New Achievable Secrecy Rate Regions for the Two Way Wiretap Channel

Aly El Gamal*, O. Ozan Koyluoglu†, Moustafa Youssef*, and Hesham El Gamal†
* Wireless Intelligent Networks Center (WINC)
Nile University, Cairo, Egypt
Email: ali.melgamal@nileu.edu.eg,mayoussef@nileuniversity.edu.eg
† Department of Electrical and Computer Engineering
The Ohio State University, Columbus, Ohio
Email: {koyluogo,helgamal}@ece.osu.edu

***Abstract*—[1] This work develops new achievable rate regions for the two way wiretap channel. In our setup, Alice and Bob wish to exchange messages securely in the presence of a passive eavesdropper Eve. In the full-duplex scenario, our achievability argument relies on allowing the two users to *jointly* optimize their channel prefixing distributions, such that the *new* channel conditions are favorable compared to that of Eve. Random binning and private key sharing over the channel are then used to exploit the secrecy advantage available in the equivalent cascade channel and to distribute the available secrecy rate among users. For the half-duplex case, we introduce the idea of *randomized scheduling* and establish the significant gain it offers in terms of the achievable secrecy sum-rate. We also quantify the gains that can be leveraged from the proposed schemes in the modulo-2 and Gaussian channels via numerical results in certain selected scenarios.**

I. Introduction

In a pioneering paper [1], Shannon established the achievability of perfectly secure communication in the presence of an eavesdropper with unbounded computational complexity. However, the necessary condition for perfect secrecy, i.e., that the entropy of the private key is larger than that of the message, appears to be prohibitive for most practical applications. In [2], Wyner revisited this problem and proved the achievability of a positive secrecy rate over a degraded discrete memoryless channel, via a *key-less* secrecy approach, by relaxing the *noiseless* assumption and the strict notion of perfect secrecy employed in [1]. Wyner's results were later extended to the Gaussian and Broadcast channels in [3] and [4]; respectively. In [5], Maurer showed how to exploit the presence of a *public discussion* channel to achieve positive secrecy over the one way wiretap channel even when the Eve's channel is less noisy than that seen by Bob. In [6], the authors considered a more practical feedback scenario where the role of the noiseless public discussion channel is played by *receiver feedback* over the same noisy channel. Under this assumption, it was shown that the perfect secrecy capacity is equal to the capacity of the main channel in the absence of the eavesdropper for full-duplex modulo-additive discrete memoryless channels. More interestingly, [6] established the achievability of positive secrecy rates, even under the half-duplex constraint where each feedback symbol introduces an erasure event in the main channel.

This work studies the two way wiretap channel, where Alice and Bob wish to exchange secure messages in the presence of a passive eavesdropper Eve. It is easy to see that the one way channel with feedback considered in [6] is a special case of this model. Using the cooperative channel prefixing and binning technique proposed in [9] together with a private key sharing over the channel, we derive an inner bound on the secrecy capacity region of the full-duplex discrete memoryless two way wiretap channel, which is strictly larger than the region reported in [7] and [8]. By specializing our results to the modulo-2 additive and Gaussian channels, we highlight the role of **cooperative** channel prefixing in creating an advantage for Alice and Bob, over Eve. In the half-duplex setting, we develop the *randomized scheduling for secrecy* concept, whereby Alice and Bob send their symbols at random time instants. This approach is shown to offer significant gains in the achievable secrecy sum-rate by introducing ambiguity at Eve regarding the source of any particular received symbol.

The rest of the paper is organized as follows. In Section II, we develop an achievable secrecy rate region for the general discrete memoryless two way wiretap channel, and specialize the result to the modulo-2 additive setting. In this section, we also derive the achievable rate region with randomized scheduling in the modulo-2 half-duplex channel. Section III extends these results to the Gaussian channel, and some concluding remarks are provided in Section IV.

II. Discrete Memoryless Channels

In the two way wiretap channel, each of the two legitimate terminals is equipped with a transmitter and a receiver. The two users intend to *exchange* messages in the presence of a passive eavesdropper. More specifically, the k^{th} user has a secret message selected from a set of *equiprobable* messages $\mathcal{W}_k = \{1, \ldots, M_k\}$, and the message $w_k \in \mathcal{W}_k$ is transmitted to the other user, in n channel uses. For message w_k, a codeword $\mathbf{X}_k(w_k) = \{X_k(1), \ldots, X_k(n)\}$ is transmitted at a rate $R_k = \frac{1}{n}\log_2 M_k$. The k^{th} decoder employs a decoding function $\phi_k(.)$ to map the received sequence $\mathbf{Y}_k$ to an estimate

[1]This work has been partially supported by a grant from the Egyptian National Telecommunications Regulatory Authority.

$\hat{w}_k$ of w_k. The two way communication is governed by *reliability* and *secrecy* constraints. The former is measured by the average probability of error,

$$P_{e,k} = \frac{1}{M_k} \sum_{w_k \in \mathcal{W}_k} P\{\hat{w}_k \neq w_k | w_k \text{ is sent}\}, \text{ for } k = 1, 2; \tag{1}$$

and the latter is given by the mutual information leakage rate to the eavesdropper, i.e.,

$$\frac{1}{n} I(W_1, W_2; \mathbf{Z}), \tag{2}$$

where $\mathbf{Z} = \{Z(1), \ldots, Z(n)\}$ is the observed sequence at the eavesdropper. Here, we focus on the *perfect secrecy* ([2]) rate region as formalized in the following definition.

Definition 1: We say that the rate tuple (R_1, R_2) is achievable for the two way wiretap channel, if for any given $\epsilon > 0$, there exists an $(n, M_1, M_2, P_{e,1}, P_{e,2})$ code such that,

$$\begin{aligned} R_1 &= \frac{1}{n} \log_2 M_1 \\ R_2 &= \frac{1}{n} \log_2 M_2 \\ \max(P_{e,1}, P_{e,2}) &\leq \epsilon \\ \frac{1}{n} I(W_1, W_2; \mathbf{Z}) &\leq \epsilon, \end{aligned}$$

for sufficiently large n.

We note that the last condition implies the following

$$\frac{1}{n} H(W_k | \mathbf{Z}) \geq R_k - \epsilon,$$

for $k = 1, 2$ (see, e.g., [9, Lemma 15]).

The secrecy capacity region is defined as the set of all achievable rates (R_1, R_2). We use the following shorthand notations for probability distributions: $p(x) \triangleq p(X = x)$, $p(x|y) \triangleq p(X = x|Y = y)$, and $p(x, y) \triangleq p(X = x, Y = y)$, where X and Y denote arbitrary random variables. We also use $\log(x)$ to denote $\log_2(x)$, and $[a]^+$ to denote $\max(a, 0)$. Finally, we use the following superscripts: 1) F: Full-duplex discrete memoryless channel, 2) FM: Full-duplex modulo-2 channel, and 3) HM: Half-duplex modulo-2 channel.

For the general *discrete memoryless two way channel with an external passive eavesdropper* (DM-TWC-E), we use the calligraphic letters $\mathcal{X}_1$ and $\mathcal{X}_2$ to denote the discrete input finite alphabets for user 1 and user 2; and $\mathcal{Y}_1$, $\mathcal{Y}_2$, and $\mathcal{Z}$, to denote the output alphabets observed at the decoders of user 1, user 2, and the eavesdropper, respectively. The channel is given by $p(y_1, y_2, z|x_1, x_2)$ and is memoryless in the following sense.

$$\begin{aligned} &p(y_1(i), y_2(i), z(i) | \mathbf{x}_1^i, \mathbf{x}_2^i, \mathbf{y}_1^{i-1}, \mathbf{y}_2^{i-1}, \mathbf{z}^{i-1}) \\ &= p(y_1(i), y_2(i), z(i) | x_1(i), x_2(i)). \end{aligned}$$

We use a coding scheme inspired by the one proposed in [9] (see also [10]): The codewords $\mathbf{C}_1$ and $\mathbf{C}_2$ for respective messages W_1 and W_2 are input to the prefix channels, where, to maximize the ambiguity at Eve, cooperation is allowed in the design of both binning codebooks and channel prefixing. The following result characterize the set of achievable rates using our coding scheme.

Theorem 1: The set of achievable rates for the full-duplex DM-TWC-E is given by,

$$\mathcal{R}^F \triangleq \text{ closure of } \left\{ \bigcup_{p \in \mathcal{P}^F} \mathcal{R}^F(p) \right\},$$

where $\mathcal{P}^F$ denotes the set of all joint distributions of the random variables Q, C_1, C_2, X_1, and X_2 satisfying

$$p(q, c_1, c_2, x_1, x_2) = p(q)p(c_1|q)p(c_2|q)p(x_1|c_1)p(x_2|c_2) \tag{3}$$

and $\mathcal{R}^F(p)$ is the closure of all non-negative rate tuples (R_1, R_2) satisfying

$$\begin{aligned} R_1 &\leq I(C_1; Y_2 | X_2, Q) && (4) \\ R_2 &\leq I(C_2; Y_1 | X_1, Q) && (5) \\ R_1 + R_2 &\leq I(C_1; Y_2 | X_2, Q) + I(C_2; Y_1 | X_1, Q) \\ &\quad - I(C_1, C_2; Z | Q) && (6) \end{aligned}$$

Proof: The achievability argument follows in the footsteps of [9, Theorem 1] with the addition of private key sharing over the channel. The detailed proof will be reported in the journal version. ■

To shed more light on the structural properties of the achievable rate region, we now focus on the full-duplex modulo-2 two way wiretap channel described by the following set of input-output relations.

$$\begin{aligned} \mathbf{Y}_1 &= \mathbf{X}_1 \oplus \mathbf{X}_2 \oplus \mathbf{N}_1 && (7) \\ \mathbf{Y}_2 &= \mathbf{X}_1 \oplus \mathbf{X}_2 \oplus \mathbf{N}_2 && (8) \\ \mathbf{Z} &= \mathbf{X}_1 \oplus \mathbf{X}_2 \oplus \mathbf{N}_e, && (9) \end{aligned}$$

where $\mathbf{N}_1 = \{N_1(1), \ldots, N_1(n)\}$, $\mathbf{N}_2 = \{N_2(1), \ldots, N_2(n)\}$, and $\mathbf{N}_e = \{N_e(1), \ldots, N_e(n)\}$ are the additive binary noise vectors impairing Alice, Bob, and Eve; respectively. The corresponding transition probabilities are given by: $p(N_1(i) = 1) = \epsilon_1$, $p(N_2(i) = 1) = \epsilon_2$, and $p(N_e(i) = 1) = \epsilon_e$ for $i = 1, \ldots, n$.

In this special case, the transmitted codeword reduces to the modulo-2 sum of a binning codeword and an independent *prefix* noise component, i.e.,

$$\begin{aligned} \mathbf{X}_1 &= \mathbf{C}_1 \oplus \bar{\mathbf{N}}_1 && (10) \\ \mathbf{X}_2 &= \mathbf{C}_2 \oplus \bar{\mathbf{N}}_2, && (11) \end{aligned}$$

where $\bar{\mathbf{N}}_1 = \{\bar{N}_1(1), \ldots, \bar{N}_1(n)\}$, $\bar{\mathbf{N}}_2 = \{\bar{N}_2(1), \ldots, \bar{N}_2(n)\}$ are the *prefix* noise vectors transmitted by Alice and Bob. The components of these vectors are generated according to i.i.d. distributions with the following marginals: $p(\bar{N}_1(i) = 1) = \bar{\epsilon}_1$, $p(\bar{N}_2(i) = 1) = \bar{\epsilon}_2$ for $i = 1, \ldots, n$. The binning codebooks, on the other hand, are generated according to i.i.d. distributions with the following marginals: $p(C_1(i) = 1) = \mu_1$ and $p(C_2(i) = 1) = \mu_2$. We further define the following crossover

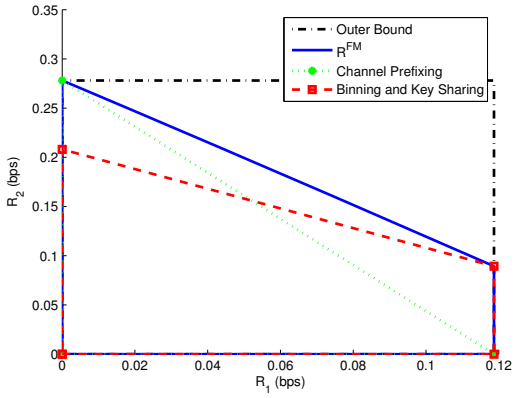

Fig. 1. Boundaries of achievable rate regions for the modulo-2 channel, when $\epsilon_1 = 0.2$, $\epsilon_2 = 0.3$, $\epsilon_e = 0.25$, and $\mu_1 = \mu_2 = 0.5$. The outer bound is the capacity of the two way channel without the secrecy constraints.

probabilities to describe the cascade of the prefix and original channels.

$$\hat{\epsilon}_1 = \epsilon_1(1-\bar{\epsilon}_2) + \bar{\epsilon}_2(1-\epsilon_1) \quad (12)$$
$$\hat{\epsilon}_2 = \epsilon_2(1-\bar{\epsilon}_1) + \bar{\epsilon}_1(1-\epsilon_2) \quad (13)$$
$$\bar{\epsilon}_{12} = \bar{\epsilon}_2(1-\bar{\epsilon}_1) + \bar{\epsilon}_1(1-\bar{\epsilon}_2) \quad (14)$$
$$\hat{\epsilon}_e = \epsilon_e(1-\bar{\epsilon}_{12}) + \bar{\epsilon}_{12}(1-\epsilon_e) \quad (15)$$

Using this notation, the achievable region in Theorem 1 reduces to the following.

Corollary 1: The set of achievable rates for the full-duplex modulo-2 two way wiretap channel is given by,

$$\mathcal{R}^{FM} \triangleq \text{closure of convex hull of} \left\{ \bigcup_{0\le\bar{\epsilon}_1,\bar{\epsilon}_2\le 1} \mathcal{R}^{FM}(\bar{\epsilon}_1,\bar{\epsilon}_2) \right\}$$

where $\mathcal{R}^{FM}(\bar{\epsilon}_1,\bar{\epsilon}_2)$ is the closure of all non-negative rate tuples (R_1, R_2) satisfying

$$R_1 \le 1 - H(\hat{\epsilon}_2) \quad (16)$$
$$R_2 \le 1 - H(\hat{\epsilon}_1) \quad (17)$$
$$R_1 + R_2 \le 1 + H(\hat{\epsilon}_e) - H(\hat{\epsilon}_1) - H(\hat{\epsilon}_2) \quad (18)$$

The region in Corollary 1 is strictly larger than the ones reported in [7], [8]; as demonstrated by the numerical results of Fig. 1. Here we compare our region with the one achieved by random binning and key sharing only; and channel prefixing only ([7, Section 5]). On the other hand, we remark that the corner points of the region in Corollary 1 is achieved by random binning and key sharing only if $\epsilon_e > \max(\epsilon_1, \epsilon_2)$; and achieved by only channel prefixing if $\epsilon_e < \min(\epsilon_1, \epsilon_2)$. Moreover, the previous result identifies the separate role of channel prefixing and binning. First, channel prefixing is used to create an advantage of Alice and Bob over Eve; via the **joint** optimization of $\bar{\epsilon}_1$ and $\bar{\epsilon}_2$. Then, the binning codebooks are used to transform this advantage into a secrecy gain for the two terminals.

Next, we turn our attention to the *half-duplex* modulo-2 channel in which each terminal can only transmit or receive at any point in time. We model this scenario as a *ternary input* channel where the third input corresponds to the no-transmission event. This way, the three nodes can identify the symbol intervals when no one is transmitting. Moreover, we give the eavesdropper the advantage of identifying the symbol intervals at which both users are transmitting. These assumptions are intended to model a worst case scenario where Eve can identify the three different states; via the different received power levels for example.

Let P_1 and P_2 be the probability of transmission for user 1 and user 2, respectively (known *a-priori* by the three nodes). It is easy to see that the eavesdropper channel will have four possible states. The silence symbols will be identified and erased, and the crossover probabilities corresponding to the other three states are given by,

$$p(z \neq c_1 | \text{only user 1 is transmitting}) = \epsilon_{e1}$$
$$p(z \neq c_2 | \text{only user 2 is transmitting}) = \epsilon_{e2}$$
$$p(z \neq (c_1 \oplus c_2) | \text{both users are transmitting}) = \hat{\epsilon}_e$$

where $\hat{\epsilon}_e$ is given as above, and,

$$\epsilon_{e1} = \epsilon_e(1-\bar{\epsilon}_1) + \bar{\epsilon}_1(1-\epsilon_e) \quad (19)$$
$$\epsilon_{e2} = \epsilon_e(1-\bar{\epsilon}_2) + \bar{\epsilon}_2(1-\epsilon_e) \quad (20)$$

For simplicity of presentation, we obtain the following results assuming that the binary binning codebooks used by Alice and Bob are generated according to an i.i.d uniform distribution (one can potentially obtain a larger rate by optimizing the binning codebook distribution).

Proposition 1: The set of achievable rates for the half-duplex modulo-2 two way wiretap channel is given by

$$\mathcal{R}^{HM} \triangleq \text{closure of the convex hull of} \left\{ \bigcup_{p\in\mathcal{P}^{HM}} \mathcal{R}^{HM}(p) \right\}$$

where $\mathcal{P}^{HM}$ is defined as,

$$\mathcal{P}^{HM} \triangleq \{(\bar{\epsilon}_1, \bar{\epsilon}_2, P_1, P_2) : 0 \le \bar{\epsilon}_1, \bar{\epsilon}_2, P_1, P_2 \le 1\},$$

and $\mathcal{R}^{HM}(p)$ is the closure of all non-negative rate tuples (R_1, R_2) satisfying

$$R_1 \le P_1(1-P_2)(1-H(\hat{\epsilon}_2)) \quad (21)$$
$$R_2 \le P_2(1-P_1)(1-H(\hat{\epsilon}_1)) \quad (22)$$
$$\begin{aligned} R_1 + R_2 \le\ & P_1(1-P_2)(1-H(\hat{\epsilon}_2)) \\ & + P_2(1-P_1)(1-H(\hat{\epsilon}_1)) \\ & - P_1P_2(1-H(\hat{\epsilon}_e)) \\ & - (P_1(1-P_2) + P_2(1-P_1)) \\ & \Big(1 - 0.5H(d_1\epsilon_{e1} + d_2\epsilon_{e2}) \\ & - 0.5H(d_1(1-\epsilon_{e1}) + d_2\epsilon_{e2})\Big), \end{aligned}$$

where

$$d_1 = \frac{P_1(1-P_2)}{P_1(1-P_2) + P_2(1-P_1)} \quad (23)$$
$$d_2 = 1 - d_1 \quad (24)$$

Proof: Here, we provide the computation of $I(C_1, C_2; Z)$. The complete proof will be provided in the journal version.

$$
\begin{aligned}
& I(C_1, C_2; Z) \\
\stackrel{(a)}{=} \; & (1-P_1)(1-P_2) I(C_1, C_2; Z | \text{no transmission}) \\
& + P_1 P_2 I(C_1, C_2; Z | \text{both users are transmitting}) \\
& + (P_1(1-P_2) + P_2(1-P_1)) \\
& \quad I(C_1, C_2; Z | \text{only one user is transmitting}) \\
= \; & P_1 P_2 (1 - H(\hat{\epsilon}_e)) \\
& + (P_1(1-P_2) + P_2(1-P_1))[1 - \\
& \sum_{i,j} p(C_1 = i, C_2 = j) H(Z | C_1 = i, C_2 = j)] \\
\stackrel{(b)}{=} \; & P_1 P_2 (1 - H(\hat{\epsilon}_e)) \\
& + (P_1(1-P_2) + P_2(1-P_1)) \\
& \big(1 - 0.5 H(d_1 \epsilon_{e1} + d_2 \epsilon_{e2}) \\
& - 0.5 H(d_1(1-\epsilon_{e1}) + d_2 \epsilon_{e2})\big) \qquad (25)
\end{aligned}
$$

where (a) follows from the assumption that Eve can identify both silence and concurrent transmission symbol intervals, (b) is a direct results of the following computation.

$$
\begin{aligned}
& H(Z | C_1 = 0, C_2 = 0) = H(d_1 \epsilon_{e1} + d_2 \epsilon_{e2}) \\
& H(Z | C_1 = 1, C_2 = 1) = H(Z | C_1 = 0, C_2 = 0) \\
& H(Z | C_1 = 1, C_2 = 0) = H(d_1(1-\epsilon_{e1}) + d_2 \epsilon_{e2}) \\
& H(Z | C_1 = 0, C_2 = 1) = H(Z | C_1 = 1, C_2 = 0)
\end{aligned}
$$

■

To illustrate the advantage offered by *randomized scheduling*, we first observe that cooperative binning and channel prefixing scheme with *deterministic* scheduling fails to achieve a non-zero secrecy rate under our *restrictive half-duplex scenario* if Eve's channel is **not** more noisy than the legitimate channels (this includes, as a special case, the randomized feedback approach for one-way channel proposed in [6]). Now, consider the noiseless case, i.e., $\epsilon_1 = \epsilon_2 = \epsilon_e = 0$. By setting $P_1 = P_2 = 0.5$ and $\bar{\epsilon}_2 = 0.5$, Proposition 1 shows that the randomized scheduling approach allows user 1 to achieve the following secure rate $R_1 = 0.25 - 0.5(1 - H(0.25))$.

III. The Gaussian Channel

In a full-duplex Gaussian setting, the channel is given by,

$$\mathbf{Y}_1 = \mathbf{X}_1 + \sqrt{g_{12}}\mathbf{X}_2 + \mathbf{N}_1 \qquad (26)$$

$$\mathbf{Y}_2 = \sqrt{g_{21}}\mathbf{X}_1 + \mathbf{X}_2 + \mathbf{N}_2 \qquad (27)$$

$$\mathbf{Z} = \sqrt{g_{e1}}\mathbf{X}_1 + \sqrt{g_{e2}}\mathbf{X}_2 + \mathbf{N}_e \qquad (28)$$

where g_{12}, g_{21}, g_{e1}, and g_{e2} are channel coefficients, $\mathbf{N}_1$, $\mathbf{N}_2$, and $\mathbf{N}_e$ are noise vectors with i.i.d. zero-mean unit-variance white Gaussian entries at user 1, user 2, and Eve, respectively. We assume the following average power constraints.

$$\frac{1}{n}\sum_{i=1}^{n}(X_1(i))^2 \le \rho_1 \qquad (29)$$

$$\frac{1}{n}\sum_{i=1}^{n}(X_2(i))^2 \le \rho_2 \qquad (30)$$

We define $\gamma(x) \triangleq \frac{1}{2}\log(1+x)$, $h(X)$ is given by $h(X) = -\int f_X(x)\log f_X(x)$, and use the following superscripts: 1) FG: Full-duplex Gaussian channel and 2) HG: Half-duplex Gaussian channel.

Let $C_1(i)$ and $\bar{N}_1(i)$ be $i.i.d.$ with respect to the time index, and each element is generated according to $C_1 \sim \mathcal{N}(0, \rho_1^c)$ and $\bar{N}_1 \sim \mathcal{N}(0, \rho_1^n)$, where $\rho_1^c + \rho_1^n = \rho_1 - \epsilon$. The prefix channel is chosen as $\mathbf{X}_1 = \mathbf{C}_1 + \bar{\mathbf{N}}_1$. By the weak law of large numbers, $\frac{1}{n}\sum_{i=1}^{n}(X_1(i))^2 \to \rho_1 - \epsilon$ as $n \to \infty$. By similarly constructing $\mathbf{X}_2$, we obtain

Corollary 2: The set of achievable rates for the full-duplex Gaussian two way wiretap channel is given by

$$\mathcal{R}^{FG} \triangleq \text{closure of the convex hull of } \left\{ \bigcup_{p \in \mathcal{P}^{FG}} \mathcal{R}^{FG}(p) \right\}$$

where $\mathcal{P}^{FG}$ is defined as,

$$\mathcal{P}^{FG} \triangleq \quad \{(\rho_1^c, \rho_1^n, \rho_2^c, \rho_2^n) : \rho_1^c + \rho_1^n \le \rho_1, \rho_2^c + \rho_2^n \le \rho_2\},$$

and $\mathcal{R}^{FG}(p)$ is the closure of all non-negative rate tuples (R_1, R_2) satisfying

$$R_1 \le \gamma\left(\frac{\rho_1^c g_{21}}{1 + \rho_1^n g_{21}}\right) \qquad (31)$$

$$R_2 \le \gamma\left(\frac{\rho_2^c g_{12}}{1 + \rho_2^n g_{12}}\right) \qquad (32)$$

$$
\begin{aligned}
R_1 + R_2 \; \le \; & \gamma\left(\frac{\rho_1^c g_{21}}{1 + \rho_1^n g_{21}}\right) \\
& + \gamma\left(\frac{\rho_2^c g_{12}}{1 + \rho_2^n g_{12}}\right) \\
& - \gamma\left(\frac{\rho_1^c g_{e1} + \rho_2^c g_{e2}}{1 + \rho_1^n g_{e1} + \rho_2^n g_{e2}}\right) \qquad (33)
\end{aligned}
$$

In Fig. 2, we compare the region of Corollary 2 with the regions of the following special cases: 1) Both users implement cooperative binning and key sharing without channel prefixing and 2) While one of the users implement individual secrecy encoding ([2]), the other one helps only with channel prefixing. The same trends of the modulo-2 case are observed here except for the fact that channel prefixing does not achieve the two extreme points of $\mathcal{R}^{FG}$. We note that the region reported in [8, Theorem 2] can be achieved by implementing binning without key sharing, and it is a sub-region of Corollary 2. The scheme in [8, Section V] is either binning only at both users, or binning at one user and channel prefixing (jamming) at the other user. Resulting regions of both schemes are subregions of Corollary 2. (The first one is a subregion of the red-dashed region and the second one is the green-dotted region in Fig. 2.)

Assuming half-duplex nodes, with P_1 and P_2 being the probability of transmission for the two users, and that Eve can *perfectly* identify the no transmission and simultaneous transmission states. To further increase its ambiguity, we assume both users know the channel coefficients, hence they

jointly set $\frac{\rho_1}{P_1}g_{e1}$ and $\frac{\rho_2}{P_2}g_{e2}$, to the same value ρ_r. We obtain the following result.

Proposition 2: The set of achievable rates for the half-duplex Gaussian two way wiretap channel is given by,

$$\mathcal{R}^{HG} \triangleq \text{closure of the convex hull of } \left\{ \bigcup_{p\in\mathcal{P}^{HG}} \mathcal{R}^{HG}(p) \right\}$$

where $\mathcal{P}^{HG}$ is defined as,

$$\begin{aligned}\mathcal{P}^{HG} \triangleq \quad & \{(\rho_1^c, \rho_1^n, \rho_2^c, \rho_2^n, P_1, P_2) : \\ & 0 \le P_1, P_2 \le 1, \frac{\rho_1}{P_1}g_{e1} = \frac{\rho_2}{P_2}g_{e2} = \rho_r \\ & P_1(\rho_1^c + \rho_1^n) \le \rho_1, P_2(\rho_2^c + \rho_2^n) \le \rho_2\},\end{aligned}$$

and $\mathcal{R}^{HG}(p)$ is the closure of all non-negative rate tuples (R_1, R_2) satisfying

$$R_1 \le P_1(1-P_2)\gamma\left(\frac{\rho_1^c g_{21}}{1+\rho_1^n g_{21}}\right) \tag{34}$$

$$R_2 \le P_2(1-P_1)\gamma\left(\frac{\rho_2^c g_{12}}{1+\rho_2^n g_{12}}\right) \tag{35}$$

$$\begin{aligned}R_1 + R_2 \quad \le \quad & \Bigg[P_1(1-P_2)\gamma\left(\frac{\rho_1^c g_{21}}{1+\rho_1^n g_{21}}\right) \\ & + P_2(1-P_1)\gamma\left(\frac{\rho_2^c g_{12}}{1+\rho_2^n g_{12}}\right) \\ & + h(Z|C_1,C_2) - h(Z)\Bigg]^+\end{aligned} \tag{36}$$

$$\begin{aligned}h(Z) - h(Z|C_1,C_2) = {} & P_1P_2\gamma\left(\frac{\rho_1^c g_{e1} + \rho_2^c g_{e2}}{1+\rho_1^n g_{e1} + \rho_2^n g_{e2}}\right) \\ & +(P_1(1-P_2) + P_2(1-P_1)) \\ & \Bigg[\frac{1}{2}\log(2\pi e(1+\rho_r)) \\ & - \int f_{C_1}(i) f_{C_2}(j) h(Z|i,j) df_{C_1} df_{C_2}\Bigg]\end{aligned} \tag{37}$$

and

$$\begin{aligned}f_{Z|C_1,C_2}(z|i,j) \quad = \quad & d_1\mathcal{N}(i, 1+\rho_1^n g_{e1}) \\ & +d_2\mathcal{N}(j, 1+\rho_2^n g_{e2})\end{aligned} \tag{38}$$

$$d_1 = \frac{P_1(1-P_2)}{P_1(1-P_2) + P_2(1-P_1)} \tag{39}$$

$$d_2 = 1 - d_1 \tag{40}$$

IV. Conclusions

In this paper, we used the cooperative binning and channel prefixing approach to obtain achievable secrecy rates for both the discrete memoryless and Gaussian full-duplex two way wiretap channels. In the proposed scheme, channel prefixing is used to create *an advantage* for the legitimate terminals over the eavesdropper which is transformed by the binning codebooks into a non-trivial secrecy rate region. Moreover, private key sharing is used to distribute the secrecy sum-rate between two users. We then introduced the idea of randomized scheduling and established its fundamental role in the half-duplex two way wiretap channel. Numerical results that illustrate the performance gains offered by joint binning, channel prefixing, key sharing, and randomized scheduling were reported. Our current investigations focus on deriving outer bounds to the secrecy capacity region aiming at obtaining sharp results; whenever possible.

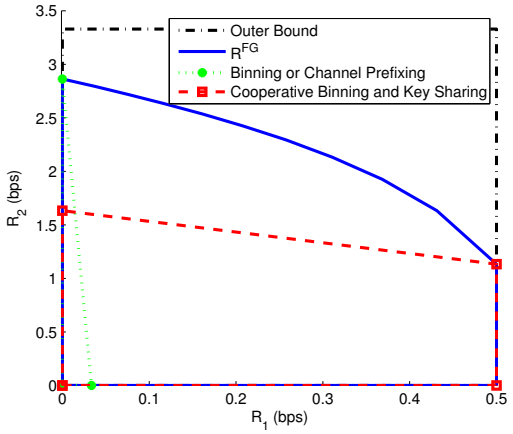

Fig. 2. Boundaries of achievable rate regions for the Gaussian channel, when $g_{21} = 0.1$, $g_{12} = 10$, $g_{e1} = g_{e2} = 1$, and $\rho_1 = \rho_2 = 10$. The outer bound is the capacity of the two way channel without the secrecy constraints.

References

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

[2] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, 1974.

[3] S. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, pp. 451–456, July 1978.

[4] I. Csiszár and J.Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, pp. 339–348, May 1978.

[5] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, pp. 733–742, 1993.

[6] 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.

[7] E. Tekin and A. Yener, "Achievable rates for two-way wire-tap channels," in *Proc. IEEE Int. Symp. on Information Theory (ISIT)*, pp. 941–945, 2007.

[8] ——, "The general Gaussian multiple-access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, pp. 2735–2751, 2008.

[9] O. O. Koyluoglu and H. El Gamal, "Cooperative binning and channel prefixing for secrecy in interference channels," *IEEE Trans. Inf. Theory*, submitted for publication.

[10] ——, "On the secrecy rate region for the interference channel," in *Proc. 2008 IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'08)*, Cannes, France, Sep. 2008.

[11] T. Cover and J. Thomas, "Elements of information theory." John Wiley Sons, Inc., 1991.

[12] A. El Gamal, M. Youssef, and H. El Gamal "Randomization for security in half-duplex two-way Gaussian channels," in *Proc. 2009 IEEE Globecom*.