The Wiretap Channel With Feedback: Encryption Over the Channel

Lifeng Lai, *Member, IEEE*, Hesham El Gamal, *Senior Member, IEEE*, and H. Vincent Poor, *Fellow, IEEE*

***Abstract*—In this work, the critical role of noisy feedback in enhancing the secrecy capacity of the wiretap channel is established. Unlike previous works, where a noiseless public discussion channel is used for feedback, the feed-forward and feedback signals share the same noisy channel in the present model. Quite interestingly, this noisy feedback model is shown to be more advantageous in the current setting. More specifically, the discrete memoryless modulo-additive channel with a full-duplex destination node is considered first, and it is shown that the judicious use of feedback increases the secrecy capacity to the capacity of the source–destination channel in the absence of the wiretapper. In the achievability scheme, the feedback signal corresponds to a private key, known only to the destination. In the half-duplex scheme, a novel feedback technique that always achieves a positive perfect secrecy rate (even when the source–wiretapper channel is less noisy than the source–destination channel) is proposed. These results hinge on the modulo-additive property of the channel, which is exploited by the destination to perform encryption over the channel without revealing its key to the source. Finally, this scheme is extended to the continuous real valued modulo-Λ channel where it is shown that the secrecy capacity with feedback is also equal to the capacity in the absence of the wiretapper.**

***Index Terms*—Feedback, modulo-additive, noisy, secrecy capacity, wiretap channel.**

I. Introduction

THE study of secure communication from an information-theoretic perspective was pioneered by Shannon [1]. In Shannon's model, both the sender and the destination possess a common secret key K, which is unknown to the wiretapper, and they use this key to encrypt and decrypt a message M. Shannon considered a scenario in which both the legitimate receiver and the wiretapper have direct access to the transmitted signal and introduced the perfect secrecy condition $I(M;Z)=0$, where $I(\cdot;\cdot)$ denotes mutual information between its two arguments. This implies that the signal Z received by the wiretapper does not provide any additional information about the source message M. Under this model, he proved that a one-time pad achieves perfect secrecy if the entropy of the shared private key K is at least equal to the entropy of the message itself (i.e., $H(K) \geq H(M)$ for perfect secrecy, where $H(\cdot)$ denotes the entropy of its argument).

In a second pioneering work [2], Wyner introduced the wiretap channel and established the possibility of creating an almost perfectly secure source–destination link without relying on private (secret) keys. In the wiretap channel, both the wiretapper and destination observe the source's encoded message through noisy channels. Similar to Shannon's model, the wiretapper is assumed to have unlimited computational resources. Wyner showed that when the source–wiretapper channel is a degraded version of the source–destination channel, the source can send perfectly secure[1] messages to the destination at a nonzero rate. The main idea is to hide the information stream in the additional noise impairing the wiretapper by using a stochastic encoder which maps each message to many codewords according to an appropriate probability distribution. This way, one induces maximal equivocation at the wiretapper. By ensuring that the equivocation rate is arbitrarily close to the message rate, one achieves perfect secrecy in the sense that the wiretapper is now limited to learn *almost nothing* about the source–destination messages from its observations. Follow-up work by Leung-Yan-Cheong and Hellman has characterized the secrecy capacity of the additive white Gaussian noise (AWGN) wiretap channel [4]. In a landmark paper, Csiszár and Körner generalized Wyner's approach by considering the transmission of confidential messages over broadcast channels [5]. This work characterized the secrecy capacity of the broadcast channel, and showed that the secrecy capacity is positive unless the source–wiretapper channel is *less noisy* than the source–destination channel (referred to as the main channel in the sequel).[2]

Positive secrecy capacity is not always possible to achieve in practice. In an attempt to transmit messages securely in these unfavorable scenarios, [6] and [7] considered the wiretap channel with noiseless feedback.[3] They showed that one may leverage the feedback to achieve a positive perfect secrecy rate, even when the feed-forward secrecy capacity is zero. In this model, there exists a separate noiseless public channel, through which the transmitter and receiver can exchange information. The wiretapper is assumed to obtain a perfect copy of the messages transmitted over this public channel. Upper and lower

Manuscript received April 12, 2007; revised May 3, 2008. Current version published October 22, 2008. This work was supported by the National Science Foundation under Grants ANI-03-38807, CNS-06-25637, and CCF-07-28208. The material in this paper was presented in part at the Conference on Communication, Control, and Computing, Monticello, IL, September 2007.

L. Lai and H. V. Poor are with the Department of Electrical Engineering, Princeton University, Princeton, NJ, 08544 USA (e-mail: llai@princeton.edu; poor@princeton.edu).

H. El Gamal is with the Department of Electrical and Computer Engineering, Ohio State University, Columbus, OH, 43210 USA. He also serves as the Founding Director for the Wireless Intelligent Networks Center (WINC), Nile University, Cairo, Egypt (e-mail: helgamal@ece.osu.edu).

Communicated by G. Kramer, Associate Editor for Shannon Theory.

Digital Object Identifier 10.1109/TIT.2008.929914

[1]Wyner's notion of per-symbol equivocation is weaker than Shannon's notion of perfect secrecy [3].

[2]The source–wiretapper channel is said to be less noisy than the main channel if, for every V satisfying the Markov chain relationship $V \rightarrow X \rightarrow YZ$, $I(V;Z) \geq I(V;Y)$, where X is the signal transmitted by the source, and where Y and Z are the signal received at the receiver and the wiretapper, respectively.

[3]The authors also considered a more general secret sharing problem.

bounds were derived for the secrecy capacity with noiseless feedback in [6], [7]. In several cases, as discussed in detail in the sequel, these bounds coincide. But, in general, the secrecy capacity with noiseless feedback remains unknown. Along the same lines, [8] established the critical role of a trusted/untrusted helper in enhancing the secret key capacity of public discussion algorithms. The multiterminal generalization of the basic setup of [6], [7] was studied in [9]. Finally, in [10]–[12], the public discussion paradigm was extended to handle the existence of active adversaries.

Our work represents a marked departure from the public discussion paradigm. In our model, we do not assume the existence of a separate noiseless feedback channel. Instead, the feedback signal from the destination, which is allowed to depend on the signal received so far, is transmitted over the same noisy channel used by the source. Based on the noisy feedback signal, the source can then causally adapt its transmission scheme, hoping to increase the perfect secrecy rate. The wiretapper receives a mixture of the signal from the source and the feedback signal from the destination. Quite interestingly, we show that in the modulo-additive discrete memoryless channel (DMC) with a full-duplex destination, the secrecy capacity with noisy feedback equals the capacity of the main channel in the absence of the wiretapper. Furthermore, the capacity is achieved with a simple scheme in which the source ignores the feedback signal and the destination feeds back randomly generated symbols from a certain alphabet set. This feedback signal plays the role of a private key, known only by the destination, and encryption is performed by the modulo-additive channel. The more challenging scenario with a half-duplex destination, which cannot transmit and receive simultaneously, is considered next. Here, the active transmission periods by the destination will introduce erasures in the feed-forward source–destination channel. In this setting, we propose a novel feedback scheme that achieves a positive perfect secrecy rate for any nontrivial channel distribution. The feedback signal in our approach acts as a private *destination only* key which strikes the optimal tradeoff between introducing erasures at the destination and errors at the wiretapper. Finally, the proposed scheme is extended to the continuous modulo-Λ lattice channel where it is shown to achieve the capacity of the main channel.

Overall, our work proposes a novel approach for encryption where 1) the feedback signal is used as a private key known only to the destination; and 2) the encryption is performed by exploiting the modulo-additive property of the channel. This encryption approach is shown to be significantly superior to the classical public discussion paradigm. The achievable scheme proposed here for the full-duplex scenario also appeared concurrently and independently in [13] under a different setup. In [13], a two-way wiretap channel is considered, in which both the source and receiver transmit information over the channel to each other in the presence of a wiretapper. Achievable rates for the two-way Gaussian channel and the two-way binary additive channel are derived. It is shown that in this setup, it is possible to gain a secrecy sum-rate larger than the capacity of the source–destination channel in the absence of the wiretapper. Our goal, however, is to understand the role of feedback on enhancing security in communication. Hence, in general, the codeword sent by the source and receiver will depend on what has been received so far. It turns out that in the modulo-additive channel, this dependence is not necessary. A simple scheme achieves the capacity. On the other hand, it is not clear whether this is true for general channels or not.

Recently, there has been a resurgent interest in studying secure communications from an information-theoretic perspective under various scenarios. The point-to-point fading eavesdropper channel was considered in [14]–[18] under different assumptions on the delay constraints and the available transmitter channel state information (CSI). In [19]–[22], the information-theoretic limits of secure communications over multiple-access channels were explored. The relay channel with confidential messages, where the relay acts both as a wiretapper and a helper, was studied in [23], [24]. In [25], the interference channel with confidential messages was studied. In [26], the four-terminal relay–eavesdropper channel was introduced and analyzed. The wiretap channel with side information was studied in [27].

The rest of the paper is organized as follows. In Section II, we introduce the system model of interest and our notation. Section III describes and analyzes the proposed feedback scheme that achieves the capacity of the full duplex modulo-additive DMC. Taking the binary symmetric channel (BSC) as an example, we then compare the performance of the proposed scheme with the public discussion approach. The half-duplex scenario is studied in Section IV. In Section V, we extend our results to the modulo-Λ lattice channel. Finally, Section VI offers some concluding remarks and outlines possible venues for future research.

II. The Modulo-Additive Discrete Memoryless Channel (DMC)

Throughout the sequel, an upper-case letter X will denote a random variable, a lower-case letter x will denote a realization of the random variable, a calligraphic letter $\mathcal{X}$ will denote a finite alphabet set, and a boldface letter $\boldsymbol{x}$ will denote a vector. Furthermore, we let $[x]^+ = \max\{0, x\}$.

Without feedback, our modulo-additive discrete memoryless wiretap channel is described by the following model:

$$\begin{aligned} Y &= X + N_1 \\ Z &= X + N_2 \end{aligned} \tag{1}$$

where Y is the received symbol at the destination, Z is the received symbol at the wiretapper, X is the channel input, N_1 and N_2 are the noise samples at the destination and wiretapper, respectively. Here N_1 and N_2 are allowed to be correlated. Also, we assume that X ranges over a finite set $\mathcal{X} = \{0, 1, \ldots, |\mathcal{X}| - 1\}$, Y and N_1 range over a finite set $\mathcal{Y} = \{0, 1, \ldots, |\mathcal{Y}| - 1\}$, and Z and N_2 range over a finite set $\mathcal{Z} = \{0, 1, \ldots, |\mathcal{Z}| - 1\}$. We denote the alphabet size of the sets $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$ by $|\mathcal{X}|$, $|\mathcal{Y}|$, and $|\mathcal{Z}|$ respectively. Here "+" is understood to be modulo addition with respect to the corresponding alphabet size, i.e., $Y = [X + N_1] \bmod |\mathcal{Y}|$ and $Z = [X + N_2] \bmod |\mathcal{Z}|$ with addition in the real field.

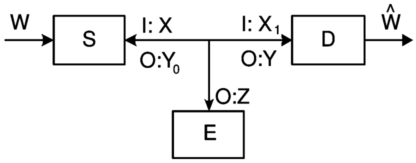

Fig. 1. The wiretap channel with noisy feedback. In this figure, "I" represents Input and "O" represents Output. The relationships among the variables are given in (2).

In this paper, we focus on the wiretap channel with noisy feedback.[4] More specifically, at time i, the destination sends the causal feedback signal $X_1(i)$ over the same noisy channel used for feed-forward transmission, i.e., we do not assume the existence of a separate noiseless feedback channel. The causal feedback signal is allowed to depend on time index i and the signal received so far $Y^{i-1} = \{Y(1), \dots, Y(i-1)\}$, i.e., $X_1(i) = \Psi_i(Y^{i-1})$, where Ψ_i can be any (possibly stochastic) function. In general, we allow the destination to choose the alphabet of the feedback signal $\mathcal{X}_1$ and the corresponding size $|\mathcal{X}_1|$. With this *noisy* feedback from the destination, the received signals at the source, wiretapper and destination are

$$\begin{aligned} Y_0 &= X + X_1 + N_0 \\ Y &= X + X_1 + N_1 \quad \text{and} \\ Y &= X + X_1 + N_2 \end{aligned} \tag{2}$$

respectively. Here Y_0 is the received noisy feedback signal at the source, which ranges over a finite set $\mathcal{Y}_0 = \{0, 1, \dots, |\mathcal{Y}_0| - 1\}$; and N_0 is the feedback noise, which ranges over the finite set $\mathcal{Y}_0$ and may be correlated with N_1 and N_2. We denote the alphabet size of the set $\mathcal{Y}_0$ by $|\mathcal{Y}_0|$. Again, all "+" operation should be understood to be modulo-addition with respect to the corresponding alphabet size. Fig. 1 shows the model described above.

Now, the source wishes to send the message W ranging over the set $\mathcal{W} = \{1, \dots, M\}$ to the destination using an (M, n) code consisting of: 1) a sequence of causal stochastic encoders $f_i, i = 1, \dots, n$ at the source that maps the message w and the received noisy feedback signal $Y_0^{i-1} = \{Y_0(1), \dots, Y_0(i-1)\}$ to $X(i)$ sent at time i, i.e.,

$$X(i) = f_i\left(W, Y_0^{i-1}\right); \tag{3}$$

2) a sequence of stochastic feedback encoders $\Psi_i, i = 1, \dots, n$ at the destination that maps the received signal into $X_1(i)$ with $X_1(i) = \Psi_i(Y^{i-1})$; and 3) a decoding function at the destination d: $\mathcal{Y}^n \to \mathcal{W}$. The average error probability of the (M, n) code is

$$P_e^n = \sum_{w \in \mathcal{W}} \frac{1}{M} \Pr\{d(\boldsymbol{y}) \neq w | w \text{ was sent}\}. \tag{4}$$

The equivocation rate at the wiretapper is defined as

$$R_e = \frac{1}{n} H(W|\boldsymbol{Z}). \tag{5}$$

We are interested in perfectly secure transmission rates defined as follows.

[4]In this paper, by noisy feedback, we mean that the source receives a noisy version of the feedback signal sent by the receiver.

Definition 1: A secrecy rate R^f is said to be achievable over the wiretap channel with noisy feedback if for any $\epsilon > 0$, there exists a positive number n_0 and a sequence of codes (M, n) such that for all $n \geq n_0$, we have

$$R^f = \frac{1}{n} \log_2 M \tag{6}$$

$$P_e^n \leq \epsilon \tag{7}$$

and

$$\frac{1}{n} H(W|\boldsymbol{Z}) \geq R^f - \epsilon. \tag{8}$$

Definition 2: The secrecy capacity with noisy feedback C_s^f is the maximum rate at which messages can be sent to the destination with perfect secrecy; i.e.,

$$C_s^f = \sup_{f_i, \Psi_i, i=1,\dots,n} \{R^f : R^f \text{ is achievable}\}. \tag{9}$$

Note that in our model, the wiretapper is assumed to have unlimited computational resources and to know the coding scheme of the source and the feedback function Ψ_i used by the destination. This feedback model captures realistic scenarios in which the terminals exchange information over noisy channels.

III. The Wiretap Channel With Full-Duplex Feedback

A. Known Results

The secrecy capacity C_s of the wiretap DMC without feedback was characterized in [5]. Specializing to our modulo-additive channel, one obtains

$$C_s = \max_{V \to X \to YZ} [I(V;Y) - I(V;Z)]^+. \tag{10}$$

The wiretap DMC with public discussion was introduced and analyzed in [6], [7]. More specifically, these papers considered a more general model in which all the nodes observe correlated variables,[5] and there exists an extra noiseless public channel with infinite capacity, through which both the source and the destination can send information. Combining the correlated variables and the publicly discussed messages, the source and the destination generate a key about which the wiretap has only negligible information. Please refer to [7] for rigorous definitions of these notions. Since the public discussion channel is noiseless, the wiretapper is assumed to observe a noiseless version of the information transmitted over it. The following theorem gives upper and lower bounds on the secret key capacity of the public discussion paradigm C_s^p.

Theorem 3 ([6], [7]): The secret key capacity of the public discussion approach satisfies the following conditions:

$$\max\left\{\max_{P_X}[I(X;Y) - I(X;Z)], \max_{P_X}[I(X;Y) - I(Y;Z)]\right\} \leq C_s^p \leq \min\left\{\max_{P_X} I(X;Y), \max_{P_X} I(X;Y|Z)\right\}.$$

Proof: Please refer to [6], [7]. □

These bounds are known to be tight in the following cases [6], [7].

[5]The wiretap channel model is a particular mechanism for the nodes to observe the correlated variables, and corresponds to the "channel type model" studied in [7].

1) $P_{YZ|X} = P_{Y|X}P_{Z|X}$, i.e., the main channel and the source–wiretapper channel are independent; in this case

$$C_s^p = \max_{P_X}\{I(X;Y) - I(Y;Z)\}. \tag{11}$$

2) $P_{XZ|Y} = P_{X|Y}P_{Z|Y}$, i.e., $X \to Y \to Z$ forms a Markov chain, and hence the source–wiretapper channel is a degraded version of the main channel. In this case

$$C_s^p = \max_{P_X}\{I(X;Y) - I(X;Z)\}. \tag{12}$$

This is also the secrecy capacity of the degraded wiretap channel without feedback. Hence, public discussion does not increase the secrecy capacity for the degraded wiretap channel.

3) $P_{XY|Z} = P_{X|Z}P_{Y|Z}$, i.e., $X \to Z \to Y$, so that the main channel is a degraded version of the wiretap channel. In this case

$$C_s^p = 0. \tag{13}$$

Again, public discussion does not help in this scenario.

B. The Main Result

The following theorem characterizes the secrecy capacity of the wiretap channel with noisy feedback. Moreover, achievability is established through a novel encryption scheme that exploits the modulo-additive structure of the channel and uses a private key known only to the destination.

Theorem 4: The secrecy capacity of the discrete memoryless modulo-additive wiretap channel with noisy feedback is

$$C_s^f = C \tag{14}$$

where C is the capacity of the main channel in the absence of the wiretapper.

Proof:

1. Converse.

The set of achievable secrecy rates with feedback is a subset of the set of achievable rates of an ordinary (i.e., without security constraints) DMC with feedback. It is well known that feedback does not increase the capacity of an ordinary DMC, and hence C is the supremum of the set of the achievable rates of an ordinary DMC with feedback. Thus, C is also an upper bound of the achievable secrecy rate with feedback.

2. Achievability.

We use the following scheme.

For the feedback part, the destination sets $\mathcal{X}_1 = \mathcal{Z}$, and at any time i, sets $X_1 = a$, $a \in \{0, \dots, |\mathcal{Z}| - 1\}$ with probability $1/|\mathcal{Z}|$. Hence, $\boldsymbol{X}_1$ is uniformly distributed over $\mathcal{Z}^n$.

If the source transmits $\boldsymbol{x}$, the wiretapper will receive

$$\boldsymbol{Z} = \boldsymbol{x} + \boldsymbol{X}_1 + \boldsymbol{N}_2 \tag{15}$$

and $\boldsymbol{X}_1$ is uniformly distributed over $\mathcal{Z}^n$ and is independent of $\boldsymbol{x}$. Based on the crypto lemma [28], for any given $\boldsymbol{x}$, $\boldsymbol{x} + \boldsymbol{X}_1$ is uniformly distributed over $\mathcal{Z}^n$, and hence, $\boldsymbol{z}$ is uniformly distributed over $\mathcal{Z}^n$ for any transmitted codeword $\boldsymbol{x}$ and noise realization $\boldsymbol{n}_2$. Moreover, $\boldsymbol{Z}$ is independent of $\boldsymbol{X}$, and thus

$$I(\boldsymbol{X};\boldsymbol{Z}) = 0. \tag{16}$$

Hence, we have $I(W;\boldsymbol{Z}) \leq I(\boldsymbol{X};\boldsymbol{Z}) = 0$; therefore

$$\frac{1}{n}H(W|\boldsymbol{Z}) = \frac{H(W) - I(W;\boldsymbol{Z})}{n} = \frac{H(W)}{n}, \tag{17}$$

and we achieve perfect secrecy.

Thus, by this feedback scheme, for **any** codebook used by the source, we achieve perfect secrecy at the receiver. Now in our scheme, the source ignores the feedback signal from the destination, and uses a codebook that achieves rate R^f for the main channel. For decoding, after receiving $\boldsymbol{y}$, the destination sets $\hat{\boldsymbol{y}} = \boldsymbol{y} - \boldsymbol{x}_1$, where "$-$" is understood to be a component-wise modulo $|\mathcal{Y}|$ operation. It is easy to see that $\hat{\boldsymbol{y}} = \boldsymbol{x} + \boldsymbol{n}_1$. The destination then claims that $\hat{w}$ was sent if $(\hat{\boldsymbol{y}}, \boldsymbol{x}(\hat{w}))$ is jointly typical. For any given $\epsilon > 0$, the probability that $\hat{w} \neq w$ goes to zero as n increases, provides $R^f = I(X;\hat{Y}) - \epsilon = I(X;Y|X_1) - \epsilon$. The channel $X \to \hat{Y}$ is equivalent to the main channel without feedback. Hence, as long as $R^f < C$, there exists a code with sufficient code length such that $P_e^n \leq \epsilon$ for any $\epsilon > 0$. □

The following observations are now in order.

1) Our scheme achieves $I(W;\boldsymbol{Z}) = 0$. This implies perfect secrecy in the strong sense of Shannon [1] as opposed to Wyner's notion of perfect secrecy [2], which has been pointed out to be insufficient for certain encryption applications [3].
2) The enabling observation behind our achievability scheme is that, by judiciously exploiting the modulo-additive structure of the channel, one can render the channel output at the wiretapper independent of the codeword transmitted by the source. Here, the feedback signal $\boldsymbol{x}_1$ serves as a private key and the encryption operation is carried out by the channel. Instead of requiring both the source and destination to know a common encryption key, we show that only the destination needs to know the encryption key, hence eliminating the burden of secret key distribution.
3) Remarkably, the secrecy capacity with *noisy* feedback is shown to be larger than the secret key capacity of public discussion schemes. This point will be further illustrated by the BSC example discussed next. This presents a marked departure from the conventional wisdom, inspired by the data processing inequality, which suggests the superiority of noiseless feedback. This result is due to the fact that the noiseless feedback signal is also available to the wiretapper, while in the proposed noisy feedback scheme neither the source nor the wiretapper knows the feedback signal perfectly. In fact, the source in our scheme ignores the feedback signal, which is used primarily to *confuse* the wiretapper.
4) Our result shows that complicated feedback functions Ψ are not needed to achieve optimal performance in this setting (i.e., a random number generator suffices). Also, the alphabet size of the feedback signal can be set equal to the alphabet size of the wiretapper channel, and the coding

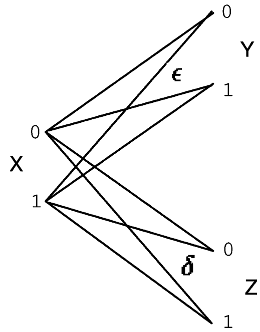

Fig. 2. The binary symmetric wiretap channel.

scheme used by the source is the same as the one used in the absence of the wiretapper.

C. The Binary Symmetric Channel (BSC) Example

To illustrate the idea of encryption over the channel, we consider in some detail the wiretap BSC shown in Fig. 2, where $\mathcal{X}=\mathcal{Y}=\mathcal{Z}=\{0,1\}$, $\Pr\{N_1=1\}=\epsilon$, and $\Pr\{N_2=1\}=\delta$. The secrecy capacity of this channel without feedback is known to be [6]

$$C_s = [H(\delta) - H(\epsilon)]^+$$

with $H(x) = -x \log x - (1-x)\log(1-x)$. We differentiate between the following special cases.

1) $\epsilon = \delta = 0$
In this case, both the main channel and wiretap channel are noiseless, hence

$$C_s = 0.$$

Also, we have

$$C_s^p = 0$$

since the wiretapper sees exactly the same as what the destination sees. Specializing our scheme to this BSC, at time i, the destination randomly chooses $X_1 = 1$ with probability $1/2$ and sends X_1 over the channel. This creates a virtual BSC at the wiretapper with $\delta' = 1/2$. On the other hand, since the destination knows the value of X_1, it can cancel it by adding X_1 to the received signal. This converts the original channel to an equivalent BSC with $\epsilon' = 0$. Hence, through our noisy feedback approach, we obtain an equivalent wiretap BSC with parameters $\epsilon' = 0, \delta' = 1/2$ resulting in

$$C_s^f = H(\delta') - H(\epsilon') = 1.$$

2) $0 < \delta < \epsilon < 1/2$, N_1, and N_2 are independent.
Since $\delta < \epsilon$, we have

$$C_s = 0.$$

Also, N_1 and N_2 are independent, so $P_{YZ|X} = P_{Y|X}P_{Z|X}$. Then from (11), one can easily obtain that [6]

$$C_s^p = H(\epsilon + \delta - 2\epsilon\delta) - H(\epsilon).$$

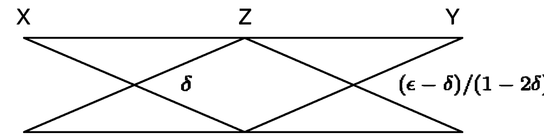

Fig. 3. The binary symmetric wiretap channel with a degraded main channel.

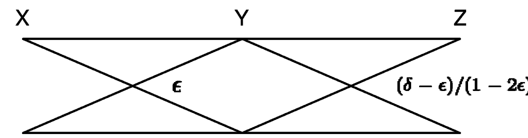

Fig. 4. The binary symmetric wiretap channel with a degraded source–wiretapper channel.

Our feedback scheme, on the other hand, achieves

$$C_s^f = 1 - H(\epsilon).$$

Since $H(\epsilon+\delta-2\epsilon\delta) \le 1$, we have $C_s^f \ge C_s^p$ with equality if and only if $\epsilon + \delta - 2\epsilon\delta = 1/2$.

3) $0 < \delta < \epsilon < 1/2$ and $N_1 = N_2 + N'$, where $\Pr\{N' = 1\} = (\epsilon - \delta)/(1 - 2\delta)$.
The main channel is a degraded version of the source–wiretapper channel $X \to Z \to Y$, as shown in Fig. 3. Hence, from (13), we have

$$C_s = C_s^p = 0$$

while $C_s^f = 1 - H(\epsilon)$.

4) $0 < \epsilon < \delta < 1/2$, and $N_2 = N_1 + N'$, where $\Pr\{N' = 1\} = (\delta - \epsilon)/(1 - 2\epsilon)$.
In this case, the source-wiretapper channel is a degraded version of the main channel as shown in Fig. 4; $X \to Y \to Z$, so from (12)

$$C_s = C_s^p = H(\delta) - H(\epsilon).$$

But

$$C_s^f = 1 - H(\epsilon) \ge C_s^p$$

with equality if and only if $\delta = 1/2$.

5) N_1 and N_2 are correlated and the channel is not degraded.
In this case

$$C_s = [H(\delta) - H(\epsilon)]^+.$$

The value of C_s^p is unknown in this case but can be bounded by

$$C_s = [H(\delta) - H(\epsilon)]^+ \le C_s^p \le 1 - H(\epsilon) = C_s^f.$$

In summary, the secrecy capacity with noisy feedback is always larger than or equal to that of the public discussion paradigm when the underlying wiretap channel is a BSC. More strongly, the gain offered by the noisy feedback approach, over the public discussion paradigm, is rather significant in many relevant special cases.

IV. Even Half-Duplex Feedback Is Sufficient

It is reasonable to argue against the *practicality* of the full duplex assumption adopted in the previous section. In certain applications, nodes may not be able to transmit and receive with the same degrees of freedom. This motivates extending our results to the half-duplex wiretap channel in which the terminals can either transmit or receive but never both at the same time. Under this situation, if the destination wishes to feed back at time i, it loses the opportunity to receive the ith symbol transmitted by the source, which effectively results in an erasure (assuming that the source is unaware of the destination decision). The proper feedback strategy must, therefore, strike a balance between confusing the wiretapper and degrading the source–destination link. In order to simplify the following presentation, we first focus on the wiretap BSC. The extension to arbitrary modulo-additive channels is briefly outlined afterwards.

In the full-duplex case, the optimal scheme is to let the destination send X_1, which equals 0 or 1 with equal probabilities of $1/2$. But in the half-duplex case, if the destination always keeps sending, it does not have a chance to receive information from the source, and hence, the achievable secrecy rate is zero. This problem, however, can be solved by observing that if $X_1 = 0$, the signal the wiretapper receives, i.e.,

$$Z = X + N_2,$$

is the same as in the case in which the destination does not transmit. The crucial difference in this case is that the wiretapper does not know whether the feedback has taken place or not, since X_1 can be randomly generated at the destination and thus kept private.

The previous discussion inspires the following feedback scheme for the half-duplex channel. The destination first fixes a fraction $0 \leq t \leq 1$ which is revealed to both the source and wiretapper. At time i, the destination randomly generates $X_1 = 1$ with probability t and $X_1 = 0$ with probability $1 - t$. If $X_1 = 1$, the destination sends X_1 over the channel, which causes an erasure at the destination and a potential error at the wiretapper. On the other hand, when $X_1 = 0$, the destination does not send a feedback signal and spends the time on receiving from the channel. The key to this scheme is that although the source and wiretapper know t, neither is aware of the exact timing of the events $X_1 = 1$. The source ignores the feedback and keeps sending information. The following result characterizes the achievable secrecy rate with the proposed feedback scheme.

Theorem 5: For a BSC with half-duplex nodes and parameters ϵ and δ, the scheme proposed above achieves

$$R_s^f = \max_{\mu,t}\Big[(1-t)\left[H(\epsilon+\mu-2\mu\epsilon) - H(\epsilon)\right] - \left[H(\hat{\delta}+\mu-2\mu\hat{\delta}) - H(\hat{\delta})\right]\Big]^+ \quad (18)$$

with $\hat{\delta} = \delta + t - 2\delta t$.

Proof: For the main channel, if the destination spends a fraction t of its time on sending, the equivalent main channel

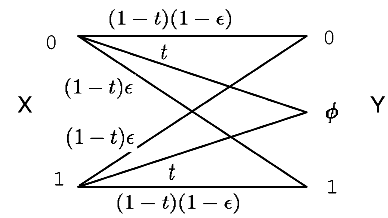

Fig. 5. The equivalent main channel.

is shown in Fig. 5. In this figure, the output $\hat{Y}$ ranges over a finite-alphabet set $\{0, \phi, 1\}$, where ϕ represents an erasure. The erasure probability is t. In the remaining $1 - t$ fraction of the time, the channel is a BSC with parameter ϵ. Hence, the transition matrix of this equivalent channel is

$$\begin{bmatrix} (1-t)(1-\epsilon) & t & (1-t)\epsilon \\ (1-t)\epsilon & t & (1-t)(1-\epsilon) \end{bmatrix}.$$

Meanwhile for the wiretapper, the equivalent channel is still a BSC, but with an increased error probability

$$\hat{\delta} = (1-t)\delta + t(1-\delta) = \delta + t - 2\delta t. \quad (19)$$

Thus, the original binary symmetric wiretap channel with noisy feedback is equivalent to a new wiretap channel $X \rightarrow (\hat{Y}, Z)$ without feedback, and the channel parameters are given as above.

As shown in [5], for this equivalent wiretap channel the following secrecy rate is achievable for any input distribution P_X:

$$R^f = [I(X;\hat{Y}) - I(X;Z)]^+. \quad (20)$$

Hence, by using the input distribution $\Pr\{X = 1\} = \mu$, one can see that

$$R^f = \max_{\mu,t}\Big[(1-t)\left[H(\epsilon+\mu-2\mu\epsilon) - H(\epsilon)\right] - \left[H(\hat{\delta}+\mu-2\mu\hat{\delta}) - H(\hat{\delta})\right]\Big]^+ \quad (21)$$

is achievable. □

In general, one can obtain the optimal values of μ and t by setting the partial derivative of R^f, with respect to μ and t to 0, and solving the corresponding equations. Unfortunately, except for some special cases, we do not have a closed-form solution for these equations at the moment. Interestingly, using the not necessarily optimal choice of $\mu = t = 1/2$, we obtain $R^f = (1 - H(\epsilon))/2$ implying that we can achieve a nonzero secrecy rate as long as $\epsilon \neq 1/2$ irrespective of the wiretapper channel conditions. Hence, even for half-duplex nodes, noisy feedback from the destination allows for transmitting information securely for *almost* any wiretap BSC. Finally, we compare the performance of different schemes in some special cases of the wiretap BSC.

1) $\epsilon = \delta = 0$.

As mentioned above, here we have $C_s = C_s^p = 0$. It is easy to verify that the optimal choice of μ and t are $1/2$ and $1/3$, respectively, and we thus have $R_s^f = \log 3 - 1$.

2) $0<\delta<\epsilon<1/2$ and $N_1=N_2+N'$, where $\Pr\{N'=1\}=(\epsilon-\delta)/(1-2\delta)$.
The main channel is a degraded version of the wiretap channel, so

$$C_s = C_s^p = 0. \tag{22}$$

But by setting $\mu = t = 1/2$ in our half-duplex noisy feedback scheme, we obtain $R_s^f = (1-H(\epsilon))/2$.

The extension to the general discrete modulo-additive channel is natural. The destination can set $\mathcal{X}_1 = \mathcal{Z}$, and generates X_1 with a certain distribution P_{X_1}. If the randomly generated $X_1 \neq 0$, the destination sends a feedback signal, incurring an erasure to itself. On the other hand, if $X_1 = 0$, it does not send the feedback signal and spends the time listening to the source. The achievable performance could be calculated based on the equivalent channels as done in the BSC. This scheme guarantees a positive secrecy capacity as seen in the case where P_{X_1} is chosen to be uniformly distributed over $\mathcal{Z}$. This is because a uniform distribution over $\mathcal{Z}$ renders the output at the wiretapper independent from the source input, i.e., $I(W;Z) = 0$, while the destination can still spend $1/|\mathcal{Z}|$ part of the time listening to the source. Finding the optimal distribution P_{X_1}, however, is tedious.

V. The Modulo-Λ Channel

In this section, we take a step toward extending our approach to continuous-valued channels. In particular, we consider the modulo-Λ channel [29]–[32]. This choice is motivated by two considerations: 1) this channel still enjoys the *modulo* structure which proved instrumental in deriving our results in the discrete case, and 2) the modulo-Λ channel has been shown to play an important role in achieving the capacity of the AWGN channel using lattice coding/decoding techniques [31]. In other words, an AWGN source–destination channel can be well approximated by a modulo-Λ channel. In the following, we show that, similar to the discrete case, noisy feedback can increase the secrecy capacity of the wiretap modulo-Λ channel to that of the main channel capacity in the absence of the wiretapper.

Before proceeding further, we need to introduce a few more definitions. We let $\mathbb{R}$ denote the set of real numbers. An m-dimensional lattice $\Lambda \subset \mathbb{R}^m$ is a set of points

$$\Lambda \triangleq \{\boldsymbol{\lambda} = \boldsymbol{G}\boldsymbol{u} : \boldsymbol{u} \in \mathbb{Z}^m\} \tag{23}$$

where $\boldsymbol{G} \in \mathbb{R}^{m\times m}$ denotes the lattice generator matrix. A fundamental region $\Omega \in \mathbb{R}^m$ of Λ is a set such that each $\boldsymbol{x} \in \mathbb{R}^m$ can be written uniquely in the form $\boldsymbol{x} = \boldsymbol{\lambda} + \boldsymbol{e}$ with $\boldsymbol{\lambda} \in \Lambda$, $\boldsymbol{e} \in \Omega$, and $\mathbb{R}^m = \Lambda + \Omega$. There are many different choices of the fundamental region, each with the same volume, which will be denoted as $V(\Lambda)$. Given a lattice Λ, a fundamental region Ω of Λ, and a zero-mean white Gaussian noise process with variance σ_1^2 per dimension, the modulo-Λ (mod-Λ) channel is defined as follows [29].

Definition 6 ([29]): The input of the mod-Λ channel consists of points $\boldsymbol{X} \in \Omega$; the output of the mod-$\Lambda$ channel is $\boldsymbol{Y} = (\boldsymbol{X} + \boldsymbol{N}_1) \bmod \Lambda$, where $\boldsymbol{N}_1$ is an m-dimensional white Gaussian noise variable with variance σ_1^2 per dimension. Hence, $\boldsymbol{Y}$ is the unique element of Ω that is congruent to $\boldsymbol{X} + \boldsymbol{N}_1$.

In our wiretap mod-Λ channel, the output at the wiretapper (in the absence of feedback) is also given by $\boldsymbol{Z} = (\boldsymbol{X} + \boldsymbol{N}_2) \bmod \Lambda$. Here $\boldsymbol{N}_2$ is an m-dimensional white Gaussian noise variable with variance σ_2^2 per dimension. Similar to Section II, we consider noisy feedback, where the destination sends a feedback signal $\boldsymbol{X}_1 \in \Omega$ based on its received signal, and the received signal at the source is $\boldsymbol{Y}_0 = (\boldsymbol{X} + \boldsymbol{X}_1 + \boldsymbol{N}_0) \bmod \Lambda$, where $\boldsymbol{N}_0$ is an m-dimensional white Gaussian noise with variance σ_0^2 per dimension. Now, the received signal at the destination and wiretapper are $\boldsymbol{Y} = (\boldsymbol{X}+\boldsymbol{X}_1+\boldsymbol{N}_1) \bmod \Lambda$ and $\boldsymbol{Z} = (\boldsymbol{X}+\boldsymbol{X}_1+\boldsymbol{N}_2) \bmod \Lambda$, respectively.

For example, if $m = 1$, $\Lambda = \mathbb{Z}$ is a lattice in $\mathbb{R}$, with $[-1/2, 1/2)$ being one of its fundamental regions. With this lattice and fundamental region, the output at the destination is $Y = (X + X_1 + N_1) \bmod \Lambda = X + X_1 + N_1 - \lfloor X + X_1 + N_1 + 1/2 \rfloor$, where N_1 is a one-dimensional Gaussian random variable with variance σ_1^2. Here, $\lfloor x \rfloor$ denotes the largest integer that is smaller than x. One can easily check that $Y \in [1/2, 1/2)$. The output at the wiretapper and source can be written in a similar manner. This $m = 1$ example can be viewed as the continuous counterpart of the discrete channels considered in Section III.

On setting $\boldsymbol{N}' = \boldsymbol{N}_1 \bmod \Lambda$, and letting $f_{\Lambda,\sigma_1^2}(\boldsymbol{n}')$ be the probability density function of $\boldsymbol{N}'$, one can easily verify that [29]

$$f_{\Lambda,\sigma_1^2}(\boldsymbol{n}') = \sum_{\boldsymbol{b}\in\Lambda} \left(2\pi\sigma_1^2\right)^{-\frac{m}{2}} \exp^{-\|\boldsymbol{n}'+\boldsymbol{b}\|^2/2\sigma_1^2}, \quad \boldsymbol{n}' \in \Omega. \tag{24}$$

Denote the differential entropy of the noise term $\boldsymbol{N}'$ by $h\left(\Lambda, \sigma_1^2\right)$. Then

$$h\left(\Lambda, \sigma_1^2\right) = -\int_{\Omega(\Lambda)} f_{\Lambda,\sigma_1^2}(\boldsymbol{n}') \log f_{\Lambda,\sigma_1^2}(\boldsymbol{n}') \mathrm{d}\boldsymbol{n}'. \tag{25}$$

We are now ready to prove the following.

Theorem 7: The secrecy capacity of the mod-Λ channel with noisy feedback is

$$C_s^f = \log(V(\Lambda)) - h\left(\Lambda, \sigma_1^2\right). \tag{26}$$

Proof: The proof follows along the same lines as that of Theorem 4. For the converse, (26) was shown to be the capacity of the mod-Λ channel in the absence of the wiretap in [29], which naturally serves as an upper bound for the secrecy capacity, as argued in the proof of Theorem 4.

To achieve this secrecy capacity, the source generates length-n codewords $\boldsymbol{x}$, with the ith element $\boldsymbol{x}(i)$ being chosen uniformly from Ω. Hence, each codeword $\boldsymbol{x} \in \Omega^n \subset \mathbb{R}^{n\times m}$. Now, at time i, the destination generates feedback signals $\boldsymbol{x}_1(i)$ uniformly over the set Ω, and thus the feedback signal $\boldsymbol{X}_1$ is uniformly distributed over Ω^n. Based on the crypto lemma, for any codeword $\boldsymbol{x}$ and any particular noise realization $\boldsymbol{n}_1$, the length-n random variable received at the wiretapper

$$\boldsymbol{Z} = \boldsymbol{x} + \boldsymbol{X}_1 + \boldsymbol{n}_1 \bmod \Lambda$$

is uniformly distributed over Ω^n and is independent of $\boldsymbol{X}$. Hence, we have

$$I(\boldsymbol{X};\boldsymbol{Z}) = 0. \tag{27}$$

On the other hand, with $\boldsymbol{X}$ uniformly distributed over Ω^n, the mutual information between X and $\boldsymbol{Y}$ given $\boldsymbol{X}_1$ (the destination knows $\boldsymbol{X}_1$) is

$$\frac{1}{n}I(\boldsymbol{X};\boldsymbol{Y}|\boldsymbol{X}_1) = \log(V(\Lambda)) - h\left(\Lambda, \sigma_1^2\right). \tag{28}$$

So, for any $\epsilon > 0$, there exists a code with rate $R^f = C^f - \epsilon$ and $I(M;\boldsymbol{Z}) = 0$. This completes the achievablity part. □

Our result for the modulo-Λ channel sheds some light on the more challenging scenario of the wiretap AWGN channel with feedback. The difference between the two cases results from the *modulo* restrictions imposed on the destination and wiretapper outputs. The first constraint does not entail any loss of generality due to the optimality of the modulo-Λ approach in the AWGN setting [31]. Relaxing the second constraint, however, poses a challenge because it destroys the *modulo* structure necessary to hide the information from the wiretapper (i.e., the crypto lemma needs the group structure). In other words, if the wiretapper is not limited by the modulo-operation, then it can gain some additional information about the source message from its observations. Therefore, finding the secrecy capacity of the wiretap AWGN channel with noisy feedback remains elusive. At the moment, one can compute an achievable rate using a Gaussian signal as the feedback signal from the receiver [13]. This achievable rate approaches the capacity of the main channel only when the available power at the receiver is infinite.

VI. Conclusion

In this paper, we have obtained the secrecy capacity (or achievable rate) for several instantiations of the wiretap channel with noisy feedback. More specifically, with a full-duplex destination, it has been shown that the secrecy capacity of modulo-additive channels is equal to the capacity of the source–destination channel in the absence of the wiretapper. Furthermore, the secrecy capacity is achieved with a simple scheme in which the destination randomly chooses its feedback signal from a certain alphabet set. Interestingly, with a slightly modified feedback scheme, we are able to achieve a positive secrecy rate for the half-duplex channel. Overall, our work has revealed a new encryption paradigm that exploits the structure of the wiretap channel and uses a private key known only to the destination. We have shown that this paradigm significantly outperforms the public discussion approach for sharing private keys between the source and destination.

Our results motivate several interesting directions for future research. For example, characterizing the secrecy capacity of arbitrary DMCs (and the AWGN channel) with feedback remains an open problem. From an algorithmic perspective, it is also important to understand how to exploit different channel structures (in addition to the modulo-additive one) for encryption purposes. Finally, extending our work to multiuser channel (e.g., the relay–eavesdropper channel [26]) is of definite interest.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, Oct. 1949.

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.

[3] U. M. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Proc. Advances in Cryptology-EUROCRYPT*, Bruges (Brugge), Belgium, May 2000, pp. 356–373.

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

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

[6] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[7] 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, Jul. 1993.

[8] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 344–366, Mar. 2000.

[9] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3047–3061, Dec. 2004.

[10] U. M. Maurer and S. Wolf, "Secret key agreement over a nonauthenticated channel–Part I: Definitions and bounds," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 822–831, Apr. 2003.

[11] U. M. Maurer and S. Wolf, "Secret key agreement over a nonauthenticated channel–Part II: The simulatability condition," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 832–838, Apr. 2003.

[12] U. M. Maurer and S. Wolf, "Secret key agreement over a nonauthenticated channel–Part III: Privacy amplification," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 839–851, Apr. 2003.

[13] E. Tekin and A. Yener, "Achievable rates for two-way wire-tap channels," in *Proc. IEEE Intl. Symp. Information Theory*, Nice, France, Jun. 2007, pp. 941–945.

[14] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[15] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[16] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[17] Z. Li, R. Yates, and W. Trappe, "Secure communication over wireless channels," in *Proc. Information Theory and Application Workshop*, La Jolla, CA, Jan. 2007.

[18] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. IEEE Int. Symp. Information Theory*, Adelaide, Australia, Sep. 2005, pp. 2152–2155.

[19] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, to be published.

[20] E. Tekin and A. Yener, "The general Gaussian multiple access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[21] Y. Liang and H. V. Poor, "Multiple access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[22] R. Liu, I. Maric, R. D. Yates, and P. Spasojevic, "The discrete memoryless multiple access channel with confidential messages," in *Proc. IEEE Intl. Symp. Information Theory*, Seattle, WA, Jul. 2006, pp. 957–961.

[23] Y. Oohama, "Coding for relay channels with confidential messages," in *Proc. IEEE Information Theory Workshop*, Cairns, Australia, Sep. 2001, pp. 87–89.

[24] Y. Oohama, "Relay channels with confidential messages," *IEEE Trans. Inf. Theory*, submitted for publication.

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

[26] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory.*, vol. 54, no. 9, Sep. 2008.

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

[28] G. D. Forney, Jr, "On the role of MMSE estimation in approaching the information-theoretic limits of linear Gaussian channels: Shannon meets Wiener," in *Proc. Allerton Conf. Communication, Control, and Computing*, Monticello, IL, 2003.

[29] G. D. Forney, Jr, "Sphere-bound-achieving coset codes and multilevel coset codes," *IEEE Trans. Inf. Theory*, vol. 46, no. 3, pp. 820–850, May 2000.

[30] M. V. Eyuboglu and G. D. Forney, Jr, "Trellis precoding: Combined coding, precoding and shaping for intersymbol interference channels," *IEEE Trans. Inf. Theory*, vol. 38, no. 2, pp. 301–314, Mar. 1992.

[31] U. Erez and R. Zamir, "Achieving $\frac{1}{2}\log(1+\mathrm{SNR})$ on the AWGN channel with lattice encoding and decoding," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2293–2314, Oct. 2004.

[32] H. El Gamal, G. Caire, and M. O. Damen, "Lattice coding and decoding achieve the optimal diversity–multiplexing tradeoff of MIMO channels," *IEEE Trans. Inf. Theory*, vol. 50, no. 6, pp. 968–985, Jun. 2004.