Presented at the 2016 NASIT at Duke

Information Theoretic Security

PennState

Wireless Communications
& Networking Laboratory
WCAN@PSU

Aylin Yener
yener@ee.psu.edu

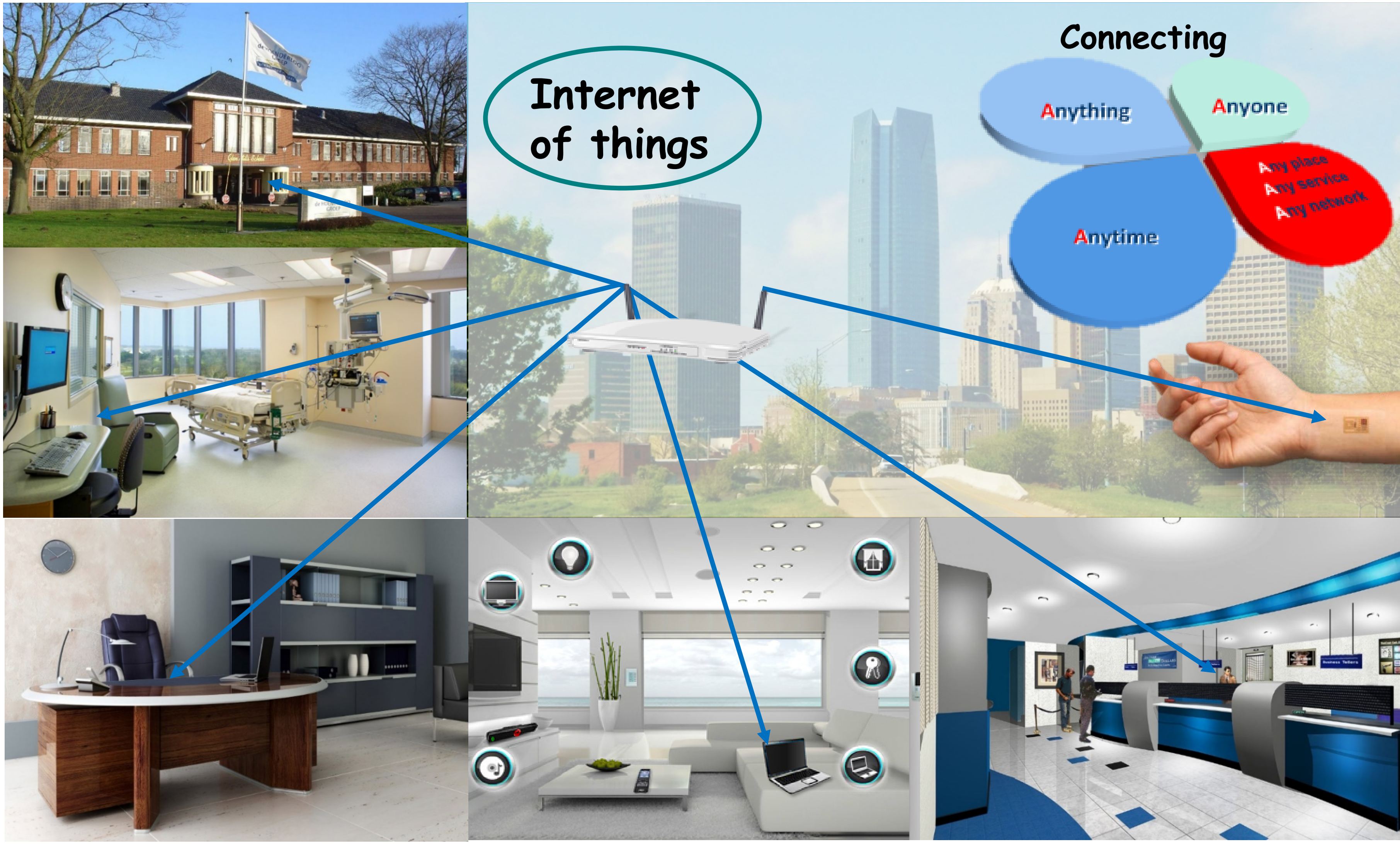
June 21, 2016

Outline

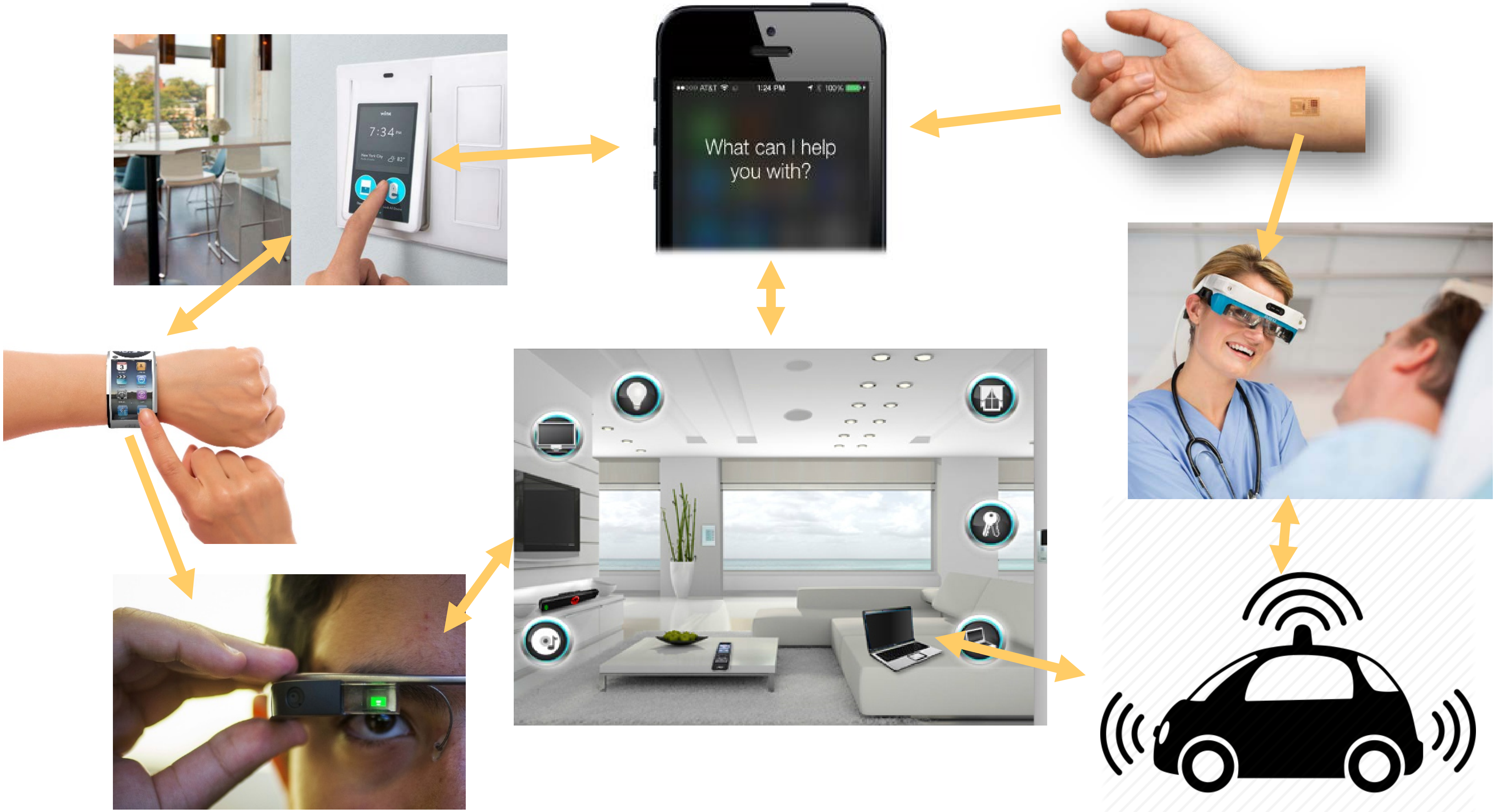
- Motivation and Potential Impact
- Historical Background and basics
- The wiretap channel - the original

- "Wireless" wiretap models - the golden decade
- Enablers for more "realistic" settings
- New models and forward look

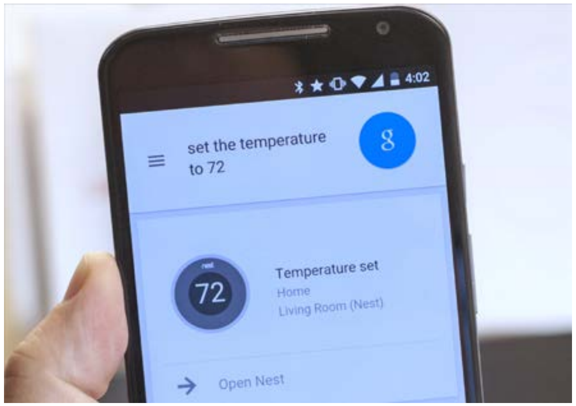
Why (Wireless) information security?



Networked Systems



Security of Networked Systems



Smart phone

Smart thermostat

What is different in wireless?

Wireless: broadcast medium

Wireless has **inherent security vulnerabilities**:

Jamming
Tampering/Injection
Eavesdropping
...

Securing wireless communication links is essential.

Q: Could the wireless medium provide advantages for securing the links?

Securing Wireless Networked Communication

Conventional network design paradigm:

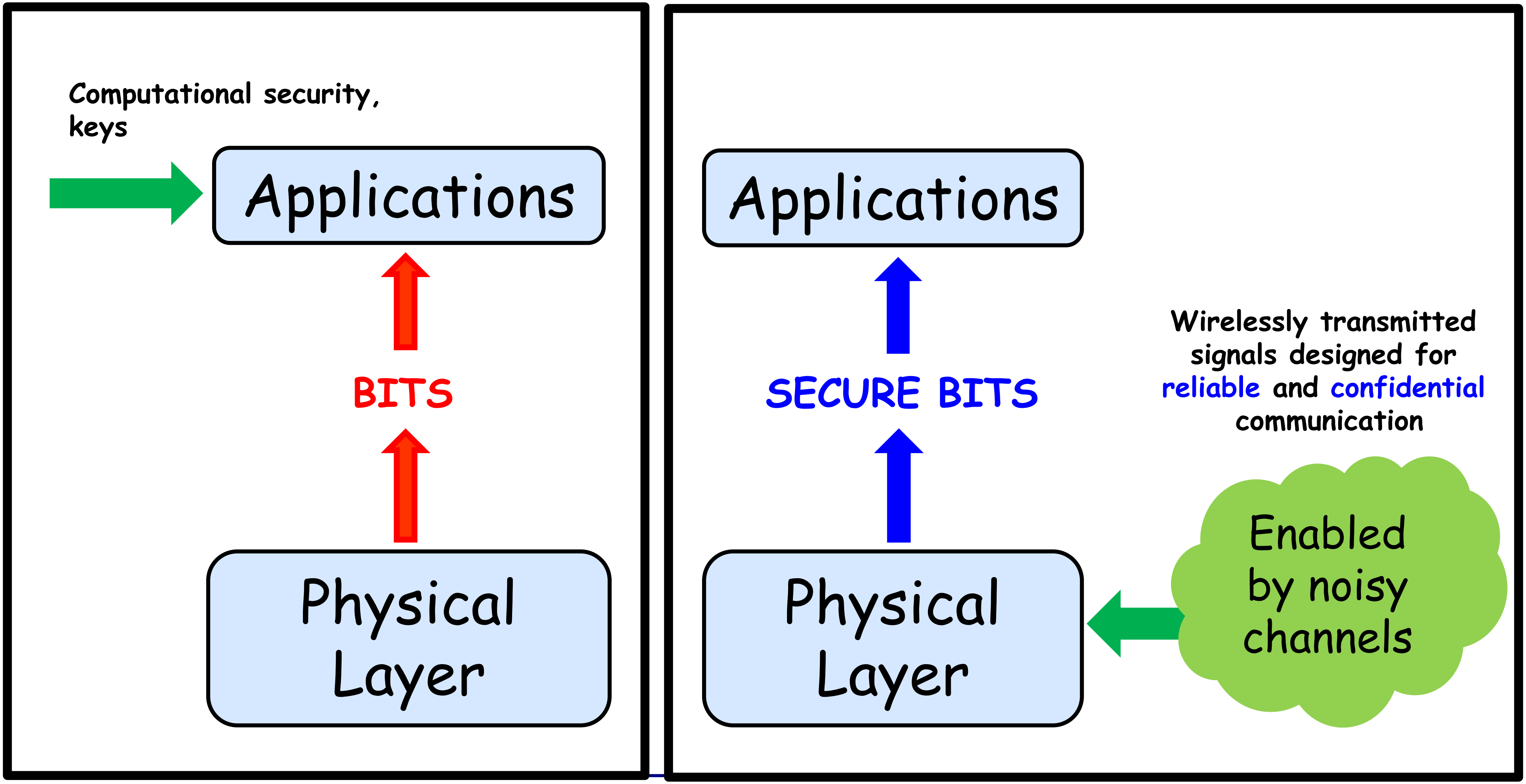
- Layered approach (protocol stack)
- Security as an added feature at the application layer
- Pro: "simple"/practical; Con: breakable?

Wireless Networked Communication Security:

- Design from the bottom (PHY) up.
- Abandon the notion of security as an add-on.
- Pro: unbreakable; Con: not yet practical?

allows us to use physical medium, and the transmitted signals to aid in providing security.

AP vs PHY Confidentiality



[Shannon 1945]

- **Secrecy** is measured with **mutual information.**
- Adversary **"enemy-cryptanalyst"** is not computationally limited.
- **Noiseless** communication channels.
- **Perfect Secrecy**:

  a-posteriori uncertainty = a-priori uncertainty

- Perfect secrecy if key rate >= message rate (use key only once.)

COVER SHEET FOR TECHNICAL MEMORANDA

RESEARCH DEPARTMENT

SUBJECT: A Mathematical Theory of Cryptography - Case 20878 (u)

ROUTING:

1 – HWB-HF-Case Files
2 – CASE FILES
3 – J. W. McRae
4 – L. Espenschied
5 – H. S. Black
6 – F. B. Llewellyn
7 – H. Nyquist
8 – B. M. Oliver
9 – R. K. Potter
10 – C. B. H. Feldman
11 - R. C. Mathes
12 - R. V. L. Hartley
13 - J. R. Pierce
14 - H. W. Bode
15 - R. L. Dietzold
16 - L. A. MacCall
17 - W. A. Shewhart
18 - S. A. Schelkunoff
19 - C. E. Shannon
20 - Dept. 1000 Files

MM– 45-110-92
DATE September 1, 1945
AUTHOR C. E. Shannon
INDEX NO. P 0.4

SECRET

~~ABSTRACT~~

DOWNGRADED AT 3 YEAR INTERVALS
DECLASSIFIED AFTER 12 YEARS
DOD DIR 5200.10

From Shannon's Miscellaneous Writings courtesy of N. Sloane

Shannon (1945)

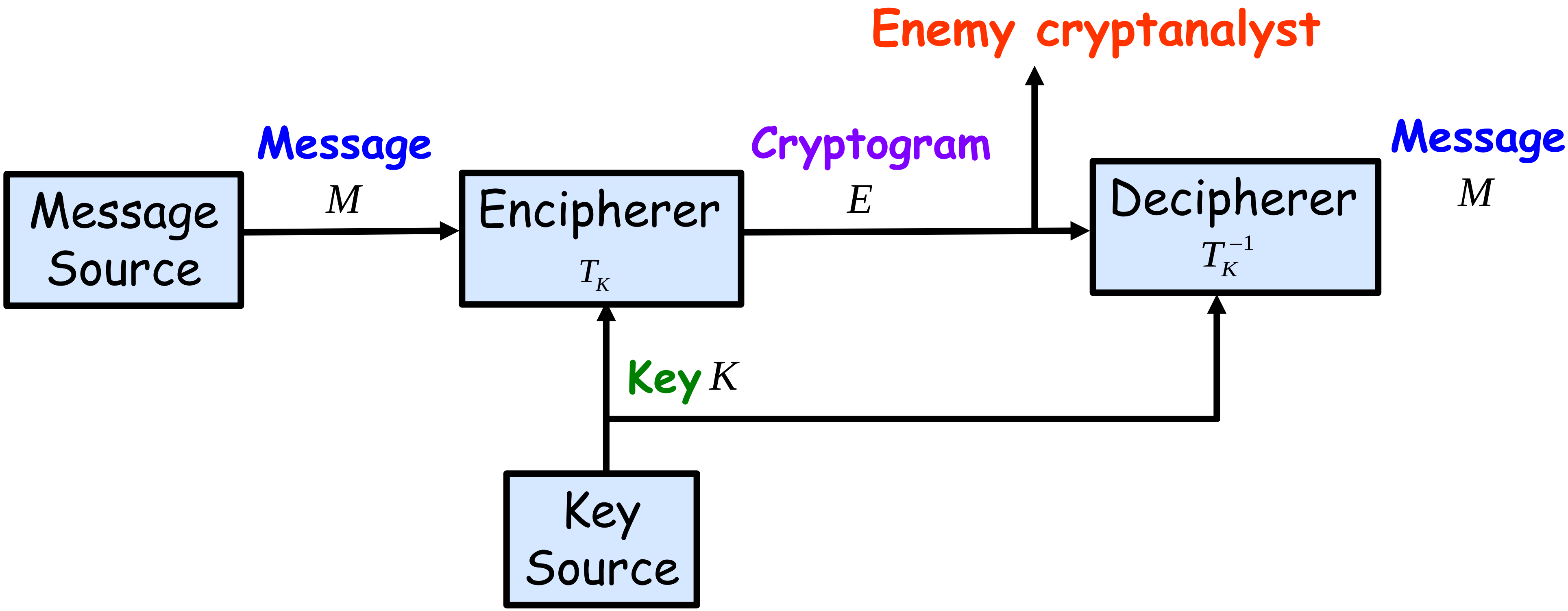
ABSTRACT

A mathematical theory of secrecy systems is developed. Three main problems are considered. (1) A logical formulation of the problem and a study of the mathematical structure of secrecy systems. (2) The problem of "theoretical secrecy," i.e., can a system be solved given unlimited time and how much material must be intercepted to obtain a unique solution to cryptograms. A secrecy measure called the "equivocation" is defined and its properties developed. (3) The problem of "practical secrecy." How can systems be made difficult to solve, even though a solution is theoretically possible.

THIS DOCUMENT CONTAINS INFORMATION AFFECTING THE NATIONAL DEFENSE OF THE UNITED STATES WITHIN THE MEANING OF THE ESPIONAGE LAWS, TITLE 18 U.S.C., SECTIONS 793 AND 794. ITS TRANSMISSION OR THE REVELATION OF ITS CONTENTS IN ANY MANNER TO AN UNAUTHORIZED PERSON IS PROHIBITED BY LAW.

Perfect Secrecy

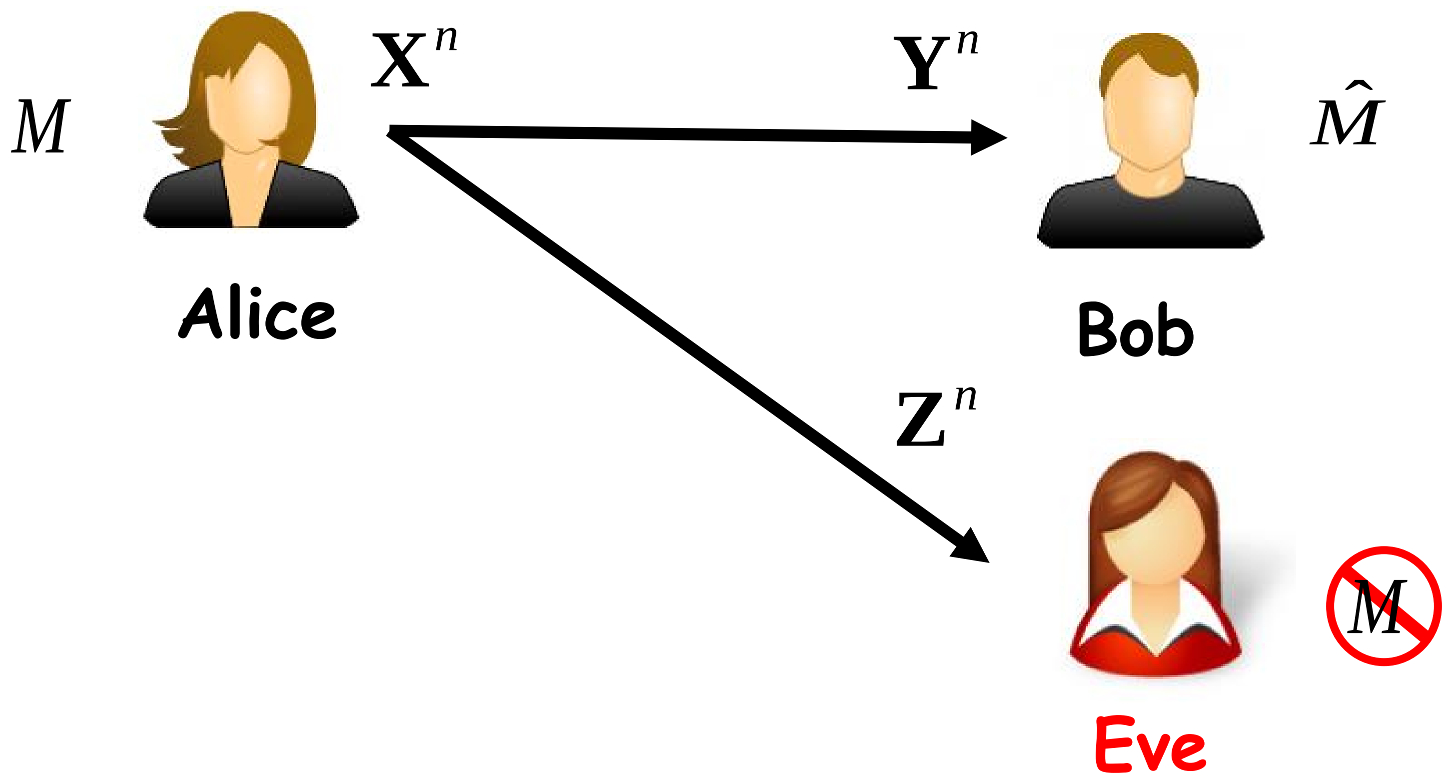
- Shannon – Secrecy Systems (1945)



- Perfect Secrecy: $H(M \mid E) = H(M)$

[Wyner 1975]

- The **Wiretap Channel (WTC):**



Secrecy

- Secrecy is measured by the **equivocation rate** at **Eve**:

$$R_e = \lim_{n\to\infty} \frac{1}{n} H(M \mid \mathbf{Z}^n) \quad \Rightarrow \quad R_e \le R = \lim_{n\to\infty} \frac{1}{n} H(M)$$

- **Objective:** Have an R_e **as high as possible.**

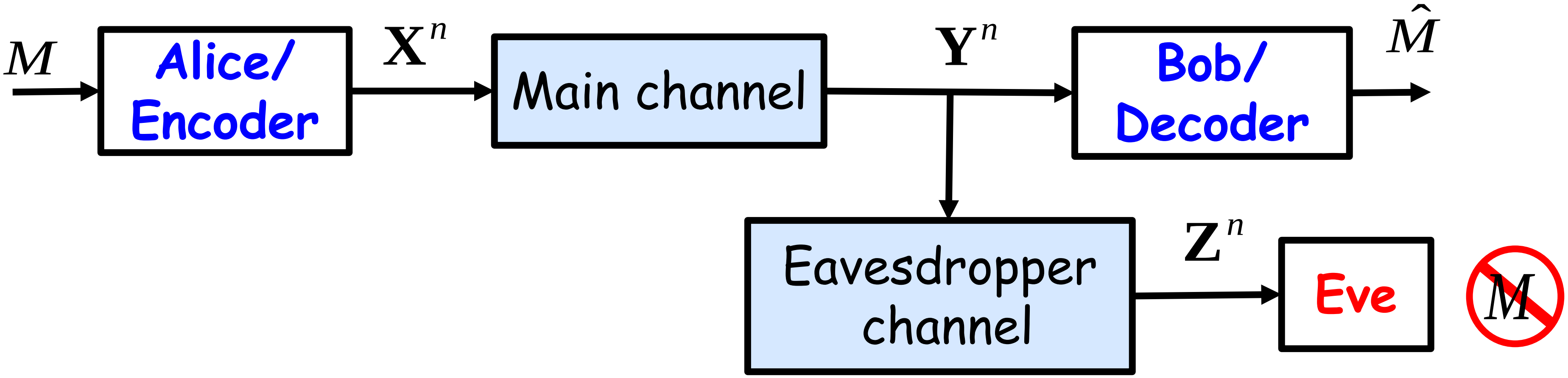
- When $R_e = R$ $\Rightarrow$ $\lim_{n\to\infty} \frac{1}{n} [H(M) - H(M \mid \mathbf{Z}^n)] = 0$

$$\Rightarrow \quad \lim_{n\to\infty} \frac{1}{n} I(M; \mathbf{Z}^n) = 0$$ **(Weak Secrecy Constraint)**

[Wyner's WTC 1975]

- Communication channels are not noiseless bit pipes!
  - Eve's channel is "***worse***" than Bob's channel;
    (is degraded w.r.t. Bob's channel.)
- An information theoretically (weakly) secure and reliable communication rate → the notion of **Secrecy Capacity.**
- **No shared key needed.**
- Channel codes can be designed to leverage the physical channel advantage of Bob over **Eve.**

WTC



Achievable rate satisfies:

1) **Reliability** condition: $P_e^{(n)} = \Pr\{\hat{M} \neq M\} \leq \varepsilon$

2) **Equivocation** constraint: $\dfrac{H(M \mid \mathbf{Z}^n)}{H(M)} \geq d - \varepsilon$

Secrecy is **measure by equivocation** at Eve: $R_e = \lim\limits_{n \to \infty} \dfrac{1}{n} H(M \mid \mathbf{Z}^n)$

Wyner's WTC

- **Key ingredient:** Stochastic Encoding
  - Encoder confuses the eavesdropper by reducing its rate and using a stochastic mapping
  - Implemented with **local randomness** that needs to be shared with no one!
- Design channel codebooks that are "**inflated**".
- Get secure rate as high as the max difference of MI.

Secrecy Capacity

- Secrecy capacity when

$$R_e = \lim_{n\to\infty}\frac{1}{n}H(M\,|\,\mathbf{Z}^n) = \lim_{n\to\infty}\frac{1}{n}H(M) = R \qquad (d=1)$$

- The secrecy capacity of **Wyner's degraded WTC** is

$$C_s = \max_{X-Y-Z}\,[I(X;Y) - I(X:Z)]^+$$

- **Stochastic Encoding:**
  - **Code rate** = $I(X;Y)$ (no. of cws = $2^{nI(X;Y)}$).
  - **Randomization rate** = $I(X;Z)$ (Each message $\mapsto 2^{nI(X;Z)}$ cws).
  - **Rate reduction** due to secrecy = $I(X;Z)$.

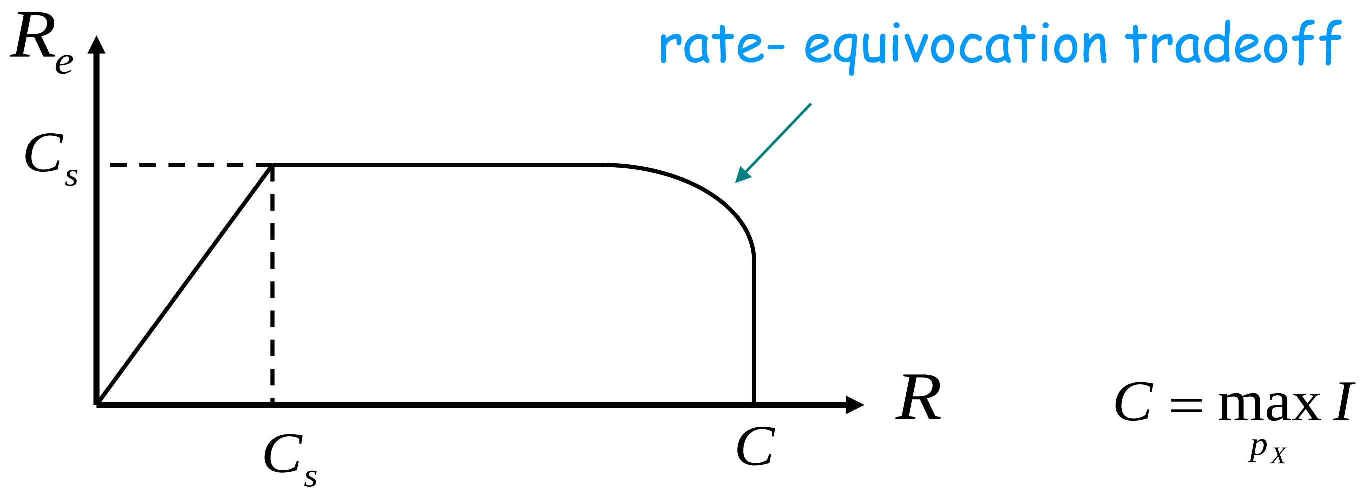
Capacity-Equivocation Region

- The capacity-equivocation region for Wyner's WTC is the set of all pairs (R, R_e) satisfying

$$0 \le R \le I(X;Y)$$

$$0 \le R_e \le I(X;Y) - I(X;Z)$$

- A typical (R, R_e) region:



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

Achievability

- For any p_X s.t. $X - Y - Z$, the rate
  $R_s = I(X;Y) - I(X:Z)$ is achievable.

- Fix p_X.
- Generate $2^{n(R_s+\tilde{R}_s)}$ cws x^n through $p(x^n) = \prod_{i=1}^{n} p_X(x_i)$.
- Index the cws as $x^n(m, \tilde{m})$ where

$$m \in \{1, \ldots, 2^{nR_s}\}, \qquad \tilde{m} \in \{1, \ldots, 2^{n\tilde{R}_s}\}$$

denotes the actual secret message

denotes the confusion (dummy) message [carries no information]

Codebook Structure

$$
2^{nR_s}\left\{
\overbrace{
\begin{array}{|c|c|c|c|c|c|}
\hline
(1,1) & (1,2) & \cdots & (1,j) & \cdots & (1,2^{n\tilde{R}_s}) \\
\hline
(2,1) & (2,2) & \cdots & (2,j) & \cdots & (2,2^{n\tilde{R}_s}) \\
\hline
\vdots & \vdots & & \vdots & & \vdots \\
\hline
(i,1) & (i,2) & \cdots & (i,j) & \cdots & (i,2^{n\tilde{R}_s}) \\
\hline
\vdots & \vdots & & \vdots & & \vdots \\
\hline
(2^{nR_s},1) & (2^{nR_s},2) & \cdots & (2^{nR_s},j) & \cdots & (2^{nR_s},2^{n\tilde{R}_s}) \\
\hline
\end{array}
}^{2^{n\tilde{R}_s}}
\right.
$$

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

Encoding and Decoding

- **Encoding:**
  - To send a message m, encoder randomly selects $\tilde{m} \in \{1, \ldots, 2^{n\tilde{R}_s}\}$ and transmits $x^n(m, \tilde{m})$.

- **Decoding:**
  - **Bob** decides on $\hat{m}$ if $(x^n(\hat{m}, \tilde{m}), y^n)$ is jointly typical for some $\tilde{m}$ **(typicality-decoder)**.
  - **Bob** decodes both secret and dummy messages $m, \tilde{m}$ reliably since

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

  - Thus, **reliability condition is satisfied.**

Secrecy Analysis

- We show that $\lim_{n\to\infty}\frac{1}{n}I(M;\mathbf{Z}^n)=0$ as follows:

$$
\begin{aligned}
H(M\mid\mathbf{Z}^n) &= H(M,\tilde{M}\mid\mathbf{Z}^n)-H(\tilde{M}\mid M,\mathbf{Z}^n)\\
&= H(M,\tilde{M})-I(M,\tilde{M};\mathbf{Z}^n)-H(\tilde{M}\mid M,\mathbf{Z}^n)\\
&\geq H(M)+H(\tilde{M})-I(\mathbf{X}^n;\mathbf{Z}^n)-H(\tilde{M}\mid M,\mathbf{Z}^n)
\end{aligned}
$$

Data processing inequality (DPI): $(M,\tilde{M})-\mathbf{X}^n-\mathbf{Z}^n$

$$\Rightarrow\quad I(M;\mathbf{Z}^n)\leq I(\mathbf{X}^n;\mathbf{Z}^n)+H(\tilde{M}\mid M,\mathbf{Z}^n)-H(\tilde{M})$$

Secrecy Analysis

- We show that $\lim\limits_{n\to\infty} \frac{1}{n} I(M;\mathbf{Z}^n) = 0$ as follows:

$$\Rightarrow \quad I(M;\mathbf{Z}^n) \le I(\mathbf{X}^n;\mathbf{Z}^n) + H(\tilde{M} \mid M, \mathbf{Z}^n) - H(\tilde{M})$$

$\le n(I(X;Z)+\varepsilon_n)$

$\le n\tilde{\varepsilon}_n$

Given M, Eve can decode $\tilde{M}$ reliably since $\tilde{R}_s = I(X;Z)$

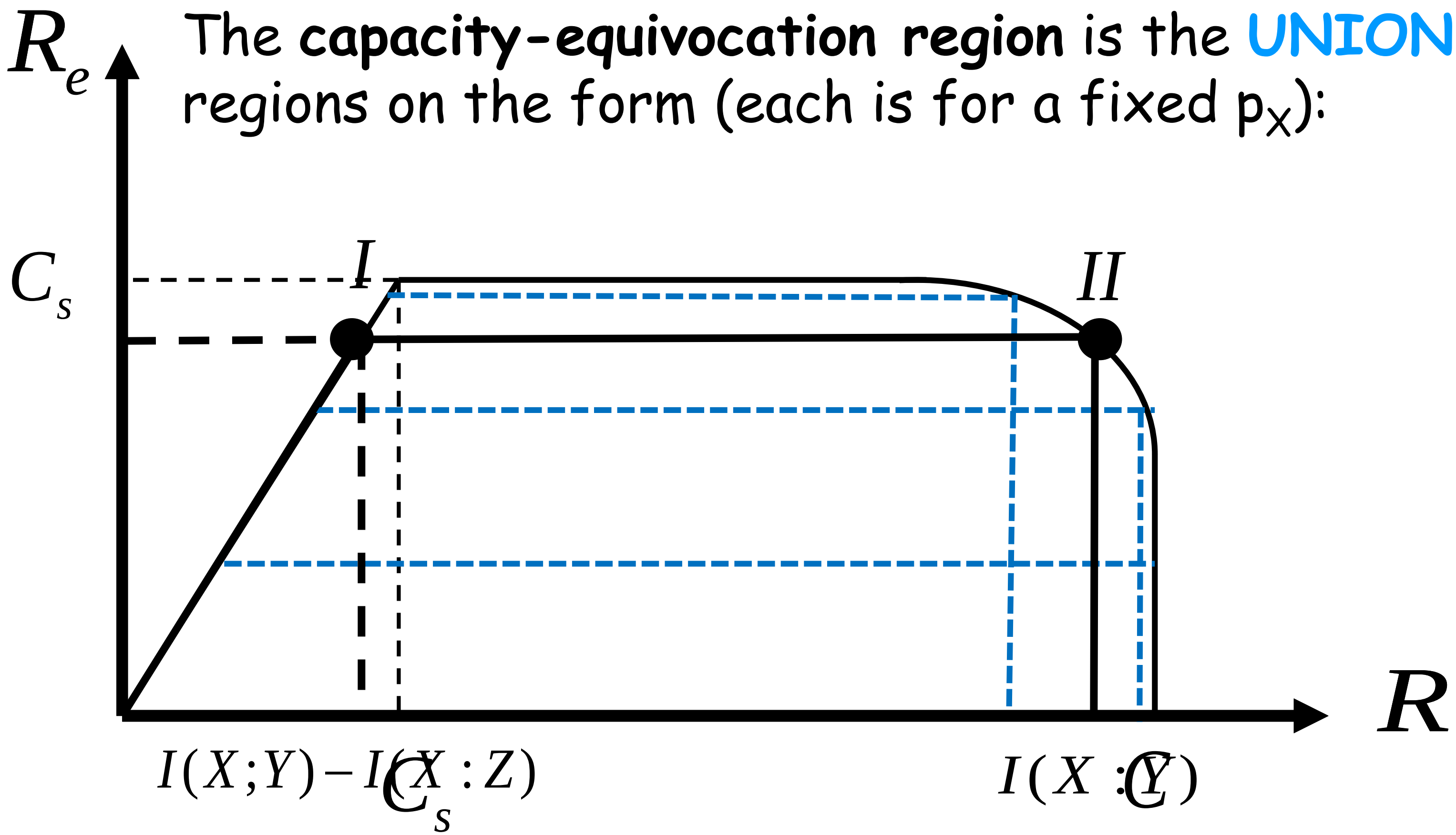
$= n\tilde{R}_s = nI(X;Z)$

$$\Rightarrow \quad \lim_{n\to\infty} \frac{1}{n} I(M;\mathbf{Z}^n) = 0$$

secrecy condition is satisfied

Achievability of Capacity-Equivocation region

The **capacity-equivocation region** is the UNION of regions on the form (each is for a fixed p_X):



Achievability of I

- We have shown the achievability of I (Secrecy capacity when $R = R_e$):

$$R = R_e = I(X;Y) - I(X:Z)$$

Achievability of II

- Decompose M into M_s (secret message) and M_p (public message).

- Using similar steps to achievability of I, we show the achievability of $R = I(X;Y),\ \ R_e = I(X;Y) - I(X:Z)$

$$m_s \in \{1,\ldots,2^{nR_s}\}, \quad m_p \in \{1,\ldots,2^{nR_p}\}$$

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

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

- The difference here is that the randomization message also carries information.

Converse I

- $R \le I(X;Y)$: By channel coding theorem.

- We also have

$$
\begin{aligned}
nR_e &= H(M \mid \mathbf{Z}^n) \\
&\le H(M \mid \mathbf{Z}^n) - H(M \mid \mathbf{Y}^n) + n\varepsilon \qquad \text{Fano's inequality} \\
&= I(M;\mathbf{Y}^n) - I(M;\mathbf{Z}^n) + n\varepsilon \\
&\le I(M;\mathbf{Y}^n,\mathbf{Z}^n) - I(M;\mathbf{Z}^n) + n\varepsilon \\
&= I(M;\mathbf{Y}^n \mid \mathbf{Z}^n) + n\varepsilon
\end{aligned}
$$

Converse II

$$nR_e \le I(M;\mathbf{Y}^n \mid \mathbf{Z}^n) + n\varepsilon$$

$$= \sum_{i=1}^{n} I(M;Y_i \mid \mathbf{Y}^{i-1}, \mathbf{Z}^n) + n\varepsilon$$

$$\le \sum_{i=1}^{n} [H(Y_i \mid Z_i) - H(Y_i \mid X_i, Z_i)] + n\varepsilon$$

Chain rule & conditioning cannot increase entropy

$$= \sum_{i=1}^{n} I(X_i;Y_i \mid Z_i) + n\varepsilon$$

$$= \sum_{i=1}^{n} [I(X_i;Y_i) - I(X_i;Z_i)] + n\varepsilon$$

Degradedness $(X_i - Y_i - Z_i)$

$$\le n[I(X;Y) - I(X;Z)] + n\varepsilon$$

Single letterization

Observations

- Achievability of $R_s = \max[I(X;Y) - I(X:Z)]^+$: we did not use degradedness.

- Degradedness is used in the converse proof.

Non-degraded Channels

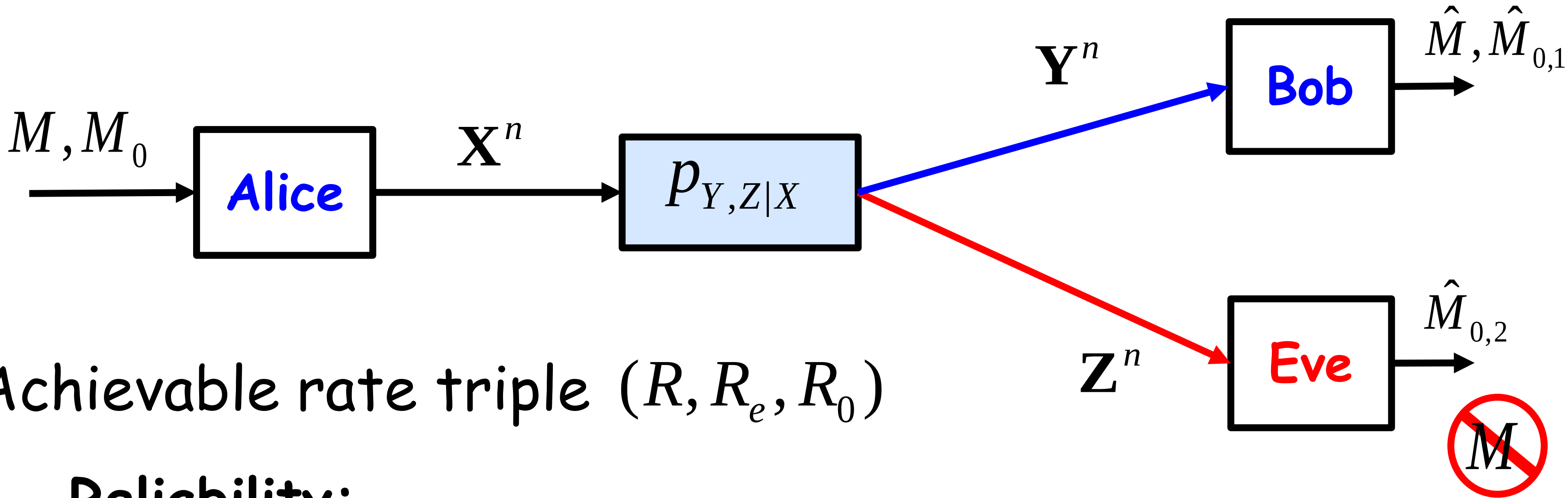
- When the channel is **not degraded (as it is in Wyner's set up)**:
  - is it possible to achieve **positive** secrecy rate?
  - is it possible to create an **equivalent degraded channel** with some virtual input?

The General Wiretap Channel

[Csiszar-Korner 1978] "BC with confidential messages"

- Extended **Wyner's wiretap channel** to
  1. Wiretap channel with **Eve's** channel is **not degraded** w.r.t. **Bob's** channel.
  2. There is a **common message** for both **Bob** and **Eve.**
- **New ingredients:**
  1. Super-position coding (to accommodate the common message.)
  2. Channel prefixing.

General WTC (1978)



Achievable rate triple (R, R_e, R_0)

1. **Reliability:**

$$\lim_{n\to\infty} P_e^{(n)} = \lim_{n\to\infty} \Pr\left((\hat{M}, \hat{M}_{0,1}) \neq (M, M_0) \cup \{\hat{M}_{0,2} \neq M_0\}\right) = 0$$

2. **Equivocation:** $R_e \le \lim_{n\to\infty} \frac{1}{n} H(M \mid \mathbf{Z}^n)$

Secrecy Capacity

The secrecy capacity of the general wiretap channel is

$$C_s = \max_{V - X - (Y,Z)} [I(V;Y) - I(V:Z)]^+$$

where the maximization is over all distributions $p_{V,X}$ such that $V - X - (Y,Z)$ is a Markov chain.

Capacity-Equivocation Region

The **capacity-equivocation region** for the **general wiretap channel** is the **union** of all rate triples satisfying (R, R_e, R_0)

$$R_0 \le \min\{I(U;Y), I(U;Z)\}$$

$$R_0 + R_1 \le I(V;Y|U) + \min\{I(U;Y), I(U;Z)\}$$

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

for some (U,V) such that $U - V - X - (Y,Z)$ is a Markov chain.

Auxiliary Variables

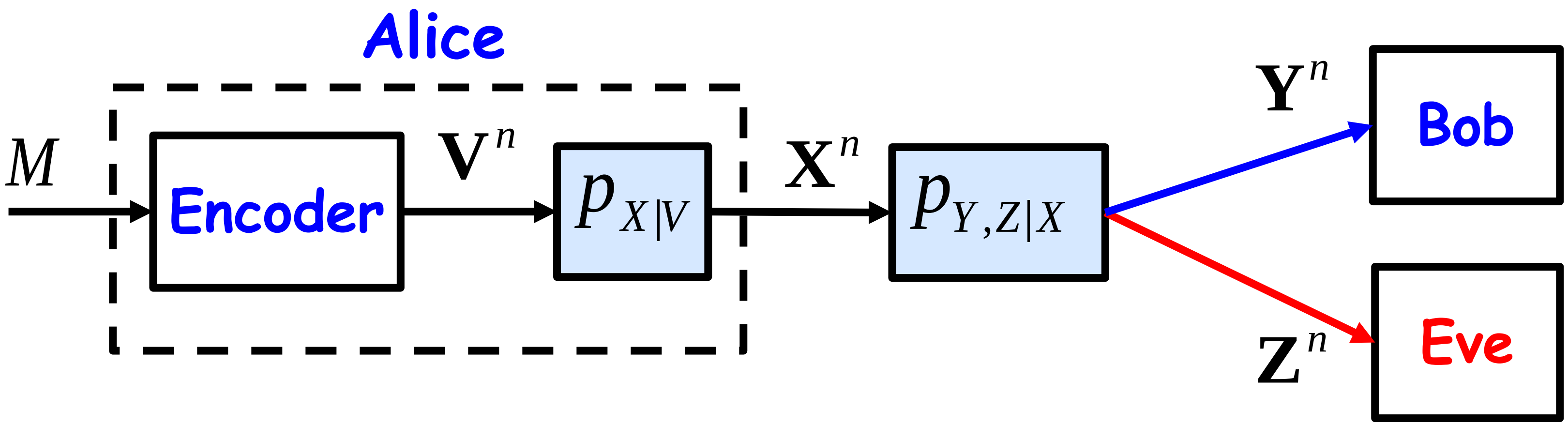
- U represents a common message that is needed to be decoded at both Bob and Eve (**Rate splitting**).

- V represents a virtual input to the channel (**Channel prefixing**).

Channel Prefixing

- A virtual channel from V to X.
- Additional stochastic mapping from the message to the channel input: $M \to V \to X$.
- **Actual channel:** $X \to Y$ and $X \to Z$.
- **Constructed channel:** $V \to Y$ and $V \to Z$.
- No channel prefixing is a special case of channel prefixing by setting $V = X$.

Channel Prefixing



- Channel prefixing results in $V - X - (Y, Z)$.
- From DPI, both mutual-information terms decrease, but their difference may **increase**.

Rate Splitting

- **Eve** decodes a part of the transmitted message by **Alice**.
- **Rate splitting:** inserting auxiliary random variable U such that $U - V - X - (Y, Z)$ is a Markov chain.
- Note that $I(U, V; Y) = I(V; Y)$

$$U - V - Y$$

Outline of Achievability

- For some (U,X) such that $U-X-(Y,Z)$, the achievability of

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

is shown using stochastic encoding & super-position coding.

- By prefixing the channel $p_{X|V}$ such that $U-V-X-(Y,Z)$ the claimed (larger) achievable region is obtained.

Outline of Converse

- New ingredient: **Csiszar's Sum Identity**

Let $\mathbf{T}^n, \mathbf{U}^n$ be length-n random vectors, and G be a random variable. We have

$$\sum_{i=1}^{n} I(\mathbf{U}_{i+1}^{n}; T_i \mid G, \mathbf{T}^{i-1}) = \sum_{i=1}^{n} I(\mathbf{T}^{n}; U_i \mid G, \mathbf{U}_{i+1}^{n})$$

- Used to establish a similar proof for Wyner's **without the degradedness assumption** $(X - Y - Z)$.

Capacity-Equivocation Region for R_0=0

- When there is **no common message**, the capacity-equivocation is the union of all pairs (R, R_e) satisfying:

$$R \leq I(V;Y)$$

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

for some (U,V) s.t. $U - V - X - (Y,Z)$ is a Markov chain.

- We still need the **two** auxiliary random variables:
  - V : Channel prefixing
  - U : Rate splitting (**still need** super-position coding!)

Observation I

$$R \le I(V;Y), \qquad R_e \le I(V;Y|U) - I(V;Z|U)$$

$$(U,V) \quad \text{s.t.} \quad U - V - X - (Y,Z)$$

Capacity-Equivocation region at $R_0 = 0$

We can limit the search to U s.t. $I(U;Y) \le I(U;Z)$:

$$I(V:Y|U) - I(V;Z|U) = I(V;Y) - I(V;Z)$$
$$-[I(U;Y) - I(U;Z)]$$

If no U s.t. $I(U;Y) \le I(U;Z)$; Set U =empty set

Secrecy Capacity Derivation

$$C_s = \max_{V-X-(Y,Z)} [I(V;Y) - I(V:Z)]^+$$

At $R = R_e$

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

$$= \sum_{u\in\mathcal{U}} p(U=u)\left[I(V;Y|U=u) - I(V;Z|U=u)\right]$$

$$\le \max_{u\in\mathcal{U}} \left[I(V;Y|U=u) - I(V;Z|U=u)\right]$$

$$= I(V;Y|U=u^*) - I(V;Z|U=u^*) = I(V';Y) - I(V';Z)$$

maximizer

when $U = u^*, \quad V = V'$

Observation II

- For secrecy capacity,

$$C_s = \max_{V-X-(Y,Z)} [I(V;Y) - I(V:Z)]^+$$

(no rate splitting needed.)

Channel Orderings

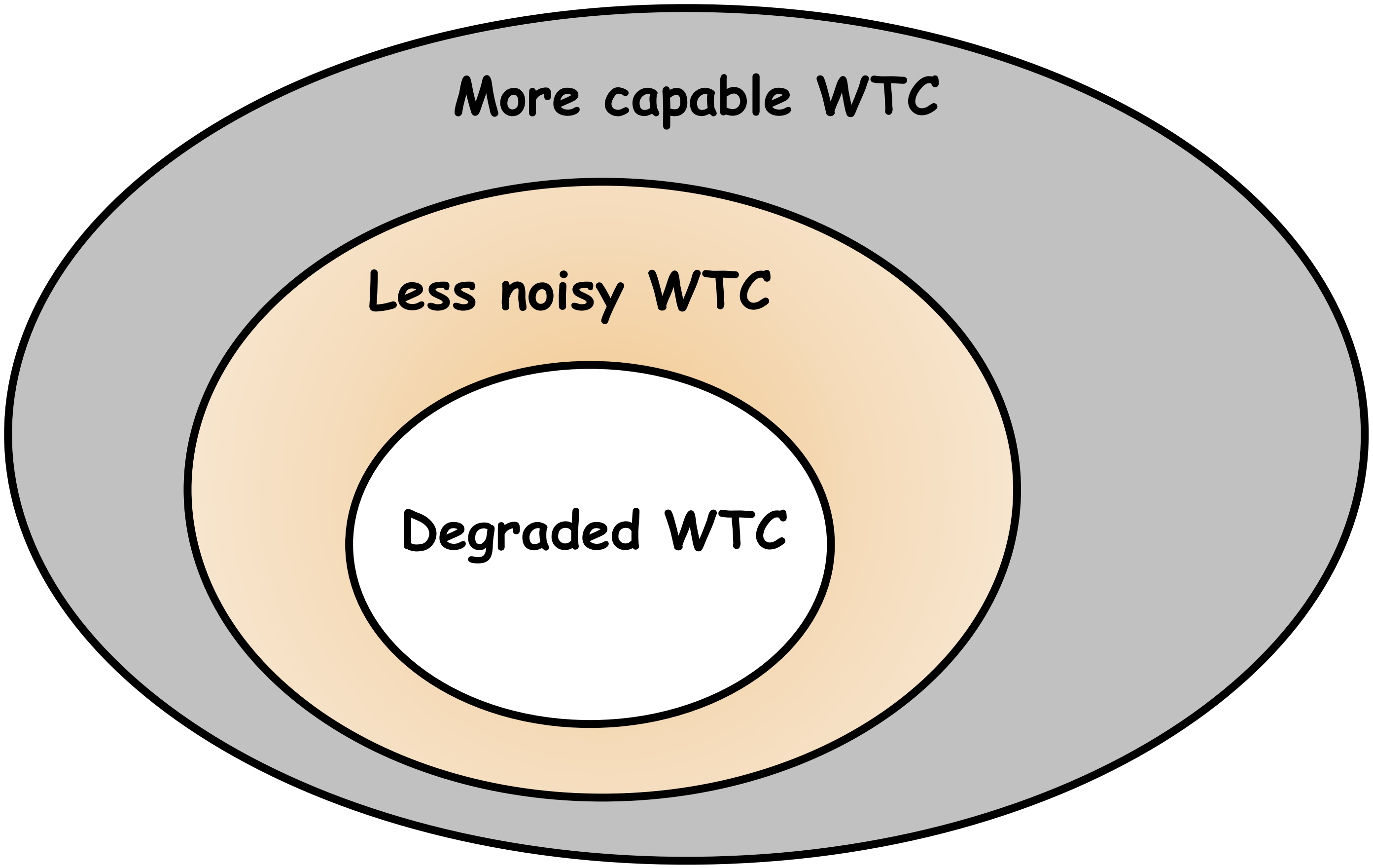
- **More capable channel:** A wiretap channel is more capable if for all X, $I(X;Y) \geq I(X;Z)$.
- **Less noisy channel:** A wiretap channel is less noisy if for all V such that $V - X - (Y,Z)$,

$$I(V;Y) \geq I(V;Z)$$

- **Degraded channel:** A wiretap channel is degraded if

$$p_{Y,Z|X}(y,z\,|\,x) = p_{Y|X}(y\,|\,x)\,p_{Z|X}(z\,|\,x), \qquad \forall x,y,z$$

Orderings Relation



Observation III

$$C_s = \max_{V - X - (Y,Z)} [I(V;Y) - I(V:Z)]^+$$

The secrecy capacity is always **POSITIVE**,

$$C_s \geq 0,$$

unless the channel to Eve ***is less noisy than*** the channel to Bob.

Observation IV

- **If the wiretap channel is less noisy**

Capacity-Equivocation Region:

$$R \le I(X;Y)$$

$$R_e \le I(X;Y) - I(X;Z)$$

Secrecy Capacity:

$$C_s = \max_{p_X} \left[I(X;Y)\text{-}I(X;Z) \right]$$

Wyner's result holds for the Broader class of less noisy channels

Proof

$$
\begin{aligned}
R_e &\le I(V;Y|U) - I(V;Z|U) \\
&= I(V;Y) - I(V;Z) - \left[I(U;Y) - I(U;Z)\right] \\
&= I(X;Y) - I(X:Z) \\
&\qquad - \underbrace{\left[I(X;Y|V) - I(X;Z|V)\right]} - \underbrace{\left[I(U;Y) - I(U;Z)\right]} \\
&\le I(X;Y) - I(X:Z)
\end{aligned}
$$

≥ 0 due to the less noisy assumption

Set U to be the empty set and $V = X$

Observation V

If the wiretap channel is more capable:

$$C_s = \max_{p_X} \left[I(X;Y) - I(X;Z) \right] \quad (V = X \text{ is optimal})$$

Proof:

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

$$= \max_{V-X-(Y,Z)} I(X;Y) - I(X:Z) - \underbrace{[I(X;Y|V) - I(X;Z|V)]}_{\geq 0 \text{ with equality at } V=X}$$

$$= \max_{X-(Y,Z)} I(X;Y) - I(X:Z)$$

Observations

Observation VI

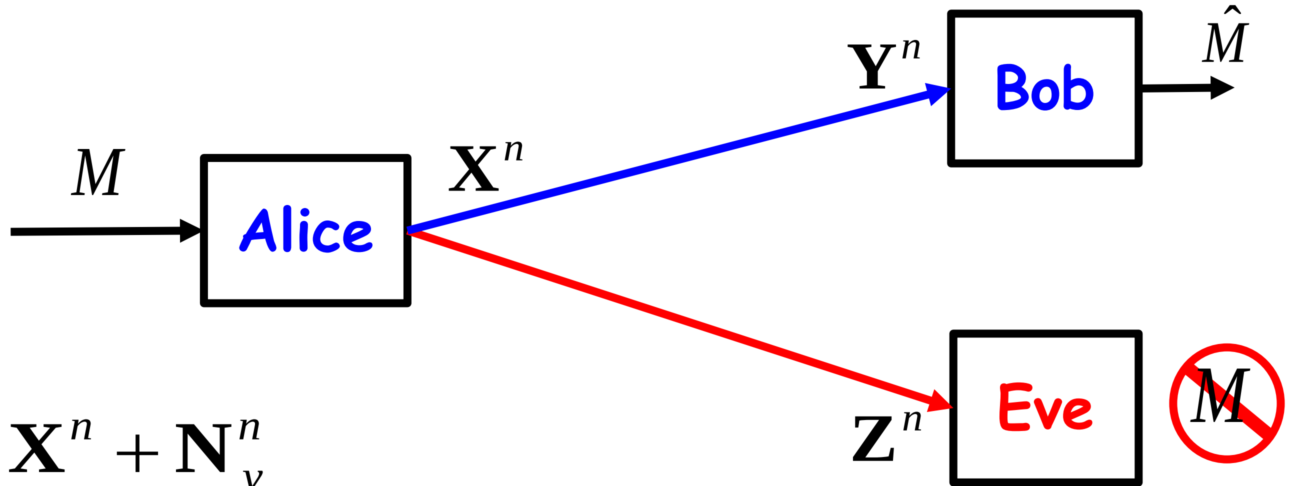
The wiretap channel is **less noisy** iff $I(X;Y)-I(X;Z)$ is concave in $p(x)$.

Observation VII

If the wiretap channel is **less noisy** and $\exists\, p^*(x)$ which maximizes both $I(X;Y), I(X:Z)$, then $C_s = C_B - C_E$.

The Gaussian Wiretap Channel

[Leung-Yang-Cheong and Hellman 1978]:



$$\mathbf{Y}^n = \mathbf{X}^n + \mathbf{N}_y^n$$

$$\mathbf{Z}^n = \mathbf{X}^n + \mathbf{N}_z^n$$

$$\left.\begin{array}{l} \mathbf{N}_y^n \sim \mathcal{CN}(\mathbf{0}, \sigma_y^2 \mathbf{I}_{n\times n}) \\ \mathbf{N}_z^n \sim \mathcal{CN}(\mathbf{0}, \sigma_z^2 \mathbf{I}_{n\times n}) \end{array}\right\} \text{Gaussian noise}$$

Observations

- Secrecy capacity does not depend on the correlation between $\mathbf{N}_y^n, \mathbf{N}_z^n$.

- The Gaussian wiretap channel **is degraded:**

Eve's signal = Bob's signal + **Gaussian noise** (or vice versa)

1. If $\sigma_z^2 \geq \sigma_y^2$: $\mathbf{Y}^n = \mathbf{Z}^n + \tilde{\mathbf{N}}^n$ $\Rightarrow$ $\mathbf{X}^n - \mathbf{Z}^n - \mathbf{Y}^n$
2. If $\sigma_y^2 \geq \sigma_z^2$: $\mathbf{Z}^n = \mathbf{Y}^n + \tilde{\mathbf{N}}^n$ $\Rightarrow$ $\mathbf{X}^n - \mathbf{Y}^n - \mathbf{Z}^n$

$$\tilde{\mathbf{N}}^n \sim \mathcal{CN}(\mathbf{0}, |\sigma_y^2 - \sigma_z^2| \mathbf{I}_{n\times n})$$

Secrecy Capacity

- The secrecy capacity of the Gaussian wiretap channel is

$$C_s = \left[\frac{1}{2} \log\left(1 + \frac{P}{\sigma_y^2}\right) - \frac{1}{2} \log\left(1 + \frac{P}{\sigma_z^2}\right) \right]^+$$

$$= [C_B - C_E]^+$$

- P is the power constraint at Alice
- C_B is the capacity of the channel to Bob
- C_E is the capacity of the channel to Eve

Positive Secrecy Rates

$$C_s = [C_B - C_E]^+$$

- When Bob's channel is better, $C_s \geq 0.$
- When Eve's channel is better, $C_s = 0.$

Proof of Secrecy Capacity

- **Recall:** For degraded wiretap channel

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

- For $\sigma_z^2 \geq \sigma_y^2$, we have

$$\begin{aligned} I(X;Y) - I(X;Z) &= h(Z \mid X) - h(Z \mid Y) - [h(Z) - h(Y)] \\ &= \frac{1}{2}\log(2\pi e \sigma_z^2) - \frac{1}{2}\log(2\pi e \sigma_y^2) - [h(Y + \tilde{N}) - h(Y)] \end{aligned}$$

where $\tilde{N} \sim \mathcal{CN}(0, \sigma_z^2 - \sigma_y^2)$

Proof II

$$I(X;Y)-I(X;Z)=\frac{1}{2}\log(2\pi e\sigma_z^2)-\frac{1}{2}\log(2\pi e\sigma_y^2)\underbrace{-[h(Y+\tilde{N})-h(Y)]}_{(*)}$$

- Which X maximizes (*)?

- **Entropy Power Inequality (EPI):** If U,V are independent random variables, then

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

and the equality holds if and only if U,V are Gaussian

Proof III

- Use EPI to **maximize** $h(Y)-h(Y+\tilde{N})$:

$$h(Y)-h(Y+\tilde{N}) \leq h(Y)-\frac{1}{2}\log\left(2^{2h(Y)}+2\pi e(\sigma_z^2-\sigma_y^2)\right)$$

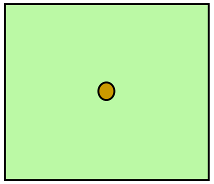
$$\leq \frac{1}{2}\log(2\pi e)(P+\sigma_y^2)-\frac{1}{2}\log\left(2^{2h(Y)}+2\pi e(\sigma_z^2-\sigma_y^2)\right)$$

$$=\frac{1}{2}\log\left(1+\frac{P}{\sigma_y^2}\right)-\frac{1}{2}\log\left(1+\frac{P}{\sigma_z^2}\right)$$

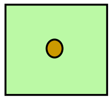
- Both inequalities are achieved with equality when X is Gaussian, i.e., $X\sim\mathcal{CN}(0,P)$.

Stochastic Encoding: Example

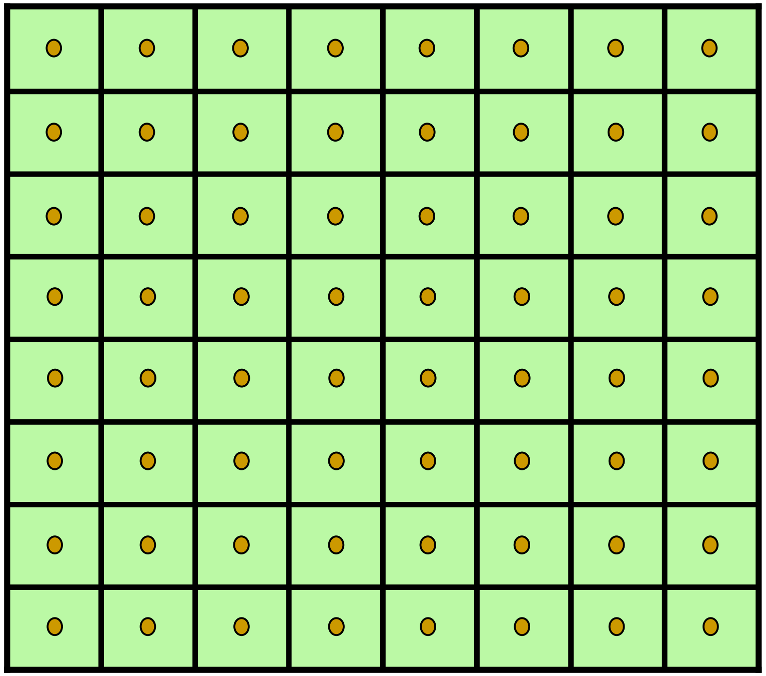
Eve's noise



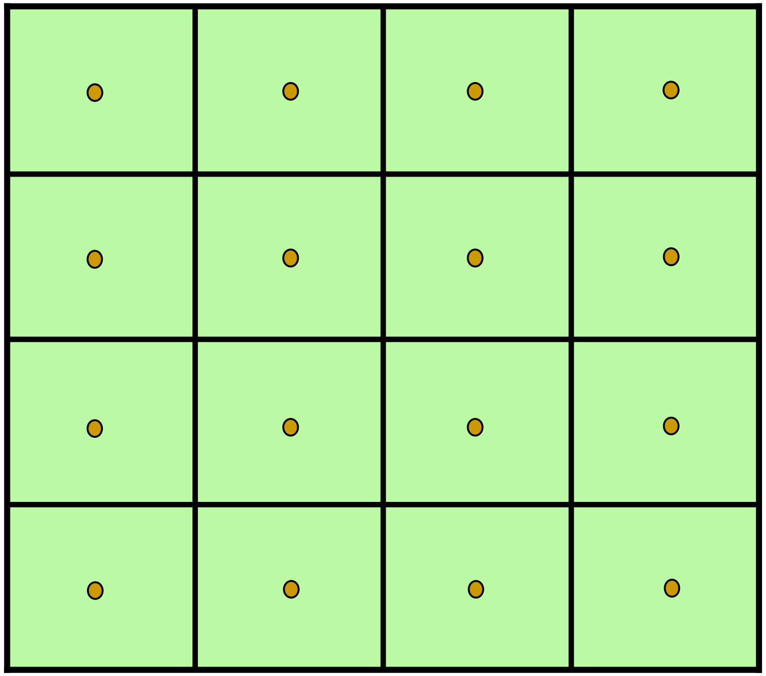
Bob's noise



Bob's constellation



Eve's constellation

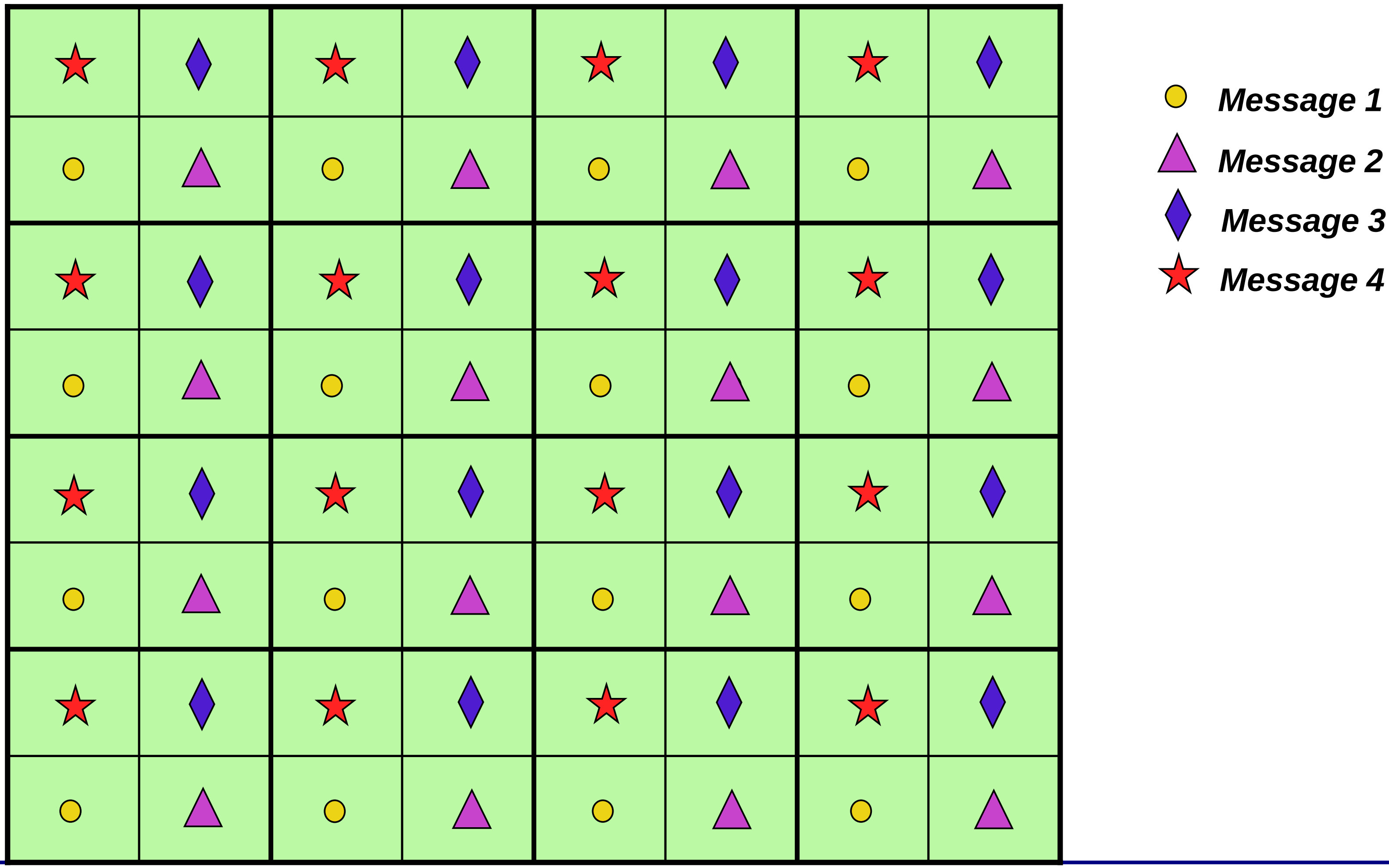


$$C_B = \log_2 64 = 6 \text{ b/s}$$

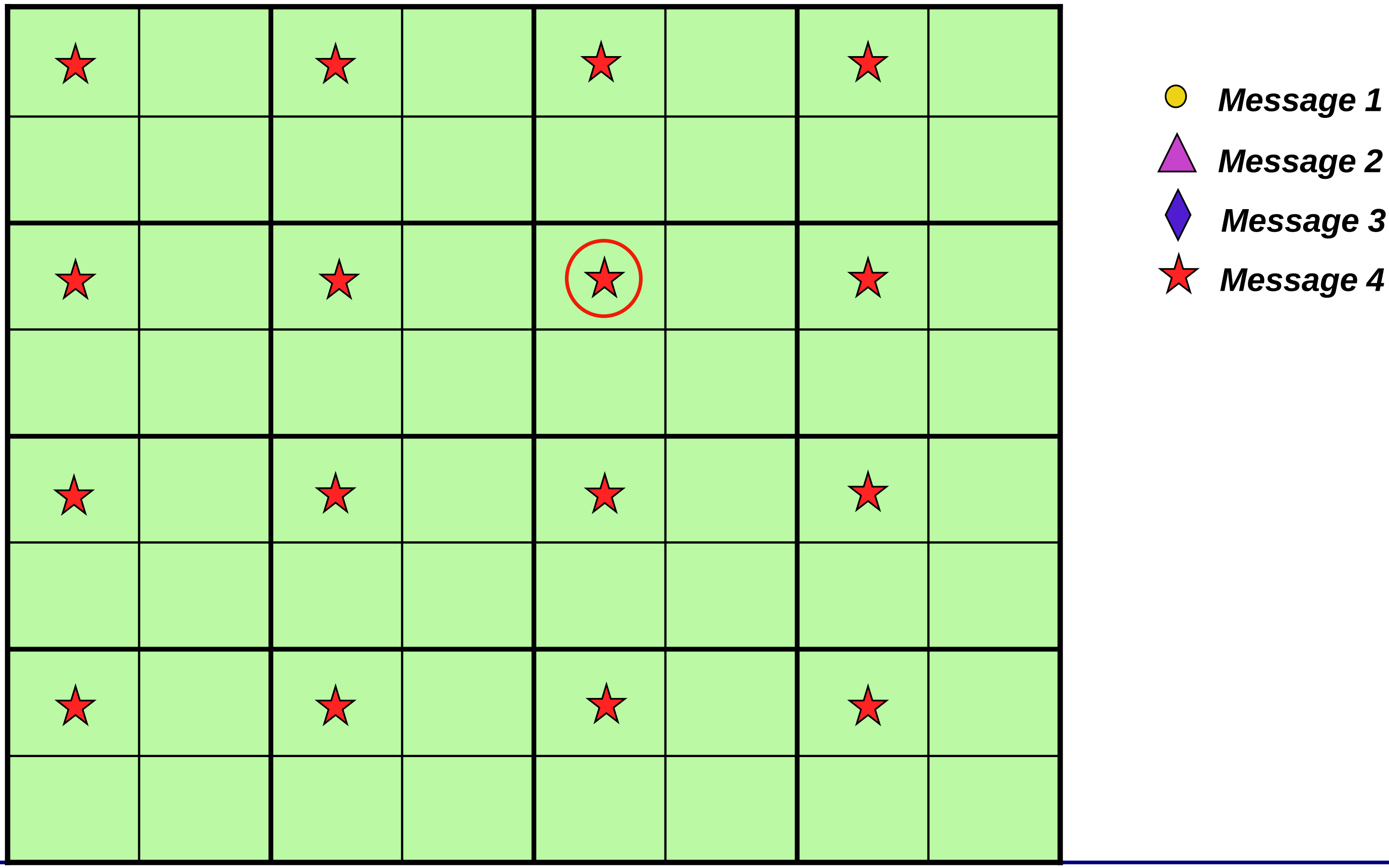
$$\boxed{\begin{aligned} C_s &= C_B - C_E \\ &= 2 \text{ b/s} \end{aligned}}$$

$$C_E = \log_2 16 = 4 \text{ b/s}$$

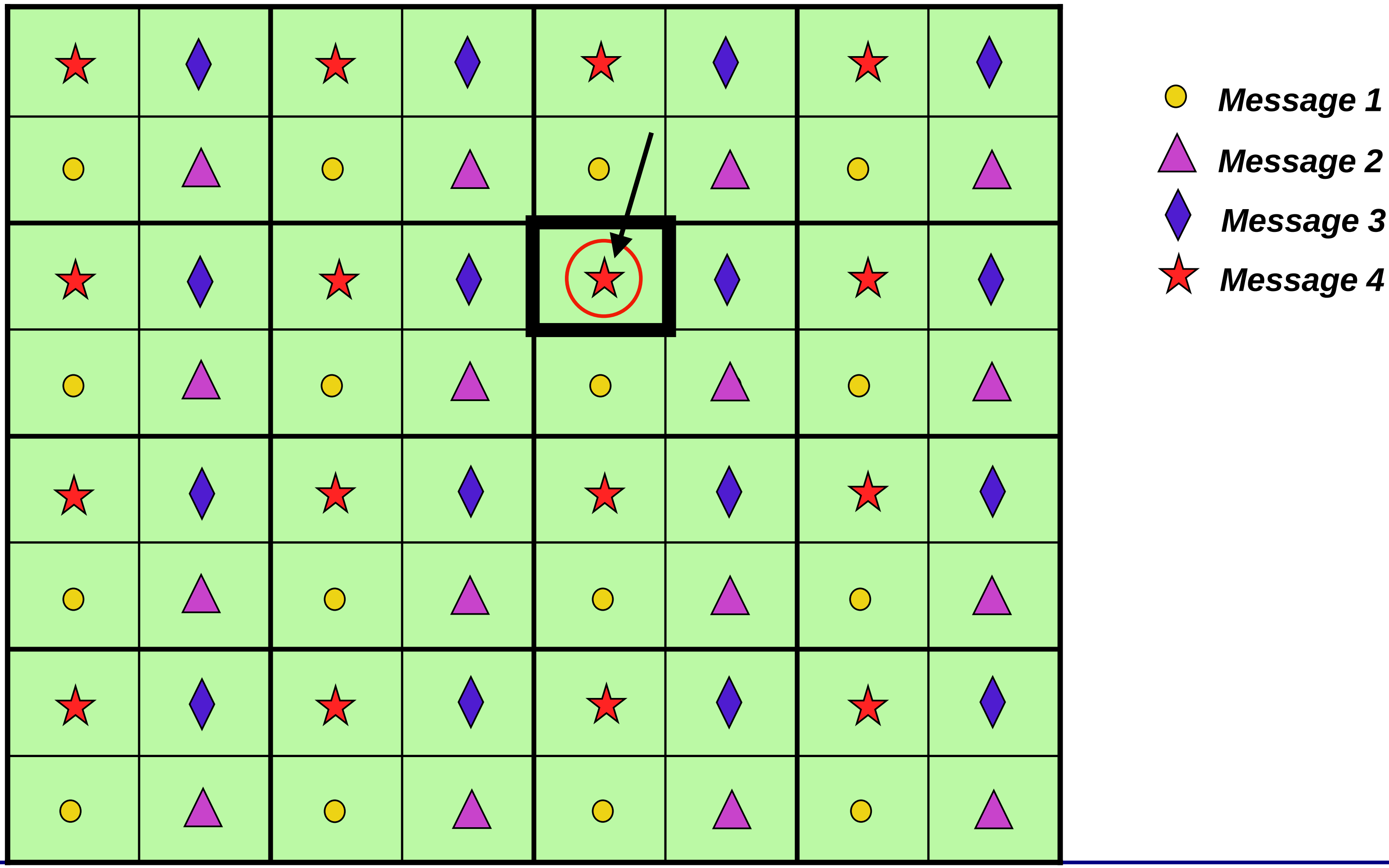
Divide Bob's constellation into subsets of 4 messages.



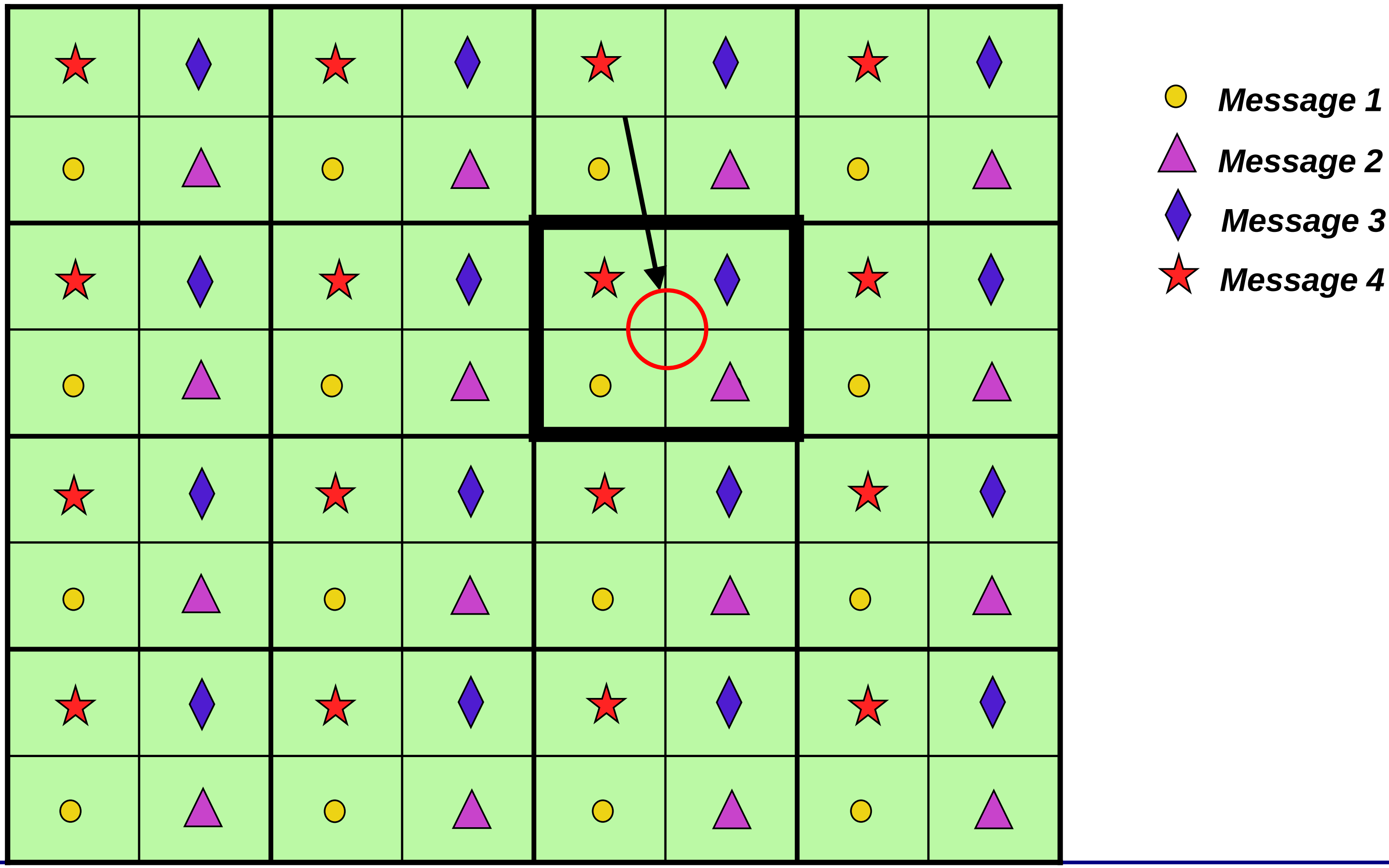
All red stars denote the same message. Pick one randomly.



Bob can decode the message reliably.



For Eve, all 4 messages are equally-likely.



From 1970's to 2000s

- **Information theoretic secrecy is very powerful:**
  - Unlimited computational power at Eve,
  - Eve knows everything Bob does (codebook, scheme),
  - Unbreakable, provable, and quantifiable secrecy.
- BUT: we need channel advantage for + secrecy rates:

Can this advantage be created?

Multi-terminal Scenarios

- Wireless networks:
  - Signals naturally superpose over the air
  - Interference
  - Fading (time-variations in the channel)
  - Cooperation/relaying
  - Multiple antennas

Each of these are potential resources for providing information theoretic guarantees for confidentiality.

Network Design

- Mixing of signals on air is an asset for confidentiality (even better if we design transmitted signals carefully!!!)

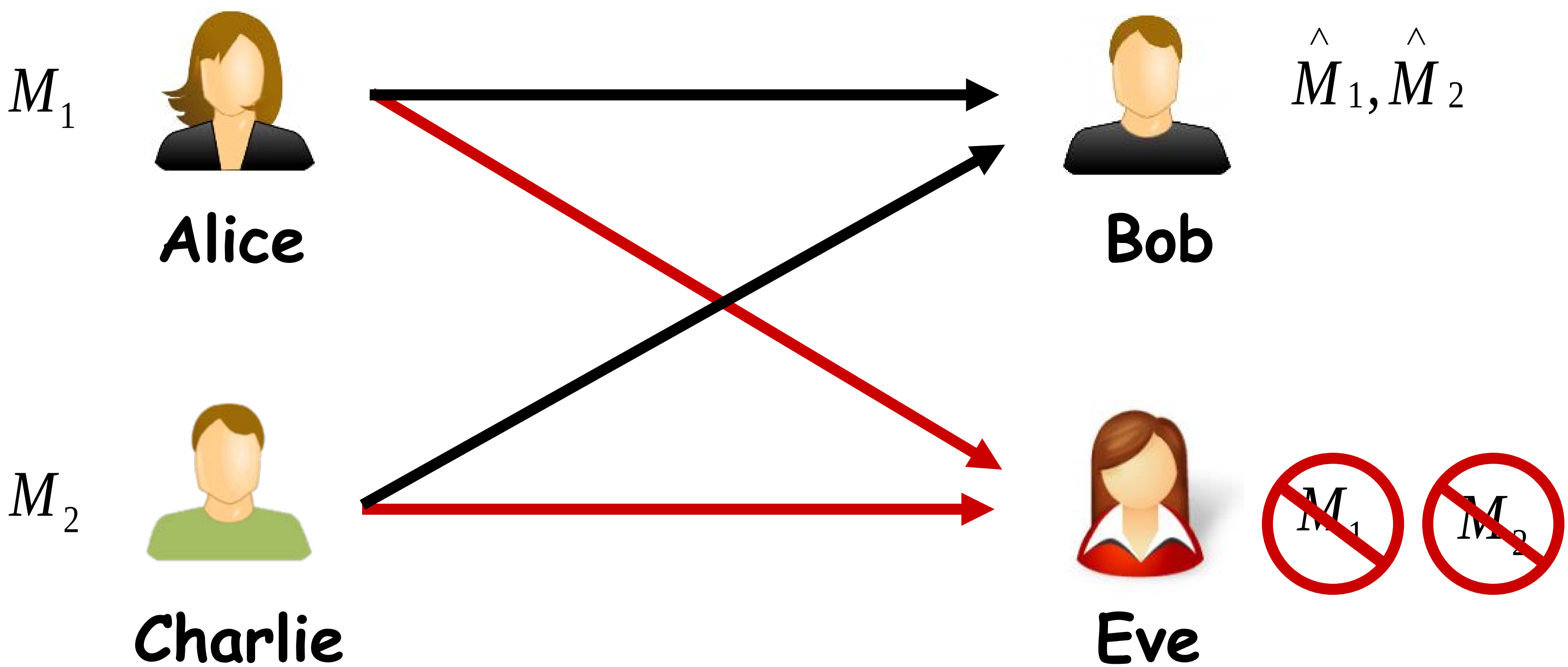
- **Bottom-line:**

  Network can be designed to bring an "effective" channel advantage to legitimate entities.

The Gaussian Multiple Access Wiretap Channel

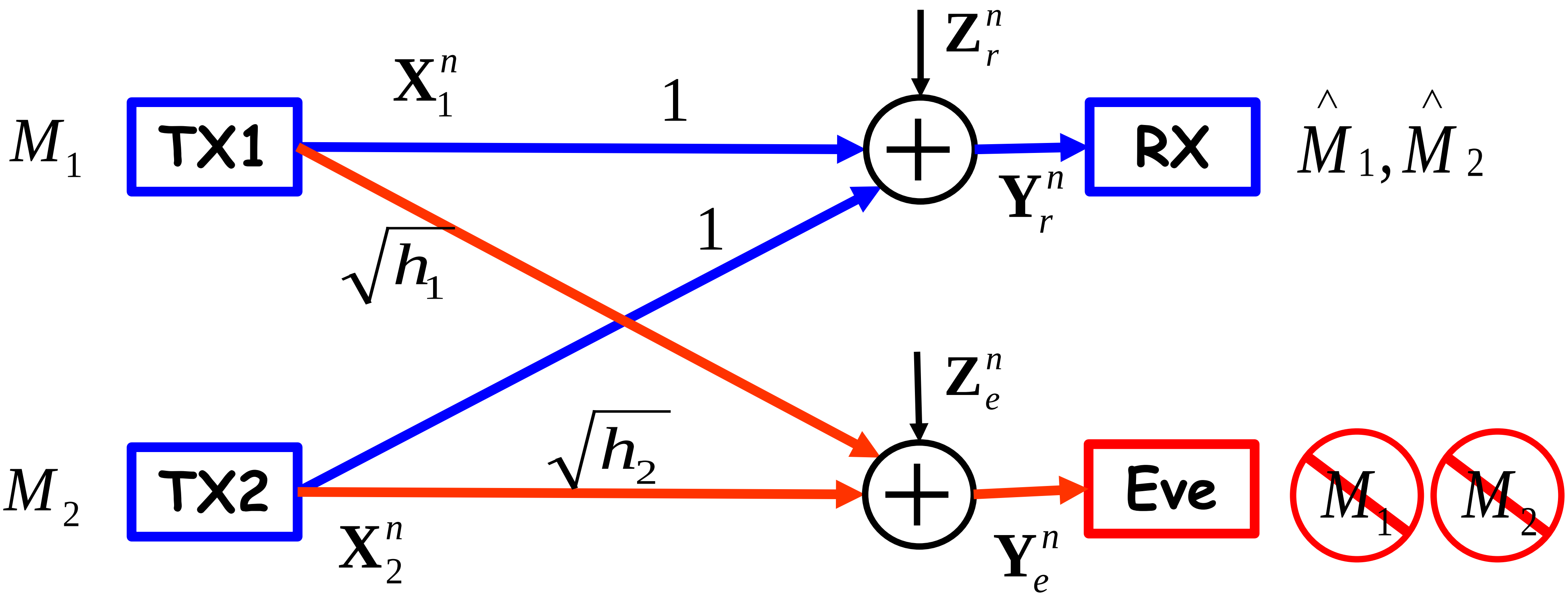
Wireless Communications & Networking Laboratory
WCAN@PSU

[Tekin-Serbetli-Y., 2005]



Secrecy constraint: $\lim_{n\to\infty} \frac{1}{n} I(M_1, M_2; \mathbf{Z}^n) = 0$

Channel Model



- The power constraint at user k is P_k.
- Secrecy capacity is open in general.

Achievable Region [Tekin-Y. 2008]

The following region is achievable

$$\left\{\left(R_1, R_2\right): R_1 \le \frac{1}{2}\left[\log\left(1+P_1\right)-\log\left(1+\frac{h_1 P_1}{1+h_2 P}\right)\right]\right.$$

$$R_2 \le \frac{1}{2}\left[\log\left(1+P_2\right)-\log\left(1+\frac{h_2 P_2}{1+h_1 P_1}\right)\right]$$

$$\left.R_1+R_2 \le \frac{1}{2}\left[\log\left(1+P_1+P_2\right)-\log(1+h_1 P_1+h_2 P_2)\right]\right\}$$

Achievable Region

TDMA: The following region is achievable

Time sharing $0 \le \alpha_k \le 1$

$$\bigcup_{\substack{0\le\alpha_k\le1 \\ \alpha_1+\alpha_2=1}} \left\{ (R_1, R_2) : R_k \le \frac{\alpha_k}{2}\left[\log\left(1+\frac{P_k}{\alpha_k}\right) - \log\left(1+\frac{h_k P_k}{\alpha_k}\right)\right], \quad k=1,2 \right\}$$

The convex closure of the union of the two regions is achievable

Achievability Outline I

Random-Binning region:

- Each user performs stochastic encoding (random binning):
  - Generate code C_k : consists of $2^{n(R_k+\tilde{R}_k)}$ i.i.d. cws ~ $\mathcal{N}(0, P_k - \varepsilon)$.
  - Randomly and independently distribute cws of C_k into 2^{nR_k} sub-codes $\tilde{C}_k(m_k)$, $m_k = 1, \dots, 2^{nR_k}$, of equal size ($2^{n\tilde{R}_k}$ cws.)
- **Encoding:** To send message M_k, user k picks a cw randomly at uniform from $\tilde{C}_k(M_k)$ and transmits it.
- **Decoding:** Joint-typicality decoding.

Achievability Outline II

TDMA region:

- Obtained when users who can achieve single-user secrecy, use a single-user wiretap code in a TDMA schedule.
  - The time share of user k is $0 \leq \alpha_k \leq 1$, where $\alpha_1 + \alpha_2 = 1$.
  - Transmitter k (having $h_k < 1$) transmits for α_k portion of time using power $\frac{P_k}{\alpha_k}$ while the other user is silent.

- When the WTC is degraded, i.e., $h_1 = h_2 = h$, the **TDMA region** is **a subset** from the region achieved by **random binning**.

General Multiple Access Wiretap Channel

- **Achievable rate region:**

$$
\textbf{Conv} \bigcup \{ (R_1, R_2):\ R_1, R_2 \geq 0,
$$

Convex hull

$$
R_1 \leq I(V_1; Y \mid V_2) - I(V_1; Z)
$$

$$
R_2 \leq I(V_2; Y \mid V_1) - I(V_2; Z)
$$

$$
R_1 + R_2 \leq I(V_1, V_2; Y) - I(V_1, V_2; Z) \}
$$

where the union is over all joint distributions that factorizes as

$$
p(x_1)\, p(x_2)\, p(v_1 \mid x_1)\, p(v_2 \mid x_2)\, p(y, z \mid x_1, x_2)
$$

Achievability Outline

- First, we show the following region is achievable using stochastic encoding at both users:

$$\bigcup\Big\{(R_1,R_2):\ R_1,R_2 \ge 0,$$
$$R_1 \le I(X_1;Y\,|\,X_2) - I(X_1;Z)$$
$$R_2 \le I(X_2;Y\,|\,X_1) - I(X_2;Z)$$
$$R_1 + R_2 \le I(X_1,X_2;Y) - I(X_1,X_2;Z)\Big\}$$

where $p(x_1,x_2,y,z) = p(x_1)p(x_2)p(y,z\,|\,x_1,x_2)$.

- Next, use channel prefixing at both users: $V_1 \to X_1,\ \ V_2 \to X_2$.

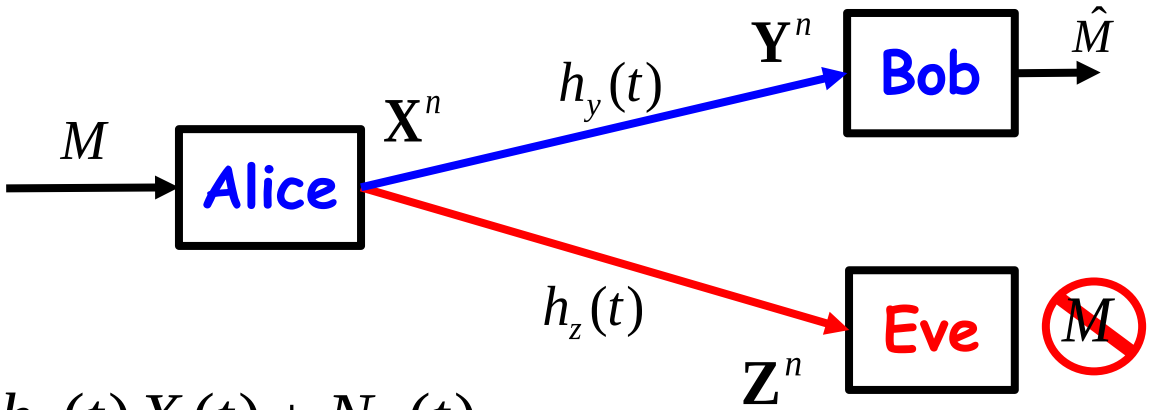
- Using time-sharing, the convex hull is achievable.

Fading Wiretap Channel

- In the Gaussian WTC, a channel advantage is needed for secrecy: $C_E \leq C_B$
- Fading (time-varying channel) ➔ opportunistic secrecy
  - Channel varies over time.
  - Can we use this channel variation to obtain or improve secrecy?

[Gopala-Lai-ElGamal 2008] [Liang-Poor-Shamai 2008] [Khisti-Tchamkerten-Wornell 2008]

Fading Wiretap Channel



$$\mathbf{X}^n = [X(1)\dots X(n)]$$
$$\mathbf{Y}^n = [Y(1)\dots Y(n)]$$
$$\mathbf{Z}^n = [Z(1)\dots Z(n)]$$

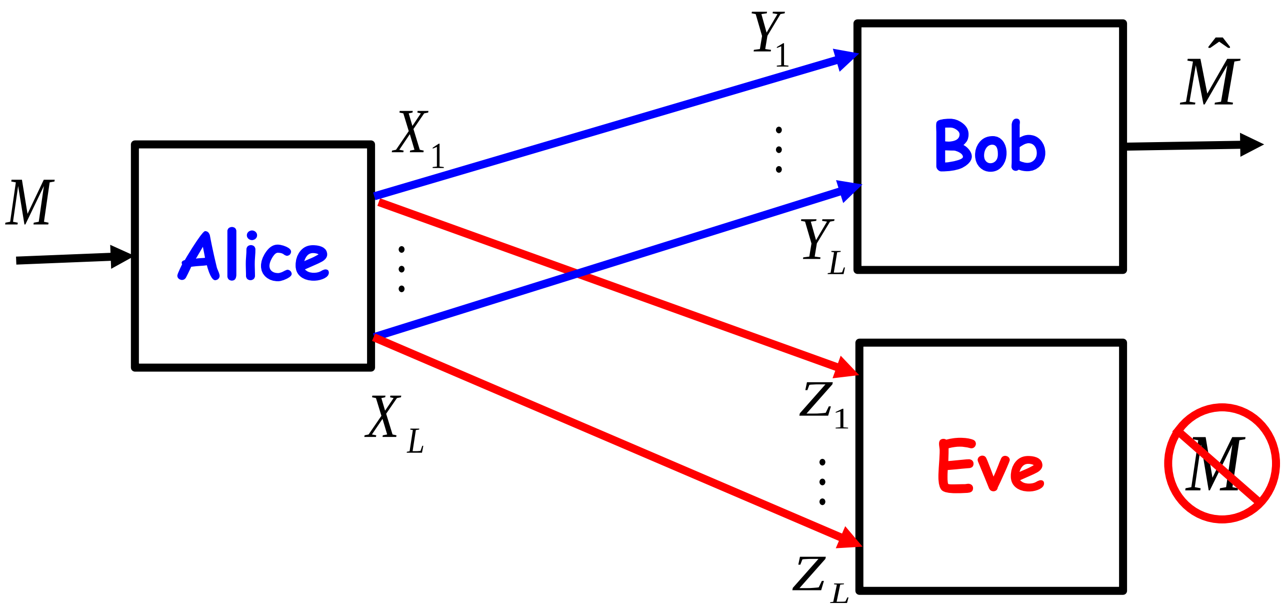
$$Y(t) = h_y(t)X(t) + N_y(t)$$
$$Z(t) = h_z(t)X(t) + N_z(t)$$
$$t = 1,2,\dots n$$
$$N_y \sim \mathcal{CN}(0,\sigma_y^2)$$
$$N_z \sim \mathcal{CN}(0,\sigma_z^2)$$

Gaussian noise indep. over time

Parallel Wiretap channel provides the framework to analyze the fading WTC **[Liang-Poor-Shamai 2008]**

Secrecy Capacity of Parallel WTC

[Liang-Poor-Shamai 2008]



Secrecy capacity of a sub-channel

$$C_s = \sum_{l=1}^{L} \max_{V_l - X_l - (Y_l, Z_l)} [I(V_l; Y_l) - I(V_l : Z_l)]^+ = \sum_{l=1}^{L} C_{s,l}$$

Fading WTC: Ergodic Secrecy Capacity

- Each realization of $h_y(t), h_z(t)$ can be viewed as a sub-channel that occurs with a positive probability.

- **By averaging** over all possible channel realization, we obtain the **ergodic secrecy capacity**

$$C_s = \max \mathrm{E}\left(\frac{1}{2}\log\left(1+\frac{h_y^2 P(h_y,h_z)}{\sigma_y^2}\right)-\frac{1}{2}\log\left(1+\frac{h_z^2 P(h_y,h_z)}{\sigma_z^2}\right)\right)$$

The maximization is over all possible power allocation schemes $P(h_y,h_z)$ satisfying $\mathrm{E}_{h_y,h_z}(P(h_y,h_z)) \le P$

Power Allocation

$$C_s = \max \mathrm{E}\left(\frac{1}{2}\log\left(1+\frac{h_y^2 P(h_y,h_z)}{\sigma_y^2}\right)-\frac{1}{2}\log\left(1+\frac{h_z^2 P(h_y,h_z)}{\sigma_z^2}\right)\right)$$

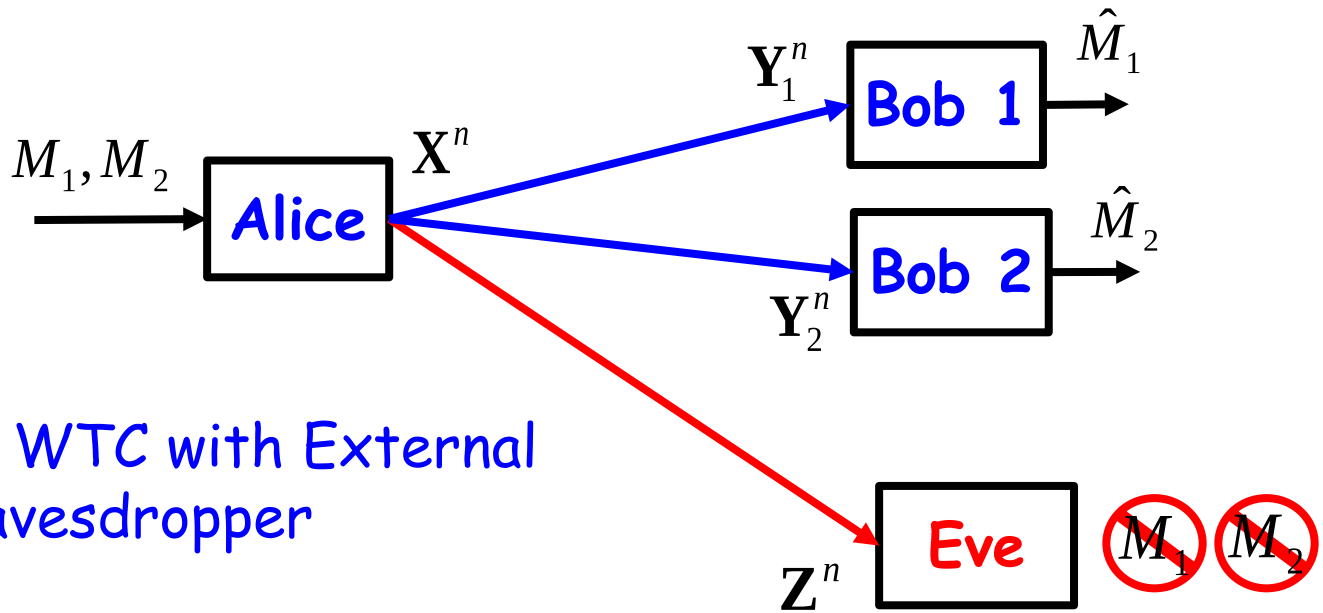
- **If $\frac{h_y^2}{\sigma_y^2} \le \frac{h_z^2}{\sigma_z^2}$, the term inside expectation = 0**

$\Rightarrow$ $P(h_y,h_z)=0$ if $\frac{h_y^2}{\sigma_y^2} \le \frac{h_z^2}{\sigma_z^2}$

No power should be allocated for such channel realizations

$\Rightarrow$ **Optimal power allocation** is **water-filling** over the channel realizations satisfying $\frac{h_y^2}{\sigma_y^2} > \frac{h_z^2}{\sigma_z^2}$

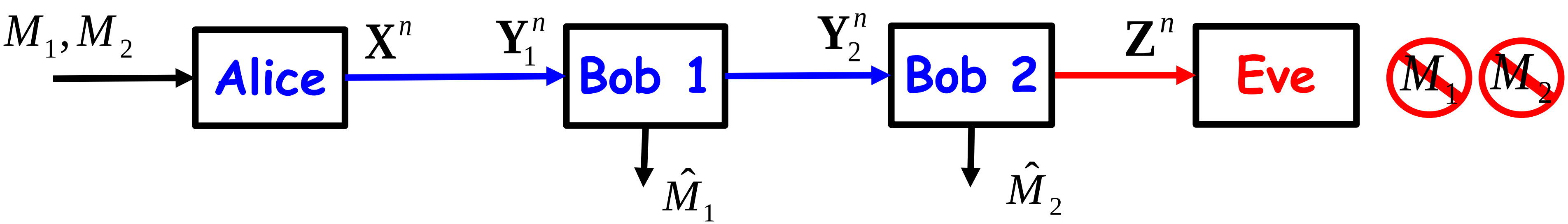
Broadcast Wiretap Channel



Broadcast WTC with External Eavesdropper

- **Secrecy Constraint:** $\lim_{n\to\infty} \frac{1}{n} I(M_1, M_2; \mathbf{Z}^n) = 0$

Degraded Broadcast Wiretap Channel



- Signals received by **Bob1**, **Bob2**, and **Eve** satisfy the degradedness order $X - Y_1 - Y_2 - Z$
- This generalizes Wyner's WTC model to a **multi-receiver** channel. **[Ekrem-Ulukus 2009]**

Secrecy Capacity Region

[Ekrem-Ulukus 2009]:

Secrecy capacity region for the **degraded broadcast wiretap channel** is

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

where U satisfies $U - X - Y_1 - Y_2 - Z$ is a Markov chain.

Achievability: Super-position coding + stochastic encoding

Achievable Rate Region: General Case

- An achievable rate region for the **Broadcast wiretap channel** is

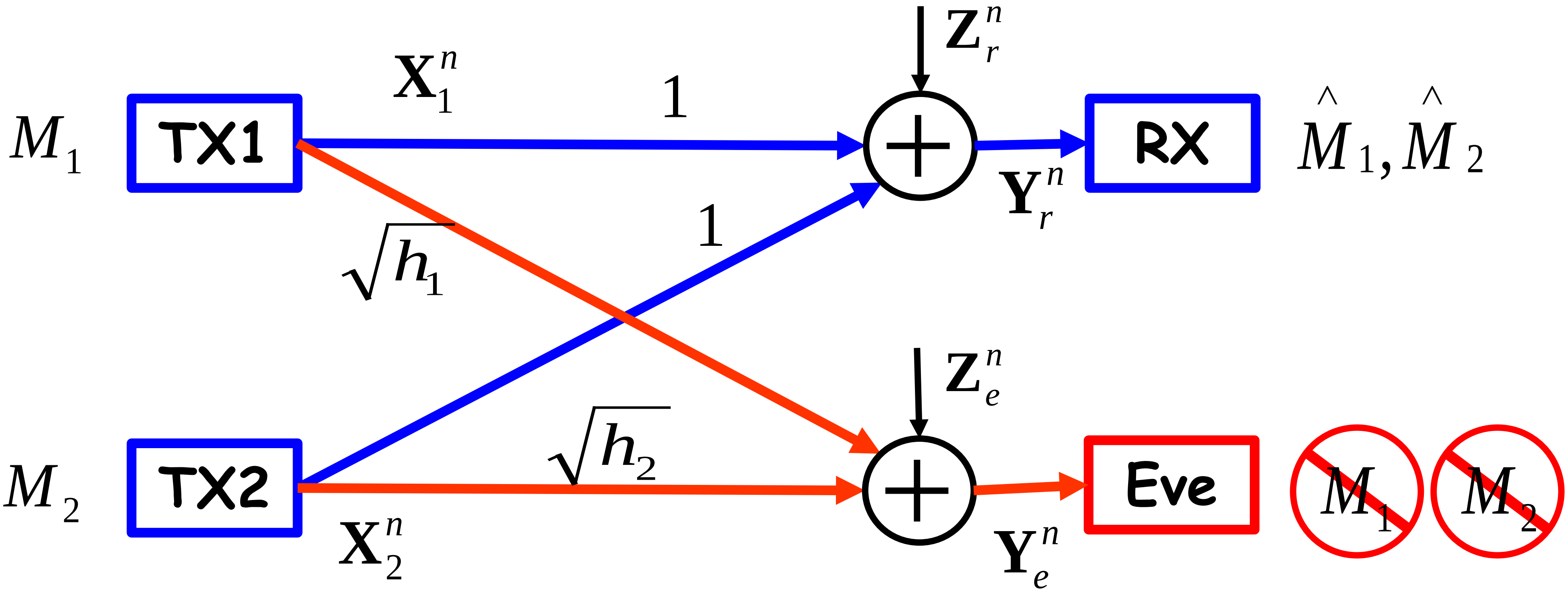
$$\mathcal{R}^{\text{in}} = \text{conv}\left(\mathcal{R}_{12} \cup \mathcal{R}_{21}\right)$$

where
$$\mathcal{R}_{12} = \Big\{(R_1, R_2) : R_1 \le I(V_1;Y_1) - I(V_1;Z)$$
$$R_2 \le I(V_2;Y_2) - I(V_2;Z \,|\, V_1) - I(V_1;V_2)\Big\}$$

for some (V_1,V_2) s.t. $(V_1,V_2) - X - (Y_1,Y_2,Z)$ is a Markov chain. $\mathcal{R}_{21}$ is obtained by switching the rate constraints.

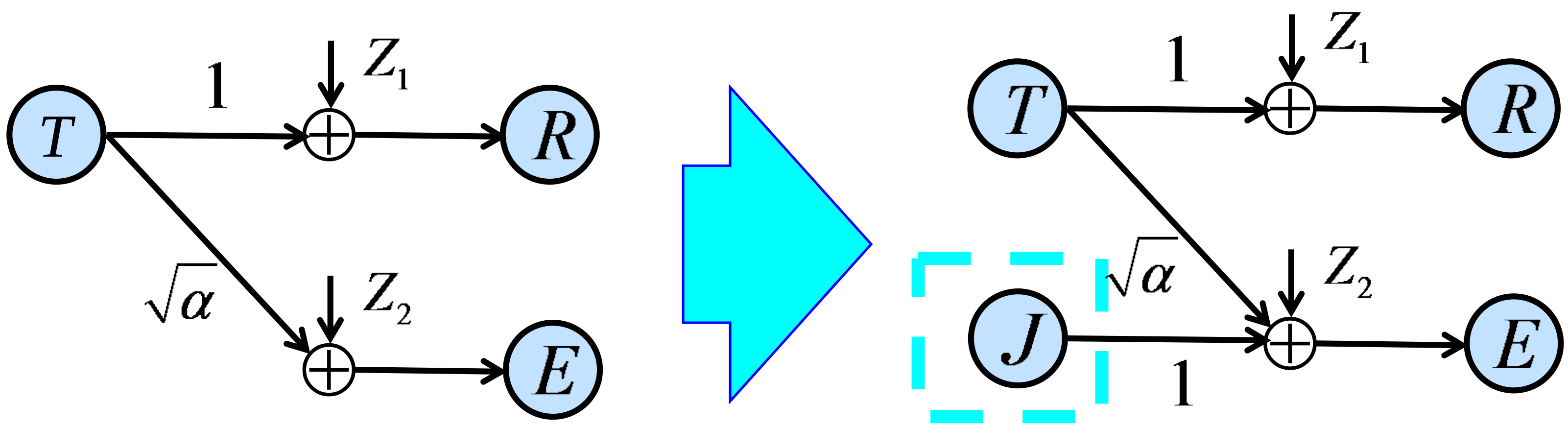
Achievability: Marton coding + stochastic encoding

Back to Multiple Transmitters…



- Can we improve the achievable rates?

Utilizing Interference



- "J" can transmit noise to interfere the eavesdropper "E".
- Information can be transmitted from "T" to "R" at a higher rate with this "Cooperative Jamming".

➡ **Interference can benefit secrecy.**

Cooperative Jamming

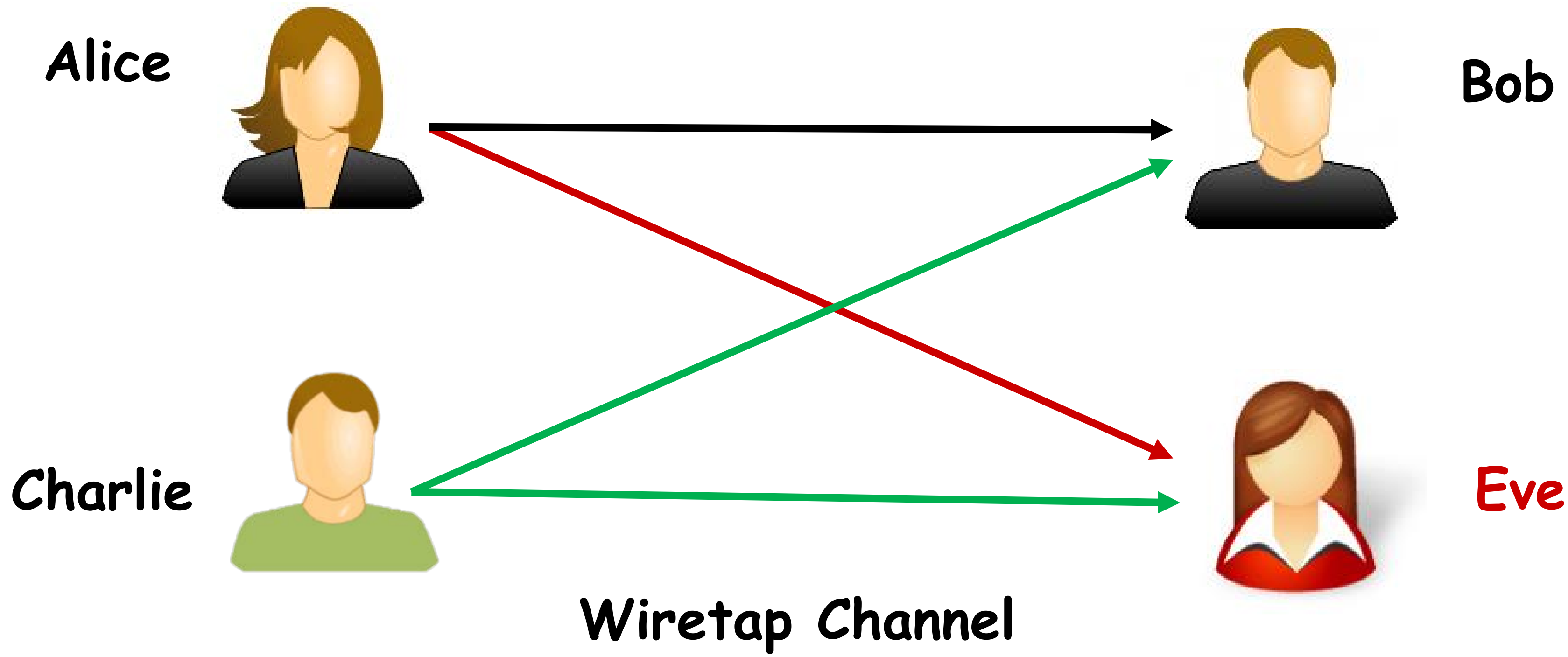
[Tekin-Y., 2006]

- In MAC-WT, a user who can not achieve positive secrecy rate for his own, can opt to transmit noise to hurt the eavesdropper Eve.

- This user has *a better channel* to Eve than his channel to Bob, hence, hurting the reception of Eve more than Bob.

Creating a channel advantage!

MAC-WT: Cooperative Jamming



Wiretap Channel with a Cooperative Jammer

[Tekin-Y., 2006]

Cooperative Jamming Scheme

- Users are partitioned into two groups: "transmitting users" and "jamming users".
- Jamming user k transmits $\mathbf{X}_k \sim \mathcal{N}(0, P_k\mathbf{I})$ instead of transmitting cws.
- **Higher secrecy** rates can be achieved when "**weaker**" users are jamming.

  Weaker users = have better channel to Eve.

Achievable Sum-Secrecy Rate

Assume $h_1 < h_2$, hence user 2 is jamming.

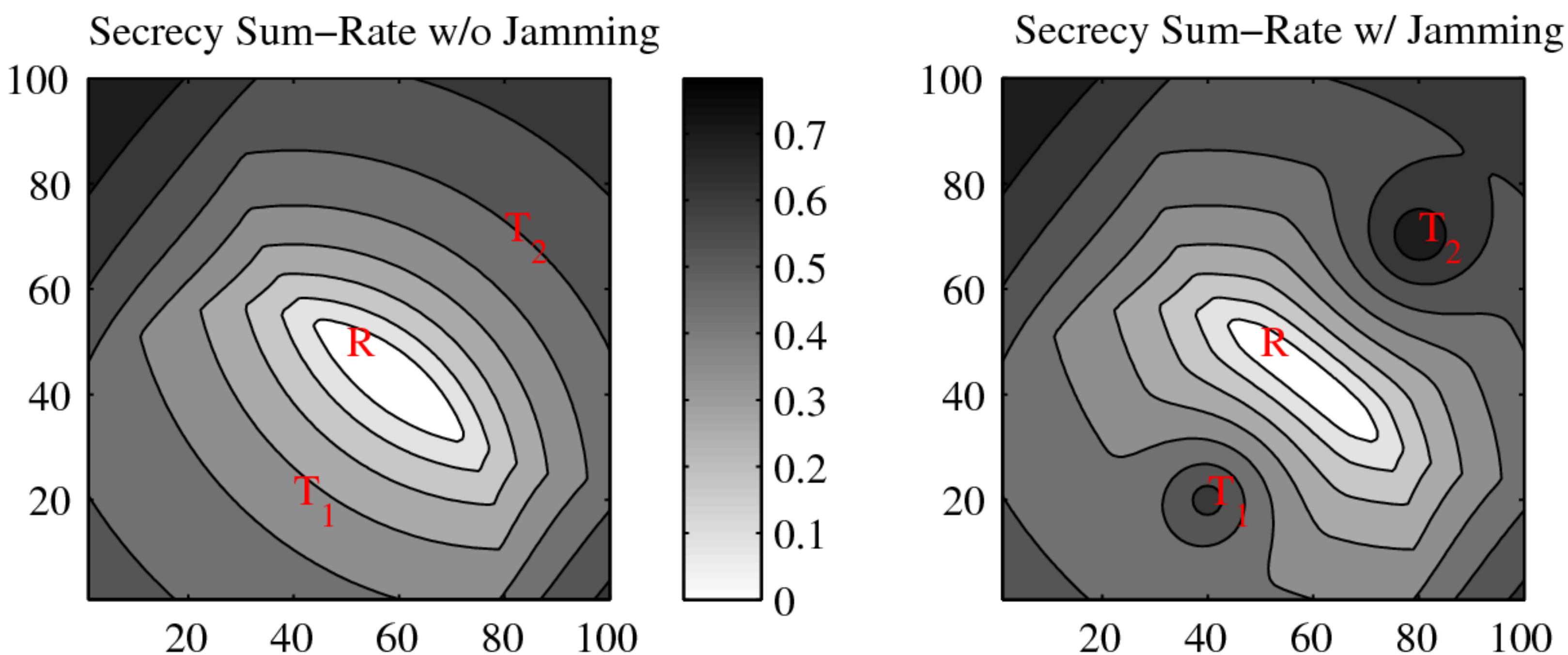
- Secrecy **sum-rate** achievable with cooperative jamming

$$R_1 + R_2 \le \frac{1}{2}\left[\log\left(1+\frac{P_1}{1+P_2}\right) - \log\left(1+\frac{h_1 P_1}{1+h_2 P_2}\right)\right]$$

- This sum-rate can be > $\frac{1}{2}\left[\log(1+P_1+P_2) - \log(1+h_1 P_1 + h_2 P_2)\right]$

Sum-Secrecy rate without cooperative jamming

Cooperative Jamming [Tekin-Y., 2006]



When Eve is close to one transmitter, that transmitter can hurt Eve more leading to a higher secrecy sum rate than if it tried to communicate.

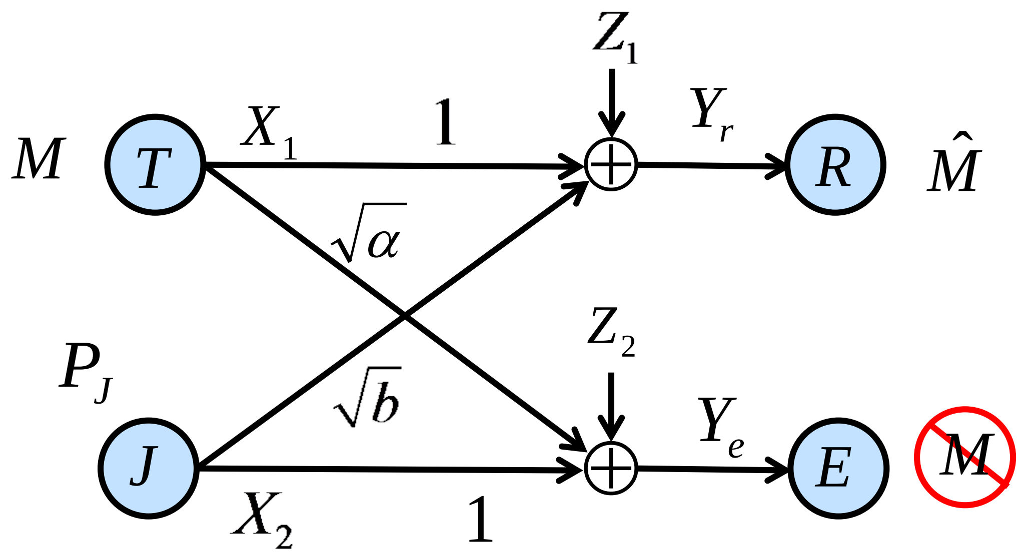
Cooperative Jamming [Tekin-Y., 2006]

Cooperative jamming can be noise [Tekin-Y. 2006-2008]

or from a codebook [Lai-H.ElGamal 2008], [He-Y. 2009/14]

When Eve is close to one transmitter, that transmitter can hurt Eve more leading to a higher secrecy sum rate than if it tried to communicate.

Cooperative Jamming with Noise



γ_b : SINR at Bob

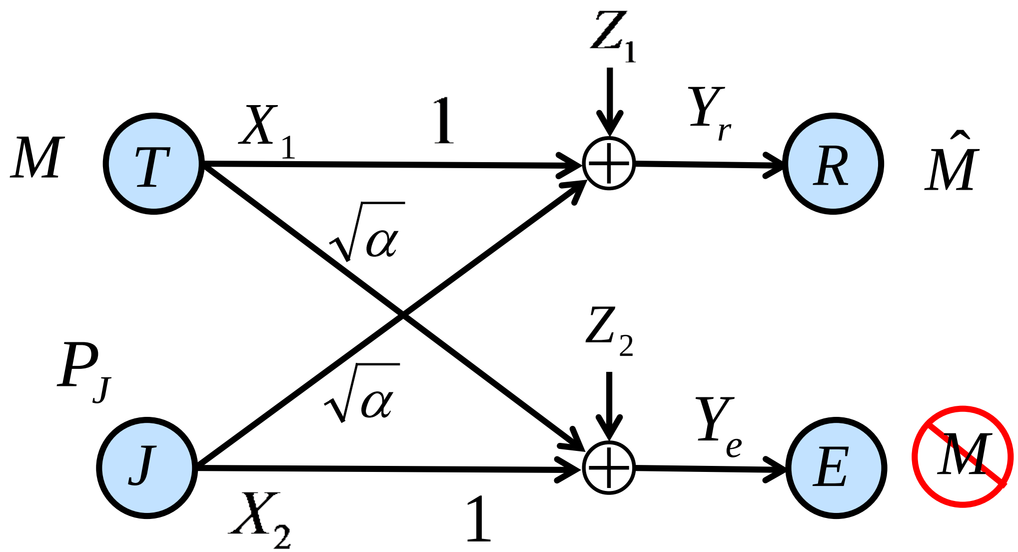
$\gamma_{e.}$: SINR at Eve

Gaussian Wiretap Channel with a cooperative jammer

- Cooperative Jammer J sends Gaussian noise to jam Eve.
- Jamming does affect the receiver R as well.
- Used when jamming cause more harm at Eve than Bob.

$$R_s = \frac{1}{2}\log\left(1+\gamma_b\right) - \frac{1}{2}\log\left(1+\gamma_e\right), \qquad P_J \uparrow \rightarrow \gamma_b \downarrow, \gamma_{e.} \downarrow$$

Cooperative Jamming with Random Codebook



- When $\alpha > 1$, cooperative jamming causes more harm at Bob than Eve.
- However, If jamming signal is from a codebook, Bob can decode this interference (The channel of interference to Bob is better than Eve.)

Cooperative Jamming with Random Codebook

- Cooperative jammer transmits a cw from a Gaussian codebook $\sim \mathcal{N}(0, P_J)$.
- Rate R_J is chosen s.t. Bob can decode the jamming signal by treating the rest part as noise;

$$R_J = \frac{1}{2}\log\left(1 + \frac{\alpha P_J}{1+P}\right)$$

- Bob subtracts the jamming signal from its received signal.

Cooperative Jamming with Random Codebook

- Alice uses stochastic encoding with randomization rate

$$\tilde{R}_s = \frac{1}{2}\log(1+\alpha P + P_J) - \frac{1}{2}\log\left(1+\frac{\alpha P_J}{1+P}\right)$$

- The achievable secrecy rate is:

$$R_s = \frac{1}{2}\log\left(\frac{1+P+\alpha P_J}{1+\alpha P + P_J}\right)$$

- R_s is positive when $P_J > P$.

Gaussian Signaling

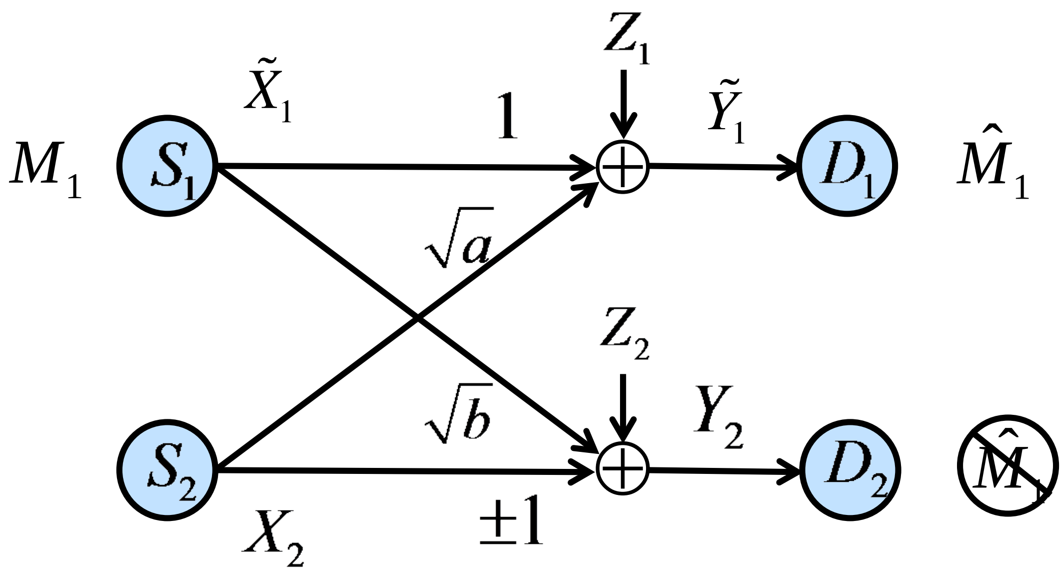
- **At low SNR,**

Gaussian i.i.d. signaling is within **0.5bit/ch use** from the secrecy capacity **[Ekrem-Ulukus, 2008].**

- **At high SNR,**

Gaussian signaling is **suboptimal** **[He-Y., 2009].**

Gaussian Signaling: Secrecy rate saturates as power increases.



Despite optimizing transmission power, and cooperative jamming, the secrecy rate converges to a constant with increasing signal power, when Gaussian signaling is used.

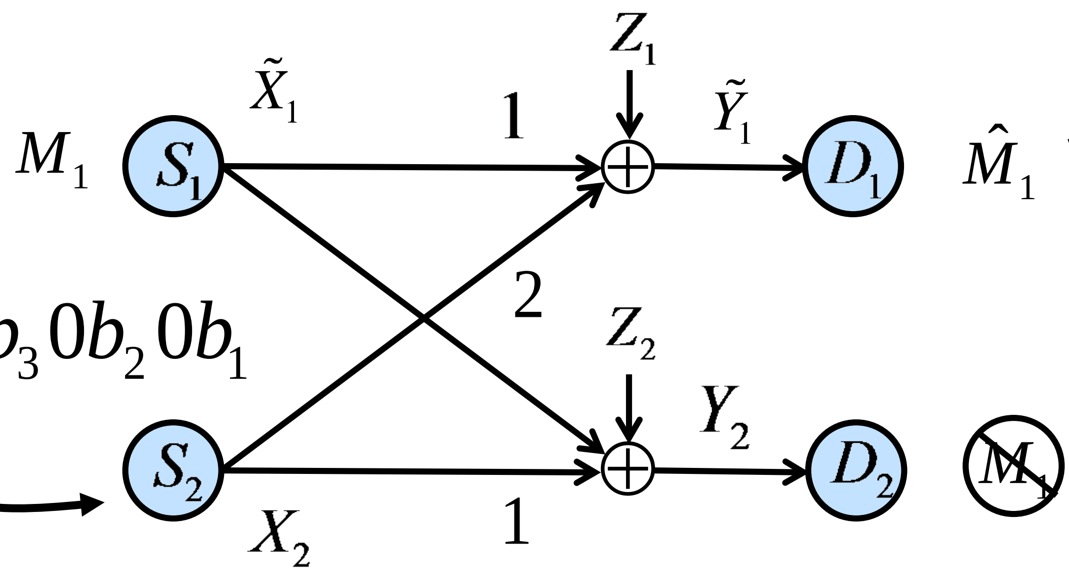
Can we do better?

Utilizing "Structure" in Transmissions

Binary Representation of

$$\tilde{X}_1 = a_K \ldots 0a_4 0a_3 0a_2 0a_1$$

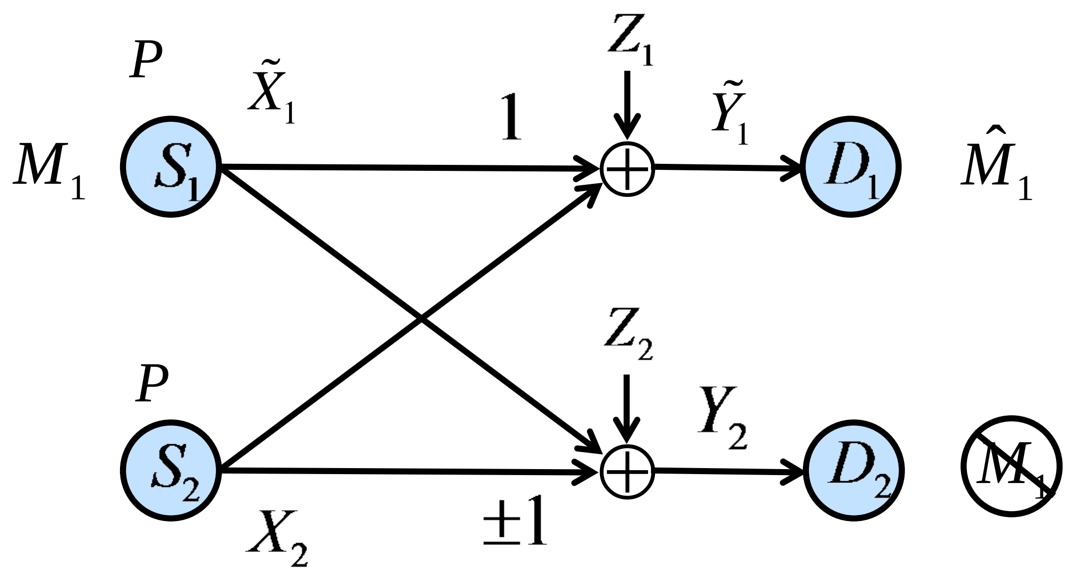
$$\tilde{X}_1 + 2X_2 = b_K a_K \ldots b_3 a_3 b_2 a_2 b_1 a_1$$



$$X_2 = b_K \ldots 0b_4 0b_3 0b_2 0b_1$$

$$\tilde{X}_1 + X_2 = b_K + a_K, \ldots, b_4 + a_4, b_3 + a_3, b_2 + a_2, b_1 + a_1$$

Gaussian WTC with a Cooperative Jammer: structured signaling



$$P \uparrow \rightarrow K \uparrow \rightarrow R_s \uparrow$$

Secrecy rate scales with power.

Can secrecy rate scale for all channel gains?

Achievable secrecy rate

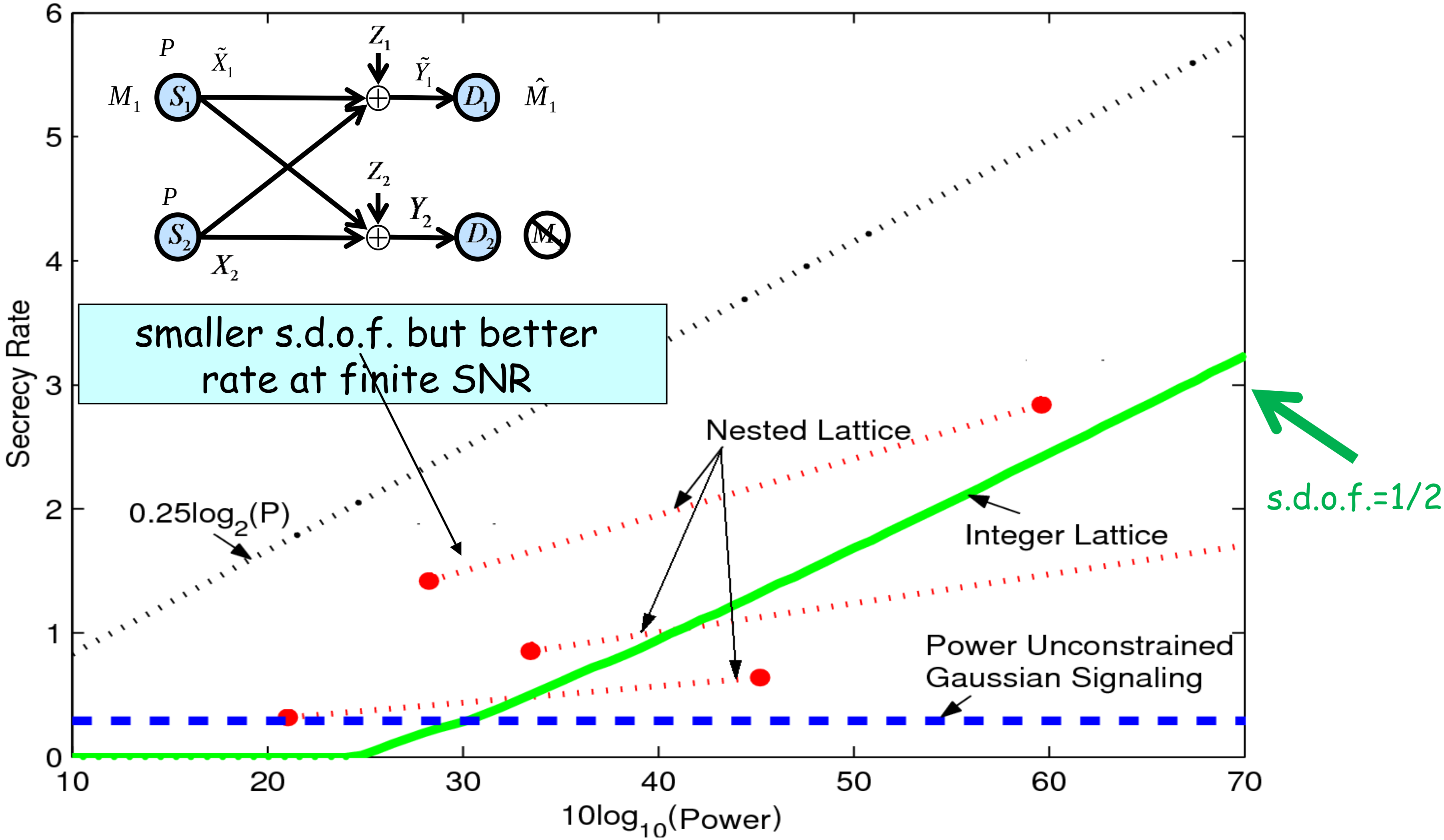
Secure degrees of freedom (s.d.o.f.) = $\lim_{P \to \infty} \frac{R_s}{\log P}$

Power constraint

YES. [He-Y. 2009/IT-2014]

- Achievable scheme uses Nested Lattice (NL) Codes and Integer Lattice Codes (ILC).
- **Enabler (NL):** Bound the leakage to Eve utilizing the structure of NL.
- Achievable scheme **can produce 1/2 (ILC).**
- **s.d.o.f. upper bound =2/3** [He (Thesis) 2010].

Achievable s.d.o.f. [He-Y. 2009/14]



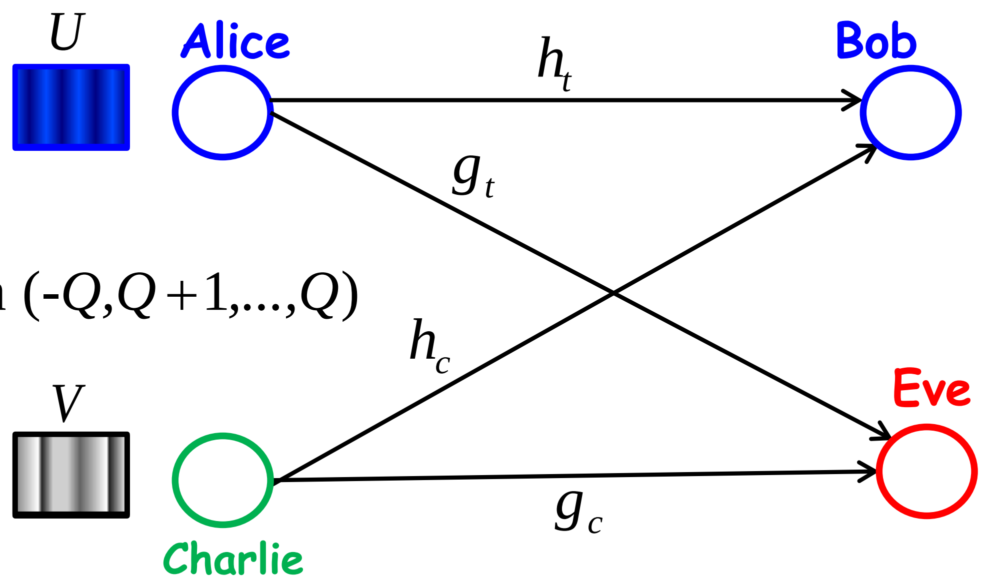
Settling the problem: s.d.o.f. of GWTC with a Cooperative Jammer

[Xie-Ulukus, 2012]:

$$X_t = \frac{1}{g_t} U$$

$$X_c = \frac{1}{g_c} V$$

$$U, V \sim \text{Uniform } (-Q, Q+1, \ldots, Q)$$



$$Y_r = \frac{h_t}{g_t} U + \frac{h_c}{g_c} V + Z_r$$

$$Y_e = (U + V) + Z_e$$

$\frac{h_t}{g_t}, \frac{h_c}{g_c}$ are **rationally independent**

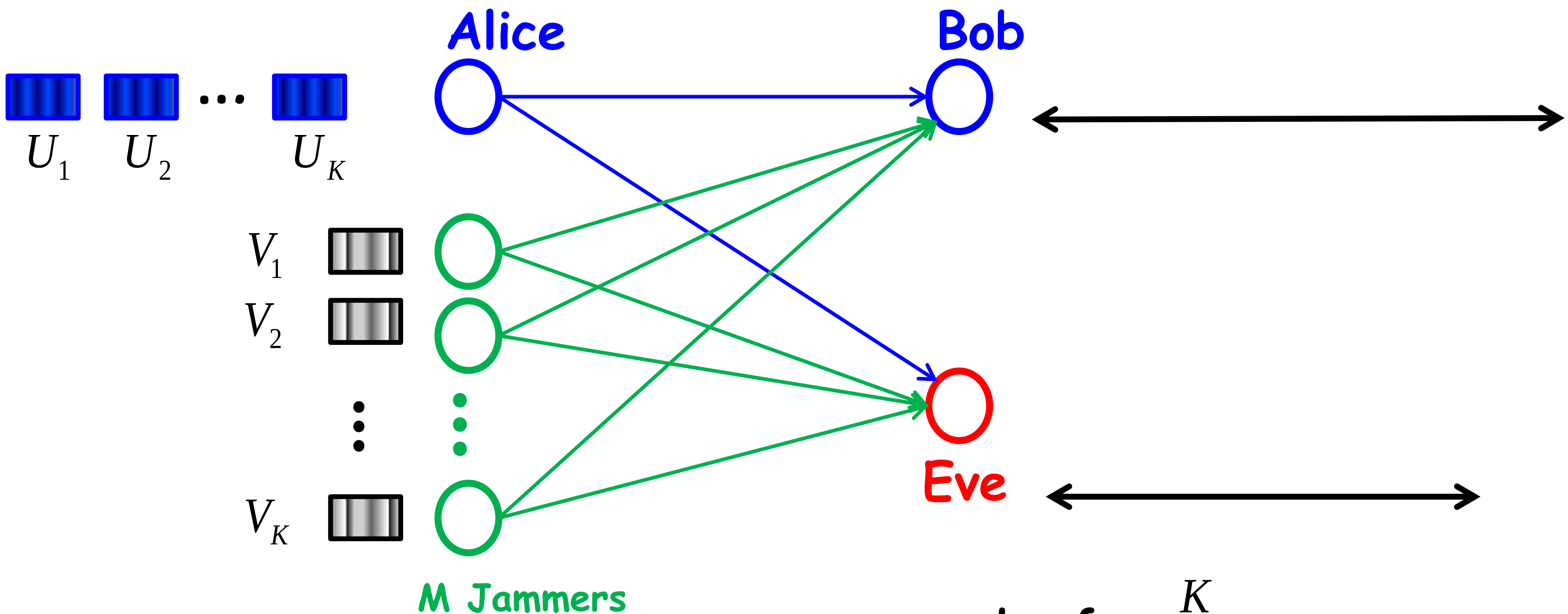
U is **uniquely** decoded at Bob [Motahari et.al. RIA]

Xie-Ulukus upperbound matches the achievable s.d.o.f.

$$\boxed{\text{s.d.o.f.} = \frac{1}{2}}$$

Single Antenna GWTC with K Independent Jammers

[Xie-Ulukus-2012]:

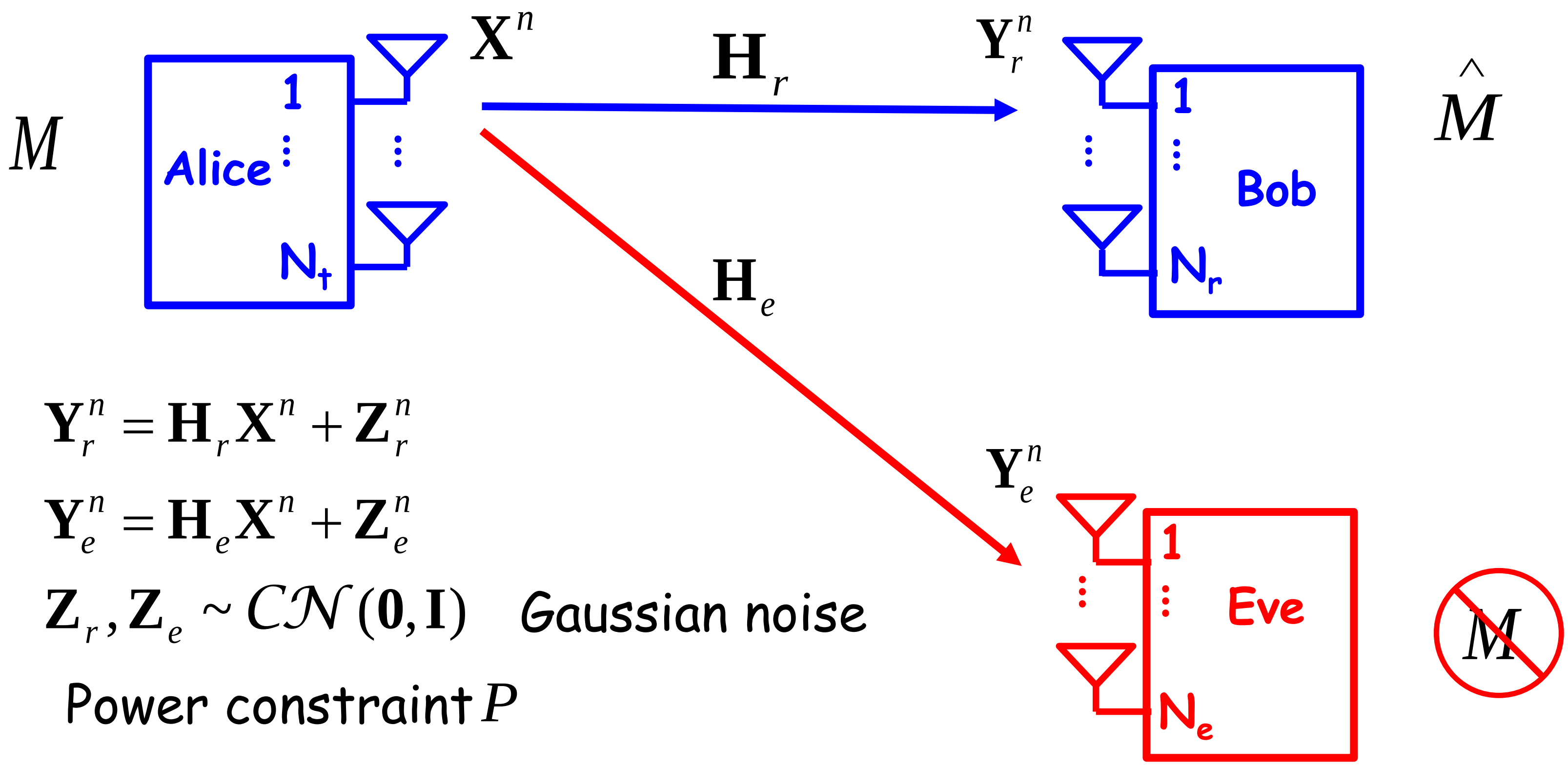


$$U_i, V_i \sim \text{Uniform}(-Q, Q+1, \ldots, Q)$$

$$\text{s.d.o.f.} = \frac{K}{K+1}.$$

Gaussian MIMO Wiretap Channel

[Khisti-Wornell, 2007] [Oggier-Hassibi, 2007] [Shafie-Liu-Ulukus, 2007]:



$$\mathbf{Y}_r^n = \mathbf{H}_r \mathbf{X}^n + \mathbf{Z}_r^n$$

$$\mathbf{Y}_e^n = \mathbf{H}_e \mathbf{X}^n + \mathbf{Z}_e^n$$

$\mathbf{Z}_r, \mathbf{Z}_e \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ Gaussian noise

Power constraint P

Secrecy Capacity

[Khisti-Wornell, 2007] [Oggier-Hassibi, 2007] [Shafie-Liu-Ulukus, 2007]:

- The secrecy capacity of the Gaussian MIMO WTC is

$$C_s = \max_{V - \mathbf{X}^n - (\mathbf{Y}_r^n, \mathbf{Y}_e^n)} I(V; \mathbf{Y}_r^n) - I(V; \mathbf{Y}_e^n)$$

$$= \max_{\mathbf{Q}:\, \mathrm{tr}(\mathbf{Q}) \le P} \frac{1}{2} \log \frac{\left|\mathbf{I} + \mathbf{H}_r \mathbf{Q} \mathbf{H}_r^H\right|}{\left|\mathbf{I} + \mathbf{H}_e \mathbf{Q} \mathbf{H}_e^H\right|}$$

- No channel prefixing is needed and Gaussian signaling is optimal.
- **Multiple antennas** help in creating a channel advantage.

Proof Outline

- The Gaussian MIMO wiretap channel **is *not degraded*:**

Secrecy capacity: $$C_s = \underbrace{\max_{V - \mathbf{X}^n - (\mathbf{Y}_r^n, \mathbf{Y}_e^n)} I(V;\mathbf{Y}_r^n) - I(V;\mathbf{Y}_e^n)}_{\substack{\text{Optimization problem} \\ \text{Hard to solve}}}$$

Approach:

1. Find a computable upper bound.
2. Compute an achievable secrecy rate by using a potentially suboptimal $(V, \mathbf{X}^n)$.
3. Show that the achievable rate matches the upper bound.

Computable Upper Bound

- **Consider an enhanced channel to Bob:**
  - A genie provides Eve's observation to Bob, i.e., $\tilde{\mathbf{Y}}_r^n = (\mathbf{Y}_r^n, \mathbf{Y}_e^n)$.
  - The enhanced channel is degraded (no channel prefixing is needed.)

$$\tilde{C}_s = \max_{\mathbf{X}^n} I(\mathbf{X}^n; \mathbf{Y}_r^n) - I(\mathbf{X}^n; \mathbf{Y}_e^n) = \max_{\mathbf{X}^n} I(\mathbf{X}^n; \mathbf{Y}_r^n \mid \mathbf{Y}_e^n)$$

  - The Optimal $\mathbf{X}^n$ is shown to be **Gaussian**.
- **The outer bound is tightened:**
  - The secrecy capacity of the original channel depends only on marginal distributions $p_{\mathbf{Y}_r|\mathbf{X}}$ and $p_{\mathbf{Y}_e|\mathbf{X}}$.
  - Yet, $I(\mathbf{X}^n; \mathbf{Y}_r^n \mid \mathbf{Y}_e^n)$ depends on the joint distribution $p_{\mathbf{Y}_r,\mathbf{Y}_e|\mathbf{X}}$.
  - Introducing **correlation between noises at Eve and Bob** tightens the upper bound.

Observations

- **Achievability:** Set $V = \mathbf{X}^n \sim \mathcal{CN}(\mathbf{0}, \mathbf{Q}_x)$.

  ➡ The derived outer bound is achievable.

- The upper bound corresponds to the secrecy capacity of an enhanced wiretap channel which is degraded.
  - Bob observes Eve's signal as well.
- This upper bound **is achievable** for the MIMO wiretap channel.
- The **optimal transmission** results in *an effective degraded channel*:
  - transmit over directions where Bob's channel is better than the channel to Eve).

High SNR Characterization

[Khisti-Wornell-2007]:

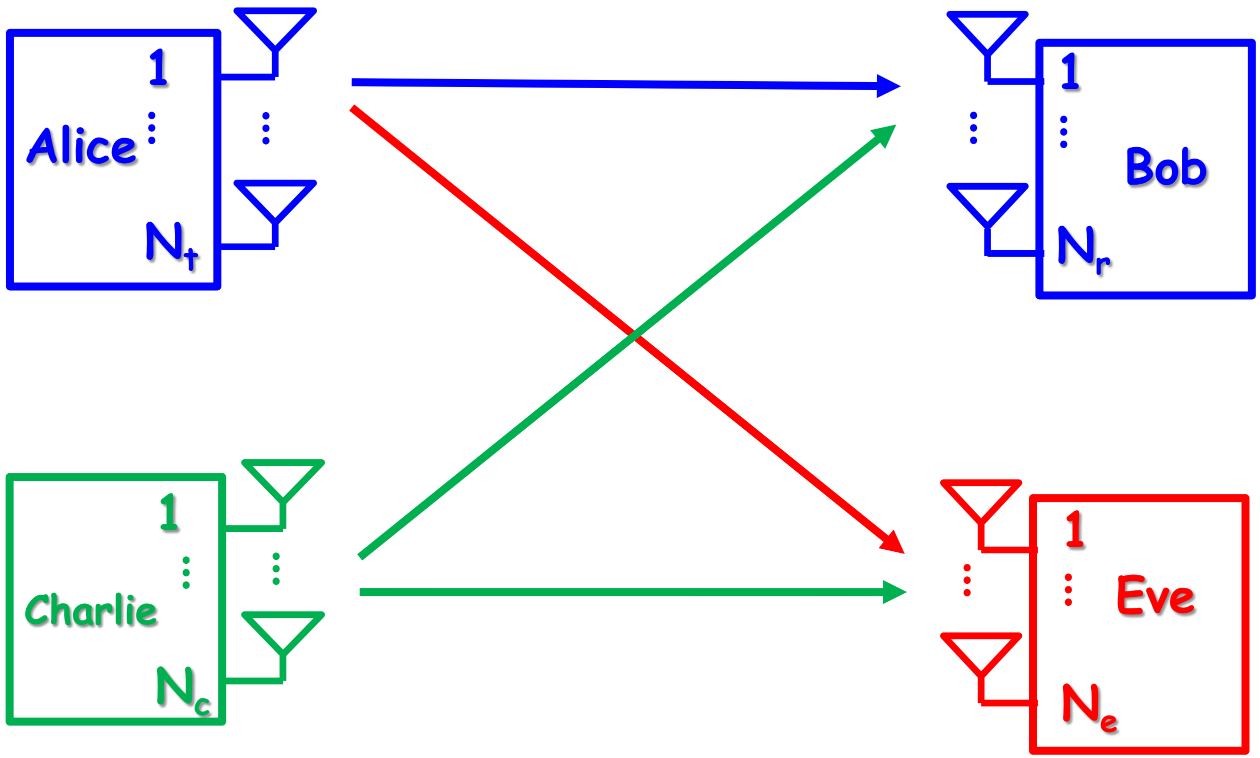
- s.d.o.f. equals ZERO when
  no. of Eve's antennas ≥ no. of Alice's antennas

  (Rate does not scale w/ transmit power.)

Q) Does a multi-antenna cooperative jammer improve the s.d.o.f. of the MIMO WTC?

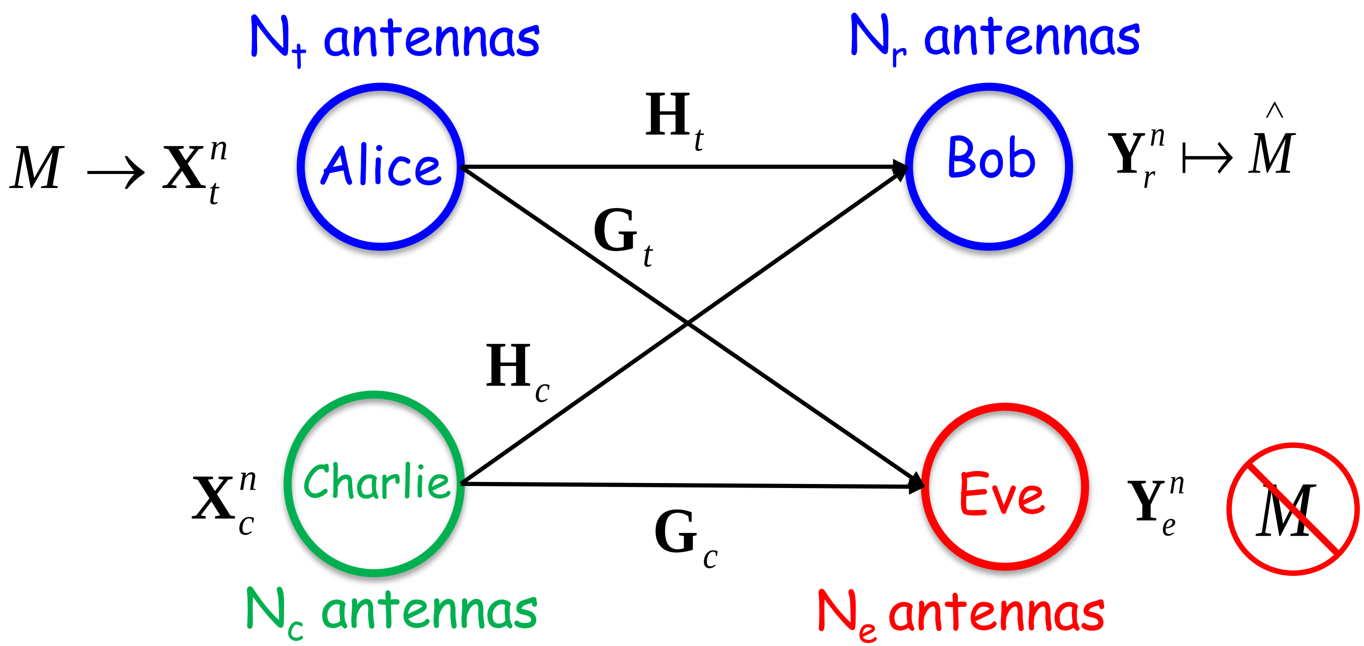
A) YES!

MIMO-WTC w/ MA Cooperative Jammer [Nafea-Y.2015]



(N_t×N_r×N_e) WTC with N_c-antenna CJ

Channel Model



$$\mathrm{E}[\mathbf{X}_t^H(i)\mathbf{X}_t(i)],\ \mathrm{E}[\mathbf{X}_c^H(i)\mathbf{X}_c(i)] \le P$$ (Power constraints)

$$D_s = \lim_{P\to\infty} \frac{R_s}{\log P}$$ Reliability and $\frac{1}{\mathrm{n}} \lim_{n\to\infty} I(M;\mathbf{Y}_e^n) = 0$

Settling s.d.o.f. [Nafea-Y., 2015]

$N \times N \times N_e \times N_c$ channel $(N_t=N_r=N)$:

$$D_s = \begin{cases} \left[N + N_c - N_e\right]^+, & 0 \le N_c \le N_e - N_{\min} \\ N - N_{\min}, & N_e - N_{\min} < N_c \le N_{\max} \\ (N + N_c - N_e)/2, & N_{\max} < N_c \le N + N_e. \end{cases}$$

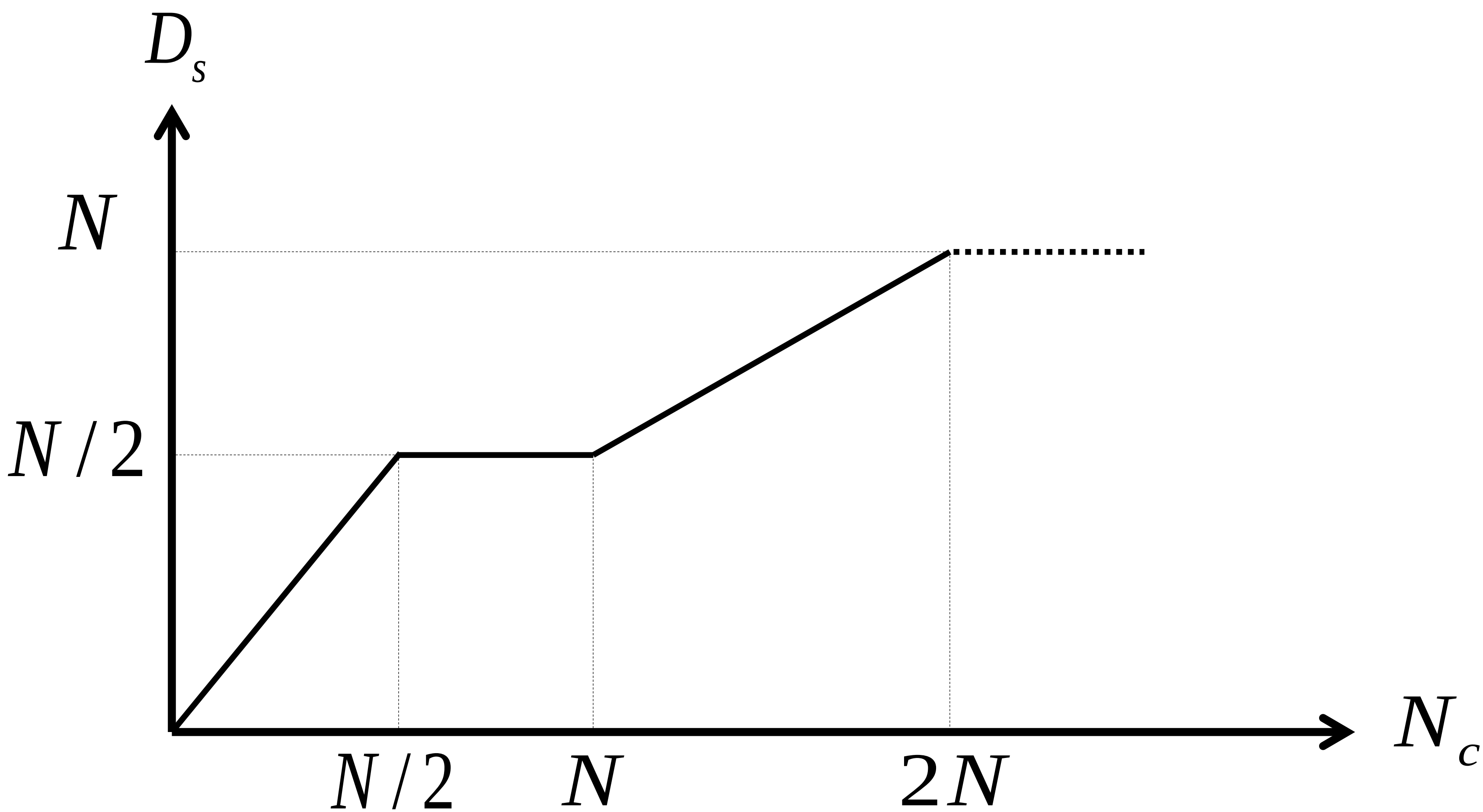
$$N_{\min} = \min\{N, N_e\}/2, \quad N_{\max} = \max\{N, N_e\}.$$

N_e=N

(N×N×N) Gaussian WTC with a N_c-antenna Charlie

$$D_s = \begin{cases} N_c, & 0 \le N_c \le \dfrac{N}{2} \\ \dfrac{N}{2}, & \dfrac{N}{2} < N_c \le N \\ \dfrac{N_c}{2}, & N < N_c \le 2N. \end{cases}$$

N_e=N



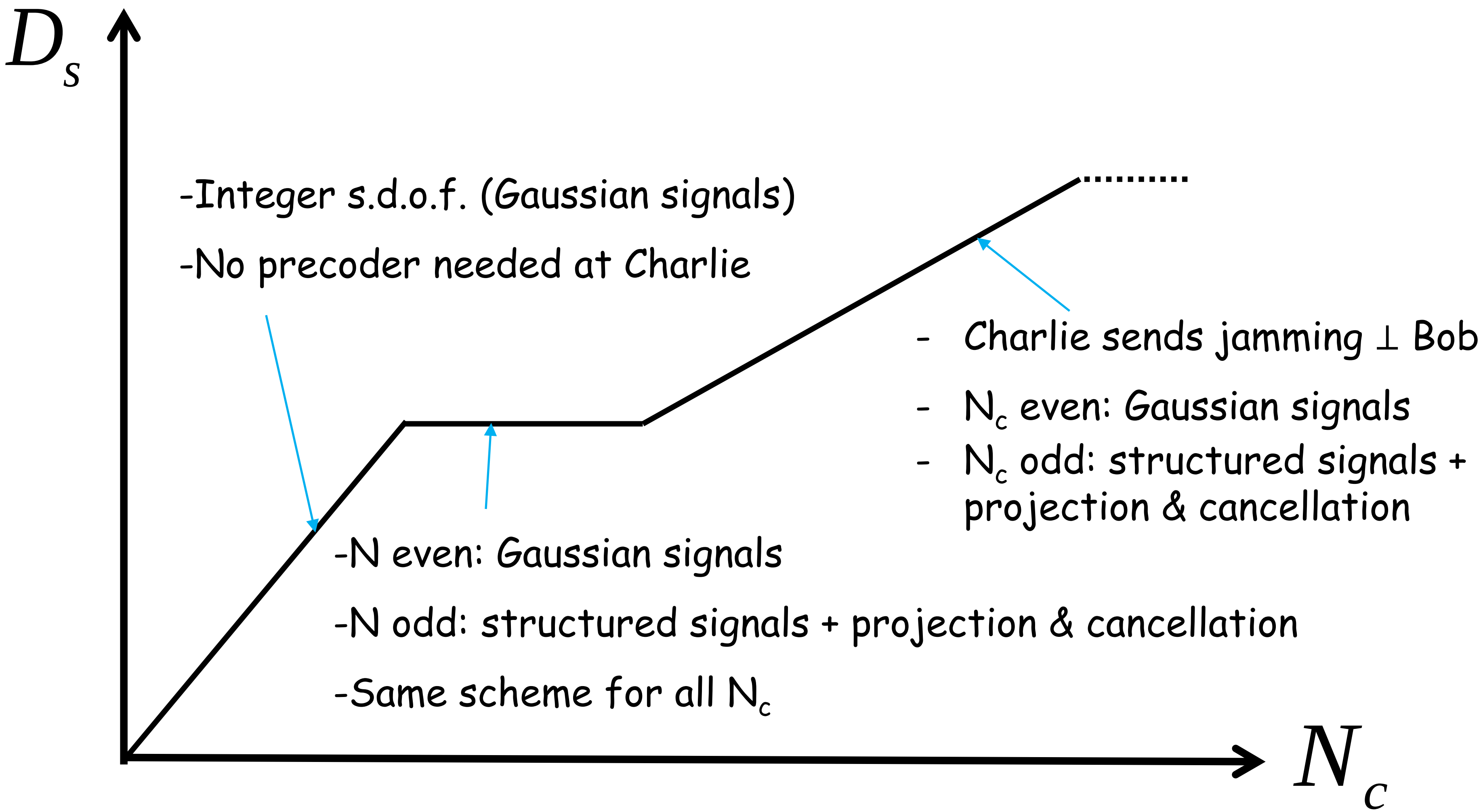
Achievable schemes

- Ranges of K need to be treated separately.
  - ✓ **Signal space alignment:**
    Linear precoding + linear receiver processing.
  - ✓ **Signal scale alignment:**
    - **Complex analogy** to "real" interference alignment
    - **projection and cancellation** decoding scheme.

- D_s=integer: **Gaussian** streams are sufficient.
- $D_s \neq$ integer: **structured** streams are needed.

- In all cases, achievable results match the upper bounds.

Achievable schemes



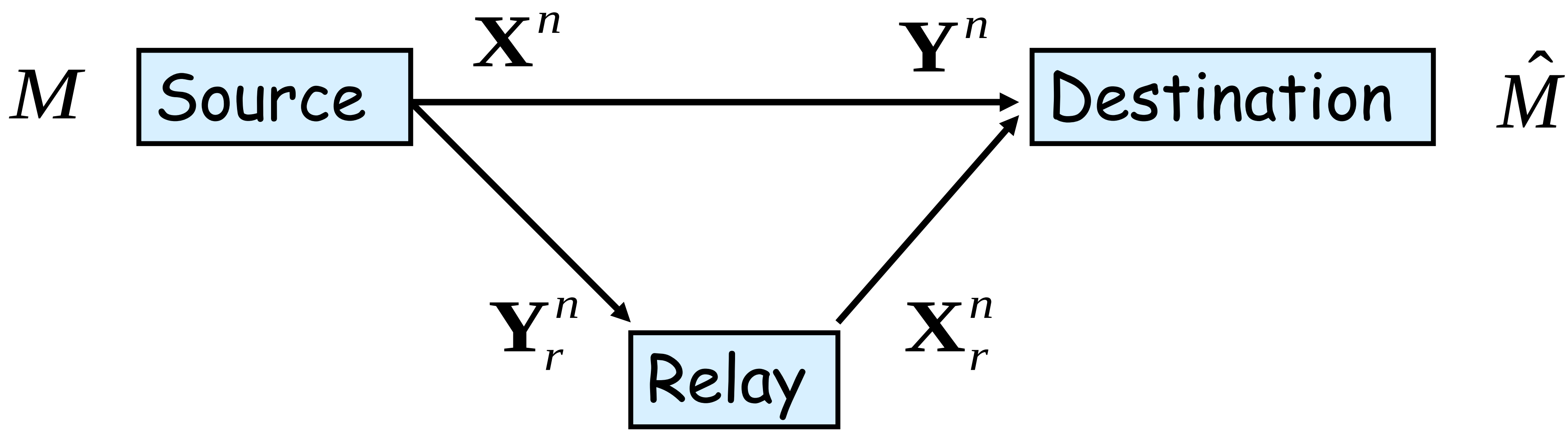
Lessons learned so far…

- **Interference:**
  - Interference can help!
  - Structured codes/transmissions can outperform Gaussian codes.
  - ➢ **Structured interference** is good for securing wireless networks.

- High SNR behavior of secrecy capacity can be insightful!

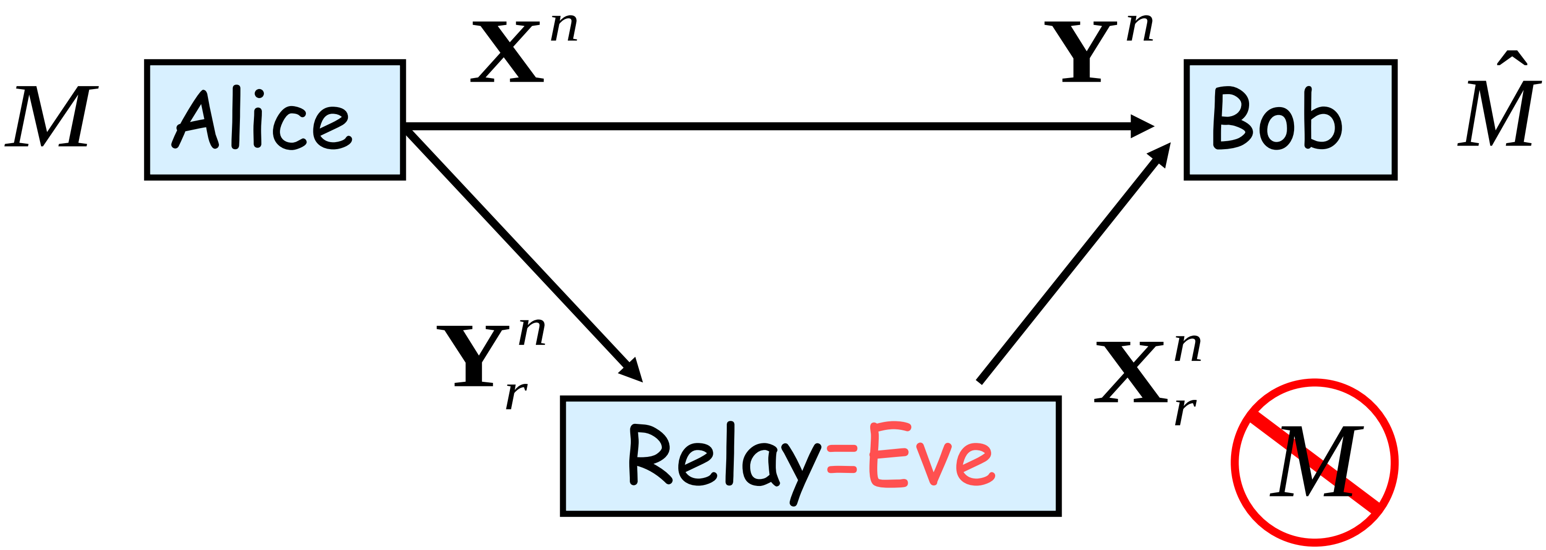
  ➢ **Cooperation?**

Cooperation



$$X_{r,i} = f_{r,i}\left(X_r^{i-1}, Y_r^{i-1}\right)$$

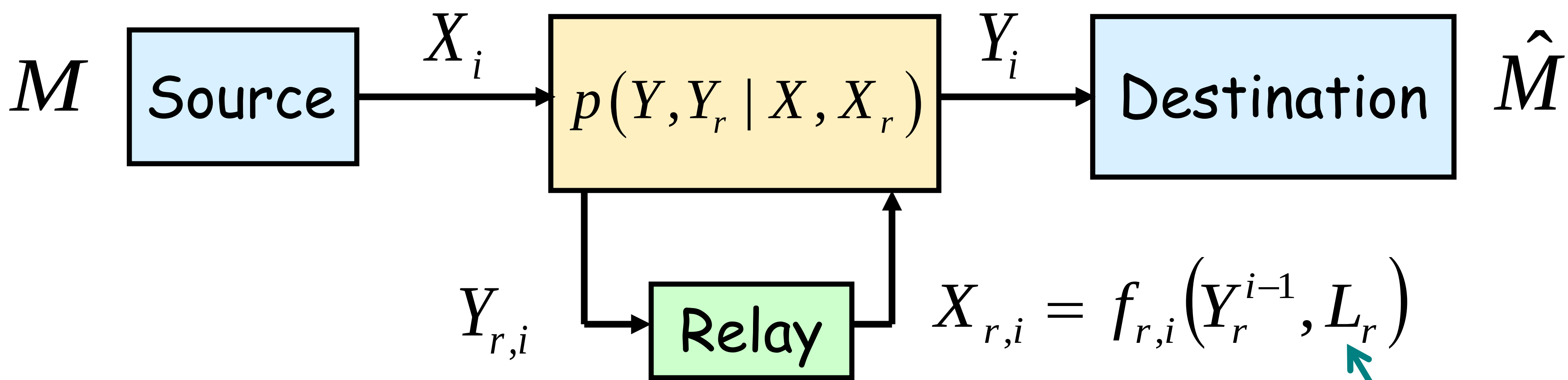
Cooperation with Secrecy



Question: Can an "untrusted" relay ever be useful?

Untrusted Relay Channel [He-Y.2010]

Untrusted Relay: Relay which is "honest but curious":

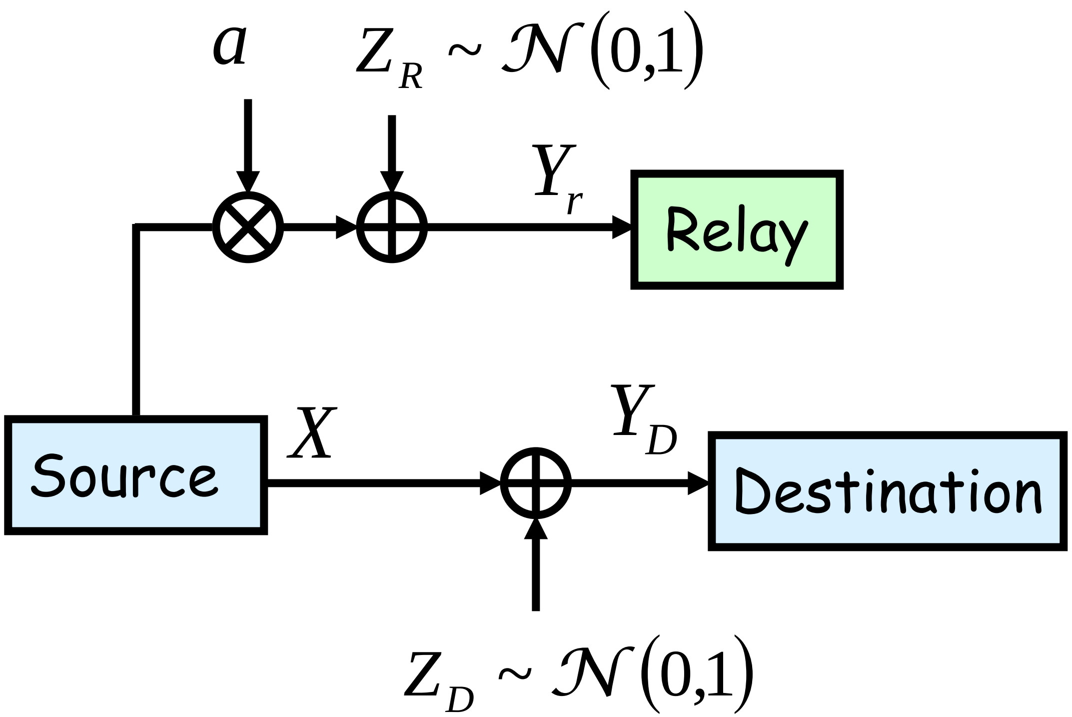


Local randomness at the relay

Secrecy rate is defined as:

$$R_s = \lim_{n \to \infty} \frac{1}{n} H(M) \quad \text{s.t.} \quad \lim_{n \to \infty} \frac{1}{n} I(M; \mathbf{X}_r^n, \mathbf{Y}_r^n) = 0$$

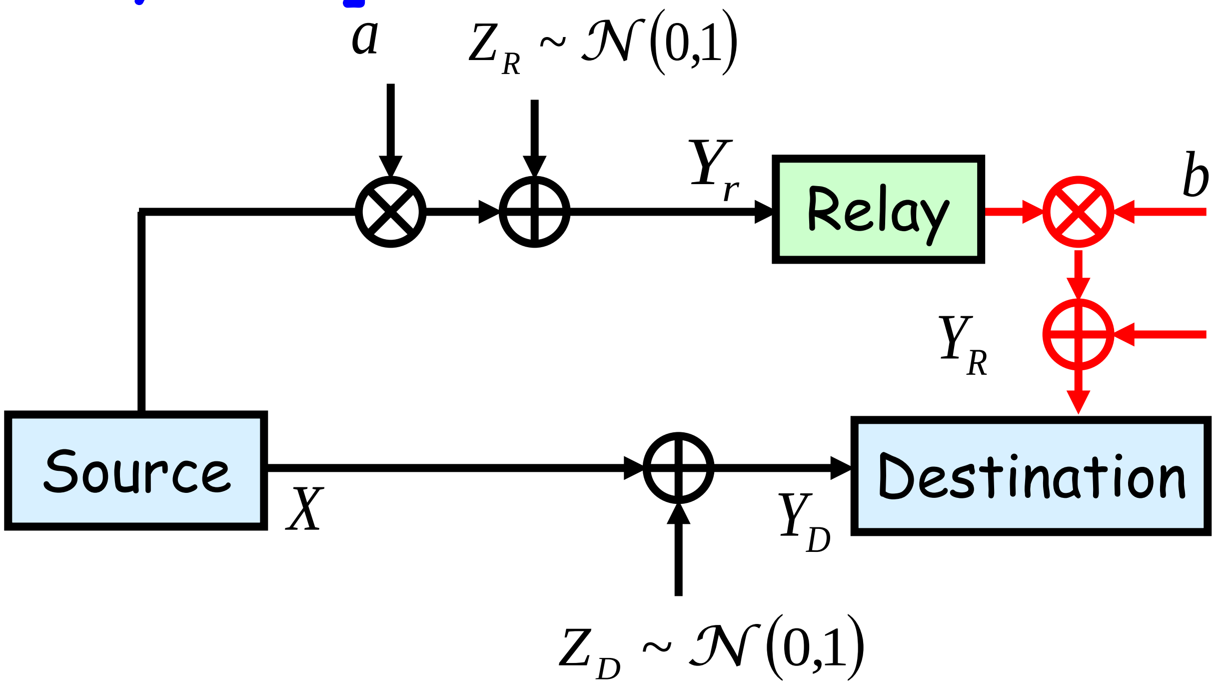
First Phase: The Gaussian Wiretap Channel



- In the first phase, i.e., **without relay-destination link**, this is **the Gaussian wiretap channel**.
- **If $a > 1$, then it is impossible to achieve positive secrecy rate.**

Untrusted Relay Channel with a Direct Link

[He-Y.,2010]



Orthogonal link: AWGN
$Z_R \sim \mathcal{N}(0,1)$

Quantization noise variance

$$0 \le R_s \le \max_{0 \le p \le P} \frac{1}{2}\log\left(1 + p + \frac{a^2 p}{1+\sigma_Q^2}\right) - \frac{1}{2}\log\left(1 + a^2 p\right),$$

$$\sigma_Q^2 = \frac{(a^2+1)p+1}{b^2 P_r (p+1)}$$

$$b \uparrow \infty \rightarrow \sigma_Q^2 \downarrow 0 \rightarrow R_s > 0$$

A positive secrecy rate is achievable.

Achievability outline

- **In phase 1:**

Source performs stochastic encoding with bin size $\frac{1}{2}\log\left(1+a^2 p\right)$ to confuse the relay.

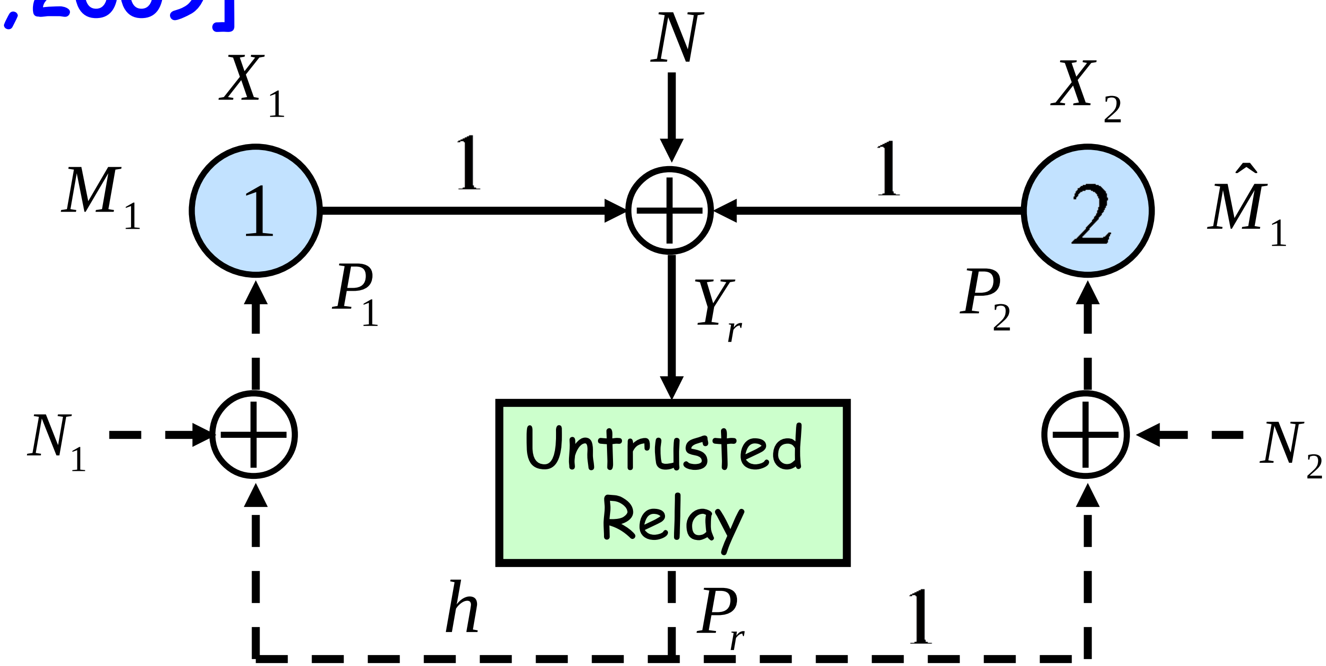
- **In phase 2:**

Relay performs compress-and-forward.

- Destination uses the received signals over the two phases to decode the confidential message.
- ***A positive secrecy rate is achievable!***

Untrusted Relay Channel Without a Direct Link

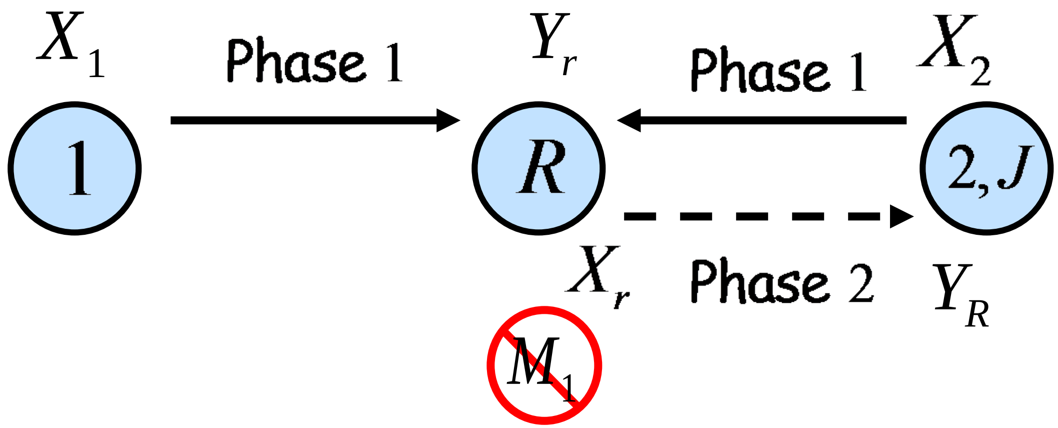
[He-Y.,2009]



- There is no direct link from node 1 to node 2.
- The destination (node 2) can transmit.

$$0 \le R_s \le \max_{0 \le p_1 \le P_1} \frac{1}{2}\log\left(1+\frac{p_1}{1+\sigma_Q^2}\right) - \frac{1}{2}\log\left(1+\frac{p_1}{1+P_2}\right).$$

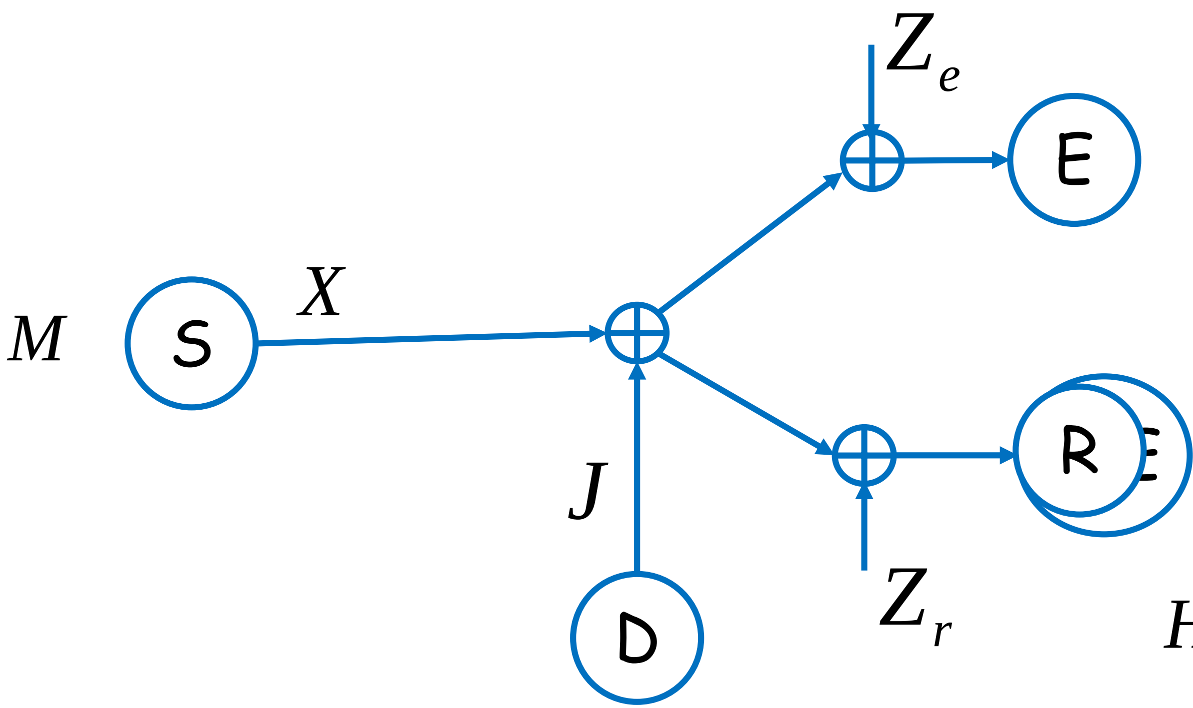
Achievability Outline



- In phase 1, Node "1" (source) transmits. Node J jams the relay node "R". Node "2" (destination) listens.
- In phase 2: the relay node sends out the signal received during phase 1 via compress-and-forward /compute-and-forward.
- Node 2 decodes M_1 based the signal it receives during the two phases
- ***A positive secrecy rate is achievable!***

Upper Bound Development

- Relay\Eavesdropper separation [He-Y.2009]:



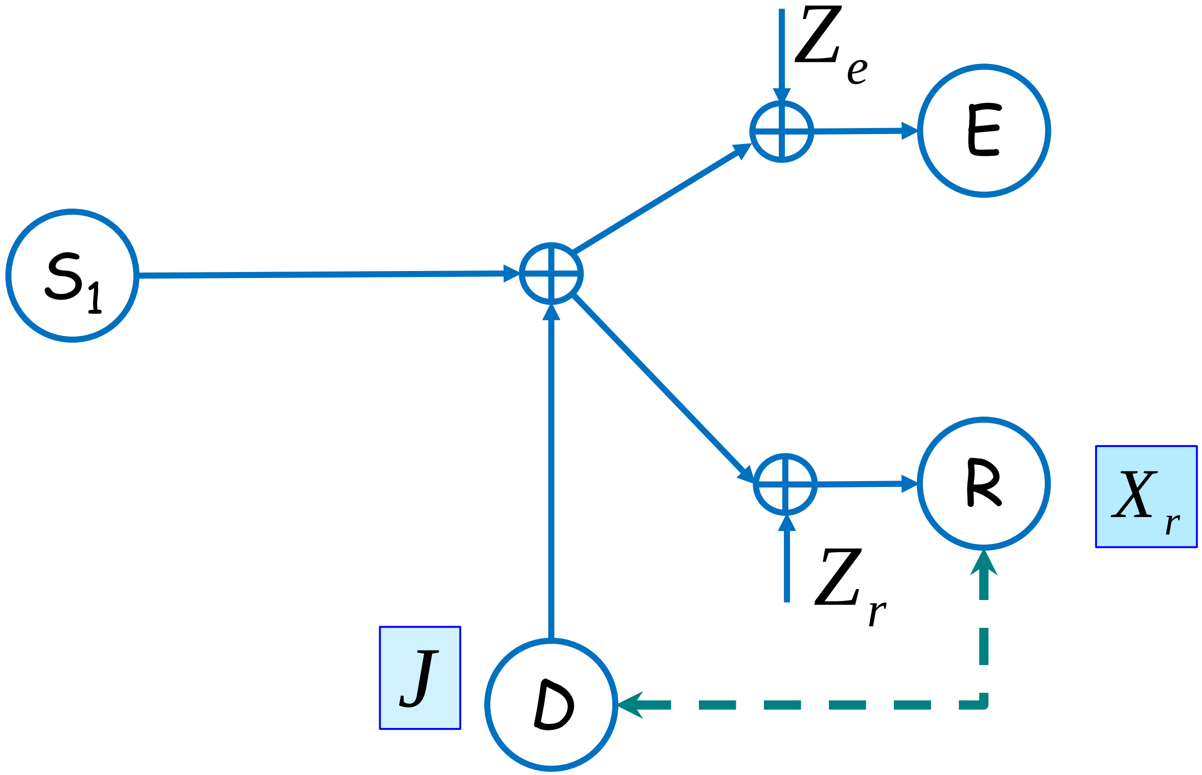
$$Y_e = X + J + Z_e$$

$$Y_r = X + J + Z_r$$

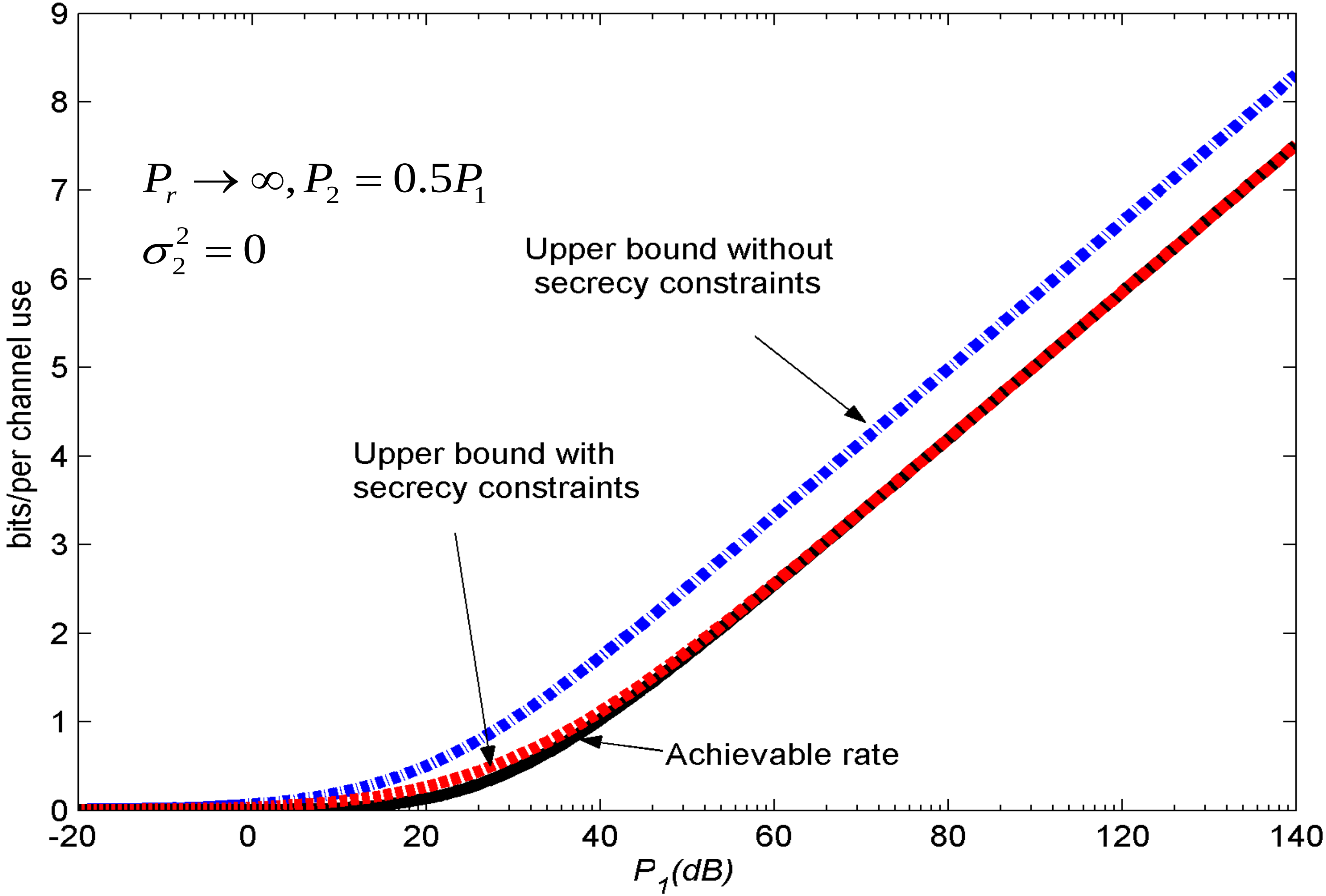
$$H(M \mid Y_r) = H(M \mid Y_e)$$

$Z_e \sim \mathcal{N}(0,1)$ and correlated with Z_r by ρ.

Genie transfers …



$$R \le \max_{0\le\alpha\le1} \min_{-1\le\rho\le1} \min\left\{ \begin{array}{c} \frac{\alpha}{2}\log_2 \frac{(1+P_S)(1+P_S+P_J)-(P_S+\rho)^2}{(P_S+P_J+1)(1+-\rho^2)}, \\ (1-\alpha)C(P_r) \end{array} \right\}$$


$P_r \to \infty, P_2 = 0.5P_1$
$\sigma_2^2 = 0$
Upper bound without
secrecy constraints
Upper bound with
secrecy constraints
Achievable rate
bits/per channel use
$P_1(dB)$
9
8
7
6
5
4
3
2
1
0
-20
0
20
40
60
80
120
140

Observations

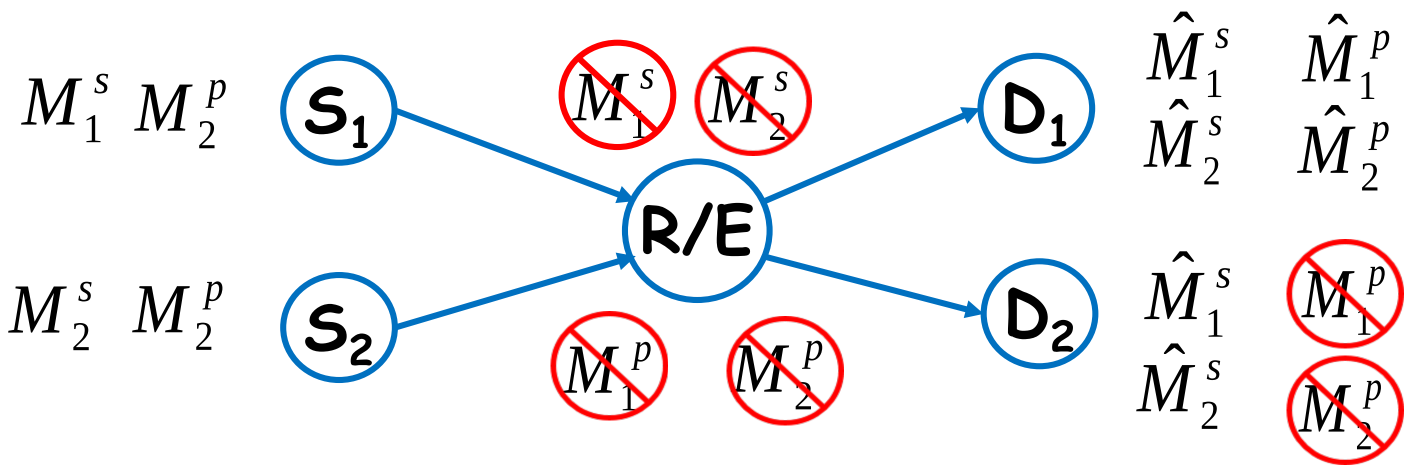
- A two-hop link with untrusted relay is considered.
- The cooperation from the relay is essential to communicate in this scenario.
- An achievable scheme based on cooperative jamming and compress-and-forward relay scheme is proposed.
- Cooperative jamming is the enabler of secure communication in this case.
- Can we afford to be this optimistic for 'larger' networks?

Untrusted Relays

Multiple sources/destinations

Different levels of security clearance [Zewail-Nafea-Y. 2014]:

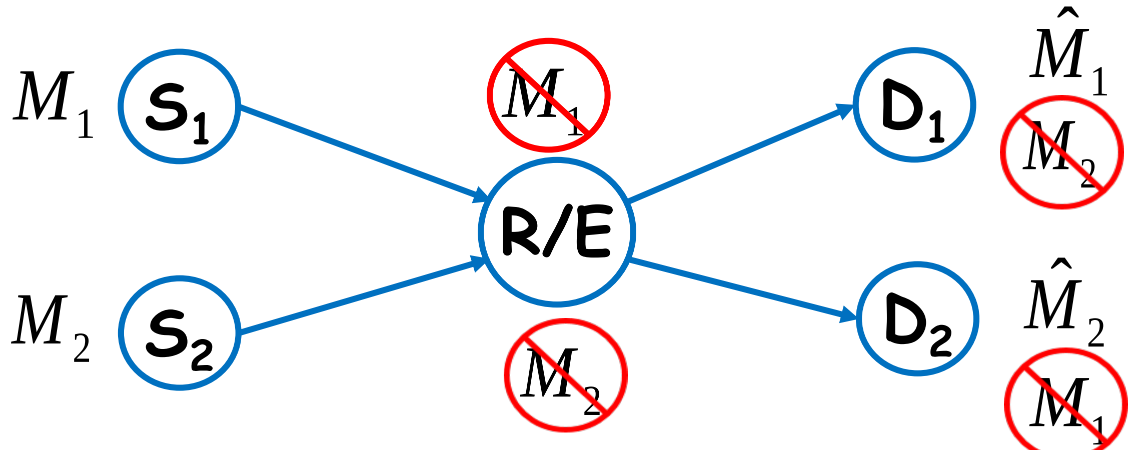
- Cooperative jamming by the destinations, using Gaussian noise, is again useful and necessary.
- Stochastic encoding and superposition at the sources
- Relay performs compress-and-forward.
- Gaussian signaling.



Multiple Sources/Destinations

Confidentiality at the end users [Zewail-Y. 2015]:

- Sources performs stochastic encoding over nested lattice codebooks.
- Destinations jam with lattice points.
- Relay performs scaled-compute-and-forward to decode two combinations of the received lattice points and forwards to the destinations.
- Structured signaling.

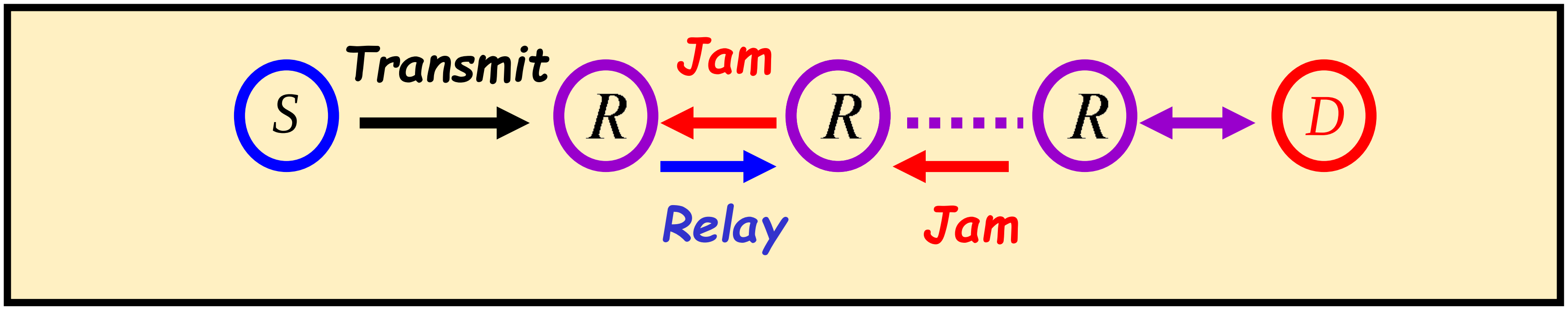


Multiple Hops [He-Y., 2013]

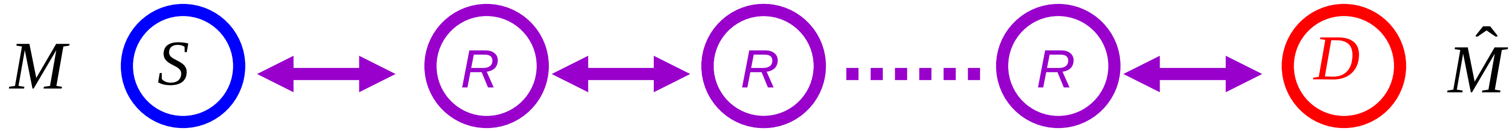
- Multi-hop line network with a chain of untrusted relays:
  - **Structured jamming** by each destination is **essential**.
- Constant secrecy rate irrespective of hops.
- Nested lattice codes.

Line Network w/ Untrusted Relays [He-Y., 2013]

- An eavesdropper may be located at any one of the relay nodes, trying to intercept M. Hence all of these relay nodes are untrusted.
- Each node can only receive from the previous node, so all that is sent from the source has to flow through the relays!
- **Solution:** Recruit the next destination as a cooperative jammer for the current relay.



Line Network w/ Untrusted Relays



- The same principle as the two-hop case should work, but…
- Compress-and-forward scheme is not scalable to arbitrary number of hops.
  - Channel noise will accumulate over hops and decrease the rate.
- Use nested lattice codes to transmit the secret message and for cooperative jamming.

The Achievable Secrecy Rate

Let the power constraint of each node be P, and assume unit channel gains and noise variance. For any $\varepsilon > 0$ secrecy rate of at least

$$0.5R_0 - 0.5 - \varepsilon$$

is achievable irrespective of the number of hops, where

$$R_0 = \frac{1}{2}\log_2\left(2P + 0.5\right)$$

Secrecy rate does not decrease with number of hops.

The rate penalty, i.e., cost for secrecy is upper bounded by 0.5 bit/ch.use.

Strengthening the Security Metric

- **Weak secrecy [Wyner 1975]:**

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

Rate of information leakage goes to Zero

- Weak secrecy constraint is satisfied with any information leakage **that grows at a rate strictly less than n**.

Can we do better?

Strong Secrecy

[Csiszar 1996; Maurer-Wolf 2000]:

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

The WHOLE information leakage goes to Zero

- Stronger metric; No information is leaked, asymptotically!
- Recently, a number of secrecy results have been extended to strong secrecy.
- There is no proof of equivalence or strict containment.
- There is no standard technique for proving strong secrecy.

Strong Secrecy Proofs

1) Channel Resolvability [Wyner 1975b][Han-Verdu 1993]

What is the max. randomization rate required to **induce an output distribution** at **Eve** s.t. Z^n is **independent** from M?

- **Randomization rate** $\widetilde{R}_s$
  - rate of the sub-code (stochastic encoding).

Strong Secrecy Proof Methodologies

1) Channel Resolvability

- **Statistical independence** is measured in
  - **Kullback-Leibler divergence** (Relative Entropy), or
  - **Variational distance.**
- **Strong secrecy for Wiretap Channel:**

$$\tilde{R}_s > I(X;Z) \Rightarrow D(p_{M,\mathbf{Z}^n} \| p_M \, p_{\mathbf{Z}^n}) \rightarrow 0 \Rightarrow I(M;\mathbf{Z}^n) \rightarrow 0$$

Strong Secrecy Proofs

2) Privacy Amplification

[Bennett et.al. 1989; Maurer-Wolf 2000]

- Weak secrecy scheme is repeated many times.
- Alice & Bob compress X^n to a shorter string S that is **uniform and indep. from** Eve's observation.
- Secrecy capacity is not reduced by privacy amplification.

Strong Secrecy Proofs

2) Privacy Amplification

[Bennett et.al. 1989; Maurer-Wolf 2000]

Distilling strongly secure string from $\mathbf{X}^n$:

- **Universal Hashing;**
  - select a hash function h at random from a family of hash functions s.t. $\Pr\left(h(\mathbf{X}^n)\,\text{not unifrom}\right)$ **is small,**
- **Extractors;**
  - isolate randomness of $\mathbf{X}^n$ using a small additional number of perfectly-random bits)

Mitigating the Assumption of Known Eve CSI

- Most work assumes Eve's CSI is known to the system
- **Compound models 2008-2010: [Liang et al] [Ekrem-Ulukus], [Kobayashi et al]:**
  Channel can be one of a set of possibilities.
- **Fading setting [Goppala-Lai-ElGamal 2008]:**
  Eve's CSI distribution known.

Mitigating the Assumption of Known Eve CSI

- **Reality:** Eve's channel completely unknown.
- **Question:** How can we create advantage against a channel we have no idea about?
- **Answer:**

  Multiple antennas == directional signaling and jamming!

- MIMO WTC **[He-Y.,2010/IT 2014]**,
- s.d.o.f MIMO-MAC-WT **[He-Khisti-Y.,2013]**,
- s.d.o.f MIMO-Broadcast-WTC **[He-Khisti-Y.,2014]**.

MIMO-WTC w/ Unknown Eve CSI

- **Multiple antennas** at Alice and Bob can be used to inject "artificial noise" in *directions orthogonal* to those of the main channel **[Goel-Negi, 2008]**.
- While this early work has the nice insight for signaling, it is incomplete since the actual coding scheme requires care.
- In other words, existence of a coding scheme that will "work" for **all Eve CSI's** needs to be proved.

MIMO-WTC w/ Unknown Eve CSI: Universal Coding Scheme

- CSI completely unknown, varies from ch use to ch use.
- MIMO Wiretap setting.
- **[He-Y.,2010/2014]:** A universal coding scheme does exist.
  - Strong secrecy can be provided where ever Eve may be, as long as the legitimate parties have more antennas.

Problem Formulation

Find the rate of M such that:

$$\lim_{n\to\infty} \Pr\left(\hat{M} \neq M\right) = 0$$

$$\lim_{n\to\infty} I(M;\tilde{\mathbf{Y}}^n, \tilde{\mathbf{H}}^n) = 0$$

The convergence must be uniform over all possible $\tilde{\mathbf{H}}^n$

By assumption, M is indep. from $\tilde{\mathbf{H}}^n$

$$\lim_{n\to\infty} I(M;\tilde{\mathbf{Y}}^n \mid \tilde{\mathbf{H}}^n) = 0$$

We do not want the secrecy constraint to depend on the distribution of $\tilde{\mathbf{H}}^n$ Hence we require:

$$\lim_{n\to\infty} I(M;\tilde{\mathbf{Y}}^n \mid \tilde{\mathbf{H}}^n = \tilde{\mathbf{h}}^n) = 0$$ for all possible realizations of $\tilde{\mathbf{h}}^n$.

Main Result [He-Y. 2014]

- **Theorem:** For the MIMO wiretap channel, if $\mathbf{H}$ has full rank, then the following secrecy rate is achievable:

Bob's channel

$$0 \le R_s < \max\left\{\left(\sum_{i=1}^{N_{T,R}} C\left(\frac{s_i^2 P}{\left(s_i^2+1\right) N_{T,R}}\right)\right) - N_E C(P), 0\right\}$$

where $P = \max\{\overline{P} - N_{T,R}, 0\}$

$N_{T,R} = \min\{N_T, N_R\}$, s_i : singular value of $\mathbf{H}$

$$\text{s.d.o.f.} = \max\{N_{T,R} - N_E, 0\}$$

Proof Highlights

1. Introduce artificial noise at Alice to limit the received SNR of Eve. **[Goel-Negi,2005]**.

2. Need to prove Strong Secrecy directly.
([Maurer,2000] is not applicable).

3. Prove Strong Secrecy through variational distance d.
If variational distance decreases exponentially fast to 0 w.r.t. the number of channel uses, strong secrecy can be proved from **[Csiszar,1996]**.

4. To bound d, use information spectrum method.
[Han,1993] [Csiszar,1996][Bloch-Laneman,2008]

To handle infinitely many sequences of Eve CSI…

1. Construct a finite set S of Eve CSI sequences by quantizing the channel gain **[Blackwell et.al.,1959].**

2. Find a small set of codebooks, s.t. aveage of d, dav, is uniformly bounded over all possible Eve CSI sequences in the set S **[Ahlswede, 1978].**

3. Prove when Eve CSI sequence is not in S, its dav is bounded by the dav when Eve CSI sequence is in S. **[Blackwell et.al., 1959].**

Coding Scheme

- Given the small set of good codebooks, the communication is divided into 2 stages, as in [Ahlswede, 1978].
- **Stage 1:** Alice randomly chooses a codebook from the small set of codebooks to transmit confidential message.
- **Stage 2:** Alice tells Bob which codebook she chose in Stage 1.
  - Alice's choice is taken from a uniform distribution but need not be kept secret from Eve. In fact, we assume Eve knows Alice's choice perfectly.

(It can be shown the rate loss due to stage 2 can be made arbitrarily small).

Strengthening Eve Capabilities

- Eve traditionally is **a passive observer**.

- **Adversarial Eve:**
  - Eve tampers with the legitimate channel, e.g.,

  [Aggarwal et. al. 2009; MolavianJazi et.al.2009].

- **Adaptive Eve:**
  - Eve controls her channel states, e.g.,

[He-Y. 2011]: Two-way channel and cooperative jamming essential for achievability.

More Capable Eavesdropper Models

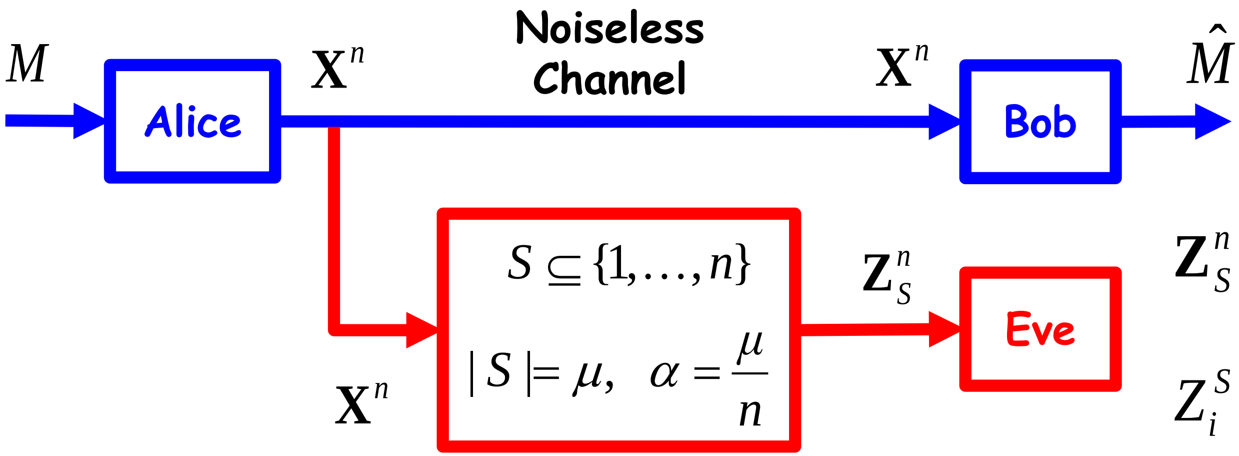
Objectives:

- Strengthening Eve's capabilities.
- Extending attacker/threat models and providing quantifiable metrics for secure wireless networked communication.
    - Can PHY-security 'replace' or complement computational security?

Wiretap Channel II

[Ozarow-Wyner 1985]:

- Eve accesses μ out of n symbols (of her choice.)
- Noiseless main channel. Binary input alphabet.



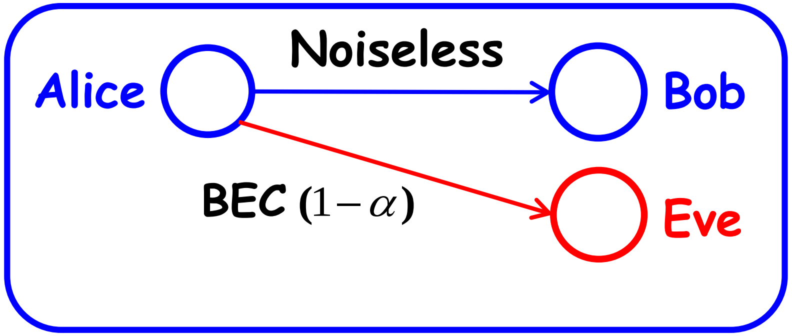
$$\mathbf{Z}_S^n = [Z_1^S \ldots Z_n^S]$$

$$Z_i^S = \begin{cases} X_i, & i \in S \\ ?, & \text{o.w.} \end{cases}$$

Secrecy constraint: $\frac{1}{n} \max_S I(M; \mathbf{Z}_S^n) \to 0$ (Weak Secrecy)

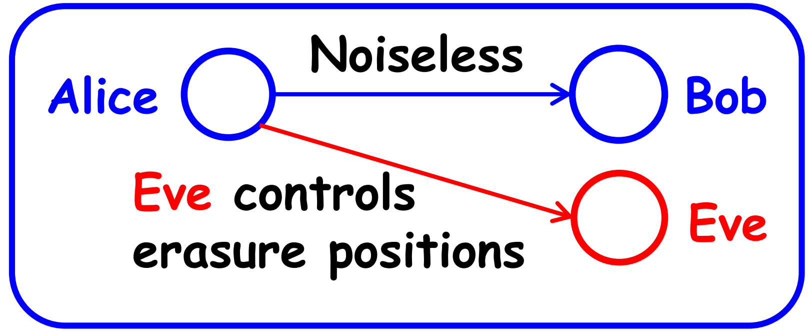
Wiretap Channel II

WTC



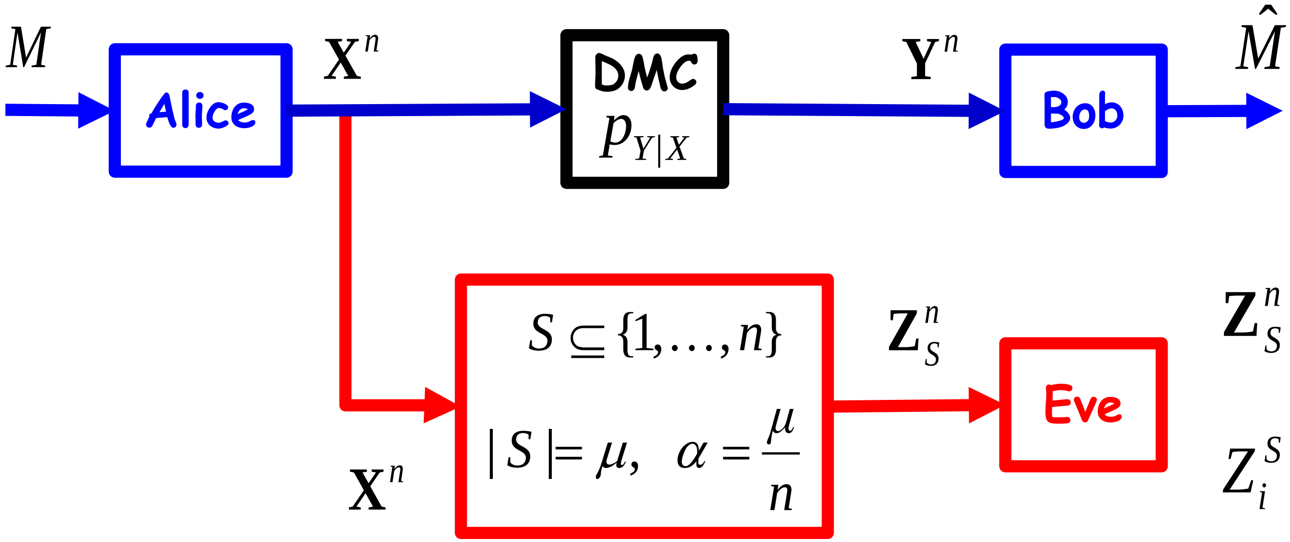
- Random Erasures
- DM Eve channel
- Secrecy capacity:
  $$C_s = 1-\alpha$$
- Achievability:
  Stochastic Encoding

WTC-II



- Eve chooses erasure positions
- Eve channel with memory
- Secrecy capacity: $C_s = 1-\alpha$
- Achievability: Random partitioning
  $C_o = \{0,1\}^n$ + combinatorial arguments

WTC-II with Noisy Main Channel [Nafea-Y.,2015]



$$\mathbf{Z}_S^n = [Z_1^S \ldots Z_n^S]$$

$$Z_i^S = \begin{cases} X_i, & i \in S \\ ?, & \text{o.w.} \end{cases}$$

WTC-II with noisy main channel

Secrecy constraint: $$\frac{1}{n}\max_S I(M;\mathbf{Z}_S^n) \to 0.$$

WTC-II with NMC

[Nafea-Y., 2015]:

- Inner and outer bounds for capacity-equivocation region are derived.
- Secrecy rate bounds: $R_s(\alpha) \le (1-\alpha)\max_{p_X} I(X;Y)$.

$$R_s(\alpha) \ge \left[I(X;Y) - \alpha H(X)\right]^+ \Big|_{p_X \sim \text{Uniform}}.$$

- Secrecy capacity **[Cuff et.al., 2015]:**

$$C_s(\alpha) = \max_{U-X-Y} \left[I(U;Y) - \alpha I(U;X)\right]^+$$

Equals secrecy capacity of a WTC with a DM-EC $(1-\alpha)$ to Eve.

$\xrightarrow{U=X}$ $\max_{p_X} \left[I(X;Y) - \alpha H(X)\right]^+ = R_s(\alpha)$ when a uniform maximizer.

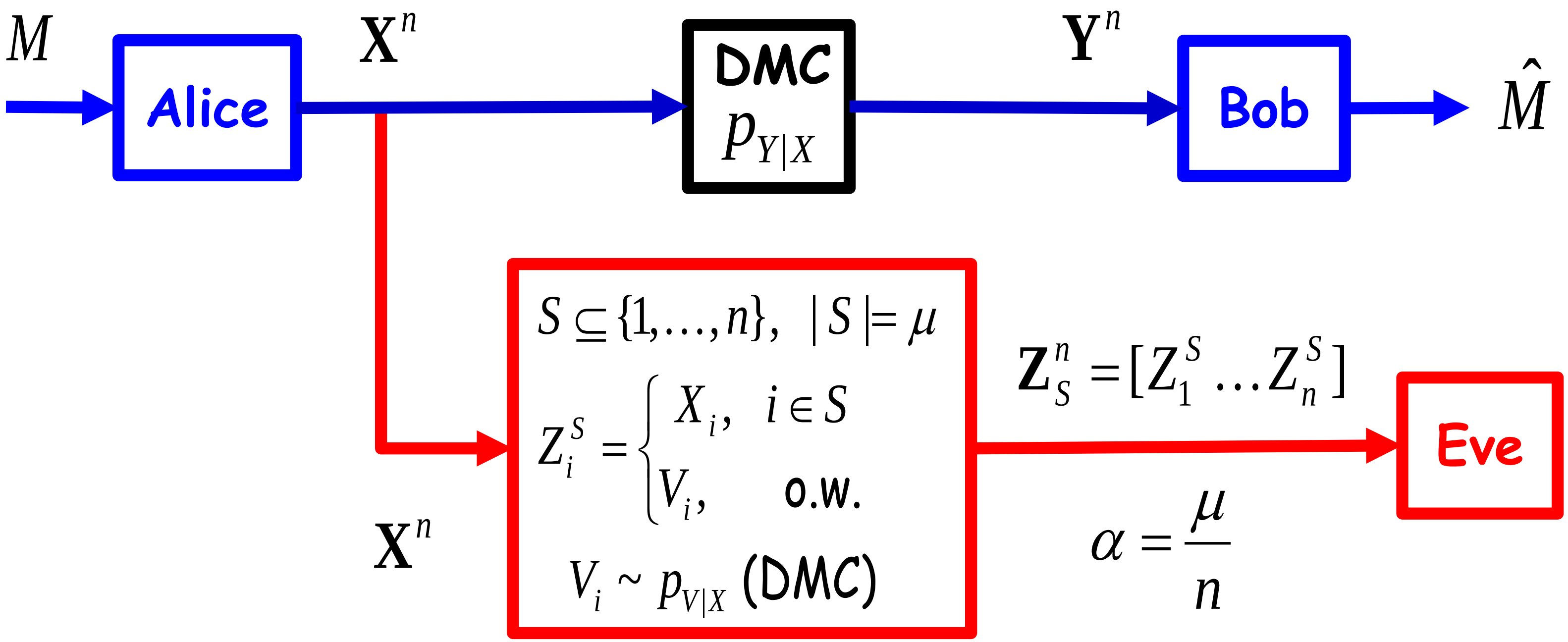
Can we model a powerful Eve in a realistic scenario?

- WTC→ Eve not capable enough
- WTC-II → Not practical
- WTC-II with NMC → Eve cannot "see" portion of cw.

YES!

- New model:
  - Eve sees all through a (noisy) channel.
  - Eve can choose the portion she can tap perfectly.
  - Generalizes and more "evil" Eve than all previous models!

A New WTC model [Nafea-Y., ISIT 2016]

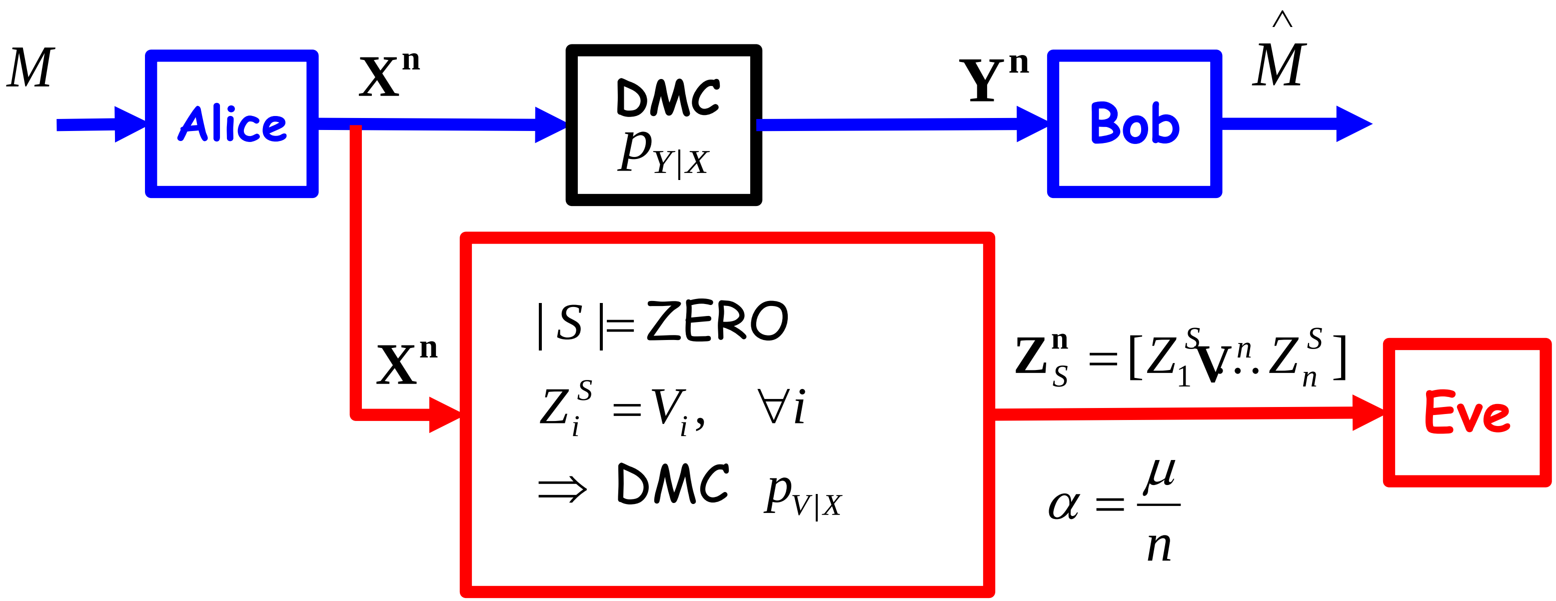


Strong Secrecy (against any Eve selection):

$$\max_S I(M;\mathbf{Z}_S^n) \to 0.$$

Special cases

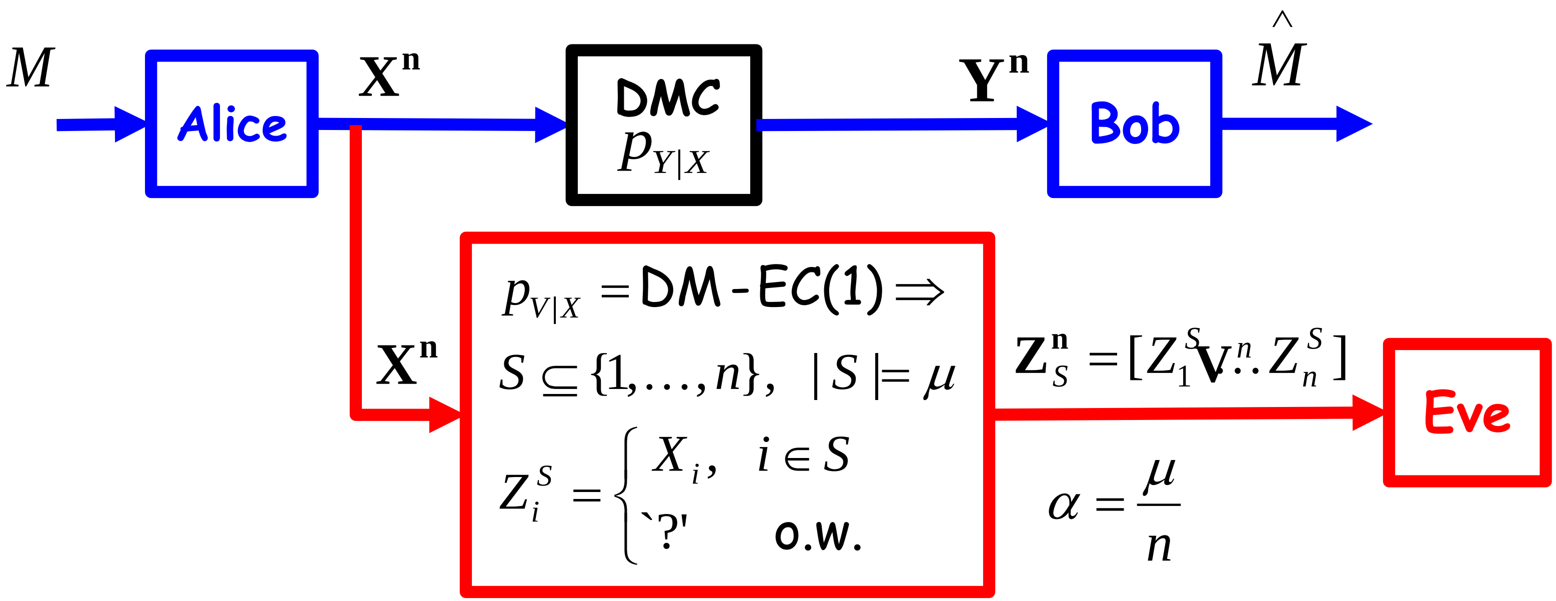
- The new model generalizes known WTC models.



Classical WTC

Special cases

- The new model generalizes known WTC models.



WTC-II with a noisy main channel

Strong Secrecy Capacity [Nafea-Y., ISIT 2016]

- The strong secrecy capacity of the new wire-tap channel model is :

$$C_s(\alpha) = \max_{p_{UX}:\, U-X-YV} \left[I(U;Y) - I(U;V) - \alpha I(U;X|V) \right]^+$$

with $|\mathcal{U}|$ upper bounded as $|\mathcal{U}| \leq |\mathcal{X}|$.

Special cases

- At $|S|=0$: $C_s(0)=\max\limits_{p_{UX}:\,U-X-YV}[I(U;Y)-I(U;V)]^+.$

  = WTC secrecy capacity.

Secrecy capacity of the new WTC model

$$C_s(\alpha)=\max_{p_{UX}:\,U-X-YV}[I(U;Y)-I(U;V)\underbrace{\boxed{-\alpha I(U;X|V)}}_{\text{Secrecy cost}}]^+.$$

- At $V=$`?': $C_s(\alpha)=\max\limits_{p_{UX}:\,U-X-Y}[I(U;Y)-\alpha I(U;X)]^+$

  = Secrecy capacity of WTC-II with NMC

Secrecy capacity of the new WTC model

$$C_s(\alpha)=\max_{p_{UX}:\,U-X-YV}[I(U;Y)-\alpha I(U;X)\underbrace{\boxed{-(1-\alpha)I(U;V)}}_{\text{Secrecy cost}}]^+.$$

Smarter Wire-tappers in Multi-transmitter models

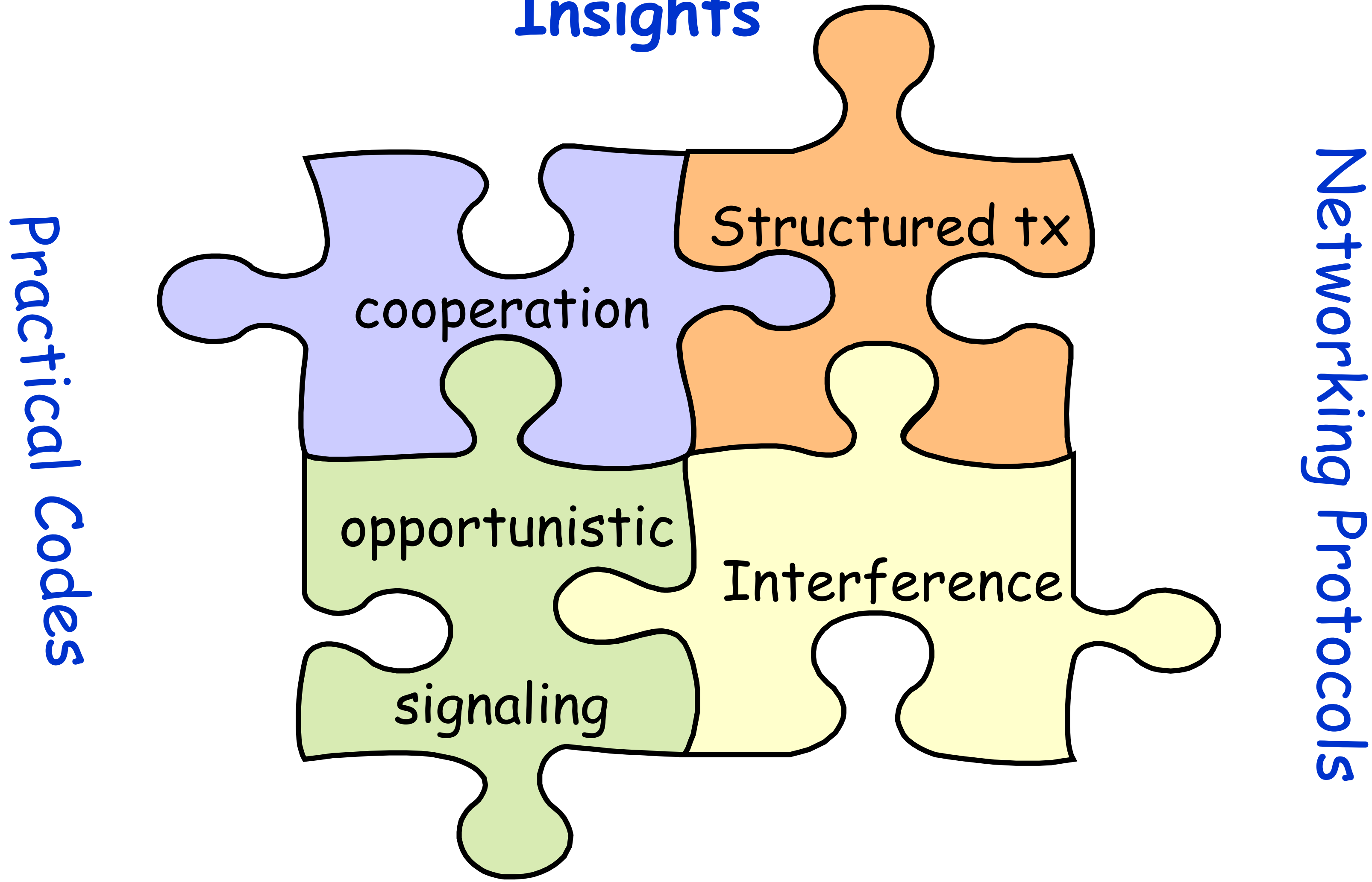
- Wire-tap channel [Wyner1975]→ Multiple access wire-tap channel [Tekin-Y.2005]
- Multi-transmitter extensions for WTC-II with noisy main channel: [Nafea, Y. 2016] upcoming at ISIT 2016, ITW 2016

Summary*

- Information Theory offers quantifiable security guarantees. Does not require computational approaches.
- Information theory offers a clean slate design starting from the physical layer providing strong secrecy guarantees for wireless networks.
- "Idealized" assumptions can be removed (with some rate penalty, but same security guarantees)
- Insights for such realistic scenarios bring us one step closer to the future wireless networks where security is provided at the foundation, i.e., by PHY!

*The following grants are gratefully acknowledged: DARPA-ITMANET; NSF: CCF-0514813, CNS-0721445, CT-0716325, CIF-0964362, CCF-1319338, CNS-1314719;

Information Theory: Design Insights



SECURE WIRELESS NETWORKS