Securing Wireless Communications in the Physical Layer using Signal Processing

Şennur Ulukuş

Department of ECE

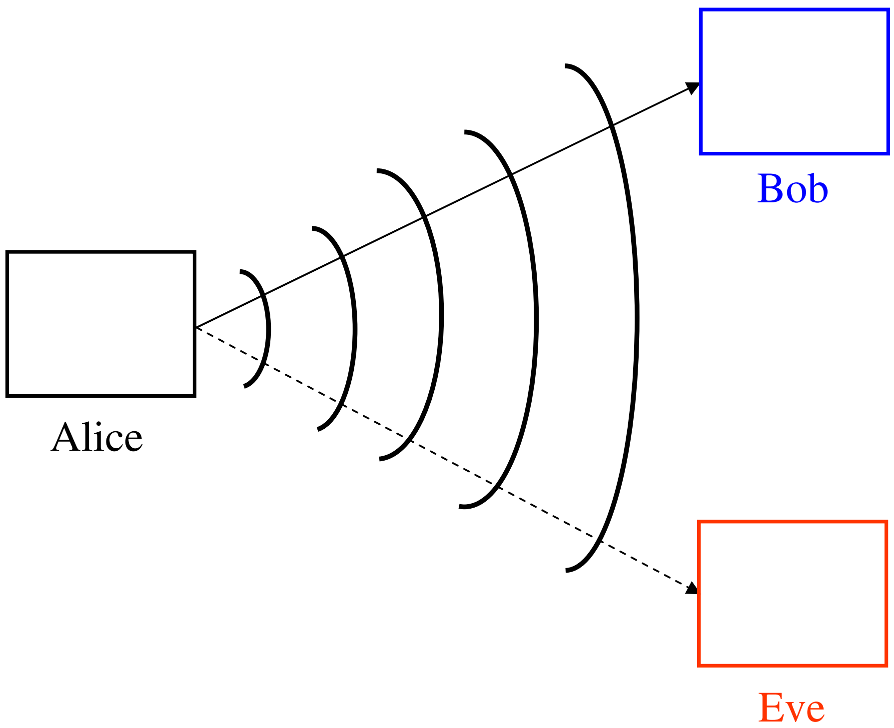
University of Maryland

ulukus@umd.edu

Joint work with Raef Bassily, Ersen Ekrem, Nan Liu, Shabnam Shafiee, Ravi Tandon.

Security in Wireless Systems

- Inherent openness in wireless communications channel: eavesdropping and **jamming** attacks



Countering Security Threats in Wireless Systems

- Cryptography
  - at higher layers of the protocol stack
  - based on the assumption of **limited computational power** at Eve
  - vulnerable to large-scale implementation of quantum computers
- Techniques like frequency hopping, CDMA
  - at the physical layer
  - based on the assumption of **limited knowledge** at Eve
  - vulnerable to rogue or captured node events
- Information theoretic security
  - at the physical layer
  - no assumption on Eve's computational power
  - no assumption on Eve's available information
  - **unbreakable, provable,** and **quantifiable** (in bits/sec/hertz)
  - implementable by signal processing, communications, and coding techniques
- Combining all: multi-dimensional, multi-faceted, cross-layer security

Cryptography

- One-time pad [Shannon 1949]
- $Y = X \oplus K$
- If K is uniform and independent of X, then Y is independent of X.
- If we know K, then $X = Y \oplus K$
- For perfect secrecy, length of K (key rate) must be as large as length of X (message rate)
- Two implications:
  - Need "absolutely secure" links to exchange keys
  - Need constant rates (equal to message rate) on these links

Private Key Cryptography

- Based on one-time pad
- There are separate secure communication links for key exchange
- Encryption and decryption are done using these keys
- Hard to construct "absolutely secure" links
- Hard to distribute and maintain secure keys
  - Especially in wireless and/or infrastructureless networks, i.e., ad-hoc and sensor networks
- Number of keys rapidly increases with the number of nodes
  - Need a distinct key for each transmitter-receiver pair

Public Key Cryptography

- Encryption is based on publicly known key (or method)
- Decryption can be performed only by the desired destination
- No need for “absolutely secure” links to distribute and maintain keys
- Security based on computational advantage
- Security against computationally limited adversaries
- Basic idea: Certain operations are easy in one direction, difficult in the other direction
  - Multiplication is easy, factoring is difficult (RSA)
  - Exponentiation is easy, discrete logarithm is difficult (Diffie-Hellman)

Rivest-Shamir-Adleman (RSA)

- Choose two large integers p and q. Let $n = pq$ and $\phi = (p-1)(q-1)$.
- Choose two numbers D and E such that $DE \mod \phi = 1$. Also, E is co-prime with ϕ.
- Make E and n public.
- ***E*** **is the encryption key, which is publicly known.** D is the decryption key.
- Alice wants to send a message m (which is a number between 0 and $n-1$) to Bob.
- Alice calculates $c = m^E$ and sends it.
- Bob, knowing D, calculates $c^D = m^{DE}$ in mod n.
- It is known that $m^{DE} \mod n = m$, hence Bob gets the message.
- For Eve to decode the message, she needs D.
- To find D, Eve needs to factor n into p and q, and calculate ϕ, and knowing E, find D.
- Factoring a large integer into its prime multipliers is known to be a difficult problem.

Diffie-Hellman

- Alice and Bob wish to settle on a secret key.
- Choose a large base n, and an integer g.
- Alice chooses a key k_1, Bob chooses a key k_2.
- Alice calculates g^{k_1} and sends it to Bob.
- Bob calculates g^{k_2} and sends it to Alice.
- Alice raises what she receives from Bob to power k_1, and gets $g^{k_1 k_2}$.
- Bob raises what he receives from Alice to power k_2, and gets $g^{k_1 k_2}$.
- Alice and Bob agree on the secret key $g^{k_1 k_2}$.
- For Eve to decypher the key, she needs to take discrete logarithms of what she observes.
- Eve needs to find k_1 by $\log(g^{k_1})$ and find k_2 by $\log(g^{k_2})$ and calculate $g^{k_1 k_2}$
- Taking the discrete logarithm of a large number is known to be a difficult problem.

Single-User Channel

- We first consider the single-user channel:

- Channel is memoryless

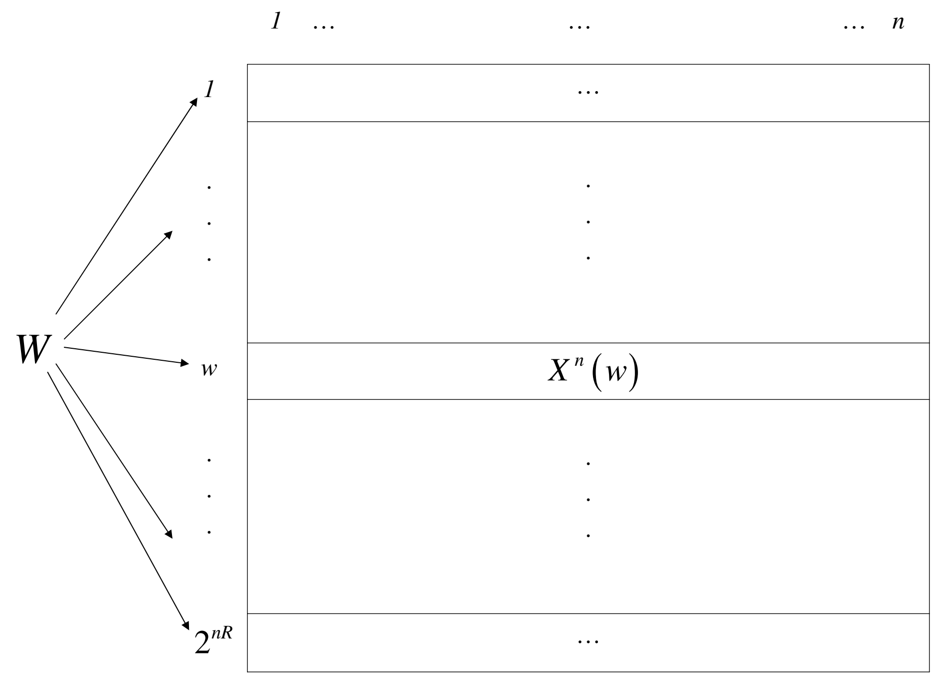
$$p(y^n|x^n) = \prod_{i=1}^{n} p(y_i|x_i)$$

- Capacity of a single-user memoryless channel is

$$C = \max_{p(x)} I(X;Y)$$

Single-User Channel-Achievability

- Fix a $p(x)$. Fill the $2^{nR} \times n$ codebook with i.i.d. realizations:



- Receiver decides $\hat{w}$ is sent, if it is the unique message such that $(x^n(\hat{w}), y^n)$ is jointly typical
- Probability of error goes to zero as $n \to \infty$, if

$$R \leq C = \max_{p(x)} I(X;Y)$$

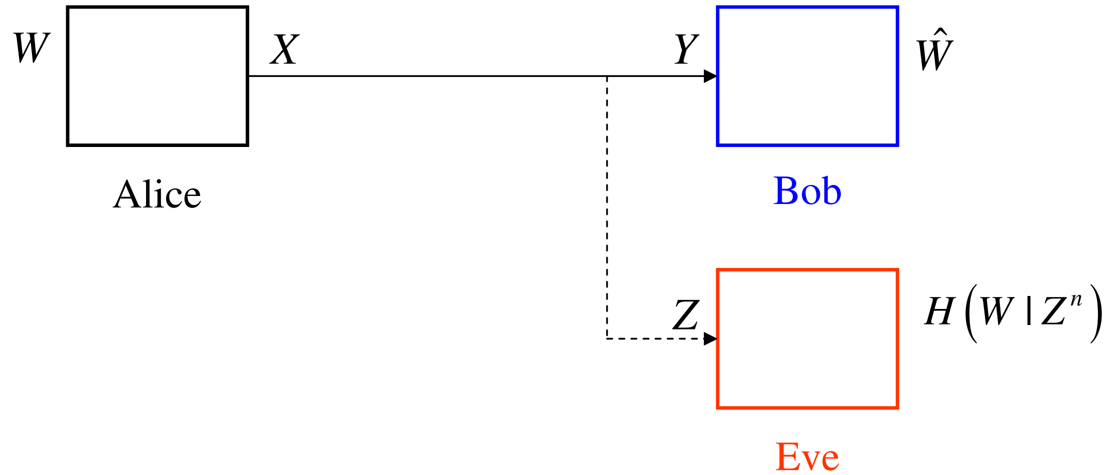
Single-User Channel-Converse

- The converse proof goes as follows

$$
\begin{aligned}
nR &= H(W) \\
&= I(W;Y^n) + H(W|Y^n) \\
&\leq I(W;Y^n) + n\varepsilon_n \\
&\leq I(W,X^n;Y^n) + n\varepsilon_n \\
&= I(X^n;Y^n) + n\varepsilon_n \\
&= \sum_{i=1}^{n} I(X^n;Y_i|Y^{i-1}) + n\varepsilon_n \\
&\leq \sum_{i=1}^{n} H(Y_i) - H(Y_i|X_i) + n\varepsilon_n \\
&= \sum_{i=1}^{n} I(X_i;Y_i) + n\varepsilon_n \\
&\leq nC + n\varepsilon_n
\end{aligned}
$$

Wiretap Channel

- Wyner introduced the **wiretap** channel in 1975.
- Eve gets a worse (degraded) version of Bob's signal:



- Secrecy is measured by **equivocation**, R_e, at Eve, i.e., the **confusion** at Eve:

$$R_e = \lim_{n \to \infty} \frac{1}{n} H(W|Z^n)$$

Notions of Perfect Secrecy

- Perfect secrecy is achieved if $R = R_e$
- Two notions of perfect secrecy
- Weak secrecy: The normalized mutual information between the message and Eve's observation vanishes

$$\lim_{n \to \infty} \frac{1}{n} I(W;Z^n) = 0$$

- Strong secrecy: The message and Eve's observation are almost independent

$$\lim_{n \to \infty} I(W;Z^n) = 0$$

- All capacity results obtained for weak secrecy have been extended for strong secrecy
- However, there is still no proof of equivalence or strict containment

Capacity-Equivocation Region-I

- Wyner characterized the optimal (R, R_e) region:

$$R \leq I(X;Y)$$
$$R_e \leq I(X;Y) - I(X;Z)$$

- Main idea is to split the message W into two coordinates, secret and public: (W_s, W_p).
- W_s needs to be transmitted in perfect secrecy:

$$\lim_{n \to \infty} \frac{1}{n} I(W_s; Z^n) = 0$$

- W_p has two roles
  - Carries some information on which there is no secrecy constraint
  - Provides protection for W_s

Capacity-Equivocation Region-II

- Perfect secrecy when $R = R_e$.
- The maximum perfect secrecy rate, i.e., the secrecy capacity:

$$C_s = \max_{X \rightarrow Y \rightarrow Z} I(X;Y) - I(X;Z)$$

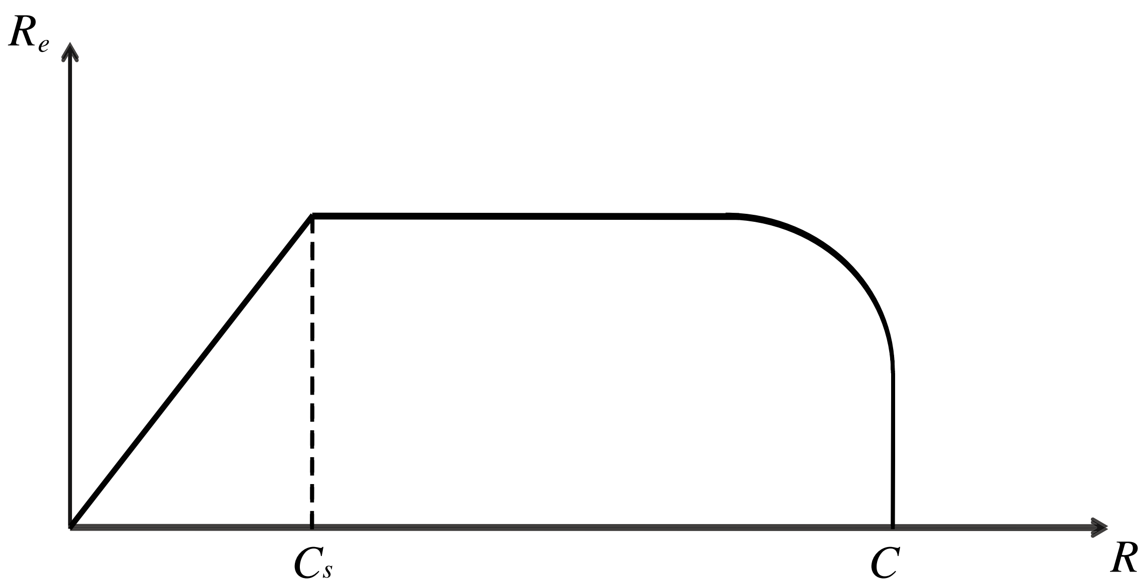
- Main idea is to replace W_p with dummy indices
- In particular, each W_s is mapped to **many** codewords:
  - Stochastic encoding (a.k.a. random binning)
- This one-to-many mapping aims to confuse the eavesdropper

Capacity-Equivocation Region-III

- Wyner characterized the optimal (R, R_e) region:

$$R \leq I(X;Y)$$
$$R_e \leq I(X;Y) - I(X;Z)$$

- A typical (R, R_e) region:



- There might be a tradeoff between rate and its equivocation:
  - Capacity and secrecy capacity might not be simultaneously achievable

Capacity-Equivocation Region-IV

- Wyner characterized the optimal (R, R_e) region:

$$R \leq I(X;Y)$$
$$R_e \leq I(X;Y) - I(X;Z)$$

- Wyner's model mainly considers the wireline networks
  - Eve's observation is strictly worse than Bob's observation, i.e., $X \rightarrow Y \rightarrow Z$

Achievability-I

- First we show the achievability of the perfect secrecy rate

$$R_s = I(X;Y) - I(X;Z)$$

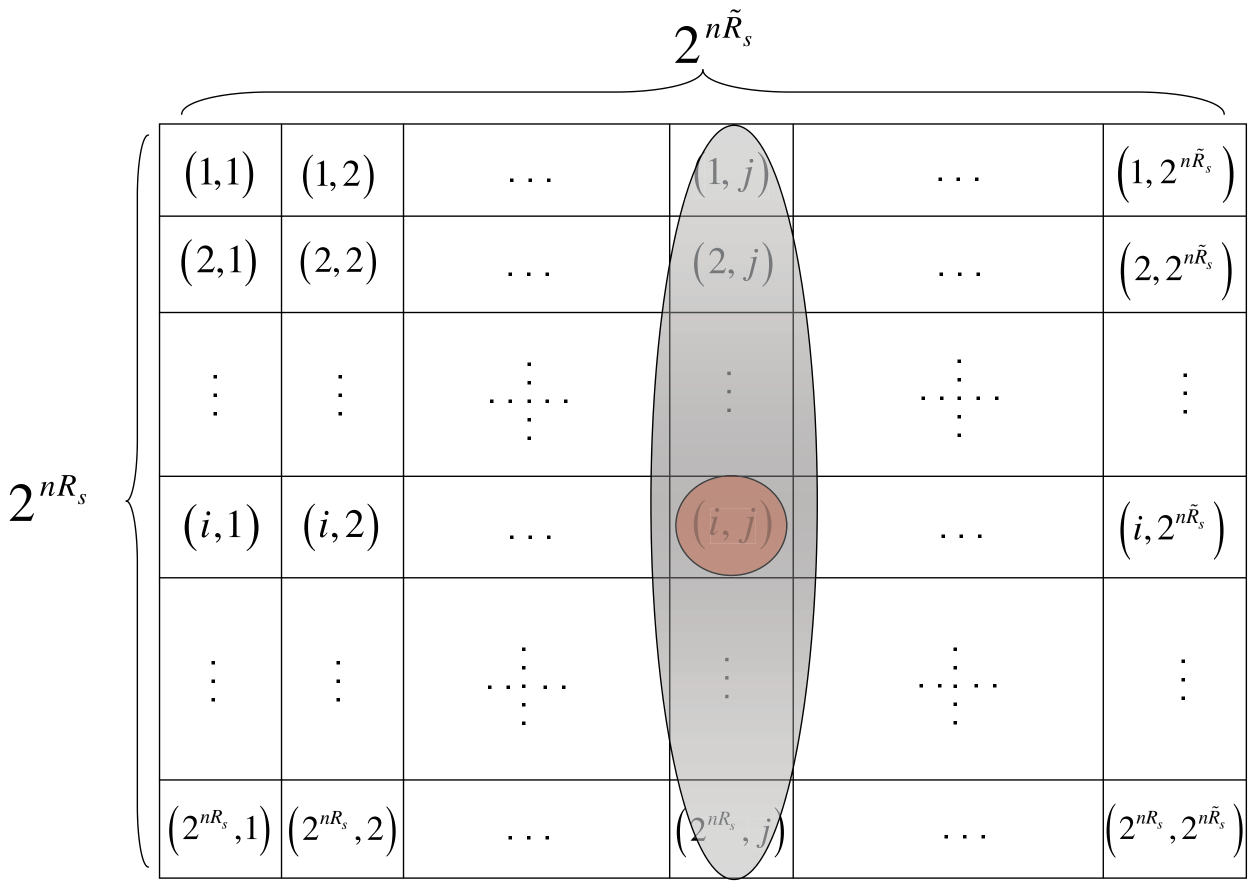
- Fix a distribution $p(x)$
- Generate $2^{n(R_s+\tilde{R}_s)}$ x^n sequences through $p(x^n) = \prod_{i=1}^{n} p(x_i)$
- Index these sequences as $x^n(w_s, \tilde{w}_s)$ where

$$w_s \in \left\{1, \ldots, 2^{nR_s}\right\}$$
$$\tilde{w}_s \in \left\{1, \ldots, 2^{n\tilde{R}_s}\right\}$$

- w_s denotes the actual secret message
- $\tilde{w}_s$ denotes the protection (confusion) messages with no information content
  - Their sole purpose is to confuse the eavesdropper, i.e., ensure the confidentiality of w_s

Achievability-II

- Codebook structure



$$R_s = I(X;Y) - I(X;Z), \quad \tilde{R}_s = I(X;Z)$$

Achievability-III

- If w_s is the secret message to be sent, the encoder selects $\tilde{w}_s$ randomly from $\left\{1,\ldots,2^{n\tilde{R}_s}\right\}$, and sends $x^n(w_s,\tilde{w}_s)$
- Legitimate user decides on $\hat{w}_s$ if it is the unique index such that $(x^n(\hat{w}_s,\tilde{w}_s),y^n)$ is jointly typical:

$$R_s+\tilde{R}_s \leq I(X;Y)$$

- Next we show that this code satisfies the perfect secrecy requirement:

$$\lim_{n\to\infty}\frac{1}{n}I(W_s;Z^n)=0$$

- To this end, we set $\tilde{R}_s$ as

$$\tilde{R}_s = I(X;Z)-\varepsilon$$

where $\varepsilon > 0$.

Achievability-IV

- We have the following

$$
\begin{aligned}
H(W_s|Z^n) &= H(W_s,\tilde{W}_s|Z^n) - H(\tilde{W}_s|W_s,Z^n) \\
&= H(W_s,\tilde{W}_s) - I(W_s,\tilde{W}_s;Z^n) - H(\tilde{W}_s|W_s,Z^n) \\
&\geq H(W_s,\tilde{W}_s) - I(W_s,\tilde{W}_s,X^n;Z^n) - H(\tilde{W}_s|W_s,Z^n) \\
&= H(W_s,\tilde{W}_s) - I(X^n;Z^n) - H(\tilde{W}_s|W_s,Z^n) \\
&= H(W_s) + H(\tilde{W}_s) - I(X^n;Z^n) - H(\tilde{W}_s|W_s,Z^n)
\end{aligned}
$$

  which is

$$
I(W_s;Z^n) \leq I(X^n;Z^n) + H(\tilde{W}_s|W_s,Z^n) - H(\tilde{W}_s)
$$

- We treat each term separately

Achievability-V

- We have

$$H(\tilde{W}_s) = n\tilde{R}_s = n(I(X;Z) - \varepsilon)$$

- We have

$$I(X^n;Z^n) \leq \sum_{i=1}^{n} I(X_i;Z_i) \leq n(I(X;Z) + \gamma_n)$$

where $\gamma_n \to 0$ as $n \to \infty$.

- Finally, we consider

$$H(\tilde{W}_s|W_s, Z^n)$$

- Given $W_s = w_s$, $X^n(w_s, \tilde{W}_s)$ can take $2^{n\tilde{R}_s}$ values where $\tilde{R}_s = I(X;Z) - \varepsilon$
- Thus, the eavesdropper can decode $\tilde{W}_s$ given $W_s = w_s$ by looking for the unique $\tilde{w}_s$ such that $(X^n(w_s, \tilde{w}_s), Z^n)$ is jointly typical
- Hence, Fano's lemma reads

$$H(\tilde{W}_s|W_s, Z^n) \leq n\beta_n$$

where $\beta_n \to 0$ as $n \to \infty$.

Achievability-VI

- Combining all these findings yield

$$\frac{1}{n}I(W_s;Z^n) \leq \beta_n + \gamma_n + \varepsilon$$

- Since ε was arbitrary, we have

$$\lim_{n\to\infty} \frac{1}{n}I(W_s;Z^n) = 0$$

  i.e., perfect secrecy is achieved.

- Thus, $R_s = I(X;Y) - I(X;Z)$ is an achievable perfect secrecy rate

Achievability of Rate-Equivocation Region-I

- In perfect secrecy case, each secret message W_s is associated with many codewords

$$X^n(W_s, \tilde{W}_s)$$

- Legitimate user decodes both W_s and $\tilde{W}_s$
- There is a rate for $\tilde{W}_s$ which does not carry any information content
- $\tilde{W}_s$ can be replaced with some information on which there is no secrecy constraint, i.e., it does not need to be confidential:
  - Rate-equivocation region

Achievability of Rate-Equivocation Region-II

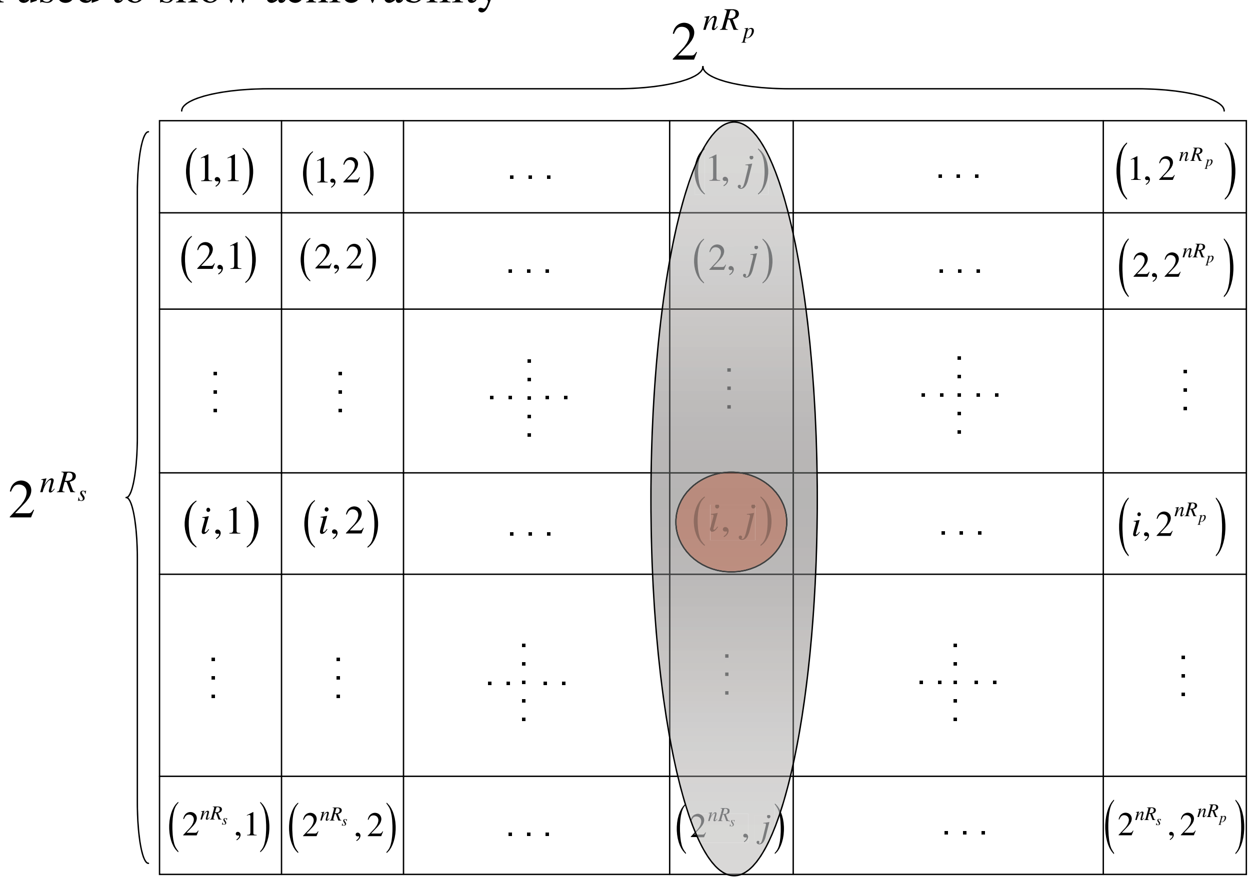
- Each message W is divided into two parts:
  - Secret message W_s
  - Public message W_p
- We have doubly indexed codewords

$$X^n(W_s, W_p)$$

- We need to show
  - Rate $R = R_s + R_p$ can be delivered to Bob
  - Rate R_s can be kept hidden from Eve

Achievability of Rate-Equivocation Region-III

- Codebook used to show achievability



$$R_s = I(X;Y) - I(X;Z), \quad R_p = I(X;Z)$$

Achievability of Rate-Equivocation Region-IV

- $R = R_s + R_p$ can be delivered to Bob as long as

$$R_s + R_p \leq I(X;Y)$$

- We set R_p as

$$R_p = I(X;Z)$$

- Equivocation computation

$$\begin{aligned} H(W|Z^n) &= H(W_s, W_p|Z^n) \\ &= H(W_s, W_p) - I(W_s, W_p; Z^n) \\ &\geq H(W_s, W_p) - I(W_s, W_p, X^n; Z^n) \\ &= H(W_s, W_p) - I(X^n; Z^n) \\ &= H(W_s) + H(W_p) - I(X^n; Z^n) \end{aligned}$$

- As $n \to \infty$, $(X^n(w_s, w_p), Z^n)$ will be jointly typical with high probability:

$$I(X^n; Z^n) \leq nI(X;Z) + n\varepsilon_n$$

where $\varepsilon_n \to 0$ as $n \to \infty$

Achievability of Rate-Equivocation Region-V

- Equivocation computation proceeds as follows

$$\begin{aligned} H(W|Z^n) &\geq H(W_s) + H(W_p) - nI(X;Z) - n\varepsilon_n \\ &= H(W_s) - n\varepsilon_n \\ &= n\left[I(X;Y) - I(X;Z)\right] - n\varepsilon_n \end{aligned}$$

- Thus, we have

$$\lim_{n\to\infty} \frac{1}{n} H(W|Z^n) \geq I(X;Y) - I(X;Z)$$

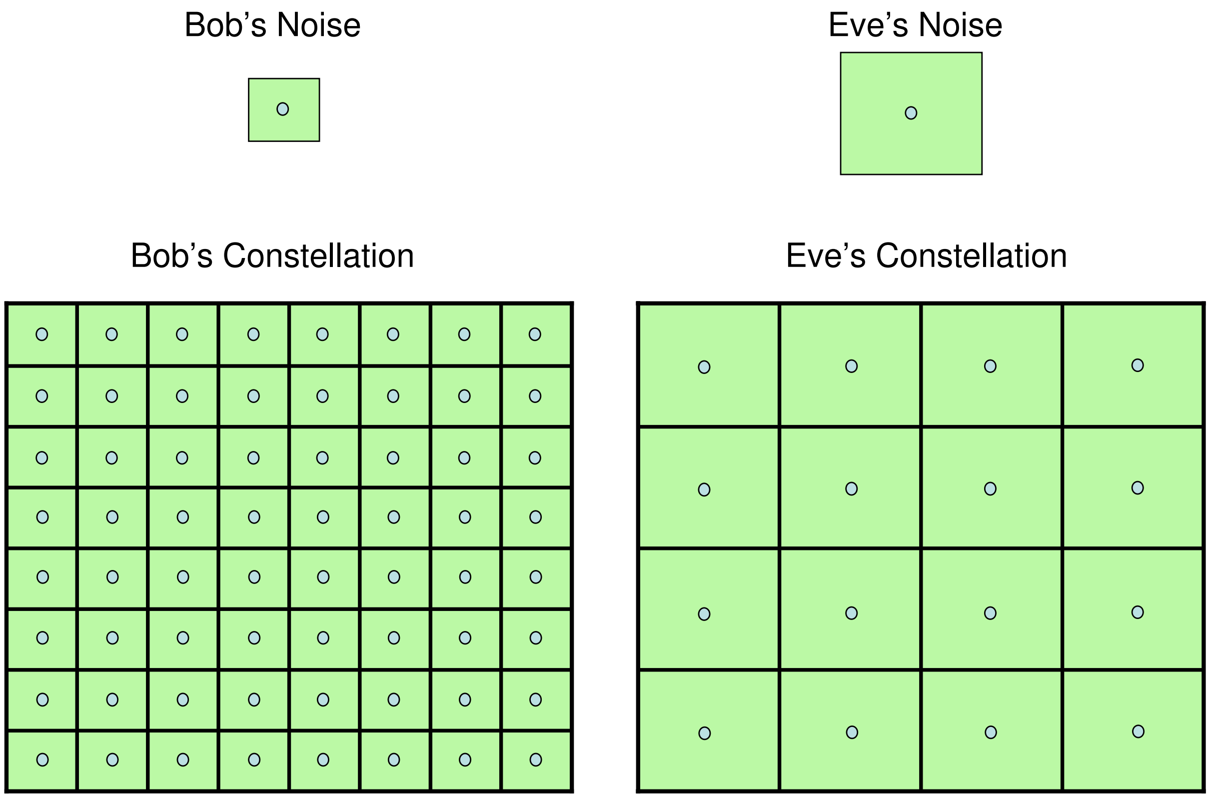
i.e., $I(X;Y) - I(X;Z)$ is an achievable equivocation rate.

- Using the analysis for perfect secrecy case, we can also show

$$\lim_{n\to\infty} \frac{1}{n} I(W_s;Z^n) = 0$$

i.e., W_s is transmitted in perfect secrecy.

Stochastic Encoding: 64-QAM Example-I

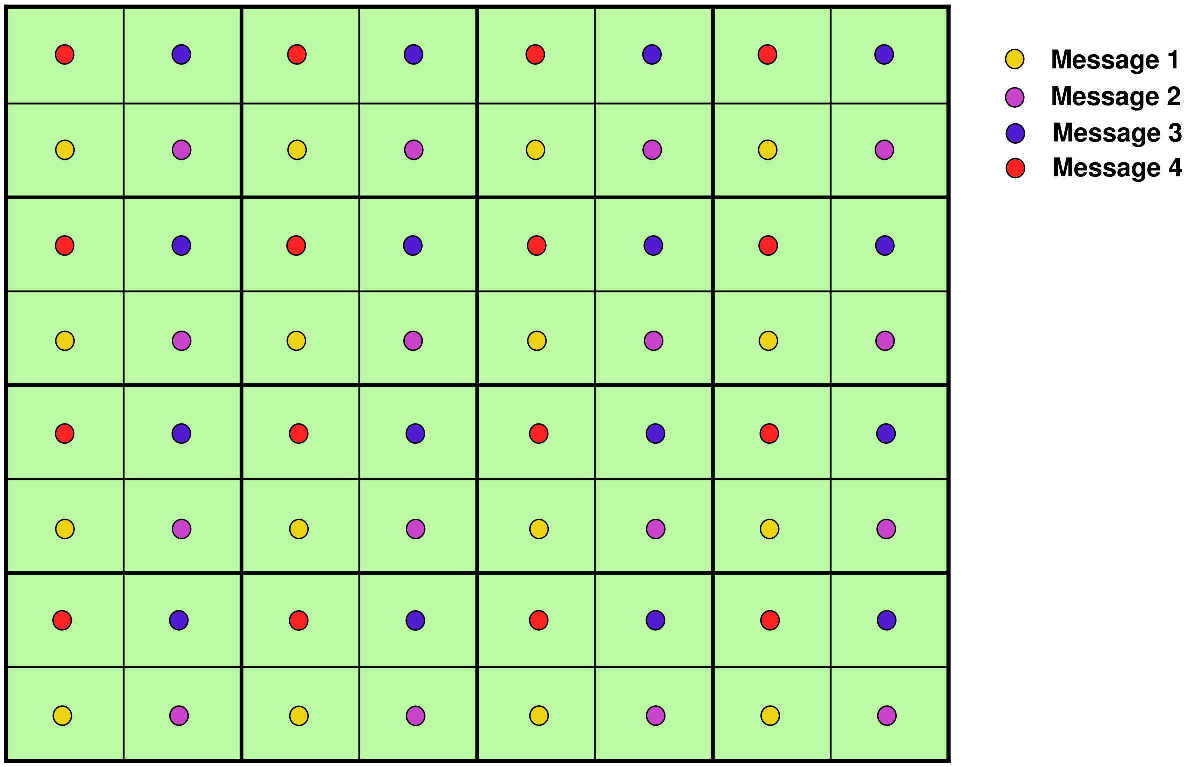


$C_B = \log_2 64 = 6$ b/s

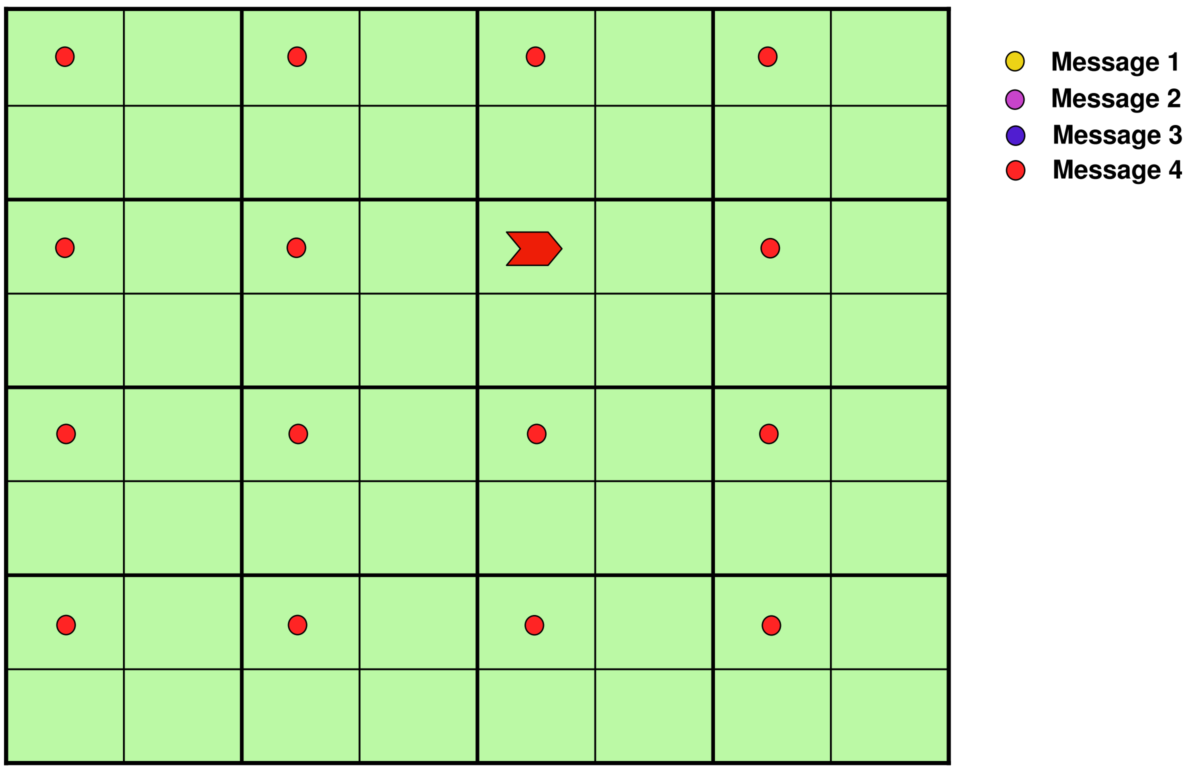
$C_E = \log_2 16 = 4$ b/s

$C_s = C_B - C_E = 2$ b/s

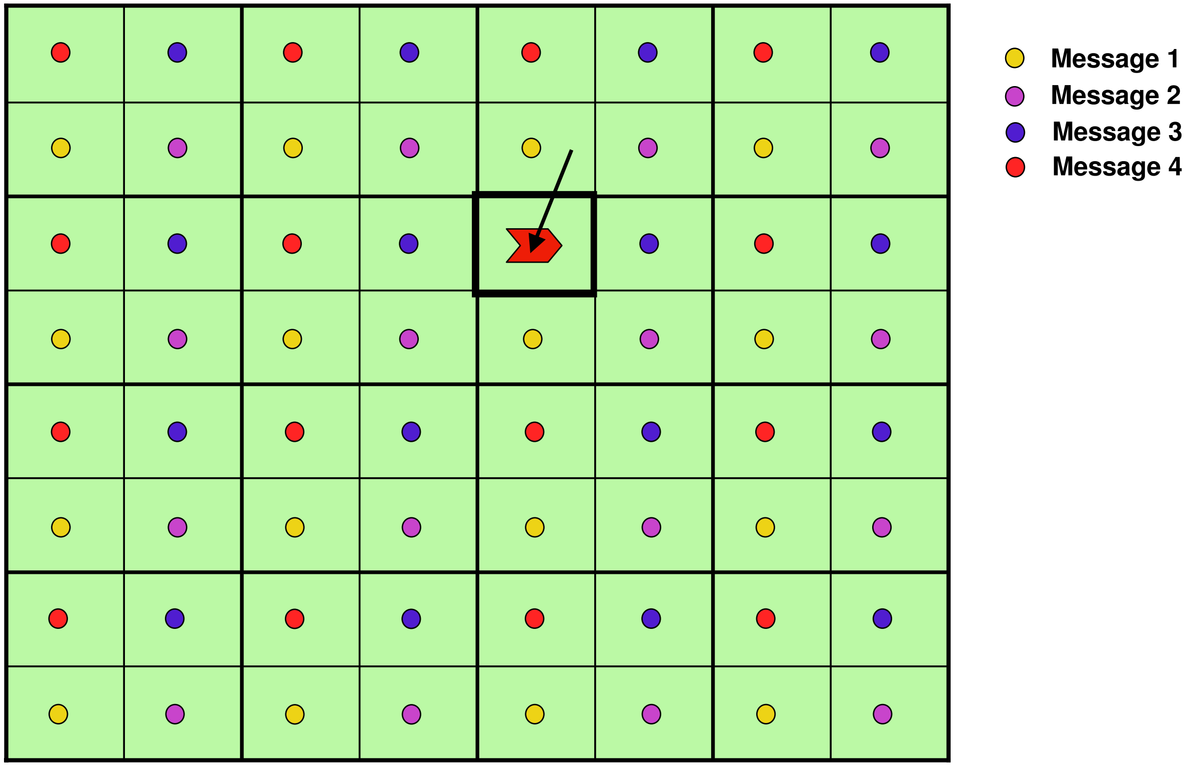
Stochastic Encoding: 64-QAM Example-II



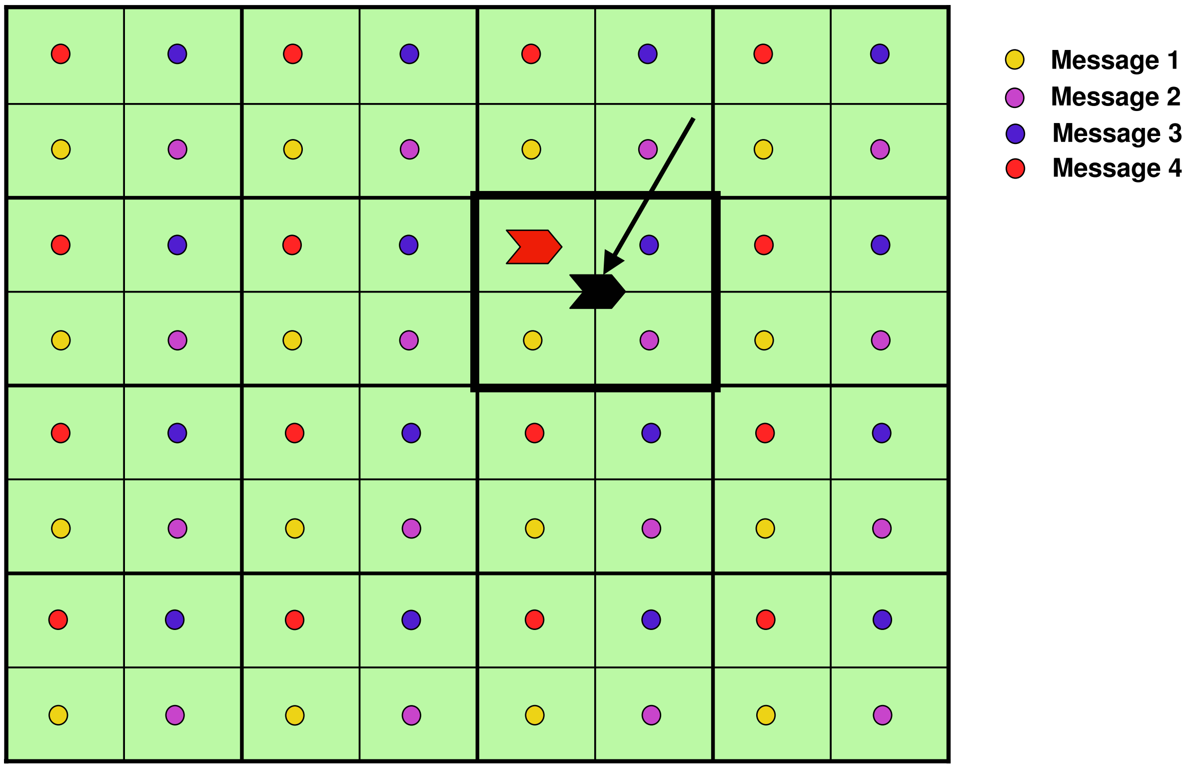
Stochastic Encoding: 64-QAM Example-III



Stochastic Encoding: 64-QAM Example-IV

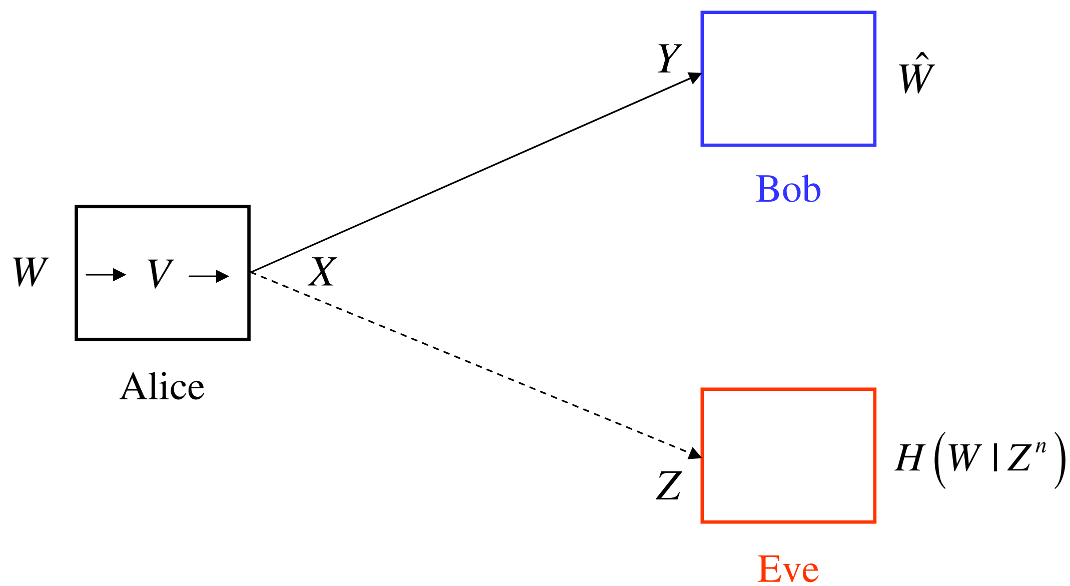


Stochastic Encoding: 64-QAM Example-V



Broadcast Channel with Confidential Messages-I

- Csiszar and Korner considered the general wiretap channel in 1978.
- They extended Wyner's model in two ways
  - Eve's signal is not necessarily a degraded version of Bob's signal.
  - There is a common message for both Eve and Bob



Broadcast Channel with Confidential Messages-II

- Capacity-equivocation region is obtained as union of rate triples (R_0, R_1, R_e) satisfying

$$
\begin{aligned}
R_0 &\leq \min\{I(U;Y), I(U;Z)\} \\
R_0 + R_1 &\leq I(V;Y|U) + \min\{I(U;Y), I(U;Z)\} \\
R_e &\leq I(V;Y|U) - I(V;Z|U)
\end{aligned}
$$

  for some (U,V) such that

$$
U \to V \to X \to Y \to Z
$$

- New ingredients in the achievable scheme:
  - Superposition coding to accommodate the common message
  - Channel prefixing

Outline of the Achievability

- Achievability of the following region is shown

$$R_0 \leq \min\{I(U;Y), I(U;Z)\}$$
$$R_0 + R_1 \leq I(X;Y|U) + \min\{I(U;Y), I(U;Z)\}$$
$$R_e \leq I(X;Y|U) - I(X;Z|U)$$

  for some (U,X) such that

$$U \rightarrow X \rightarrow Y \rightarrow Z$$

- Channel prefixing, i.e., introduction of a hypothetical channel between U and X by means of V, gives the capacity region

Capacity-Equivocation Region for $R_0 = 0$-I

- When there is no common message, capacity-equivocation region

$$R_1 \leq I(V;Y)$$
$$R_e \leq I(V;Y|U) - I(V;Z|U)$$

for some (U,V) such that

$$U \rightarrow V \rightarrow X \rightarrow Y \rightarrow Z$$

- Even if common message is not present, we still need two auxiliary rv.s
- In other words, we still need superposition coding

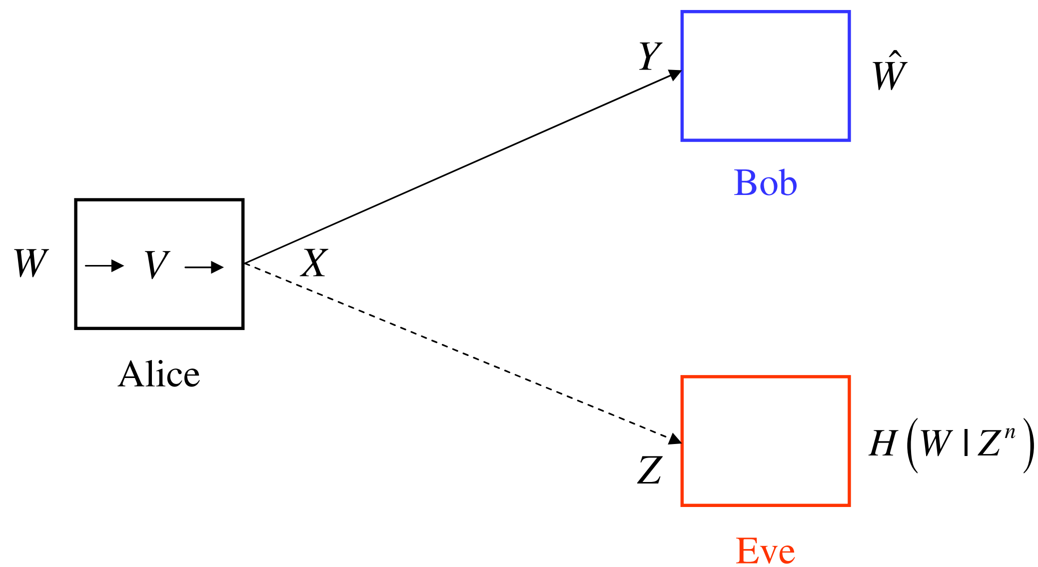
Capacity-Equivocation Region for $R_0 = 0$-II

- Divide message W into three parts: W_p', W_p'', W_s
- W_p', W_p'' are public messages on which there is no secrecy constraint
- W_s is the confidential part which needs to be transmitted in perfect secrecy
- W_p' is transmitted by the first layer, i.e., U
- W_p'', W_s are transmitted by the second layer, i.e., V
- Similar to Wyner's scheme, W_p'' has two roles
  - Carries part of the public information on which there is no secrecy constraint
  - Provides protection for W_s

Secrecy Capacity for Broadcast Channel with Confidential Messages-I

- Secrecy capacity is

$$
\begin{aligned}
C_s &= \max_{U \to V \to X \to (Y,Z)} I(V;Y|U) - I(V;Z|U) \\
&= \max_{U \to V \to X \to (Y,Z)} \sum_u p_U(u) I(V;Y|U=u) - I(V;Z|U=u) \\
&= \max_{V \to X \to (Y,Z)} I(V;Y) - I(V;Z)
\end{aligned}
$$



Secrecy Capacity for Broadcast Channel with Confidential Messages-II

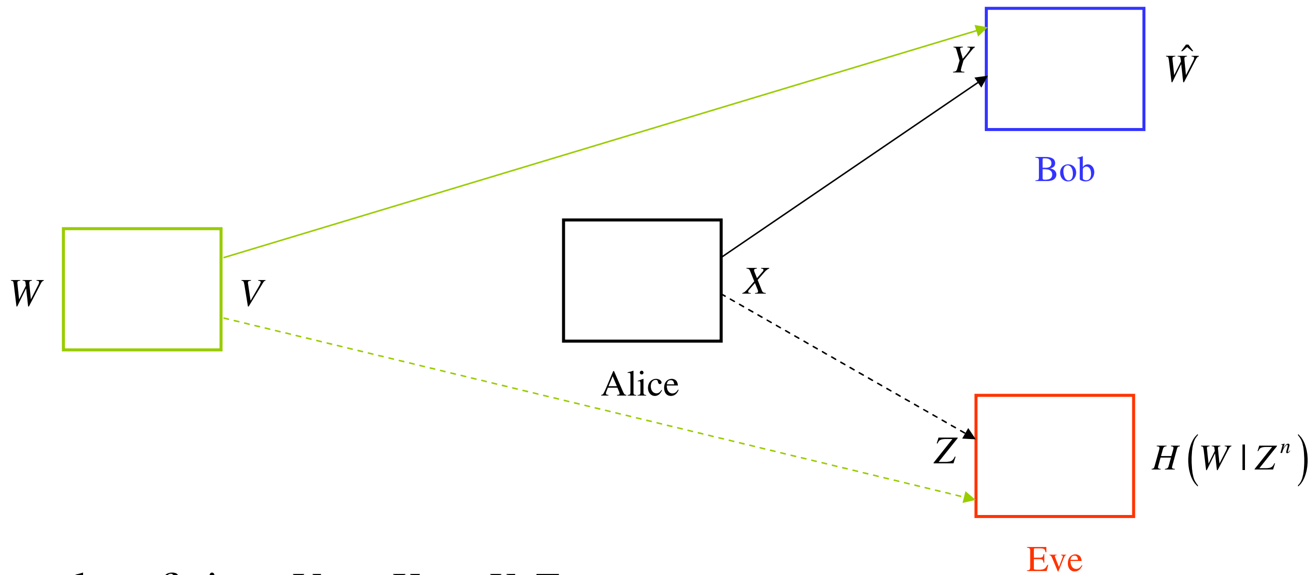
- The secrecy capacity:

$$C_s = \max_{V \to X \to YZ} I(V;Y) - I(V;Z)$$

- The new ingredient: **channel prefixing** through the introduction of V.
- No channel prefixing is a special case of channel prefixing by choosing $V = X$.

Channel Prefixing

- A virtual channel from V to X.
- Additional stochastic mapping from the message to the channel input: $W \to V \to X$.
- Real channel: $X \to Y$ and $X \to Z$. Constructed channel: $V \to Y$ and $V \to Z$.



- With channel prefixing: $V \to X \to Y, Z$.
- From DPI, both mutual informations decrease, but the difference may increase.
- The secrecy capacity:

$$C_s = \max_{V \to X \to YZ} I(V;Y) - I(V;Z)$$

Converse-I

- Csiszar sum lemma is crucial:

  Lemma 1 *Let T^n, U^n be length-n random vectors, and G be a random variable. We have*

$$\sum_{i=1}^{n} I(U_{i+1}^n; T_i | G, T^{i-1}) = \sum_{i=1}^{n} I(T^{i-1}; U_i | G, U_{i+1}^n)$$

- Due to secrecy condition, we have

$$I(W_s; Z^n) \leq n\gamma_n$$

  where $\gamma_n \to 0$ as $n \to \infty$.

- Fano's lemma implies

$$H(W_s | Y^n) \leq n\varepsilon_n$$

  where $\varepsilon_n \to 0$ as $n \to \infty$.

Converse-II

- Thus, we have

$$
\begin{aligned}
nR_s &= H(W_s) \\
&\leq I(W_s;Y^n) + n\varepsilon_n \\
&\leq I(W_s;Y^n) - I(W_s;Z^n) + n(\varepsilon_n + \gamma_n) \\
&= \sum_{i=1}^{n} I(W_s;Y_i|Y^{i-1}) - I(W_s;Z_i|Z_{i+1}^n) + n(\varepsilon_n + \gamma_n) \\
&= \sum_{i=1}^{n} I(W_s;Y_i|Y^{i-1}) - I(W_s;Z_i|Z_{i+1}^n) + \underline{I(Z_{i+1}^n;Y_i|W_s,Y^{i-1})} - \underline{I(Y^{i-1};Z_i|W_s,Z_{i+1}^n)} + n(\varepsilon_n + \gamma_n) \\
&= \sum_{i=1}^{n} I(W_s,Z_{i+1}^n;Y_i|Y^{i-1}) - I(W_s,Y^{i-1};Z_i|Z_{i+1}^n) + n(\varepsilon_n + \gamma_n) \\
&= \sum_{i=1}^{n} I(W_s;Y_i|Y^{i-1},Z_{i+1}^n) - I(W_s;Z_i|Z_{i+1}^n,Y^{i-1}) + \underline{I(Z_{i+1}^n;Y_i|Y^{i-1})} - \underline{I(Y^{i-1};Z_i|Z_{i+1}^n)} + n(\varepsilon_n + \gamma_n) \\
&= \sum_{i=1}^{n} I(W_s;Y_i|Y^{i-1},Z_{i+1}^n) - I(W_s;Z_i|Z_{i+1}^n,Y^{i-1}) + n(\varepsilon_n + \gamma_n)
\end{aligned}
$$

where the underlined terms are equal due to Csiszar sum lemma.

Converse-III

- We define

$$U_i = Y^{i-1} Z_{i+1}^n$$
$$V_i = W_s U_i$$

which satisfy

$$U_i \rightarrow V_i \rightarrow X_i \rightarrow Y_i, Z_i$$

- Thus, we have

$$nR_s \leq \sum_{i=1}^{n} I(V_i; Y_i | U_i) - I(V_i; Z_i | U_i) + n(\varepsilon_n + \gamma_n)$$

- After single-letterization

$$R_s \leq I(V; Y | U) - I(V; Z | U)$$

- Thus, we have

$$\begin{aligned} C_s &\leq \max_{U \rightarrow V \rightarrow X \rightarrow Y,Z} I(V; Y | U) - I(V; Z | U) \\ &= \max_{V \rightarrow X \rightarrow Y,Z} I(V; Y) - I(V; Z) \end{aligned}$$

Converse-IV

- If channel is degraded, i.e.,

$$X \rightarrow Y \rightarrow Z$$

we have

$$\begin{aligned} I(X;Y|V) - I(X;Z|V) &= I(X;Y,Z|V) - I(X;Z|V) \\ &= I(X;Y|V,Z) \\ &\geq 0 \end{aligned}$$

where V is such that $V \rightarrow X \rightarrow Y \rightarrow Z$.

- Hence, for degraded wiretap channel, we have

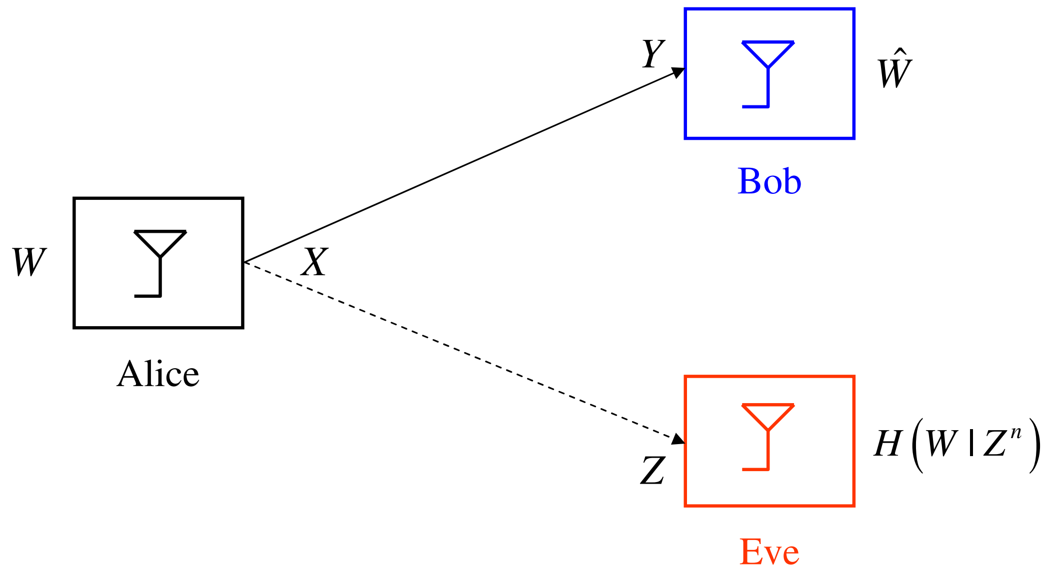
$$\begin{aligned} C_s &\leq \max_{V \rightarrow X \rightarrow Y,Z} I(V;Y) - I(V;Z) \\ &\leq \max_{V \rightarrow X \rightarrow Y,Z} I(V;Y) - I(V;Z) + I(X;Y|V) - I(X;Z|V) \\ &\leq \max_{V \rightarrow X \rightarrow Y,Z} I(V,X;Y) - I(V,X;Z) \\ &\leq \max_{X \rightarrow Y,Z} I(X;Y) - I(X;Z) \end{aligned}$$

Gaussian Wiretap Channel-I

- Leung-Yang-Cheong and Hellman considered the Gaussian wire-tap channel in 1978.

$$Y = X + N_Y$$

$$Z = X + N_Z$$



- Key observation: Capacity-equivocation region depends on the marginal distributions $p(y|x)$ and $p(z|x)$, but not the joint distribution $p(y,z|x)$
- Gaussian case: Capacity-equivocation region does not depend on the correlation between N_Y and N_Z

Gaussian Wiretap Channel-II

- Eve's signal is Bob's signal plus Gaussian noise, or vice versa: a **degraded** wiretap channel:
  - If $\sigma_Y^2 \geq \sigma_Z^2$, $Y = Z + \tilde{N}$

$$X \rightarrow Z \rightarrow Y$$

  - If $\sigma_Z^2 \geq \sigma_Y^2$, $Z = Y + \tilde{N}$

$$X \rightarrow Y \rightarrow Z$$

- No channel prefixing is necessary and Gaussian signalling is optimal.
- The secrecy capacity:

$$C_s = \max_{X \rightarrow Y \rightarrow Z} I(X;Y) - I(X;Z) = [C_B - C_E]^+$$

i.e., the difference of two capacities.

Gaussian Wiretap Channel-III

- Secrecy capacity can be obtained in three ways:
  - Entropy-power inequality

$$e^{2h(U+V)} \geq e^{2h(U)} + e^{2h(V)}$$

  - I-MMSE formula

$$I(X;\sqrt{\mathrm{snr}}X+N) = \frac{1}{2}\int_0^{snr} \mathrm{mmse}(X/\sqrt{t}X+N)dt$$

  - Conditional maximum entropy theorem

$$h(V|U) \leq h(V^G|U^G)$$

Gaussian Wiretap Channel-IV

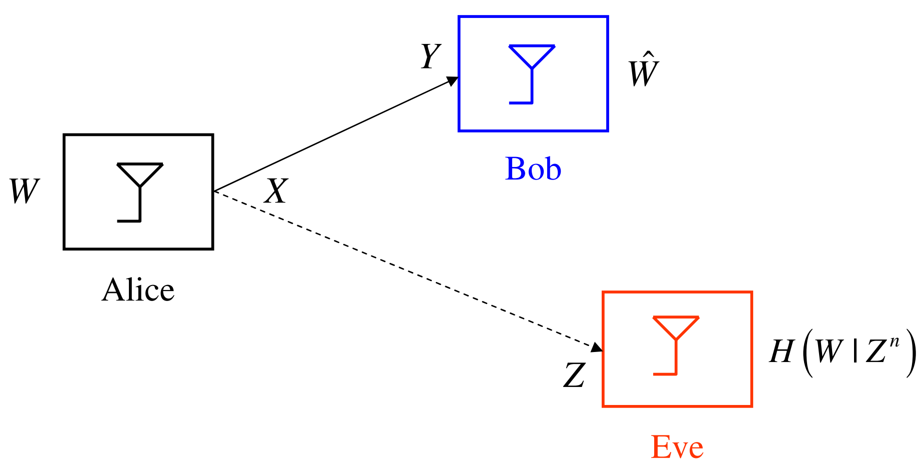
- Using entropy-power inequality

$$
\begin{aligned}
I(X;Y) - I(X;Z) &= I(X;Y) - I(X;Y+\tilde{N}) \\
&= h(Y) - h(Y+\tilde{N}) - \frac{1}{2}\log\frac{\sigma_Y^2}{\sigma_Z^2} \\
&\leq h(Y) - \frac{1}{2}\log(e^{2h(Y)} + 2\pi e(\sigma_Z^2 - \sigma_Y^2)) - \frac{1}{2}\log\frac{\sigma_Y^2}{\sigma_Z^2} \\
&\leq \frac{1}{2}\log(2\pi e)(P+\sigma_Y^2) - \frac{1}{2}\log((2\pi e)(P+\sigma_Y^2) + (2\pi e)(\sigma_Z^2 - \sigma_Y^2)) - \frac{1}{2}\log\frac{\sigma_Y^2}{\sigma_Z^2} \\
&= \frac{1}{2}\log\left(1+\frac{P}{\sigma_Y^2}\right) - \frac{1}{2}\log\left(1+\frac{P}{\sigma_Z^2}\right) \\
&= C_B - C_E
\end{aligned}
$$

Caveat: Need Channel Advantage

The secrecy capacity: $C_s = [C_B - C_E]^+$

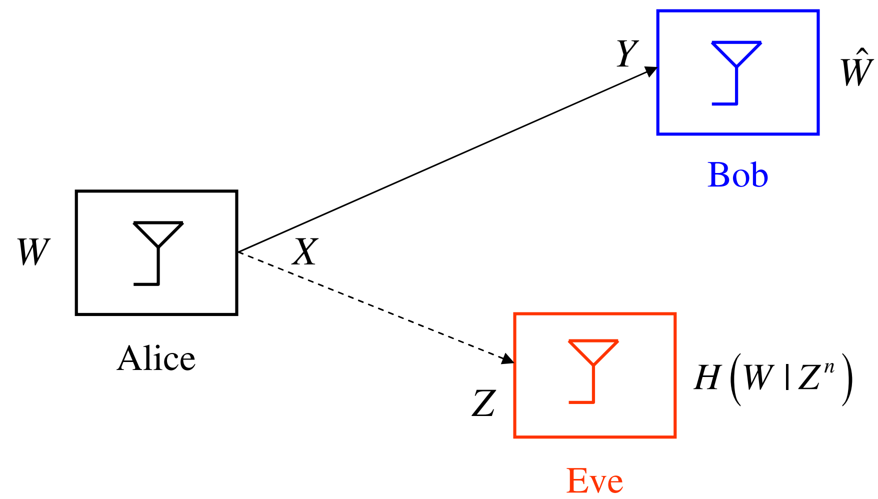
Bob's channel is better



positive secrecy

$$C_s = C_B - C_E$$

Eve's channel is better



no secrecy

$$C_s = 0$$

Outlook at the End of 1970s and Transition into 2000s

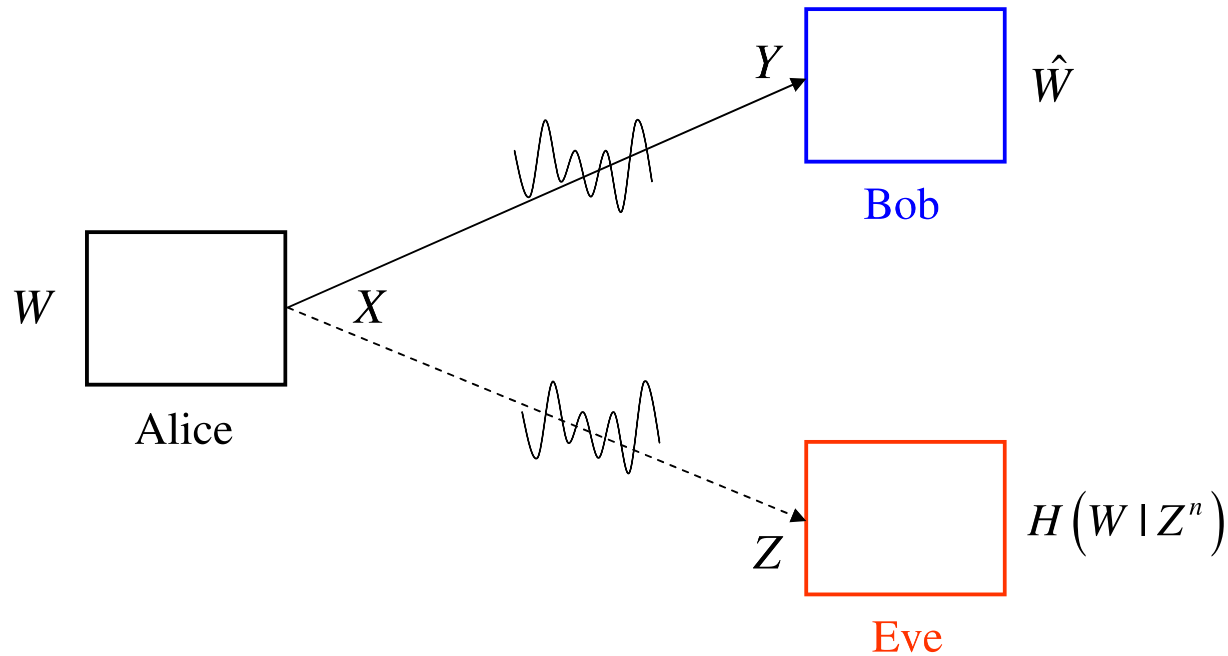
- Information theoretic secrecy is extremely powerful:
  - no limitation on Eve's computational power
  - no limitation on Eve's available information
  - yet, we are able to provide secrecy to the legitimate user
  - **unbreakable, provable,** and **quantifiable** (in bits/sec/hertz) secrecy
- We seem to be at the mercy of the nature:
  - if Bob's channel is stronger, positive perfect secrecy rate
  - if Eve's channel is stronger, no secrecy
- We need channel advantage. Can we create channel advantage?
- Wireless channel provides many options:
  - time, frequency, multi-user diversity
  - cooperation via overheard signals
  - use of multiple antennas
  - signal alignment

Fading Wiretap Channel

- In the Gaussian wiretap channel, secrecy is not possible if

$$C_B \leq C_E$$

- Fading provides time-diversity: Can it be used to obtain/improve secrecy?

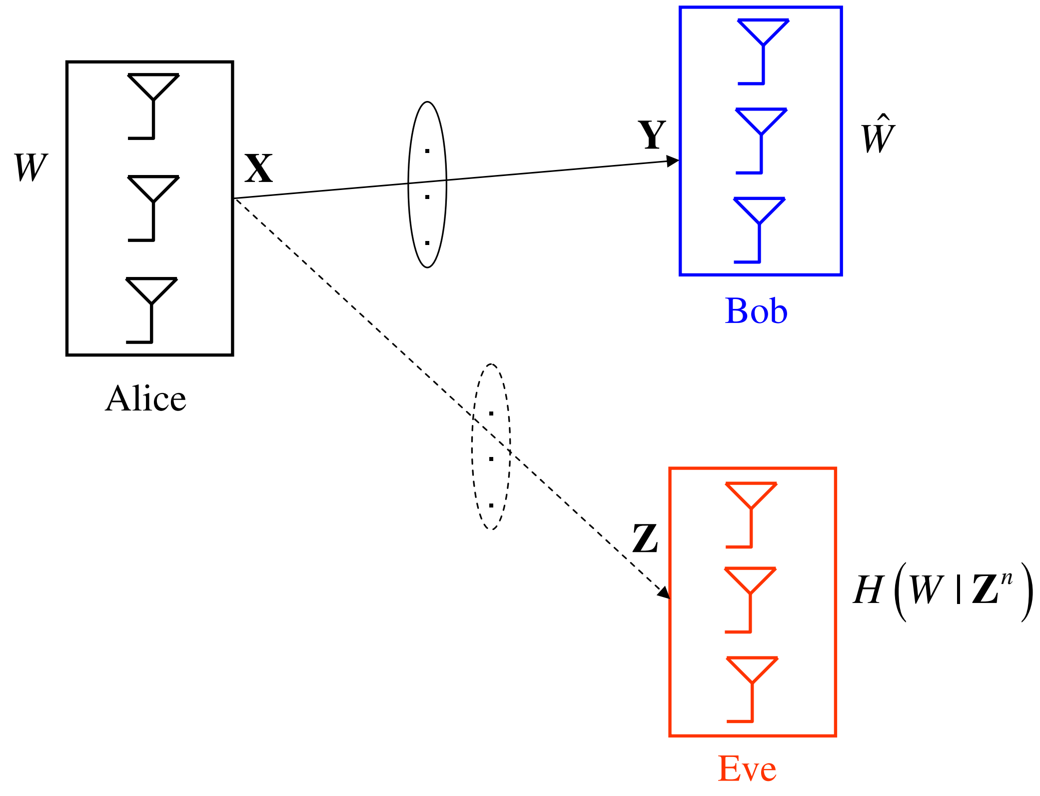


MIMO Wiretap Channel

- In SISO Gaussian wiretap channel, secrecy is not possible if

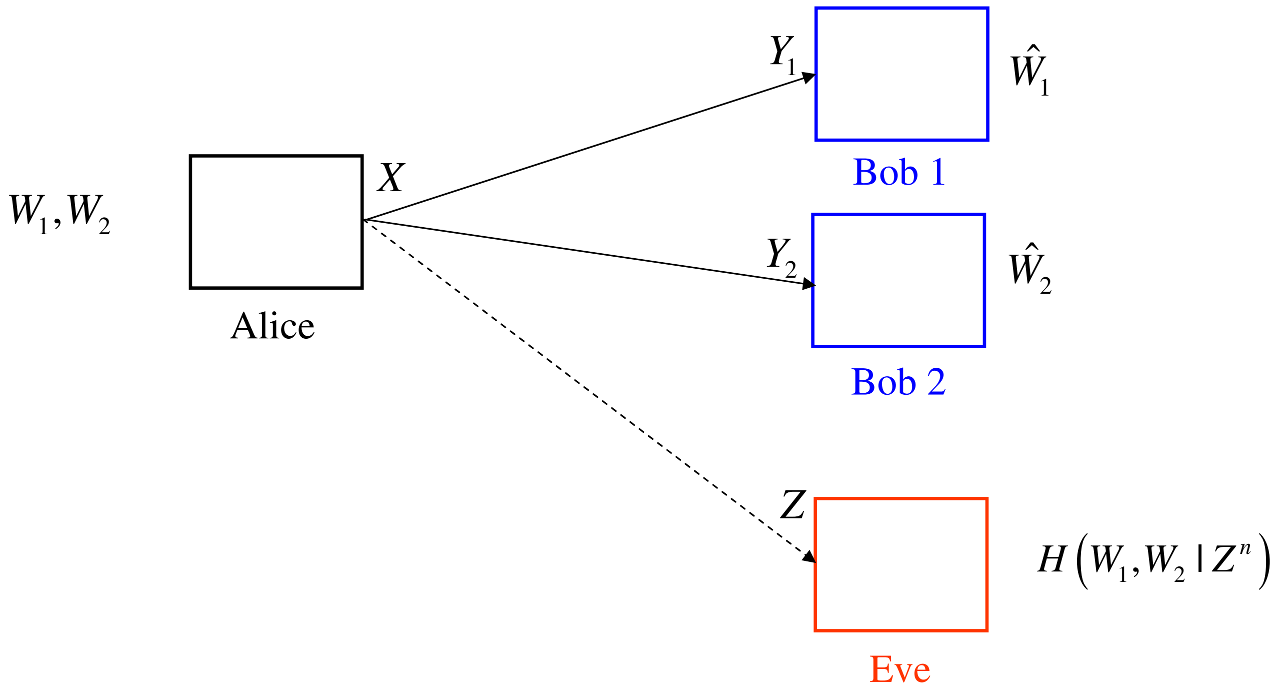
$$C_B \leq C_E$$

- Multiple antennas improve reliability and rates. How about secrecy?



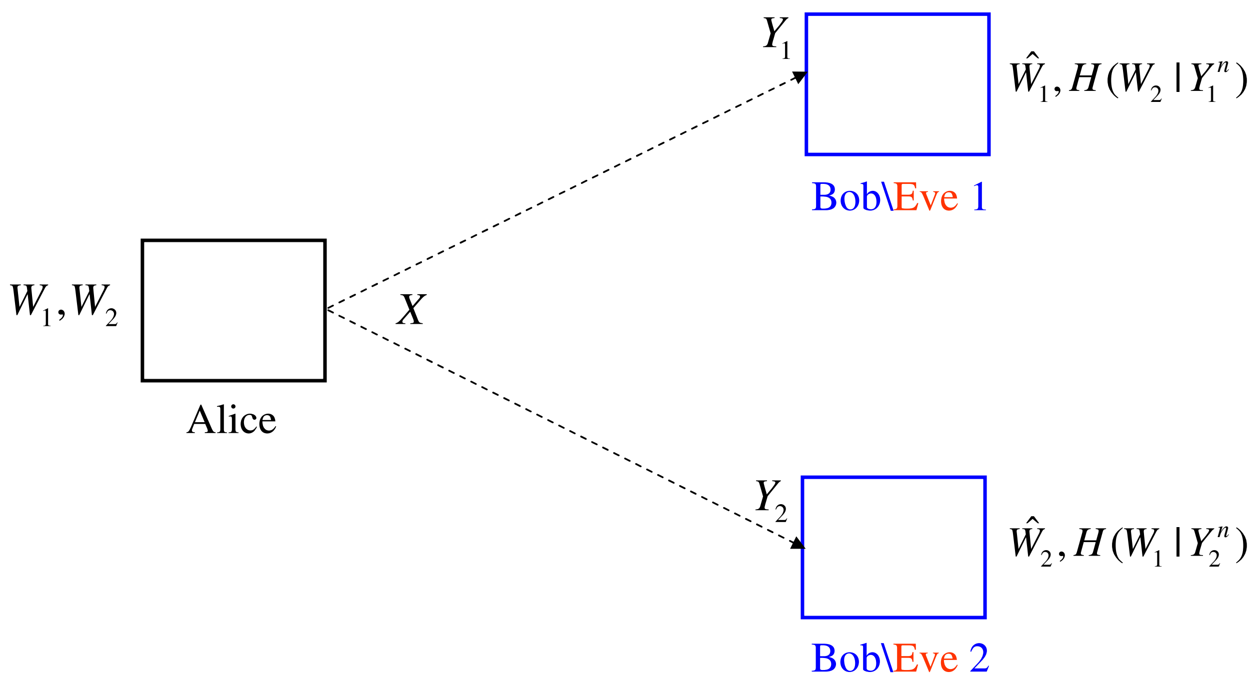
Broadcast (Downlink) Channel

- In cellular communications: base station to end-users channel can be eavesdropped.
- This channel can be modelled as a broadcast channel with an external eavesdropper.



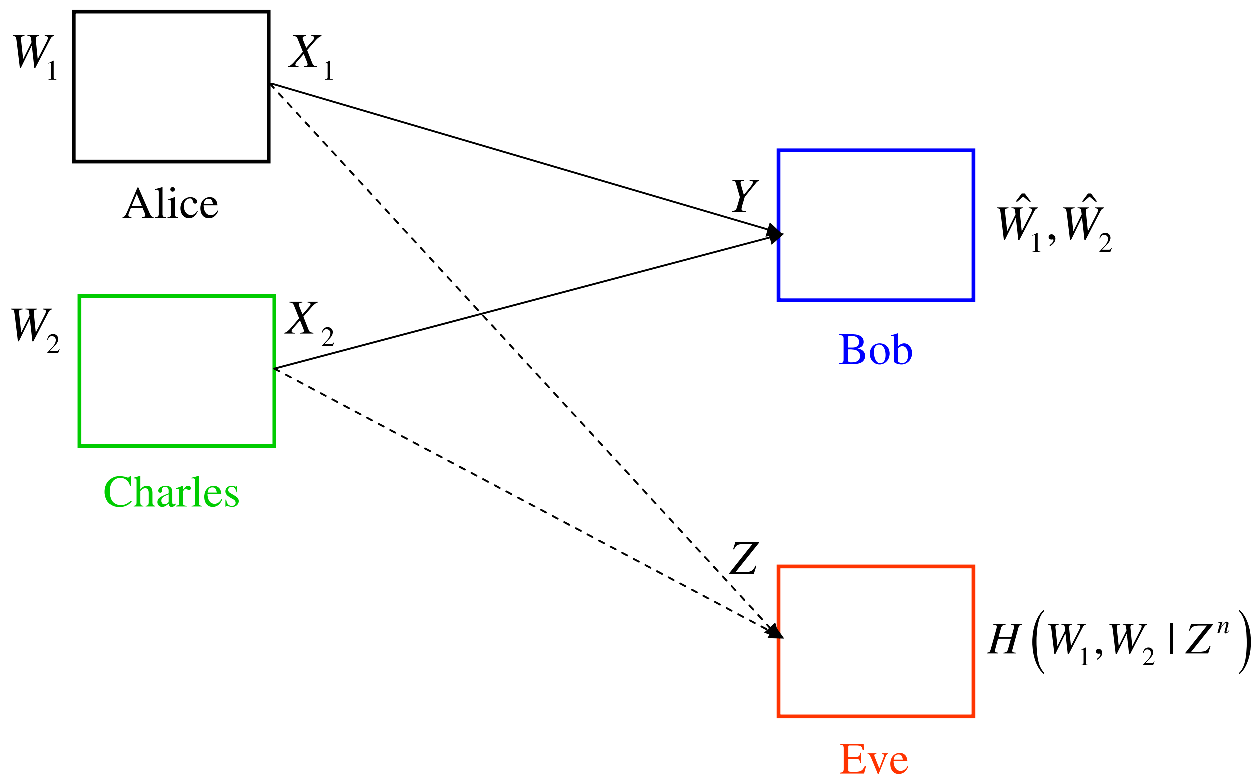
Internal Security within a System

- Legitimate users may have different security clearances.
- Some legitimate users may have paid for some content, some may not have.
- Broadcast channel with two confidential messages.



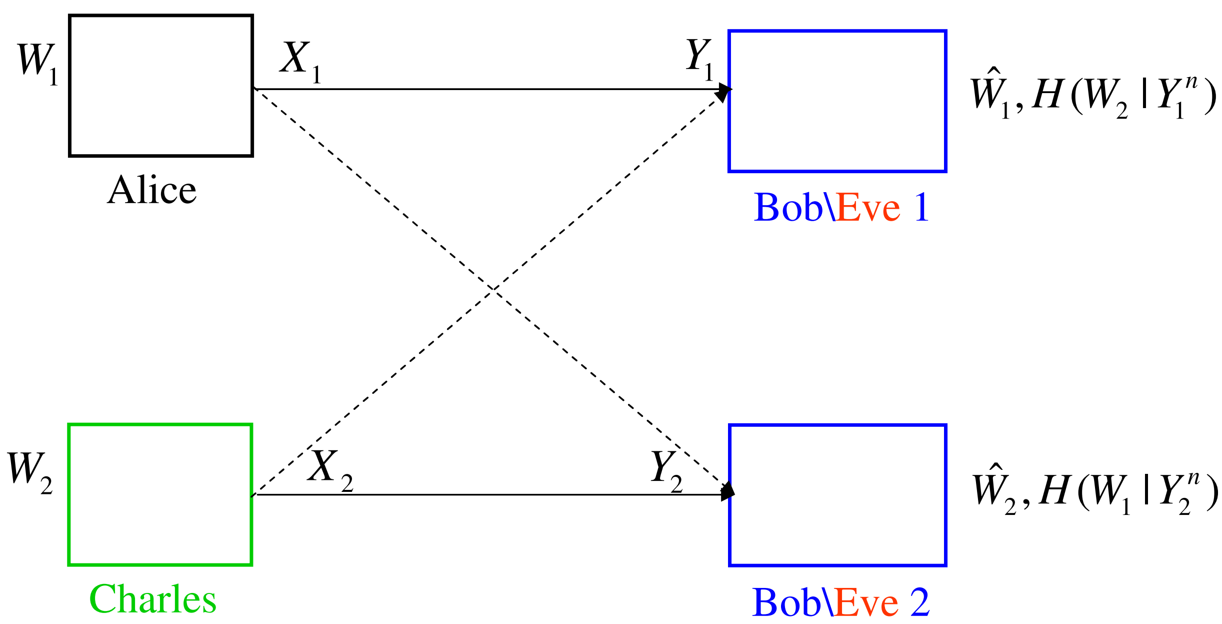
Multiple Access (Uplink) Channel

- In cellular communications: end-user to the base station channel can be eavesdropped.
- This channel can be modelled as a multiple access channel with an external eavesdropper.



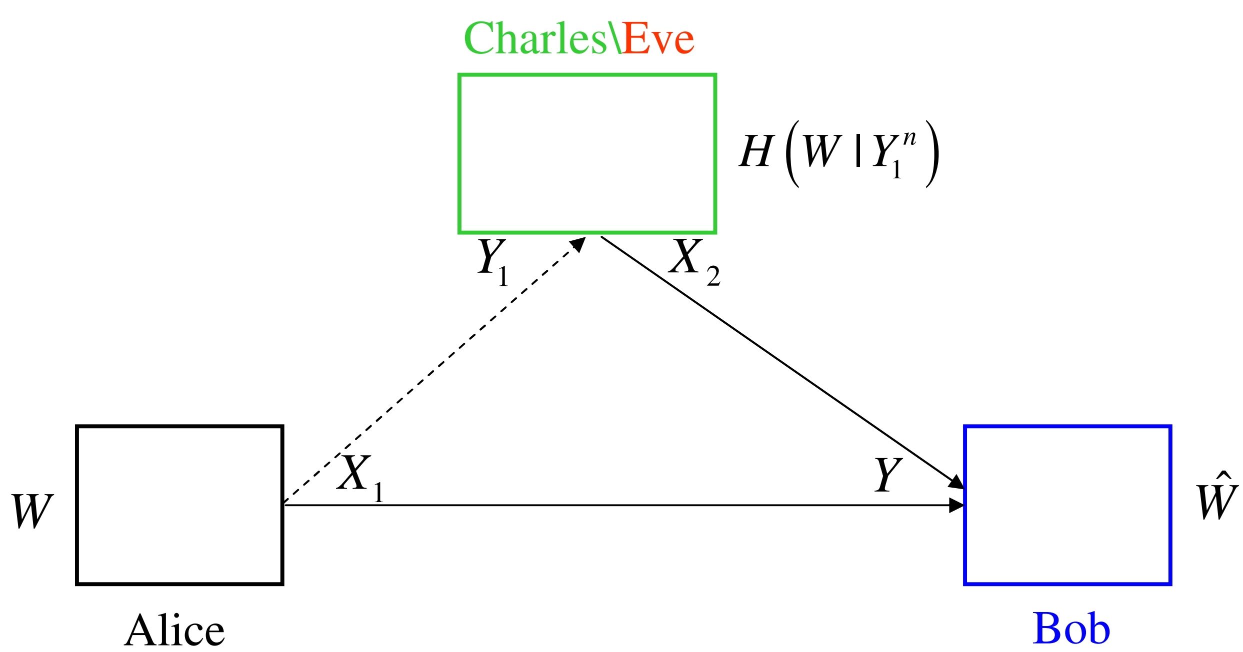
Interference as a Leakage of Information

- Interference is common in wireless communications:
  - Results in performance degradation, requires sophisticated transceiver design.
- From a secrecy point of view, results in the loss of confidentiality.
- Interference channel with confidential messages.



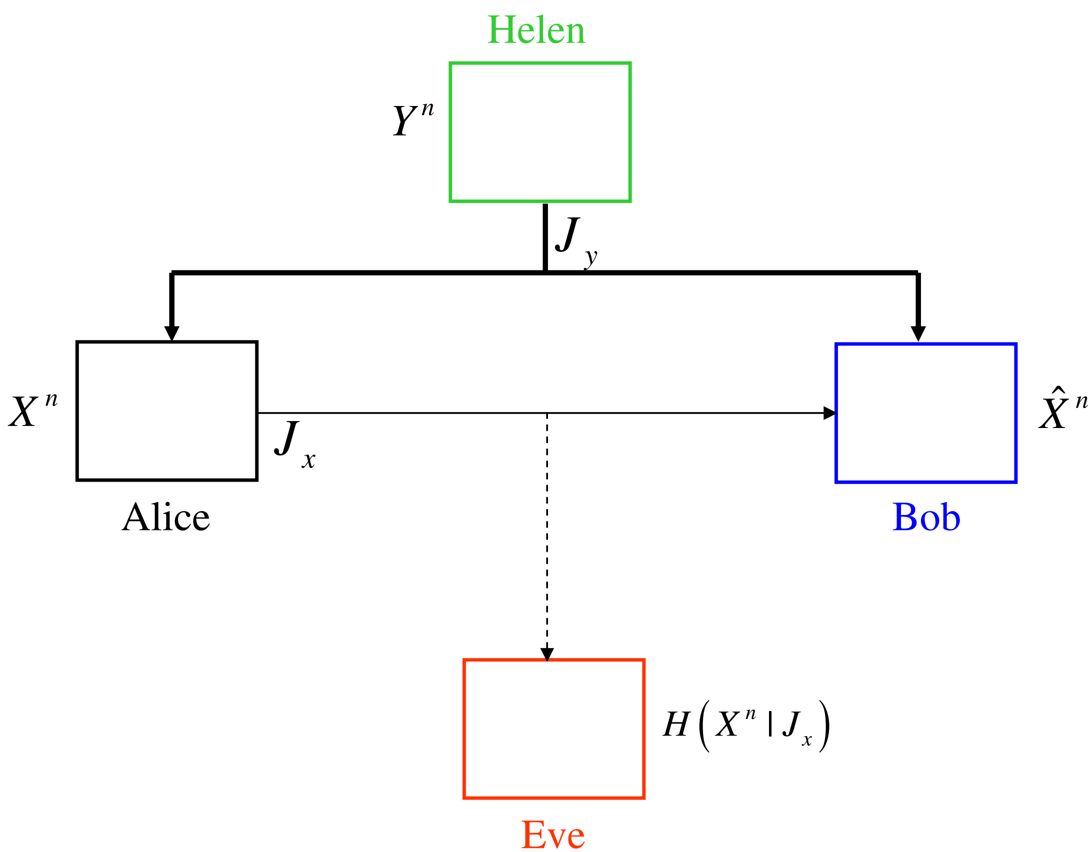
Cooperative Channels

- **Overheard information** at communicating parties:
  - Forms the basis for cooperation
  - Results in loss of confidentiality
- How do cooperation and secrecy interact?
- Simplest model to investigate this interaction: relay channel with secrecy constraints.
  - Can Charles help without learning the messages going to Bob?



Secure Distributed Source Coding: Wireless Sensor Networks

- There is an underlying random process which needs to be constructed at a central node.
- Sensors get **correlated** observations.
- Some sensors might be untrusted or even malicious, while some sensors might be helpful.
- This scenario can be modelled as a source coding problem with secrecy concerns.



Relevant (Potentially Incomplete) Literature

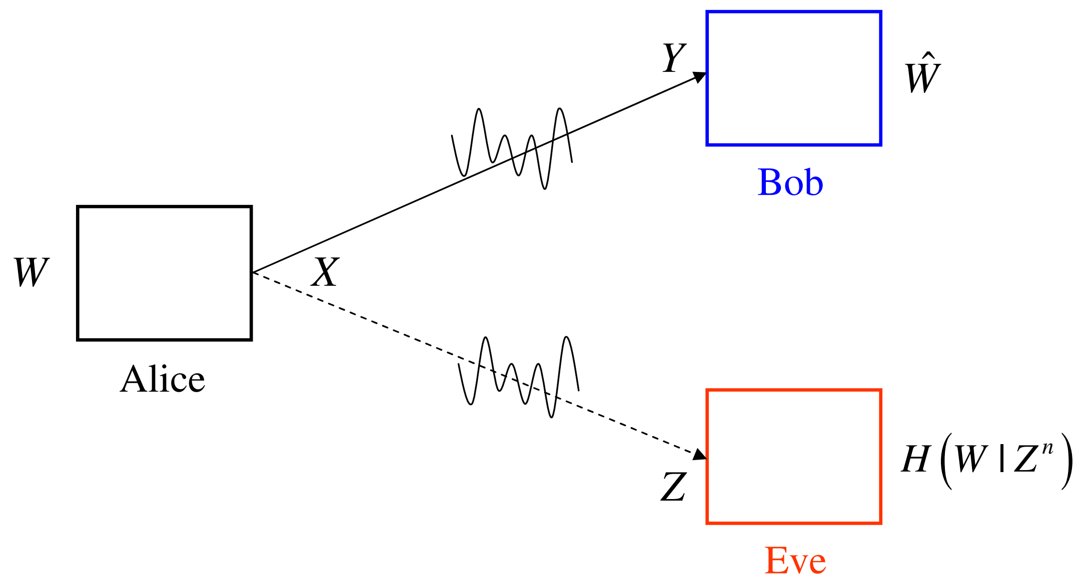
- Fading wiretap channel: Liang-Poor-Shamai, Li-Yates-Trappe, Gopala-Lai-El Gamal, Khisti-Tchamkerten-Wornell, Bloch-Barros-Rogrigues-McLaughlin, Parada-Blahut, Ekrem-Ulukus.
- Gaussian MIMO wiretap channel: Parada-Blahut, Negi-Goel, Shafiee-Ulukus, Li-Trappe-Yates, Khisti-Wornell-Wiesel-Eldar, Shafiee-Liu-Ulukus, Khisti-Wornell, Oggier-Hassibi, Liu-Shamai.
- Broadcast channels with confidential messages: Liu-Maric-Spasojevic-Yates, Liu-Liu-Poor-Shamai, Bagherikaram-Motahari-Khandani, Ekrem-Ulukus, Liu-Liu-Poor-Shamai, Kang-Liu.
- Multiple access channel with a wiretapper: Tekin-Yener, Ekrem-Ulukus, Bassily-Ulukus, He-Yener, Simeone-Yener.
- Interference channel with confidential messages: Liu-Maric-Spasojevic-Yates, Ekrem-Ulukus, Li-Yates-Trappe, Yates-Tse-Li, Koyluoglu-El Gamal-Lai-Poor, He-Yener.
- Interaction of cooperation and secrecy: Oohama, He-Yener, Yuksel-Erkip, Ekrem-Ulukus, Tang-Liu-Spasojevic-Yates, He-Yener, Lai-El Gamal.
- Source coding with secrecy concerns: Yamamoto, Hayashi-Yamamoto, Grokop-Sahai-Gastpar, Prabhakaran-Ramchandran, Luh-Kundur, Gunduz-Erkip-Poor, Prabhakaran-Eswaran-Ramchandran, Tandon-Ulukus-Ramchandran.

Fading Wiretap Channel-I

- In the Gaussian wiretap channel, secrecy is not possible if

$$C_B \leq C_E$$

- Fading provides a time-diversity: It can be used to obtain/improve secrecy.



- Two scenarios for the ergodic secrecy capacity:
  - CSIT of both Bob and Eve: Liang-Poor-Shamai, Li-Yates-Trappe, Gopala-Lai-El Gamal.
  - CSIT of Bob only: Khisti-Tchamkerten-Wornell, Li-Yates-Trappe, Gopala-Lai-El Gamal.

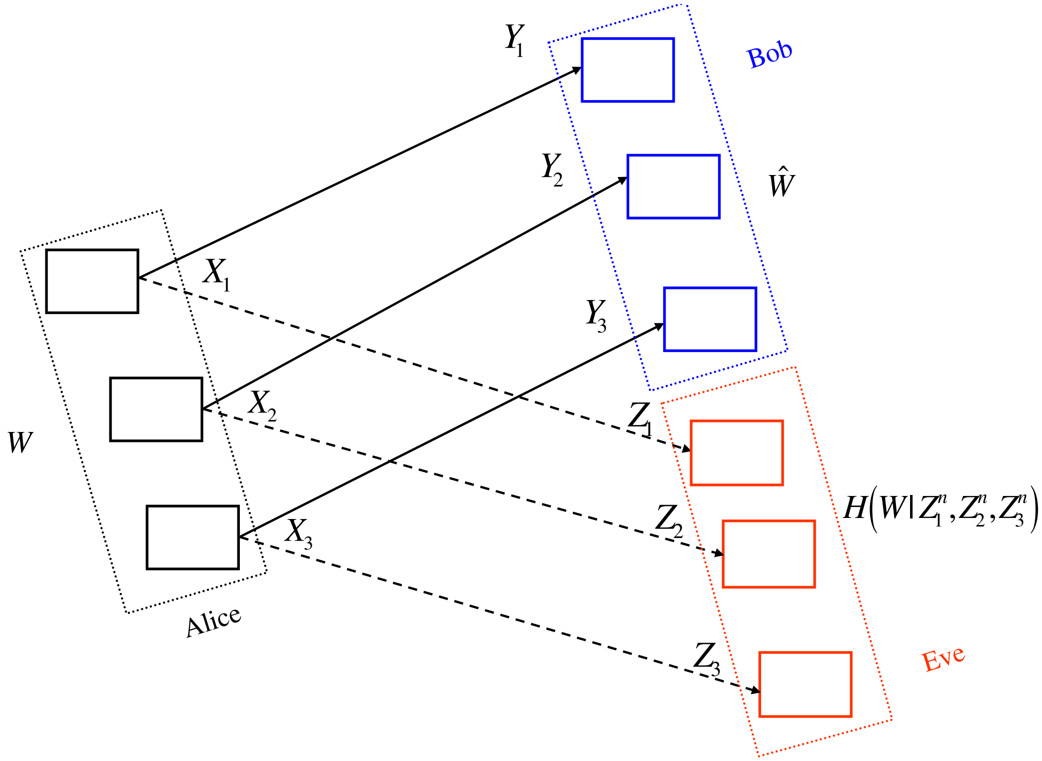
Fading (i.e., Parallel) Wiretap Channel-II

- Fading channel model:

$$Y = h_Y X + N_Y$$

$$Z = h_Z X + N_Z$$

- Assume full CSIT and CSIR.
- Parallel wiretap channel provides the framework to analyze the fading wiretap channel



Fading Wiretap Channel-III

- Secrecy capacity of the parallel wiretap channel can be obtained as follows [Liang-Poor-Shamai, 2008]

$$
\begin{aligned}
C_s &= \max_{V \to X^L \to (Y^L, Z^L)} \quad I(V; Y_1, \ldots, Y_L) - I(V; Z_1, \ldots, Z_L) \\
&= \max_{V \to X^L \to (Y^L, Z^L)} \quad \sum_{l=1}^{L} I(V; Y_l | Y^{l-1}) - I(V; Z_l | Z_{l+1}^L) \\
&= \max_{V \to X^L \to (Y^L, Z^L)} \quad \sum_{l=1}^{L} I(V, Z_{l+1}^L; Y_l | Y^{l-1}) - I(V, Y^{l-1}; Z_l | Z_{l+1}^L) + \underline{I(Z_{l+1}^L; Y_l | Y^{l-1}, V)} \\
&\qquad - \underline{I(Y^{l-1}; Z_l | Z_{l+1}^L, V)} \\
&= \max_{V \to X^L \to (Y^L, Z^L)} \quad \sum_{l=1}^{L} I(V, Z_{l+1}^L; Y_l | Y^{l-1}) - I(V, Y^{l-1}; Z_l | Z_{l+1}^L)
\end{aligned}
$$

where underlined terms are identical due to Csiszar sum lemma.

Fading Wiretap Channel-IV

$$
\begin{aligned}
C_s &= \max_{V \to X^L \to (Y^L, Z^L)} \sum_{l=1}^{L} I(V, Z_{l+1}^L; Y_l | Y^{l-1}) - I(V, Y^{l-1}; Z_l | Z_{l+1}^L) \\
&= \max_{V \to X^L \to (Y^L, Z^L)} \sum_{l=1}^{L} I(V; Y_l | Y^{l-1}, Z_{l+1}^L) - I(V; Z_l | Z_{l+1}^L, Y^{l-1}) + \underline{I(Z_{l+1}^L; Y_l | Y^{l-1})} - \underline{I(Y^{l-1}; Z_l | Z_{l+1}^L)} \\
&= \max_{V \to X^L \to (Y^L, Z^L)} \sum_{l=1}^{L} I(V; Y_l | Y^{l-1}, Z_{l+1}^L) - I(V; Z_l | Z_{l+1}^L, Y^{l-1}) \\
&= \max_{V \to X^L \to (Y^L, Z^L)} \sum_{l=1}^{L} I(V, Y^{l-1}, Z_{l+1}^L; Y_l | Y^{l-1}, Z_{l+1}^L) - I(V, Y^{l-1}, Z_{l+1}^L; Z_l | Z_{l+1}^L, Y^{l-1}) \\
&= \max_{\{Q_l \to V_l \to X_l \to (Y_l, Z_l)\}_{l=1}^L} \sum_{l=1}^{L} I(V_l; Y_l | Q_l) - I(V_l; Z_l | Q_l) \\
&= \sum_{l=1}^{L} \max_{Q_l \to V_l \to X_l \to (Y_l, Z_l)} I(V_l; Y_l | Q_l) - I(V_l; Z_l | Q_l) \\
&= \sum_{l=1}^{L} \max_{V_l \to X_l \to (Y_l, Z_l)} I(V_l; Y_l) - I(V_l; Z_l) \qquad \left(= \sum_{l=1}^{L} C_{sl} \right)
\end{aligned}
$$

Fading Wiretap Channel-V

- Each realization of (h_Y, h_Z) can be viewed as a sub-channel occurring with some probability
- Averaging over all possible channel realizations gives the ergodic secrecy capacity

$$C_s = \max \; E\left[\frac{1}{2}\log\left(1+\frac{h_Y^2 P(h_Y,h_Z)}{\sigma_Y^2}\right) - \frac{1}{2}\log\left(1+\frac{h_Z^2 P(h_Y,h_Z)}{\sigma_Z^2}\right)\right]$$

where the maximization is over all power allocation schemes $P(h_Y, h_Z)$ satisfying constraint

$$E\left[P(h_Y,h_Z)\right] \le P$$

- If $\frac{h_Y^2}{\sigma_Y^2} \le \frac{h_Z^2}{\sigma_Z^2}$, term inside the expectation is negative:

$$P(h_Y,h_Z) = 0 \quad \text{if} \;\; \frac{h_Y^2}{\sigma_Y^2} \le \frac{h_Z^2}{\sigma_Z^2}$$

- Optimal power allocation is water-filling over the states (h_Y, h_Z) satisfying

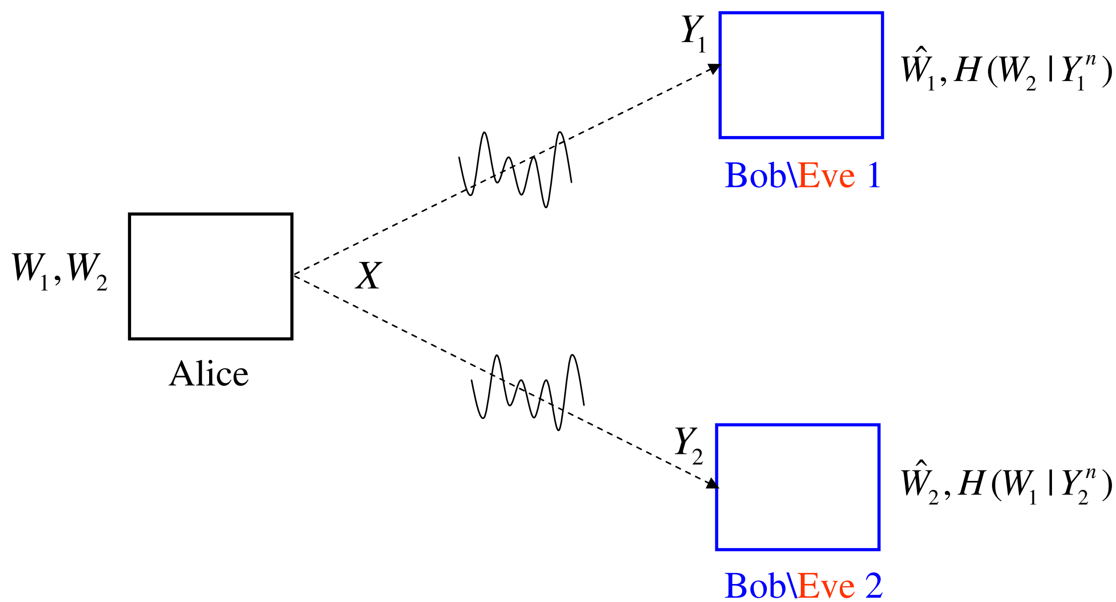
$$\frac{h_Y^2}{\sigma_Y^2} \ge \frac{h_Z^2}{\sigma_Z^2}$$

Fading Broadcast Channel with Confidential Messages-I

- The symmetric case, i.e., both users want secrecy against each other [Ekrem-Ulukus].
- In a non-fading setting, only one user can have a positive secure rate.
- Fading channel model:

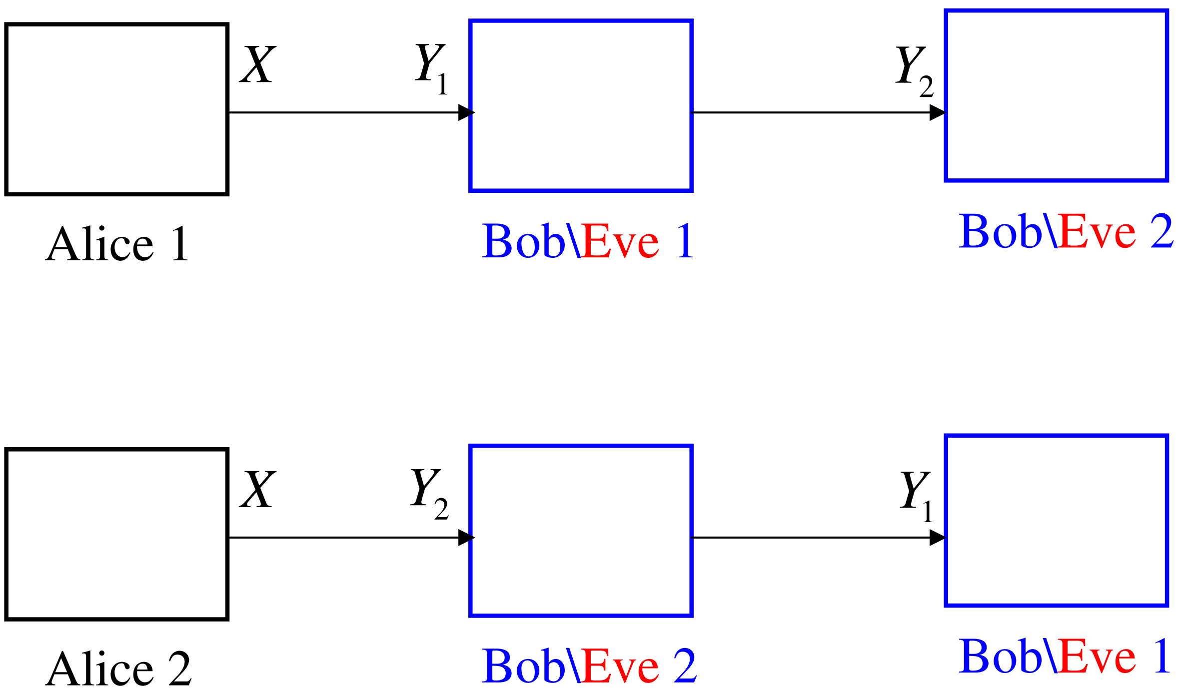
$$Y_1 = h_1 X + N_1$$
$$Y_2 = h_2 X + N_2$$

- Assume full CSIT and CSIR.



Fading Broadcast Channel with Confidential Messages-II

- Similar to previous case, parallel broadcast channel provides the framework
- Parallel broadcast channel with degraded sub-channels
  - In each sub-channel, one user is degraded wrt the other user



Fading Broadcast Channel with Confidential Messages-III

- The secrecy capacity region is given by the union of rate pairs (R_1, R_2) satisfying

$$R_1 \leq \sum_{l \in \mathcal{S}_1} I(X_l; Y_{1l}) - I(X_l; Y_{2l})$$
$$R_2 \leq \sum_{l \in \mathcal{S}_2} I(X_l; Y_{2l}) - I(X_l; Y_{1l})$$

where $\mathcal{S}_1, \mathcal{S}_2$ are

$$\mathcal{S}_1 = \{l : X_l \rightarrow Y_{1l} \rightarrow Y_{2l}\}$$
$$\mathcal{S}_2 = \{l : X_l \rightarrow Y_{2l} \rightarrow Y_{1l}\}$$

- Using the parallel channel model, the ergodic secrecy capacity region of the fading model can be obtained

Fading Broadcast Channel with Confidential Messages-IV

- The ergodic secrecy capacity region is given by the union of rate pairs (R_1, R_2) satisfying

$$R_1 \leq \frac{1}{2} \int_{\mathcal{H}_1} \left[\log(1+\alpha_1(\mathbf{h})h_1^2) - \log(1+\alpha_1(\mathbf{h})h_2^2 \right] dF(\mathbf{H})$$
$$R_2 \leq \frac{1}{2} \int_{\mathcal{H}_2} \left[\log(1+\alpha_2(\mathbf{h})h_2^2) - \log(1+\alpha_2(\mathbf{h})h_1^2 \right] dF(\mathbf{H})$$

where $\mathcal{H}_1, \mathcal{H}_2$ are

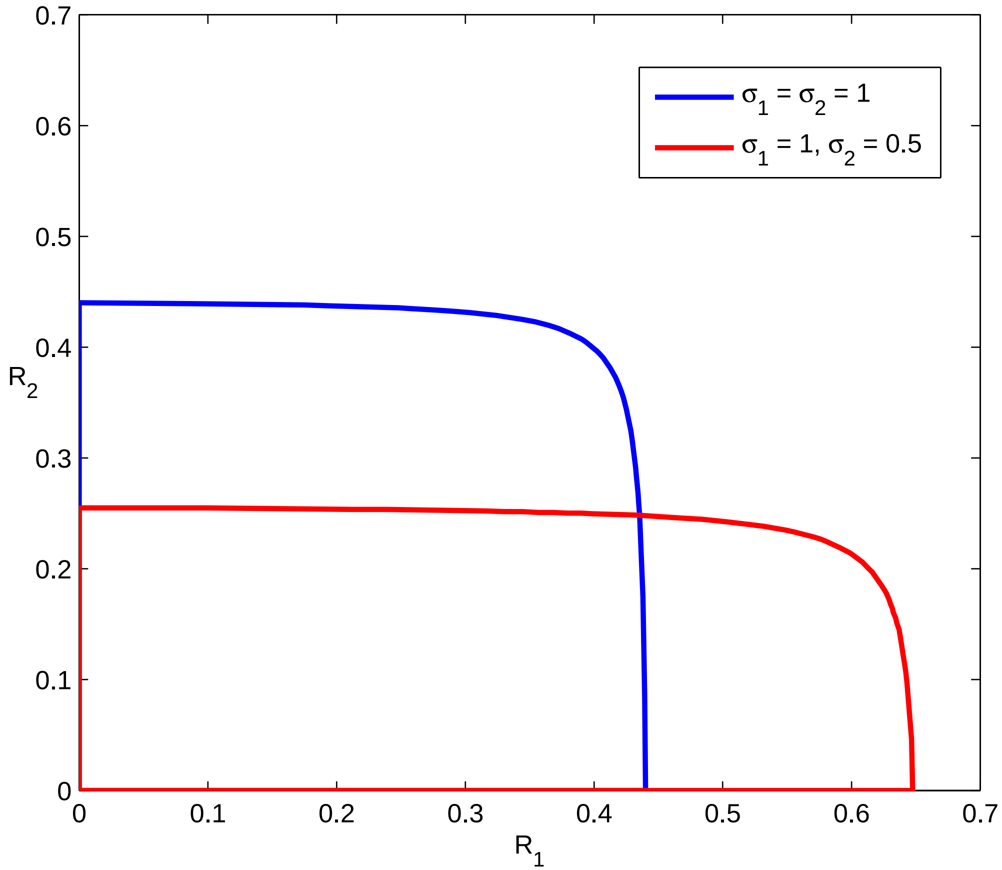
$$\mathcal{H}_1 = \{\mathbf{h} : h_1 > h_2\} \qquad \mathcal{H}_2 = \{\mathbf{h} : h_1 < h_2\}$$

$\alpha_1(\mathbf{h})$ and $\alpha_2(\mathbf{h})$ are the power allocations satisfying

$$\int_{\mathcal{H}_1} \alpha_1(\mathbf{h}) dF(\mathbf{h}) + \int_{\mathcal{H}_2} \alpha_2(\mathbf{h}) dF(\mathbf{h}) \leq P$$

The Secrecy Capacity Region

- h_1^2, h_2^2 are exponential random variables with means σ_1, σ_2, respectively.



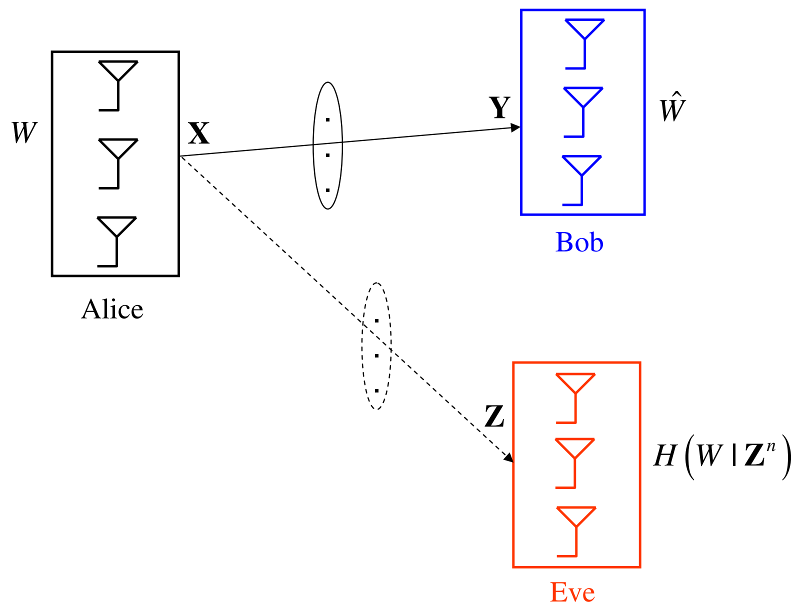
- Fading (channel variation over time) is beneficial for secrecy.
- Both users can have positive secrecy rates in fading. This is not possible without fading.

Gaussian MIMO Wiretap Channel-I

- Gaussian MIMO wiretap channel:

$$\mathbf{Y} = \mathbf{H}_Y \mathbf{X} + \mathbf{N}_Y$$

$$\mathbf{Z} = \mathbf{H}_Z \mathbf{X} + \mathbf{N}_Z$$



- As opposed to the SISO case, MIMO channel is not necessarily degraded

Gaussian MIMO Wiretap Channel-II

- Secrecy capacity [Shafiee-Liu-Ulukus, Khisti-Wornell, Oggier-Hassibi, Liu-Shamai]:

$$C_S = \max_{V \to \mathbf{X} \to \mathbf{Y},\mathbf{Z}} I(V;\mathbf{Y}) - I(V;\mathbf{Z})$$
$$= \max_{\mathbf{K}:\mathrm{tr}(\mathbf{K}) \le P} \frac{1}{2}\log\left|\mathbf{H}_M\mathbf{K}\mathbf{H}_M^\top + \mathbf{I}\right| - \frac{1}{2}\log\left|\mathbf{H}_E\mathbf{K}\mathbf{H}_E^\top + \mathbf{I}\right|$$

- No channel prefixing is necessary and Gaussian signalling is optimal.
- As opposed to the SISO case, $C_S \neq C_B - C_E$.
- Multiple antennas improve reliability and rates. They improve secrecy as well.

Gaussian MIMO Wiretap Channel – Finding the Capacity

- Secrecy capacity of any wiretap channel is known as an optimization problem:

$$C_s = \max_{(V,\mathbf{X})} I(V;\mathbf{Y}) - I(V;\mathbf{Z})$$

- MIMO wiretap channel is not degraded in general.
  - Therefore, $V = \mathbf{X}$ is potentially suboptimal.
- There is no general methodology to solve this optimization problem, i.e., find optimal $(V,\mathbf{X})$.
- The approach used by [Shafiee-Liu-Ulukus, Khisti-Wornell, Oggier-Hassibi]:
  - Compute an achievable secrecy rate by using a potentially suboptimal $(V,\mathbf{X})$:
    - $*$ Jointly Gaussian $(V,\mathbf{X})$ is a natural candidate.
  - Find a computable outer bound.
  - Show that these two expressions (achievable rate and outer bound) match.

Gaussian MIMO Wiretap Channel – Finding the Capacity (Outer Bound)

- Using Sato's approach, a computable outer bound can be found:
  - Consider the enhanced Bob with observation $\tilde{\mathbf{Y}} = (\mathbf{Y}, \mathbf{Z})$
  - This new channel is degraded, no need for channel prefixing:

$$\max_{\mathbf{X}} I(\mathbf{X}; \tilde{\mathbf{Y}}) - I(\mathbf{X}; \mathbf{Z}) = \max_{\mathbf{X}} I(\mathbf{X}; \mathbf{Y} | \mathbf{Z})$$

  - And, optimal $\mathbf{X}$ is Gaussian.

- This outer bound can be tightened:
  - The secrecy capacity is the same for channels having the same marginal distributions
  - We can correlate the receiver noises.

- The tightened outer bound is:

$$\min \ \max_{\mathbf{X}} I(\mathbf{X}; \mathbf{Y} | \mathbf{Z})$$

  where the minimization is over all noise correlations.

- The outer bound so developed matches the achievable rate.

Insights from the Outer Bound

- Sato-type outer bound is tight
- This outer bound constructs a degraded wiretap channel from the original non-degraded one
- Secrecy capacity of the constructed degraded channel is potentially larger than the original non-degraded one
- However, they turn out to be the same
- Indeed, these observations are a manifestation of channel enhancement:
  - Liu-Shamai provide an alternative proof for secrecy capacity via channel enhancement

Secrecy Capacity via Channel Enhancement

- Aligned Gaussian MIMO wiretap channel

$$\mathbf{Y} = \mathbf{X} + \mathbf{N}_Y$$
$$\mathbf{Z} = \mathbf{X} + \mathbf{N}_Z$$

  where $\mathbf{N}_Y \sim \mathcal{N}(\mathbf{0}, \mathbf{\Sigma}_Y)$, $\mathbf{N}_Z \sim \mathcal{N}(\mathbf{0}, \mathbf{\Sigma}_Z)$.

- Channel input $\mathbf{X}$ is subject to a covariance constraint

$$E\left[\mathbf{X}\mathbf{X}^\top\right] \preceq \mathbf{S}$$

- Covariance constraint has advantages
  - A rather general constraint including total power and per-antenna power constraints as special cases
  - Yields an easier analysis

Secrecy Capacity of Degraded Gaussian MIMO Wiretap Channel

- Channel is degraded if it satisfies

$$\mathbf{X} \rightarrow \mathbf{Y} \rightarrow \mathbf{Z}$$

  which is equivalent to have $\mathbf{\Sigma}_Y \preceq \mathbf{\Sigma}_Z$

- In other words, we have $\mathbf{N}_Z = \mathbf{N}_Y + \tilde{\mathbf{N}}$ where $\tilde{\mathbf{N}}$ is Gaussian with covariance matrix $\mathbf{\Sigma}_Z - \mathbf{\Sigma}_Y$
- Corresponding secrecy capacity

$$\begin{aligned}
C_s &= \max_{p(\mathbf{x})} I(\mathbf{X};\mathbf{Y}) - I(\mathbf{X};\mathbf{Z}) \\
&= \max_{p(\mathbf{x})} h(\mathbf{Y}) - h(\mathbf{Z}) - \frac{1}{2}\log\frac{|\mathbf{\Sigma}_Y|}{|\mathbf{\Sigma}_Z|} \\
&= \max_{p(\mathbf{x})} h(\mathbf{Y}) - h(\mathbf{Y}+\tilde{\mathbf{N}}) - \frac{1}{2}\log\frac{|\mathbf{\Sigma}_Y|}{|\mathbf{\Sigma}_Z|} \\
&= \max_{p(\mathbf{x})} -I(\tilde{\mathbf{N}};\mathbf{Y}+\tilde{\mathbf{N}}) - \frac{1}{2}\log\frac{|\mathbf{\Sigma}_Y|}{|\mathbf{\Sigma}_Z|} \\
&= \max_{\mathbf{0}\preceq\mathbf{K}\preceq\mathbf{S}} \frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_Y|}{|\mathbf{K}+\mathbf{\Sigma}_Z|} - \frac{1}{2}\log\frac{|\mathbf{\Sigma}_Y|}{|\mathbf{\Sigma}_Z|} \\
&= \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Y|}{|\mathbf{\Sigma}_Y|} - \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|}
\end{aligned}$$

Secrecy Capacity via Channel Enhancement-I

- The following secrecy rate is achievable

$$C_s \geq \max_{\mathbf{0} \preceq \mathbf{K} \preceq \mathbf{S}} \quad \frac{1}{2} \log \frac{|\mathbf{K} + \mathbf{\Sigma}_Y|}{|\mathbf{\Sigma}_Y|} - \frac{1}{2} \log \frac{|\mathbf{K} + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|}$$

- Optimal covariance matrix $\mathbf{K}^*$ needs to satisfy

$$(\mathbf{K}^* + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M} = (\mathbf{K}^* + \mathbf{\Sigma}_Z)^{-1} + \mathbf{M}_S$$

$$\mathbf{K}^* \mathbf{M} = \mathbf{M} \mathbf{K}^* = \mathbf{0}$$

$$(\mathbf{S} - \mathbf{K}^*) \mathbf{M}_S = \mathbf{M}_S (\mathbf{S} - \mathbf{K}^*) = \mathbf{0}$$

- We enhance the legitimate user as follows

$$\left(\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Y\right)^{-1} = (\mathbf{K}^* + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M}$$

  which also implies

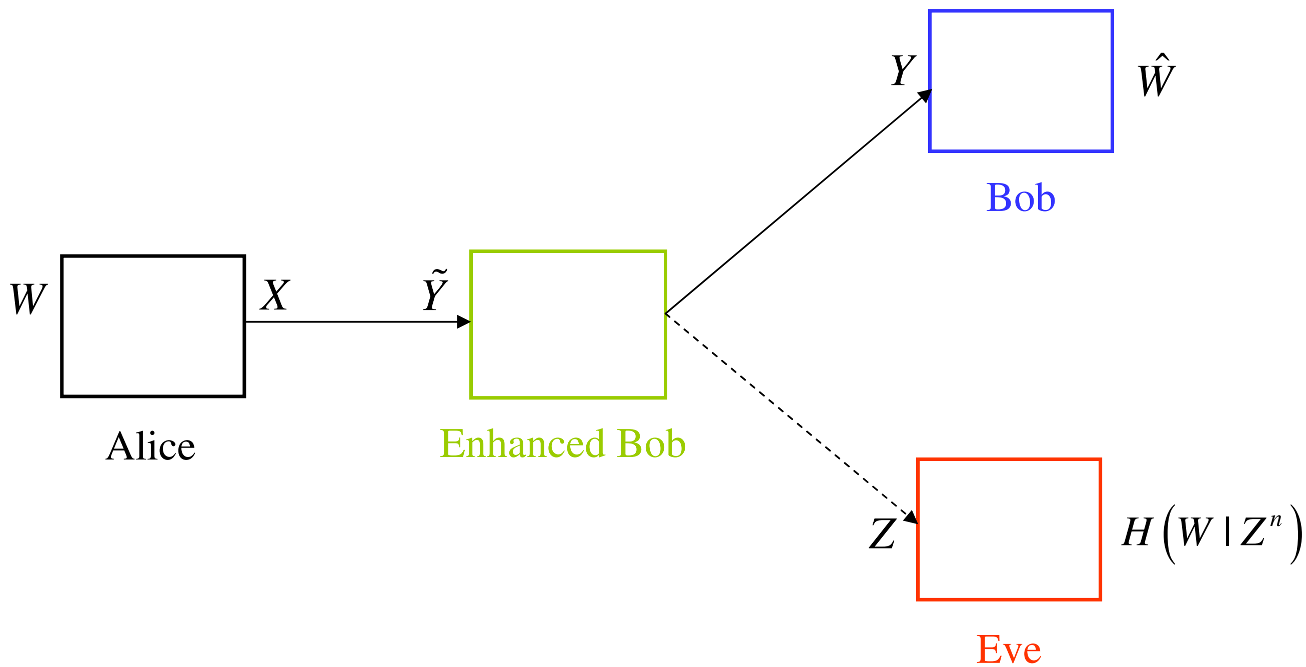
$$\left(\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Y\right)^{-1} = (\mathbf{K}^* + \mathbf{\Sigma}_Z)^{-1} + \mathbf{M}_S$$

- Thus, $\tilde{\mathbf{\Sigma}}_Y$ satisfies

$$\tilde{\mathbf{\Sigma}}_Y \preceq \mathbf{\Sigma}_Y \quad \text{and} \quad \tilde{\mathbf{\Sigma}}_Y \preceq \mathbf{\Sigma}_Z$$

Secrecy Capacity via Channel Enhancement-II

- Enhanced channel:



Secrecy Capacity via Channel Enhancement-III

- Enhanced wiretap channel

$$\tilde{\mathbf{Y}} = \mathbf{X} + \tilde{\mathbf{N}}_Y$$
$$\mathbf{Z} = \mathbf{X} + \mathbf{N}_Z$$

where $\tilde{\mathbf{N}}_Y \sim \mathcal{N}(\mathbf{0}, \tilde{\mathbf{\Sigma}}_Y)$.

- Since $\tilde{\mathbf{\Sigma}}_Y \preceq \{\mathbf{\Sigma}_Y, \mathbf{\Sigma}_Z\}$, we have

$$\mathbf{X} \rightarrow \tilde{\mathbf{Y}} \rightarrow \{\mathbf{Y}, \mathbf{Z}\}$$

- Thus, the enhanced channel is degraded and $\tilde{C}_s \geq C_s$

$$\tilde{C}_s = \frac{1}{2} \log \frac{|\mathbf{S} + \tilde{\mathbf{\Sigma}}_Y|}{|\tilde{\mathbf{\Sigma}}_Y|} - \frac{1}{2} \log \frac{|\mathbf{S} + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|}$$

Secrecy Capacity via Channel Enhancement-IV

- Although secrecy capacity is potentially improved through the enhancement, indeed, there is a rate preservation

$$(\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Y)^{-1}(\mathbf{S} + \tilde{\mathbf{\Sigma}}_Y) = (\mathbf{K}^* + \mathbf{\Sigma}_Z)^{-1}(\mathbf{S} + \mathbf{\Sigma}_Z)$$
$$(\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Y)^{-1}\tilde{\mathbf{\Sigma}}_Y = (\mathbf{K}^* + \mathbf{\Sigma}_Y)^{-1}\mathbf{\Sigma}_Y$$

- These identities imply

$$\begin{aligned}\frac{1}{2}\log\frac{|\mathbf{K}^* + \mathbf{\Sigma}_Y|}{|\mathbf{\Sigma}_Y|} - \frac{1}{2}\log\frac{|\mathbf{K}^* + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} &= \frac{1}{2}\log\frac{|\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Y|}{|\tilde{\mathbf{\Sigma}}_Y|} - \frac{1}{2}\log\frac{|\mathbf{K}^* + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \\ &= \frac{1}{2}\log\frac{|\mathbf{S} + \tilde{\mathbf{\Sigma}}_Y|}{|\tilde{\mathbf{\Sigma}}_Y|} - \frac{1}{2}\log\frac{|\mathbf{S} + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|}\end{aligned}$$

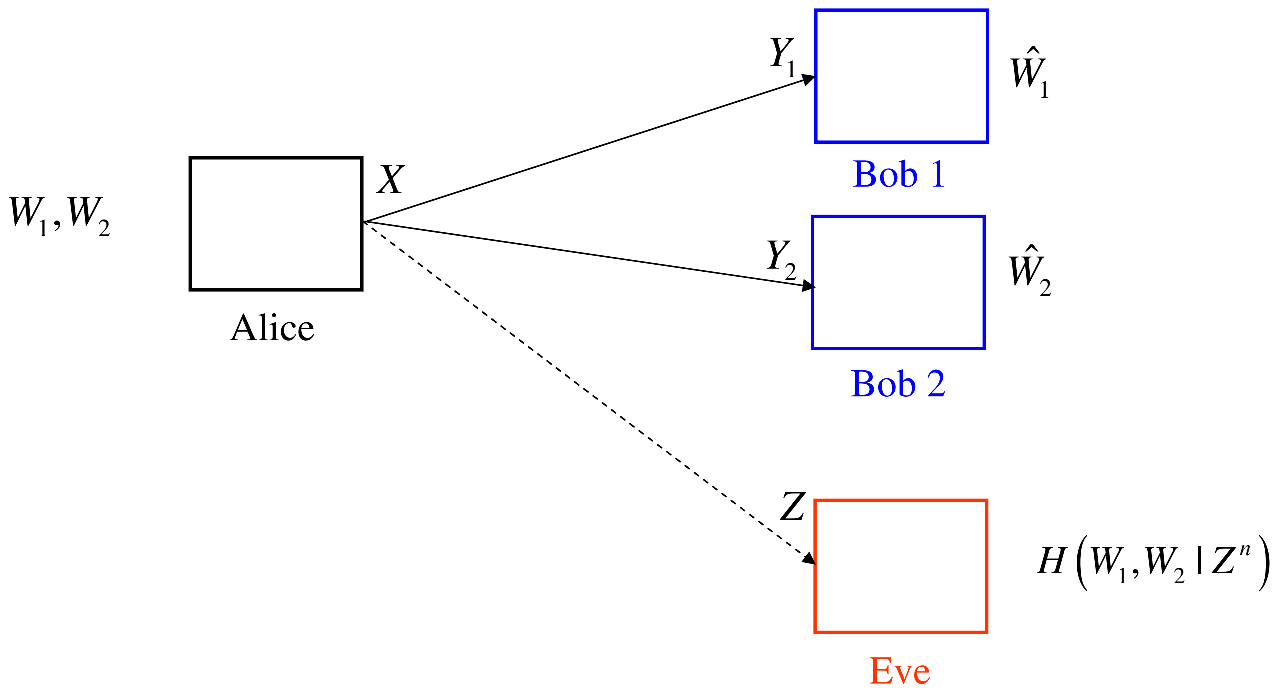
Secrecy Capacity via Channel Enhancement-V

- We can obtain the secrecy capacity of the original channel as follows [Liu-Shamai, 2009]

$$
\begin{aligned}
C_s &\leq \tilde{C}_s \\
&= \max_{\substack{\mathbf{X}\rightarrow\tilde{\mathbf{Y}},\mathbf{Z} \\ E\left[\mathbf{X}\mathbf{X}^\top\right]\preceq\mathbf{S}}} I(\mathbf{X};\tilde{\mathbf{Y}}) - I(\mathbf{X};\mathbf{Z}) \\
&= \frac{1}{2}\log\frac{|\mathbf{S}+\tilde{\mathbf{\Sigma}}_Y|}{|\tilde{\mathbf{\Sigma}}_Y|} - \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \\
&= \frac{1}{2}\log\frac{|\mathbf{K}^*+\tilde{\mathbf{\Sigma}}_Y|}{|\tilde{\mathbf{\Sigma}}_Y|} - \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \\
&= \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Y|}{|\mathbf{\Sigma}_Y|} - \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \\
&= \max_{\mathbf{0}\preceq\mathbf{K}\preceq\mathbf{S}} \frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_Y|}{|\mathbf{\Sigma}_Y|} - \frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|}
\end{aligned}
$$

Broadcast Channel with an External Eavesdropper-I

- In cellular communications: base station to end-users channel can be eavesdropped.
- This channel can be modelled as a broadcast channel with an external eavesdropper
- In general, the problem is intractable for now.
- Even an without eavesdropper, optimal transmission scheme is unknown.



Broadcast Channel with an External Eavesdropper-II

- The best known inner bound for broadcast channels is due to Marton:

$$R_1 \le I(V_1;Y_1)$$
$$R_2 \le I(V_2;Y_2)$$
$$R_1 + R_2 \le I(V_1;Y_1) + I(V_2;Y_2) - I(V_1;V_2)$$

for some V_1, V_2 satisfying $V_1, V_2 \to X \to Y_1, Y_2$.

- One corner point:

$$R_1' = I(V_1;Y_1)$$
$$R_2' = I(V_2;Y_2) - I(V_2;V_1)$$

- Encode W_1 by using V_1^n
- V_1^n is a non-causally known interference for the second user: Gelfand-Pinsker setting

Broadcast Channel with an External Eavesdropper-III

- This achievable scheme can be combined with stochastic encoding (random binning) to obtain an inner bound for broadcast channel with an external eavesdropper:

$$\mathcal{R}^{\text{in}} = \text{conv}\left(\mathcal{R}_{12}^{\text{in}} \cup \mathcal{R}_{21}^{\text{in}}\right)$$

where $\mathcal{R}_{12}^{\text{in}}$ is

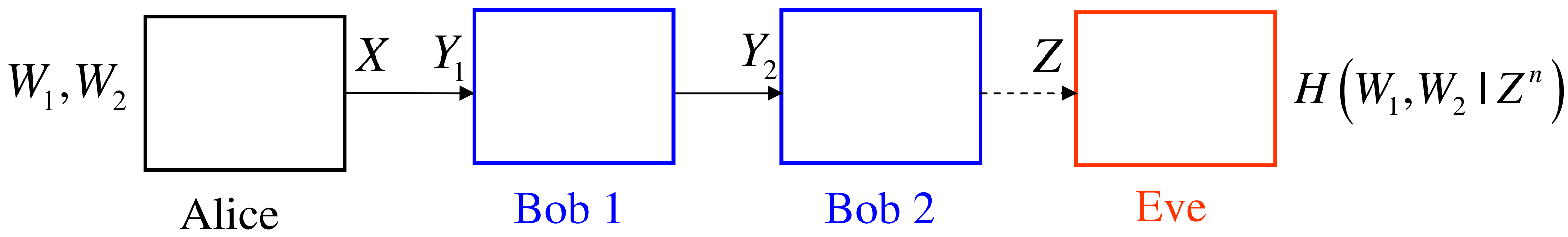
$$R_1 \leq I(V_1;Y_1) - I(V_1;Z)$$
$$R_2 \leq I(V_2;Y_2) - I(V_2;V_1,Z)$$

for some V_1, V_2 such that $V_1, V_2 \rightarrow X \rightarrow Y_1, Y_2, Z$

- This inner bound is tight for Gaussian MIMO case

Degraded Broadcast Channel with an External Eavesdropper-I

- Observations of receivers and the eavesdropper satisfy a certain order.
- This generalizes Wyner's model to a multi-receiver (broadcast) setting.



- Gaussian multi-receiver wiretap channel is an instance of this channel model.
- Plays a significant role in the Gaussian MIMO multi-receiver wiretap channel.
- The secrecy capacity region is obtained by Bagherikaram-Motahari-Khandani for $K = 2$ and by Ekrem-Ulukus for arbitrary K.

Degraded Broadcast Channel with an External Eavesdropper-II

- Capacity region for degraded broadcast channel:

$$R_1 \leq I(X;Y_1|U)$$
$$R_2 \leq I(U;Y_2)$$

where $U \rightarrow X \rightarrow Y_1, Y_2$

- Capacity region is achieved by superposition coding
- Using superposition coding with stochastic encoding, the secrecy capacity region of the degraded broadcast channel with an external eavesdropper can be obtained:

$$R_1 \leq I(X;Y_1|U) - I(X;Z|U)$$
$$R_2 \leq I(U;Y_2) - I(U;Z)$$

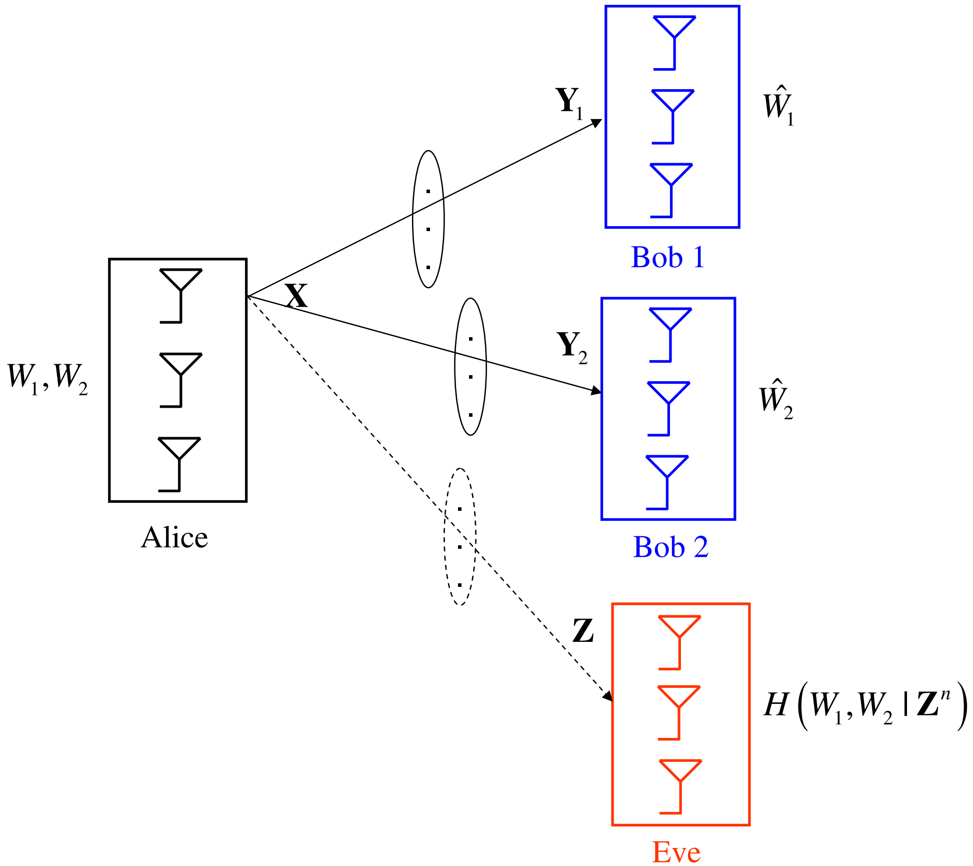
where $U \rightarrow X \rightarrow Y_1, Y_2, Z$

Gaussian MIMO Multi-receiver Wiretap Channel-I

- Channel model:

$$\mathbf{Y}_k = \mathbf{H}_k \mathbf{X} + \mathbf{N}_k, \quad k = 1, \ldots, K$$

$$\mathbf{Z} = \mathbf{H}_Z \mathbf{X} + \mathbf{N}_Z$$



- The secrecy capacity region is established by [Ekrem-Ulukus].

Gaussian MIMO Multi-receiver Wiretap Channel-II

- Secrecy capacity region is obtained in three steps
- As the first step, the degraded channel is considered

$$\mathbf{Y}_1 = \mathbf{X} + \mathbf{N}_1$$
$$\mathbf{Y}_2 = \mathbf{X} + \mathbf{N}_2$$
$$\mathbf{Z} = \mathbf{X} + \mathbf{N}_Z$$

  where the noise covariance matrices satisfy

$$\mathbf{\Sigma}_1 \preceq \mathbf{\Sigma}_2 \preceq \mathbf{\Sigma}_Z$$

- Since the secrecy capacity region depends on the marginal distributions, but not the entire joint distribution, this order is equivalent to

$$\mathbf{X} \rightarrow \mathbf{Y}_1 \rightarrow \mathbf{Y}_2 \rightarrow \mathbf{Z}$$

Gaussian MIMO Multi-receiver Wiretap Channel-III

- To obtain the secrecy capacity region of the degraded MIMO channel is tantamount to evaluating the region

$$
\begin{aligned}
R_1 &\le I(\mathbf{X};\mathbf{Y}_1|U) - I(\mathbf{X};\mathbf{Z}|U) \\
R_2 &\le I(U;\mathbf{Y}_2) - I(U;\mathbf{Z})
\end{aligned}
$$

- We show that jointly Gaussian $(U,\mathbf{X})$ is sufficient to evaluate this region
- Thus, the secrecy capacity region of the degraded MIMO channel:

$$
\begin{aligned}
R_1 &\le \frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|} - \frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \\
R_2 &\le \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}+\mathbf{\Sigma}_2|} - \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{K}+\mathbf{\Sigma}_Z|}
\end{aligned}
$$

  where $\mathbf{0} \preceq \mathbf{K} \preceq \mathbf{S}$.

Gaussian MIMO Multi-receiver Wiretap Channel-IV

- As the second step, the aligned non-degraded channel is considered

$$\mathbf{Y}_1 = \mathbf{X} + \mathbf{N}_1$$
$$\mathbf{Y}_2 = \mathbf{X} + \mathbf{N}_2$$
$$\mathbf{Z} = \mathbf{X} + \mathbf{N}_Z$$

where the noise covariance matrices does not satisfy any order

- There is no single-letter formula for the secrecy capacity region
- An achievable secrecy rate region is obtained by using dirty-paper coding in the Marton-type achievable scheme:

$$\mathcal{R}^{\text{in}} = \text{conv}\left(\mathcal{R}_{12}^{\text{in}} \cup \mathcal{R}_{21}^{\text{in}}\right)$$

where $\mathcal{R}_{12}^{\text{in}}$ is

$$R_1 \leq I(V_1;Y_1) - I(V_1;Z)$$
$$R_2 \leq I(V_2;Y_2) - I(V_2;V_1,Z)$$

for some V_1, V_2 such that $V_1, V_2 \rightarrow X \rightarrow Y_1, Y_2, Z$

Gaussian MIMO Multi-receiver Wiretap Channel-V

- The resulting achievable secrecy rate region is

$$\mathcal{R}^{\text{in}}(\mathbf{S}) = \text{conv}\left(\mathcal{R}_{12}^{\text{in}}(\mathbf{S}) \cup \mathcal{R}_{21}^{\text{in}}(\mathbf{S})\right)$$

where $\mathcal{R}_{12}^{\text{in}}(\mathbf{S})$ is

$$R_1 \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_1|}{|\mathbf{K}+\mathbf{\Sigma}_1|} - \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{K}+\mathbf{\Sigma}_Z|}$$
$$R_2 \leq \frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_2|} - \frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|}$$

where $\mathbf{0} \preceq \mathbf{K} \preceq \mathbf{S}$.

- This inner bound is shown to be tight by using channel enhancement

Gaussian MIMO Multi-receiver Wiretap Channel-VI

- For each point on the boundary of $\mathcal{R}^{\text{in}}(\mathbf{S})$, we construct an enhanced channel
- Enhanced channel is degraded, i.e., its secrecy capacity region is known
- Secrecy capacity region of the enhanced channel includes that of the original channel
- The point on $\mathcal{R}^{\text{in}}(\mathbf{S})$ for which enhanced channel is constructed is also on the boundary of the secrecy capacity region of the enhanced channel
- Thus, this point is on the boundary of the secrecy capacity region of the original channel
- $\mathcal{R}^{\text{in}}(\mathbf{S})$ is the secrecy capacity region of the original channel

Gaussian MIMO Multi-receiver Wiretap Channel-VII

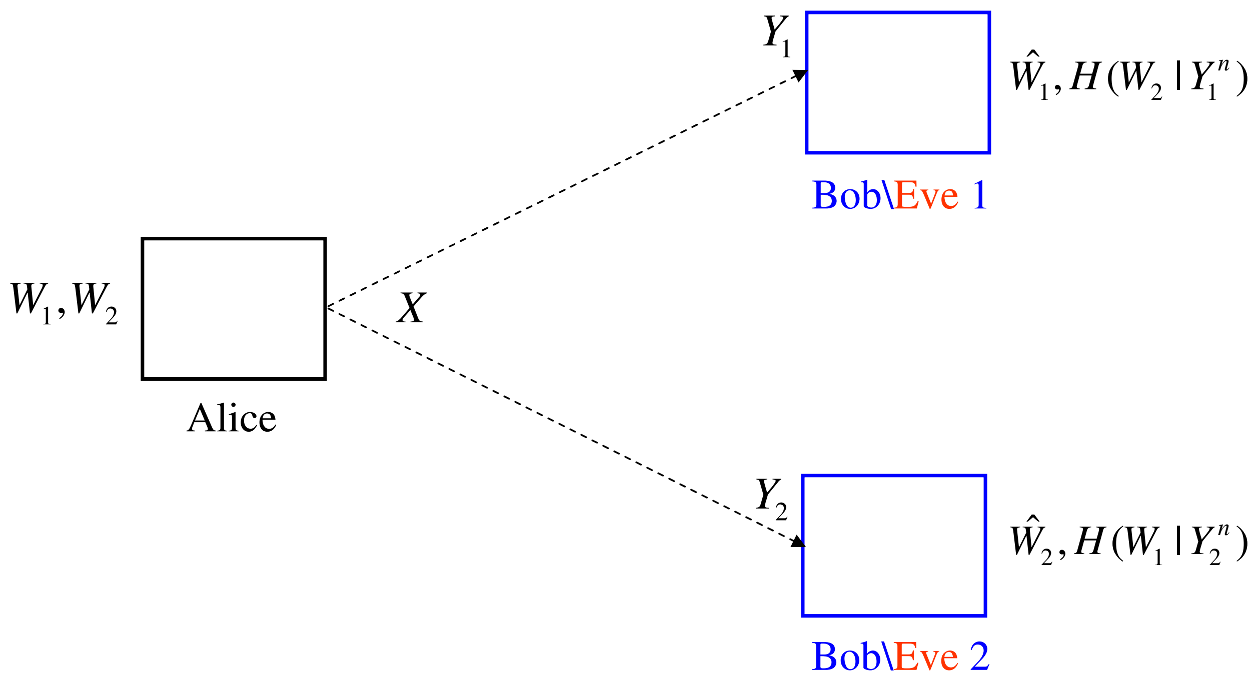
- The most general case:

$$\mathbf{Y}_1 = \mathbf{H}_1\mathbf{X} + \mathbf{N}_1$$
$$\mathbf{Y}_2 = \mathbf{H}_2\mathbf{X} + \mathbf{N}_2$$
$$\mathbf{Z} = \mathbf{H}_Z\mathbf{X} + \mathbf{N}_Z$$

- The secrecy capacity region for the most general case is obtained by using some limiting arguments in conjunction with the capacity result for the aligned case

Broadcast Channels with Confidential Messages-I

- Each user eavesdrops the other user:



- In general, problem is intractable for now
- Even without secrecy concerns, optimal transmission scheme is unknown

Broadcast Channels with Confidential Messages-II

- Best inner bound for broadcast channels is due to Marton:

$$R_1 \leq I(V_1;Y_1)$$
$$R_2 \leq I(V_2;Y_2)$$
$$R_1 + R_2 \leq I(V_1;Y_1) + I(V_2;Y_2) - I(V_1;V_2)$$

  where $V_1, V_2 \rightarrow X \rightarrow Y_1, Y_2$.

- One corner point:

$$R_1' = I(V_1;Y_1)$$
$$R_2' = I(V_2;Y_2) - I(V_2;V_1)$$

- Encode W_1 by using V_1^n
- V_1^n is a non-causally known interference for the second user: Gelfand-Pinsker setting

Broadcast Channels with Confidential Messages-III

- Marton's inner bound can be combined with stochastic encoding (random binning) to provide an achievable rate region for broadcast channels with confidential messages:

$$R_1 \leq I(V_1;Y_1) - I(V_1;Y_2,V_2)$$
$$R_2 \leq I(V_2;Y_2) - I(V_2;Y_1,V_1)$$

where $V_1,V_2 \rightarrow X \rightarrow Y_1,Y_2$.

- If there is a common message in addition to the confidential messages:

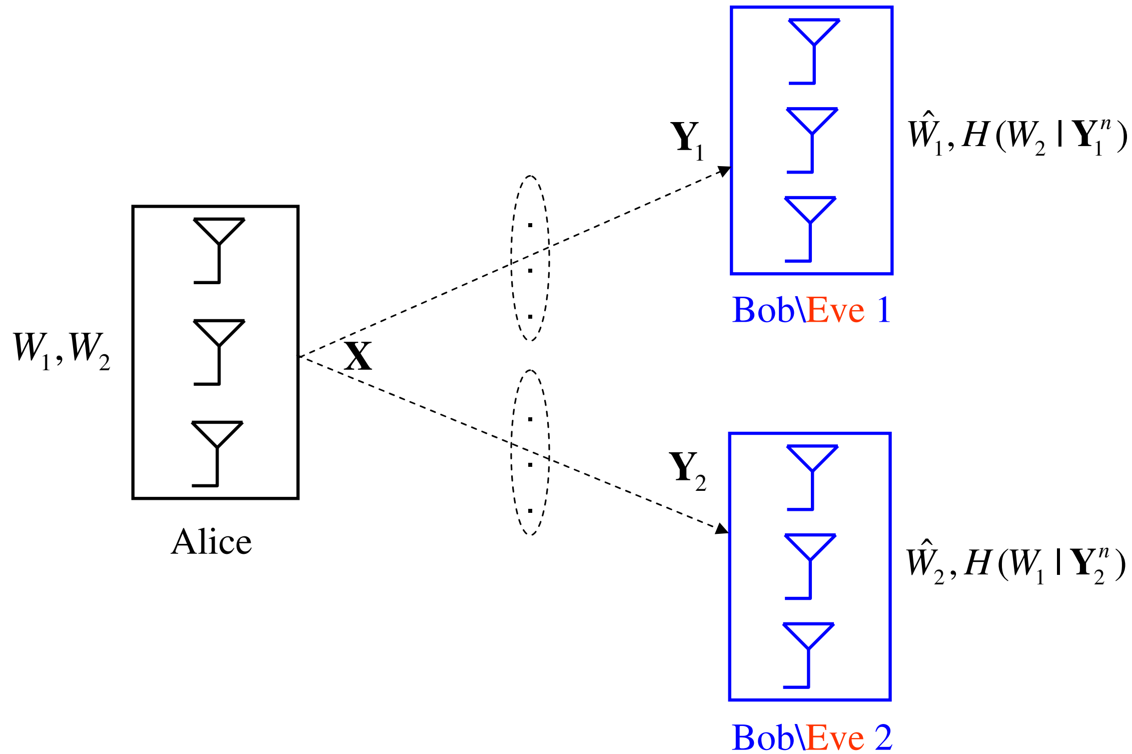
$$R_0 \leq \min\{I(U;Y_1),I(U;Y_2)\}$$
$$R_1 \leq I(V_1;Y_1|U) - I(V_1;Y_2,V_2|U)$$
$$R_2 \leq I(V_2;Y_2|U) - I(V_2;Y_1,V_1|U)$$

where $U,V_1,V_2 \rightarrow X \rightarrow Y_1,Y_2$.

- This inner bound is tight for Gaussian MIMO case.

Gaussian MIMO Broadcast Channel with Confidential Messages-I

- Each user eavesdrops the other user:



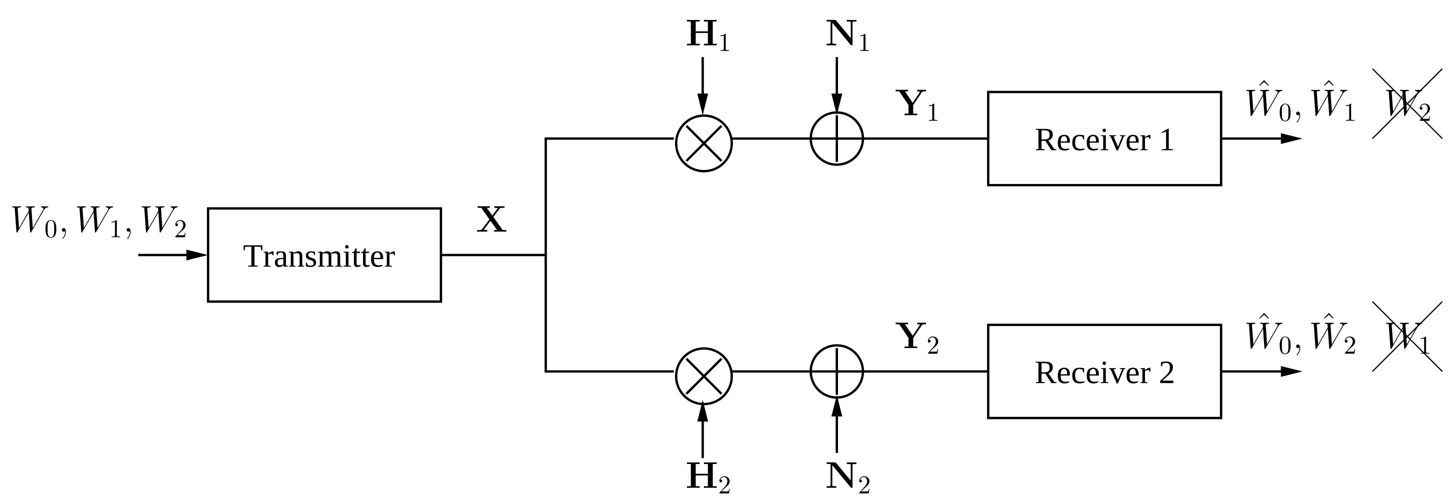
- In SISO case, only one user can have positive secrecy rate.
- In fading SISO case, both users can have positive secrecy rates [Ekrem-Ulukus].
- In MIMO case also, both users can enjoy positive secrecy rates [Liu-Liu-Poor-Shamai].
- With common messages also [Ekrem-Ulukus], [Liu-Liu-Poor-Shamai].

Gaussian MIMO Broadcast Channel with Confidential Messages-II

- Channel model

$$\mathbf{Y}_1 = \mathbf{H}_1\mathbf{X} + \mathbf{N}_1$$
$$\mathbf{Y}_2 = \mathbf{H}_2\mathbf{X} + \mathbf{N}_2$$

where $\mathbf{X}$ is subject to a covariance constraint $E\left[\mathbf{X}\mathbf{X}^{\top}\right] \preceq \mathbf{S}$



Gaussian MIMO Broadcast Channel with Confidential Messages-III

- An inner bound can be obtained by evaluating

$$R_0 \leq \min\{I(U;Y_1), I(U;Y_2)\}$$
$$R_1 \leq I(V_1;\mathbf{Y}_1|U) - I(V_1;\mathbf{Y}_2,V_2|U)$$
$$R_2 \leq I(V_2;\mathbf{Y}_2|U) - I(V_2;\mathbf{Y}_1,V_1|U)$$

with jointly Gaussian U, V_1, V_2

- We use dirty-paper coding for the confidential messages
- Depending on the encoding order for DPC, two potentially different regions arise

$$\mathcal{R}_{12}^{\text{DPC}} \quad \text{and} \quad \mathcal{R}_{21}^{\text{DPC}}$$

- We have

$$\text{conv}\left(\mathcal{R}_{12}^{\text{DPC}} \cup \mathcal{R}_{21}^{\text{DPC}}\right) \subseteq \mathcal{C}$$

Gaussian MIMO Broadcast Channel with Confidential Messages-IV

- $\mathcal{R}_{12}^{\text{DPC}}$ is given by

$$R_0 \leq \min_{j=1,2} \frac{1}{2} \log \frac{|\mathbf{H}_j \mathbf{S} \mathbf{H}_j^\top + \mathbf{\Sigma}_j|}{|\mathbf{H}_j(\mathbf{K}_1 + \mathbf{K}_2)\mathbf{H}_j^\top + \mathbf{\Sigma}_j)|}$$

$$R_1 \leq \frac{1}{2} \log \frac{|\mathbf{H}_1(\mathbf{K}_1 + \mathbf{K}_2)\mathbf{H}_1^\top + \mathbf{\Sigma}_1|}{|\mathbf{H}_1 \mathbf{K}_2 \mathbf{H}_1^\top + \mathbf{\Sigma}_1|} - \frac{1}{2} \log \frac{|\mathbf{H}_2(\mathbf{K}_1 + \mathbf{K}_2)\mathbf{H}_2^\top + \mathbf{\Sigma}_2|}{|\mathbf{H}_2 \mathbf{K}_2 \mathbf{H}_2^\top + \mathbf{\Sigma}_2|}$$

$$R_2 \leq \frac{1}{2} \log \frac{|\mathbf{H}_2 \mathbf{K}_2 \mathbf{H}_2^\top + \mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_2|} - \frac{1}{2} \log \frac{|\mathbf{H}_1 \mathbf{K}_2 \mathbf{H}_1^\top + \mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|}$$

where $\mathbf{K}_1 + \mathbf{K}_2 \preceq \mathbf{S}$.

Gaussian MIMO Broadcast Channel with Confidential Messages-V

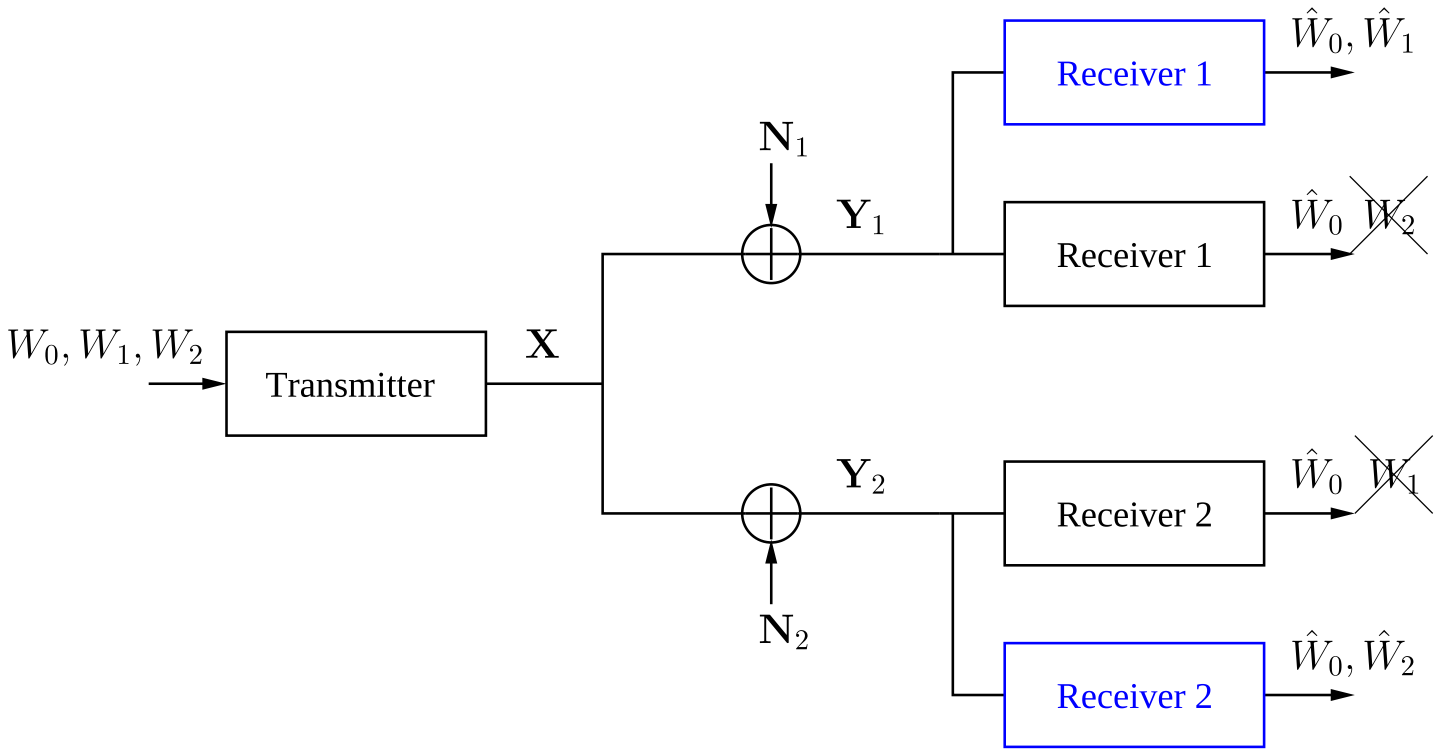
- [Ekrem-Ulukus, 2010] and [Liu-Liu-Poor-Shamai, 2010] obtain the capacity region as

$$\mathcal{C} = \mathcal{R}_{12}^{\text{DPC}} = \mathcal{R}_{21}^{\text{DPC}}$$

- Achievable rate region is invariant wrt the encoding order used in DPC
- Capacity region is proved by using channel enhancement
- For each point on the boundary of $\mathcal{R}_{12}^{\text{DPC}}$, an enhanced channel is constructed
- Capacity region of enhanced channel includes that of the original one
- Enhanced channel is degraded
- Boundary of the capacity region of the enhanced channel intersects with the boundary of $\mathcal{R}_{12}^{\text{DPC}}$ at the point for which enhanced channel is constructed
- $\mathcal{R}_{12}^{\text{DPC}}$ is the capacity region
- Due to symmetry of the analysis, $\mathcal{R}_{21}^{\text{DPC}} = \mathcal{C}$

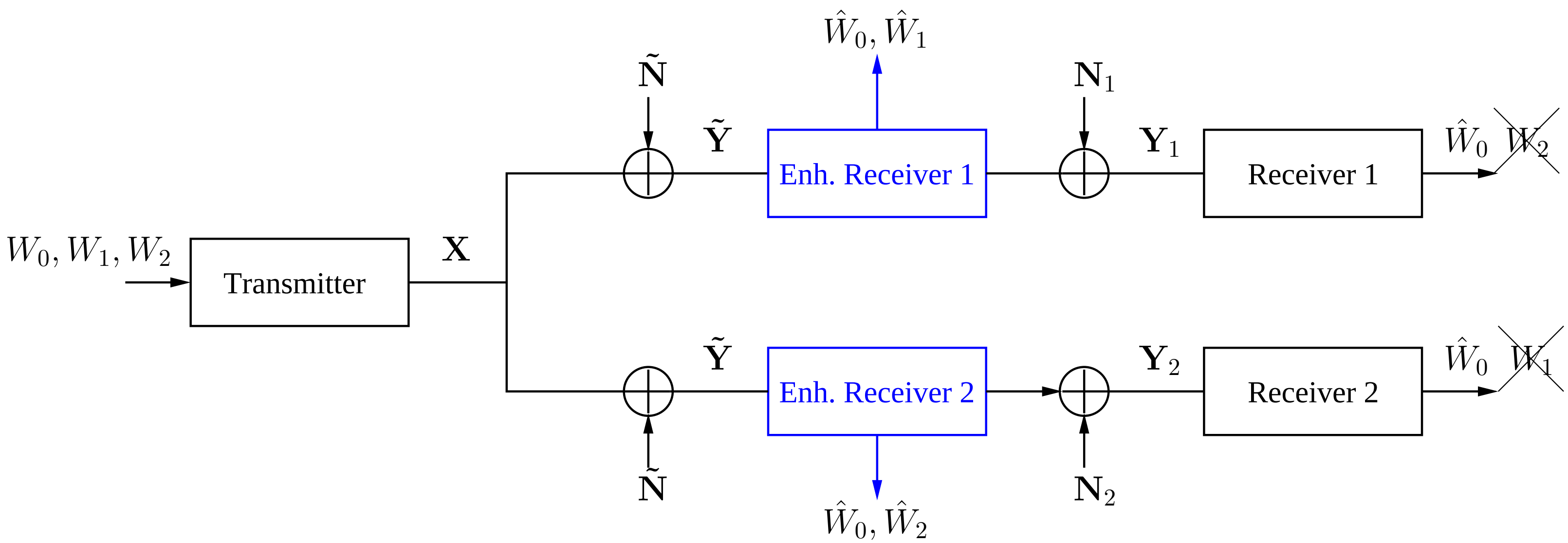
Gaussian MIMO Broadcast Channel with Confidential Messages-VI

- An alternative look at the original channel



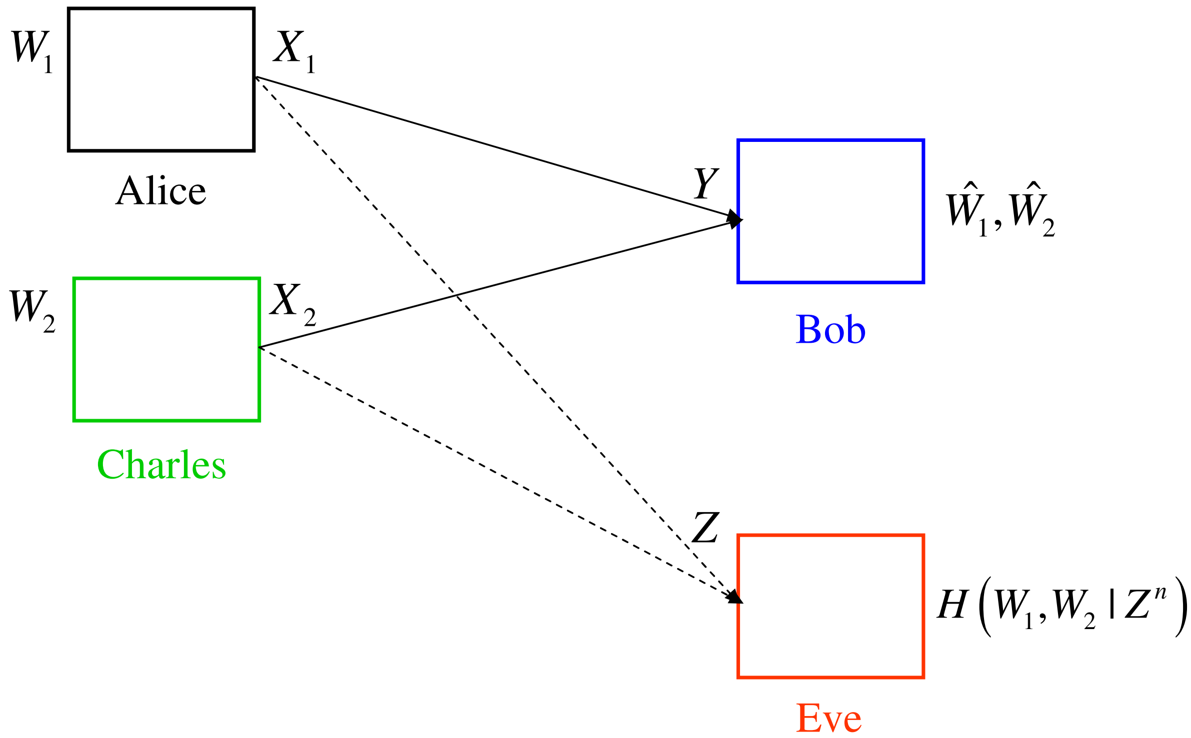
Gaussian MIMO Broadcast Channel with Confidential Messages-VII

- Enhanced channel



Multiple Access Wiretap Channel

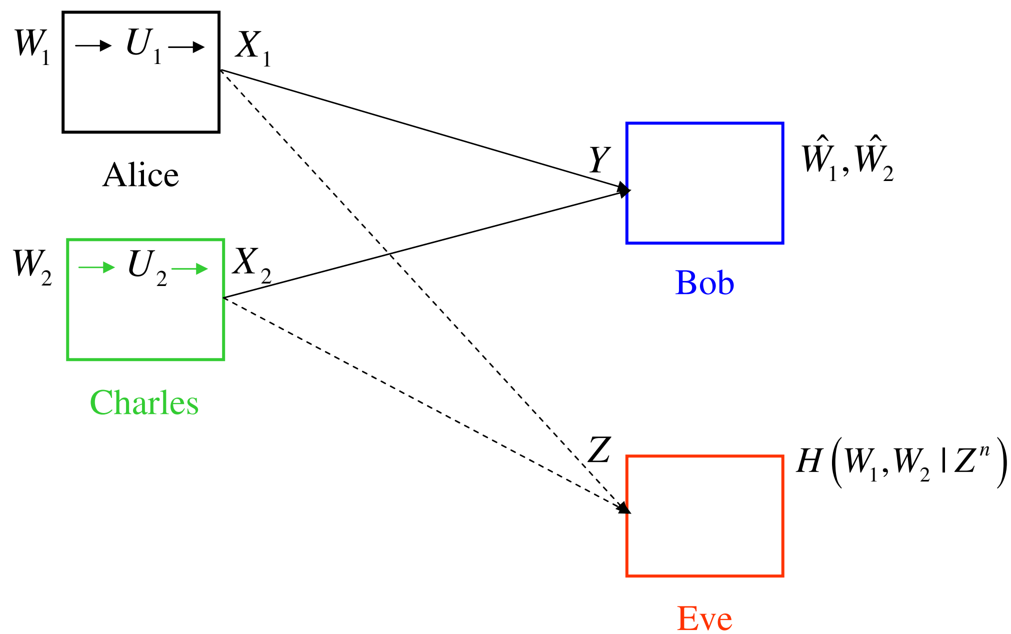
- An external eavesdropper listens in on the communication from end-users to the base station.



- Introduced by Tekin-Yener in 2005:
  - Achievability of positive secrecy rates are shown.
  - Cooperative jamming is discovered.

Achievable Rate Region for Multiple Access Wiretap Channel

- Introduce two independent **auxiliary random variables** U_1 and U_2.



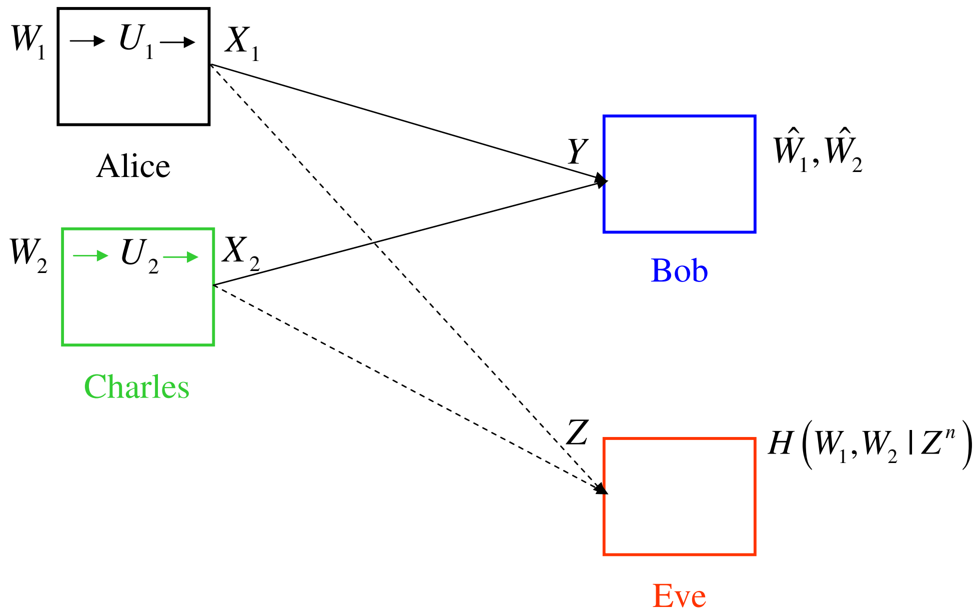
- An achievable secrecy rate region with channel pre-fixing:

$$R_1 \leq I(U_1;Y|U_2) - I(U_1;Z)$$
$$R_2 \leq I(U_2;Y|U_1) - I(U_2;Z)$$
$$R_1 + R_2 \leq I(U_1,U_2;Y) - I(U_1,U_2;Z)$$

where $p(u_1,u_2,x_1,x_2,y,z)$ factors as $p(u_1)p(u_2)p(x_1|u_1)p(x_2|u_2)p(y,z|x_1,x_2)$.

Gaussian Multiple Access Wiretap Channel: Gaussian Signalling

- Tekin-Yener 2005: Gaussian multiple access wiretap channel



- Achievable secrecy region with no channel prefixing, $X_1 = U_1$, $X_2 = U_2$, Gaussian signals:

$$R_1 \leq \frac{1}{2}\log\left(1 + h_1 P_1\right) - \frac{1}{2}\log\left(1 + \frac{g_1 P_1}{1 + g_2 P_2}\right)$$

$$R_2 \leq \frac{1}{2}\log\left(1 + h_2 P_2\right) - \frac{1}{2}\log\left(1 + \frac{g_2 P_2}{1 + g_1 P_1}\right)$$

$$R_1 + R_2 \leq \frac{1}{2}\log\left(1 + h_1 P_1 + h_2 P_2\right) - \frac{1}{2}\log(1 + g_1 P_1 + g_2 P_2)$$

- No scaling with SNRs.

Cooperative Jamming

- Tekin-Yener, 2006: **cooperative jamming** technique.
- Cooperative jamming is a form of channel pre-fixing:

$$X_1 = U_1 + V_1 \qquad \text{and} \qquad X_2 = U_2 + V_2$$

where U_1 and U_2 carry messages and V_1 and V_2 are jamming signals.

- Achievable secrecy rate region with cooperative jamming:

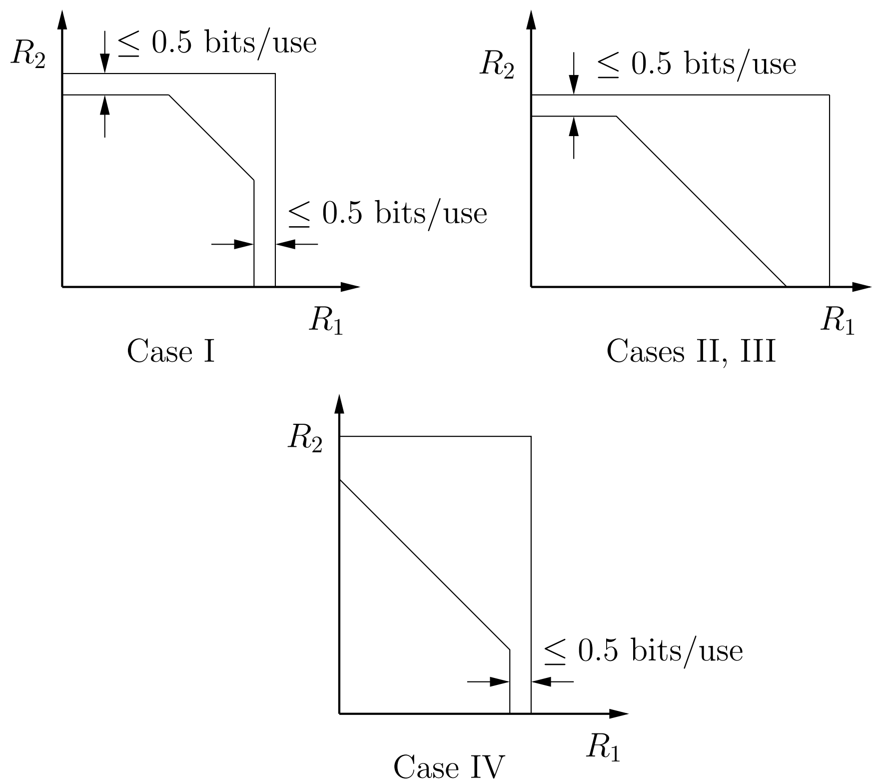
$$\begin{aligned}
R_1 &\leq \frac{1}{2}\log\left(1+\frac{h_1P_1}{1+h_1Q_1+h_2Q_2}\right)-\frac{1}{2}\log\left(1+\frac{g_1P_1}{1+g_1Q_1+g_2(P_2+Q_2)}\right)\\
R_2 &\leq \frac{1}{2}\log\left(1+\frac{h_2P_2}{1+h_1Q_1+h_2Q_2}\right)-\frac{1}{2}\log\left(1+\frac{g_2P_2}{1+g_1(P_1+Q_1)+g_2Q_2}\right)\\
R_1+R_2 &\leq \frac{1}{2}\log\left(1+\frac{h_1P_1+h_2P_2}{1+h_1Q_1+h_2Q_2}\right)-\frac{1}{2}\log\left(1+\frac{g_1P_1+g_2P_2}{1+g_1Q_1+g_2Q_2}\right)
\end{aligned}$$

where P_1 and P_2 are the powers of U_1 and U_2 and Q_1 and Q_2 are the powers of V_1 and V_2.

- No scaling with SNR.

Weak Eavesdropper Multiple Access Wiretap Channel

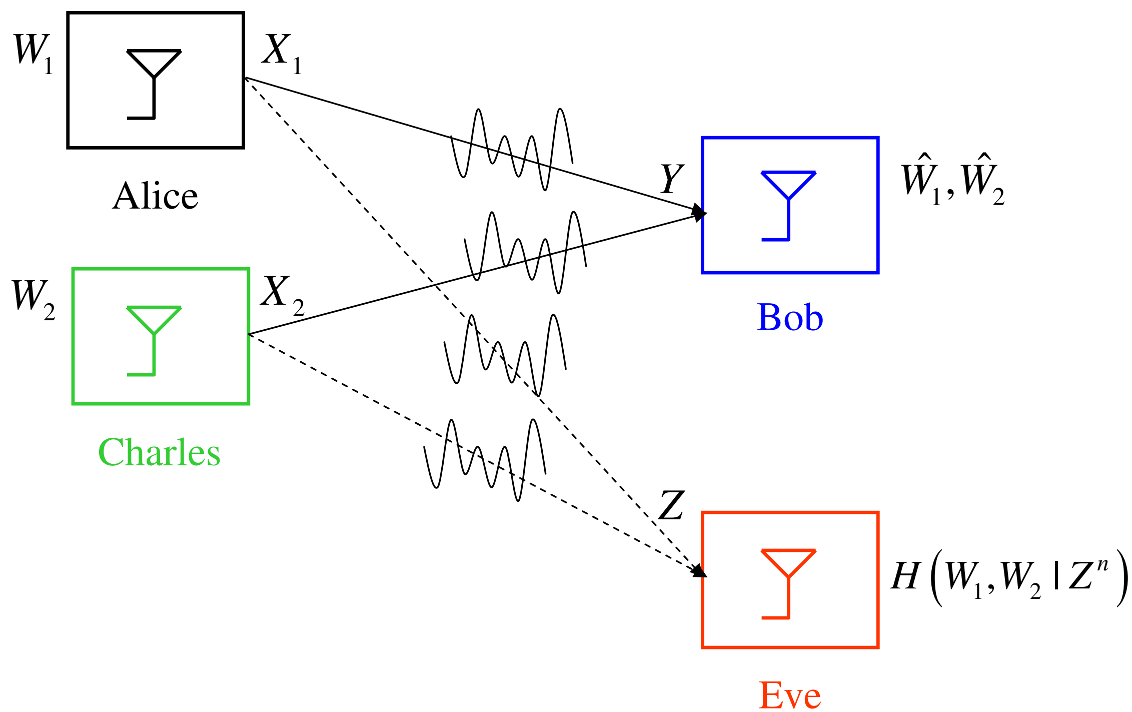
- For the weak eavesdropper case, Gaussian signalling is nearly optimal [Ekrem-Ulukus].



- In general, Gaussian signalling is not optimal:
  - He-Yener showed that structured codes (e.g., lattice codes) outperform Gaussian codes.
  - Structured codes can provide secrecy rates that scale with $\log \text{SNR}$.
- The secrecy capacity of the multiple access wiretap channel is still open.

Fading Multiple Access Wiretap Channel-I

- Introduced by Tekin-Yener in 2007.
- They provide achievable secrecy rates based on Gaussian signalling.
- Main assumption: Channel state information is known at all nodes.



Fading Multiple Access Wiretap Channel-II

- Achievable rates without cooperative jamming:

$$R_1 \leq \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \left[\log\left(1+h_1P_1\right) - \frac{1}{2}\log\left(1+\frac{g_1P_1}{1+g_2P_2}\right)\right]$$

$$R_2 \leq \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \left[\log\left(1+h_2P_2\right) - \frac{1}{2}\log\left(1+\frac{g_2P_2}{1+g_1P_1}\right)\right]$$

$$R_1+R_2 \leq \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \left[\log\left(1+h_1P_1+h_2P_2\right) - \frac{1}{2}\log(1+g_1P_1+g_2P_2)\right]$$

- Achievable rates with cooperative jamming:

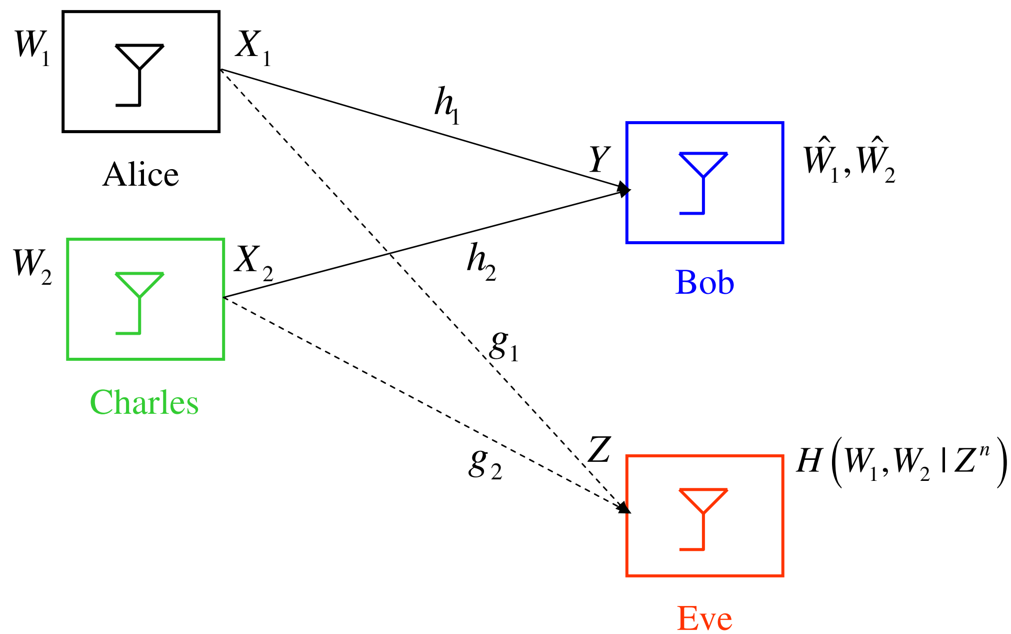
$$R_1 \leq \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \left[\log\left(1+\frac{h_1P_1}{1+h_1Q_1+h_2Q_2}\right) - \frac{1}{2}\log\left(1+\frac{g_1P_1}{1+g_1Q_1+g_2(P_2+Q_2)}\right)\right]$$

$$R_2 \leq \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \left[\log\left(1+\frac{h_2P_2}{1+h_1Q_1+h_2Q_2}\right) - \frac{1}{2}\log\left(1+\frac{g_2P_2}{1+g_1(P_1+Q_1)+g_2Q_2}\right)\right]$$

$$R_1+R_2 \leq \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \left[\log\left(1+\frac{h_1P_1+h_2P_2}{1+h_1Q_1+h_2Q_2}\right) - \frac{1}{2}\log\left(1+\frac{g_1P_1+g_2P_2}{1+g_1Q_1+g_2Q_2}\right)\right]$$

- In both cases: No scaling with SNR.

Scaling Based Alignment (SBA) – Introduction

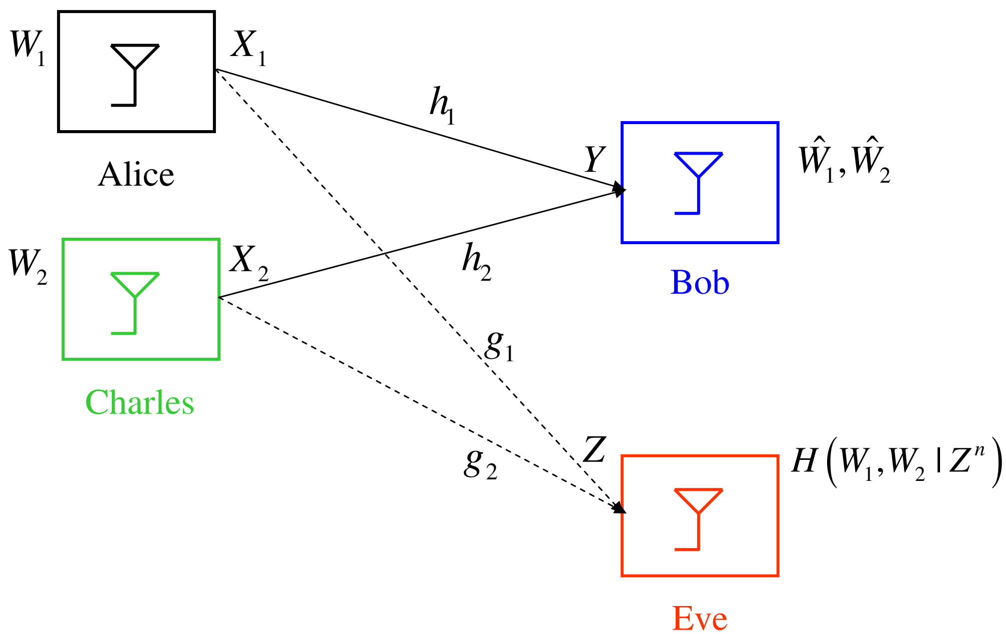


$$Y = h_1 X_1 + h_2 X_2 + N$$

$$Z = g_1 X_1 + g_2 X_2 + N'$$

Scaling Based Alignment (SBA) – Introduction

- Scaling at the transmitter:
  - Alice multiplies her channel input by the channel gain of Charles to Eve.
  - Charles multiplies his channel input by the channel gain of Alice to Eve.

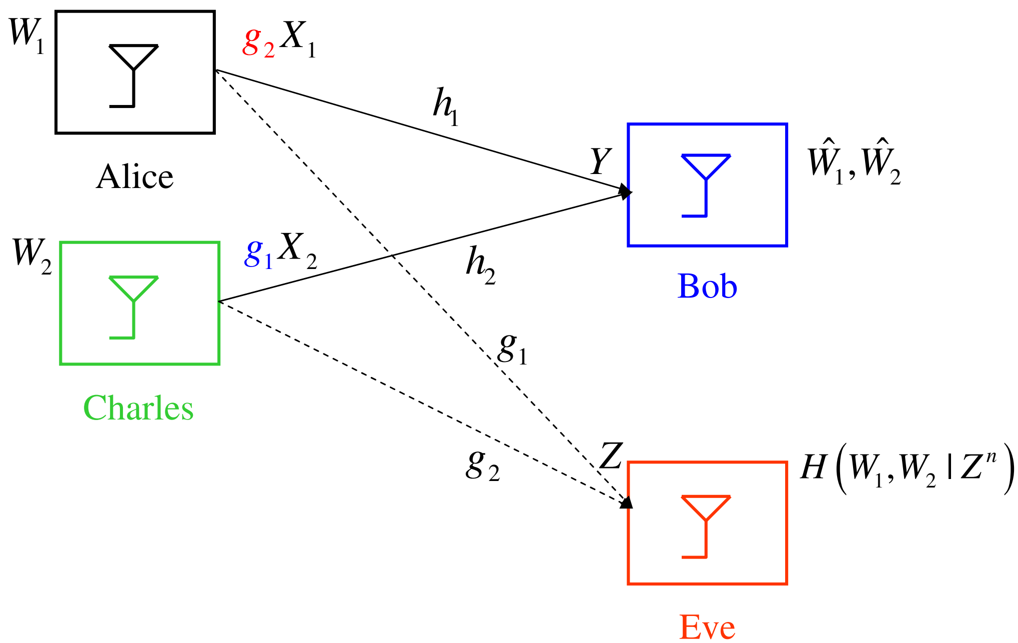


$$Y = h_1 X_1 + h_2 X_2 + N$$

$$Z = g_1 X_1 + g_2 X_2 + N'$$

Scaling Based Alignment (SBA) – Introduction

- Scaling at the transmitter:
  - Alice multiplies her channel input by the channel gain of Charles to Eve.
  - Charles multiplies his channel input by the channel gain of Alice to Eve.

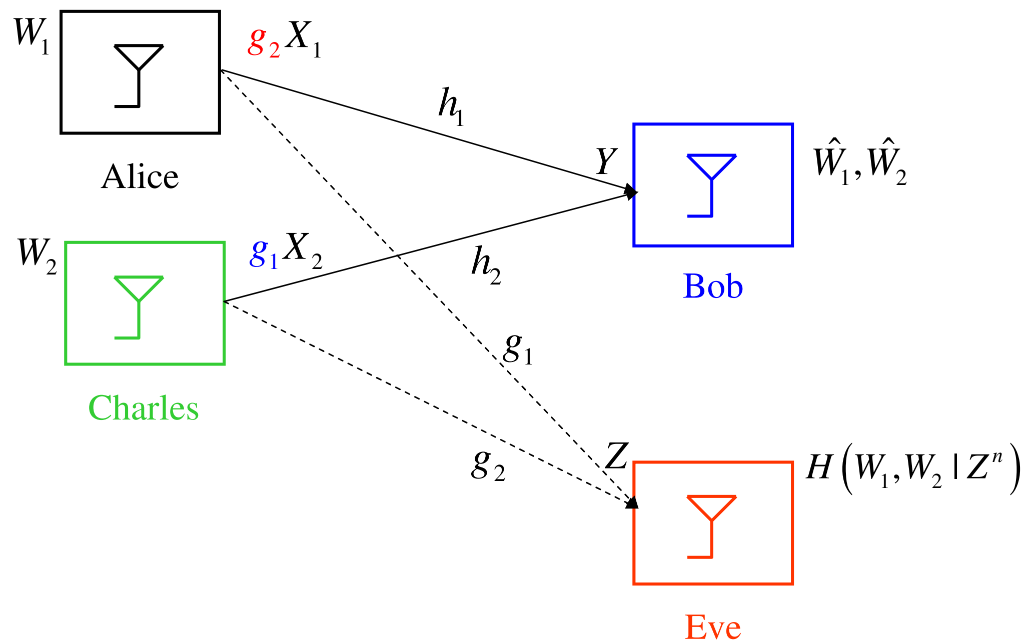


$$Y = h_1 g_2 X_1 + h_2 g_1 X_2 + N$$

$$Z = g_1 g_2 X_1 + g_2 g_1 X_2 + N'$$

Scaling Based Alignment (SBA) – Introduction

- Scaling at the transmitter:
  - Alice multiplies her channel input by the channel gain of Charles to Eve.
  - Charles multiplies his channel input by the channel gain of Alice to Eve.



$$Y = h_1 g_2 X_1 + h_2 g_1 X_2 + N$$

$$Z = g_1 g_2 X_1 + g_2 g_1 X_2 + N'$$

- Repetition: Both Alice and Charles repeat their symbols in two **consecutive** intervals.

Scaling Based Alignment (SBA) – Analysis

- Received signal at Bob (odd and even time indices):

$$Y_o = h_{1o} g_{2o} X_1 + h_{2o} g_{1o} X_2 + N_o$$
$$Y_e = h_{1e} g_{2e} X_1 + h_{2e} g_{1e} X_2 + N_e$$

- Received signal at Eve (odd and even time indices):

$$Z_o = g_{1o} g_{2o} X_1 + g_{2o} g_{1o} X_2 + N'_o$$
$$Z_e = g_{1e} g_{2e} X_1 + g_{2e} g_{1e} X_2 + N'_e$$

- At high SNR (imagine negligible noise):
  - Bob has two independent equations.
  - Eve has one equation.

  to solve for X_1 and X_2.

Scaling Based Alignment (SBA) – Analysis

- Received signal at Bob (odd and even time indices):

$$Y_o = h_{1o}g_{2o}X_1 + h_{2o}g_{1o}X_2$$

$$Y_e = h_{1e}g_{2e}X_1 + h_{2e}g_{1e}X_2$$

- Received signal at Eve (odd and even time indices):

$$Z_o = g_{1o}g_{2o}X_1 + g_{2o}g_{1o}X_2$$

$$Z_e = g_{1e}g_{2e}X_1 + g_{2e}g_{1e}X_2$$

- At high SNR (imagine negligible noise):
  - Bob has two independent equations.
  - Eve has one equation.

  to solve for X_1 and X_2.

Scaling Based Alignment (SBA) – Achievable Rates

- Following rates are achievable:

$$R_1 \leq \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \left\{ \log\left(1 + (|h_{1o} g_{2o}|^2 + |h_{1e} g_{2e}|^2) P_1\right) - \log\left(1 + \frac{(|g_{1o} g_{2o}|^2 + |g_{1e} g_{2e}|^2) P_1}{1 + (|g_{1o} g_{2o}|^2 + |g_{1e} g_{2e}|^2) P_2}\right) \right\}$$

$$R_2 \leq \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \left\{ \log\left(1 + (|h_{2o} g_{1o}|^2 + |h_{2e} g_{1e}|^2) P_2\right) - \log\left(1 + \frac{(|g_{1o} g_{2o}|^2 + |g_{1e} g_{2e}|^2) P_2}{1 + (|g_{1o} g_{2o}|^2 + |g_{1e} g_{2e}|^2) P_1}\right) \right\}$$

$$\begin{aligned} R_1 + R_2 \leq \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \Bigg\{ & \log\Bigg(1 + \left(|h_{1o} g_{2o}|^2 + |h_{1e} g_{2e}|^2\right) P_1 + \left(|h_{2o} g_{1o}|^2 + |h_{2e} g_{1e}|^2\right) P_2 \\ & \qquad + |h_{1e} h_{2o} g_{1o} g_{2e} - h_{1o} h_{2e} g_{1e} g_{2o}|^2 P_1 P_2 \Bigg) \\ & - \log\left(1 + \left(|g_{1o} g_{2o}|^2 + |g_{1e} g_{2e}|^2\right) (P_1 + P_2)\right) \Bigg\} \end{aligned}$$

where

$$E\left[\left(|g_{2o}|^2 + |g_{2e}|^2\right) P_1\right] \leq \bar{P}_1$$

$$E\left[\left(|g_{1o}|^2 + |g_{1e}|^2\right) P_2\right] \leq \bar{P}_2$$

- P_1 and P_2 should be understood as $P_1(\mathbf{h},\mathbf{g})$ and $P_2(\mathbf{h},\mathbf{g})$.

Scaling Based Alignment (SBA) – Scaling with SNR and Secure DoF

- Secrecy sum rate achievable by the SBA scheme:

$$R_s = \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \Bigg\{ \log \Bigg(1 + \left(|h_{1o} g_{2o}|^2 + |h_{1e} g_{2e}|^2 \right) P_1 + \left(|h_{2o} g_{1o}|^2 + |h_{2e} g_{1e}|^2 \right) P_2$$

$$+ |h_{1e} h_{2o} g_{1o} g_{2e} - h_{1o} h_{2e} g_{1e} g_{2o}|^2 P_1 P_2 \Bigg)$$

$$- \log \Bigg(1 + \left(|g_{1o} g_{2o}|^2 + |g_{1e} g_{2e}|^2 \right) (P_1 + P_2) \Bigg) \Bigg\}$$

- A total of $\frac{1}{2}$ secure DoF is achievable.

Ergodic Secret Alignment (ESA)

- Instead of repeating at two **consecutive** time instances, repeat at well-chosen time instances.
- Akin to [Nazer-Gastpar-Jafar-Vishwanath, 2009] ergodic interference alignment.
- At any given instant t_1, received signal at Bob and Eve is,

$$\begin{pmatrix} Y_{t_1} \\ Z_{t_1} \end{pmatrix} = \begin{pmatrix} h_1 & h_2 \\ g_1 & g_2 \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \end{pmatrix} + \begin{pmatrix} N_{t_1} \\ N'_{t_1} \end{pmatrix}$$

- Repeat at time instance t_2, and the received signal at Bob and Eve is,

$$\begin{pmatrix} Y_{t_2} \\ Z_{t_2} \end{pmatrix} = \begin{pmatrix} h_1 & -h_2 \\ g_1 & g_2 \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \end{pmatrix} + \begin{pmatrix} N_{t_2} \\ N'_{t_2} \end{pmatrix}$$

- This creates orthogonal MAC to Bob, but a scalar MAC to Eve.

Ergodic Secret Alignment (ESA) – Achievable Rates

- Following rates are achievable:

$$R_1 \leq \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \left\{ \log\left(1+2|h_1|^2 P_1\right) - \log\left(1+\frac{2|g_1|^2 P_1}{1+2|g_2|^2 P_2}\right) \right\}$$

$$R_2 \leq \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \left\{ \log\left(1+2|h_2|^2 P_2\right) - \log\left(1+\frac{2|g_2|^2 P_2}{1+2|g_1|^2 P_1}\right) \right\}$$

$$R_1 + R_2 \leq \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \left\{ \log\left(1+2|h_1|^2 P_1\right) + \log\left(1+2|h_2|^2 P_2\right) - \log\left(1+2(|g_1|^2 P_1 + |g_2|^2 P_2)\right) \right\}$$

  where $E[P_1] \leq \bar{P}_1$ and $E[P_2] \leq \bar{P}_2$.

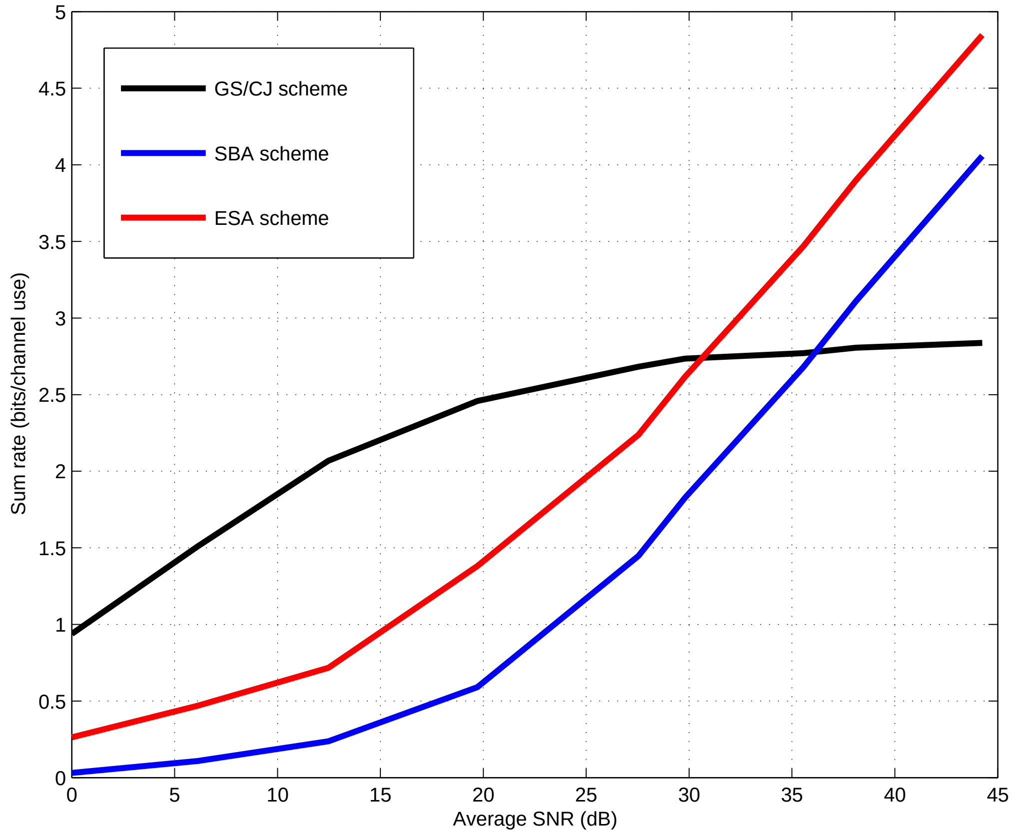
- P_1 and P_2 should be understood as $P_1(\mathbf{h},\mathbf{g})$ and $P_2(\mathbf{h},\mathbf{g})$.

- Rates scale with SNR as in the SBA scheme: A total of $\frac{1}{2}$ secure DoF is achievable.

- Rates achieved here are larger than those with our first scheme.

- We have shown recently that using cooperative jamming on the top of the ESA scheme achieves even larger secrecy rates.

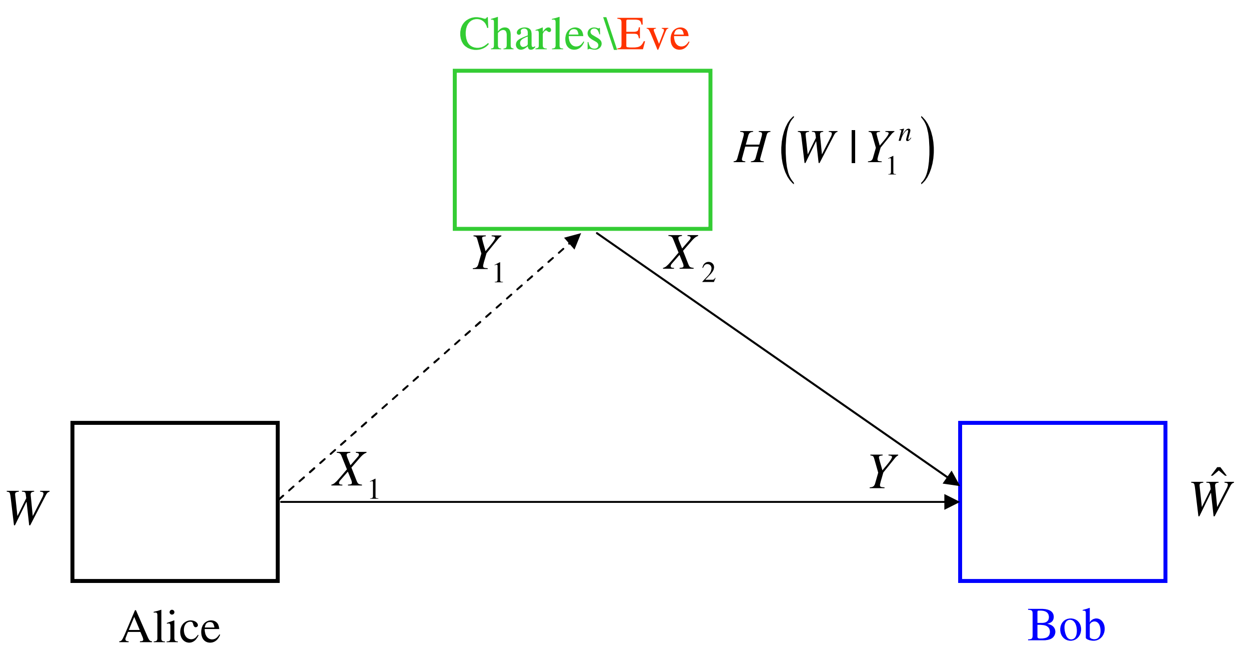
Fading Multiple Access Wiretap Channel – Achievable Rates



- Rates with Gaussian signalling (with or without cooperative jamming) do not scale.
- Rates with scaling based alignment (SBA) and ergodic secret alignment (ESA) scale.
- ESA performs better than SBA.

Cooperative Channels and Secrecy

- How do cooperation and secrecy interact?
- Is there a trade-off or a synergy?



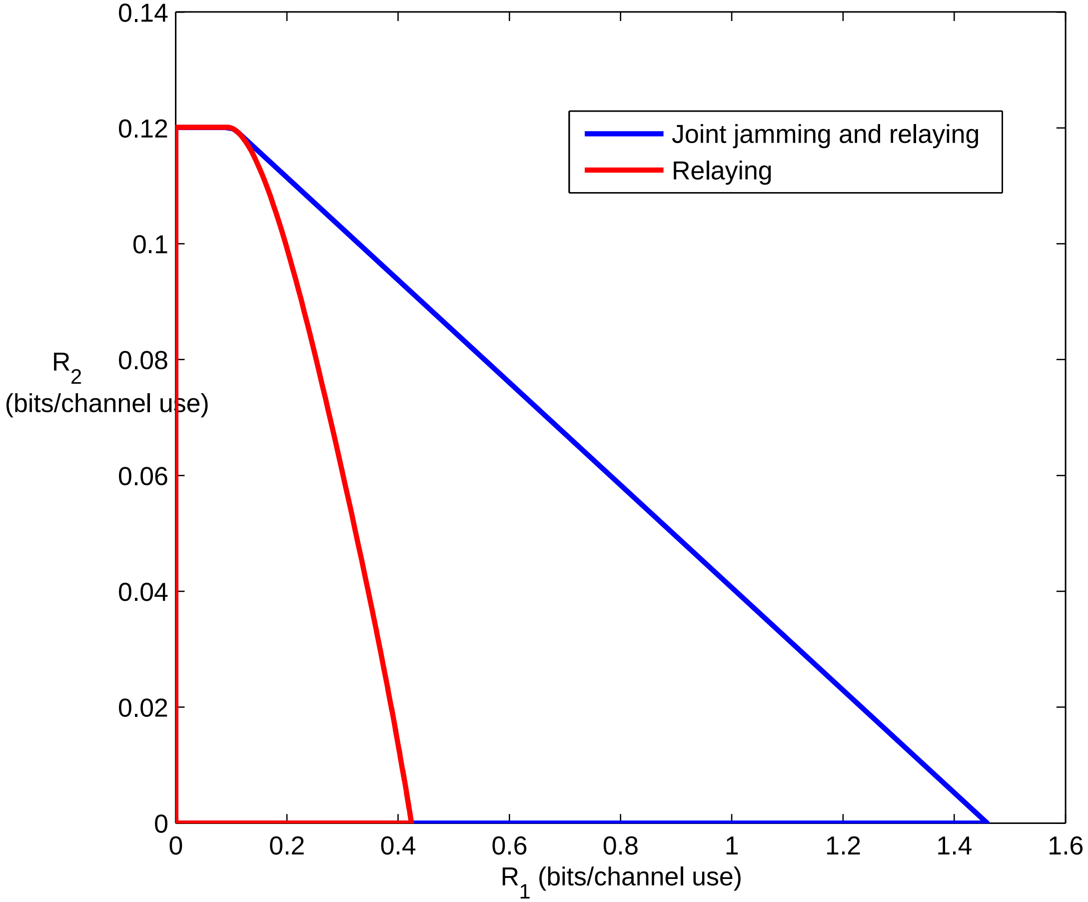
- Relay channel [He-Yener].
- Cooperative broadcast and cooperative multiple access channels [Ekrem-Ulukus].

Interactions of Cooperation and Secrecy

- Existing cooperation strategies:
  - Decode-and-forward (DAF)
  - Compress-and-forward (CAF)
- Decode-and-forward:
  - Relay decodes (learns) the message.
  - No secrecy is possible.
- Compress-and-forward:
  - Relay does not need to decode the message.
  - Can it be useful for secrecy?
- Achievable secrecy rate when relay uses CAF:

$$I(X_1;Y_1,\hat{Y}_1|X_2) - I(X_1;Y_2|X_2) = \underbrace{I(X_1;Y_1|X_2) - I(X_1;Y_2|X_2)}_{\text{secrecy rate of the wiretap channel}} + \underbrace{I(X_1;\hat{Y}_1|X_2,Y_1)}_{\text{additional term due to CAF}}$$

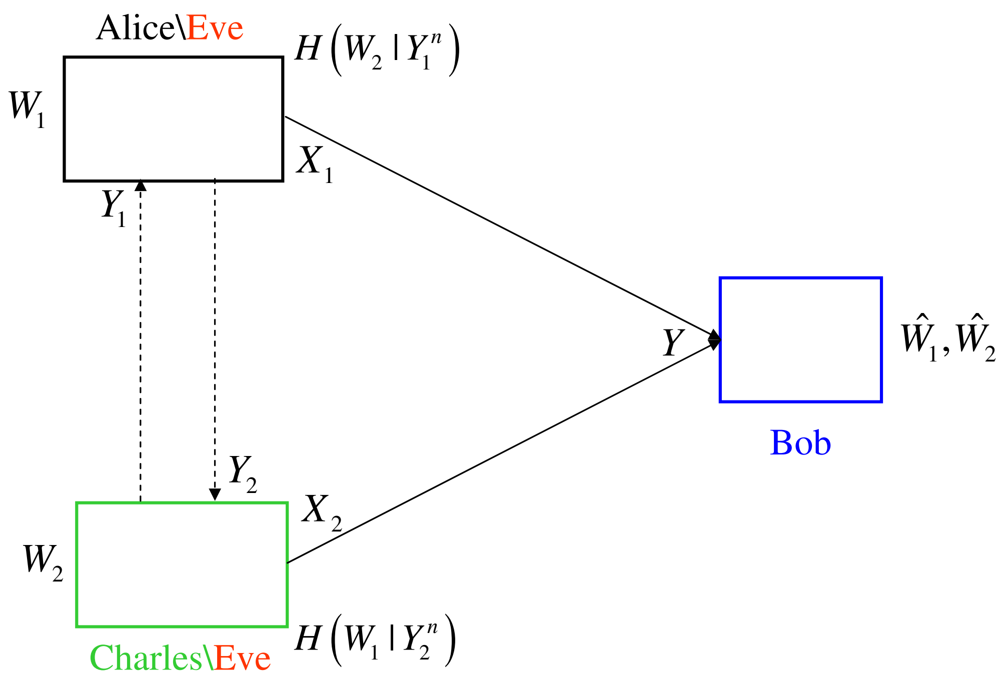
Example: Gaussian Relay Broadcast Channel (Charles is Stronger)



- Bob cannot have any positive secrecy rate without cooperation.
- Cooperation is beneficial for secrecy if CAF based relaying (cooperation) is employed.
- Charles can further improve his own secrecy by joint relaying and jamming.

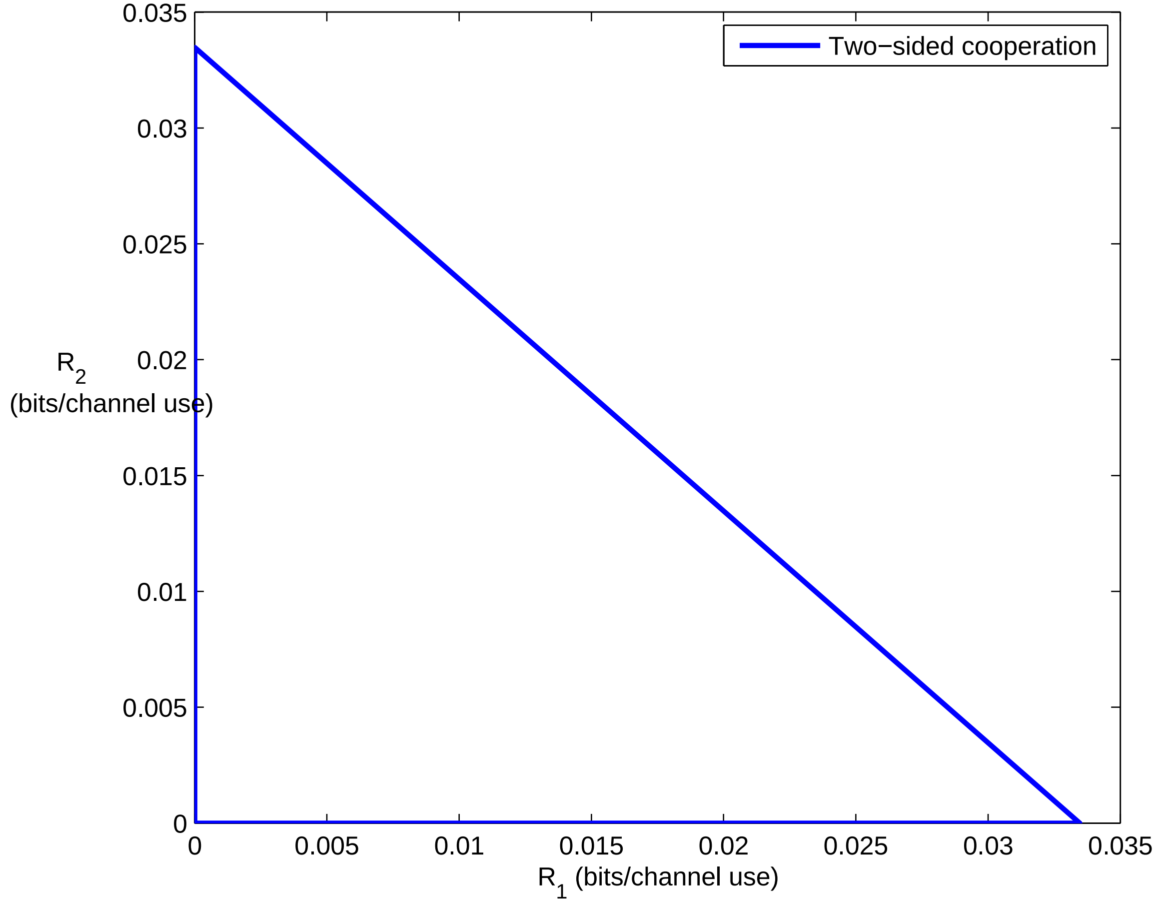
Multiple Access (Uplink) Channel with Cooperation

- **Overheard information** at users can be used to improve achievable rates.
- This overheard information results in loss of confidentiality.
- Should the users ignore it or can it be used to improve (obtain) secrecy?
  - DAF cannot help.
  - CAF may help.
  - CAF may increase rate of a user beyond the decoding capability of the cooperating user.



Example: Gaussian Multiple Access Channel with Cooperation

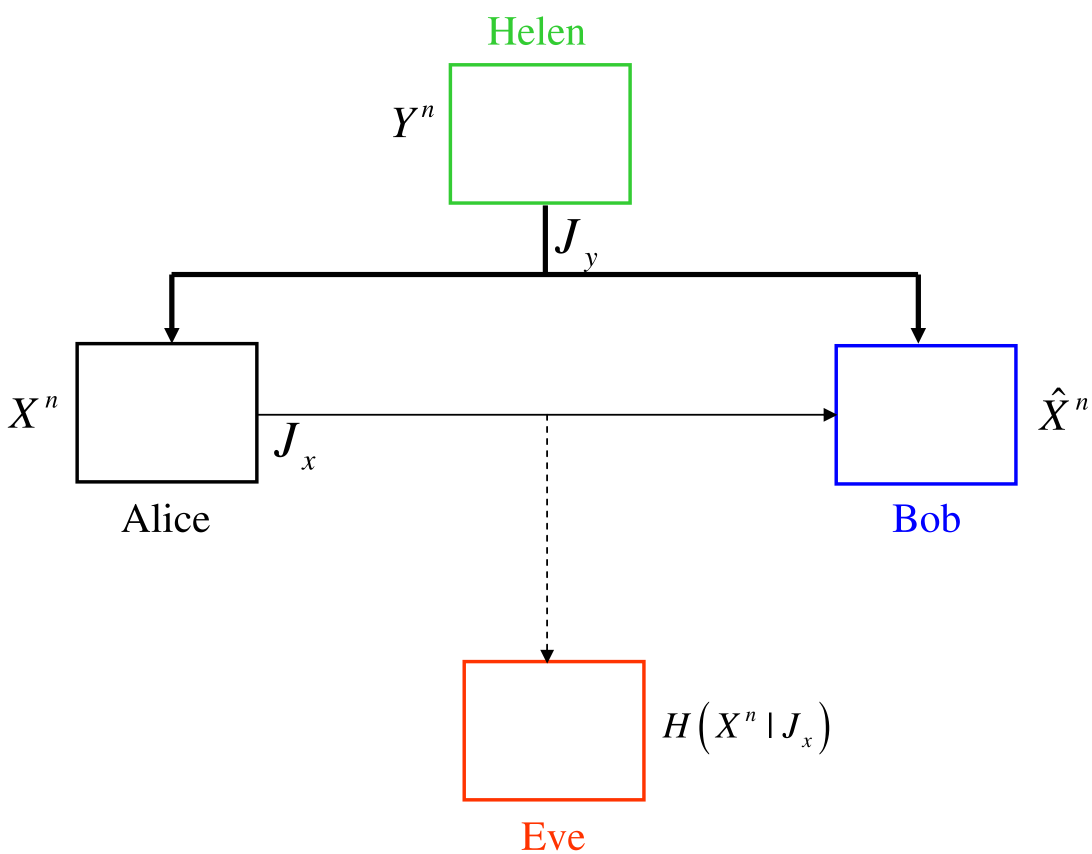
- Both inter-user links are stronger than the main link.
- Without cooperation, none of the users can get a positive secrecy rate.



- Cooperation is beneficial for secrecy if CAF is employed.

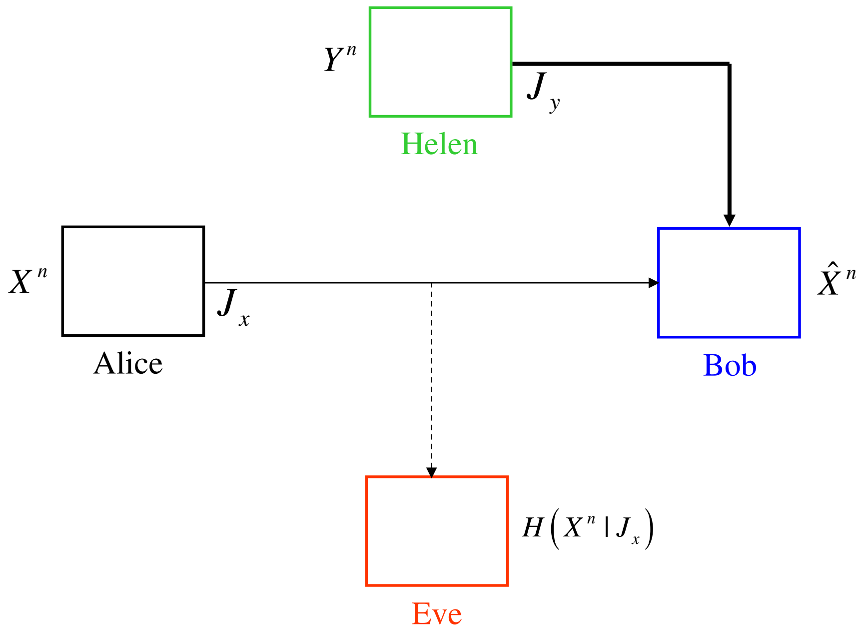
Secure Distributed Source Coding

- Sensors get correlated observations.
- Some sensors might be untrusted or even malicious, while some sensors might be helpful.
- Lossless transmission of X to Bob while minimizing information leakage to Eve.
  - One-sided and two-sided helper cases [Tandon-Ulukus-Ramchandran].



Secure Source Coding with One-Sided Helper

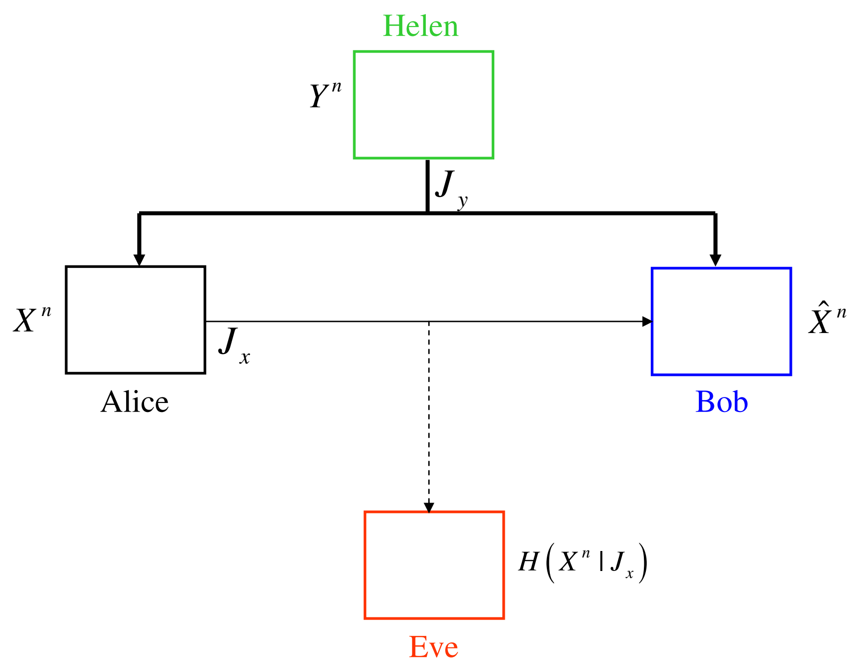
- One-sided helper:



- Achievability scheme:
  - Helen uses a rate-distortion code to describe Y to Bob.
  - Alice performs Slepian-Wolf binning of X w.r.t. the side information at Bob.
- Slepian-Wolf coding of X is optimal.

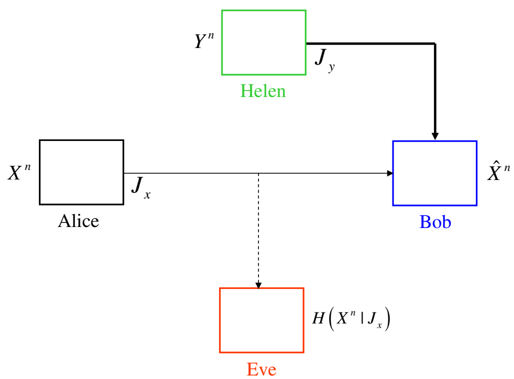
Secure Source Coding with Two-Sided Helper

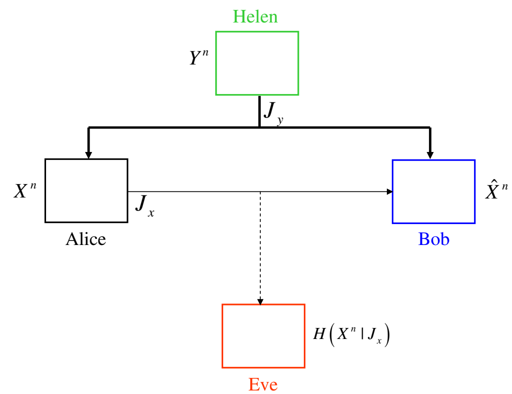
- Two-sided helper:



- Achievability Scheme:
  - Helen uses a rate-distortion code to describe Y to both Bob and Alice through V.
  - Alice creates U using a conditional rate-distortion code of rate $I(X;U|V)$.
  - Alice also bins the source X at a rate $H(X|U,V)$.
- Slepian-Wolf coding of X is not optimal.

Comparison of One-Sided and Two-Sided Helper Cases



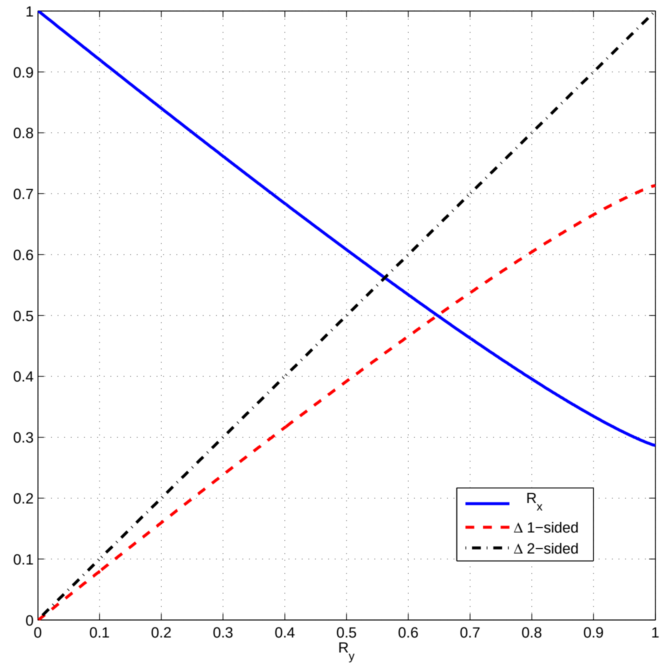


- Rate-regions:

$\mathcal{R}_{1-sided}$	$\mathcal{R}_{2-sided}$
$R_x \geq H(X\|V)$	$R_x \geq H(X\|V)$
$R_y \geq I(Y;V)$	$R_y \geq I(Y;V)$
$\Delta \leq I(X;V)$	$\Delta \leq \min(I(X;V\|U), R_y)$

- Choosing $U = \phi$ corresponds to Slepian-Wolf coding of X.
- Slepian-Wolf coding is optimal for one-sided, sub-optimal for two-sided.
- Dropping the security constraint:
  - Both rate-regions are the same. Additional side-information at Alice is of no-value.

Example: Secure Source Coding for Binary Symmetric Sources



- For all $R_y > 0$, we have $\Delta_{2-sided} > \Delta_{1-sided}$.
- For $R_y \geq 1$:
  - No need to use correlated source Y.
  - Using one-time-pad, perfectly secure communication is possible.
- For $R_y < 1$, two-sided coded output V plays a dual role:
  - Being secure, reduces information leakage to Eve.
  - Being correlated to X, reduces rate of transmission.

Conclusions

- Wireless communication is susceptible to eavesdropping and **jamming** attacks.
- Wireless medium also offers ways to neutralize the loss of confidentiality:
  - time, frequency, multi-user diversity
  - spatial diversity through multiple antennas
  - cooperation via overheard signals
  - signal alignment
- Information theory directs us to methods that can be used to achieve:
  - **unbreakable, provable,** and **quantifiable** (in bits/sec/hertz) security
  - irrespective of the adversary's computation power or inside knowledge
- Resulting schemes implementable by signal processing, communications and coding tech.
- We need practical solutions that can be built on top of the existing structures.