Securing Wireless Communications in the Physical Layer using Signal Processing

Şennur Ulukuş

Department of ECE

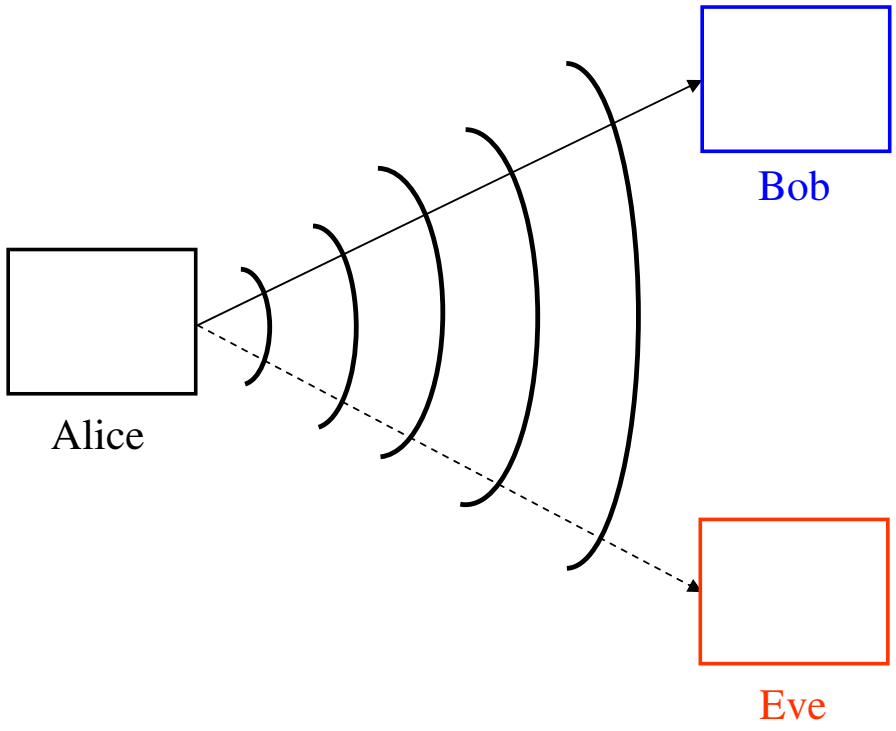
University of Maryland

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

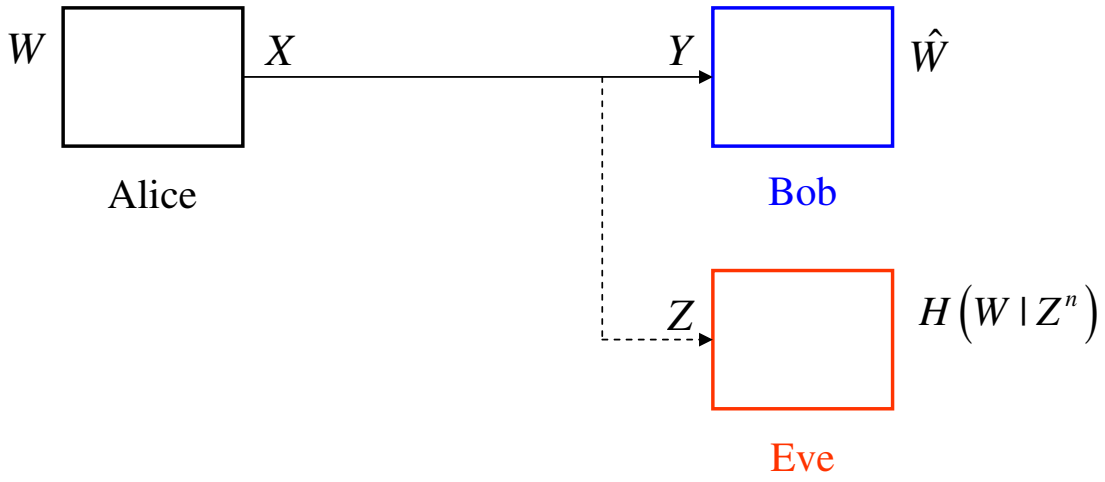


Countering Security Threats in Wireless Systems

- 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

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:

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

- Perfect secrecy when the message and Eve's observation are almost independent, i.e.,

$$H(W|Z^n) \approx H(W)$$

Capacity-Equivocation Region

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

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

- Main idea:
  - Split the message W into two coordinates, secret and public: (W_s, W_p).
  - Eve can learn W_p, but not W_s.
- Perfect secrecy when $R = R_e$.
- The maximum perfect secrecy rate, i.e., the secrecy capacity:

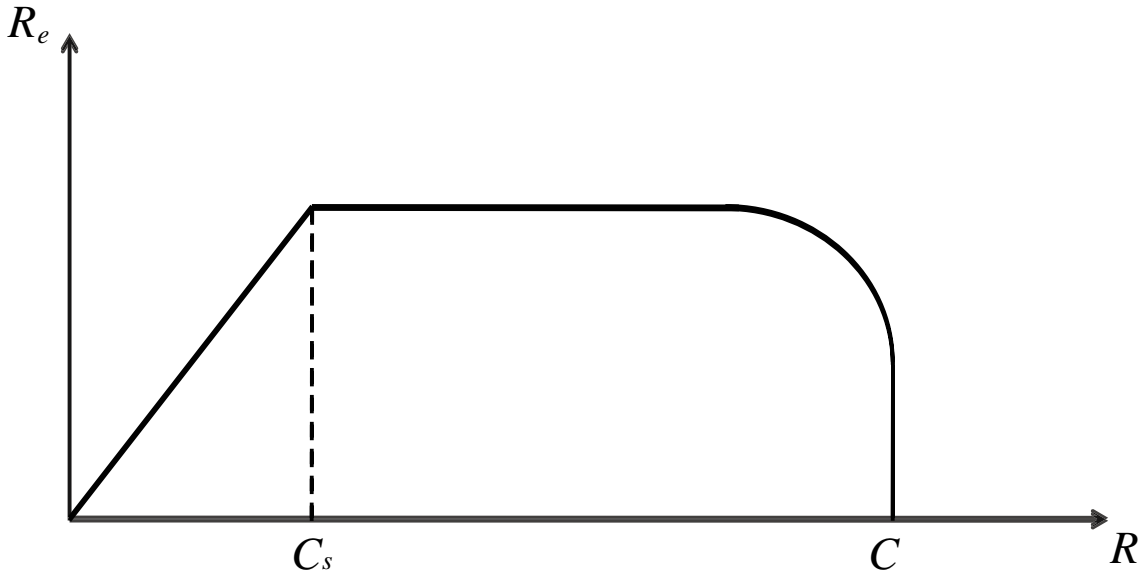
$$C_s = \max_{X \to Y \to Z} I(X;Y) - I(X;Z)$$

- Wyner's model is limited to the case when Eve's observation is strictly worse than Bob's.

Capacity-Equivocation Region

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

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



Capacity-Equivocation Region

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

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

- Main idea:
  - Split the message W into two coordinates, secret and public: (W_s, W_p).
  - Eve can learn W_p, but not W_s.
- Perfect secrecy when $R = R_e$.
- The maximum perfect secrecy rate, i.e., the secrecy capacity:

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

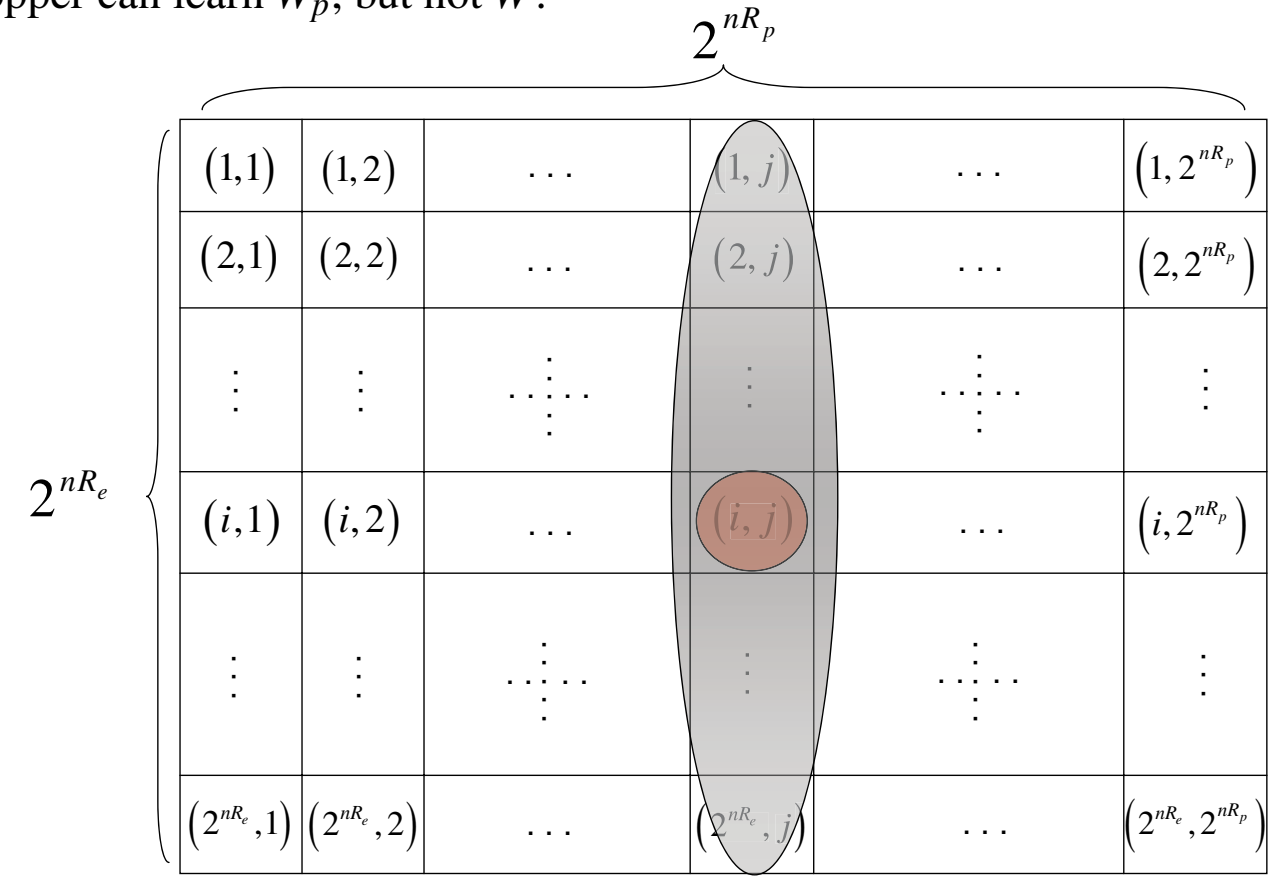
- Wyner's model is limited to the case when Eve's observation is strictly worse than Bob's.

Main Tool: Stochastic Encoding

- Each message W is associated with many codewords:

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

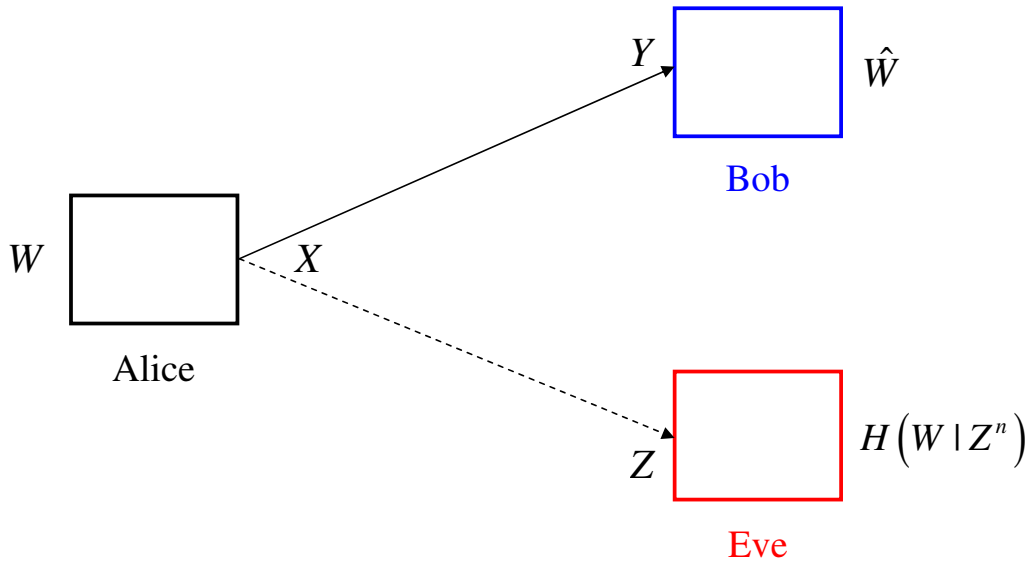
- Eavesdropper can learn W_p, but not W.



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

Broadcast Channel with Confidential Messages

- Csiszar and Korner considered the general wiretap channel in 1978.
- Eve's signal is not necessarily a degraded version of Bob's signal.



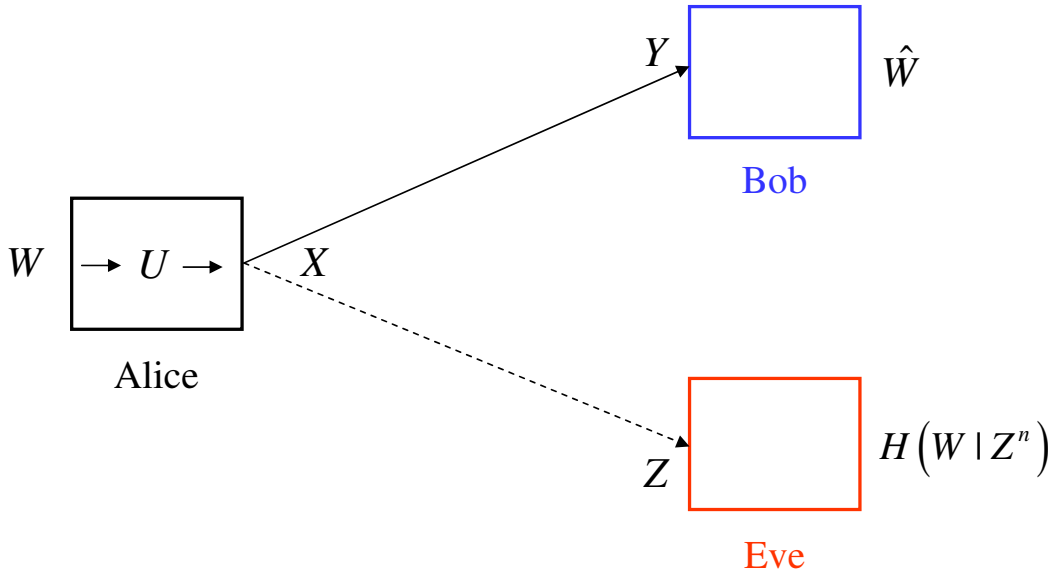
- The secrecy capacity:

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

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

Broadcast Channel with Confidential Messages

- Csiszar and Korner considered the general wiretap channel in 1978.
- Eve's signal is not necessarily a degraded version of Bob's signal.



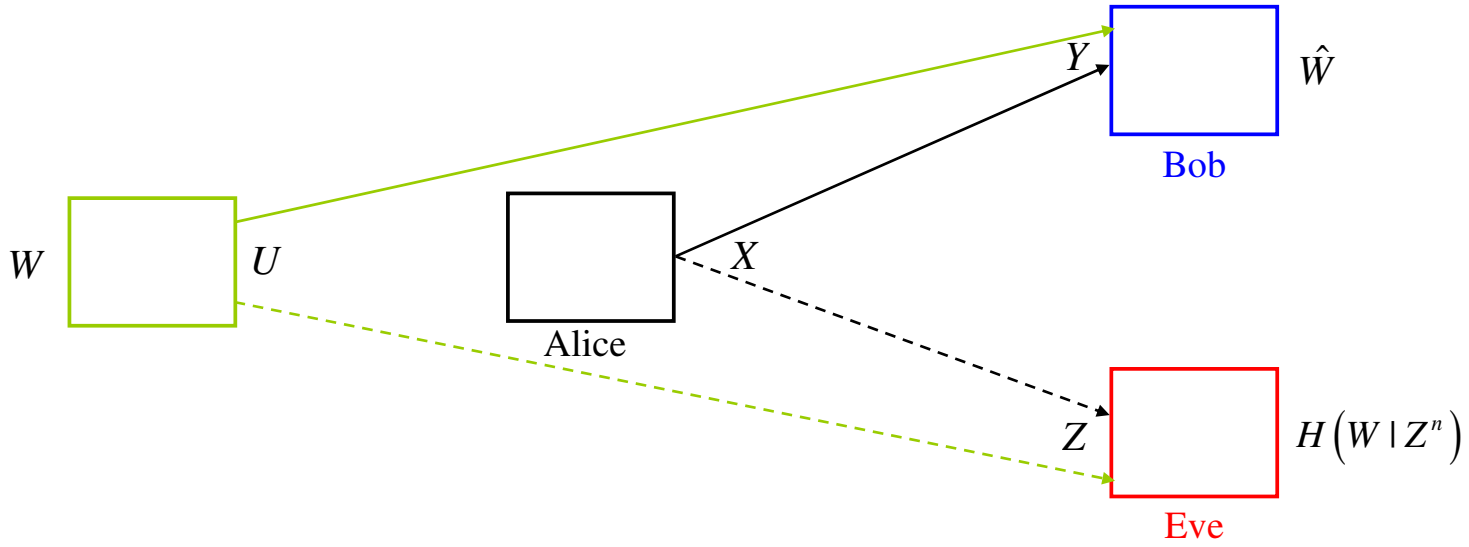
- The secrecy capacity:

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

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

Main Tool: Channel Prefixing

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

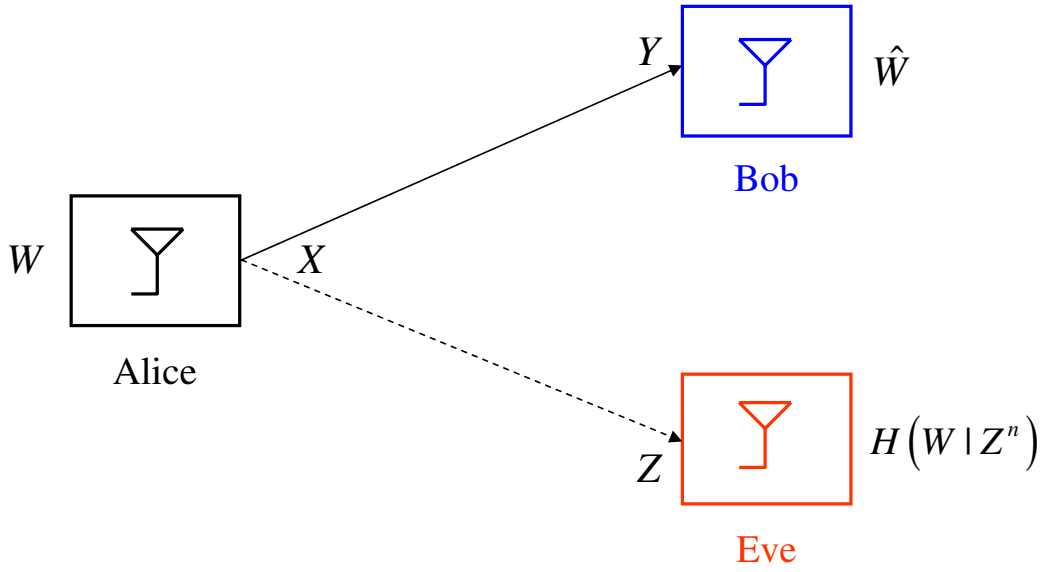


- With channel prefixing: $U \to X \to Y, Z$.
- From DPI, both mutual informations decrease, but the difference may increase.
- The secrecy capacity:

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

Gaussian Wiretap Channel

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



- Eve's signal is Bob's signal plus Gaussian noise, or vice versa: a **degraded** wiretap channel.
- No channel prefixing is necessary and Gaussian signalling is optimal.
- The secrecy capacity:

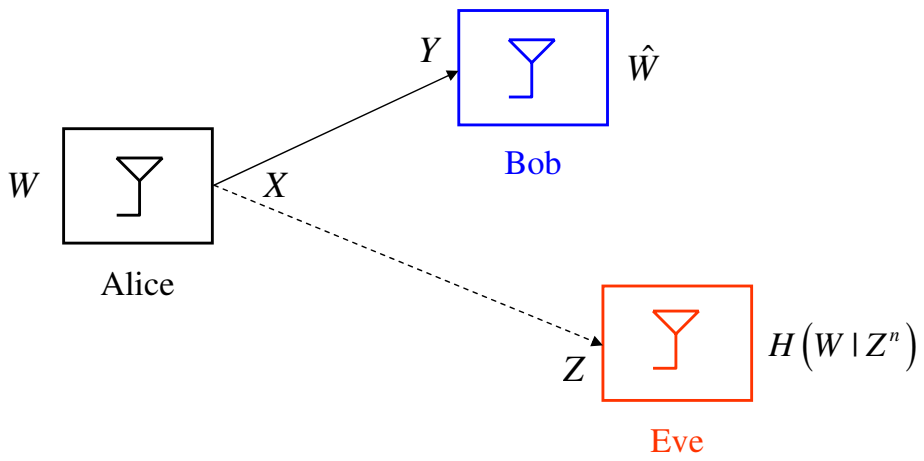
$$C_s = \max_{X \to Y \to Z} I(X;Y) - I(X;Z) = [C_B - C_E]^+$$

i.e., the difference of two capacities.

Caveat: Need Channel Advantage

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

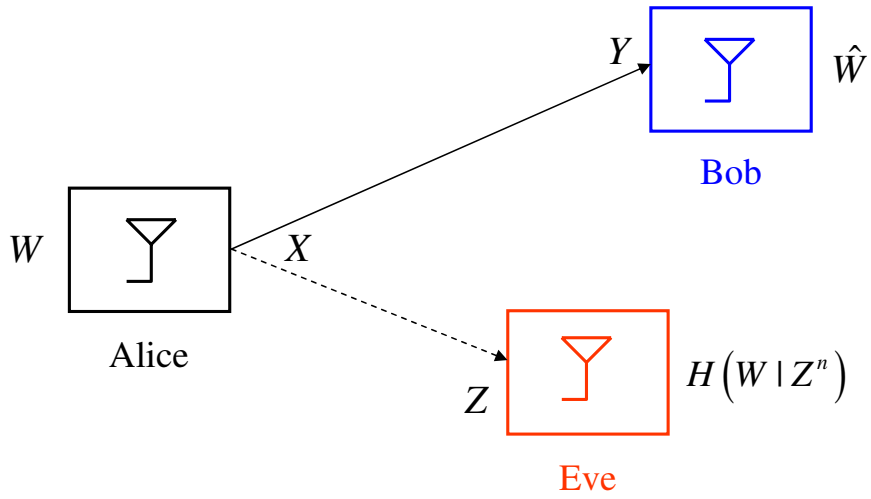
Bob's channel is better



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

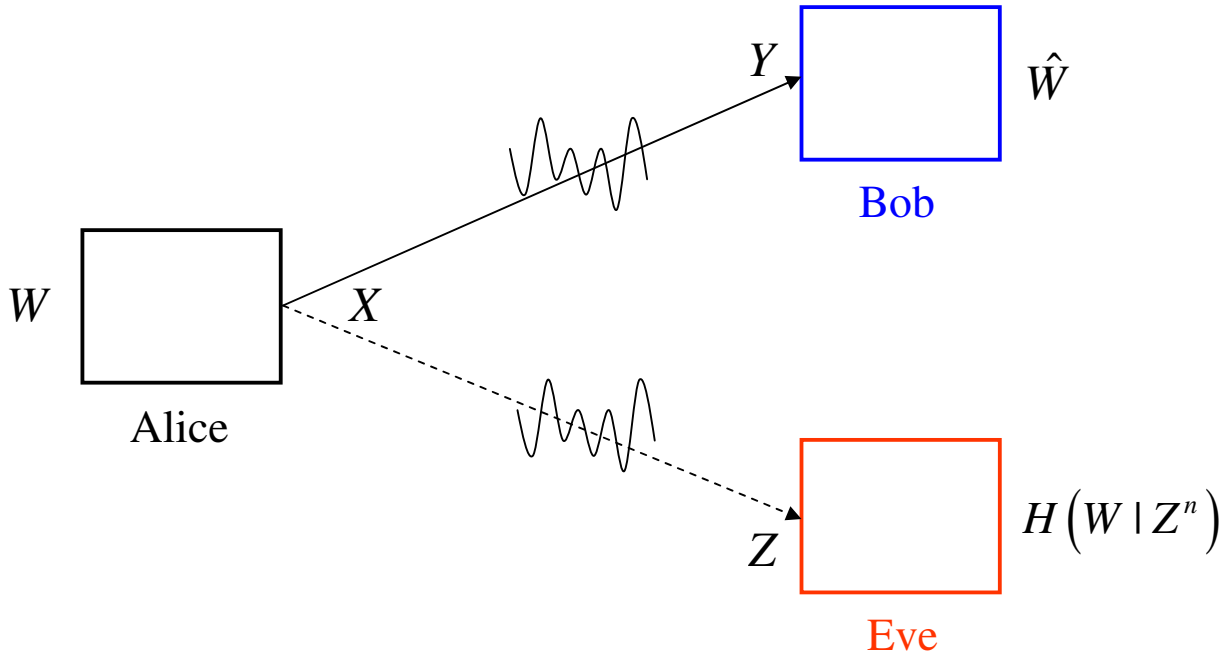
- Information theoretic secrecy is extremely powerful:
  - no limitation on Eve's computational power
  - no limitation on Eve's available information
  - yet, we are able to provide secrecy to the legitimate user
  - **unbreakable, provable,** and **quantifiable** (in bits/sec/hertz) secrecy
- We seem 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?

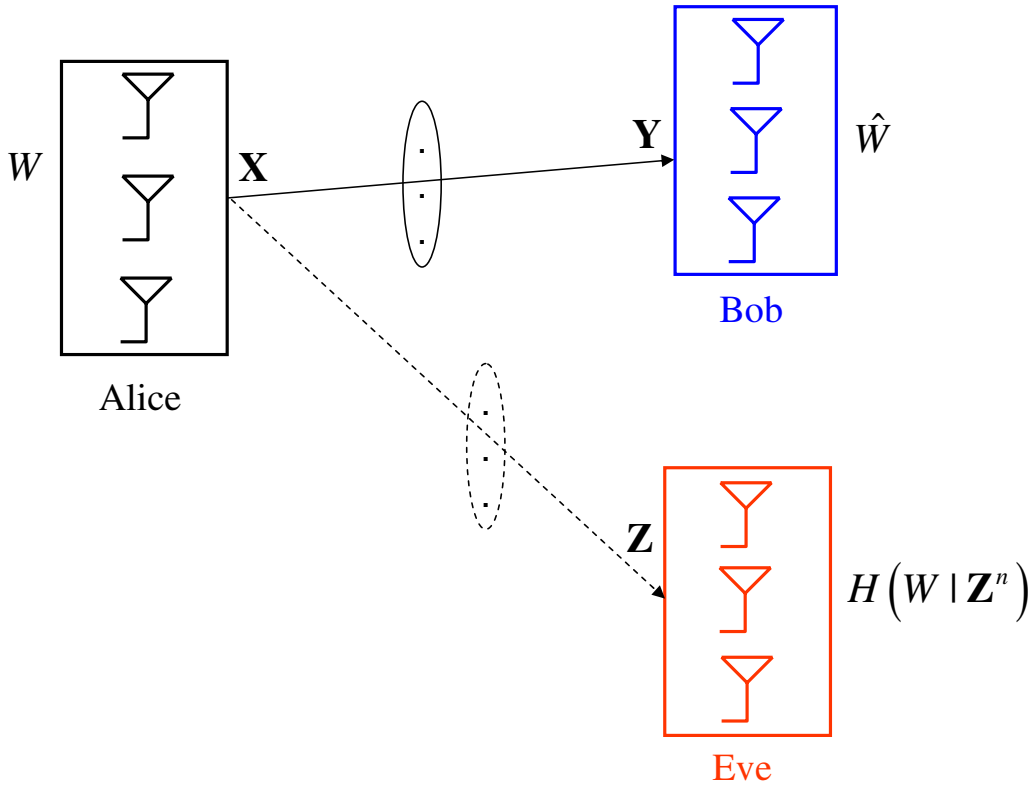


MIMO Wiretap Channel

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

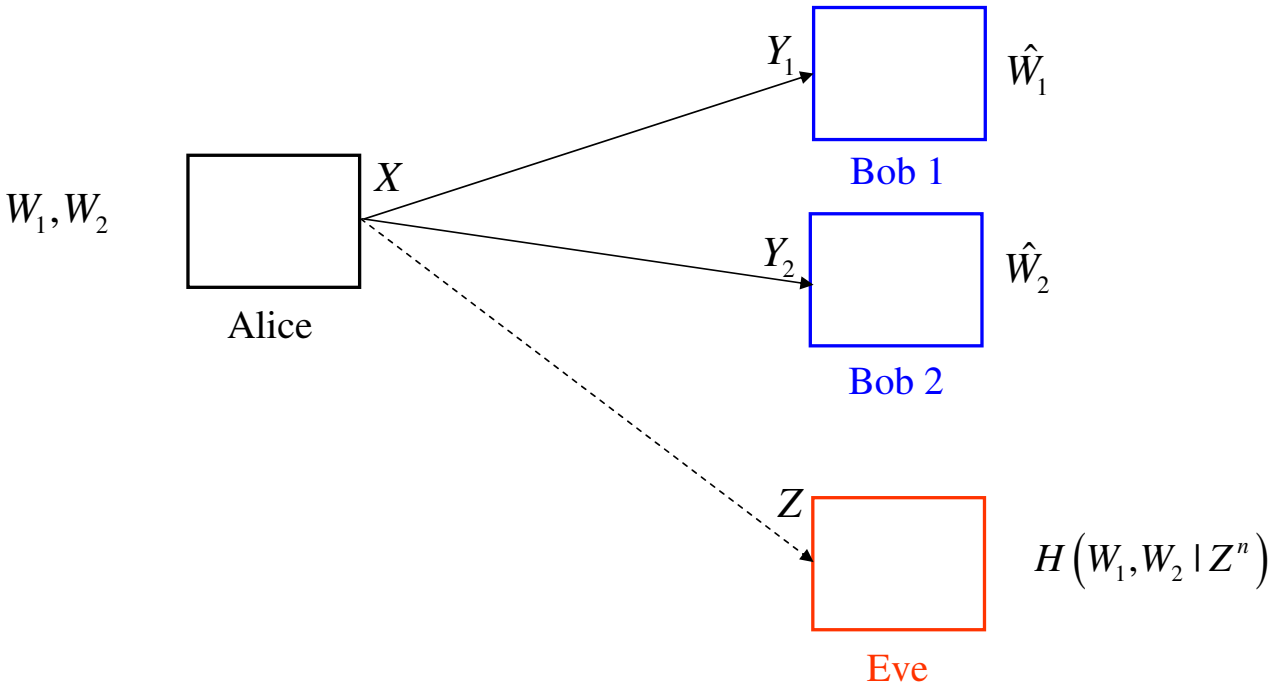
$$C_B \leq C_E$$

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



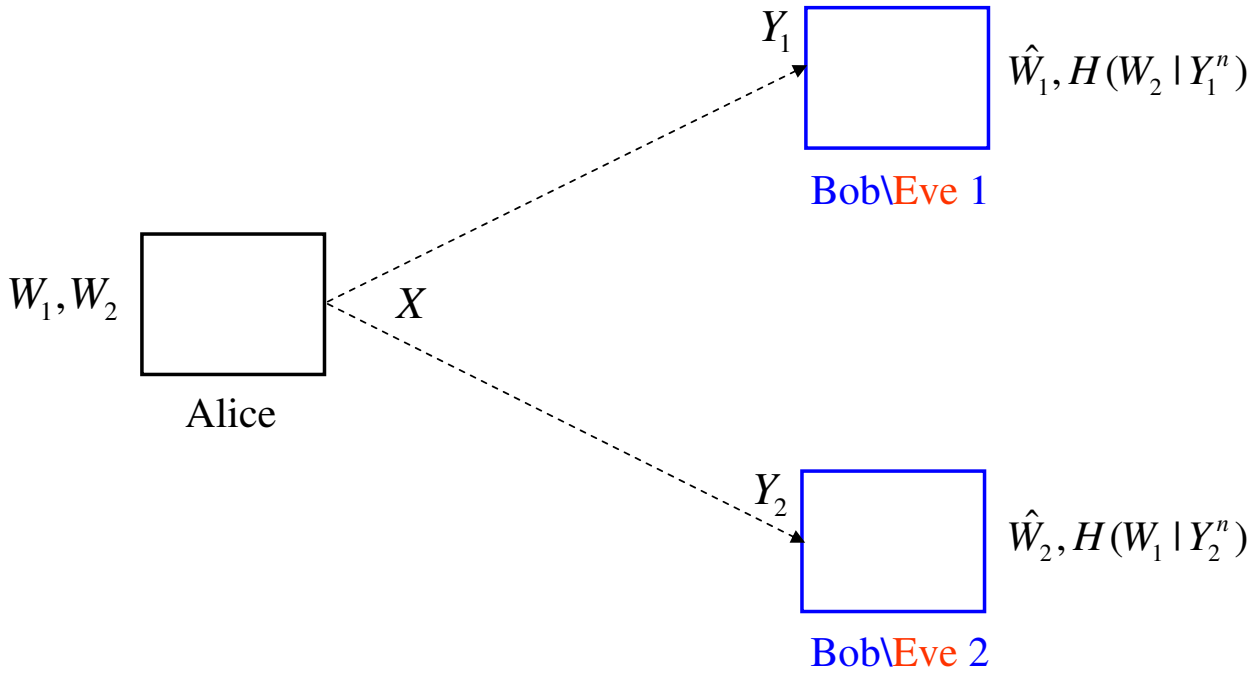
Broadcast (Downlink) Channel

- 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.



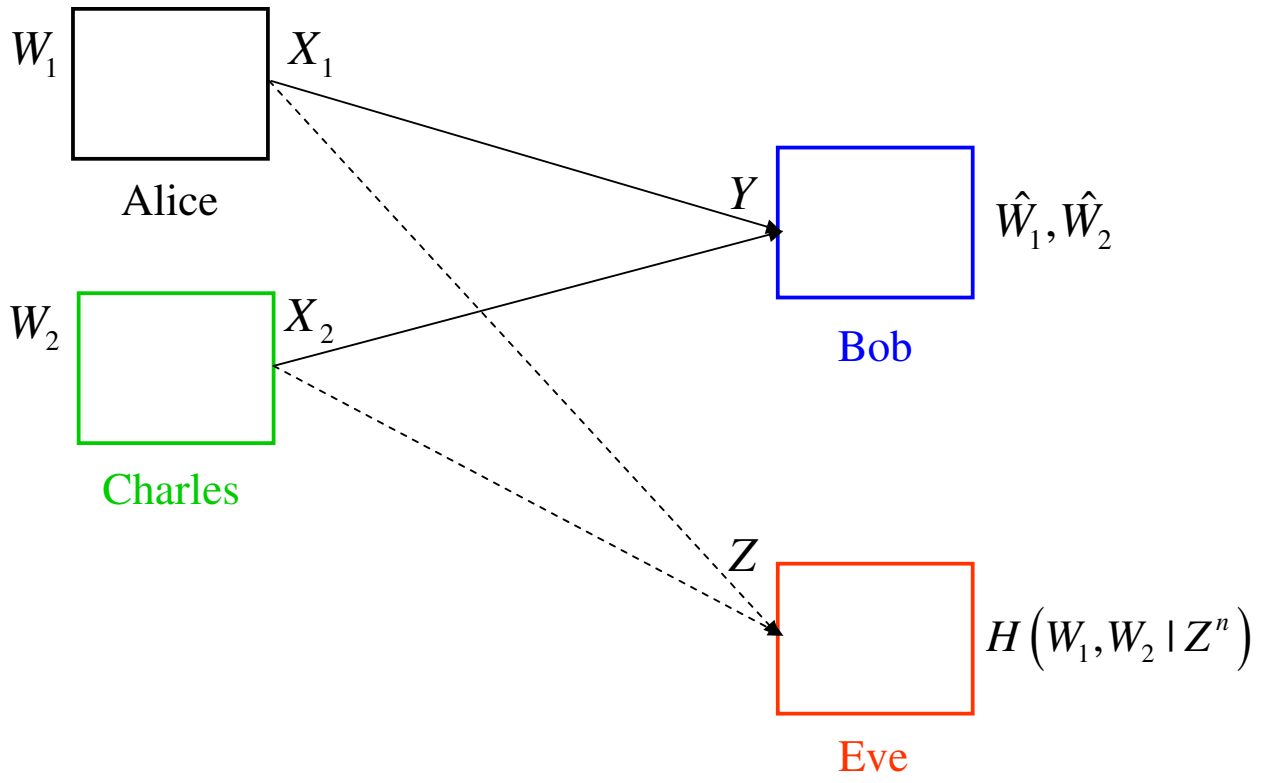
Internal Security within a System

- 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.



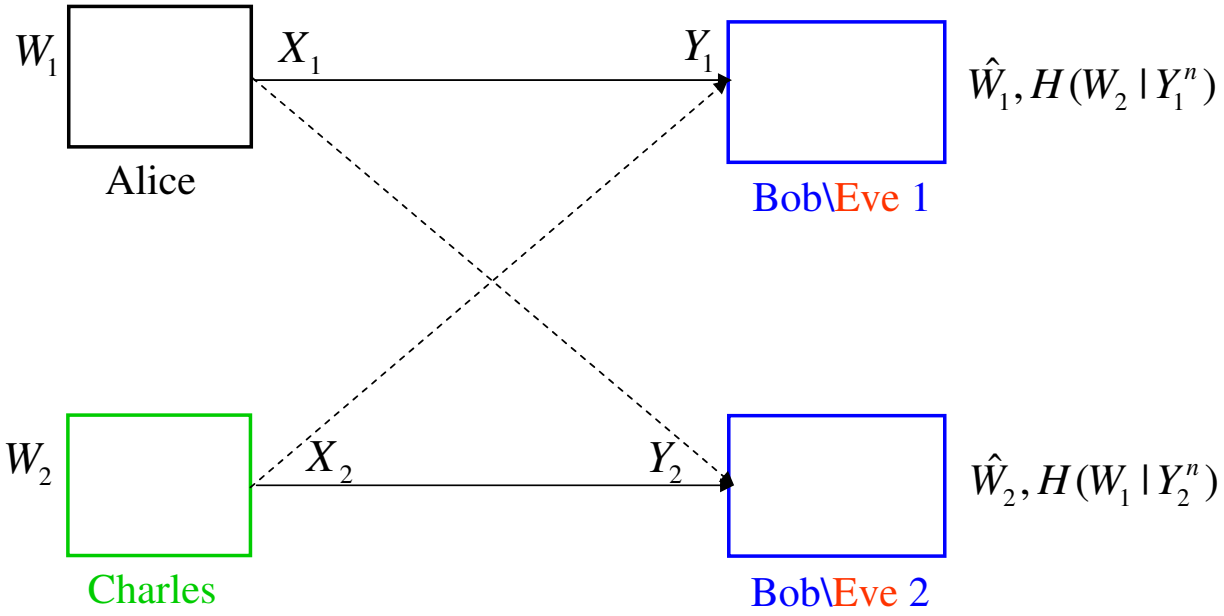
Multiple Access (Uplink) Channel

- 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.



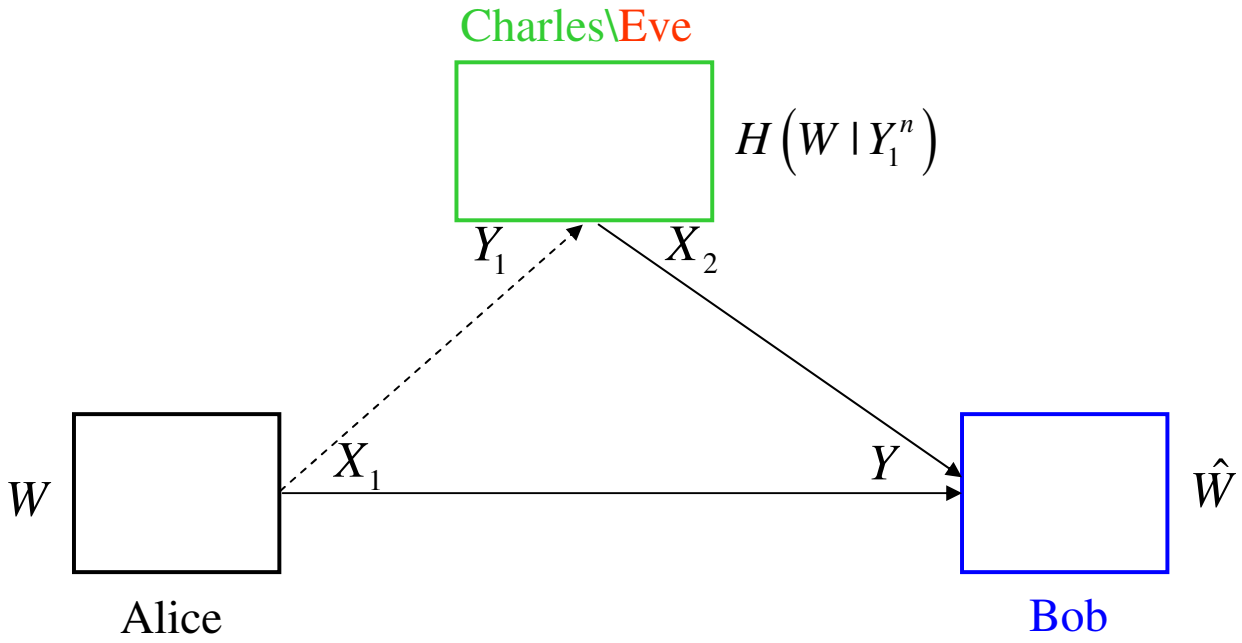
Interference as a Leakage of Information

- 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.



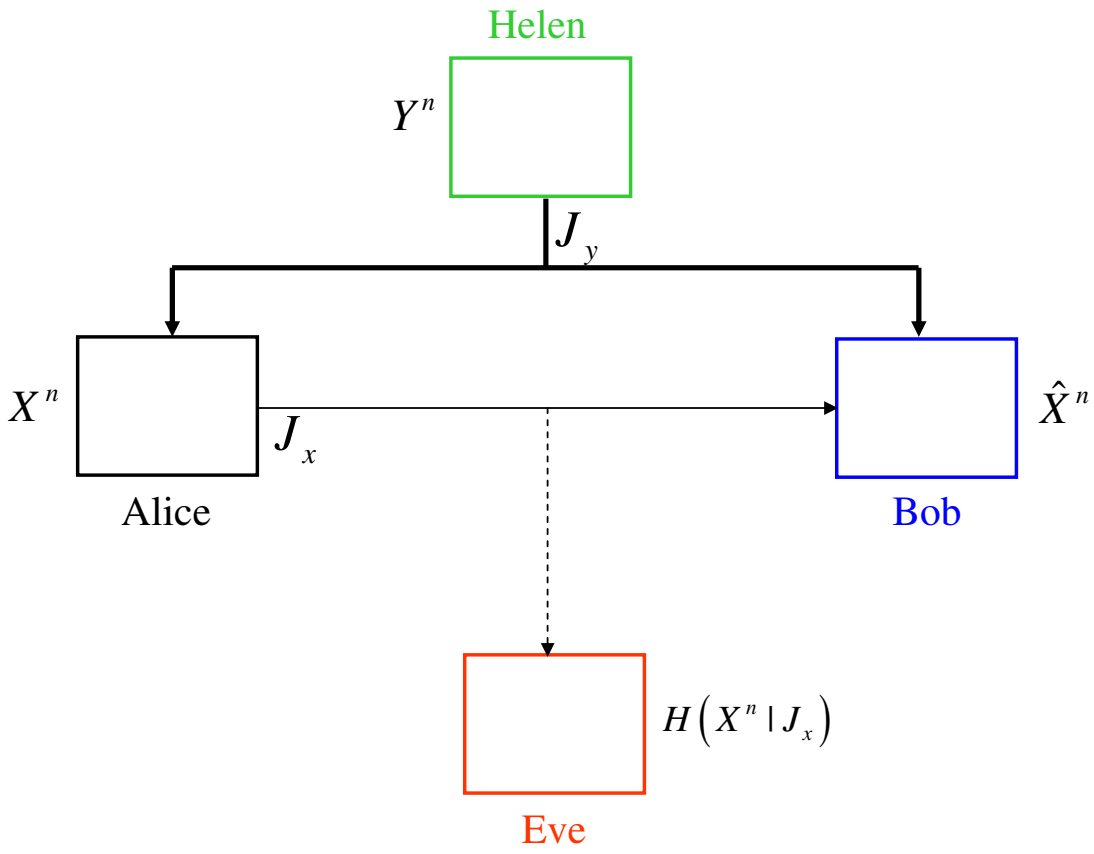
Cooperative Channels

- **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

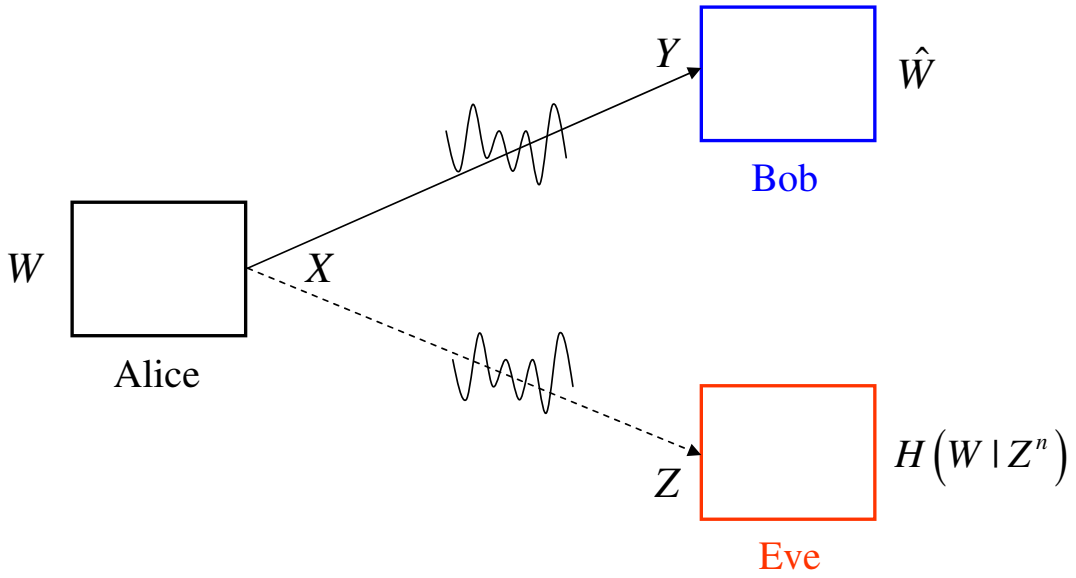
- Fading wiretap channel: Liang-Poor-Shamai, Li-Yates-Trappe, Gopala-Lai-El Gamal, Khisti-Tchamkerten-Wornell, Bloch-Barros-Rogrigues-McLaughlin, Parada-Blahut, Ekrem-Ulukus.
- Gaussian MIMO wiretap channel: Parada-Blahut, Negi-Goel, Shafiee-Ulukus, Li-Trappe-Yates, Khisti-Wornell-Wiesel-Eldar, Shafiee-Liu-Ulukus, 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

- 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.



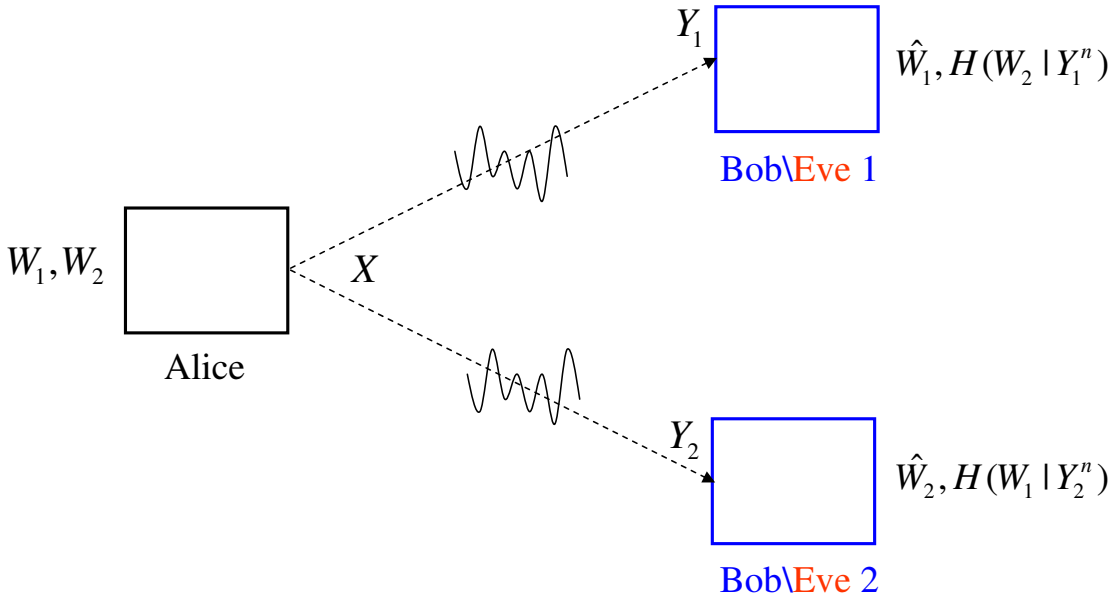
- Two scenarios for the ergodic secrecy capacity:
  - CSIT of both Bob and Eve: Liang-Poor-Shamai, Li-Yates-Trappe, Gopala-Lai-El Gamal.
  - CSIT of Bob only: Khisti-Tchamkerten-Wornell, Li-Yates-Trappe, Gopala-Lai-El Gamal.

Fading Broadcast Channel with Confidential Messages

- 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:

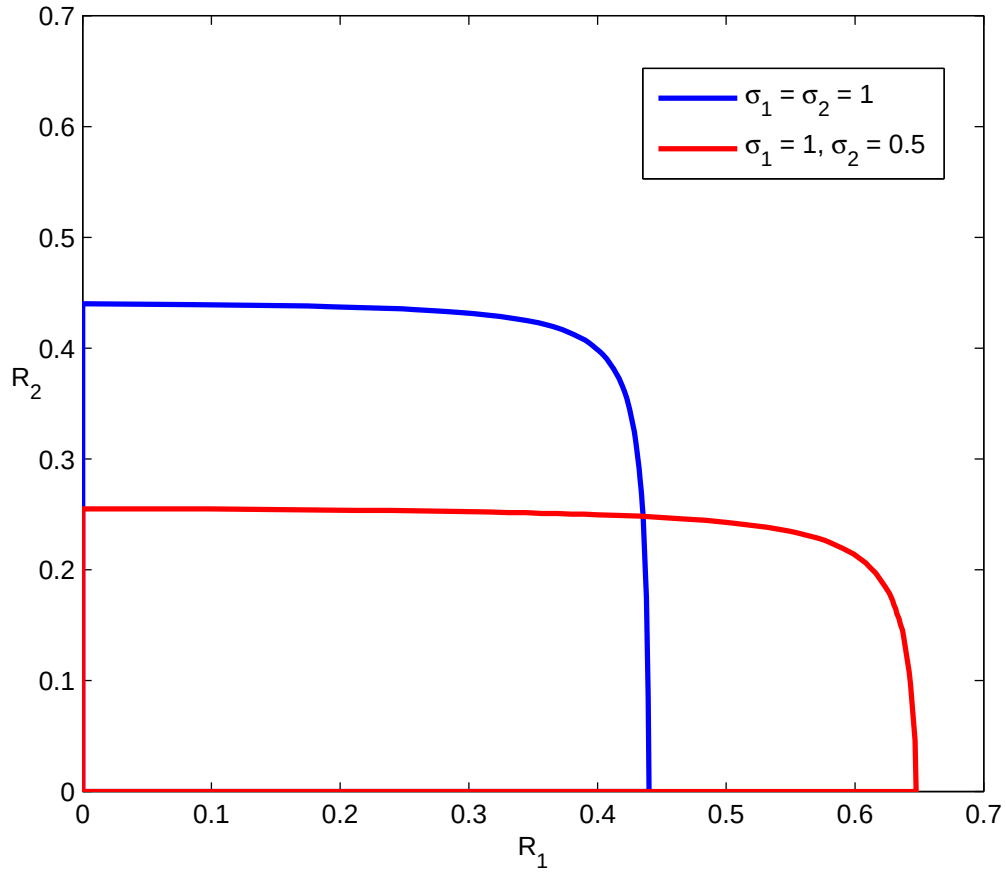
$$Y_1 = h_1 X + N_1$$
$$Y_2 = h_2 X + N_2$$

- Assume full CSIT and CSIR.



The Secrecy Capacity Region

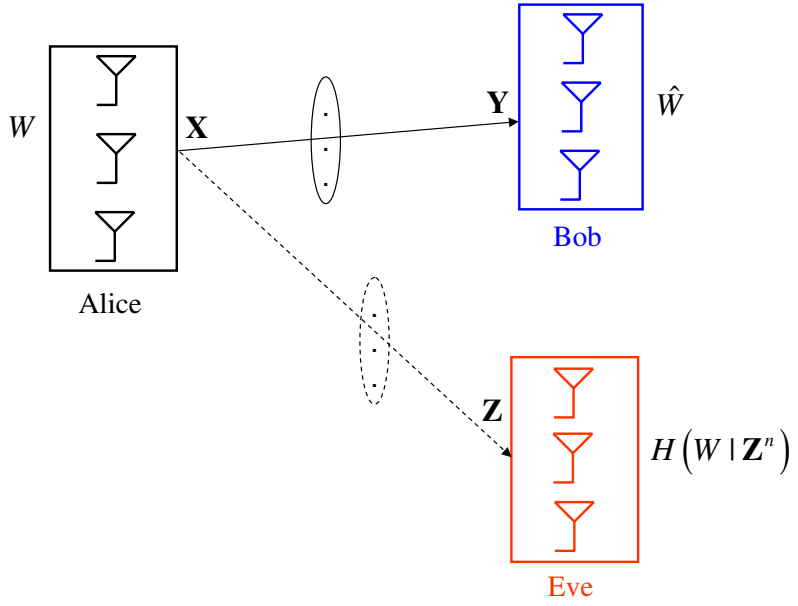
- h_1^2, h_2^2 are exponential random variables with means σ_1, σ_2, respectively.



- 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

- Multiple antennas improve reliability and rates. They improve secrecy as well.



- No channel prefixing is necessary and Gaussian signalling is optimal.
- The secrecy capacity [Shafiee-Liu-Ulukus, Khisti-Wornell, Oggier-Hassibi, Liu-Shamai]:

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

- As opposed to the SISO case, $C_S \neq C_B - C_E$.
- Tradeoff between the rate and its equivocation.

Gaussian MIMO Wiretap Channel – Finding the Capacity

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

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

- MIMO wiretap channel is not degraded in general.
  - Therefore, $U = \mathbf{X}$ is potentially suboptimal.
- There is no general methodology to solve this optimization problem, i.e., find optimal $(U,\mathbf{X})$.
- The approach used by [Shafiee-Liu-Ulukus, Khisti-Wornell, Oggier-Hassibi]:
  - Compute an achievable secrecy rate by using a potentially suboptimal $(U,\mathbf{X})$:
    - Jointly Gaussian $(U,\mathbf{X})$ 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:

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

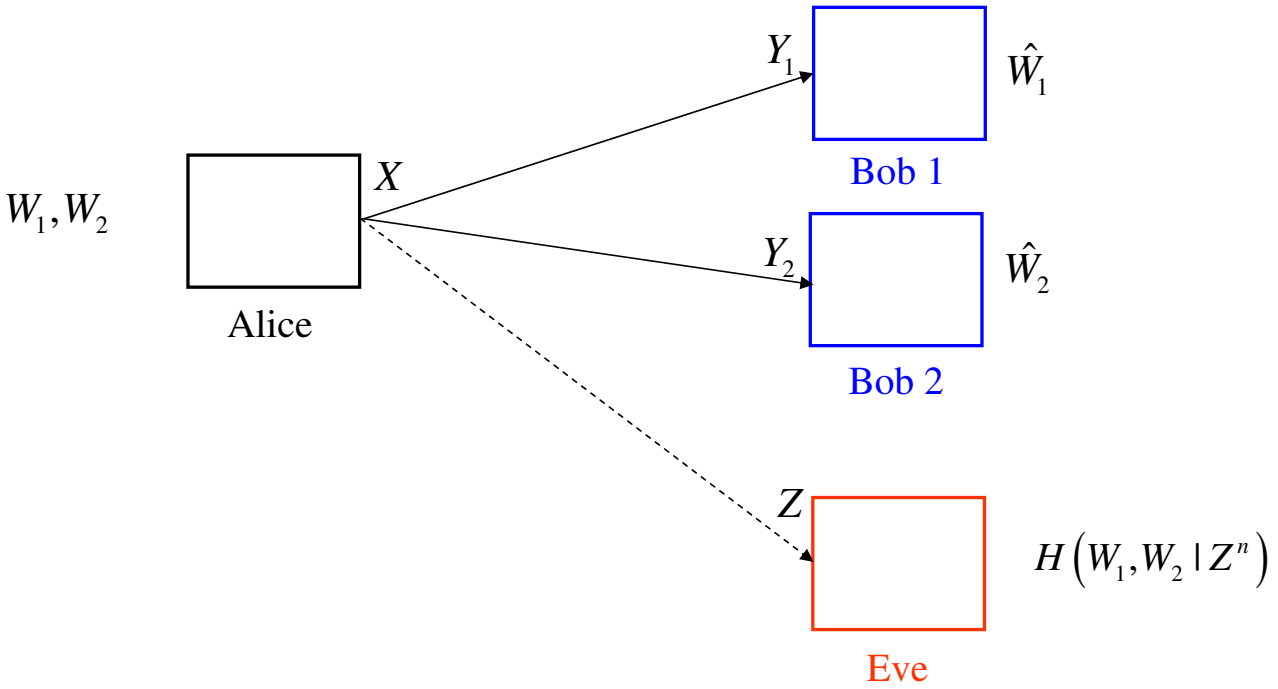
  - And, optimal $\mathbf{X}$ is Gaussian.
- This outer bound can be tightened:
  - The secrecy capacity is the same for channels having the same marginal distributions
  - We can correlate the receiver noises.
- The tightened outer bound is:

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

  where the minimization is over all noise correlations.
- The outer bound so developed matches the achievable rate.

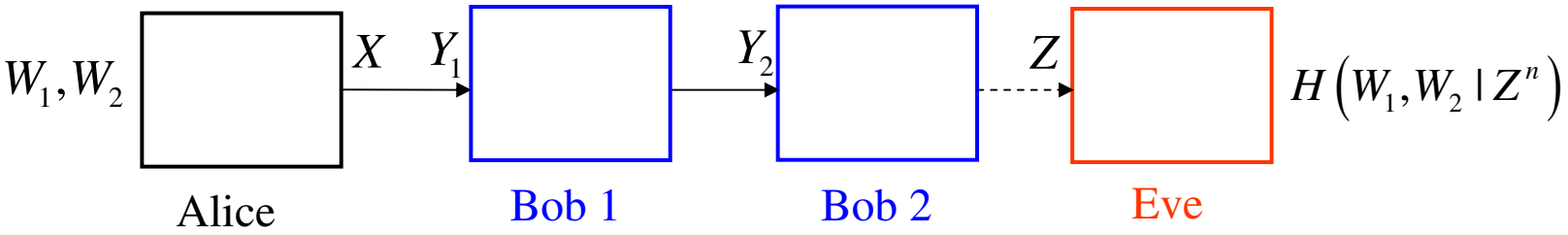
Broadcast Channel with an External Eavesdropper

- 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.



Degraded Broadcast Channel with an External Eavesdropper

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



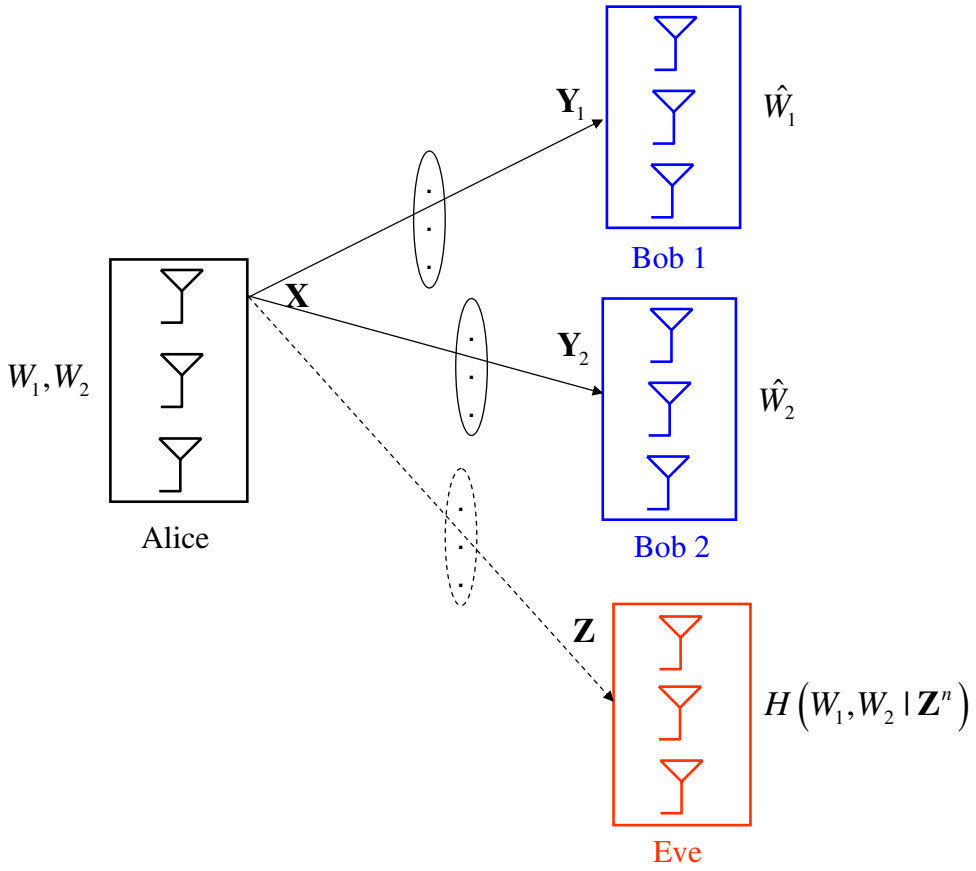
- Gaussian multi-receiver wiretap channel is an instance of this channel model.
- Plays a significant role in the Gaussian MIMO multi-receiver wiretap channel.
- The secrecy capacity region is obtained by Bagherikaram-Motahari-Khandani for $K = 2$ and by Ekrem-Ulukus for arbitrary K.

Gaussian MIMO Multi-receiver Wiretap Channel

- Channel model:

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

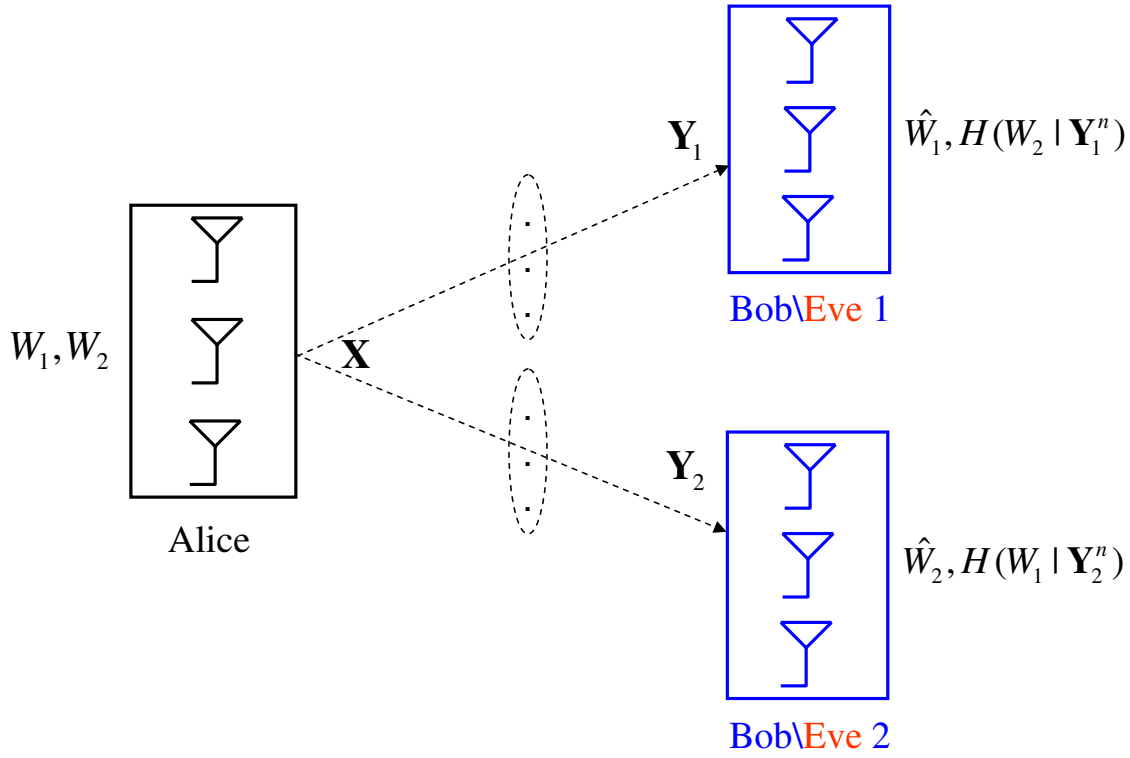
$$\mathbf{Z} = \mathbf{H}_Z\mathbf{X} + \mathbf{N}_Z$$



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

Gaussian MIMO Broadcast Channel with Confidential Messages

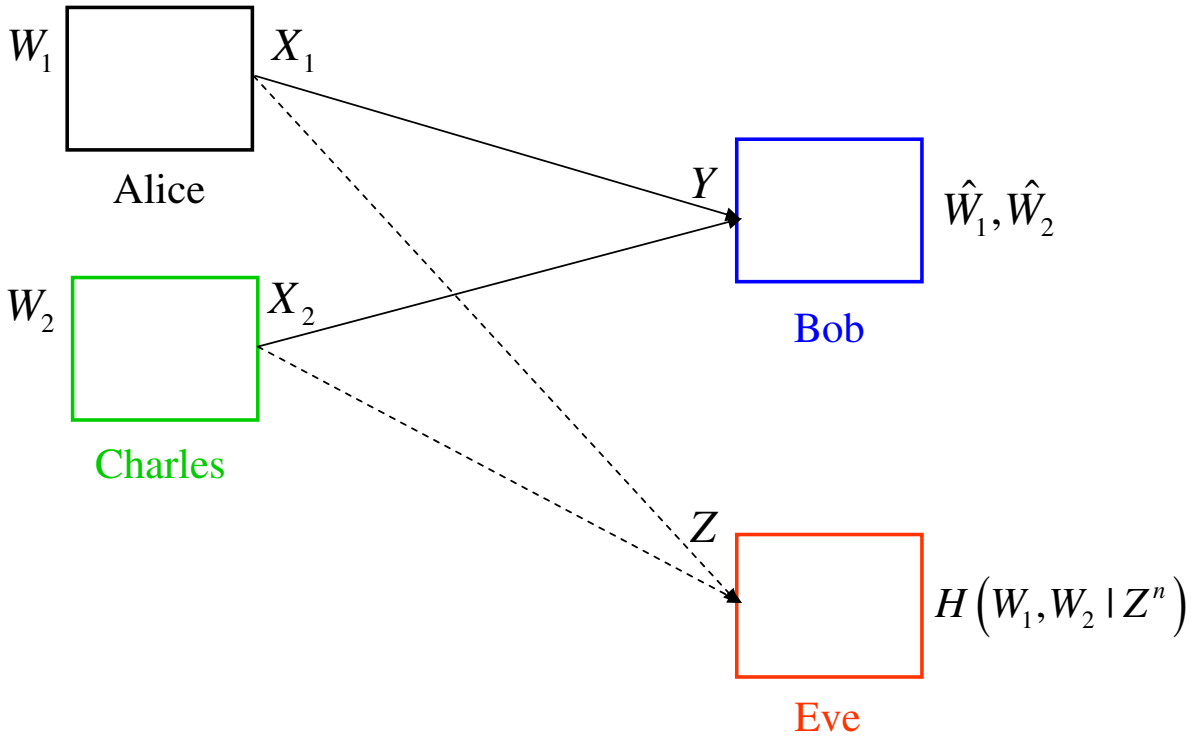
- Each user eavesdrops the other user:



- 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].

Multiple Access Wiretap Channel

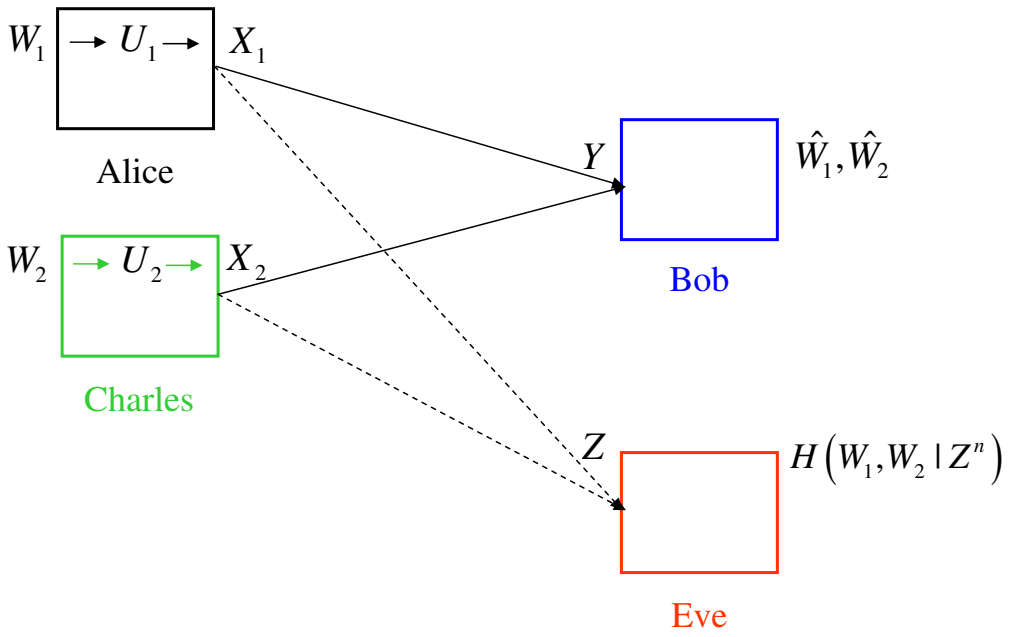
- An external eavesdropper listens in on the communication from end-users to the base station.



- 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.



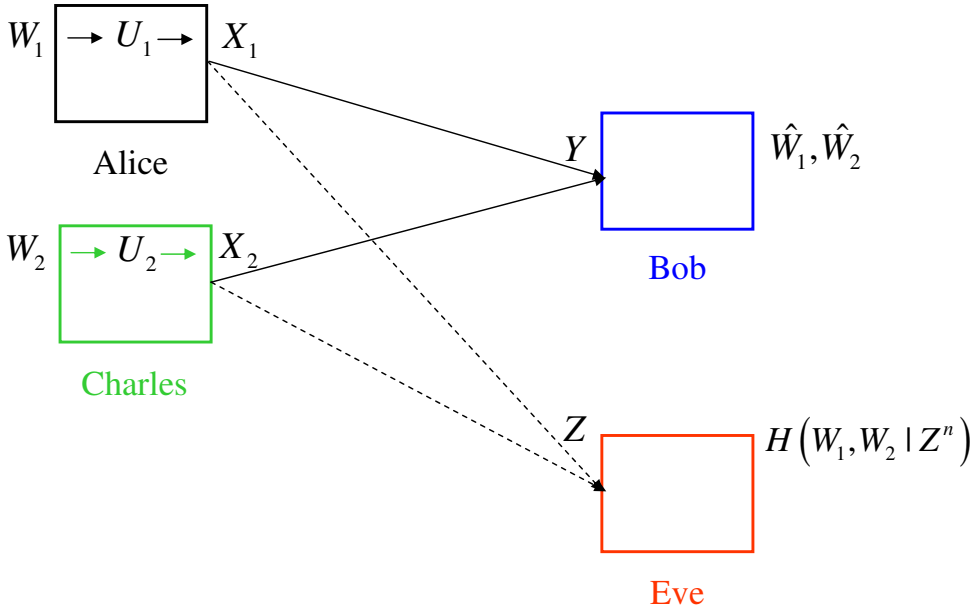
- An achievable secrecy rate region with channel pre-fixing:

$$
\begin{aligned}
R_1 &\leq I(U_1;Y|U_2) - I(U_1;Z) \\
R_2 &\leq I(U_2;Y|U_1) - I(U_2;Z) \\
R_1 + R_2 &\leq I(U_1,U_2;Y) - I(U_1,U_2;Z)
\end{aligned}
$$

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:

$$R_1 \leq \frac{1}{2}\log(1+h_1P_1) - \frac{1}{2}\log\left(1+\frac{g_1P_1}{1+g_2P_2}\right)$$

$$R_2 \leq \frac{1}{2}\log(1+h_2P_2) - \frac{1}{2}\log\left(1+\frac{g_2P_2}{1+g_1P_1}\right)$$

$$R_1+R_2 \leq \frac{1}{2}\log(1+h_1P_1+h_2P_2) - \frac{1}{2}\log(1+g_1P_1+g_2P_2)$$

- 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:

$$R_1 \leq \frac{1}{2}\log\left(1+\frac{h_1P_1}{1+h_1Q_1+h_2Q_2}\right)-\frac{1}{2}\log\left(1+\frac{g_1P_1}{1+g_1Q_1+g_2(P_2+Q_2)}\right)$$

$$R_2 \leq \frac{1}{2}\log\left(1+\frac{h_2P_2}{1+h_1Q_1+h_2Q_2}\right)-\frac{1}{2}\log\left(1+\frac{g_2P_2}{1+g_1(P_1+Q_1)+g_2Q_2}\right)$$

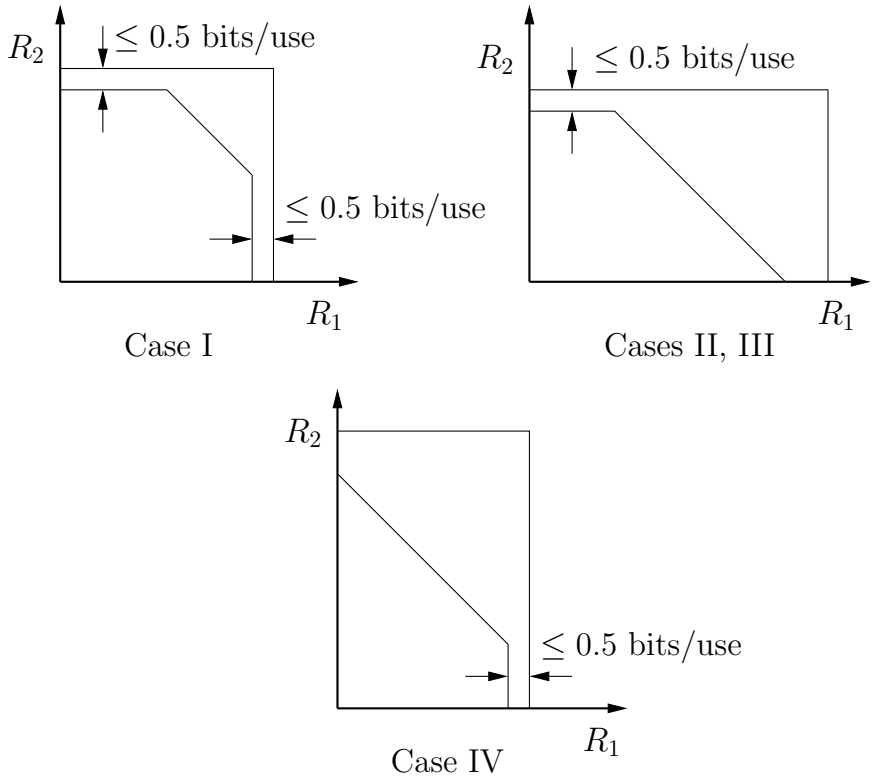
$$R_1+R_2 \leq \frac{1}{2}\log\left(1+\frac{h_1P_1+h_2P_2}{1+h_1Q_1+h_2Q_2}\right)-\frac{1}{2}\log\left(1+\frac{g_1P_1+g_2P_2}{1+g_1Q_1+g_2Q_2}\right)$$

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

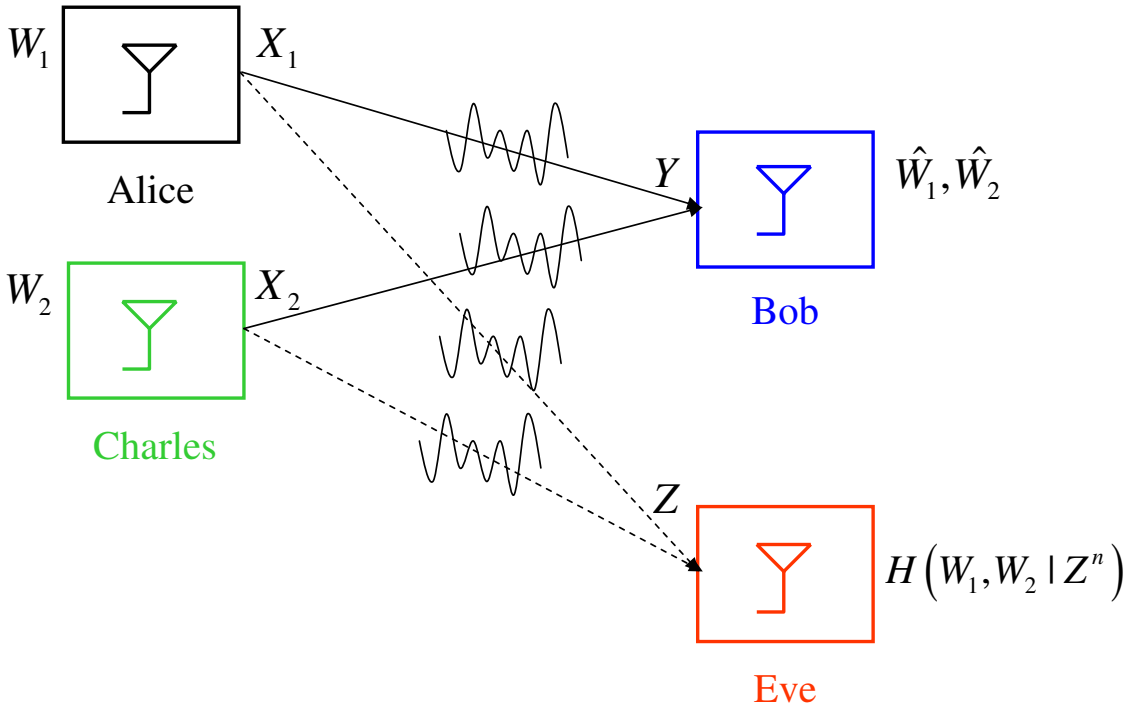
- For the weak eavesdropper case, Gaussian signalling is nearly optimal [Ekrem-Ulukus].



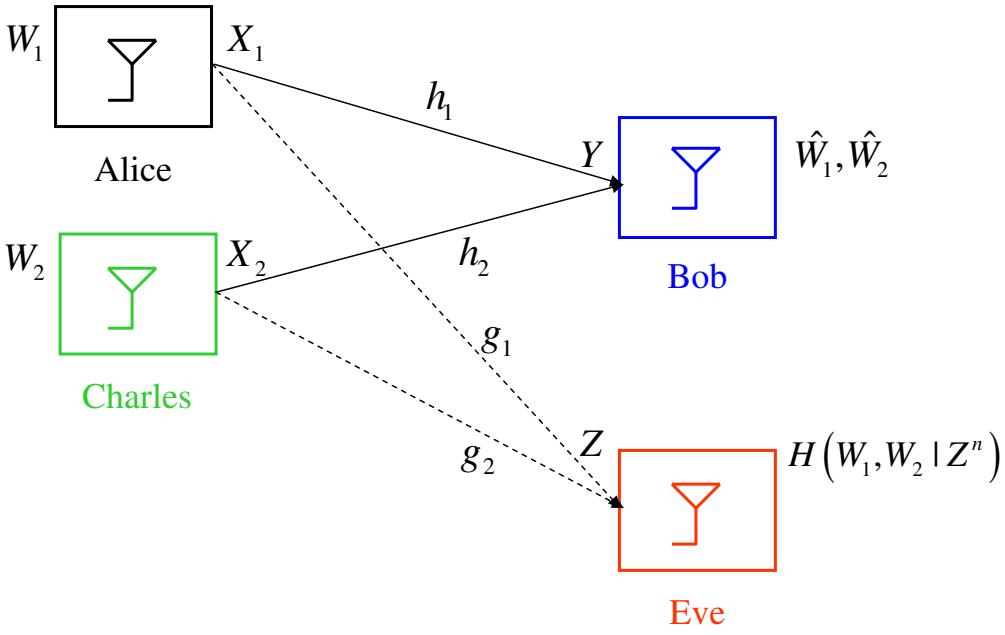
- In general, Gaussian signalling is not optimal:
  - He-Yener showed that structured codes (e.g., lattice codes) outperform Gaussian codes.
  - Structured codes can provide secrecy rates that scale with $\log \mathrm{SNR}$.
- The secrecy capacity of the multiple access wiretap channel is still open.

Fading Multiple Access Wiretap Channel

- Introduced by Tekin-Yener in 2007.
- They provide achievable secrecy rates based on Gaussian signalling.
- These rates (with our without cooperative jamming) do not scale with SNR.



Scaling Based Alignment (SBA) – Introduction

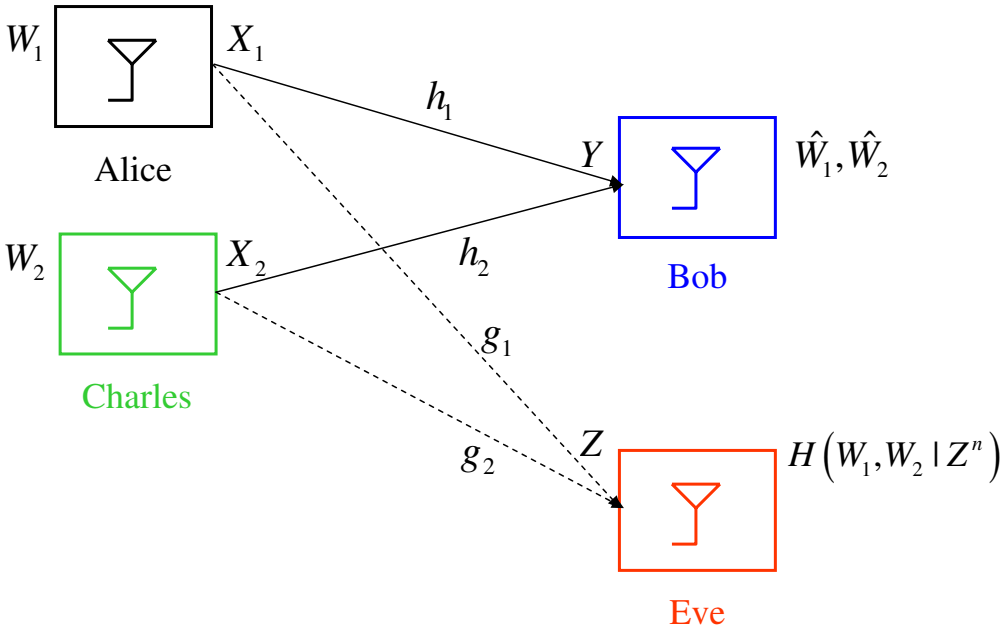


$$Y = h_1 X_1 + h_2 X_2 + N$$

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

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.

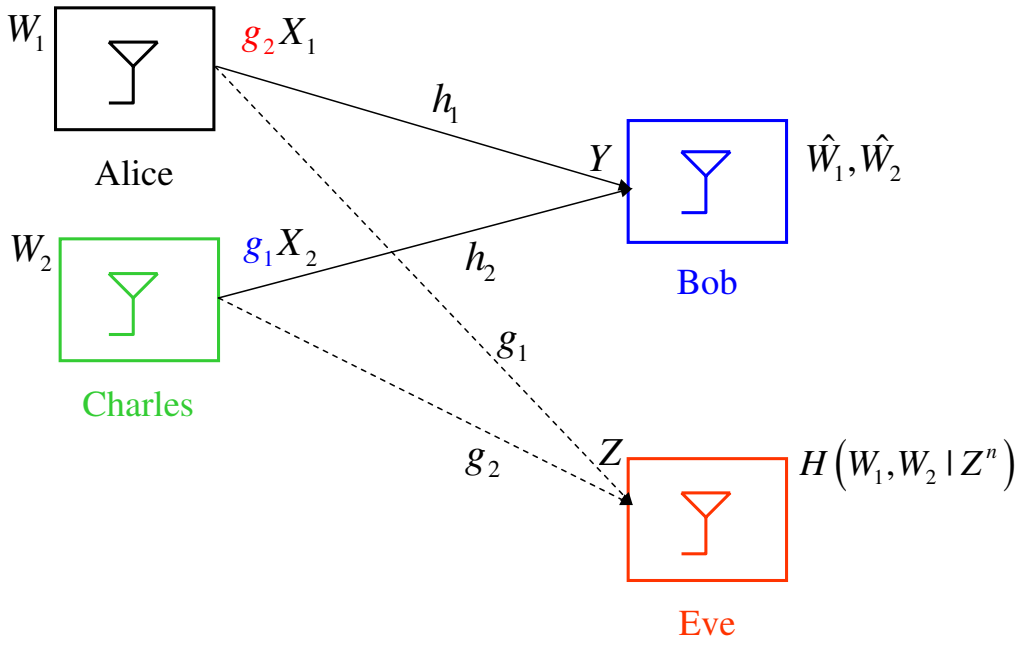


$$Y = h_1 X_1 + h_2 X_2 + N$$

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

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.

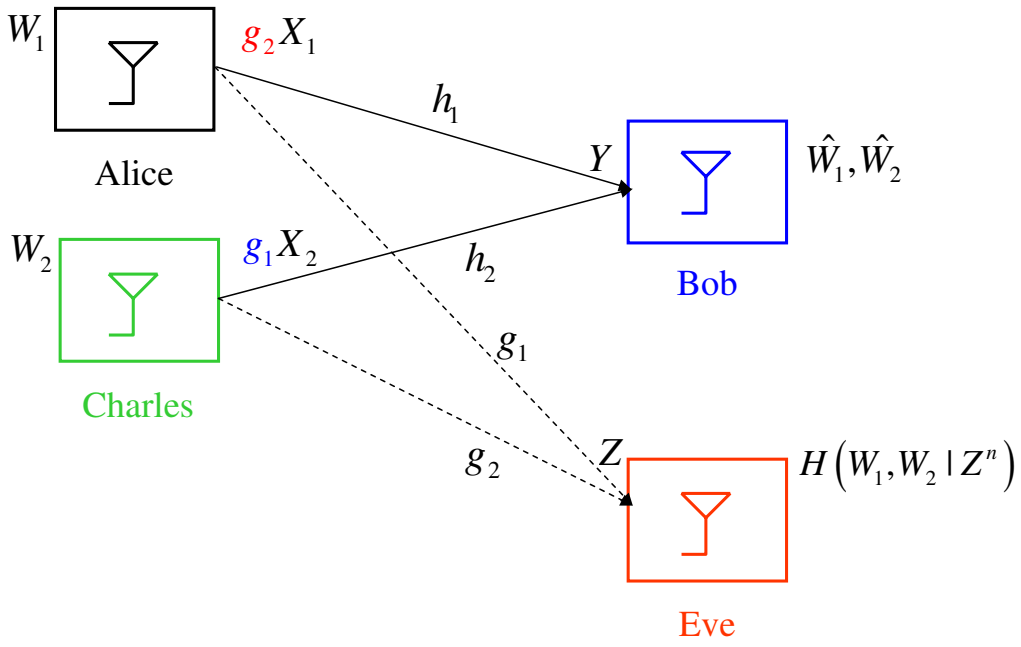


$$Y = h_1 g_2 X_1 + h_2 g_1 X_2 + N$$

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

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.

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,

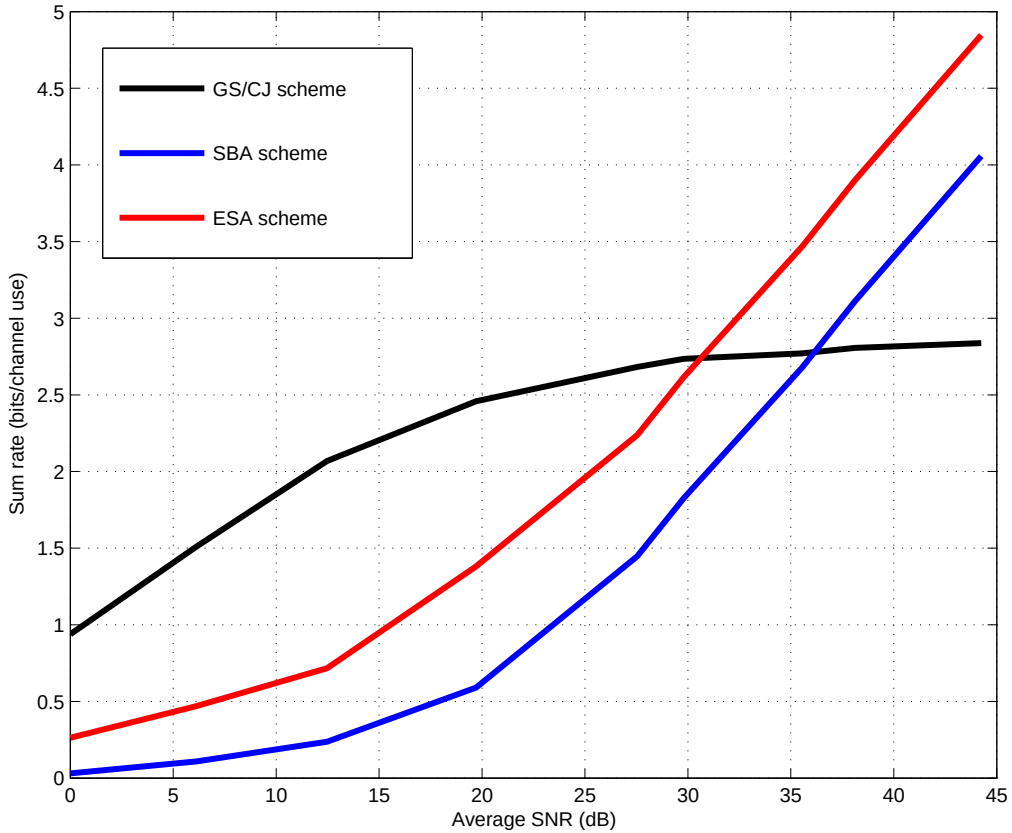
$$\begin{pmatrix} Y_{t_1} \\ Z_{t_1} \end{pmatrix} = \begin{pmatrix} h_1 & h_2 \\ g_1 & g_2 \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \end{pmatrix} + \begin{pmatrix} N_{t_1} \\ N'_{t_1} \end{pmatrix}$$

- 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.

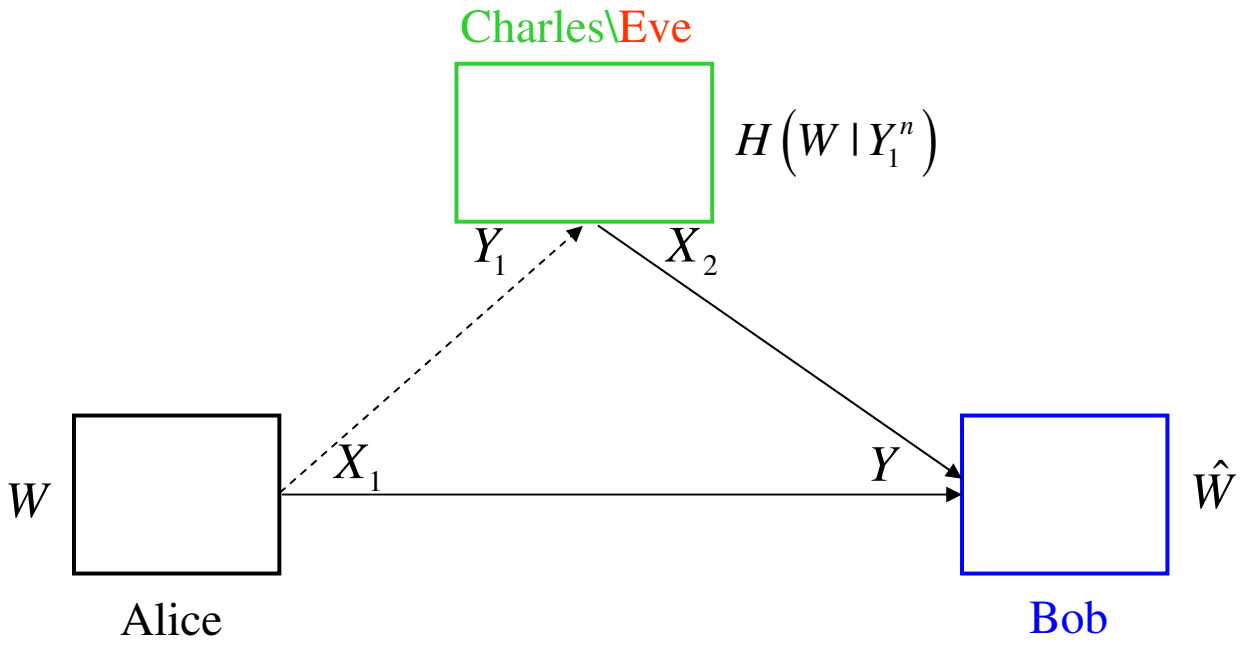
Fading Multiple Access Wiretap Channel – Achievable Rates



- 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?



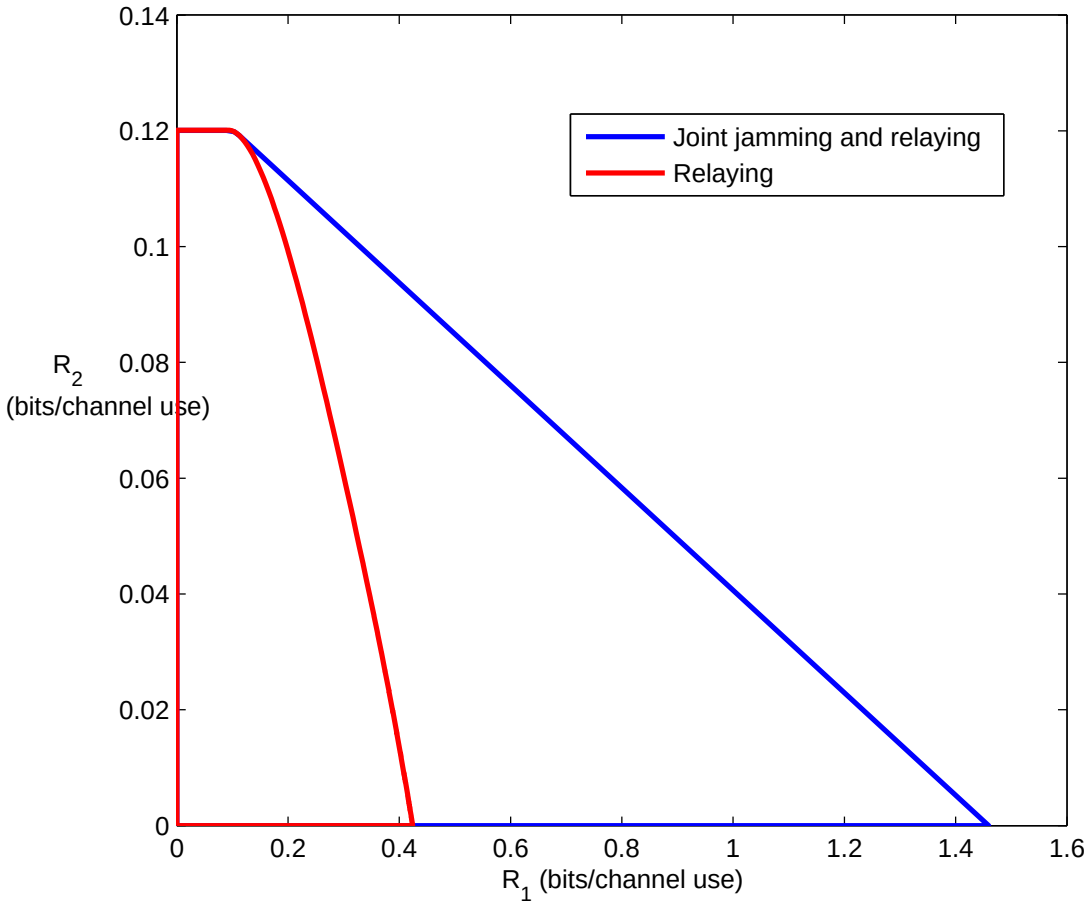
- Relay channel [He-Yener].
- Cooperative broadcast and cooperative multiple access channels [Ekrem-Ulukus].

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:

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

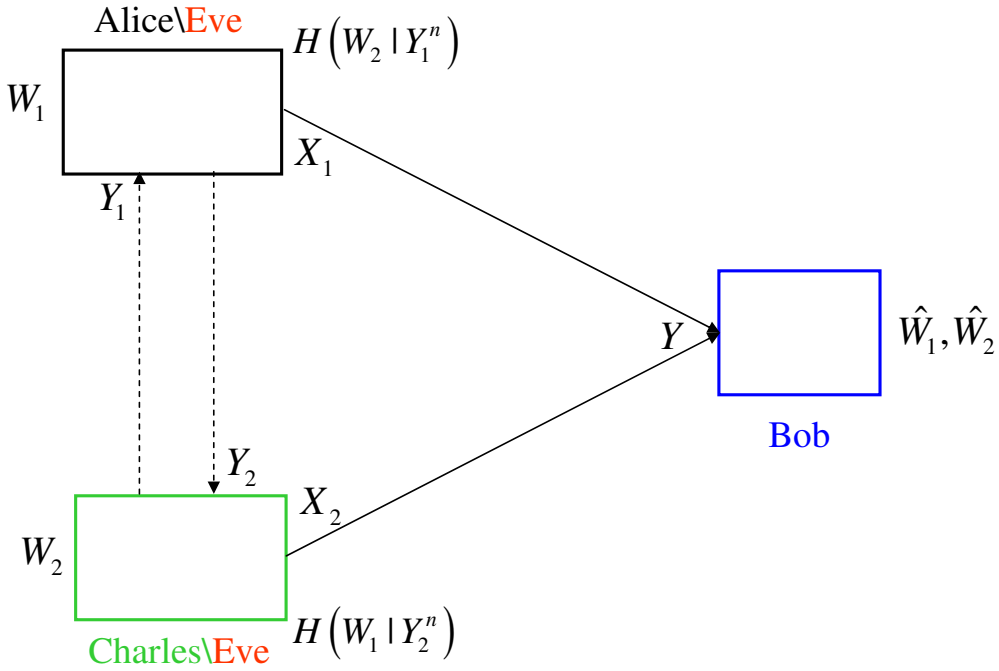
Example: Gaussian Relay Broadcast Channel (Charles is Stronger)



- 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.

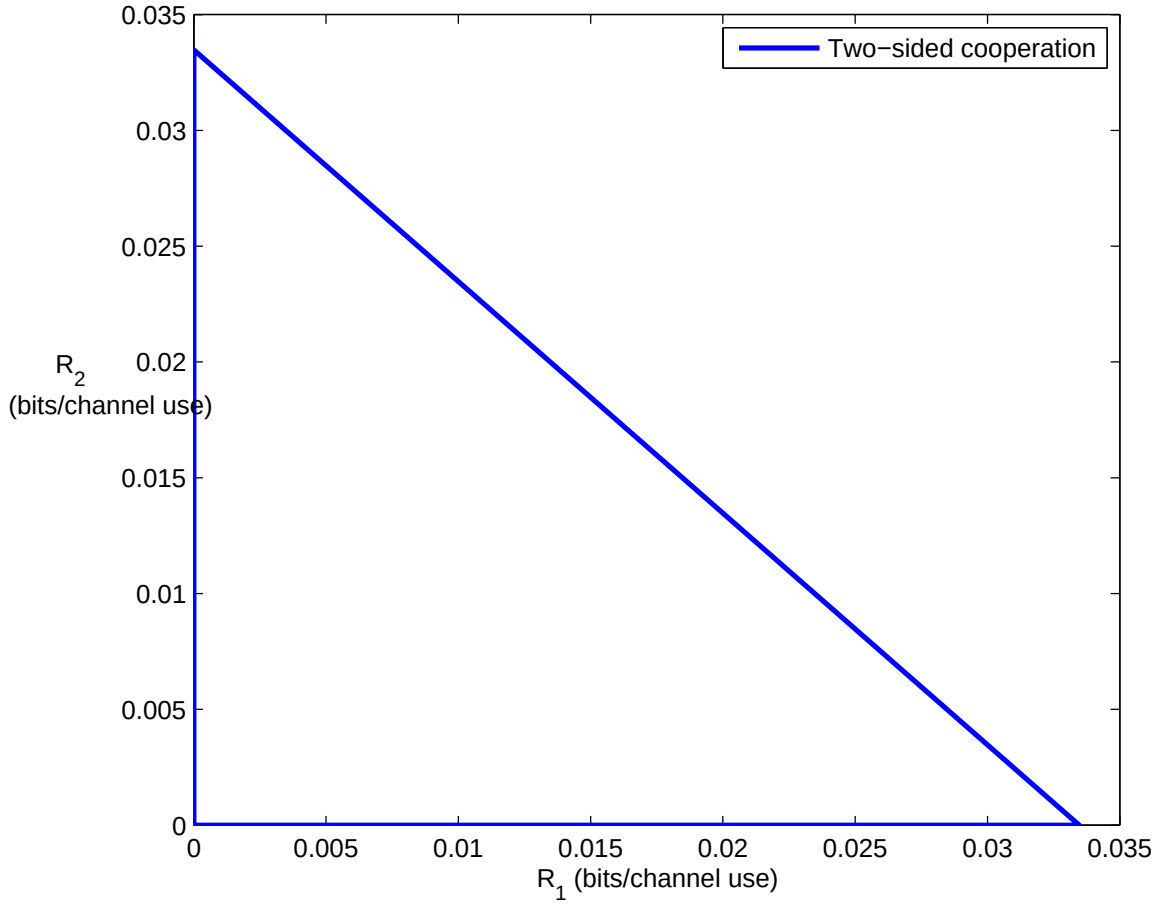
Multiple Access (Uplink) Channel with Cooperation

- **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

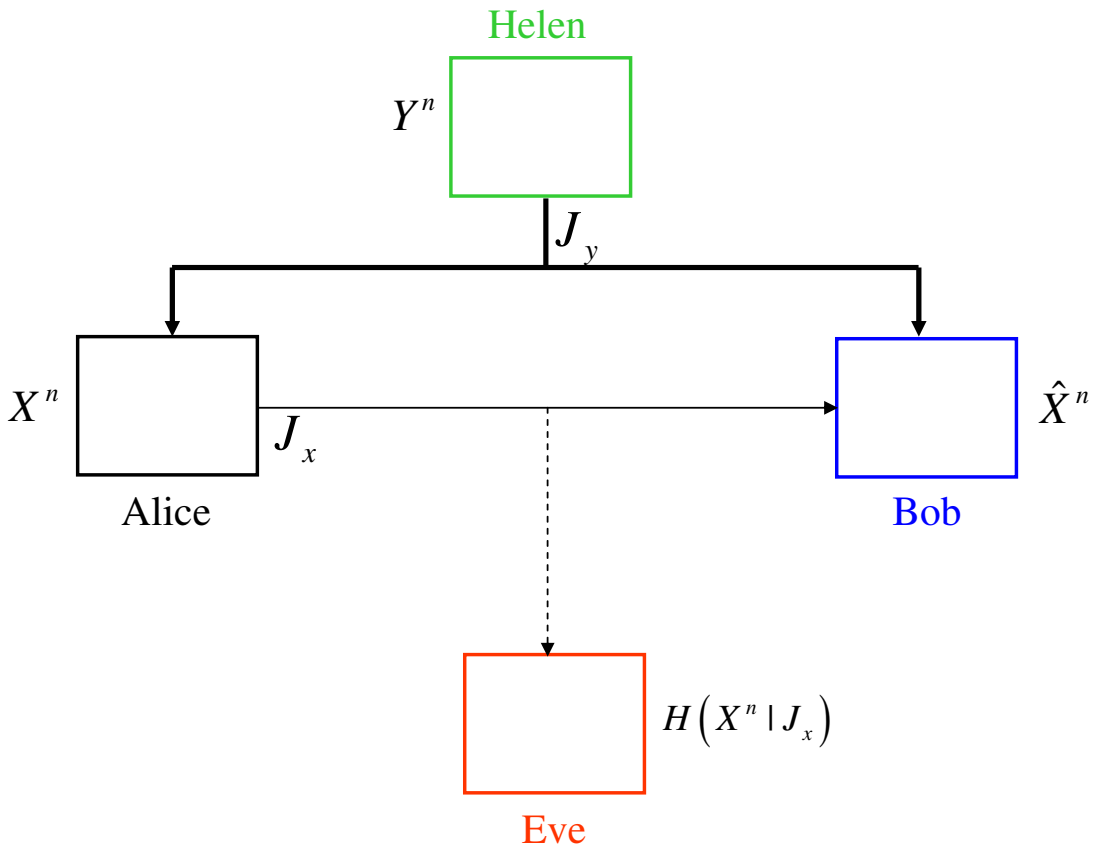
- Both inter-user links are stronger than the main link.
- Without cooperation, none of the users can get a positive secrecy rate.



- Cooperation is beneficial for secrecy if CAF is employed.

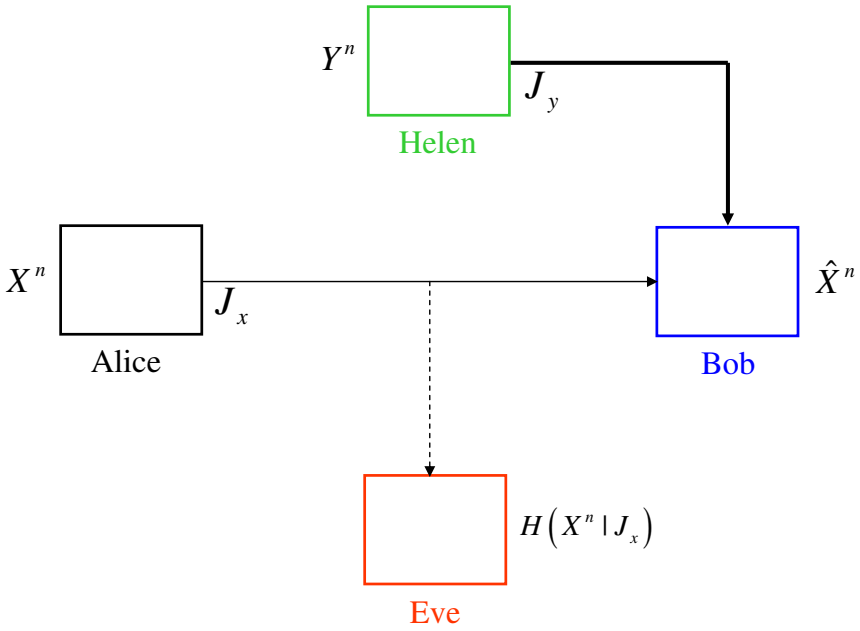
Secure Distributed Source Coding

- 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

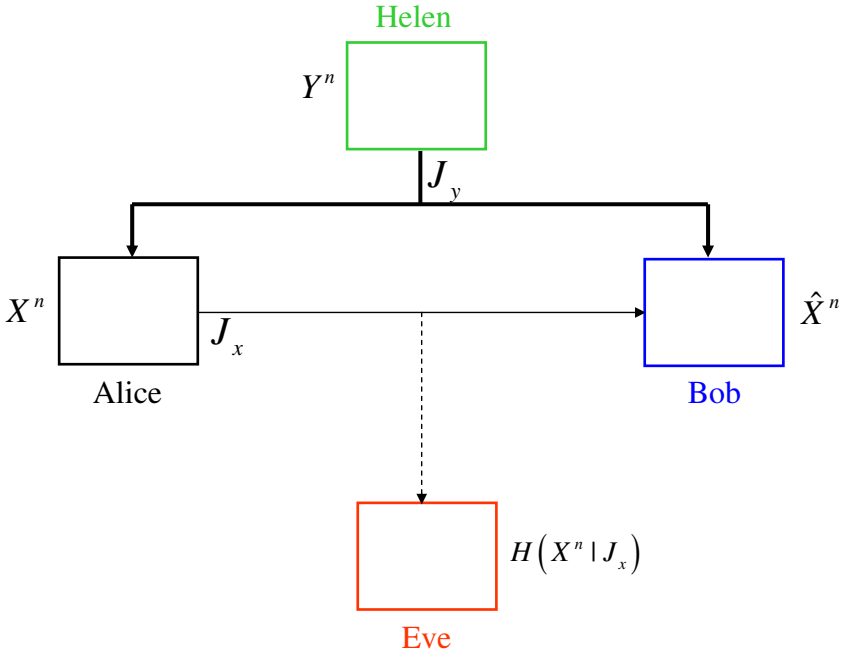
- One-sided helper:



- 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.

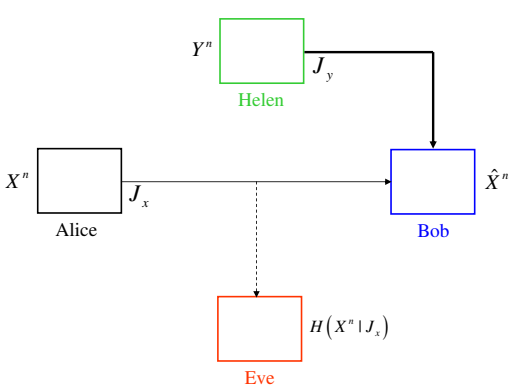
Secure Source Coding with Two-Sided Helper

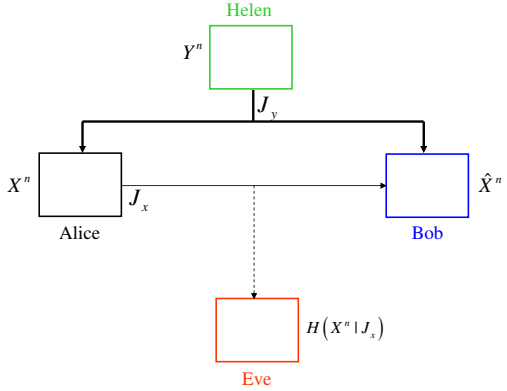
- Two-sided helper:



- 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:

$$\mathcal{R}_{1-sided} \qquad\qquad \mathcal{R}_{2-sided}$$

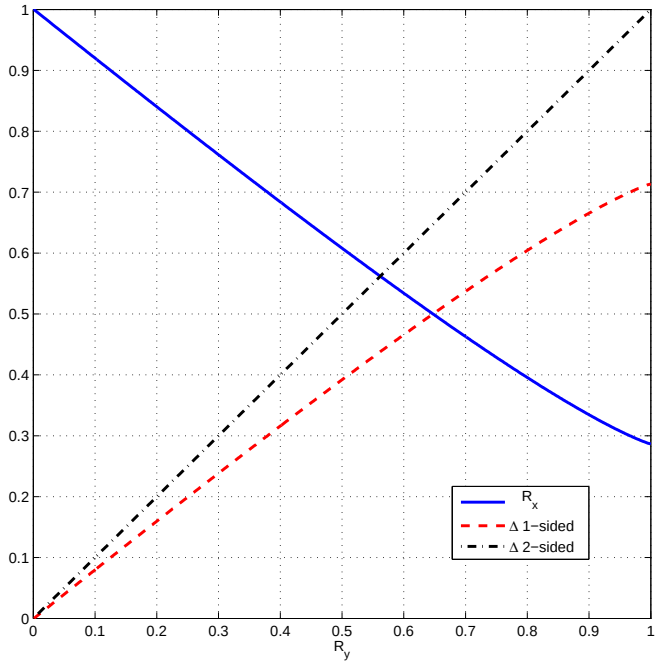
$$R_x \geq H(X|V) \qquad R_x \geq H(X|V)$$

$$R_y \geq I(Y;V) \qquad R_y \geq I(Y;V)$$

$$\Delta \leq I(X;V) \qquad \Delta \leq \min(I(X;V|U), R_y)$$

- 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.