A Coding Scheme for Colored Gaussian Wiretap Channels with Feedback

Chong Li*, Yingbin Liang†, H. Vincent Poor‡, and Shlomo Shamai(Shitz)§
*Qualcomm Research, Bridgewater, NJ, United States, chongl@qti.qualcomm.com
†The Ohio State University, Columbus, OH, United States, liang.889@osu.edu
‡Princeton University, Princeton, NJ, United States, poor@princeton.edu
§Technion-Israel Institute of Technology, Haifa, Israel, sshlomo@ee.technion.ac.il

***Abstract*—In this paper, the finite-order autoregressive moving average (ARMA) Gaussian wiretap channel with noiseless causal feedback is considered, in which an eavesdropper receives noisy observations of the signals in both forward and feedback channels. It is shown that the generalized *Schalkwijk-Kailath* scheme, a capacity-achieving coding scheme for the feedback Gaussian channel, achieves the same maximum rate for the same channel with the presence of an eavesdropper. Therefore, the secrecy capacity is equal to the feedback capacity without the presence of an eavesdropper for the feedback channel. Furthermore, the results are extended to the additive white Gaussian noise (AWGN) channel with quantized feedback. It is shown that the proposed coding scheme achieves a positive secrecy rate. As the amplitude of the quantization noise decreases to zero, the secrecy rate converges to the capacity of the AWGN channel.**

I. Introduction

Secure communication over feedback channels has recently attracted considerable attention. Substantial progress has been made towards understanding this type of channels. In particular, although the feedback may not increase the capacity of open-loop additive white Gaussian noise (AWGN) channels, [1]–[7] showed that feedback can increase the secrecy capacity by sharing a secret key between legitimate users. For instance, [1] and [2] showed the achievement of a positive secrecy rate by using noiseless feedback even when the secrecy capacity of the feed-forward channel is zero. Moreover, [8] proved the usefulness of noisy feedback for a class of full-duplex two-way wiretap channels. Furthermore, [9] presented an achievable scheme for the wiretap channel with generalized feedback, which is a generalization and unification of several relevant previous results in the literature. Very recently, [10] proposed an improved feedback coding scheme for the wiretap channel with noiseless feedback, which was shown to outperform the existing ones in the literature. A more comprehensive review of the previous work can be found in the extended version of this paper [11].

However, it is noteworthy that most of the aforementioned results considered *memoryless* wiretap channels with only a few exceptions such as [12], which studied the *memory* Gaussian channel (i.e., the ARMA(1) Gaussian channel) with feedback under an eavesdropping attack, and showed that the feedback secrecy capacity equals the standard feedback capacity without an eavesdropper. In this paper, we make two major contributions.

1) We generalize the results in [12] to the finite-order ARMA Gaussian wiretap channel with feedback. The construction and analysis of the feedback scheme are much more involved here for the finite-order ARMA channel than that in [12]. In particular, we show that the feedback secrecy capacity C_{sc} of the finite-order ARMA Gaussian channel equals the feedback capacity C_{fb} of such a channel. Namely, $C_{sc} = C_{fb}$.
2) We further study the AWGN channel with quantized feedback, which is a more realistic channel model for the feedback link. In this case, the coding scheme in [12] for ARMA(1) is not applicable any more. We thus propose a new coding scheme and show that the proposed coding scheme provides non-trivial positive secrecy rates and achieves the feedback capacity of the AWGN channel as the amplitude of the quantization noise vanishes to zero.

The rest of the paper is organized as follows. In Sections II and III, we introduce the system model and the preliminary results, respectively. Section IV presents the main results of our paper. Finally, we conclude the paper in Section V.

Notation: Uppercase and the corresponding lowercase letters $(e.g., Y, Z, y, z)$ denote random variables and their realizations, respectively. We use log to denote the logarithm with base 2, and $0 \log 0 = 0$. We use $\mathbf{x}'$ to denote the transpose of a vector or matrix $\mathbf{x}$.

II. System Model

In this section, we present the mathematical system model. First of all, we consider a discrete-time Gaussian channel with noiseless feedback (See Fig. 1). The additive Gaussian channel is modeled as

$$y(k) = u(k) + w(k), \qquad k = 1, 2, \cdots, \tag{1}$$

where the Gaussian noise $\{w(k)\}_{k=1}^{\infty}$ is assumed to be stationary with power spectrum density $\mathbb{S}_w(e^{j\theta})$ for $\forall \theta \in [-\pi, \pi)$. Unless the contrary is explicitly stated, "stationary" without specification refers to stationary in wide sense. Moreover, we assume that the power spectral density satisfies the *Paley-Wiener* condition $\frac{1}{2\pi}\int_{-\pi}^{\pi} |\log \mathbb{S}_w(e^{j\theta})| d\theta < \infty$.

978-1-5386-4780-6/18/$31.00©2018 IEEE

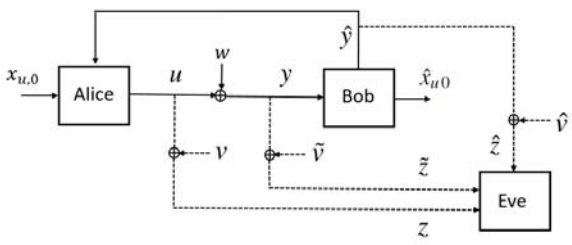

Fig. 1. Finite-order ARMA Gaussian wiretap channel with feedback.

Let $\mathscr{RH}_2$ be the set of stable and proper rational filters in Hardy space $\mathscr{H}_2$.

Assumption 1. *(Finite-order ARMA Gaussian Channel) In this paper, noise w is assumed to be the output of a finite-dimensional linear time invariant (LTI) minimum-phase stable system $\mathbb{H} \in \mathscr{RH}_2$, driven by white Gaussian noise with zero mean and unit variance. The power spectral density (PSD) of w is colored (nonwhite), bounded away from zero and has a canonical spectral factorization given by $\mathbb{S}_w(e^{j\theta}) = |\mathbb{H}(e^{j\theta})|^2$.*

As shown in Fig.1, the feedback wiretap channel of interest includes a forward channel from Alice to Bob as described by (1), a causal noiseless feedback $\hat{y}$ from Bob to Alice, and three noisy observation channels to the eavesdropper Eve. Note that a classical wiretap channel model can be recovered if the eavesdropper's channel inputs from u and $\hat{y}$ are removed. In this paper, we assume that the eavesdropper is powerful and can access three inputs [1]. The noisy wiretap channels are modeled as

$$\begin{aligned} z(k) =& u(k) + v(k), \\ \tilde{z}(k) =& y(k) + \tilde{v}(k), \\ \hat{z}(k) =& \hat{y}(k) + \hat{v}(k), \qquad k = 1, 2, \cdots. \end{aligned}$$

The additive noises v, $\tilde{v}$ and $\hat{v}$ are assumed to be arbitrarily finite-memory processes, i.e.,

$$\begin{aligned} p(v(k)|v_1^{k-1}) &= p(v(k)|v_{k-d}^{k-1}), \qquad k \geq d, \\ p(\tilde{v}(k)|\tilde{v}_1^{k-1}) &= p(\tilde{v}(k)|\tilde{v}_{k-\tilde{d}}^{k-1}), \qquad k \geq \tilde{d}, \\ p(\hat{v}(k)|\hat{v}_1^{k-1}) &= p(\hat{v}(k)|\hat{v}_{k-\hat{d}}^{k-1}), \qquad k \geq \hat{d}, \end{aligned} \tag{2}$$

where d, $\tilde{d}$ and $\hat{d}$ respectively represent the sizes of the finite memories and the notation v_a^b represents a sequence $\{v_a, v_{a+1}, \cdots, v_b\}$ in a compact form. In this paper, we assume these noises have strictly positive and bounded variance for all k. But they are not necessarily uncorrelated.

We specify a sequence of $(n, 2^{nR_s})$ channel codes with an achievable secrecy rate R_s as follows. We denote the message index by x_{u0}, which is uniformly distributed over the set $\{1, 2, 3, \cdots, 2^{nR_s}\}$. The encoding process $u_i(x_{u0}, \hat{y}^{i-1})$ at Alice satisfies the average transmit power constraint P, where $\hat{y}^{i-1} = \{\hat{y}_0, \hat{y}_1, \cdots, \hat{y}_{i-1}\}$ ($\hat{y}_0 = \emptyset$) for $i = 1, 2, \cdots, n$, and $u_1(x_{u0}, \hat{y}^0) = u_1(x_{u0})$. Bob decodes the message as $\hat{x}_{u0}$ following a decoding function $g : y^n \to \{1, 2, \cdots, 2^{nR_s}\}$ with an error probability satisfying $P_e^{(n)} = \frac{1}{2^{nR_s}} \sum_{x_{u0}=1}^{2^{nR_s}} p(x_{u0} \neq g(y^n)|x_{u0}) \leq \varepsilon_n$, where $\lim_{n\to\infty} \varepsilon_n = 0$. Meanwhile, the information received by Eve should asymptotically vanish, i.e., $\lim_{n\to\infty} \frac{1}{n} I(x_{u0}; z_1^n, \tilde{z}_1^n, \hat{z}_1^n) = 0$. The objective of secure communications is to send x_{u0} to Bob at as high a rate R_s as possible. The secrecy capacity C_{sc} is defined as the supremium of all achievable rates R_s. Mathematically,

$$\begin{aligned} C_{sc} = & \sup_{\text{feasible coding schemes}} R_s \\ & \text{s.t.} \lim_{n\to\infty} \frac{1}{n} I(x_{u0}; z_1^n, \tilde{z}_1^n, \hat{z}_1^n) = 0, \end{aligned} \tag{3}$$

where the argument "feasible coding schemes" is referred to as all feedback codes that satisfy the secrecy requirements and the power constraint. Note that the feedback capacity (without the secrecy constraint) from Alice to Bob, denoted as C_{fb}, can be recovered by removing the secrecy constraint. This implies $C_{sc} \leq C_{fb}$.

III. Preliminaries of the Feedback Capacity and Capacity-Achieving Coding Scheme

In this section, we present a characterization of the feedback capacity C_{fb} and the construction of C_{fb}-achieving feedback codes without the presence of an eavesdropper. The materials here are useful for us to further investigate the channel model with an eavesdropper.

A. Feedback Capacity C_{fb} Revisited

Firstly, we present a feedback capacity characterization for the Gaussian channel under Assumption 1. As proved in [13], the feedback capacity from Alice to Bob for such a channel with the average power budget P can be characterized by

$$\begin{aligned} C_{fb} =& \max_{\mathbb{Q}} \frac{1}{2\pi} \int_{-\pi}^{\pi} \log|1 + \mathbb{Q}(e^{i\theta})| d\theta, \\ s.t. \quad & \frac{1}{2\pi} \int_{-\pi}^{\pi} |\mathbb{Q}(e^{j\theta})|^2 \mathbb{S}_w(e^{j\theta}) d\theta \leq P, \\ & \mathbb{Q} \in \mathscr{RH}_2 \text{ is strictly causal.} \end{aligned} \tag{4}$$

Remark 1. *Under Assumption 1, the optimal $\mathbb{Q}$ has no zeros on the unit circle (Proposition 5.1 (ii) in [13]).*

Since this optimization problem has an infinite dimensional search space, except for the ARMA(1) Gaussian channels, the solution $\mathbb{Q}(e^{j\theta})$ in an analytical form is unknown. One recent result in [14] and [15] provides a numerical solution to this problem, which can be efficiently solved by the standard convex optimization tools. We refer the interested reader to [14] and [15] for details.

In what follows, we describe, given an optimal $\mathbb{Q}$ in (4), how to construct an implementable coding scheme that achieves the feedback capacity from Alice to Bob.

[1] Note that in [12] access to only the channel input u and channel output y is considered. Based on the generalized results in this paper, however, the results in [12] with three noisy observation channels to the eavesdropper as assumed in this paper still hold.

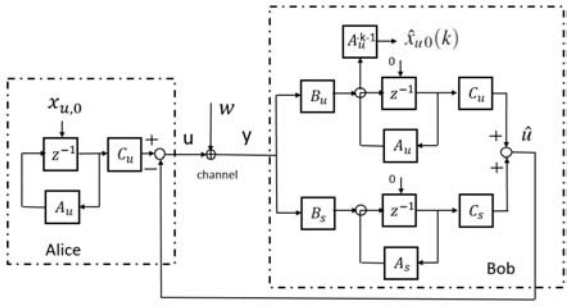

Fig. 2. Representation I: Decomposition of filter $\mathbb{K}$ into the feedback encoder (Alice) and decoder (Bob). The eavesdropper channels are not included. The z-transform is used to represent the dynamics of LTI systems.

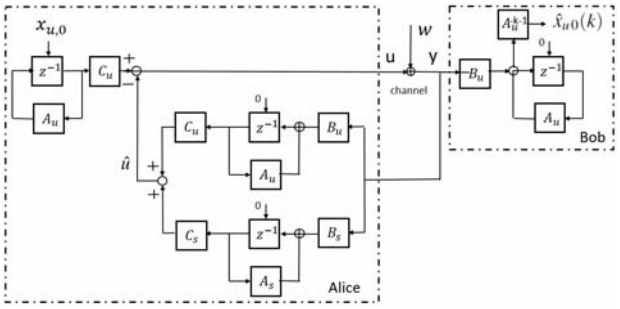

Fig. 3. Representation II: Decomposition of filter $\mathbb{K}$ into the feedback encoder (Alice) and decoder (Bob). The eavesdropper channels are not included.

B. C_{fb}-achieving Feedback Coding Scheme

First of all, once an optimal $\mathbb{Q}$ is found for the above optimization, we can obtain a feedback filter $\mathbb{K} = -\mathbb{Q}(1+\mathbb{Q})^{-1}$ stabilizing the channel within the prescribed input average power budget (see [14] for proofs). Next, based on the transfer function $\mathbb{K}$, we construct an explicit feedback coding scheme as follows, which is deterministic (time-invariant) and has doubly exponentially decaying decoding error probability.

We first present controller $\mathbb{K}$ as an LTI single-input-single-output (SISO) finite-dimensional discrete-time unstable system with the following state-space model:

$$\mathbb{K}: \quad \begin{bmatrix} x_s(k+1) \\ x_u(k+1) \end{bmatrix} = \begin{bmatrix} A_s & 0 \\ 0 & A_u \end{bmatrix} \begin{bmatrix} x_s(k) \\ x_u(k) \end{bmatrix} + \begin{bmatrix} B_s \\ B_u \end{bmatrix} y(k) \qquad u(k) = \begin{bmatrix} C_s & C_u \end{bmatrix} \begin{bmatrix} x_s(k) \\ x_u(k) \end{bmatrix}. \tag{5}$$

Based on Remark 1, we assume that the eigenvalues of A_u are strictly outside the unit disc while the eigenvalues of A_s are strictly inside the unit disc. Without loss of generality, we assume that A_s and A_u are in Jordan form. Assume that A_u has m eigenvalues, denoted by $\lambda_i(A_u), i = 1,2,\cdots,m$. Next, as shown in Fig. 2, we can decompose $\mathbb{K}$ into an encoder (Alice) and a decoder (Bob), in which an estimate from the decoder is fed back to the encoder via the noiseless feedback channel. We denote this coding scheme as *Representation I* (decoder-estimation-based feedback coding scheme). Due to space limitations, we refer the readers to [12] for details.

We next propose an equivalent representation of the above decoder-estimation-based feedback coding scheme. As will be seen later, this new representation is vital to extend our results to channels with noisy feedback.

Representation II: *Channel-output-based Feedback Coding Scheme (Fig. 3).*

Decoder: The decoder runs $\mathbb{K}$ driven by the channel output y. That is, $\hat{x}_u(k+1) = A_u\hat{x}_u(k) + B_u y(k)$, $\hat{x}_u(0) = 0$.

It produces an estimate of the initial condition of the encoder

$$\hat{x}_{u0}(k) = A_u^{-k-1}\hat{x}_u(k+1).$$

Encoder: The encoder runs the following dynamics driven by the initial state, i.e., the message:

$$\begin{aligned} \tilde{x}_u(k+1) &= A_u\tilde{x}_u(k), \quad \tilde{x}_u(0) = x_{u0}, \\ \tilde{u}_u(k) &= C_u\tilde{x}_u(k). \end{aligned}$$

It receives y and runs dynamics driven by the received feedback y,

$$\begin{aligned} x_s(k+1) &= A_s x_s(k) + B_s y(k), \quad x_s(0) = 0, \\ \hat{x}_u(k+1) &= A_u\hat{x}_u(k) + B_u y(k), \quad \hat{x}_u(0) = 0, \end{aligned}$$

and produces a signal $\hat{u}(k) = C_s x_s(k) + C_u\hat{x}_u(k)$,

Then, the encoder produces the channel input

$$u(k) = \tilde{u}_u(k) - \hat{u}(k).$$

By comparing the two representations, we see that the only difference comes from the feedback signal. In *Representation I*, the feedback signal $\hat{u}$ is generated by the decoder, while in *Representation II*, the feedback signal is simply the raw channel output. The equivalence can be directly verified by comparing the channel inputs u (encoder) and the estimate of the message $\hat{x}_{u0}$ (decoder) between the two representations.

IV. Main Results

In this section, we first present our results for the finite-order ARMA feedback channel with an eavesdropper, and then extend our results to the case with quantization noise in the feedback. We provide only the outline of some technical proofs here due to space limitations. The complete proofs can be found in the technical report [11] available online.

A. Finite-order ARMA Feedback Channel with an Eavesdropper

We first present our new development on the properties of the feedback coding scheme for the finite-order ARMA Gaussian channels without the presence of an eavesdropper. We then use these properties to establish our main theorem, which characterizes the feedback secrecy capacity and its achieving coding scheme.

The following result shows that, by choosing the particular m-step initializations (in the state-space representation) for the proposed coding scheme, the channel inputs ($k \geq m+1$) are

only determined by the past additive Gaussian noise w, a fact that is vital to guarantee the asymptotic secrecy from Eve.

Proposition 1. *For the proposed coding scheme in Fig. 2 or Fig. 3, assume the first m-step channel inputs $u_1^m = A_u^{m+1}x_{u0}$ (where A_u^{m+1} refers to matrix A_u to the power $m+1$), $\hat{x}_u(m+1) = y_1^m$ (i.e., the estimated message $\hat{x}_{u0}(m) = A_u^{-m-1}y_1^m$) and $x_s(m+1) = 0$, where m is the number of eigenvalues of matrix A_u. Then the induced channel inputs $u(k)$ for $k \geq m+1$ are determined only by the past Gaussian noise w_1^{k-1}.*

Proof. (*Sketch*) Following the coding scheme in *Representation I* with the proposed initializations and taking nontrivial algebra, we can obtain $u(m+1) = -C_u w_1^m$ and, for $k \geq m+2$,

$$u(k) = -C_u A_u^k \left(\prod_{i=m+1}^{k-1} \alpha_i A_u^{-m-1} w_1^m + \sum_{i=m+1}^{k-1} \prod_{j=i+1}^{k-1} \alpha_j \beta_i (w(i) - C_s x_s(i)) \right) - C_s x_s(k),$$
$$\text{and} \qquad x_s(k) = A_s x_s(k-1) + B_s(u(k-1) + w(k-1)), \tag{6}$$

where $\alpha_i = I - A_u^{-i-1} B_u C_u A_u^i$ and $\beta_i = A_u^{-i-1} B_u$. Starting with $u(m+1) = -C_u w_1^m$ and $x_s(m+1) = 0$, the above coupled iterations produce values of $u(k)$ and $x_s(k)$ that depend only on the past noise w_1^{k-1}. Due to the equivalence between *Representation I* and *Representation II* of the coding scheme, this result directly holds for *Representation II*. □

Proposition 2. *With the initializations defined in Proposition 1, the coding scheme $\mathbb{K}$ in Fig. 2 or Fig. 3 remains C_{fb}-achieving.*

It is noteworthy that the above propositions implicitly reveal an interesting behavior of the proposed coding scheme $\mathbb{K}$ with the selected initializations. Specifically, in the first m-step, Alice transmits a (scaled) message while Bob receives a noisy (unbiased) message. In the sequential steps, Alice sends projected values of the past noise (shared key with Bob) to refine Bob's estimate. In the meanwhile, Eve receives only the noisy refinements from Alice due to the additive noises v, $\tilde{v}$ and $\hat{v}$ on the eavesdropper channels. The next theorem proves that the noisiness of these refinements for Eve leads to the asymptotic ignorance of the message.

Theorem 1. *Consider the finite-order ARMA Gaussian wiretap channel with feedback (Fig. 1) under the average channel input power constraint $P > 0$. Then,*

1) *the feedback secrecy capacity equals the feedback (Shannon) capacity, i.e., $C_{sc} = C_{fb}$, where C_{fb} is obtained from Section III-A; and*
2) *the feedback secrecy capacity is achieved by the C_{fb}-achieving feedback coding scheme $\mathbb{K}$ with $u_1^m = A_u^{m+1}x_{u0}$, $\hat{x}_u(m+1) = y_1^m$ (i.e., the estimated message $\hat{x}_{u0}(m) = A_u^{-m-1}y_1^m$), and $x_s(m+1) = 0$.*

Proof. (*Sketch*) The key to the proof is to show that under the selected initializations, the proposed coding scheme $\mathbb{K}$ satisfies the secrecy requirement $\lim_{n\to\infty} \frac{1}{n} I(x_{u0}; z_1^n, \tilde{z}_1^n, \hat{z}_1^n) = 0$.

Following the coding scheme $\mathbb{K}$, we first have

$$\begin{aligned} z_1^m &= u_1^m + v_1^m = A_u^{m+1}x_{u0} + v_1^m, \\ \tilde{z}_1^m &= u_1^m + \tilde{v}_1^m + w_1^m = A_u^{m+1}x_{u0} + \tilde{v}_1^m + w_1^m, \\ \hat{z}_1^m &= u_1^m + \hat{v}_1^m + w_1^m = A_u^{m+1}x_{u0} + \hat{v}_1^m + w_1^m. \end{aligned} \tag{7}$$

Then, for $n \geq k + \max\{d, \tilde{d}, \hat{d}\} + 1$ and $k \geq m+1$, we have

$$\begin{aligned} h(x_{u0}|z_1^n, \tilde{z}_1^n, \hat{z}_1^n) &\overset{(a)}{\geq} h(x_{u0}|z_1^n, \tilde{z}_1^n, \hat{z}_1^n, w_1^n, v_{m+1}^n, \tilde{v}_{m+1}^n, \hat{v}_{m+1}^n) \\ &\overset{(b)}{=} h(x_{u0}|z_1^m, \tilde{z}_1^m, \hat{z}_1^m, w_1^n, v_{m+1}^n, \tilde{v}_{m+1}^n, \hat{v}_{m+1}^n) \\ &= h(x_{u0}|A_u^{m+1}x_{u0} + v_1^m, A_u^{m+1}x_{u0} + \tilde{v}_1^m, \\ &\quad A_u^{m+1}x_{u0} + \hat{v}_1^m, v_{m+1}^{m+d}, \tilde{v}_{m+1}^{m+\tilde{d}}, \hat{v}_{m+1}^{m+\hat{d}}), \end{aligned} \tag{8}$$

where step (a) follows from the fact that conditioning does not increase entropy and step (b) follows from Proposition 1. The last step follows from (7), the finite memory assumption of the wiretap channel noise processes and the fact that the noise w is independent of the others. Recall that the message x_{u0} is uniformly selected from the index set $\{1, 2, \cdots, 2^{nR}\}$, where the messages are equally spaced in an m-dimensional unit hypercube (proof of Theorem 4.3, [16]). As a consequence, the covariance matrix of x_{u0} is $\frac{1}{12}I_m$ as n becomes sufficiently large. Also, for a fixed covariance, a vector Gaussian input distribution maximizes the mutual information. Therefore, from (8), we can prove

$$\begin{aligned} &\lim_{n\to\infty} \frac{1}{n} I(x_{u0}; z_1^n, \tilde{z}_1^n, \hat{z}_1^n) \\ &\leq \lim_{n\to\infty} \frac{1}{2n} \log\det\left(E[\mathbb{B}\mathbb{B}^T] + \frac{1}{12}\mathbb{A}\mathbb{A}^T \right) - h(\mathbb{B}) = 0, \end{aligned} \tag{9}$$

where $\mathbb{A} = [A_u^{m+1}, A_u^{m+1}, A_u^{m+1}, \mathbf{0}]'$ ($\mathbf{0}$ is an $(d + \tilde{d} + \hat{d}) \times m$ zero matrix) and $\mathbb{B} = [v_1^m, \tilde{v}_1^m, \hat{v}_1^m, v_{m+1}^{m+d}, \tilde{v}_{m+1}^{m+\tilde{d}}, \hat{v}_{m+1}^{m+\hat{d}}]$. □

This theorem shows that there exists a feedback coding scheme such that the secrecy requirement can be achieved without loss of the communication rate of the legitimate users. In addition, Section III-B provides such a feedback coding scheme that achieves the feedback secrecy capacity. In particular, a C_{sc}-achieving feedback code can be constructed from the optimal $\mathbb{Q}$ in (4) by following the procedures in Section III-B with the initializations defined in Proposition 1. The next corollary shows that the well-known *S-K* scheme [17] is a special case of our proposed coding scheme[2].

Corollary 1. *Consider the AWGN wiretap channel with feedback (see Fig. 1) under the average channel input power constraint $P > 0$. Assume that the additive noise w has zero mean and variance $\sigma_w^2 > 0$. Then the proposed coding scheme $\mathbb{K}$ with $A_u = \sqrt{\frac{P+\sigma_w^2}{\sigma_w^2}}$, $B_u = -\frac{\sqrt{A_u^2-1}}{A_u}$, $C_u = -\sqrt{A_u^2-1}$, and $A_s = B_s = C_s = 0$ becomes the original S-K scheme, and achieves the secrecy capacity $C_{sf} = C_{fb} = \frac{1}{2}\log(1 + \frac{P}{\sigma_w^2})$.*

[2]This result has been shown in [12]. For completeness, we re-state this result in this paper.

B. Feedback with Quantization Noise

In this section, we extend our result to Gaussian channels with quantized feedback. It is noteworthy that the capacity of colored Gaussian channels with noisy feedback remains an open problem, even when simplified to quantized feedback. Therefore, in this paper, as an initial step towards the secrecy capacity of noisy feedback Gaussian channels, we focus on the AWGN channel with quantized feedback. In [18], the authors presented a linear coding scheme featuring a positive information rate and a positive error exponent for the AWGN channel with feedback corrupted by quantization or bounded noise. In what follows, we show that our proposed *linear* coding scheme, when specified to the AWGN channel with quantized feedback, converges to the scheme in [18] and, more importantly, leads to a positive secrecy rate. Furthermore, this achievable secrecy rate converges to the capacity of the AWGN channel as the amplitude of the quantization noise decreases to zero. Firstly, we define a memoryless uniform quantizer with sensitivity σ_q as follows [18].

Definition 1. *Given a real parameter $\sigma_q > 0$, a uniform quantizer with sensitivity σ_q is a function $\Phi_{\sigma_q}: \mathbb{R} \to \mathbb{R}$ defined as $\Phi_{\sigma_q}(y) = 2\sigma_q \lfloor \frac{y+\sigma_q}{2\sigma_q} \rfloor$, where $\lfloor \cdot \rfloor$ represents the floor function. The quantization error at instant k, i.e., the feedback noise, is given by $q(k) = \Phi_{\sigma_q}(y(k)) - y(k)$.*

Notice that, for a given channel output $y(k)$, the quantization noise $q(k)$ can be recovered by the decoder. In other words, the decoder can access both the channel outputs and the feedback noise while the encoder can only access the corrupted channel output. On the other hand, with quantized feedback, the coding schemes *Representation I* and *Representation II* are no longer equivalent due to the different feedback signals. The *Representation I* in [12] may not be applicable here. Therefore, we next tailor the proposed coding scheme *Representation II* to obtain the following theorem.

Theorem 2. *Consider an AWGN channel with uniformly memoryless quantized feedback defined in Definition 1, where the channel input power constraint is $P > 0$ and the noise variance of the AWGN channel and the quantization sensitivity in the feedback link are assumed to be σ_w^2 and σ_q, respectively. Assume the channel input $u(1) = A_u^2 x_{u0}$, and the estimate message $\hat{x}_{u0}(1) = A_u^{-2}(y(1) + q(1))$. Then, our proposed coding scheme (Representation II) with $A_u = 2^r, B_u = -1, C_u = A_u - \frac{1}{Au}$ and $A_s = B_s = C_s = 0$ achieves a secrecy rate r for all $r < r_q$, where r_q is defined as follows.*

1) *If $4\sigma_q \le P$, r_q is the nonnegative real solution of the following equation: $\sigma_w\sqrt{2^{2r_q} - 1} = \sqrt{P} - \sigma_q(1 + 2^{r_q})$, which yields $\lim_{\sigma_q \to 0^+} r_q = \frac{1}{2}\log(1 + \frac{P}{\sigma_w^2})$.*
2) *If $4\sigma_q > P$, then $r_q = 0$.*

V. Conclusion

In this paper, we have considered the finite-order ARMA Gaussian wiretap channel with feedback and have shown that the feedback secrecy capacity equals the feedback capacity without the presence of an eavesdropper. We have further extended our scheme to the AWGN channel with quantized feedback and proved that our scheme can achieve a positive secrecy rate, which converges to the AWGN channel capacity as the quantization noise decreases to zero.

VI. Acknowledgement

The work of Y. Liang was supported in part by the U.S. National Science Foundation under Grant CCF-1801846. The work of H. V. Poor was supported in part by the U.S. National Science Foundation under Grants CNS-1702808 and ECCS-1647198. The work of S. Shamai was supported by the European Union's Horizon 2020 Research And Innovation Programme, grant agreement no. 694630.

References

[1] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, 1993.
[2] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography, part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.
[3] 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*, Springer, Berlin, Heidelberg, 2006, pp. 258–275.
[4] L. Lai, H. El-Gamal, and H. V. Poor, "The wiretap channel with feedback: Encryption over the channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 11, pp. 5059–5067, 2008.
[5] D. Gündüz, D. R. Brown, and H. V. Poor, "Secret communication with feedback," in *Proc. Int. Symp. Inf. Theory and Its Applications*, Auckland, New Zealand, 2008.
[6] 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, 2009.
[7] B. Dai, Z. Ma, and L. Yu, "Feeding back the output or sharing state, which is better for the state-dependent degraded wiretap channel with noncausal csi at the transmitter?" *Entropy*, vol. 17, no. 12, pp. 7900–7925, 2015.
[8] X. He and A. Yener, "The role of feedback in two-way secure communications," *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 8115–8130, 2013.
[9] G. Bassi, P. Piantanida, and S. Shamai, "On the capacity of the wiretap channel with generalized feedback," in *Proc. IEEE Int. Symp. Inf. Theory*, Hong Kong, China, 2015, pp. 1154–1158.
[10] B. Dai, "An improved feedback coding scheme for the wire-tap channel," *[online] ArXiv*, 2017.
[11] C. Li, Y. Liang, H. V. Poor, and S. Shamai, "Secrecy capacity of colored Gaussian noise channels with feedback," *[online] ArXiv*, 2018.
[12] C. Li and Y. Liang, "Secrecy capacity of the first-order autoregressive moving average Gaussian channel with feedback," in *Proc. IEEE Int. Symp. Inf. Theory*, Aachen, Germany, 2017, pp. 1963–1967.
[13] Y. H. Kim, "Feedback capacity of stationary Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 56, no. 1, pp. 57–85, 2010.
[14] C. Li and N. Elia, "Control approach to computing the feedback capacity for stationary finite dimensional Gaussian channels," in *Proc. 53th Annu. Allerton Conf. Commun., Control, Comput.*, Monticello, IL, 2015, pp. 1038–1045.
[15] ——, "Youla coding and computation of Gaussian feedback capacity," *IEEE Trans. Inf. Theory*, vol. 64, no. 4, pp. 3197–3215, 2018.
[16] N. Elia, "When Bode meets Shannon: Control-oriented feedback communication schemes," *IEEE Trans. Autom. Control*, vol. 49, no. 9, pp. 1477–1488, 2004.
[17] J. P. M. Schalkwijk, "A coding scheme for additive noise channels with feedback II: Band-limited signals," *IEEE Trans. Inf. Theory*, vol. IT-12, no. 2, pp. 183–189, 1966.
[18] N. C. Martins and T. Weissman, "Coding for additive white noise channels with feedback corrupted by quantization or bounded noise," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4274–4282, 2008.