Lecture 11

Physical layer secrecy

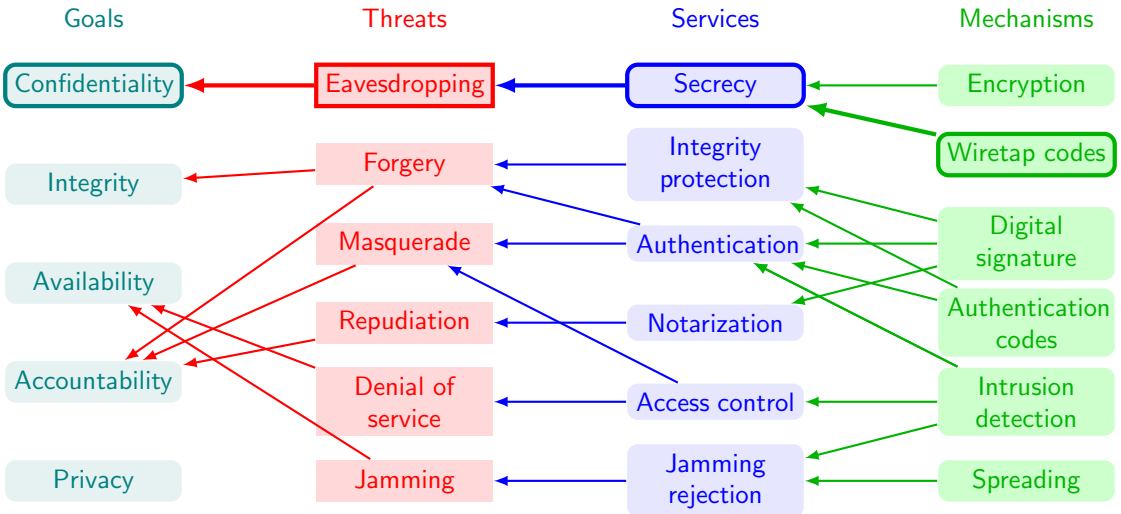
Nicola Laurenti November 4, 2020

Lecture 11— Contents

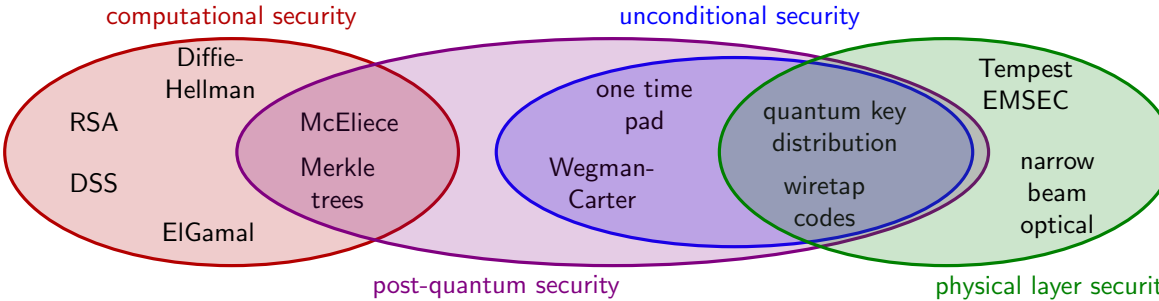
Physical layer security - Motivation

- Wireless communications are inherently vulnerable to various attacks
- Any device is a potential eavesdropper/jammer
- Cryptographic mechanisms (e.g., WPA) require costly key renewal
- Little is done to protect transmissions at the physical layer directly
- Diversity and randomness of the channels can be leveraged to provide security

Security goals, threats, services and mechanisms



Unconditional vs computational security

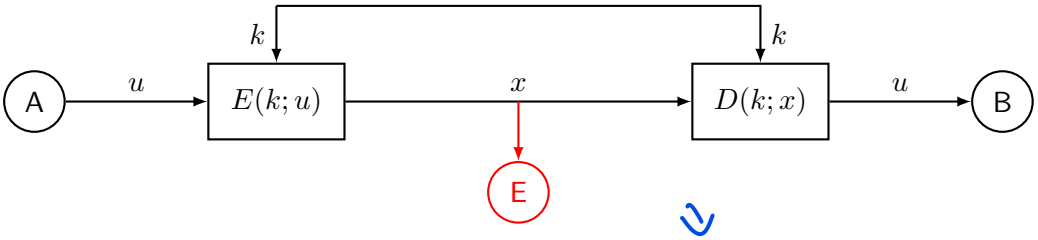


Computational security systems can be broken by an attacker with enough computational power

Post-quantum security systems have not been shown breakable by quantum computers in short time

In unconditional security, the attacker is not better off at guessing by observing the protocol communications. However, in designing the system, (statistical) knowledge of the attacker channel is often required

Unconditional secrecy [Shannon, '49]



Kerchoff's Assumption

E knows:

- the functions $C(\cdot;\cdot)$, $D(\cdot;\cdot)$
- the distributions $p_u(\cdot)$, $p_k(\cdot)$

Secrecy of u is only based on hiding the key k

Perfect secrecy

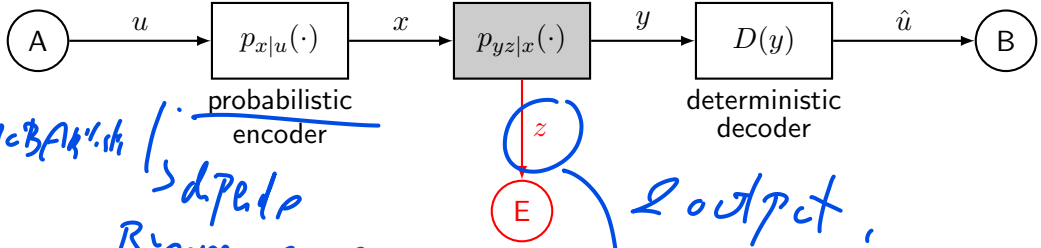
u statistically independent of x

$$p_u(\alpha) = p_{u|x}(\alpha|\beta) \quad , \quad I(u;x) = 0$$

Theorem

Perfect secrecy requires $H(k) \geq H(u)$

The wiretap channel [Wyner, '75]



We aim for reliable transmissions to B, and secrecy with respect to E

- perfect reliability: $\hat{u} = u$
- perfect secrecy: z, u statistically independent

In terms of unconditional distinguishability from the ideal counterpart

reliability is measured by the error probability $\mathrm{P}\left[\hat{u} \neq u\right] = d_{\mathsf{V}}(p_{\hat{u}|u}, p_{u|u})$

secrecy is measured by the mutual information $I(u; z) = \mathrm{D}\left(p_{uz} \| p_u p_z\right)$

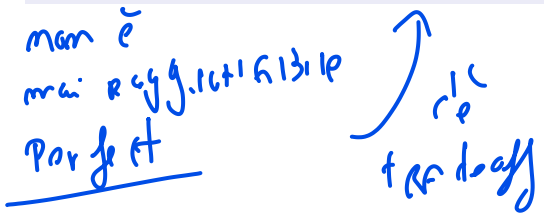
The finite and the asymptotic view

In general, the ideal case is not achievable, we can take either of two views

Finite view

We must seek a tradeoff among

- amount of information: $H(u)$
- reliability: $\mathrm{P}\left[u \neq \hat{u}\right] \leq \varepsilon$
- secrecy: $I(u;z) \leq \delta$



Asymptotic view: secrecy capacity

By processing blocks of length n, $\boldsymbol{u} = [u_1, \ldots, u_n]$, $\boldsymbol{x} = [x_1, \ldots, x_n]$ and letting $n \to \infty$, we seek the secrecy capacity

$$C_{\mathsf{s}} = \lim_{n\to\infty} \max_{p_{\boldsymbol{u}}, p_{\boldsymbol{x}|\boldsymbol{u}}, D} \left[\tfrac{1}{n} H(\boldsymbol{u})\right]$$

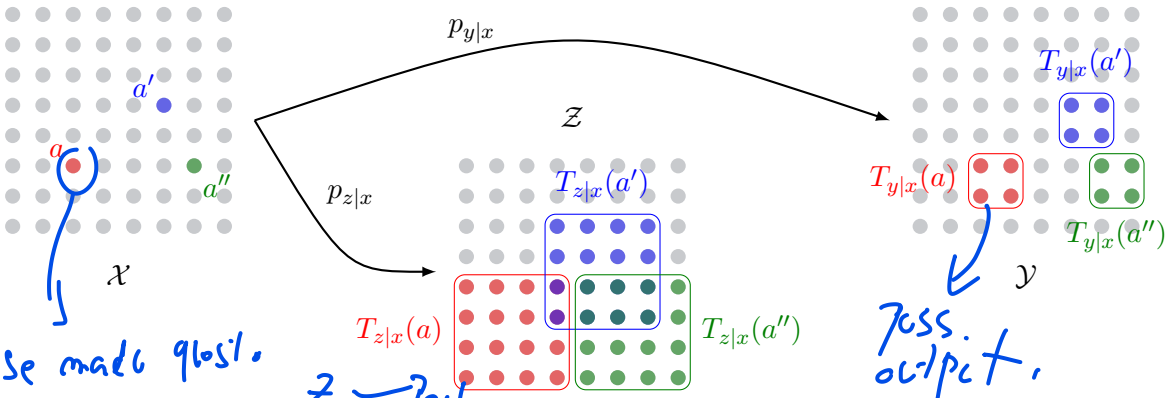
subject to the constraints:

- reliability: $\lim_{n\to\infty} P\left[\boldsymbol{u} \neq \hat{\boldsymbol{u}}\right] = 0$
- (strong) secrecy: $\lim_{n\to\infty} I(\boldsymbol{u};\boldsymbol{z}) = 0$
- or (weak) secrecy: $\lim_{n\to\infty} \frac{1}{n} I(\boldsymbol{u};\boldsymbol{z}) = 0$

Toy example: uniform channel

Consider a wiretap channel in which

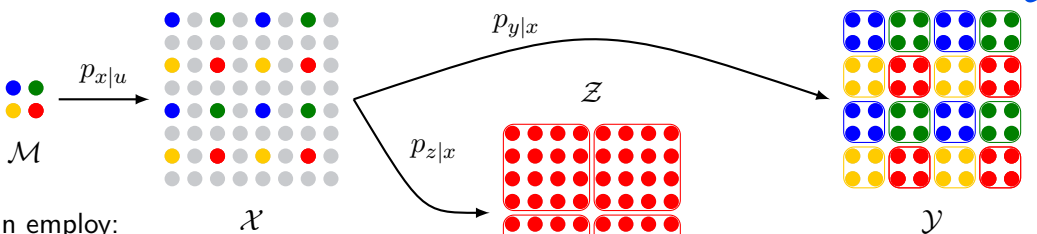
$$p_{y|x}(b|a) = \begin{cases} 1/N_{y|x} \ , \ b \in T_{y|x}(a) \\ 0 \qquad\quad , \ b \notin T_{y|x}(a) \end{cases} \quad , \quad p_{z|x}(c|a) = \begin{cases} 1/N_{z|x} \ , \ c \in T_{z|x}(a) \\ 0 \qquad\quad , \ c \notin T_{z|x}(a) \end{cases}$$



Random binning encoding

If we can find:

- a subset $\mathcal{X}' \subset \mathcal{X}$ such that $\forall a \neq a' \in \mathcal{X}'$, $T_{y|x}(a) \cap T_{y|x}(a') = \emptyset$
- a message set $\mathcal{M}$
- a partition of $\mathcal{X}'$ into $\{T_{x|u}(d)\}_{d\in\mathcal{M}}$ such that $\bigcup_{a\in T_{x|u}(d)} T_{z|x}(a) = \mathcal{Z}\ ,\ \forall d \in \mathcal{M}$



we can employ:

probabilistic uniform binning encoder

$$p_{x|u}(a|d) = \begin{cases} 1/N_{x|u} & , a \in T_{x|u}(d) \\ 0 & , a \notin T_{x|u}(d) \end{cases}$$

deterministic decoder

$\hat{u} = d$ if $y \in \bigcup_{a\in T_{x|u}(d)} T_{y|x}(a)$

Perfect reliability

Theorem

Let $p_{yz|x}$ be a uniform wiretap channel and $\mathcal{M}$ the message space for secret transmission over it. If:

- $\exists \mathcal{X}' \subset \mathcal{X}$ *such that* $\forall a \neq a' \in \mathcal{X}'$, $T_{y|x}(a) \cap T_{y|x}(a') = \emptyset$
- $\exists$ *a collection* $\left\{T_{x|u}(d)\right\}_{d \in \mathcal{M}}$ *of subsets of* $\mathcal{X}'$ *such that* $\forall d \neq d' \in \mathcal{X}'$, $T_{x|u}(d) \cap T_{x|u}(d') = \emptyset$
- *the random encoder satisfies* $p_{x|u}(a|d) = 0$, $\forall a \notin T_{x|u}(d)$

then there exist a decoding rule that achieves perfect reliability

Perfect reliability

Proof.

Let $T_{y|u}(d) = \cup_{a \in T_{x|u}(d)} T_{y|x}(a)$ be the subset of $\mathcal{Y}$ reachable from each $d \in \mathcal{M}$. Since the $T_{y|u}(d)$ are all disjoint, we can define the decoder

$$\hat{u} = d \quad , \quad \text{if } y \in T_{y|u}(d)$$

and we can compute the probability of correct detection as

$$\begin{aligned} \mathrm{P}\left[\hat{u} = u\right] &= \sum_{d \in \mathcal{M}} \mathrm{P}\left[\hat{u} = d | u = d\right] p_u(d) \\ &= \sum_{d \in \mathcal{M}} \mathrm{P}\left[y \in T_{y|u}(d) | u = d\right] p_u(d) = \sum_{d \in \mathcal{M}} p_u(d) = 1 \end{aligned}$$

□

Perfect secrecy

Theorem

Let $p_{yz|x}$ be a uniform wiretap channel and $\mathcal{M}$ the message space for secret transmission over it. If:

- *$\exists$ a collection $\left\{T_{x|u}(d)\right\}_{d\in\mathcal{M}}$ of subsets of $\mathcal{X}$ such that by letting $\mathcal{X}_{d\to c} = \left\{a \in \mathcal{X} \,:\, a \in T_{x|u}(d), c \in T_{z|x}(a)\right\}$ it holds $|\mathcal{X}_{d\to c}| = N \;,\; \forall c \in \mathcal{Z}, d \in \mathcal{M}$*
- *the random encoder satisfies*

$$p_{x|u}(a|d) = \begin{cases} 1/N_{x|u} & , \, a \in T_{x|u}(d) \\ 0 & , \, a \notin T_{x|u}(d) \end{cases}$$

then we have perfect secrecy of u wrt z

Perfect secrecy

Proof.

We show that u and z are independent. In fact:

$$\begin{aligned} p_{z|u}(c|d) &= \sum_{a \in \mathcal{X}} p_{z|xu}(c|a,d) p_{x|u}(a|d) \\ &= \sum_{a \in \mathcal{X}_{d \to c}} p_{z|x}(c|a) p_{x|u}(a|d) \\ &= N \frac{1}{N_{z|x}} \frac{1}{N_{x|u}} \end{aligned}$$

which is independent of the particular value d of u (and also uniform wrt $c \in \mathbb{Z}$) □

How many secret bits can be sent?

For perfect reliability to B:

$$\left|\mathcal{X}'\right| \leq \frac{|\mathcal{Y}|}{N_{y|x}}$$

For perfect secrecy with respect to E:

$$N_{x|u} \geq \frac{|\mathcal{Z}|}{N_{z|x}}$$

For both reliability and secrecy:

$$M = |\mathcal{M}| \leq \frac{|\mathcal{X}'|}{N_{x|u}} \leq \frac{|\mathcal{Y}|}{N_{y|x}} \frac{N_{z|x}}{|\mathcal{Z}|}$$

Secret bits in one channel use: $\log_2 M$

Memoryless channels

By considering n-symbol sequences, $\boldsymbol{x} = [x_1, \ldots, x_n]$ (and similarly for $\boldsymbol{y}$ and $\boldsymbol{z}$) and memoryless channels, $p_{\boldsymbol{yz}|\boldsymbol{x}}(\boldsymbol{b}, \boldsymbol{c}|\boldsymbol{a}) = \prod_{i=1}^{n} p_{yz|x}(b_i, c_i|a_i)$, we define:

Definition

$R_\mathsf{s} \geq 0$ is an achievable secrecy rate for memoryless channel $p_{yz|x}$ if, $\forall n \geq n_0$, there exist: a message set $\mathcal{M}_n$, an encoder and decoder such that

- $|\mathcal{M}_n| \geq 2^{nR_\mathsf{s}}$
- $\lim_{n\to\infty} \mathrm{P}\left[\hat{u} \neq u\right] = 0$
- $\lim_{n\to\infty} I(u; \boldsymbol{z}) = 0$

Definition

The secrecy capacity of memoryless channel $p_{yz|x}$ is

$$C_\mathsf{s} = \sup\left\{R_\mathsf{s} \,:\, R_\mathsf{s} \text{ is an achievable secrecy rate}\right\}$$

Memoryless channels

Theorem

If there exists some input PMD p_x such that $R_s < I(x;y) - I(x;z)$, then R_s is an achievable secrecy rate for channel $p_{yz|x}$.

Intuition

By fixing p_x and making use of typical sequences, we have as $n \to \infty$

$$|\mathcal{Y}| \to 2^{nH(y)} \quad , \quad N_{y|x} \to 2^{nH(y|x)} \quad , \quad |\mathcal{Z}| \to 2^{nH(z)} \quad , \quad N_{z|x} \to 2^{nH(z|x)}$$

so that, by the hypothesis on R_s, $2^{nR_s} < 2^{n[I(x;y)-I(x;z)]} = 2^{n[H(y)-H(y|x)-H(z)+H(z|x)]}$
It is therefore possible, for a large enough n, to find $\mathcal{M}_n$ such that

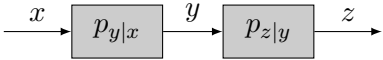
$$2^{nR_s} \leq |\mathcal{M}_n| \leq \frac{2^{nH(y)}}{2^{nH(y|x)}} \frac{2^{nH(z|x)}}{2^{nH(z)}} \approx \frac{|\mathcal{Y}|}{N_{y|x}} \frac{N_{z|x}}{|\mathcal{Z}|}$$

and leverage the uniform channel result for the existence of encoder and decoder.

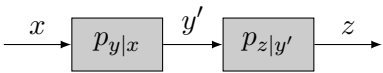
Channel orderings

We consider the following channel orderings, in decreasing order of strength

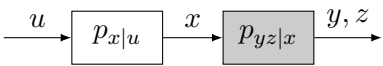
1. channel A $\to$ E is physically degraded with respect to A $\to$ B if z is independent of x given y



2. channel A $\to$ E is (stochastically) degraded with respect to A $\to$ B if z is independent of x given some other y', with $p_{y'|x} = p_{y|x}$



3. channel A $\to$ E is more noisy than A $\to$ B if for any precoder $u \to x$ with u independent of (y, z) given x, we have $I(u; y) > I(u; z)$



4. channel A $\to$ E is less capable than A $\to$ B if, for any x, we have $I(x; y) > I(x; z)$

Secrecy capacity: general results

Proposition

If $\mathsf{A} \to \mathsf{B}$ *is not more noisy than* $\mathsf{A} \to \mathsf{E}$,

$$C_{\mathsf{s}} = \max_{u} \left[I(u;y) - I(u;z) \right]$$

Proposition

If $\mathsf{A} \to \mathsf{E}$ *is less capable than* $\mathsf{A} \to \mathsf{B}$,

$$C_{\mathsf{s}} = \max_{x} \left[I(x;y) - I(x;z) \right]$$

Proposition

If $\mathsf{A} \to \mathsf{E}$ *is more noisy than* $\mathsf{A} \to \mathsf{B}$, *and both are weakly symmetric*,

$$C_{\mathsf{s}} = C_{\mathsf{AB}} - C_{\mathsf{AE}}$$

Secrecy capacity: universal result

With the notation $[\alpha]^+ = \max\{\alpha, 0\}$ we can state

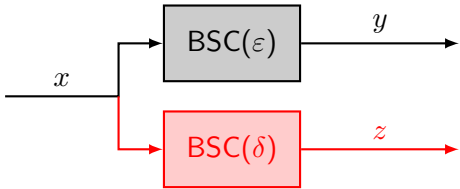
Theorem [Csiszàr-Körner, '78]

For any memoryless channel

$$\begin{aligned} C_{\mathsf{s}} &= \max_{p_u, p_{x|u}} [I(u;y) - I(u;z)]^+ \\ &\geq \max_{p_x} [I(x;y) - I(x;z)]^+ \\ &\geq [\max_{p_x} I(x;y) - \max_{p_x} I(x;z)]^+ \\ &= [C_{\mathsf{AB}} - C_{\mathsf{AE}}]^+ \end{aligned}$$

Secrecy capacity for the wiretap BSC

Let the channels from A to B and from A to E be memorlyess binary symmetric with error rates ε and δ, respectively



If $\left|\varepsilon - \frac{1}{2}\right| < \left|\delta - \frac{1}{2}\right|$
legitimate channel is more noisy
(e.g., $0 < \delta < \varepsilon < \frac{1}{2}$)

$$C_{\mathsf{s}} = 0$$

no secrecy is possible

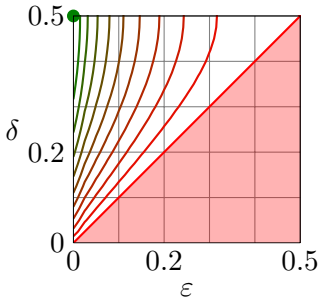
If $\left|\varepsilon - \frac{1}{2}\right| > \left|\delta - \frac{1}{2}\right|$
eavesdropper channel is more noisy
(e.g., $0 < \varepsilon < \delta < \frac{1}{2}$)

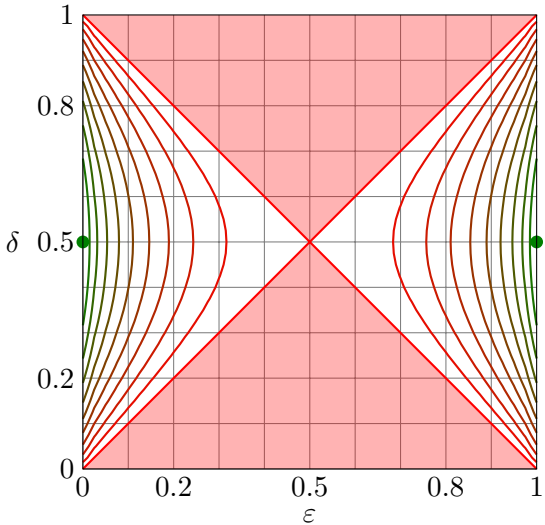
$$C_{\mathsf{s}} = C_{\mathsf{AB}} - C_{\mathsf{AE}} = h_2(\delta) - h_2(\varepsilon)$$

where
$h_2(\varepsilon) = \varepsilon \log_{1/2} \varepsilon + (1-\varepsilon) \log_{1/2}(1-\varepsilon)$

Secrecy capacity for the wiretap BSC

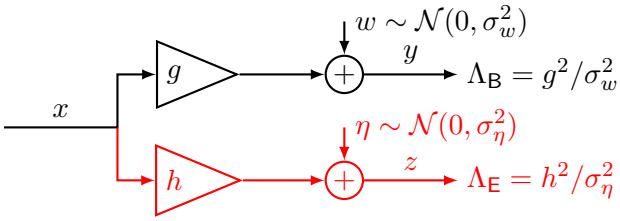
$C_s = 0, 0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 1$ [bit/channel use]





Secrecy capacity for the wiretap AWGN channel

Let the channels A $\to$ B and A $\to$ E be additive white Gaussian noise



If $\Lambda_E \geq \Lambda_B$
legitimate channel is degraded

$$C_s = 0$$

no secrecy is possible

If $\Lambda_E < \Lambda_B$
eavesdropper channel is degraded

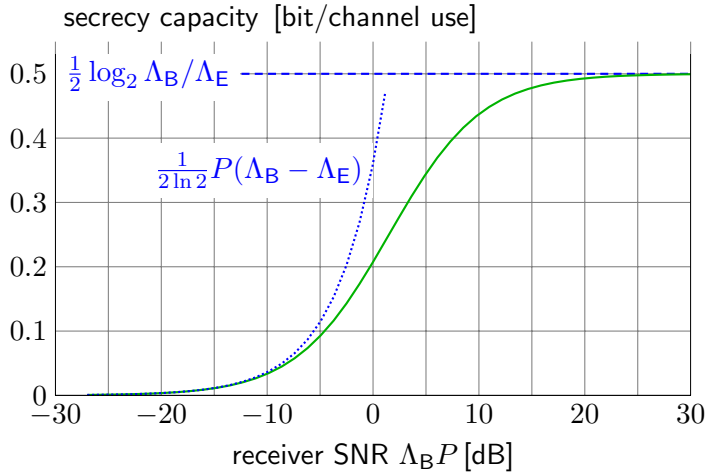
$$C_s = C_{AB} - C_{AE} = \frac{1}{2} \log_2 \frac{1 + \Lambda_B P}{1 + \Lambda_E P}$$

and it is achieved with $x \sim \mathcal{N}(0, P)$.

$$\lim_{P \to \infty} C_s = \frac{1}{2} \log_2 \frac{\Lambda_B}{\Lambda_E}$$

Secrecy capacity for wiretap AWGN

For a fixed SNR advantage $\Lambda_B/\Lambda_E = 2 \approx 3\,\text{dB}$



High SNR

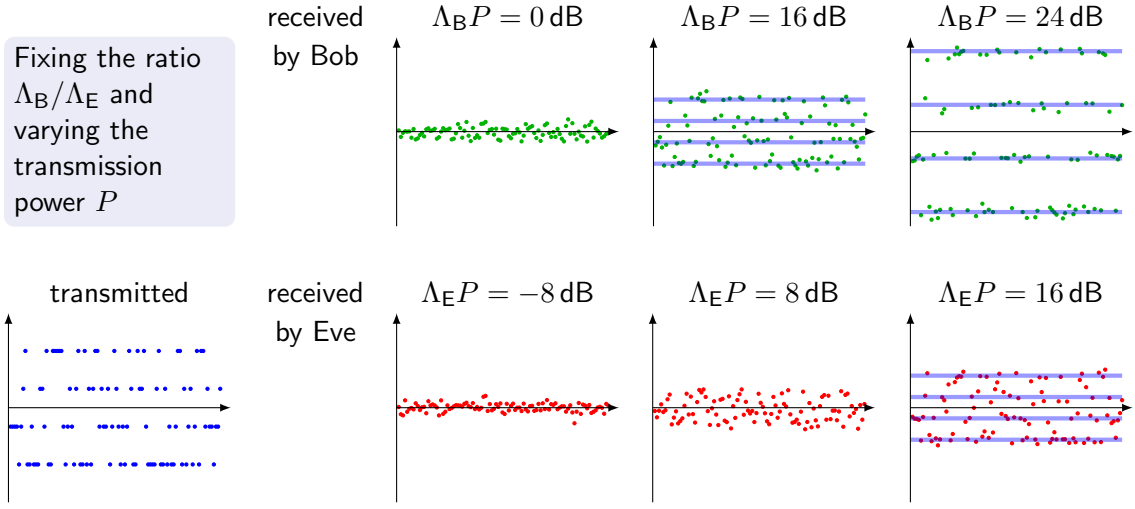
Contrary to the unconstrained capacity C_{AB}, C_s saturates as $P \to \infty$.

Low SNR

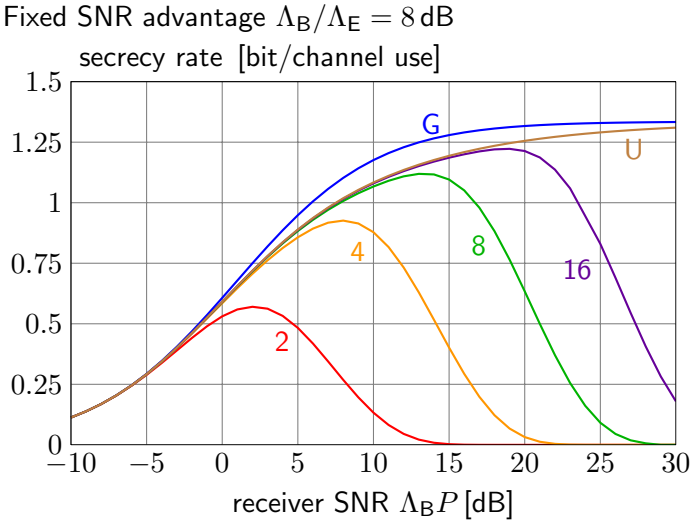
As $P \to 0$, C_s is proportional to P and the SNR difference

Physical layer secrecy with finite constellations

Fixing the ratio Λ_B/Λ_E and varying the transmission power P



Achievable secrecy rates with uniform PAM constellations



- For each constellation the secrecy rate has a maximum corresponding to its optimal transmitted power [Rodrigues, '10]
- As the size $\mathcal{C} \to \infty$, convergence to the secrecy rate of uniform input over the interval $(-\sqrt{3P}, \sqrt{3P})$.
- In the high SNR limit, AWGN C_s is also achievable by uniform PAM inputs with sufficient cardinality

Are we playing fair?

PHY secrecy requires the legitimate channel to be somehow better than the eavesdropper. Is this a reasonable assumption?

Generally speaking, no. However if the channels have sufficient diversity: in time (fading), in frequency (dispersive), in space (MIMO), the transmitter can choose to use only those time intervals, subchannel bands, space directions where the legitimate channel is better

This requires the transmitter to know the state of both the legitimate and eavesdropper channels. Is this a reasonable assumption?

Generally speaking, no. However, if the transmitter knows the state of the legitimate channel by receiver cooperation, he can choose only those subchannels where the legitimate channel is very good. If there is low correlation between the legimitate and eavesdropper channel, it is unlikely that the eavesdropper channel is very good in the same subchannels

Summary

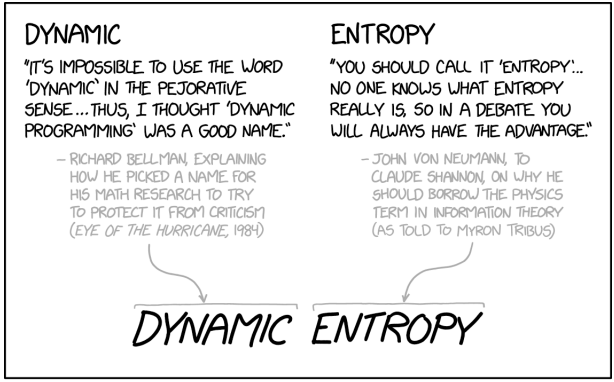
In this lecture we have:

- introduced the wiretap channel model and the requirements for physical layer secrecy
- introduced the notion of random binning encoding
- defined the information theoretic measures of secrecy rate and secrecy capacity
- shown and discussed secrecy capacity values for the BSC and the AWGN channels

Assignment

- class notes

End of lecture



Dynamic Entropy, reproduced from xkcd URL: xkcd.com/2318