty$. Here note that (A3) indicates that if

$$R^*+R^{'} \geq I(U;Z), \tag{A5}$$

choosing sufficiently large N such that $\epsilon_1+\epsilon_2+\epsilon_3 \leq \epsilon$, $\Delta \geq R-\epsilon$ is proved.

Finally using Fourier-Motzkin elimination to remove R^*, $R^{'}$ and $R^{''}$ from (A1), (A2), (A4) and (A5), Theorem 2 is proved. The proof of Theorem 2 is completed.

Appendix B
Proof of Theorem 3

For all achievable secrecy rate R, the proof of $R \leq I(U;Y)-I(U;S|A)$ follows directly from [10]. Now it remains to show that $R \leq I(X,S;Y)-I(X,S;Z)$, and the proof is given below.

$$\begin{aligned}
R-\epsilon &\overset{(1)}{\leq} \Delta = \frac{1}{N}H(M|Z^N)\\
&\leq \frac{1}{N}(I(M;Y^N|Z^N)+H(M|Y^N,Z^N))\\
&\overset{(2)}{\leq} \frac{1}{N}(I(M;Y^N|Z^N)+\delta(P_e))\\
&\overset{(3)}{\leq} \frac{1}{N}(I(X^N,S^N;Y^N|Z^N)+\delta(P_e))\\
&\overset{(4)}{=} \frac{1}{N}(I(X^N,S^N;Y^N)-I(X^N,S^N;Z^N)+\delta(P_e))\\
&\overset{(5)}{=} \frac{1}{N}\sum_{i=1}^{N}(H(Y_i|Y^{i-1})-H(Y_i|X_i,S_i)-H(Z_i|Z^{i-1})\\
&\quad +H(Z_i|X_i,S_i))+\frac{\delta(P_e)}{N}\\
&\overset{(6)}{\leq} \frac{1}{N}\sum_{i=1}^{N}(H(Y_i)-H(Y_i|X_i,S_i)-H(Z_i)\\
&\quad +H(Z_i|X_i,S_i))+\frac{\delta(P_e)}{N}\\
&\overset{(7)}{=} \frac{1}{N}\sum_{i=1}^{N}(H(Y_i|J=i)-H(Y_i|X_i,S_i,J=i)\\
&\quad -H(Z_i|J=i)+H(Z_i|X_i,S_i,J=i))+\frac{\delta(P_e)}{N}\\
&\overset{(8)}{=} H(Y_J|J)-H(Y_J|X_J,S_J,J)-H(Z_J|J)\\
&\quad +H(Z_J|X_J,S_J,J)+\frac{\delta(P_e)}{N}\\
&\overset{(9)}{\leq} H(Y_J)-H(Y_J|X_J,S_J)-H(Z_J)\\
&\quad +H(Z_J|X_J,S_J)+\frac{\delta(\epsilon)}{N}\\
&\overset{(10)}{=} I(X,S;Y)-I(X,S;Z)+\frac{\delta(\epsilon)}{N},
\end{aligned} \tag{A6}$$

where (1) follows from (2.4), (2) follows from the Fano's inequality, (3) follows from the fact that $H(M|X^N)=0$, (4) follows from the Markov chain $(X^N,S^N) \rightarrow Y^N \rightarrow Z^N$, (5) follows from the fact that the channels are discrete memoryless, (6) follows from the Markov chain $Z^{i-1} \rightarrow Y^{i-1} \rightarrow Y_i \rightarrow Z_i$, which implies that $H(Y_i|Y^{i-1})-H(Z_i|Z^{i-1}) \leq H(Y_i)-H(Z_i)$, (7) and (8) are from the fact that J is uniformly distributed over $\{1,2,\ldots,N\}$ and it is independent of X^N, S^N, Y^N and Z^N, (9) follows from $P_e \leq \epsilon$, the Markov chain $J \rightarrow (X_J,S_J) \rightarrow (Y_J,Z_J)$, and the Markov chain $J \rightarrow Y_J \rightarrow Z_J$ indicating that $H(Y_J|J)-H(Z_J|J) \leq H(Y_J)-H(Z_J)$, and (10) follows from the definitions $X \triangleq X_J$, $S \triangleq S_J$, $Y \triangleq Y_J$ and $Z \triangleq Z_J$. Letting $\epsilon \rightarrow 0$, $R \leq I(X,S;Y)-I(X,S;Z)$ is proved. Finally, note that the joint distribution (4.9) can be directly checked by the definitions $U \triangleq (M,Y^{J-1},S_{J+1}^N,A^N,J)$ and $A \triangleq A_J$ (see [10]). The proof of Theorem 3 is completed.

Authorized licensed use limited to: Technion Israel Institute of Technology. Downloaded on May 24,2020 at 05:32:54 UTC from IEEE Xplore. Restrictions apply.

APPENDIX C
PROOF OF THEOREM 4

For all achievable secrecy rate R, the proof of $R \leq I(U,K;Y) - I(U,K;S|A)$ and $R \leq I(U,K;Y) - I(U,K;S|A) - I(U;Z) + I(U;S|A)$ is given below. First, note that

$$R - \epsilon \overset{(1)}{\leq} \frac{1}{N}H(M) \leq \frac{1}{N}(I(M;Y^N) + \delta(\epsilon)), \tag{A7}$$

and

$$\begin{aligned} R - \epsilon &\overset{(2)}{\leq} \Delta = \frac{1}{N}H(M|Z^N) \leq \frac{1}{N}(I(M;Y^N|Z^N) + \delta(\epsilon)) \\ &\overset{(3)}{=} \frac{1}{N}(I(M;Y^N) - I(M;Z^N) + \delta(\epsilon)), \end{aligned} \tag{A8}$$

where (1) and (2) are from (2.4), and (3) follows from the Markov chain $M \rightarrow Y^N \rightarrow Z^N$.

The term $I(M;Y^N)$ in (A7) and (A8) can be further bounded by

$$\begin{aligned} &\frac{1}{N}I(M;Y^N) \overset{(4)}{=} \frac{1}{N}(I(M;Y^N) - I(M;S^N|A^N)) \\ &= \frac{1}{N}\sum_{i=1}^{N}(I(M;Y_i|Y^{i-1}) - I(M;S_i|S_{i+1}^N, A^N)) \\ &= \frac{1}{N}\sum_{i=1}^{N}(I(M,S_{i+1}^N,A^N;Y_i|Y^{i-1}) \\ &-I(S_{i+1}^N,A^N;Y_i|M,Y^{i-1}) - I(M,Y^{i-1};S_i|S_{i+1}^N,A^N) \\ &+I(Y^{i-1};S_i,A^N|M,S_{i+1}^N,A^N)) \\ &\overset{(5)}{=} \frac{1}{N}\sum_{i=1}^{N}(I(M,S_{i+1}^N,A^N;Y_i|Y^{i-1}) \\ &-I(M,Y^{i-1};S_i|S_{i+1}^N,A^N)) \\ &\overset{(6)}{=} \frac{1}{N}\sum_{i=1}^{N}(H(Y_i|Y^{i-1}) \\ &-H(Y_i|M,S_{i+1}^N,A^N,Y^{i-1},Z^{i-1}) \\ &-H(S_i|A_i) + H(S_i|S_{i+1}^N,A^N,M,Y^{i-1},Z^{i-1})) \\ &\overset{(7)}{=} H(Y_J|Y^{J-1},J) \\ &-H(Y_J|M,S_{J+1}^N,A^N,Y^{J-1},Z^{J-1},J) \\ &-H(S_J|A_J,J) + H(S_J|S_{J+1}^N,A^N,M,Y^{J-1},Z^{J-1},J), \end{aligned} \tag{A9}$$

where (4) follows from the Markov chain $M \rightarrow A^N \rightarrow S^N$, (5) follows from the Csisz*á*r's equality

$$\begin{aligned} &\sum_{i=1}^{N} I(S_{i+1}^N,A^N;Y_i|M,Y^{i-1}) \\ &= \sum_{i=1}^{N} I(Y^{i-1};S_i,A^N|M,S_{i+1}^N,A^N), \end{aligned} \tag{A10}$$

(6) follows from the Markov chains $Z^{i-1} \rightarrow (M,S_{i+1}^N,A^N,Y^{i-1}) \rightarrow Y_i$, $S_i \rightarrow A_i \rightarrow (A^{i-1},A_{i+1}^N,S_{i+1}^N)$ and $Z^{i-1} \rightarrow (S_{i+1}^N,A^N,M,Y^{i-1}) \rightarrow S_i$, and (7) follows from the fact that J is uniformly distributed over $\{1,2,\ldots,N\}$ and it is independent of M, A^N, S^N, Y^N and Z^N.

Analogously, the term $\frac{1}{N}I(M;Z^N)$ in (A8) can be further bounded by

$$\begin{aligned} &\frac{1}{N}I(M;Z^N) = \frac{1}{N}(I(M;Z^N) - I(M;S^N|A^N)) \\ &= \frac{1}{N}\sum_{i=1}^{N}(I(M;Z_i|Z^{i-1}) - I(M;S_i|S_{i+1}^N,A^N)) \\ &= \frac{1}{N}\sum_{i=1}^{N}(I(M,S_{i+1}^N,A^N;Z_i|Z^{i-1}) \\ &-I(S_{i+1}^N,A^N;Z_i|M,Z^{i-1}) \\ &-I(M,Z^{i-1};S_i|S_{i+1}^N,A^N)+I(Z^{i-1};S_i,A^N|M,S_{i+1}^N,A^N)) \\ &= \frac{1}{N}\sum_{i=1}^{N}(I(M,S_{i+1}^N,A^N;Z_i|Z^{i-1}) \\ &-I(M,Z^{i-1};S_i|S_{i+1}^N,A^N)) \\ &= \frac{1}{N}\sum_{i=1}^{N}(H(Z_i|Z^{i-1}) - H(Z_i|M,S_{i+1}^N,A^N,Z^{i-1}) \\ &-H(S_i|A_i) + H(S_i|S_{i+1}^N,A^N,M,Z^{i-1})) \\ &= H(Z_J|Z^{J-1},J) - H(Z_J|M,S_{J+1}^N,A^N,Z^{J-1},J) \\ &-H(S_J|A_J,J) + H(S_J|S_{J+1}^N,A^N,M,Z^{J-1},J). \end{aligned} \tag{A11}$$

Substituting (A9) into (A7), we get

$$\begin{aligned} &R - \epsilon \leq H(Y_J|Y^{J-1},J) \\ &-H(Y_J|M,S_{J+1}^N,A^N,Y^{J-1},Z^{J-1},J) - H(S_J|A_J,J) \\ &+H(S_J|S_{J+1}^N,A^N,M,Y^{J-1},Z^{J-1},J) + \frac{\delta(\epsilon)}{N} \\ &\leq H(Y_J) - H(Y_J|M,S_{J+1}^N,A^N,Y^{J-1},Z^{J-1},J) \\ &-H(S_J|A_J,J) + H(S_J|S_{J+1}^N,A^N,M,Y^{J-1},Z^{J-1},J) \\ &+\frac{\delta(\epsilon)}{N} \\ &\overset{(8)}{=} I(U,K;Y) - I(U,K;S|A) + \frac{\delta(\epsilon)}{N}, \end{aligned} \tag{A12}$$

where (8) follows from the definitions $U = (M,S_{J+1}^N,A^N,Z^{J-1},J)$, $K = Y^{J-1}$, $A = (A_J,J)$, and $S = S_J$. Letting $\epsilon \rightarrow 0$, $R \leq I(U,K;Y) - I(U,K;S|A)$ is proved.

Next, substituting (A9) and (A11) into (A8), we get

$$\begin{aligned} &R - \epsilon \leq H(Y_J|Y^{J-1},J) \\ &-H(Y_J|M,S_{J+1}^N,A^N,Y^{J-1},Z^{J-1},J) \\ &-H(S_J|A_J,J) + H(S_J|S_{J+1}^N,A^N,M,Y^{J-1},Z^{J-1},J) \\ &-H(Z_J|Z^{J-1},J) + H(Z_J|M,S_{J+1}^N,A^N,Z^{J-1},J) \\ &+H(S_J|A_J,J) - H(S_J|S_{J+1}^N,A^N,M,Z^{J-1},J) + \frac{\delta(\epsilon)}{N} \\ &\overset{(9)}{\leq} H(Y_J) - H(Y_J|M,S_{J+1}^N,A^N,Y^{J-1},Z^{J-1},J) \\ &-H(S_J|A_J,J) + H(S_J|S_{J+1}^N,A^N,M,Y^{J-1},Z^{J-1},J) \\ &-H(Z_J) + H(Z_J|M,S_{J+1}^N,A^N,Z^{J-1},J) \\ &+H(S_J|A_J,J) - H(S_J|S_{J+1}^N,A^N,M,Z^{J-1},J) + \frac{\delta(\epsilon)}{N} \\ &\overset{(10)}{=} I(U,K;Y) - I(U,K;S|A) - I(U;Z) + I(U;S|A) \\ &+\frac{\delta(\epsilon)}{N}, \end{aligned} \tag{A13}$$

Authorized licensed use limited to: Technion Israel Institute of Technology. Downloaded on May 24,2020 at 05:32:54 UTC from IEEE Xplore. Restrictions apply.

where (9) follows from the Markov chain $(Z^{J-1}, J) \rightarrow (Y^{J-1}, J) \rightarrow Y_J \rightarrow Z_J$, which indicates $H(Y_J|Y^{J-1}, J) - H(Z_J|Z^{J-1}, J) \leq H(Y_J) - H(Z_J)$, and (10) follows from the definitions $U = (M, S_{J+1}^N, A^N, Z^{J-1}, J)$, $K = Y^{J-1}$, $A = (A_J, J)$, and $S = S_J$. Letting $\epsilon \rightarrow 0$, $R \leq I(U, K; Y) - I(U, K; S|A) - I(U; Z) + I(U; S|A)$ is proved. Finally, note that the joint distribution (4.12) can be directly checked by the above definitions of U, K, A and S. The proof of Theorem 4 is completed.

References

[1] C. E. Shannon, "Channels with side information at the transmitter," *IBM J. Res. Dev.*, vol. 2, no. 4, pp. 289–293, Oct. 1958.

[2] N. V. Kuznetsov and B. S. Tsybakov, "Coding in memories with defective cells," *Probl. Control Inf. Theory*, vol. 10, no. 2, pp. 52–60, 1974.

[3] S. Gel'fand and M. Pinsker, "Coding for channel with random parameters," *Probl. Control Inf. Theory*, vol. 9, no. 1, pp. 19–31, 1980.

[4] T. Weissman and N. Merhav, "Coding for the feedback Gel'fand–Pinsker channel and the feedforward Wyner–Ziv source," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 4207–4211, Sep. 2006.

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

[6] N. Elia and J. Liu, "Writing on dirty paper with feedback," *Commun. Inf. Syst.*, vol. 5, no. 4, pp. 401–422, 2005.

[7] G. Caire and S. Shamai (Shitz), "Writing on dirty tape with LDPC codes," in *Proc. DIMACS Workshop Signal Process. Wireless Transmiss.* Camden, NJ, USA: Rutgers Univ., 2003, pp. 123–140.

[8] S. Borade and L. Zheng, "Writing on fading paper, dirty tape with little ink: Wideband limits for causal transmitter CSI," *IEEE Trans. Inf. Theory*, vol. 58, no. 8, pp. 5388–5397, Aug. 2012.

[9] U. Erez, S. Shamai (Shitz), and R. Zamir, "Capacity and lattice strategies for canceling known interference," *IEEE Trans. Inf. Theory*, vol. 51, no. 11, pp. 3820–3833, Nov. 2005.

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

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

[12] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[13] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[14] Y. Chen and A. J. Han Vinck, "Wiretap channel with side information," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 395–402, Jan. 2008.

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

[16] Y.-K. Chia and A. E. Gamal, "Wiretap channel with causal state information," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 2838–2849, May 2012.

[17] H. Fujita, "On the secrecy capacity of wiretap channels with side information at the transmitter," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 11, pp. 2441–2452, Nov. 2016.

[18] T. S. Han and M. Sasaki, "Wiretap channels with causal state information: Strong secrecy," *IEEE Trans. Inf. Theory*, vol. 65, no. 10, pp. 6750–6765, Oct. 2019.

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

[20] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.

[21] B. Dai, Z. Ma, and X. Fang, "Feedback enhances the security of state-dependent degraded broadcast channels with confidential messages," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 7, pp. 1529–1542, Jul. 2015.

[22] Q. Zhang, X. Huang, Q. Li, and J. Qin, "Cooperative jamming aided robust secure transmission for wireless information and power transfer in MISO channels," *IEEE Trans. Commun.*, vol. 63, no. 3, pp. 906–915, Mar. 2015.

[23] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.

[24] K.-H. Park, T. Wang, and M.-S. Alouini, "On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1741–1750, Sep. 2013.

[25] J. M. Liang, J. J. Chen, H. H. Cheng, and Y. C. Tseng, "An energy-efficient sleep scheduling with QoS consideration in 3GPP LTE-advanced networks for Internet of Things," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 3, no. 1, pp. 13–22, 2013.

[26] R. Ahlswede and N. Cai, "Transmission, identification and common randomness capacities for wire-tape channels with secure feedback from the decoder," in *General Theory of Information Transfer and Combinatorics* (Lecture Notes in Computer Science), vol. 4123. Berlin, Germany: Springer-Verlag, 2006, pp. 258–275.

[27] E. Ardestanizadeh, M. Franceschetti, T. Javidi, and Y.-H. Kim, "Wiretap channel with secure rate-limited feedback," *IEEE Trans. Inf. Theory*, vol. 55, no. 12, pp. 5353–5361, Dec. 2009.

[28] R. F. Schaefer, A. Khisti, and H. V. Poor, "Secure broadcasting using independent secret keys," *IEEE Trans. Commun.*, vol. 66, no. 2, pp. 644–661, Feb. 2018.

[29] E. Ekrem and S. Ulukus, "Secrecy capacity of a class of broadcast channels with an eavesdropper," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, pp. 1–29, Mar. 2009.

[30] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "The secrecy rate region of the broadcast channel," in *Proc. Allerton Conf. Commun., Control Computing*, 2008, pp. 1–12.

[31] A. Cohen and A. Cohen, "Wiretap channel with causal state information and secure rate-limited feedback," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1192–1203, Mar. 2016.

[32] X. Yin, X. Chen, and Z. Xue, "Wiretap channel with action-dependent states and rate-limited feedback," *Math. Probl. Eng.*, vol. 2013, pp. 1–19, Dec. 2013.

[33] B. Dai, A. J. Han Vinck, and Y. Luo, "Wiretap channel in the presence of action-dependent states and noiseless feedback," *J. Appl. Math.*, vol. 2013, pp. 1–17, Mar. 2013.

[34] B. Dai, Z. Ma, and Y. Luo, "Finite state Markov wiretap channel with delayed feedback," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 3, pp. 746–760, Mar. 2017.

[35] B. Dai, Z. Ma, M. Xiao, X. Tang, and P. Fan, "Secure communication over finite state multiple-access wiretap channel with delayed feedback," *IEEE J. Select. Areas Commun.*, vol. 36, no. 4, pp. 723–736, Apr. 2018.

[36] B. Dai and Y. Luo, "An improved feedback coding scheme for the wire-tap channel," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 1, pp. 262–271, Jan. 2019.

[37] H. Zhang, L. Yu, and B. Dai, "Feedback schemes for the action-dependent wiretap channel with noncausal state at the transmitter," *Entropy*, vol. 21, no. 3, p. 278, Mar. 2019.

[38] H. Zhang, L. Yu, C. Wei, and B. Dai, "A new feedback scheme for the state-dependent wiretap channel with noncausal state at the transmitter," *IEEE Access*, vol. 7, pp. 45594–45604, 2019.

[39] D. Gunduz, D. R. Brown, and H. V. Poor, "Secret communication with feedback," in *Proc. Int. Symp. Inf. Theory Appl.*, Dec. 2008, pp. 1–6.

[40] 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. IT-12, no. 2, pp. 172–182, Apr. 1966.

[41] C. Li, Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secrecy capacity of colored Gaussian noise channels with feedback," *IEEE Trans. Inf. Theory*, vol. 65, no. 9, pp. 5771–5782, Sep. 2019.

[42] G. Keshet, Y. Steinberg, and N. Merhav, "Channel coding in the presence of side information," *FNT Commun. Inf. Theory*, vol. 4, no. 6, pp. 445–586, 2008.

[43] B. Dai, A. Vinck, Y. Luo, and X. Tang, "Wiretap channel with action-dependent channel state information," *Entropy*, vol. 15, no. 2, pp. 445–473, Jan. 2013.

[44] C. Wei, L. Yu, and B. Dai, "Some new results on the Gaussian wiretap feedback channel," *Entropy*, vol. 21, no. 9, pp. 817–829, 2019.

[45] A. El Gamal and Y. Kim, *Network Information Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[46] C. S. Vaze and M. K. Varanasi, "Dirty paper coding for fading channels with partial transmitter side information," in *Proc. 42nd Asilomar Conf. Signals, Syst. Comput.*, Oct. 2008, pp. 341–345.

[47] W. Zhang, S. Kotagiri, and J. N. Laneman, "Writing on dirty paper with resizing and its application to quasi-static fading broadcast channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2007, pp. 381–385.

Authorized licensed use limited to: Technion Israel Institute of Technology. Downloaded on May 24,2020 at 05:32:54 UTC from IEEE Xplore. Restrictions apply.

[48] R. W. Yeung. *Differential Entropy*. [Online]. Available: http://www.inc.cuhk.edu.hk/InformationTheory/files/Abridged/Ch_10.pdf

[49] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, “Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.

Bin Dai received the B.Sc. degree in communications and information systems from the University of Electronic Science and Technology of China, Chengdu, China, in 2004, and the M.Sc. and Ph.D. degrees in computer science and technology from Shanghai Jiao Tong University, Shanghai, China, in 2007 and 2012, respectively. In 2011 and 2012, he was a Visiting Scholar with the Institute for Experimental Mathematics, Duisburg-Essen University, Essen, Germany. In 2018 and 2019, he was a Visiting Scholar with the Department of Electrical and Computer Engineering, Ohio State University (OSU), Columbus, USA. He is currently an Associate Professor with the Southwest Jiaotong University. His research interests include information-theoretic security and network information theory and coding.

Chong Li (Member, IEEE) received the B.E. degree in electrical engineering from the Harbin Institute of Technology and the Ph.D. degree in electrical engineering from Iowa State University. He was a Staff Research Engineer with Qualcomm. He is currently a Co-Founder with Nakamoto & Turing Labs, New York. He is also an Adjunct Assistant Professor with Columbia University, New York. He is a holder of more than 200 international/U.S. patents (granted and pending). He has been actively publishing papers on top ranking journals, including the PROCEEDINGS OF THE IEEE, the IEEE TRANSACTIONS ON INFORMATION THEORY, the *IEEE Communications Magazine*, and *Automatica*. He has authored the book *Reinforcement Learning for Cyber-physical Systems* (Taylor & Francis and CRC Press). He received MediaTek, Inc., & Wu Ta You Scholar Award from MediaTek, Inc., Rosenfeld International Scholarship and Research Excellent Award from Iowa State University. He has broad research interests including information theory, blockchain, machine learning, networked control and communications theory, and systems design for advance telecommunication technologies (5G and beyond). He has also served as a reviewer and a technical program committee member for most prestigious journals and conferences in communications and control societies.

Yingbin Liang (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from the University of Illinois at Urbana–Champaign in 2005. She served on the Faculty of University of Hawaii and Syracuse University before she joined OSU. She is currently a Professor with the Department of Electrical and Computer Engineering, The Ohio State University (OSU). Her research interests include machine learning, optimization, information theory, and statistical signal processing. She received the National Science Foundation CAREER Award and the State of Hawaii Governor Innovation Award in 2009. She also received EURASIP Best Paper Award for the *EURASIP Journal on Wireless Communications and Networking* in 2014. She served as an Associate Editor for the Shannon Theory of the IEEE TRANSACTIONS ON INFORMATION THEORY from 2013 to 2015.

Zheng Ma (Member, IEEE) received the B.Sc. and Ph.D. degrees in communications and information system from Southwest Jiaotong University in 2000 and 2006, respectively. He was a Visiting Scholar with the University of Leeds, U.K., in 2003. In 2003 and 2005, he was a Visiting Scholar with The Hong Kong University of Science and Technology. From 2008 to 2009, he was a Visiting Research Fellow with the Department of Communication Systems, Lancaster University, U.K. He is currently a Professor with Southwest Jiaotong University, and also serves as the Deputy Dean with the School of Information Science and Technology. His research interests include information theory and coding, signal design and applications, FPGA/DSP implementation, and professional mobile radio. He has authored more than 120 research articles in high-quality journals and conferences. He is currently the Area Editor of IEEE COMMUNICATIONS LETTERS. He is also the Vice-Chairman of Information Theory Chapter in the IEEE Chengdu Section. He received the Marie Curie Individual Fellowship in 2018.

Shlomo Shamai (Shitz) (Life Fellow, IEEE) received the B.Sc., M.Sc., and Ph.D. degrees in electrical engineering from the Technion—Israel Institute of Technology, in 1975, 1981, and 1986, respectively. From 1975 to 1985, he was with the Communications Research Labs, as a Senior Research Engineer. Since 1986, he has been with the Department of Electrical Engineering, Technion—Israel Institute of Technology, where he is currently a Technion Distinguished Professor, and holds the William Fondiller Chair of telecommunications. His research interests encompasses a wide spectrum of topics in information theory and statistical communications. Dr. Shamai (Shitz) is an URSI Fellow, a member of the Israeli Academy of Sciences and Humanities, and a Foreign Member of the U.S. National Academy of Engineering. He was a recipient of the 2011 Claude E. Shannon Award, the 2014 Rothschild Prize in Mathematics/Computer Sciences and Engineering, and the 2017 IEEE Richard W. Hamming Medal. He was also a co-recipient of the 2018 Third Bell Labs Prize for Shaping the Future of Information and Communications Technology. He has been awarded the 1999 van der Pol Gold Medal of the Union Radio Scientifique Internationale (URSI), and was also a co-recipient of the 2000 IEEE Donald G. Fink Prize Paper Award, the 2003 and 2004 joint IT/COM societies paper award, the 2007 IEEE Information Theory Society Paper Award, the 2009 and 2015 European Commission FP7, Network of Excellence in Wireless COMmunications (NEWCOM++, NEWCOM#) Best Paper Awards, the 2010 Thomson Reuters Award for International Excellence in Scientific Research, the 2014 EURASIP Best Paper Award (for the *EURASIP Journal on Wireless Communications and Networking*), the 2015 IEEE Communications Society Best Tutorial Paper Award and the 2018 IEEE Signal Processing Best Paper Award. He is listed as a Highly Cited Researcher (Computer Science) for the years 2013–2018. He was also a recipient of 1985 Alon Grant for Distinguished Young Scientists and the 2000 Technion Henry Taub Prize for Excellence in Research. He has served as an Associate Editor for the Shannon Theory of the IEEE TRANSACTIONS ON INFORMATION THEORY, and has also served twice on the Board of Governors of the Information Theory Society. He has also served on the Executive Editorial Board of the IEEE TRANSACTIONS ON INFORMATION THEORY, on the IEEE Information Theory Society Nominations and Appointments Committee and on the IEEE Information Theory Society, Shannon Award Committee.

Authorized licensed use limited to: Technion Israel Institute of Technology. Downloaded on May 24,2020 at 05:32:54 UTC from IEEE Xplore. Restrictions apply.