Self-Secure Capacity-Achieving Feedback Schemes of Gaussian Multiple-Access Wiretap Channels With Degraded Message Sets

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

***Abstract*— It has been shown that the SK scheme, which was proposed by Schalkwijk and Kailath, is a self-secure capacity-achieving (SSCA) feedback scheme for the Gaussian wiretap channel, i.e., the SK scheme not only achieves the feedback capacity of the Gaussian channel, but also is secure by itself and achieves the feedback secrecy capacity of the Gaussian wiretap channel. For the multi-user wiretap channels, very recently, it has been shown that Ozarow's capacity-achieving feedback scheme for the two-user Gaussian multiple-access channel (GMAC) is the SSCA feedback scheme for the two-user Gaussian multiple-access wiretap channel (GMAC-WT). In this paper, first, we propose a SSCA feedback scheme for the two-user GMAC-WT with degraded message sets (GMAC-WT-DMS). Next, we extend the above scheme to the two-user GMAC-WT-DMS with noncausal channel state information at the transmitters (NCSIT), and show that the extended scheme is also a SSCA feedback scheme. Finally, we derive outer bounds on the secrecy capacity regions of the two-user GMAC-WT-DMS with or without NCSIT, and numerical results show the rate gains by the feedback.**

Manuscript received November 24, 2021; revised March 7, 2022; accepted March 24, 2022. Date of publication April 7, 2022; date of current version April 29, 2022. This work was supported in part by the National Key Research and Development Program of China under Grant 2019YFB1803400 and Grant 2020YFB1806405; in part by the National Natural Science Foundation of China under Grant 62071392; in part by the Open Research Fund of the State Key Laboratory of Integrated Services Networks, Xidian University, under Grant ISN21-12; in part by the Central Government to Guide Local Scientific and Technological Development under Grant 2021ZYD0001; in part by the 111 Project under Grant 111-2-14; and in part by the Research Fund of the Peng Cheng Laboratory under Grant PCL2021A04. The work of Yingbin Liang was supported by the U.S. NSF under Grant CCF-1801846. The work of Shlomo Shamai was supported by the European Union's Horizon 2020 Research and Innovation Programme under Grant 694630. An earlier version of this paper was presented in the IEEE Information Theory Workshop (ITW) in April 2021 [DOI: 10.1109/ITW46852.2021.9457631]. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Rafael F. Schaefer. *(Corresponding author: Bin Dai.)*

Bin Dai is with the School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, China, also with the State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an, Shaanxi 710071, China, and also with the Peng Cheng Laboratory, Shenzhen 518055, China (e-mail: daibin@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).

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

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

Digital Object Identifier 10.1109/TIFS.2022.3164196

***Index Terms*— Degraded message sets, feedback, Gaussian multiple-access channel, noncausal channel state information, secrecy capacity region, wiretap channel.**

I. Introduction

The multiple-access channel (MAC), which characterizes the up-link of wireless communication, has received extensive attention in the literature. The capacity regions of MAC and Gaussian MAC (GMAC) were determined by [1] and [2], respectively. Unlike the well-known fact that feedback does not increase the capacity of a point-to-point discrete memoryless channel, [3], [4] found that feedback increases the capacity region of the MAC by proposing inner bounds on the capacity region of the MAC with feedback. The capacity region of the MAC with feedback remains open, and it is only determined for some special cases:

- For the two-user GMAC with feedback, Ozarow [5] proposed a hybrid scheme which combines the cooperative scheme in [3] and the Schalkwijk-Kailath (SK) scheme [6] for the point-to-point Gaussian channel with feedback, and showed that this scheme is capacity-achieving.[1] Subsequently, [7] investigated the two-user GMAC with feedback and noncausal channel state information at the transmitters (NCSIT), and showed that a variation of Ozarow's scheme [5] is capacity-achieving.
- For the two-user MAC with degraded message sets (DMS), where two independent messages are sent from two sources to a common destination, the uninformed encoder only has access to one message, while the informed encoder has access to both messages. Though it has already been shown that feedback does not increase the capacity region of the MAC with DMS (MAC-DMS) [8], [9] proposed a capacity-achieving scheme for the MAC-DMS with feedback, which is an extension of the posterior matching scheme for the point-to-point discrete memoryless channel with feedback [10].

The physical layer security (PLS), which captures the fundamental limit of secure transmission over communication channels, was first investigated by Wyner in his landmark

[1] Here note that for the N-user ($N \geq 3$) GMAC with feedback, the capacity region remains open.

paper on the wiretap channel (WTC) [11]. The secrecy capacities (channel capacities with perfect secrecy constraint) of the discrete memoryless WTC (DM-WTC) and the Gaussian WTC (G-WTC) was determined in [11], [12] and [13], respectively. In recent years, the PLS in multiple-access channels receives much attention. Specifically, [14] studied the two-user Gaussian multiple-access wiretap channel (GMAC-WT), and proposed an inner bound on the secrecy capacity region. [15] investigated arbitrarily varying MAC with strong secrecy constraint, and provided bounds on its secrecy capacity region. [16]–[18] studied variations of the MAC with secrecy constraint, and proposed bounds on the corresponding secrecy capacity regions. [19] proposed cooperative jamming schemes for the multiple-access wiretap channel (MAC-WT), which enhance the secrecy capacity region. [20] studied the MAC-WT with NCSIT, and provided bounds on its secrecy capacity region. [21] investigated the effect of feedback delay on the secrecy capacity of the finite state MAC-WT. [22] studied the secure relay schemes for the MAC-WT.

Channel feedback has been proved to be a useful tool to enhance the PLS in communication systems. Traditionally, the channel feedback is used for secret key agreement between legitimate parties [23]–[28]. Recently, [29] showed that the secrecy capacity of the G-WTC with feedback equals the capacity of the same model without secrecy constraint, and it is achieved by the classical SK scheme [6] which is not designed with the consideration of secrecy, i.e., the SK scheme is a self-secure capacity-achieving (SSCA[2]) feedback scheme for the G-WTC. Based on the surprising finding of [29], [30] and [31] respectively showed that variations of the classical SK scheme are also SSCA feedback schemes for the colored G-WTC and the G-WTC with NCSIT. Very recently, [32] showed that Ozarow's scheme [5] and its variation [7] are also SSCA feedback schemes for the two-user GMAC-WT with or without NCSIT.

Although the SSCA feedback schemes have been well studied in the Gaussian wiretap channels and the Gaussian multiple-access wiretap channels, such a topic remains open for the multiple-access wiretap channels with DMS.[3] In this paper, we focus on the two-user GMAC-WT with DMS, and with or without NCSIT, and study how to design SSCA feedback schemes for these models. We summarize our contribution as follows.

1) Since Ozarow's scheme is a SSCA feedback scheme for the two-user GMAC-WT [32], it is natural to ask: is this kind of scheme also be a SSCA feedback scheme for the two-user GMAC-WT with DMS (GMAC-WT-DMS)? Unfortunately, we find that though Ozarow's scheme is secure by itself, it *cannot* achieve the capacity region of the two-user GMAC with DMS (GMAC-DMS) and feedback, hence it is not a SSCA feedback scheme for the two-user GMAC-WT-DMS. In this paper, we propose a SSCA feedback scheme for the two-user GMAC-WT-DMS. The novelty of this new scheme is explained below.

In the two-user GMAC-DMS with feedback, since the informed encoder has access to both messages, we split this encoder into two parts, where one part encodes the message with rate R_2 as the codeword V^N, and the other part together with the uninformed encoder encode the message with rate R_1 as the codewords U^N and X_1^N. For the receiver, U^N and X_1^N are decoded first, and after successfully decoding U^N and X_1^N, the receiver subtracts them from his/her received signal and further decodes V^N.

Since U^N and X_1^N are known by the informed encoder, they can be perfectly canceled when the informed encoder encodes V^N, which indicates that for an equivalent channel model with single input V^N, the corresponding channel noise is the original white Gaussian noise η_1^N of the GMAC. Hence we directly apply the classical SK scheme [6] for the point-to-point white Gaussian channel with feedback to V^N, and from [29], we know that the coding scheme of V^N is SSCA. However, different from the encoding scheme of V^N, since V^N is not known by the uninformed encoder, for the encoding scheme of U^N and X_1^N, the noise of their equivalent channel is $V^N + \eta_1^N$, which is *non-white* Gaussian noise due to the reason that V^N is generated by classical SK scheme [6] and it is not independent identically distributed (i.i.d.) generated. In general, it is difficult to design a SSCA SK-type scheme for the *non-white* Gaussian channel. However, by letting the encoder of V^N work first (starting from time 1), and the encoder of U^N and X_1^N work later (starting from time 2), we find that the SK-type scheme of U^N and X_1^N is also SSCA, and the key step to the corresponding proof is Lemma 1 in Section III, i.e., for time instant $3 \le k \le N$, $E[\epsilon'_{k-1}\eta'_{1,k}] = 0$, where $\eta'_{1,k} = \eta_{1,k} + V_k$, $\eta_{1,k}$ and V_k are the k-th components of η_1^N and V^N, respectively, and ϵ'_{k-1} is a deterministic function of U_k and $X_{1,k}$, which are the k-th components of U^N and X_1^N, respectively. Here note that Lemma 1 is surprising and novel since both V_k and ϵ'_{k-1} depend on the previous noises $\eta_{1,1}, \ldots, \eta_{1,k-1}$. By using this surprising property in Lemma 1, we show that the two-step SK-type feedback scheme is SSCA for the two-user GMAC-WT-DMS.

2) We extend the above new feedback scheme to the two-user GMAC with NCSIT and DMS (GMAC-NCSIT-DMS), and show that this extended feedback scheme is also SSCA for the two-user GMAC-WT with NCSIT and DMS (GMAC-WT-NCSIT-DMS). The novelty of this new scheme is explained below.

In the previous two-step SK-type scheme for the two-user GMAC-DMS with feedback, after decoding one message W_1, the receiver knows U^N and X_1^N. Hence in the decoding of the other message W_2, the receiver directly subtracts U^N and X_1^N from his/her received signal and does a similar SK-type decoding to obtain W_2. However, in the two-user GMAC-NCSIT-DMS with feedback, since the receiver does not know the state interference, after decoding W_1, the receiver *cannot* obtain U^N and X_1^N, which leads to the failure of subtracting U^N and X_1^N from the receiver's received signal. Fortunately, we find that after decoding W_1, though the receiver only obtains partial information about U^N and X_1^N, by introducing

[2]In general, we say that a feedback scheme is SSCA if the feedback capacity of a channel model equals the feedback secrecy capacity of the same model with secrecy constraint, and both feedback capacities (with or without secrecy constraint) are achieved by the same scheme.

[3]In [9], a capacity-achieving feedback scheme is proposed for the MAC-DMS with feedback, but whether this scheme is self-secure or not remains unknown.

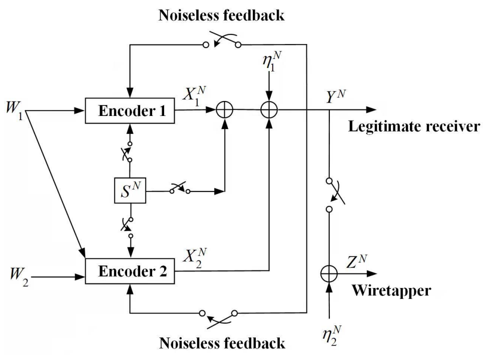

Fig. 1. The GMAC-DMS models studied in this paper.

proper offsets into the construction of V^N, U^N and X_1^N, the receiver's final estimations of the transmitted messages are the same as those in the previous two-step SK-type scheme for the GMAC-DMS with feedback, which indicates that this modified scheme is also a SSCA feedback scheme for the two-user GMAC-WT-NCSIT-DMS.

3) Outer bounds on the *secrecy* capacity regions of the GMAC-WT-DMS and the GMAC-WT-NCSIT-DMS are given, and numerical results show the rate gains by the feedback.

Throughout this paper, a random variable (RV) is denoted by an upper case letter (e.g., X), its value is denoted by an lower case letter (e.g., x), the finite alphabet of the RV is denoted by calligraphic letter (e.g., $\mathcal{X}$), and the probability distribution of an event $\{X = x\}$ is denoted by $P_X(x)$. Random vectors and their values are denoted by a similar convention. For example, X^N represents a N-dimensional random vector $(X_1, \ldots, X_N)$, and $x^N = (x_1, \ldots, x_N)$ represents a vector value in $\mathcal{X}^N$ (the N-th Cartesian power of the finite alphabet $\mathcal{X}$). In addition, define $A_j^N = (A_{j,1}, A_{j,2}, \ldots, A_{j,N})$ and $a_j^N = (a_{j,1}, a_{j,2}, \ldots, a_{j,N})$. Finally, throughout this paper, the base of the log function is 2.

The remainder of this paper is organized as follows. Formal definitions of the models studied in this paper are given in Section II. The SSCA feedback scheme for the GMAC-WT-DMS is given in Section III. The SSCA feedback scheme for the GMAC-WT-NCSIT-DMS is given in Section IV. Section V concludes this paper with potential connections to other problems and discusses future work.

II. Models Formulation

The models studied in this paper are depicted in Figure 1. In Figure 1, the message W_j $(j = 1, 2)$ transmitted in the channel is uniformly distributed in $\mathcal{W}_j = \{1, 2, \ldots, |\mathcal{W}_j|\}$. At time instant i $(i \in \{1, 2, \ldots, N\})$, the channel input $X_{j,i}$ $(j = 1, 2)$ satisfies an average power constraint $\frac{1}{N}\sum_{i=1}^{N} E[X_{j,i}^2] \leq P_j$, $\eta_{1,i} \sim \mathcal{N}(0, \sigma_1^2)$, $\eta_{2,i} \sim \mathcal{N}(0, \sigma_2^2)$ are independent channel noises and are independent identically distributed (i.i.d.) across the time index i, $S_i \sim \mathcal{N}(0, Q)$ is the Gaussian state interference with N-block covariance matrix K_{S^N}, and it is independent of the channel noises, Y_i and Z_i are the channel outputs of the legitimate receiver and the wiretapper, respectively. The legitimate receiver generates an estimation $(\hat{W}_1, \hat{W}_2) = \psi(Y^N)$, where ψ is the legitimate receiver's decoding function, and the average decoding error probability equals

$$P_e = \frac{1}{|\mathcal{W}_1| \cdot |\mathcal{W}_2|} \cdot \sum_{w_1 \in \mathcal{W}_1, w_2 \in \mathcal{W}_2} Pr\{\psi(y^N) \neq (w_1, w_2) | (w_1, w_2) \text{ sent}\}. \tag{2.1}$$

The wiretapper's equivocation rate of the messages W_1 and W_2 is defined as

$$\Delta = \frac{1}{N} H(W_1, W_2 | Z^N). \tag{2.2}$$

A rate pair (R_1, R_2) is said to be achievable if for any ϵ and sufficiently large N, there exists channel encoders and decoder such that

$$\frac{\log |\mathcal{W}_1|}{N} = R_1, \quad \frac{\log |\mathcal{W}_2|}{N} = R_2, \quad P_e \leq \epsilon. \tag{2.3}$$

A rate pair (R_1, R_2) is said to be achievable with perfect weak secrecy if for any ϵ and sufficiently large N, there exists channel encoders and decoder such that

$$\frac{\log |\mathcal{W}_1|}{N} = R_1, \quad \frac{\log |\mathcal{W}_2|}{N} = R_2, \ \Delta \geq R_1 + R_2 - \epsilon, \ P_e \leq \epsilon. \tag{2.4}$$

Figure 1 consists of four cases which are described below.

- *Case I-the GMAC-DMS with or without feedback*: at time instant i $(i \in \{1, 2, \ldots, N\})$, the channel inputs-output relationship is given by

$$Y_i = X_{1,i} + X_{2,i} + \eta_{1,i}. \tag{2.5}$$

  For the GMAC-DMS *without* feedback, the channel input $X_{1,i}$ is a function of the message W_1, and the channel input $X_{2,i}$ is a function of the messages W_1 and W_2. For the GMAC-DMS with feedback, $X_{1,i}$ is a function of the message W_1 and the feedback Y^{i-1}, and $X_{2,i}$ is a function of the messages W_1, W_2 and the feedback Y^{i-1}. The capacity regions of the GMAC-DMS with or without feedback are composed of all achievable rate pairs defined in (2.3), and they are denoted by $\mathcal{C}_{gmac-dms}^{f}$ and $\mathcal{C}_{gmac-dms}$, respectively.
- *Case II-the GMAC-WT-DMS with or without feedback*: at time instant i $(i \in \{1, 2, \ldots, N\})$, the channel inputs-outputs relationships are given by

$$Y_i = X_{1,i} + X_{2,i} + \eta_{1,i}, \quad Z_i = Y_i + \eta_{2,i}. \tag{2.6}$$

  For the GMAC-WT-DMS *without* feedback, the channel input $X_{1,i}$ is a stochastic function of the message W_1, and the channel input $X_{2,i}$ is a stochastic function of the messages W_1 and W_2. For the GMAC-WT-DMS with feedback, $X_{1,i}$ is a stochastic function of the message W_1 and the feedback Y^{i-1}, and $X_{2,i}$ is a stochastic function of the messages W_1, W_2 and the feedback Y^{i-1}. The *secrecy* capacity regions of the GMAC-WT-DMS with or without feedback are composed of all achievable weak secrecy rate pairs defined in (2.4), and they are denoted by $\mathcal{C}_{s,gmac-dms}^{f}$ and $\mathcal{C}_{s,gmac-dms}$, respectively.

- *Case III-the GMAC-NCSIT-DMS with or without feedback*: at time instant i ($i \in \{1, 2, \ldots, N\}$), the channel inputs-output relationships are given by

$$Y_i = X_{1,i} + X_{2,i} + S_i + \eta_{1,i}. \tag{2.7}$$

For the GMAC-NCSIT-DMS *without* feedback, the channel input $X_{1,i}$ is a function of the message W_1 and the state interference S^N, and the channel input $X_{2,i}$ is a function of the messages W_1, W_2 and the state interference S^N. For the GMAC-NCSIT-DMS with feedback, $X_{1,i}$ is a function of the message W_1, the state interference S^N and the feedback Y^{i-1}, and $X_{2,i}$ is a function of the messages W_1, W_2, the state interference S^N and the feedback Y^{i-1}. The capacity regions of the GMAC-NCSIT-DMS with or without feedback are composed of all achievable rate pairs defined in (2.3), and they are denoted by $\mathcal{C}^f_{gmac-ncsit-dms}$ and $\mathcal{C}_{gmac-ncsit-dms}$, respectively.

- *Case IV-the GMAC-WT-NCSIT-DMS with or without feedback*: at time instant i ($i \in \{1, 2, \ldots, N\}$), the channel inputs-outputs relationships are given by

$$Y_i = X_{1,i} + X_{2,i} + S_i + \eta_{1,i}, \quad Z_i = Y_i + \eta_{2,i}. \tag{2.8}$$

For the GMAC-WT-NCSIT-DMS *without* feedback, $X_{1,i}$ is a stochastic function of the message W_1 and the state interference S^N, and $X_{2,i}$ is a stochastic function of the messages W_1, W_2 and the state interference S^N. For the GMAC-WT-NCSIT-DMS with feedback, $X_{1,i}$ is a stochastic function of the message W_1, the state interference S^N and the feedback Y^{i-1}, and $X_{2,i}$ is a stochastic function of the messages W_1, W_2, the state interference S^N and the feedback Y^{i-1}. The *secrecy* capacity regions of the GMAC-WT-NCSIT-DMS with or without feedback are composed of all achievable weak secrecy rate pairs defined in (2.4), and they are denoted by $\mathcal{C}^f_{s,gmac-ncsit-dms}$ and $\mathcal{C}_{s,gmac-ncsit-dms}$, respectively.

III. The SSCA Feedback Scheme for the GMAC-WT-DMS

In this section, first, a two-step SK-type feedback scheme achieving the feedback capacity of GMAC-DMS is proposed. Second, we show that the proposed feedback scheme is secure by itself and also achieves the secrecy capacity region $\mathcal{C}^f_{s,gmac-dms}$ of the GMAC-WT-DMS with feedback. Finally, in order to show the rate gains by the feedback, an outer bound on the secrecy capacity region $\mathcal{C}_{s,gmac-dms}$ of GMAC-WT-DMS is provided, and the capacity results given in this section are further explained via a numerical example.

A. A Capacity-Achieving Two-Step SK-Type Scheme for the GMAC-DMS With Feedback

The model of the GMAC-DMS with feedback is formulated in Section II. In this subsection, first, we introduce capacity results on GMAC-DMS with or without feedback. Then, we propose a two-step SK-type scheme and show that this scheme achieves the capacity of GMAC-DMS with feedback.

1) Capacity Results on GMAC-DMS With or Without Feedback: The following Corollary 1 characterizes the capacity region $\mathcal{C}_{gmac-dms}$ of the GMAC-DMS.

Corollary 1: The capacity region $\mathcal{C}_{gmac-dms}$ of the GMAC-DMS is given by

$$\mathcal{C}_{gmac-dms} = \bigcup_{0\le\rho\le1} \Bigg\{ (R_1 \ge 0, R_2 \ge 0) : R_2 \le \frac{1}{2}\log\left(1+\frac{P_2(1-\rho^2)}{\sigma_1^2}\right), R_1+R_2 \le \frac{1}{2}\log\left(1+\frac{P_1+P_2+2\sqrt{P_1P_2}\rho}{\sigma_1^2}\right)\Bigg\}. \tag{3.1}$$

Proof: The proof is directly from [33] and [5, pp. 627-628], hence we omit the details here. ∎

In [8], it has been shown that feedback does not increase the capacity region $\mathcal{C}_{gmac-dms}$ of the GMAC-DMS, i.e.,

$$\mathcal{C}^f_{gmac-dms} = \mathcal{C}_{gmac-dms}, \tag{3.2}$$

where $\mathcal{C}_{gmac-dms}$ is given in (3.1). Here note that though the capacity region $\mathcal{C}^f_{gmac-dms}$ of the GMAC-DMS with feedback is determined, the SK-type feedback scheme that achieves $\mathcal{C}^f_{gmac-dms}$ remains unknown. In the remainder of this section, first, a two-step SK-type feedback scheme is proposed for the GMAC-DMS with feedback, and it is shown to be capacity-achieving. Then, we will show that this two-step SK-type scheme also achieves the secrecy capacity region $\mathcal{C}^f_{s,gmac-dms}$ of the GMAC-WT-DMS with feedback.

2) A Capacity-Achieving Two-Step SK-Type Feedback Scheme for the GMAC-DMS With Feedback: The main idea of the two-step SK-type feedback scheme is briefly illustrated by the following Figure 2. In Figure 2, the common message W_1 is encoded by both transmitters, and the private message W_2 is only available at Transmitter 2. Specifically, Transmitter 1 uses power P_1 to encode W_1 and the feedback Y^N as X_1^N. Transmitter 2 uses power $(1-\rho^2)P_2$ to encode W_2 and Y^N as V^N, and power $\rho^2 P_2$ to encode W_1 and Y^N as U^N, where $0 \le \rho \le 1$,

$$X_2^N = U^N + V^N, \tag{3.3}$$

and the average transmission power of X_2^N tends to P_2 for large N will be explained later. Here note that since W_1 is known by Transmitter 2, the codewords X_1^N and U^N can be subtracted when applying SK scheme to W_2, i.e., for the SK scheme of W_2, the equivalent channel model has input V^N, output $Y^{'N} = Y^N - X_1^N - U^N$, and channel noise η_1^N.

In addition, since W_1 is known by both transmitters and W_2 is only available at Transmitter 2, for the SK scheme of W_1, the equivalent channel model has inputs X_1^N and U^N, output Y^N, and channel noise $\eta_1^N + V^N$, which is non-white Gaussian noise since V^N is not i.i.d. generated. Furthermore, observing that

$$Y_i = X_{1,i} + U_i + V_i + \eta_{1,i} = X_i^* + V_i + \eta_{1,i}, \tag{3.4}$$

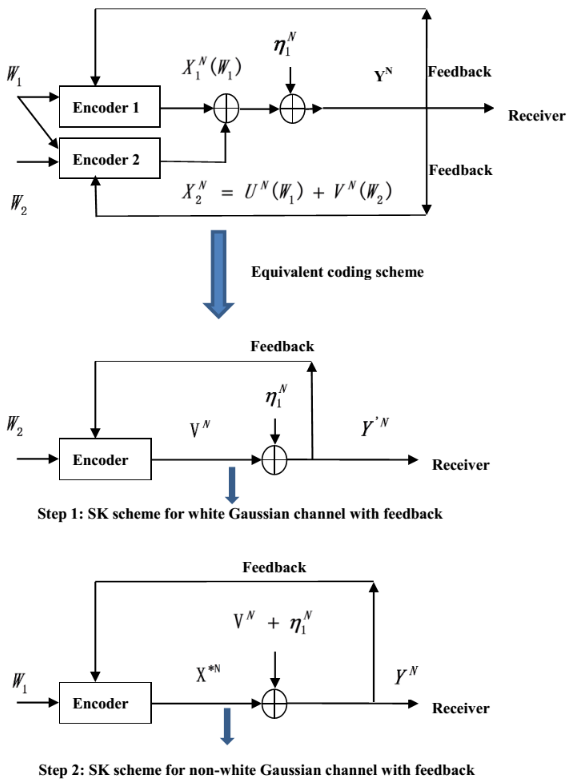

Fig. 2. The two-step SK-type feedback scheme for the GMAC-DMS with feedback.

where $X_i^* = X_{1,i} + U_i$, X_i^* is Gaussian distributed with zero mean and variance P_i^*,

$$\begin{aligned} P_i^* &= P_1 + \rho^2 P_2 + 2\sqrt{P_1 P_2}\rho\rho_i' \\ &\le P_1 + \rho^2 P_2 + 2\sqrt{P_1 P_2}\rho = P^*, \end{aligned} \tag{3.5}$$

$\rho_i' = \frac{E[X_{1,i}U_i]}{\rho\sqrt{P_1 P_2}}$ and $0 \le \rho_i' \le 1$. Hence for the SK scheme of W_1, the input of the equivalent channel model can be viewed as X_i^*. Since $X_{1,i}$ is known by Transmitter 2, let

$$U_i = \rho\sqrt{\frac{P_2}{P_1}}X_{1,i}. \tag{3.6}$$

Then we have $\rho_i' = 1$, which leads to

$$P_i^* = P^* = P_1 + \rho^2 P_2 + 2\sqrt{P_1 P_2}\rho, \tag{3.7}$$

and $X_i^* \sim \mathcal{N}(0, P^*)$. The encoding and decoding procedure of Figure 2 is described below.

Since W_j ($j = 1, 2$) takes values in $\mathcal{W}_j = \{1, 2, \ldots, 2^{NR_j}\}$, divide the interval $[-0.5, 0.5]$ into 2^{NR_j} equally spaced sub-intervals, and the center of each sub-interval is mapped to a message value in $\mathcal{W}_j$. Let θ_j be the center of the sub-interval w.r.t. the message W_j (the variance of θ_j approximately equals $\frac{1}{12}$).

Encoding: At time 1, Transmitter 1 sends

$$X_{1,1} = 0. \tag{3.8}$$

Transmitter 2 sends

$$V_1 = \sqrt{12(1-\rho^2)P_2}\theta_2, \tag{3.9}$$

and

$$U_1 = \rho\sqrt{\frac{P_2}{P_1}}X_{1,1} = 0. \tag{3.10}$$

The receiver obtains $Y_1 = X_{1,1} + X_{2,1} + \eta_{1,1} = X_{1,1} + V_1 + U_1 + \eta_{1,1} = V_1 + \eta_{1,1}$, and sends Y_1 back to Transmitter 2. Let $Y_1' = Y_1 = V_1 + \eta_{1,1}$, Transmitter 2 computes

$$\frac{Y_1'}{\sqrt{12(1-\rho^2)P_2}} = \theta_2 + \frac{\eta_{1,1}}{\sqrt{12(1-\rho^2)P_2}} = \theta_2 + \epsilon_1. \tag{3.11}$$

Let $\alpha_1 \triangleq Var(\epsilon_1) = \frac{\sigma_1^2}{12(1-\rho^2)P_2}$.

At time 2, Transmitter 2 sends

$$V_2 = \sqrt{\frac{(1-\rho^2)P_2}{\alpha_1}}\epsilon_1. \tag{3.12}$$

On the other hand, at time 2, Transmitters 1 and 2 respectively send $X_{1,2}$ and $U_2 = \rho\sqrt{\frac{P_2}{P_1}}X_{1,2}$ such that

$$X_2^* = U_2 + X_{1,2} = \sqrt{12P^*}\theta_1. \tag{3.13}$$

Once receiving the feedback $Y_2 = X_2^* + V_2 + \eta_{1,2}$, both transmitters compute

$$\frac{Y_2}{\sqrt{12P^*}} = \theta_1 + \frac{V_2 + \eta_{1,2}}{\sqrt{12P^*}} = \theta_1 + \epsilon_2'. \tag{3.14}$$

and send $X_{1,3}$ and $U_3 = \rho\sqrt{\frac{P_2}{P_1}}X_{1,3}$ such that

$$X_3^* = U_3 + X_{1,3} = \sqrt{\frac{P^*}{\alpha_2'}}\epsilon_2', \tag{3.15}$$

where $\alpha_2' \triangleq Var(\epsilon_2')$. In addition, subtracting $X_{1,2}$ and U_2 from Y_2 and let $Y_2' = Y_2 - X_{1,2} - U_2 = V_2 + \eta_{1,2}$, Transmitter 2 computes

$$\epsilon_2 = \epsilon_1 - \frac{E[Y_2'\epsilon_1]}{E[(Y_2')^2]}Y_2'. \tag{3.16}$$

and sends

$$V_3 = \sqrt{\frac{(1-\rho^2)P_2}{\alpha_2}}\epsilon_2, \tag{3.17}$$

where $\alpha_2 \triangleq Var(\epsilon_2)$.

At time $4 \le k \le N$, once receiving $Y_{k-1} = X_{1,k-1} + U_{k-1} + V_{k-1} + \eta_{1,k-1}$, Transmitter 2 computes

$$\epsilon_{k-1} = \epsilon_{k-2} - \frac{E[Y_{k-1}'\epsilon_{k-2}]}{E[(Y_{k-1}')^2]}Y_{k-1}', \tag{3.18}$$

where

$$Y_{k-1}' = Y_{k-1} - X_{1,k-1} - U_{k-1}, \tag{3.19}$$

and sends

$$V_k = \sqrt{\frac{(1-\rho^2)P_2}{\alpha_{k-1}}}\epsilon_{k-1}, \tag{3.20}$$

where $\alpha_{k-1} \triangleq Var(\epsilon_{k-1})$. In the meanwhile, Transmitters 1 and 2 respectively send $X_{1,k}$ and $U_k = \rho\sqrt{\frac{P_2}{P_1}}X_{1,k}$ such that

$$X_k^* = U_k + X_{1,k} = \sqrt{\frac{P^*}{\alpha'_{k-1}}}\epsilon'_{k-1}, \tag{3.21}$$

where

$$\epsilon'_{k-1} = \epsilon'_{k-2} - \frac{E[Y_{k-1}\epsilon'_{k-2}]}{E[(Y_{k-1})^2]}Y_{k-1}, \tag{3.22}$$

and $\alpha'_{k-1} \triangleq Var(\epsilon'_{k-1})$.

The following Lemma 1 is crucial for the analysis of the average transmission power of X_2^N and the decoding error probability.

Lemma 1: For $3 \leq k \leq N$,

$$E[\epsilon'_{k-1}\eta'_{1,k}] = 0, \tag{3.23}$$

where

$$\eta'_{1,k} = \eta_{1,k} + V_k. \tag{3.24}$$

Proof: See Appendix. ■

Analysis of the average transmission power of X_2^N: The above Lemma 1 indicates that for $3 \leq k \leq N$,

$$\begin{aligned} E[\epsilon'_{k-1}\eta'_{1,k}] &= E[\epsilon'_{k-1}(\eta_{1,k} + V_k)] \\ &= E[\epsilon'_{k-1}\eta_{1,k}] + E[\epsilon'_{k-1}V_k] \\ &\overset{(1)}{=} E[\epsilon'_{k-1}V_k] = 0, \end{aligned} \tag{3.25}$$

where (1) follows from the fact that $\eta_{1,k}$ is independent of ϵ'_{k-1} (ϵ'_{k-1} is a function of $(\eta_{1,1}, \ldots, \eta_{1,k-1})$). Since

$$U_k \overset{(2)}{=} \frac{\rho\sqrt{\frac{P_2}{P_1}}}{\rho\sqrt{\frac{P_2}{P_1}} + 1}\sqrt{\frac{P^*}{\alpha'_{k-1}}}\epsilon'_{k-1}, \tag{3.26}$$

where (2) follows from (3.21) and $U_k = \rho\sqrt{\frac{P_2}{P_1}}X_{1,k}$, substituting (3.26) into (3.25), we conclude that

$$E[U_kV_k] = 0, \tag{3.27}$$

for $3 \leq k \leq N$. In addition, from (3.9), (3.10), (3.12), (3.13) and the fact that θ_1 is independent of $\eta_{1,1}$, we conclude that

$$E[U_1V_1] = E[U_2V_2] = 0, \tag{3.28}$$

and hence $E[U_kV_k] = 0$ for $1 \leq k \leq N$.

Here note that for $1 \leq k \leq N$,

$$E[X_{2,k}^2] = E[(U_k + V_k)^2] \overset{(3)}{=} E[U_k^2] + E[V_k^2], \tag{3.29}$$

where (3) follows from $E[U_kV_k] = 0$ for $1 \leq k \leq N$. From the above encoding procedure, we conclude that $E[X_{2,1}^2] = E[U_1^2] + E[V_1^2] = (1-\rho^2)P_2$, and $E[X_{2,k}^2] = E[U_k^2] + E[V_k^2] = P_2$ for $2 \leq k \leq N$, which means that the average transmission power of X_2^N tends to P_2 for large N.

Decoding: The receiver uses a two-step decoding scheme. First, at time k ($3 \leq k \leq N$), the receiver's estimation $\hat{\theta}_{1,k}$ of θ_1 is given by

$$\hat{\theta}_{1,k} = \hat{\theta}_{1,k-1} - \frac{E[Y_k\epsilon'_{k-1}]}{E[(Y_k)^2]}Y_k, \tag{3.30}$$

where $\epsilon'_{k-1} = \hat{\theta}_{1,k-1} - \theta_1$ and it is computed by (3.22), and

$$\hat{\theta}_{1,2} = \frac{Y_2}{\sqrt{12P^*}} = \theta_1 + \frac{V_2 + \eta_{1,2}}{\sqrt{12P^*}} = \theta_1 + \epsilon'_2. \tag{3.31}$$

Second, after decoding W_1 and the corresponding codewords $X_{1,k}$ and U_k for all $1 \leq k \leq N$, the receiver subtracts $X_{1,k}$ and U_k from Y_k, and obtains $Y'_k = V_k + \eta_{1,k}$. At time k ($1 \leq k \leq N$), the receiver's estimation $\hat{\theta}_{2,k}$ of θ_2 is given by

$$\hat{\theta}_{2,k} = \hat{\theta}_{2,k-1} - \frac{E[Y'_k\epsilon_{k-1}]}{E[(Y'_k)^2]}Y'_k, \tag{3.32}$$

where $\epsilon_{k-1} = \hat{\theta}_{2,k-1} - \theta_2$ and it is computed by (3.18), and

$$\begin{aligned} \hat{\theta}_{2,1} &= \frac{Y'_1}{\sqrt{12(1-\rho^2)P_2}} \\ &= \theta_2 + \frac{\eta_{1,1}}{\sqrt{12(1-\rho^2)P_2}} = \theta_2 + \epsilon_1. \end{aligned} \tag{3.33}$$

Decoding Error Probability Analysis: The decoding error probability P_e of the receiver is upper bounded by

$$P_e \leq P_{e1} + P_{e2}, \tag{3.34}$$

where P_{ej} ($j = 1, 2$) is the receiver's decoding error probability of W_j. Observing that the transmission of W_2 is through an equivalent white Gaussian channel with power $(1-\rho^2)P_2$ and Gaussian noise variance σ_1^2, hence from the classical SK scheme [6], we conclude that the decoding error probability P_{e2} of W_2 tends to 0 as $N \to \infty$ if

$$R_2 < \frac{1}{2}\log(1 + \frac{(1-\rho^2)P_2}{\sigma_1^2}), \tag{3.35}$$

and hence we omit the derivation here. Now it remains to bound P_{e1}, see the followings.

First, from (A10) and $\alpha'_k = Var(\epsilon'_k)$, we conclude that

$$\alpha'_k \overset{(a)}{=} \frac{\alpha'_{k-1}r^2(r^2 + P^*)}{(P^* + r^2)^2} = \frac{\alpha'_{k-1}r^2}{P^* + r^2}, \tag{3.36}$$

where (a) follows from (A2), Lemma 1 and the definition in (A17).

Then, from (3.36), we can conclude that

$$\begin{aligned} \sqrt{\alpha'_N} &\overset{(c)}{=} (\frac{r}{\sqrt{r^2 + P^*}})^{N-2}\sqrt{\alpha'_2} \\ &\overset{(d)}{=} (\frac{r}{\sqrt{r^2 + P^*}})^{N-2}\frac{r}{\sqrt{12P^*}}, \end{aligned} \tag{3.37}$$

where (c) follows from (3.36), and (d) follows from $\alpha'_2 = Var(\epsilon'_2)$, (A14) and (A17).

Finally, we bound P_{e1} as follows. From $\epsilon'_N = \hat{\theta}_{1,N} - \theta_1$ and the definition of θ_1, we have

$$\begin{aligned} P_{e1} &\leq Pr\left\{|\epsilon'_N| > \frac{1}{2(|\mathcal{W}_1|-1)}\right\} \\ &\overset{(e)}{\leq} 2Q\left(\frac{1}{2\cdot 2^{NR_1}}\cdot\frac{1}{\sqrt{\alpha'_N}}\right) \\ &\overset{(f)}{=} 2Q\left(\frac{1}{2}\cdot 2^{-NR_1}\left(\frac{r}{\sqrt{r^2+P^*}}\right)^{-N+2}\sqrt{\frac{12P^*}{r^2}}\right) \\ &= 2Q\left(\frac{1}{2}\sqrt{\frac{12P^*}{r^2}}2^{-2\log\frac{\sqrt{r^2+P^*}}{r}}2^{-N(R_1-\log\frac{\sqrt{r^2+P^*}}{r})}\right), \end{aligned} \tag{3.38}$$

where (e) follows from $Q(x)$ is the tail of the unit Gaussian distribution evaluated at x, and (f) follows from (3.37) and the fact that $Q(x)$ is decreasing while x is increasing. From (3.38), we can conclude that if

$$\begin{aligned} R_1 &< \log\frac{\sqrt{r^2+P^*}}{r} = \frac{1}{2}\log(1+\frac{P^*}{r^2}) \\ &\overset{(g)}{=} \frac{1}{2}\log(1+\frac{P_1+\rho^2P_2+2\sqrt{P_1P_2}\rho}{(1-\rho^2)P_2+\sigma_1^2}), \end{aligned} \tag{3.39}$$

where (g) follows from (3.7) and (A17), $P_{e1}\to 0$ as $N\to\infty$.

Now we have shown if (3.35) and (3.39) are satisfied, the decoding error probability P_e of the receiver tends to 0 as $N \to \infty$. In other words, the rate pair $(R_1 = \frac{1}{2}\log(1+\frac{P_1+\rho^2P_2+2\sqrt{P_1P_2}\rho}{(1-\rho^2)P_2+\sigma_1^2}), R_2 = \frac{1}{2}\log(1+\frac{(1-\rho^2)P_2}{\sigma_1^2}))$ is achievable for all $0\leq\rho\leq 1$, which indicates that all rate pairs (R_1, R_2) in $\mathcal{C}^f_{gmac-dms}$ are achievable. Hence the proposed two-step SK-type feedback scheme achieves the capacity region $\mathcal{C}^f_{gmac-dms}$ of GMAC-DMS with feedback.

Similar to the self-secure property of the original SK scheme [29], in the next subsection, we will show that the proposed two-step SK-type feedback scheme for the GMAC-DMS is secure by itself.

B. Capacity Result on the GMAC-WT-DMS With Feedback

The model of the GMAC-WT-DMS with feedback is formulated in Section II. The following Theorem 1 establishes that the secrecy constraint does not reduce the capacity of GMAC-DMS with feedback.

Theorem 1: $\mathcal{C}^f_{s,gmac-dms} = \mathcal{C}_{gmac-dms}$, where $\mathcal{C}^f_{s,gmac-dms}$ is the secrecy capacity region of the GMAC-WT-DMS with feedback, and $\mathcal{C}_{gmac-dms}$ is given in Corollary 1.

Remark 1: Here note that in the Wyner's random binning scheme for the wiretap channel [11], the wiretapper's channel noise variance should be known by the transmitter, which is used to determine the length of the bin. Theorem 1 holds even if the wiretapper's channel noise variance is not known by the legitimate parties, and this is because only the legitimate receiver's channel noise is involved in the encoding-decoding procedure of the proposed scheme.

Proof: Since $\mathcal{C}^f_{s,gmac-dms}\subseteq\mathcal{C}^f_{gmac-dms}=\mathcal{C}_{gmac-dms}$, we only need to show that any achievable rate pair (R_1, R_2) in $\mathcal{C}_{gmac-dms}$ satisfies the secrecy constraint in (2.3).

In the preceding subsection, we introduce a two-step SK scheme for the GMAC-DMS with feedback, and show that this scheme achieves $\mathcal{C}^f_{gmac-dms}$. In this new scheme, the transmitted codewords $X_{1,i}$, U_i and V_i at time i $(1\leq i\leq N)$ can be expressed as

$$\begin{aligned} &X_{1,1}=0,\quad U_1=0,\quad V_1=\sqrt{12(1-\rho^2)P_2}\theta_2, \\ &X_{1,2}=\frac{\sqrt{12P^*}\theta_1}{\rho\sqrt{\frac{P_2}{P_1}}+1},\quad U_2=\rho\sqrt{\frac{P_2}{P_1}}X_{1,2}, \\ &nV_2=\sqrt{\frac{(1-\rho^2)P_2}{\sigma_1^2}}\eta_{1,1}, \\ &X_{1,3}=\frac{\sqrt{P^*P_2(1-\rho^2)}}{\sigma_1 r(\rho\sqrt{\frac{P_2}{P_1}}+1)}\eta_{1,1}+\frac{\sqrt{P^*}}{r(\rho\sqrt{\frac{P_2}{P_1}}+1)}\eta_{1,2}, \\ &U_3=\rho\sqrt{\frac{P_2}{P_1}}X_{1,3}, \\ &V_3=\frac{\sqrt{(1-\rho^2)P_2}}{r}\eta_{1,1}-\frac{(1-\rho^2)P_2}{r\sigma_1}\eta_{1,2}, \\ &\cdots \\ &X_{1,N}=\frac{1}{\rho\sqrt{\frac{P_2}{P_1}}+1}\sqrt{\frac{P^*}{\alpha'_{N-1}}}(\epsilon'_{N-2}\frac{r^2}{P^*+r^2}-(\eta_{1,N-1} \\ &\qquad +\sqrt{\frac{\alpha_{N-3}}{\alpha_{N-2}}}\frac{\sigma_1^2}{r^2}V_{N-2}-\sqrt{\frac{\alpha_{N-3}}{\alpha_{N-2}}}\frac{(1-\rho^2)P_2}{r^2}\eta_{1,N-2}) \\ &\qquad \cdot\frac{\sqrt{P^*\cdot\alpha'_{N-2}}}{P^*+r^2}), \\ &U_N=\rho\sqrt{\frac{P_2}{P_1}}X_{1,N}, \\ &V_N=\sqrt{\frac{\alpha_{N-2}}{\alpha_{N-1}}}\frac{\sigma_1^2}{r^2}V_{N-1}-\sqrt{\frac{\alpha_{N-2}}{\alpha_{N-1}}}\frac{(1-\rho^2)P_2}{r^2}\eta_{1,N-1}, \end{aligned} \tag{3.40}$$

where r is defined in (A17) and P^* is defined in (3.7).

From (3.40), we can conclude that for $3\leq k\leq N$, $X_{1,k}$, U_k and V_k are functions of $\eta_{1,1},\ldots,\eta_{1,k-1}$, and they are independent of the transmitted messages. Hence along the lines of the equivocation analysis in [29], we conclude that choosing sufficiently large N, the secrecy constraint in (2.3) is guaranteed, which indicates that any achievable rate pair (R_1, R_2) in $\mathcal{C}^f_{gmac-dms}$ is achievable with perfect weak secrecy, and hence $\mathcal{C}^f_{s,gmac-dms}=\mathcal{C}^f_{gmac-dms}$. The proof of Theorem 1 is completed. ■

For comparison, the following Corollary 2 establishes an outer bound on the secrecy capacity region $\mathcal{C}_{s,gmac-dms}$ of GMAC-WT-DMS *without feedback*.

Corollary 2: $\mathcal{C}_{s,gmac-dms}\subseteq\mathcal{C}^{out}_{s,gmac-dms}$, where $\mathcal{C}^{out}_{s,gmac-dms}$ is given by

$$\begin{aligned} \mathcal{C}^{out}_{s,gmac-dms} = \bigcup_{-1\leq\rho\leq 1}\{(R_1\geq 0, R_2\geq 0): \\ R_2\leq\frac{1}{2}\log\left(1+\frac{(1-\rho^2)P_2}{\sigma_1^2}\right), \end{aligned}$$

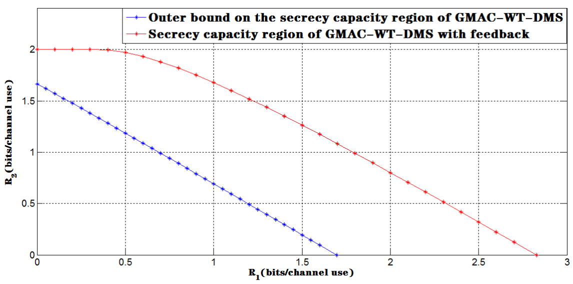

Fig. 3. Capacity results on GMAC-WT-DMS with or without feedback.

$$R_1+R_2 \leq \frac{1}{2}\log\left(1+\frac{P_1+P_2+2\sqrt{P_1P_2}\rho}{\sigma_1^2}\right) - \frac{1}{2}\log\left(1+\frac{P_1+P_2+2\sqrt{P_1P_2}\rho}{\sigma_1^2+\sigma_2^2}\right)\}. \tag{3.41}$$

Proof: See [37, Appendix B]. ∎

The following Figure 3 shows the rate gains by using channel feedback for $P_1 = 1$, $P_2 = 1.5$, $\sigma_1^2 = 0.1$ and $\sigma_2^2 = 1.2$.

IV. The SSCA Feedback Scheme for the GMAC-WT-NCSIT-DMS

In this section, first, we extend the two-step SK-type feedback scheme of the preceding section to the GMAC-NCSIT-DMS with feedback, and show that this extended scheme is also capacity-achieving. Second, we show that this extended feedback scheme is secure by itself and also achieves the secrecy capacity region $\mathcal{C}^f_{s,gmac-ncsit-dms}$ of the GMAC-WT-NCSIT-DMS with feedback. Finally, in order to show the rate gains by the feedback, an outer bound on the secrecy capacity region $\mathcal{C}_{s,gmac-ncsit-dms}$ of the GMAC-WT-NCSIT-DMS is provided, and the capacity results given in this section are further explained via a numerical example.

A. A Capacity-Achieving SK-Type Scheme for the GMAC-NCSIT-DMS With Feedback

The model of the GMAC-NCSIT-DMS with feedback is formulated in Section II. In this subsection, first, we introduce capacity results on the GMAC-NCSIT-DMS with or without feedback. Then, we propose a corresponding capacity-achieving feedback scheme.

1) Capacity Results on the GMAC-NCSIT-DMS With or Without Feedback: The following Corollary 3 characterizes the capacity region $\mathcal{C}_{gmac-ncsit-dms}$ of the GMAC-NCSIT-DMS.

Corollary 3: The capacity region $\mathcal{C}_{gmac-ncsit-dms}$ of the GMAC-NCSIT-DMS is given by

$$\begin{aligned}
&\mathcal{C}_{gmac-ncsit-dms} \\
&\quad = \mathcal{C}_{gmac-dms} \\
&\quad = \bigcup_{0\leq\rho\leq 1} \{(R_1, R_2): \\
&\qquad R_2 \leq \frac{1}{2}\log(1+\frac{P_2(1-\rho^2)}{\sigma_1^2}), \\
&\qquad R_1+R_2 \leq \frac{1}{2}\log(1+\frac{P_1+P_2+2\sqrt{P_1P_2}\rho}{\sigma_1^2})\}.
\end{aligned} \tag{4.1}$$

Proof: In [34], it has been pointed out that $\mathcal{C}_{gmac-ncsit-dms}$ equals $\mathcal{C}_{gmac-dms}$, which indicates that for the GMAC-NCSIT-DMS, the state interference can be pre-cancelled by both the transmitters and the receiver. ∎

The following Corollary 4 determines the capacity region $\mathcal{C}^f_{gmac-ncsit-dms}$ of the GMAC-NCSIT-DMS with feedback, which indicates that feedback does not increase the capacity of the GMAC-NCSIT-DMS, see the followings.

Corollary 4: $\mathcal{C}^f_{gmac-ncsit-dms} = \mathcal{C}_{gmac-ncsit-dms}$, where $\mathcal{C}_{gmac-ncsit-dms}$ is given in (4.1).

Proof: Note that $\mathcal{C}^f_{gmac-ncsit-dms} \subseteq \mathcal{C}^f_{gmac-dms} = \mathcal{C}_{gmac-dms} = \mathcal{C}_{gmac-ncsit-dms}$ directly follows from the converse proof of the bounds on R_2 and R_1+R_2 in $\mathcal{C}^f_{gmac}$ [5, pp. 627-628], and hence we omit the converse proof here. On the other hand, note that $\mathcal{C}_{gmac-ncsit-dms} \subseteq \mathcal{C}^f_{gmac-ncsit-dms}$ since non-feedback model is a special case of the feedback model, and $\mathcal{C}_{gmac-ncsit-dms} = \mathcal{C}_{gmac-dms}$ (see (4.1)), and hence the proof of Theorem 4 is completed. ∎

2) A Capacity-Achieving Two-Step SK-Type Feedback Scheme for the GMAC-NCSIT-DMS With Feedback: The SK-type scheme is almost the same as that of GMAC-NCSIT-DMS with feedback, except that at the first two time instants, proper offsets are introduced into the encoding procedure, which are used to cancel the offsets of the receiver's final estimation about the transmitted messages, see the details below.

Encoding: At time 1, $X_{1,1}$ and U_1 are encoded the same as those in (3.8) and (3.10), respectively, and V_1 is given by

$$V_1 = \sqrt{12(1-\rho^2)P_2}(\theta_2 - \frac{S_1}{\sqrt{12(1-\rho^2)P_2}} + A_2), \tag{4.2}$$

where A_2 is a linear combination of $S_1,\ldots,S_N$, and it will be determined later.

The receiver obtains

$$\begin{aligned}
Y_1 &= V_1 + X_{1,1} + U_1 + S_1 + \eta_{1,1} = V_1 + S_1 + \eta_{1,1} \\
&= \sqrt{12(1-\rho^2)P_2}\theta_2 + \sqrt{12(1-\rho^2)P_2}A_2 + \eta_{1,1},
\end{aligned} \tag{4.3}$$

and gets an estimation $\hat{\theta}_{2,1}$ of θ_2 by computing

$$\begin{aligned}
\hat{\theta}_{2,1} &= \frac{Y_1}{\sqrt{12(1-\rho^2)P_2}} \\
&= \theta_2 + A_2 + \frac{\eta_{1,1}}{\sqrt{12(1-\rho^2)P_2}} = \theta_2 + A_2 + \epsilon_1,
\end{aligned} \tag{4.4}$$

where ϵ_1 is in the same fashion as that in Section III, and define $\alpha_1 \triangleq Var(\epsilon_1) = \frac{\sigma_1^2}{12(1-\rho^2)P_2}$. Then the receiver sends Y_1 back to Transmitter 2. Let $Y_1' = Y_1 = V_1 + S_1 + \eta_{1,1}$, Transmitter 2 computes

$$\begin{aligned}
&\frac{Y_1'}{\sqrt{12(1-\rho^2)P_2}} \\
&\quad = \theta_2 + A_2 + \frac{\eta_{1,1}}{\sqrt{12(1-\rho^2)P_2}} = \theta_2 + A_2 + \epsilon_1.
\end{aligned} \tag{4.5}$$

Since A_2 is known by the transmitters, Transmitter 2 obtains ϵ_1 from (4.5).

At time 2, Transmitter 2 sends V_2 exactly in the same fashion as that in (3.12), i.e., $V_2 = \sqrt{\frac{(1-\rho^2)P_2}{\alpha_1}}\epsilon_1$. On the other hand, at time 2, Transmitters 1 and 2 respectively send $X_{1,2}$ and $U_2 = \rho\sqrt{\frac{P_2}{P_1}}X_{1,2}$ such that

$$X_2^* = U_2 + X_{1,2} = \sqrt{12P^*}(\theta_1 - \frac{S_2}{\sqrt{12P^*}} + A_1), \tag{4.6}$$

where P^* is defined in the same fashion as that in (3.7) and

$$A_1 = \sum_{i=3}^{N} \beta_{1,i} S_i, \tag{4.7}$$

and $\beta_{1,i}$ will be defined later. The receiver obtains

$$\begin{aligned} Y_2 &= X_2^* + V_2 + S_2 + \eta_{1,2} \\ &= \sqrt{12P^*}\theta_1 + \sqrt{12P^*}A_1 + V_2 + \eta_{1,2}, \end{aligned} \tag{4.8}$$

and gets an estimation $\hat{\theta}_{1,2}$ of θ_1 by computing

$$\begin{aligned} \hat{\theta}_{1,2} &= \frac{Y_2}{\sqrt{12P^*}} \\ &= \theta_1 + A_1 + \frac{V_2 + \eta_{1,2}}{\sqrt{12P^*}} = \theta_1 + A_1 + \epsilon_2', \end{aligned} \tag{4.9}$$

where ϵ_2' is in the same fashion as that in Section III, and define $\alpha_2' \triangleq Var(\epsilon_2')$. Then the receiver sends Y_2 back to both transmitters.

At time k ($3 \leq k \leq N$), the encoding procedure of U_k, V_k and $X_{1,k}$ is the same as that of GMAC-DMS with feedback since the transmitters can subtract S_{k-1} from their received feedback Y_{k-1}, i.e.,

$$V_k = \sqrt{\frac{(1-\rho^2)P_2}{\alpha_{k-1}}}\epsilon_{k-1}, \tag{4.10}$$

where $\alpha_{k-1} \triangleq Var(\epsilon_{k-1})$,

$$\epsilon_{k-1} = \epsilon_{k-2} - \beta_{2,k-1}Y_{k-1}', \tag{4.11}$$

$$Y_{k-1}' = Y_{k-1} - X_{1,k-1} - U_{k-1} - S_{k-1}, \tag{4.12}$$

$$\beta_{2,k-1} = \frac{E[Y_{k-1}'\epsilon_{k-2}]}{E[(Y_{k-1}')^2]}, \tag{4.13}$$

and $X_{1,k}$, $U_k = \rho\sqrt{\frac{P_2}{P_1}}X_{1,k}$, $X_k^* = U_k + X_{1,k}$ are given by

$$X_k^* = U_k + X_{1,k} = \sqrt{\frac{P^*}{\alpha_{k-1}'}}\epsilon_{k-1}', \tag{4.14}$$

where

$$\epsilon_{k-1}' = \epsilon_{k-2}' - \beta_{1,k-1}(Y_{k-1} - S_{k-1}), \tag{4.15}$$

$$\beta_{1,k-1} = \frac{E[(Y_{k-1} - S_{k-1})\epsilon_{k-2}']}{E[(Y_{k-1} - S_{k-1})^2]}, \tag{4.16}$$

and $\alpha_{k-1}' \triangleq Var(\epsilon_{k-1}')$.

Here note that though the use of S^N at time instants 1 and 2 causes the transmission power of the first two time instants to be larger than the average power constraint, for $k \geq 3$, the transmission power equals the average power constraint, and hence following similar analysis in [7, p. 4352, equation (31)], we conclude that for sufficiently large N, the average power constraint is preserved.

Decoding: The receiver uses a two-step decoding scheme which is similar to that in Section III. Specifically, first note that at time k ($3 \leq k \leq N$), the receiver's estimation $\hat{\theta}_{1,k}$ of θ_1 is given by

$$\hat{\theta}_{1,k} = \hat{\theta}_{1,k-1} - \beta_{1,k}Y_k, \tag{4.17}$$

where $\beta_{1,k} = \frac{E[(Y_k - S_k)\epsilon_{k-1}']}{E[(Y_k - S_k)^2]}$. Combining (4.15) with (4.17), we have

$$\begin{aligned} \hat{\theta}_{1,k} &= \hat{\theta}_{1,k-1} + \epsilon_k' - \epsilon_{k-1}' - \beta_{1,k}S_k \\ &\overset{(a)}{=} \theta_1 + \epsilon_k' + A_1 - \sum_{j=3}^{k}\beta_{1,j}S_j, \end{aligned} \tag{4.18}$$

where (a) follows from (4.9). From (4.18), we can conclude that for $k = N$,

$$\begin{aligned} \hat{\theta}_{1,N} &= \theta_1 + \epsilon_N' + A_1 - \sum_{j=3}^{N}\beta_{1,j}S_j \\ &\overset{(b)}{=} \theta_1 + \epsilon_N' + A_1 - A_1 = \theta_1 + \epsilon_N', \end{aligned} \tag{4.19}$$

where (b) follows from (4.7). Note that (4.19) indicates that the receiver's final estimation of θ_1 is in the same fashion as that in Section III, and observing that ϵ_k' ($2 \leq k \leq N$) is exactly in the same fashion as those in Section III, we can directly apply Lemma 1 to show that the decoding error probability P_{e1} of θ_1 tends to 0 as $N \to \infty$ if $R_1 < \frac{1}{2}\log(1 + \frac{P_1+\rho^2P_2+2\sqrt{P_1P_2}\rho}{(1-\rho^2)P_2+\sigma_1^2})$ is satisfied.

Second, after decoding W_1 (θ_1), the receiver obtains $\epsilon_k' + A_1 - \sum_{j=3}^{k}\beta_{1,j}S_j$ ($3 \leq k \leq N$) from (4.18), and obtains $\epsilon_2' + A_1$ from (4.9). Furthermore, from (4.14) and the fact that $\sqrt{\frac{P^*}{\alpha_k'}}$ is a constant value, we can conclude that for $3 \leq k \leq N$, the receiver knows

$$\begin{aligned} &\sqrt{\frac{P^*}{\alpha_k'}}(\epsilon_k' + A_1 - \sum_{j=3}^{k}\beta_{1,j}S_j) \\ &\qquad = X_{k+1}^* + \sqrt{\frac{P^*}{\alpha_k'}}(A_1 - \sum_{j=3}^{k}\beta_{1,j}S_j). \end{aligned} \tag{4.20}$$

In addition, for $k = 2$, the receiver knows

$$X_3^* + \sqrt{\frac{P^*}{\alpha_2'}}A_1 \tag{4.21}$$

since $X_3^* = \sqrt{\frac{P^*}{\alpha_2'}}\epsilon_2'$ and $\sqrt{\frac{P^*}{\alpha_2'}}$ is a constant value. Here for $k = 2$, define $\sum_{j=3}^{k}\beta_{1,j}S_j = 0$. Then we can conclude that the receiver knows the terms in (4.20) for $2 \leq k \leq N$. Here recall that in the SSCA feedback scheme of the GMAC-WT-DMS, after the receiver successfully obtains θ_1, he/she knows $X_{1,k}$ and U_k for all $3 \leq k \leq N$, and subtracts $X_{1,k}$ and U_k from Y_k. Then the receiver further applies SK-type decoding scheme to obtain θ_2. While, in this extended scheme for the GMAC-NCSIT-DMS, after decoding θ_1, the receiver does not know

$X_{1,k}$ and U_k, instead, he/she only knows $X_k^* + \sqrt{\frac{P^*}{\alpha'_{k-1}}}(A_1 - \sum_{j=3}^{k-1}\beta_{1,j}S_j)$, then the key to further decode θ_2 is how to choose A_2 (a linear combination of $(S_1, \ldots, S_N)$) to precancel the offset of the receiver's final estimation of θ_2.

Recall that the receiver's estimation $\hat{\theta}_{2,1}$ of θ_2 is given by (4.4). At time 2, since θ_1 is obtained by the receiver, the receiver's estimation $\hat{\theta}_{2,2}$ of θ_2 is given by

$$\begin{aligned}\hat{\theta}_{2,2} &= \hat{\theta}_{2,1} - \beta_{2,2}(Y_2 - \sqrt{12P^*}\theta_1)\\ &\overset{(c)}{=} \theta_2 + A_2 + \epsilon_1 + \epsilon_2 - \epsilon_1 - \beta_{2,2}\sqrt{12P^*}A_1\\ &= \theta_2 + \epsilon_2 + A_2 - \beta_{2,2}\sqrt{12P^*}A_1, \end{aligned}\tag{4.22}$$

where (c) follows from (4.4). At time k ($3 \le k \le N$), the receiver's estimation $\hat{\theta}_{2,k}$ of θ_2 is given by

$$\begin{aligned}\hat{\theta}_{2,k} &\overset{(e)}{=} \hat{\theta}_{2,k-1} - \beta_{2,k}(Y_k - X_k^* - \sqrt{\frac{P^*}{\alpha'_{k-1}}}(A_1 - \sum_{j=3}^{k-1}\beta_{1,j}S_j))\\ &\overset{(f)}{=} \theta_2 + \epsilon_k + A_2 - \beta_{2,2}\sqrt{12P^*}A_1\\ &\quad + \sum_{i=3}^{k}(\beta_{2,i}\sqrt{\frac{P^*}{\alpha'_{i-1}}}(A_1 - \sum_{j=3}^{i-1}\beta_{1,j}S_j) - \beta_{2,i}S_i), \end{aligned}\tag{4.23}$$

where (e) follows from the fact that the term in (4.20) is known by the receiver and hence it can be subtracted from Y_k, and (f) follows from (4.11), and (4.22). From (4.23), we can conclude that for $k = N$,

$$\begin{aligned}\hat{\theta}_{2,N} &= \theta_2 + \epsilon_N + A_2 - \beta_{2,2}\sqrt{12P^*}A_1\\ &\quad + \sum_{i=3}^{N}(\beta_{2,i}\sqrt{\frac{P^*}{\alpha'_{i-1}}}(A_1 - \sum_{j=3}^{i-1}\beta_{1,j}S_j) - \beta_{2,i}S_i). \end{aligned}\tag{4.24}$$

Observing that if

$$\begin{aligned}A_2 &= \beta_{2,2}\sqrt{12P^*}A_1\\ &\quad - \sum_{i=3}^{N}(\beta_{2,i}\sqrt{\frac{P^*}{\alpha'_{i-1}}}(A_1 - \sum_{j=3}^{i-1}\beta_{1,j}S_j) - \beta_{2,i}S_i), \end{aligned}\tag{4.25}$$

(4.24) can be re-written as

$$\hat{\theta}_{2,N} = \theta_2 + \epsilon_N, \tag{4.26}$$

which indicates that the receiver's final estimation of θ_2 is in the same fashion as that in Section III, and observing that ϵ_k ($1 \le k \le N$) is exactly in the same fashion as those in Section III, we can directly apply the same argument in Section III to show that the decoding error probability P_{e2} of θ_2 tends to 0 as $N \to \infty$ if $R_2 < \frac{1}{2}\log(1 + \frac{(1-\rho^2)P_2}{\sigma_1^2})$ is satisfied.

Finally, note that the decoding error probability P_e of the receiver is upper bounded by $P_e \le P_{e1} + P_{e2}$, and from above analysis, we can conclude that the rate pair $(R_1 = \frac{1}{2}\log(1 + \frac{P_1+\rho^2P_2+2\sqrt{P_1P_2}\rho}{(1-\rho^2)P_2+\sigma_1^2}), R_2 = \frac{1}{2}\log(1 + \frac{(1-\rho^2)P_2}{\sigma_1^2}))$ is achievable for all $0 \le \rho \le 1$, which indicates that all rate pairs (R_1, R_2) in $\mathcal{C}^f_{gmac-ncsit-dms}$ are achievable. Hence this extended two-step SK-type feedback scheme achieves the capacity region $\mathcal{C}^f_{gmac-ncsit-dms}$ of GMAC-NCSIT-DMS with feedback.

B. Capacity Results on the GMAC-WT-NCSIT-DMS With or Without Feedback

The model of the GMAC-WT-NCSIT-DMS with feedback is formulated in Section II. The following Theorem 2 establishes that the secrecy constraint does not reduce the capacity of GMAC-NCSIT-DMS with feedback.

Theorem 2: $\mathcal{C}^f_{s,gmac-ncsit-dms} = \mathcal{C}^f_{gmac-ncsit-dms}$, where $\mathcal{C}^f_{s,gmac-ncsit-dms}$ is the secrecy capacity region of the GMAC-WT-NCSIT-DMS with feedback, and $\mathcal{C}^f_{gmac-ncsit-dms}$ is given in Corollary 4.

Proof: Since $\mathcal{C}^f_{s,gmac-ncsit-dms} \subseteq \mathcal{C}^f_{gmac-ncsit-dms}$, we only need to show that any achievable rate pair (R_1, R_2) in $\mathcal{C}^f_{gmac-ncsit-dms}$ satisfies the secrecy constraint in (2.3). In the preceding subsection, we introduce an extended feedback scheme for the GMAC-NCSIT-DMS with feedback, and show that this scheme achieves $\mathcal{C}^f_{gmac-ncsit-dms}$. In this new scheme, the transmitted codewords $X_{1,i}$, U_i and V_i at time i ($1 \le i \le N$) can be expressed almost in the same fashion as those in (3.40), except that

$$\begin{aligned}V_1 &= \sqrt{12(1-\rho^2)P_2}(\theta_2 - \frac{S_1}{\sqrt{12(1-\rho^2)P_2}} + A_2),\\ X_{1,2} &= \frac{\sqrt{12P^*}(\theta_1 - \frac{S_2}{\sqrt{12P^*}} + A_1)}{\rho\sqrt{\frac{P_2}{P_1}} + 1}, \quad U_2 = \rho\sqrt{\frac{P_2}{P_1}}X_{1,2}. \end{aligned}\tag{4.27}$$

From (3.40) and (4.27), we can conclude that for $3 \le i \le N$, θ_1 and θ_2 are not contained in the transmitted $X_{1,i}$, U_i and V_i. Hence along the lines of the equivocation analysis in [29] and choosing sufficiently large N, we can prove that $\frac{1}{N}H(W_1, W_2|Z^N) \ge R_1 + R_2 - \epsilon$, which completes the proof. ■

For comparison, the following Corollary 5 establishes an outer bound on the secrecy capacity region $\mathcal{C}_{s,gmac-ncsit-dms}$ of GMAC-WT-NCSIT-DMS.

Corollary 5: $\mathcal{C}_{s,gmac-ncsit-dms} \subseteq \mathcal{C}^{out}_{s,gmac-ncsit-dms}$, where $\mathcal{C}^{out}_{s,gmac-ncsit-dms}$ is given by

$$\begin{aligned}&\mathcal{C}^{out}_{s,gmac-ncsit-dms}\\ &= \bigcup_{-1\le\rho_{12},\rho_{1s},\rho_{2s}\le 1} \{(R_1 \ge 0, R_2 \ge 0):\\ &R_2 \le \frac{1}{2}\log(1 + \frac{P_2 + \sigma_1^2 + a^2P_1 + b^2Q}{\sigma_1^2}\\ &\quad + \frac{-2a\rho_{12}\sqrt{P_1P_2} - 2b\rho_{2s}\sqrt{P_2Q} + 2ab\rho_{1s}\sqrt{P_1Q}}{\sigma_1^2}),\\ &R_1 + R_2 \le \frac{1}{2}\log(1 + \frac{P_1 + P_2 + Q + 2\sqrt{P_1P_2}\rho_{12}}{\sigma_1^2}\\ &\quad + \frac{2\rho_{1s}\sqrt{P_1Q} + 2\rho_{2s}\sqrt{P_2Q}}{\sigma_1^2}) - \frac{1}{2}\log(1 + \frac{P_1 + P_2 + Q}{\sigma_1^2 + \sigma_2^2}\\ &\quad - \frac{2\sqrt{P_1P_2}\rho_{12} + 2\rho_{1s}\sqrt{P_1Q} + 2\rho_{2s}\sqrt{P_2Q}}{\sigma_1^2 + \sigma_2^2}), \end{aligned}\tag{4.28}$$

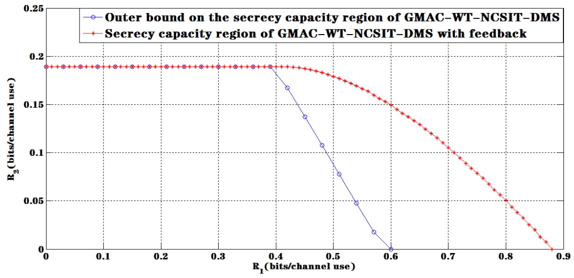

Fig. 4. Capacity results on GMAC-WT-NCSIT-DMS with or without feedback.

where

$$a = \sqrt{\frac{P_2}{P_1}} \frac{\rho_{12} - \rho_{1s}\rho_{2s}}{1 - \rho_{1s}^2}, \quad b = \sqrt{\frac{P_2}{Q}} \frac{\rho_{2s} - \rho_{12}\rho_{1s}}{1 - \rho_{1s}^2}. \tag{4.29}$$

Proof: See [37, Appendix C]. ■

The following Figure 4 shows the rate gains by using channel feedback for $P_1 = 10$, $P_2 = 3$, $Q = 5$, $\sigma_1^2 = 10$ and $\sigma_2^2 = 20$.

V. Concluding Remarks

In this paper, we determine the secrecy capacity regions of the GMAC-WT-DMS with feedback and the GMAC-WT-NCSIT-DMS with feedback by proposing SSCA feedback schemes for these models. In these schemes, the common message W_1 is encoded by a SK-type scheme with input $X^{*N} = X_1^N + U^N$, equivalent channel noise $V^N + \eta_1^N$, and output Y^N. Here V^N is a classical SK codeword for the private message W_2, and the equivalent channel noise for V^N is η_1^N (the channel noise of the GMAC-DMS). Lemma 1 indicates that if the channel noise is a white Gaussian noise added by a SK-type Gaussian noise, the classical SK scheme is still capacity-achieving, and the feedback capacity of this memory channel equals the feedback capacity of a white Gaussian channel with the same noise variance matrix. A further explanation of the above fact is given below.

The autoregressive moving average (ARMA) process of order k is defined by

$$X_t = \sum_{j=1}^{k} \alpha_j X_{t-j} + \sum_{j=1}^{k} \beta_j \eta_{t-j} + \eta_t, \tag{5.1}$$

where $t \in \{1, 2, \ldots, N\}$, $\eta_t \sim \mathcal{N}(0, \sigma^2)$ is white Gaussian noise, $\alpha = (\alpha_1, \ldots, \alpha_k)$ and $\beta = (\beta_1, \ldots, \beta_k)$ are the vectors of model coefficients. In [38], it has been shown that a k-dimensional generalization of the SK scheme achieves the feedback capacity for any ARMA noise spectrum of order k, and [30] further showed that the SK-type feedback scheme for the ARMA Gaussian channel is secure by itself.

In the proof of Lemma 1, we show that at time k ($3 \le k \le N$), the memory channel noise $\eta'_{1,k} = \eta_{1,k} + V_k$ is given by (A6) and (A7). Comparing (A6) with (5.1), we see that the memory channel noise $\eta'_{1,k}$, which is a white Gaussian noise added by a SK-type Gaussian noise, is a ARMA process of order 1. In [38], it has been shown that a k-dimensional generalization of the SK scheme achieves the feedback capacity for any ARMA noise spectrum of order k, and hence we conclude that the classical SK scheme achieves the feedback capacity for ARMA noise spectrum of order 1, which is the memory noise studied in this paper.

Moreover, the fact that feedback capacity of this memory channel equals the feedback capacity of a white Gaussian channel with the same noise variance matrix is briefly explained as follows. In [39], it has been shown that for a memory Gaussian channel with input X^N, channel noise η'^N, output Y^N, and power constraint

$$E(\frac{1}{N}\sum_{i=1}^{N} X_i^2(W, Y^{i-1})) \le P, \tag{5.2}$$

the feedback capacity C_{FB} is given by

$$C_{FB} = \lim_{N\to\infty} \max_{tr(K_{X^N}) \le NP} \frac{1}{2N} \log \frac{\det(K_{Y^N})}{\det(K_{\eta'^N})}, \tag{5.3}$$

where K_{X^N}, K_{Y^N}, $K_{\eta'^N}$ respectively denote the covariance matrices of X^N, Y^N and η'^N. Since the memory noise η'^N is defined by (A6) and (A7), it is not difficult to show that $K_{\eta'^N}$ is in fact a **diagonal matrix**, which leads to the C_{FB} given in (5.3) equals the capacity of a white Gaussian channel with i.i.d. noise η''^N which has the same covariance matrix as that of η'^N. Hence the feedback capacity of the memory channel defined in (A6) and (A7) is the same as that of a white Gaussian channel with the same noise variance matrix.

Possible future work includes:

- The rate-splitting feature used in [35] might be a good element to identify future strategies that potentially be useful for the GMACs with general (not necessarily degraded) message set, and maybe via that one can reach similar conclusions given above when the rate regions are not degraded by introducing secrecy constraint.
- To explore whether one can identify dualities of some kind between the GMAC and the Gaussian broadcast models when feedback and secrecy constraint are considered.
- The finite blocklength regime also deserves attention even in the single user wiretap case where a modified SK scheme motivated by [36] might be useful.

Appendix
Proof of Lemma 1

For $2 \le k \le N$, define

$$\eta'_{1,k} = \eta_{1,k} + V_k. \tag{A1}$$

Note that

$$\begin{aligned} E[(\eta'_{1,k})^2] &= E[(\eta_{1,k} + V_k)^2] \\ &\stackrel{(a)}{=} E[(\eta_{1,k})^2] + E[(V_k)^2] \stackrel{(b)}{=} \sigma_1^2 + (1-\rho^2)P_2, \end{aligned} \tag{A2}$$

where (a) follows from the fact that V_k is independent of $\eta_{1,k}$ since V_1 is a function of θ_1 and V_k ($2 \le k \le N$) is a function of $\eta_{1,1},\ldots,\eta_{1,k-1}$, and (b) follows from (3.20). Furthermore, from (3.18) and (3.20), V_k can be re-written as

$$\begin{aligned}V_k &= \sqrt{\frac{(1-\rho^2)P_2}{\alpha_{k-1}}}\epsilon_{k-1}\\ &\overset{(c)}{=} \sqrt{\frac{(1-\rho^2)P_2}{\alpha_{k-1}}}\\ &\quad\times\left(\epsilon_{k-2}-\frac{\sqrt{(1-\rho^2)P_2\alpha_{k-2}}}{(1-\rho^2)P_2+\sigma_1^2}(V_{k-1}+\eta_{1,k-1})\right)\\ &\overset{(d)}{=} \sqrt{\frac{\alpha_{k-2}}{\alpha_{k-1}}}V_{k-1}\\ &\quad-\sqrt{\frac{(1-\rho^2)P_2}{\alpha_{k-1}}}\frac{\sqrt{(1-\rho^2)P_2\alpha_{k-2}}}{(1-\rho^2)P_2+\sigma_1^2}(V_{k-1}+\eta_{1,k-1})\\ &= \sqrt{\frac{\alpha_{k-2}}{\alpha_{k-1}}}\frac{\sigma_1^2}{(1-\rho^2)P_2+\sigma_1^2}V_{k-1}\\ &\quad-\sqrt{\frac{\alpha_{k-2}}{\alpha_{k-1}}}\frac{(1-\rho^2)P_2}{(1-\rho^2)P_2+\sigma_1^2}\eta_{1,k-1},\end{aligned}\tag{A3}$$

where (c) follows from ϵ_{k-2} is independent of $\eta_{1,k-1}$, $V_{k-1}=\sqrt{\frac{(1-\rho^2)P_2}{\alpha_{k-2}}}\epsilon_{k-2}$ and $\alpha_{k-2}\triangleq Var(\epsilon_{k-2})$, and (d) follows from $V_{k-1}=\sqrt{\frac{(1-\rho^2)P_2}{\alpha_{k-2}}}\epsilon_{k-2}$. Substituting (A3) into (A1), we have

$$\begin{aligned}\eta'_{1,k} &= \eta_{1,k}+V_k\\ &= \eta_{1,k}+\sqrt{\frac{\alpha_{k-2}}{\alpha_{k-1}}}\frac{\sigma_1^2}{(1-\rho^2)P_2+\sigma_1^2}(V_{k-1}+\eta_{1,k-1})\\ &\quad-\sqrt{\frac{\alpha_{k-2}}{\alpha_{k-1}}}\eta_{1,k-1}\\ &= \eta_{1,k}+\sqrt{\frac{\alpha_{k-2}}{\alpha_{k-1}}}\frac{\sigma_1^2}{(1-\rho^2)P_2+\sigma_1^2}\eta'_{1,k-1}-\sqrt{\frac{\alpha_{k-2}}{\alpha_{k-1}}}\eta_{1,k-1}.\end{aligned}\tag{A4}$$

From classical SK scheme [6], we know that

$$\frac{\alpha_k}{\alpha_{k-1}}=\frac{\sigma_1^2}{(1-\rho^2)P_2+\sigma_1^2}\tag{A5}$$

for all $2\le k\le N$. Substituting (A5) into (A4), we obtain

$$\begin{aligned}\eta'_{1,k} &= \frac{\sigma_1}{\sqrt{(1-\rho^2)P_2+\sigma_1^2}}\eta'_{1,k-1}+\eta_{1,k}\\ &\quad-\sqrt{\frac{(1-\rho^2)P_2+\sigma_1^2}{\sigma_1^2}}\eta_{1,k-1}.\end{aligned}\tag{A6}$$

Observing that the above (A6) holds for $3\le k\le N$, and for $k=2$, we have

$$\eta'_{1,2}=\eta_{1,2}+V_2=\eta_{1,2}+\frac{\eta_{1,1}\sqrt{(1-\rho^2)P_2}}{\sigma_1}.\tag{A7}$$

On the other hand, from (3.22), we have

$$\begin{aligned}E[Y_{k-1}\epsilon'_{k-2}] &= E[(X^*_{k-1}+\eta'_{1,k-1})\epsilon'_{k-2}]\\ &\overset{(e)}{=} \sqrt{P^*\alpha'_{k-2}}+E[\eta'_{1,k-1}\epsilon'_{k-2}],\end{aligned}\tag{A8}$$

and

$$\begin{aligned}E[Y^2_{k-1}] &= E[(X^*_{k-1}+\eta'_{1,k-1})^2]\\ &\overset{(f)}{=} P^*+2\sqrt{\frac{P^*}{\alpha'_{k-2}}}E[\epsilon'_{k-2}\eta'_{1,k-1}]+(1-\rho^2)P_2+\sigma_1^2,\end{aligned}\tag{A9}$$

where (e) follows from (3.21), and (f) follows from (A2). Substituting (A8) and (A9) into (3.22), ϵ'_{k-1} is calculated by

$$\begin{aligned}\epsilon'_{k-1} &= \epsilon'_{k-2}-\frac{E[Y_{k-1}\epsilon'_{k-2}]}{E[Y^2_{k-1}]}Y_{k-1}\\ &= \epsilon'_{k-2}-\frac{\sqrt{P^*\alpha'_{k-2}}+E[\epsilon'_{k-2}\eta'_{1,k-1}]}{P^*+2\sqrt{\frac{P^*}{\alpha'_{k-2}}}E[\epsilon'_{k-2}\eta'_{1,k-1}]+(1-\rho^2)P_2+\sigma_1^2}\\ &\quad\cdot\left(\sqrt{\frac{P^*}{\alpha'_{k-2}}}\epsilon'_{k-2}+\eta'_{1,k-1}\right)\\ &= \epsilon'_{k-2}\frac{\sqrt{\frac{P^*}{\alpha'_{k-2}}}E[\epsilon'_{k-2}\eta'_{1,k-1}]+(1-\rho^2)P_2+\sigma_1^2}{P^*+2\sqrt{\frac{P^*}{\alpha'_{k-2}}}E[\epsilon'_{k-2}\eta'_{1,k-1}]+(1-\rho^2)P_2+\sigma_1^2}\\ &\quad-\eta'_{1,k-1}\frac{\sqrt{P^*\cdot\alpha'_{k-2}}+E[\epsilon'_{k-2}\eta'_{1,k-1}]}{P^*+2\sqrt{\frac{P^*}{\alpha'_{k-2}}}E[\epsilon'_{k-2}\eta'_{1,k-1}]+(1-\rho^2)P_2+\sigma_1^2}.\end{aligned}\tag{A10}$$

Now from (A6) and (A10), we have

$$\begin{aligned}&E[\epsilon'_{k-1}\eta'_{1,k}]\\ &\overset{(g)}{=} \frac{\sqrt{\frac{P^*}{\alpha'_{k-2}}}E[\epsilon'_{k-2}\eta'_{1,k-1}]+(1-\rho^2)P_2+\sigma_1^2}{P^*+2\sqrt{\frac{P^*}{\alpha'_{k-2}}}E[\epsilon'_{k-2}\eta'_{1,k-1}]+(1-\rho^2)P_2+\sigma_1^2}\\ &\quad\cdot\frac{\sigma_1}{\sqrt{(1-\rho^2)P_2+\sigma_1^2}}E[\epsilon'_{k-2}\eta'_{1,k-1}]\\ &\quad-\frac{\sqrt{P^*\cdot\alpha'_{k-2}}+E[\epsilon'_{k-2}\eta'_{1,k-1}]}{P^*+2\sqrt{\frac{P^*}{\alpha'_{k-2}}}E[\epsilon'_{k-2}\eta'_{1,k-1}]+(1-\rho^2)P_2+\sigma_1^2}\\ &\quad\cdot\frac{\sigma_1}{\sqrt{(1-\rho^2)P_2+\sigma_1^2}}E[(\eta'_{1,k-1})^2]\\ &\quad+\frac{\sqrt{P^*\cdot\alpha'_{k-2}}+E[\epsilon'_{k-2}\eta'_{1,k-1}]}{P^*+2\sqrt{\frac{P^*}{\alpha'_{k-2}}}E[\epsilon'_{k-2}\eta'_{1,k-1}]+(1-\rho^2)P_2+\sigma_1^2}\\ &\quad\cdot\sqrt{\frac{(1-\rho^2)P_2+\sigma_1^2}{\sigma_1^2}}E[\eta_{1,k-1}\eta'_{1,k-1}]\\ &\overset{(h)}{=} \frac{\sqrt{\frac{P^*}{\alpha'_{k-2}}}E[\epsilon'_{k-2}\eta'_{1,k-1}]+(1-\rho^2)P_2+\sigma_1^2}{P^*+2\sqrt{\frac{P^*}{\alpha'_{k-2}}}E[\epsilon'_{k-2}\eta'_{1,k-1}]+(1-\rho^2)P_2+\sigma_1^2}\\ &\quad\cdot\frac{\sigma_1}{\sqrt{(1-\rho^2)P_2+\sigma_1^2}}E[\epsilon'_{k-2}\eta'_{1,k-1}],\end{aligned}\tag{A11}$$

where (g) follows from $E[\epsilon'_{k-2}\eta_{1,k}]=E[\epsilon'_{k-2}\eta_{1,k-1}]=E[\eta'_{1,k-1}\eta_{1,k}]=0$, and (h) follows from (A6), which indicates that

$$E[\eta'_{1,k-1}\eta_{1,k-1}]\overset{(i)}{=}E[(\eta_{1,k-1})^2]=\sigma_1^2,\tag{A12}$$

where (i) follows from $E[\eta'_{1,k-2}\eta_{1,k-1}] = E[\eta_{1,k-2}\eta_{1,k-1}] = 0$.

Observing that the first item of $E[\epsilon'_{k-1}\eta'_{1,k}]$ is $E[\epsilon'_2\eta'_{1,3}]$, and it is given by

$$\begin{aligned}E[\epsilon'_2\eta'_{1,3}] &= E[\epsilon'_2(V_3+\eta_{1,3})]\\ &= E[\epsilon'_2(\eta_{1,3}+\sqrt{\frac{(1-\rho^2)P_2}{\alpha_2}}\epsilon_2)]\\ &\overset{(j)}{=} E[\frac{\sqrt{\frac{(1-\rho^2)P_2}{\sigma_1^2}}\eta_{1,1}+\eta_{1,2}}{\sqrt{12P^*}}(\eta_{1,3}+\frac{\sqrt{(1-\rho^2)P_2}}{r}\eta_{1,1}\\ &\quad -\frac{(1-\rho^2)P_2}{r\sigma_1}\eta_{1,2})]\\ &\overset{(k)}{=} \frac{(1-\rho^2)P_2}{r\sigma_1}\frac{\sigma_1^2}{\sqrt{12P^*}} - \frac{(1-\rho^2)P_2}{r\sigma_1}\frac{\sigma_1^2}{\sqrt{12P^*}} = 0,\end{aligned} \tag{A13}$$

where (j) follows from

$$\epsilon'_2 = \frac{V_2+\eta_{1,2}}{\sqrt{12P^*}} = \frac{\sqrt{\frac{(1-\rho^2)P_2}{\sigma_1^2}}\eta_{1,1}+\eta_{1,2}}{\sqrt{12P^*}}, \tag{A14}$$

$$\begin{aligned}\epsilon_2 &= \epsilon_1 - \frac{E[Y'_2\epsilon_1]}{E[Y'^2_2]}Y'_2\\ &= \frac{\sigma_1^2}{\sqrt{12(1-\rho^2)P_2r^2}}\eta_{1,1} - \frac{\sigma_1}{\sqrt{12}r^2}\eta_{1,2},\end{aligned} \tag{A15}$$

$$\alpha_2 = \frac{\sigma_1^4}{12(1-\rho^2)P_2r^2}, \tag{A16}$$

$$r = \sqrt{(1-\rho^2)P_2+\sigma_1^2}, \tag{A17}$$

and (k) follows from $E[\eta_{1,3}\eta_{1,1}] = E[\eta_{1,3}\eta_{1,2}] = E[\eta_{1,1}\eta_{1,2}] = 0$. Now substituting (A13) into (A11), we can conclude that $E[\epsilon'_{k-1}\eta'_{1,k}] = 0$ for all $3 \le k \le N$, which completes the proof.

REFERENCES

[1] H. D. Liao, "Multiple-access channels," Ph.D. dissertation, Dept. Elect. Eng., Univ. Hawaii, Honolulu, HI, USA, 1972.

[2] T. Cover, "Some advances in broadcast channels," in *Advances in Communication Systems*, vol. 4, A. Viterbi, Ed. San Francisco, CA, USA: Academic, 1975.

[3] T. Cover and C. Leung, "An achievable rate region for the multiple-access channel with feedback," *IEEE Trans. Inf. Theory*, vol. IT-27, no. 3, pp. 292–298, May 1981.

[4] R. Venkataramanan and S. S. Pradhan, "A new achievable rate region for the multiple-access channel with noiseless feedback," *IEEE Trans. Inf. Theory*, vol. 57, no. 12, pp. 8038–8054, Dec. 2011.

[5] L. H. Ozarow, "The capacity of the white Gaussian multiple access channel with feedback," *IEEE Trans. Inf. Theory*, vol. IT-27, no. 5, pp. 292–298, Jul. 1981.

[6] J. Schalkwijk and T. Kailath, "A coding scheme for additive noise channels with feedback-I: No bandwidth constraint," *IEEE Trans. Inf. Theory*, vol. IT-12, no. 2, pp. 172–182, Apr. 1966.

[7] A. Rosenzweig, "The capacity of Gaussian multi-user channels with state and feedback," *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 4349–4355, Nov. 2007.

[8] A. Bracher and A. Lapidoth, "Feedback, cribbing, and causal state information on the multiple-access channel," *IEEE Trans. Inf. Theory*, vol. 60, no. 12, pp. 7627–7654, Dec. 2014.

[9] O. Sabag, H. H. Permuter, and S. Shamai, "Capacity-achieving coding scheme for the MAC with degraded message sets and feedback," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2019, pp. 2259–2263.

[10] O. Shayevitz and M. Feder, "A simple proof for the optimality of randomized posterior matching," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 3410–3418, Jun. 2016.

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

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

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

[14] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5747–5755, Dec. 2008.

[15] Y. Chen, D. He, and Y. Luo, "Strong secrecy of arbitrarily varying multiple access channels," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 3662–3677, 2021.

[16] R. Fritschek and G. Wunder, "On the Gaussian multiple access wiretap channel and the Gaussian wiretap channel with a helper: Achievable schemes and upper bounds," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 5, pp. 1224–1239, May 2019.

[17] H. Zivarifard, M. R. Bloch, and A. Nosratinia, "Two-multicast channel with confidential messages," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 2743–2758, 2021.

[18] P. Xu, Z. Ding, and X. Dai, "Rate regions for multiple access channel with conference and secrecy constraints," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 1961–1974, Dec. 2013.

[19] H. He, X. Luo, J. Weng, and K. Wei, "Secure transmission in multiple access wiretap channel: Cooperative jamming without sharing CSI," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 3401–3411, 2021.

[20] A. Sonee and G. A. Hodtani, "On the secrecy rate region of multiple-access wiretap channel with noncausal side information," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 6, pp. 1151–1166, Jun. 2015.

[21] 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. Sel. Areas Commun.*, vol. 36, no. 4, pp. 723–736, Apr. 2018.

[22] B. Dai and Z. Ma, "Multiple-access relay wiretap channel," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 9, pp. 1835–1849, Sep. 2015.

[23] 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.

[24] 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.

[25] K. Zeng, "Physical layer key generation in wireless networks: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 33–39, Jun. 2015.

[26] A. Khisti, S. N. Diggavi, and G. W. Wornell, "Secret-key agreement with channel state information at the transmitter," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 672–681, Sep. 2011.

[27] A. Bunin, Z. Goldfeld, H. Permuter, S. Shamai, P. Cuff, and P. Piantanida, "Key and message semantic-security over state-dependent channels," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1541–1556, 2020.

[28] M. Jafari Siavoshani, S. Mishra, C. Fragouli, and S. N. Diggavi, "Multi-party secret key agreement over state-dependent wireless broadcast channels," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 2, pp. 323–337, Feb. 2017.

[29] 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.

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

[31] B. Dai, C. Li, Y. Liang, Z. Ma, and S. Shamai, "Impact of action-dependent state and channel feedback on Gaussian wiretap channels," *IEEE Trans. Inf. Theory*, vol. 66, no. 6, pp. 3435–3455, Jun. 2020.

[32] B. Dai, C. Li, Y. Liang, Z. Ma, and S. Shamai, "On the capacity of Gaussian multiple-access wiretap channels with feedback," in *Proc. Int. Symp. Inf. Theory Appl. (ISITA)*, Oct. 2020, pp. 397–401, 2020.

[33] D. Slepian and J. K. Wolf, "A coding theorem for multiple access channels with correlated sources," *Bell Syst. Tech. J.*, vol. 51, no. 7, pp. 1037–1076, 1973.

[34] Y.-H. Kim, A. Sutivong, and S. Sigurjonsson, "Multiple user writing on dirty paper," in *Proc. Int. Symp. Inf. Theory (ISIT)*, 2004, p. 534.

[35] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Multiple access channels with generalized feedback and confidential messages," in *Proc. IEEE Inf. Theory Workshop*, Sep. 2007, pp. 1–6.

[36] R. G. Gallager and B. Nakiboglu, "Variations on a theme by Schalkwijk and Kailath," *IEEE Trans. Inf. Theory*, vol. 56, no. 1, pp. 6–17, Jan. 2010.
[37] B. Dai, C. Li, Y. Liang, Z. Ma, and S. Shamai, "Self-secure capacity-achieving feedback schemes of Gaussian multiple-access wiretap channels with degraded message sets," 2020, *arXiv:2007.14555*.
[38] Y.-H. Kim, "Feedback capacity of stationary Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 56, no. 1, pp. 57–85, Jan. 2010.
[39] T. M. Cover and S. Pombra, "Gaussian feedback capacity," *IEEE Trans. Inf. Theory*, vol. 35, no. 1, pp. 37–43, Jan. 1989.

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, University of Duisburg-Essen, Essen, Germany. In 2018 and 2019, he was a Visiting Scholar with the Department of Electrical and Computer Engineering, The Ohio State University (OSU), Columbus, USA. He is currently a Professor with Southwest Jiaotong University. His research interests include information-theoretic security and networks information theory and coding.

Chong Li (Senior Member, IEEE) is the Co-Founder of Nakamoto & Turing Labs Inc. He is also an Adjunct Associate Professor with the Department of Electrical Engineering, Columbia University in the City of New York. Prior to that, he had been working with Qualcomm Research on 4G LTE and 5G systems design. He holds over 200 international/U.S. patents (granted and pending). He has been actively publishing academic papers on top-ranking journals, including PROCEEDINGS OF THE IEEE, IEEE TRANSACTIONS ON INFORMATION THEORY, *IEEE Communications Magazine*, and *Automatica*. He is the author of the book *Reinforcement Learning for Cyber-Physical Systems* (Taylor & Francis CRC Press). His broad research interests include information theory, machine learning, distributed database and computing systems (e.g., blockchain), networked control and communication, and PYH/MAC systems design for advance telecommunication technologies (5G and beyond). He is a member of the Grant Review Committee of the Natural Sciences and Engineering Research Council of Canada. He received the MediaTek Inc. and Wu Ta You Scholar Award in 2007, the Rosenfeld International Scholarship in 2012, and the Research Excellent Award in 2013. His paper "Youla Coding and Computation of Gaussian Feedback Capacity" was nominated for the 2019 IEEE Information Theory Society Paper Award. He has also served as a reviewer and a member of technical program committee for most prestigious journals and conferences in communications and control societies.

Yingbin Liang (Fellow, IEEE) received the Ph.D. degree in electrical engineering from the University of Illinois at Urbana-Champaign in 2005. She is currently a Professor with the Department of Electrical and Computer Engineering, The Ohio State University (OSU), and a core Faculty Member of the Translational Data Analytics Institute (TDAI), OSU. Currently, she is also serving as the Deputy Director for the AI-Edge Institute, OSU. Before she joined OSU, she served on the Faculty of the University of Hawaii and Syracuse University. 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 the EURASIP Best Paper Award in 2014.

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

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 position. His research interests encompass a wide spectrum of topics in information theory and statistical communications. He is a fellow of the Union Radio Scientifique Internationale (URSI), a member of the Israeli Academy of Sciences and Humanities, and a Foreign Member of the U.S. National Academy of Engineering. He has 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. 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 a co-recipient of the 2018 Third Bell Labs Prize for Shaping the Future of Information and Communications Technology, 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 has been awarded the 1999 van der Pol Gold Medal of URSI. He is listed as a Highly Cited Researcher (Computer Science) from 2013 to 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.