

Motivation

Increasing demand in securing (wireless) networks has recently resulted in tremendous amount of research efforts in physical layer security. Among many other open problems, we concentrated the following ones.

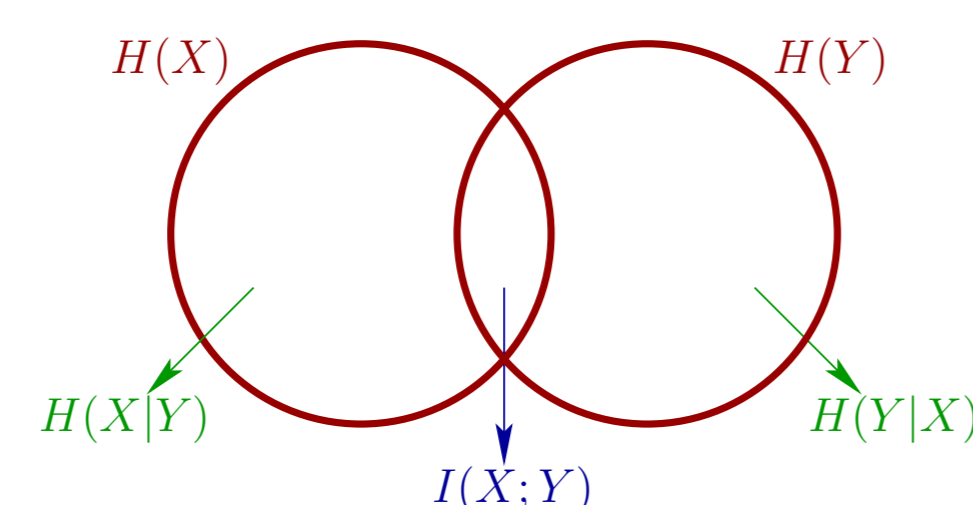
- Fundamental limits of secure transmission rates in multi-user networks
- The role of cooperation in multi-user networks to facilitate secret transmissions

In this manner, we studied one of the fundamental building blocks of multi-user networks, i.e., interference channels, with security constraints. The existence of an external eavesdropper in a two-user interference channel is assumed, where the network users would like to secure their messages from the external eavesdropper.

Preliminaries

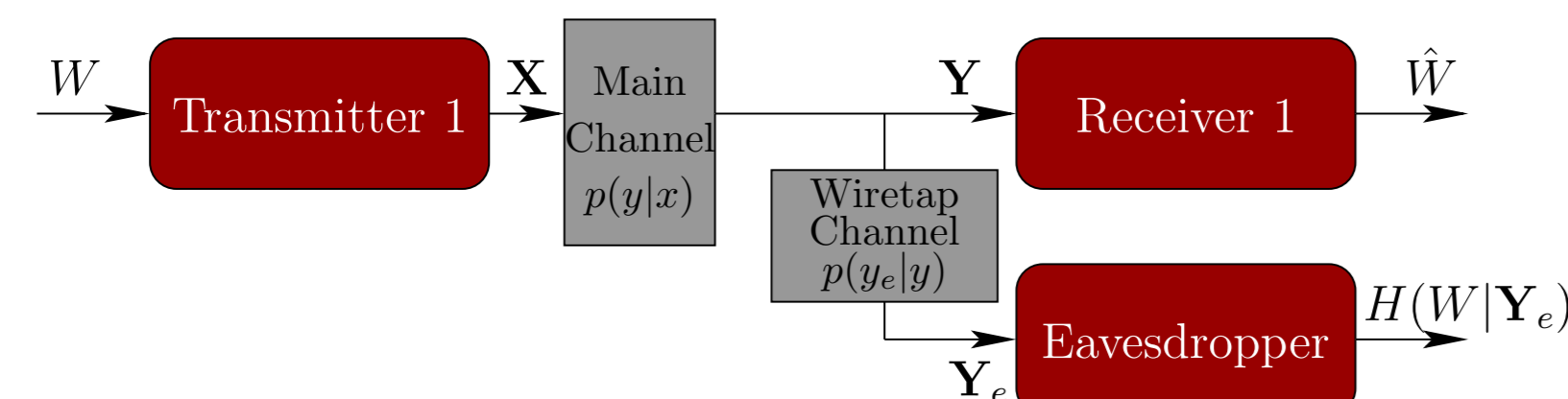
Consider random variables X and Y .

- $H(X)$ = The amount of randomness in X .
- $H(X|Y)$ = The amount of randomness that remains in X after observing Y .
- $I(X;Y)$ = The amount of randomness that is resolved from X by observing Y .



Note that $I(X;Y) = H(X) - H(X|Y)$. $H(X) = -\sum_{x \in \mathcal{X}} p(x) \log(p(x))$ for a discrete r.v. X and $H(X) = -\int f(x) \log(f(x)) dx$ for a continuous r.v. X . Please refer to [4] for further information.

Information Theoretic Secrecy - The Wiretap Channel



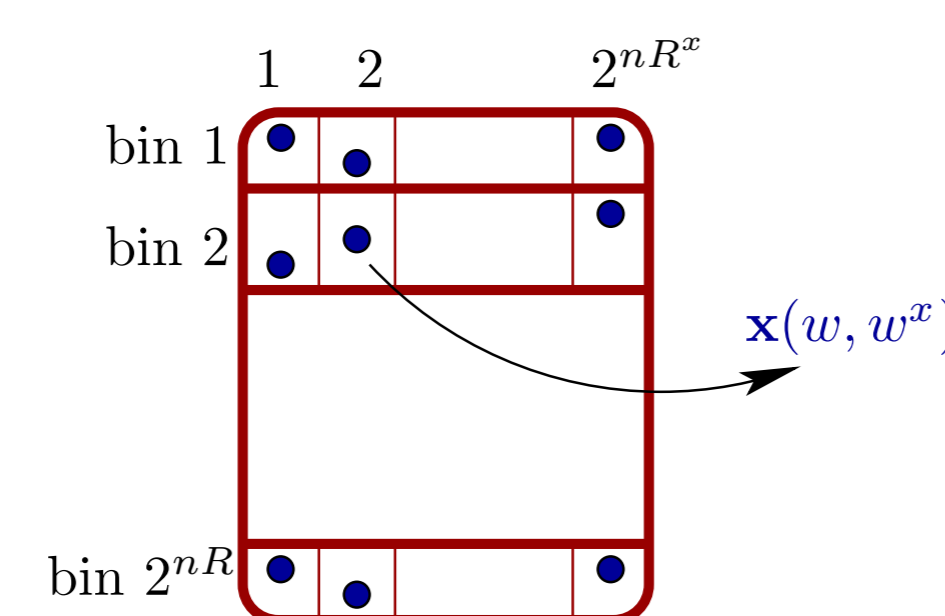
- Eavesdropper observes a degraded version of the output seen by the intended receiver.
- Binning technique [1] :

Idea: Add extra randomness to the channel that can not be resolved by the eavesdropper.

- Generate $2^{n(R+R^*)}$ codewords, distribute them into 2^{nR} bins, where each bin contains 2^{nR^*} codewords.

- To send message w , choose a codeword in the bin w randomly and transmit the corresponding codeword denoted by $\mathbf{x}(w, w^*)$.

- Set the rates such that $R + R^* \leq I(X;Y)$ and $R^* = I(X;Y_e)$. This way, receiver recovers both the bin index (w) and the codeword index (w^*). Furthermore, the eavesdropper can be confused by this choice and the secrecy requirement can be satisfied, i.e., $\frac{1}{n}I(W;Y_e)$ can be arbitrarily made small as n increases.

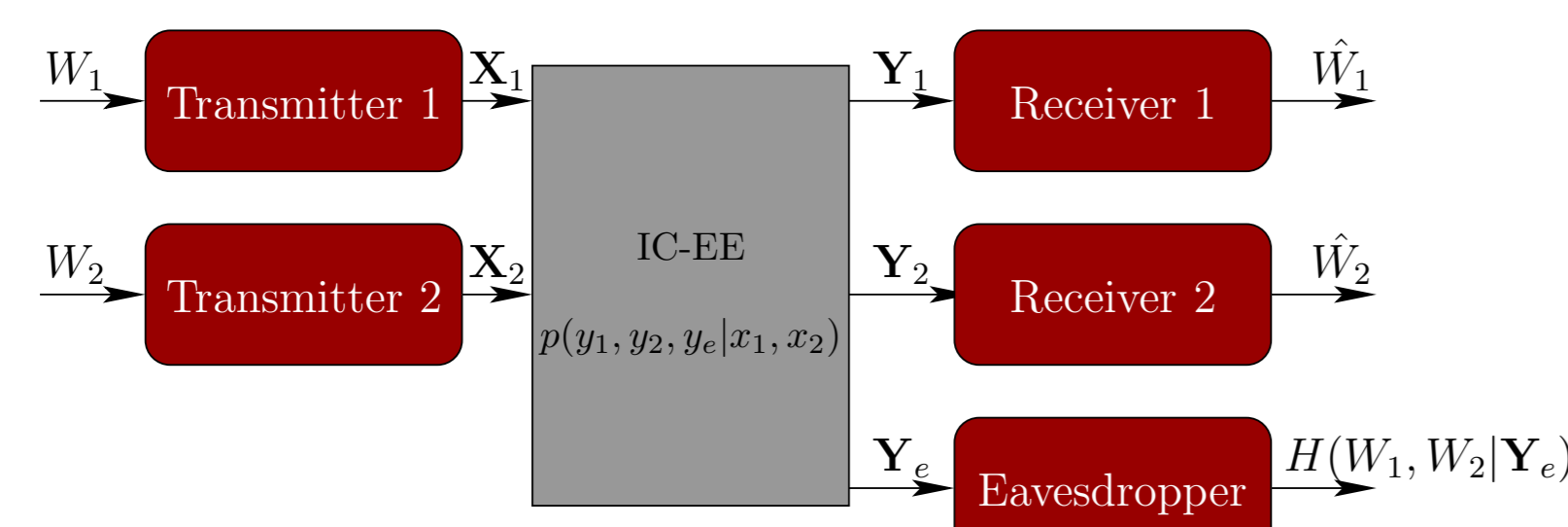


- The secrecy capacity is

$$C_s = \max_{p(X)} I(X;Y) - I(X;Y_e).$$

System Model - Interference Channel with an External Eavesdropper (IC-EE)

We assume that each transmitter $k \in \{1,2\}$ has a secret message $w_k \in \mathcal{W}_k \triangleq \{1,2,\dots,2^{nR_k}\}$ which is to be transmitted to the respective receiver in n channel uses and to be secured from the external eavesdropper.



The error probability at the receivers are defined as follows.

$$P_{e,k} \triangleq \frac{1}{|\mathcal{W}_1||\mathcal{W}_2|} \sum_{(w_1, w_2) \in \mathcal{W}_1 \times \mathcal{W}_2} \Pr\{\hat{w}_k \neq w_k | (w_1, w_2) \text{ is transmitted.}\}$$

We say that the rate tuple (R_1, R_2) is achievable for the IC-EE if, for any given $\epsilon > 0$, there exists a secret codebook such that,

$$\max\{P_{e,1}, P_{e,2}\} \leq \epsilon \quad \rightarrow \text{reliability of the transmission}$$

$$R_1 + R_2 - \frac{1}{n}H(W_1, W_2|Y_e) = \frac{1}{n}I(W_1, W_2; Y_e) \leq \epsilon \quad \rightarrow \text{secrecy of the transmission}$$

for sufficiently large n . The secrecy capacity region is the closure of the set of all achievable rate pairs (R_1, R_2) and is denoted as $\mathcal{C}^{\text{IC-EE}}$.

Proposed Scheme to Secure IC-EE

The proposed scheme allows for cooperation in adding randomness to the channel in two ways:

- **Cooperative binning** \rightarrow To add structured and decodable randomness
- **Cooperative channel prefixing** \rightarrow To add unstructured and undecodable randomness

Here, the binning technique of [1] and the channel prefixing technique of [5] are cooperatively exploited. The proposed scheme also utilizes the message-splitting technique of [3] to allow partial decoding of the interfering signals.

Consider auxiliary random variables $Q, C_1, S_1, O_1, C_2, S_2$, and O_2 . Let \mathcal{P} be the set of all joint distributions of the random variables $Q, C_1, S_1, O_1, C_2, S_2, O_2, X_1, X_2, Y_1, Y_2$, and Y_e that factors as

$$p(q, c_1, s_1, o_1, c_2, s_2, o_2, x_1, x_2, y_1, y_2, y_e) = p(q)p(c_1|q)p(s_1|q)p(o_1|q)p(c_2|q)p(s_2|q)p(o_2|q)p(x_1|c_1, s_1, o_1, q)p(x_2|c_2, s_2, o_2, q)p(y_1, y_2, y_e|x_1, x_2).$$

Here, the variable Q serves as a time-sharing parameter (See, for example, [3, 4]). The roles of the other auxiliary random variables and the proposed encoder architecture are given below. To ease the presentation, we define

$$T_1 \triangleq C_1, T_2 \triangleq S_1, T_3 \triangleq O_1, T_4 \triangleq C_2, T_5 \triangleq S_2, T_6 \triangleq O_2,$$

and corresponding rates R_{T_i} and $R_{T_i}^*$. We also define $T_S \triangleq \{T_i | i \in \mathcal{S}\}$.

Random Variable	Codebook Type	Function
C_k	Binning codebook with rates R_{C_k} and $R_{C_k}^*$	Common information of transmitter k , will be decoded at both receivers
S_k	Binning codebook with rates R_{S_k} and $R_{S_k}^*$	Self information of transmitter k , will be decoded at receiver $\{1, 2\} - k$ and considered as noise at receiver $\{1, 2\} - k$
O_k	Random codebook with rate $R_{O_k}^*$	Other information of transmitter k , will be decoded at receiver $\{1, 2\} - k$ and considered as noise at receiver k

Receiver 1 can decode the tuple $(w_{C_1}, w_{C_1}^*, w_{S_1}, w_{S_1}^*, w_{C_2}, w_{C_2}^*, w_{O_2}^*)$, if the corresponding rates are inside the region $\mathcal{R}_1(p)$.

Receiver 2 can decode the tuple $(w_{C_2}, w_{C_2}^*, w_{S_2}, w_{S_2}^*, w_{C_1}, w_{C_1}^*, w_{O_1}^*)$, if the corresponding rates are inside the region $\mathcal{R}_2(p)$.

For the eavesdropper, we would like to set the rates such that the eavesdropper can decode the codeword indices $(w_{C_1}^*, w_{S_1}^*, w_{O_1}^*, w_{C_2}^*, w_{S_2}^*, w_{O_2}^*)$ given the bin indices $(w_{C_1}, w_{S_1}, w_{C_2}, w_{S_2})$. With this construction, similar to [1], the secrecy constraint can be satisfied if the corresponding rates are chosen inside the region $\mathcal{R}_e(p)$.

To sum up, we would like to set the rates to satisfy above three rate regions.

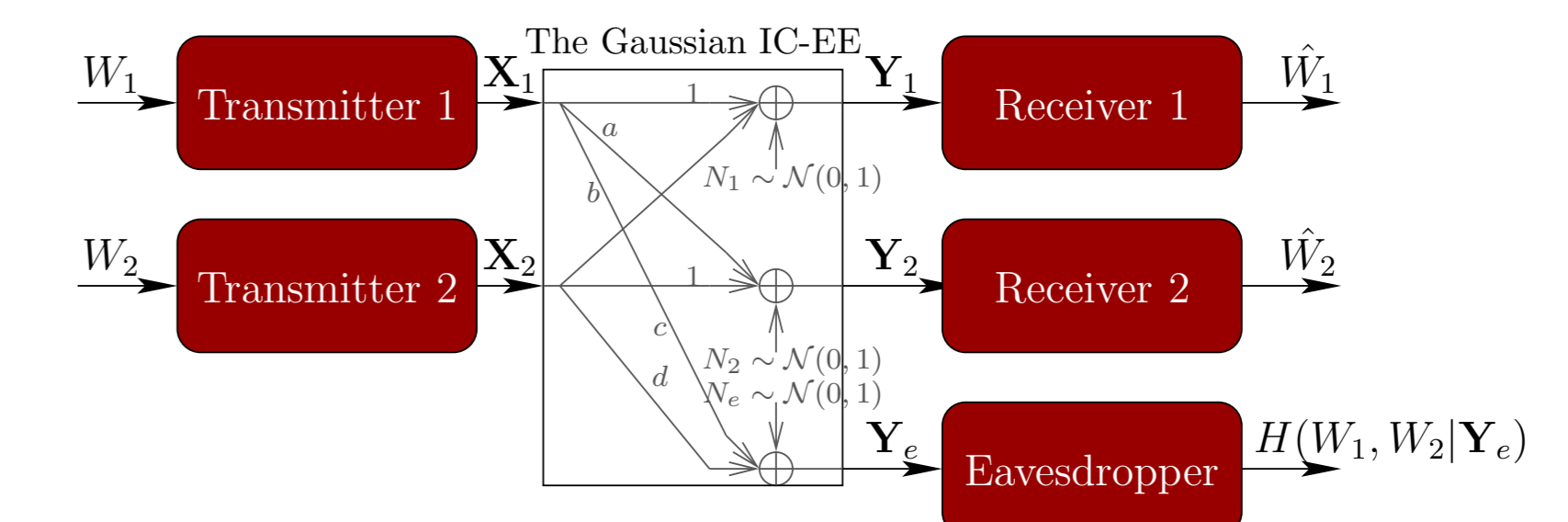
Definition: For a given joint distribution p , $\mathcal{R}(p)$ is the closure of all (R_1, R_2) satisfying

$$\begin{aligned} R_1 &= R_{C_1} + R_{S_1}, \\ R_2 &= R_{C_2} + R_{S_2}, \\ (R_{C_1}, R_{C_1}^*, R_{S_1}, R_{S_1}^*, R_{C_2}, R_{C_2}^*, R_{O_2}^*) &\in \mathcal{R}_1(p), \\ (R_{C_2}, R_{C_2}^*, R_{S_2}, R_{S_2}^*, R_{C_1}, R_{C_1}^*, R_{O_1}^*) &\in \mathcal{R}_2(p), \\ (R_{C_1}^*, R_{S_1}^*, R_{O_1}^*, R_{C_2}^*, R_{S_2}^*, R_{O_2}^*) &\in \mathcal{R}_e(p). \end{aligned}$$

We now state the main result. The achievable secrecy rate region using the cooperative binning and channel prefixing scheme is as follows.

Theorem: $\mathcal{R}^{\text{IC-EE}} \triangleq$ the closure of $\left\{ \bigcup_{p \in \mathcal{P}} \mathcal{R}(p) \right\} \subset \mathcal{C}^{\text{IC-EE}}$.

The Gaussian IC-EE and Simulation Results



- Power constrained inputs: $\frac{1}{n}\mathbf{X}_k\mathbf{X}_k^T \leq P_k$, for $k = 1, 2$.
- The auxiliary random variables are chosen according to Gaussian distribution: $p(c_k|q) \sim \mathcal{N}(0, P_{C_k}(q))$, $p(s_k|q) \sim \mathcal{N}(0, P_{S_k}(q))$, and $p(o_k|q) \sim \mathcal{N}(0, P_{O_k}(q))$.
- Channel prefixing is utilized by adding i.i.d. noise samples to the channel: **Jamming**.

- Generate n -tuple \mathbf{j}_k , where each entry is chosen i.i.d. $p(j_k|q) \sim \mathcal{N}(0, P_{j_k}(q))$.

- Add \mathbf{j}_k to the sum of the codewords (superposition).

- Powers are chosen to satisfy the power constraints:

$$\sum_{q \in \mathcal{Q}} (P_{C_k}(q) + P_{S_k}(q) + P_{O_k}(q) + P_{j_k}(q)) p(Q = q) \leq P_k$$

- The sequence \mathbf{j}_k can only be considered as noise for the receivers and the eavesdropper.

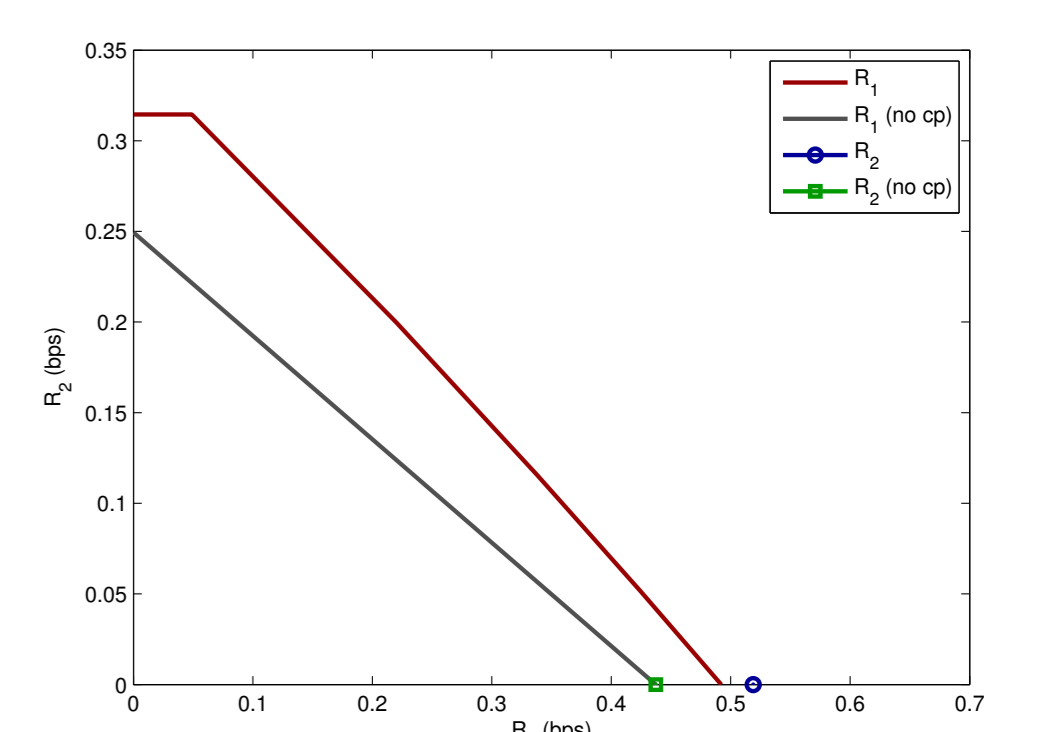
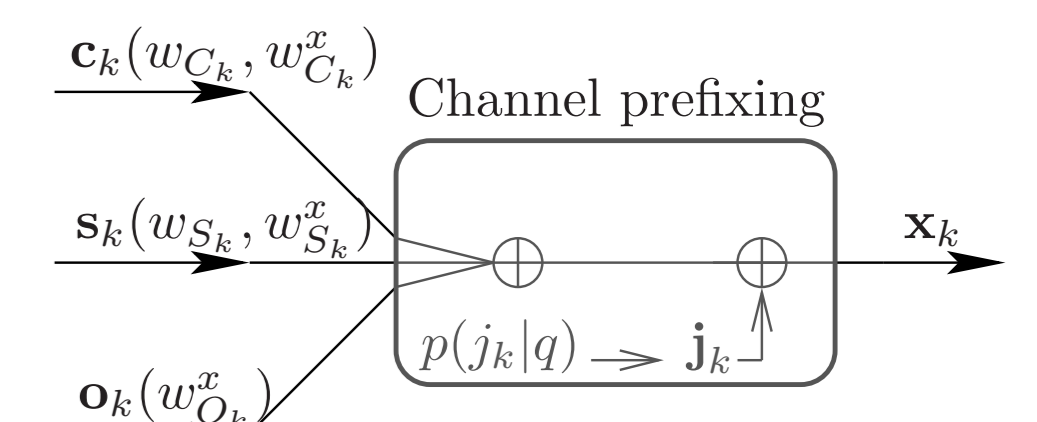
- Simulation results (4 subregions of the achievable rate region) for the Gaussian IC-EE:

- \mathcal{R}_1 : Utilizes C_1, C_2, J_1, J_2 . This is an example of **Cooperative binning and channel prefixing** scheme.

- $\mathcal{R}_1(\text{no cp})$: Utilizes C_1, C_2 . No channel prefixing (no cp). This is an example of **Cooperative binning** scheme.

- \mathcal{R}_2 : Utilizes Q, S_1, S_2, J_1, J_2 . Q is chosen as a Bernoulli random variable $p(q=0) = p(q=1) = 0.5$ to implement time-division with two slots. For $q=1$, S_1, J_1, J_2 are used; and for $q=2$, S_2, J_1, J_2 are used. This is called as **Cooperative TDMA scheme**, where a user helps to the other one by jamming the channel.

- $\mathcal{R}_2(\text{no cp})$: Utilizes Q, S_1, S_2 . Q is chosen as above. For $q=1$, S_1 is used; and for $q=2$, S_2 is used. This is conventional **TDMA scheme**, where a user is silent during the dedicated slot of the other user.



Simulation Results for the Gaussian IC-EE with $a = 1.9, b = 1, c = 0.9, d = 1.6, P_1 = P_2 = 10$.

Conclusions

- Cooperative binning and channel prefixing is proposed to cooperatively add randomness to the channel.
- Jamming the channel by exploiting the channel prefixing technique.
- Users add *sufficient* amount of randomness.

References

- [1] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.
- [2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339-348, May 1978.
- [3] T. S. Han and K. Kobayashi, "A new achievable rate region for the interference channel," *IEEE Trans. Inform. Theory*, vol. 27, no. 1, pp. 49-60, Jan. 1981.
- [4] T. Cover and J. Thomas, *Elements of Information Theory*, John Wiley and Sons, Inc., 1991.
- [5] O. O. Koyluoglu and H. El Gamal, "On the Secrecy Rate Region for the Interference Channel," in *Proc. IEEE PIMRC'08*, Cannes, France, Sept. 2008.