VII Physical Layer Security

This chapter will deal with reliable & secure communication over noisy channels in the presence of an adversarial eavesdropper (Eve).

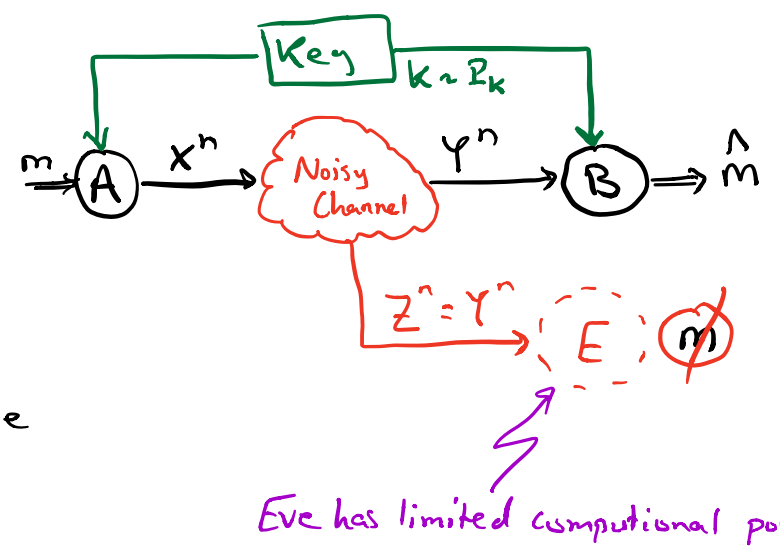
Our goal will be (once the problem is formulated) to design a code that enables Bob (the legitimate receiver) to reliably decode the message while keeping it secret from Eve, in an information theoretic sense.

Information Security vs. Cryptography

Cryptography: (i) Adversaries are assumed to have limited computational capabilities

(ii) The legitimate parties are assumed to both have access to a shared random key.

* Security is established by using the key as part of the encryption phase and showing that breaking the cryptosystem w/o knowing the key cannot be done w/in reasonable computational powers.



Information Theoretic Security:

$I(M; Z^n) \xrightarrow{n\to\infty} 0$

$I(M; A(Z^n)) \le I(M; Z^n) \xrightarrow{n\to\infty} 0$

(i) Adversaries are computationally unbounded

(ii) No shared randomness is assumed to be available to the legitimate parties (although local randomness at the transmitter will be used).

* Security is established by showing that the eavesdropper's observation Z^n carries a negligible amount of information about the secret message, i.e. devising a code such that $I(M; Z^n) \xrightarrow{n\to\infty} 0$

What's the catch?

The IT paradigm assumes that the statistics of the communication channel to the eavesdropper are known (!) to the legitimate parties, who design their code based on that knowledge.

Problem Formulation

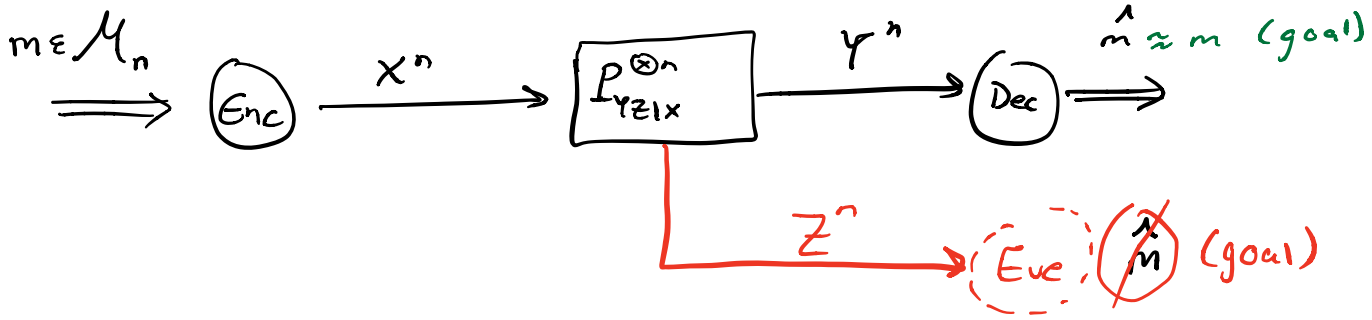
Let $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ be finite alphabets and $P_{YZ|X}$ be a transition kernel from $\mathcal{X}$ to $\mathcal{Y} \times \mathcal{Z}$. This tuple $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, P_{YZ|X})$ constitutes a wiretap channel (WTC) with input in $\mathcal{X}$ and two outputs in $\mathcal{Y}$ and $\mathcal{Z}$, corresponding to the observations at the legitimate receiver and the eavesdropper, respectively.

We assume DM-WTC w/o feedback so the n-fold extension is $(\mathcal{X}^n, \mathcal{Y}^n, \mathcal{Z}^n, P_{YZ|X}^{\otimes n})$, namely

$$P_{YZ|X}^{\otimes n}(y^n, z^n|x^n) = \prod_{i=1}^{n} P_{YZ|X}(y_i, z_i|x_i)$$

Let $\mathcal{M}_n := \{1, \ldots, \lceil 2^{nR} \rceil\}$ be the message set.

$\Rightarrow$ Our setup is thus:



We next define a wiretap code but allow for stochastic encoding!

Definition (Wiretap Code):

A $(2^{nR}, n)$ wiretap code C_n has:

(i) A message set $\mathcal{M}_n := \{1, \ldots, 2^{nR}\}$

(ii) A stochastic encoder described by a transition kernel $Q_{X^n|M}$ from $\mathcal{M}_n$ to $\mathcal{X}^n$ (i.e. $Q_{X^n|M}(\cdot|m) \in \mathcal{P}(\mathcal{X})$ $\forall\, m \in \mathcal{M}_n$)

(iii) A deterministic decoder $g_n : \mathcal{Y}^n \to \mathcal{M}_n$

Induced Distribution:

Given a WTC $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, P_{YZ|X})$, a wiretap code $C_n = (Q_{X^n|M}, g_n)$ and a message distribution $P_M \in \mathcal{P}(\mathcal{M})$, the induced joint distribution is:

$$Q^{(C_n)}_{M,X^n,Y^n,Z^n,\hat{M}}(m, x^n, y^n, z^n, \hat{m}) = P_M(m)\, Q_{X^n|M}(x^n|m)\, P^{\otimes n}_{YZ|X}(y^n, z^n|x^n)\, \mathbb{1}_{\{\hat{m} = g_n(y^n)\}}$$

Our performance metrics are reliability & security, which we define next.

Definition (Probability of Error):

For a $(2^{nR}, n)$ wiretap code C_n let

$$e_{avg}(C_n) := \frac{1}{|\mathcal{M}_n|} \sum_{m \in \mathcal{M}_n} e_m(C_n) \qquad \text{(average)}$$

$$e_{max}(C_n) := \max_{m \in \mathcal{M}_n} e_m(C_n) \qquad \text{(maximal)}$$

where

$$e_m(C_n) := P^{(C_n)}_{Q^{(C_n)}}\left(g_n(Y) \neq m \,\middle|\, M = m\right) = \sum_{y^n : g_n(y^n) \neq m} Q^{(C_n)}_{Y^n|M}(y^n|m)$$

Definition (Average & Maximal Leakage)

For a $(2^{nR}, n)$ wiretap code c_n and any $P_M \in \mathcal{P}(\mathcal{M})$ define $\ell(c_n, P_M) := I_{Q^{(c_n)}}(M; Z^n)$. This quantity is called the information leakage w.r.t c_n and P_M.

The <u>average</u> information leakage

$$\ell_{avg}(c_n) := \ell(c_n, \mathrm{Unif}(\mathcal{M}_n))$$

The <u>maximal</u> information leakage

$$\ell_{max}(c_n) := \max_{P_M \in \mathcal{P}(\mathcal{M})} \ell(c_n, P_M)$$

Definition (Achievability)

A rate $R > 0$ is achievable w/ <u>maximal</u> guarantees for the DM-WTC $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, P_{YZ|X})$ w/o feedback if there exists a sequence $\{c_n\}_{n \in \mathbb{N}}$ of $(2^{nR}, n)$ wiretap codes such that

$$\begin{cases} e_{max}(c_n) \xrightarrow{n \to \infty} 0 \\ \ell_{max}(c_n) \xrightarrow{n \to \infty} 0 \end{cases}$$

with the average guarantee definition of achievability defined analogously with $e_{avg}(c_n)$ and $\ell_{avg}(c_n)$ instead.

Definition (Secret-Capacity)

The secrecy-capacity with <u>maximal</u> guarantees for the DM-WTC $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, P_{YZ|X})$ w/o feedback is:

$$C_{max}(P_{YZ|X}) := \sup\{R : R \text{ is achievable w/ } \underline{\text{maximal}} \text{ guarantees}\}$$

Similarly

$$C_{avg}(P_{YZ|X}) := \sup\{R : R \text{ is achievable w/ } \underline{\text{average}} \text{ guarantees}\}$$

We will assume that the WTC is (physically) degraded in the following sense → For any input distribution $P_X \in \mathcal{P}(\mathcal{X})$ the tuple $(X, Y, Z) \sim P_X \cdot P_{YZ|X}$ forms a Markov chain $X \leftrightarrow Y \leftrightarrow Z$ (concatenated BSC or AWGN are physically degraded).

Theorem (Degraded WTC Secrecy-Capacity):

The secrecy-capacity (w/ maximal or average guarantees) of a degraded DM-WTC $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, P_{YZ|X})$ w/o feedback is:

$$C_{max}(P_{YZ|X}) := C_{avg}(P_{YZ|X}) = \max_{P_X \in \mathcal{P}(\mathcal{X})} (I(X;Y) - I(X;Z)) = \max_{P_X \in \mathcal{P}(\mathcal{X})} I(X;Y|Z)$$

where the underlying distribution is $P_X P_{YZ|X}$.

Discussion Section

$$\ell_{avg}(C_n, \text{Unif}(\mathcal{M}_n)) = I_{Q^{(C_n)}_{M,Z^n}}(M; Z^n)$$

← Why avg terminology makes sense

$$Q^{(C_n)}_M Q^{(C_n)}_{Z|M} = \text{Unif}(\mathcal{M}_n) Q^{(C_n)}_{Z^n|M}$$

$$= D_{KL}\left(Q^{(C_n)}_{M,Z^n} \,\|\, \text{Unif}(\mathcal{M}_n) \otimes Q^{(C_n)}_{Z^n}\right)$$

$$= D_{KL}(\text{Unif}(\mathcal{M}_n) \,\|\, \text{Unif}(\mathcal{M}_n)) + D_{KL}(Q^{(C_n)}_{Z^n|M} \,\|\, Q^{(C_n)}_Z \mid \text{Unif}(\mathcal{M}_n))$$

$\text{Unif}(\mathcal{M}_n) \to 0$

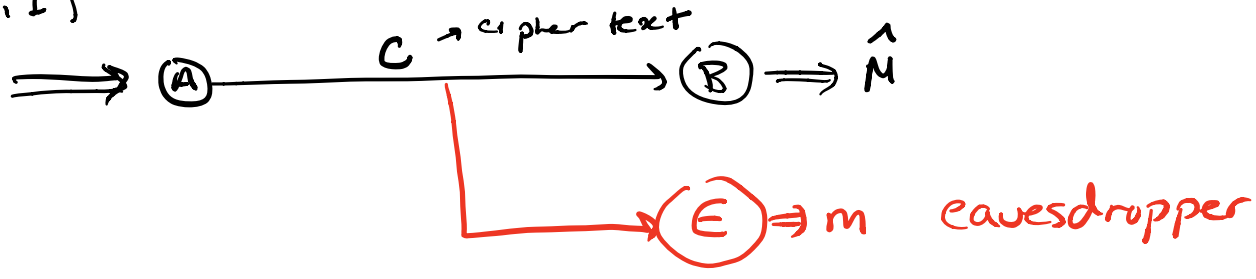
$$= \sum_{m \in \mathcal{M}_n} \frac{1}{|\mathcal{M}_n|} D_{KL}(Q^{(C_n)}_{Z^n|M}(\cdot|m) \,\|\, Q^{(C_n)}_{Z^n}(\cdot)) \xrightarrow{n\to\infty} 0$$

$$\ell_{max}(C_n) \le \max_{m \in \mathcal{M}_n} D_{KL}(Q^{(C_n)}_{Z^n|M}(\cdot|m) \,\|\, P_Z^{\otimes n}) \xrightarrow{n\to\infty} 0$$

Example

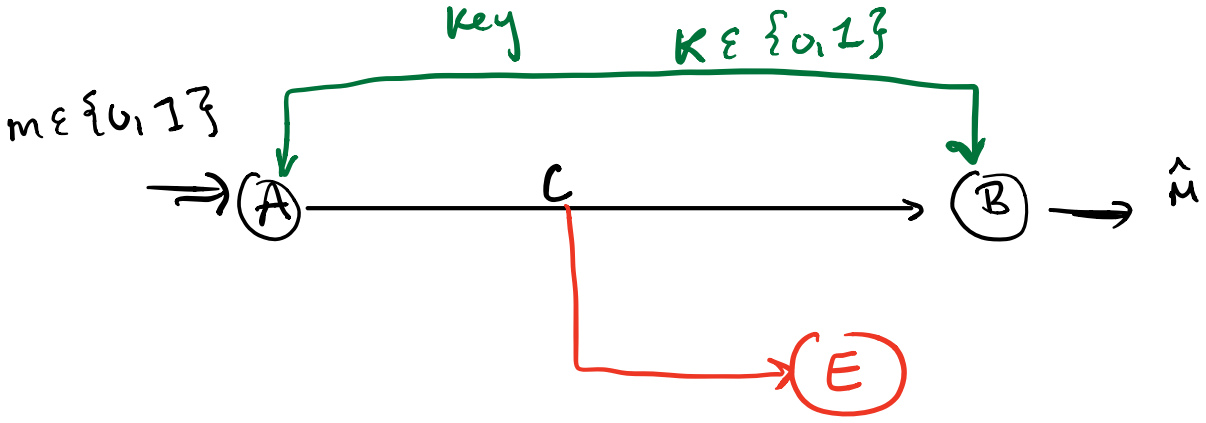
Alice wants to send Bob 1 secret bit.

$m \in \{0, 1\}$



Is reliable and secure communication possible? **NO**

Let A + B have access to same extra resource.



How to build a reliable and secure protocol?

<u>Information Theoretic Security:</u> Require $M \sim P_M = \text{Ber}(\frac{1}{2})$ and $C = f(M,K)$ are statistically independent $\Leftrightarrow I(M;C) = 0$.

<u>Protocol?</u>

Alice (encoder) $f: \mathcal{M} \times \mathcal{K} \to \mathcal{C}$

Bob (dedoder) $g: \mathcal{C} \times \mathcal{K} \to \mathcal{M}$

$M \sim P_M = \underbrace{\text{Unif}(\mathcal{M})}_{\text{Ber}(1/2)}$ $\quad K \sim P_K = \underbrace{\text{Unif}(\mathcal{K})}_{\text{Ber}(1/2)}$

- Binary Case: $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}$

<u>Goal</u>

- Reliability

$\to \mathbb{P}(\hat{M} = M) = \mathbb{P}(g(C,K) = M) = \mathbb{P}(g(f(M,K) = M) = 1$

- Security

$I(M;C) = 0$

Encoding for Reliability

M	K	f(M,K)	$M+K$ (OR)	$M \cdot K$ (AND)	$M \oplus K$ (XOR)
0	0	f(0,0)	0	0	0
0	1	f(0,1)	1	0	1
1	0	f(1,0)	1	0	1
1	1	f(1,1)	1	1	0

XOR works for reliability! AND/OR do NOT: given a key C doesn't allow recovery of M

How about security?

$$C = f(M,K) = M \oplus K$$

$M \sim Ber(1/2)$

$K \sim Ber(1/2)$

Is $C \perp M$? YES

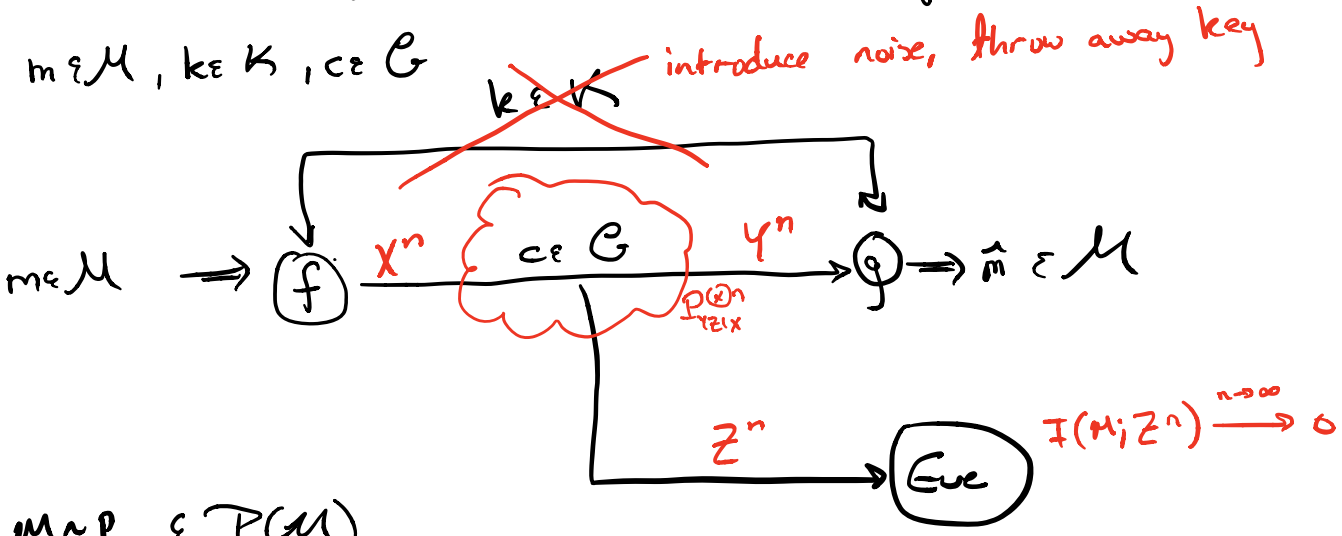
$$\mathbb{P}(M=0 \mid C=0) = 1/2$$

$$\mathbb{P}(M=0 \mid C=1) = 1/2$$

Shannon's Cipher System

Generalization of above to longer sequences

$m \in \mathcal{M}, k \in \mathcal{K}, c \in \mathcal{C}$



$M \sim P_M \in \mathcal{P}(\mathcal{M})$

$K \sim P_K \in \mathcal{P}(\mathcal{K})$

$f: \mathcal{M} \times \mathcal{K} \to \mathcal{C}$

$g: \mathcal{C} \times \mathcal{K} \to \mathcal{M}$ $\Rightarrow$ $\mathcal{A}$

$\mathbb{P}(\hat{M} = M) = 1$

$I(M;C) = 0$

$I(M;C|K) = H(M|K) - \cancel{H(M|KC)}^{\,0}$

$= H(M)$

Theorem (Converse): Any protocol (f,g) that is reliable & secure has $H(K) \geq H(M)$

Proof

Have

$$H(M|C) = H(M) \qquad \text{(security)}$$

$$H(M|K,C) = 0 \qquad \text{(reliability)}$$

$$H(K) \geq H(K) - H(K|CM) \geq H(K|C) - H(K|CM) = I(K;M|C)$$

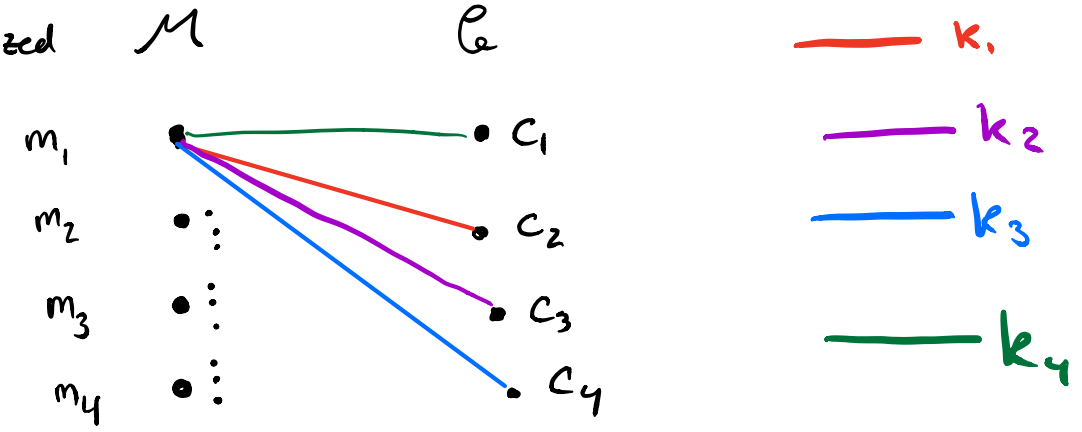
$$= H(M|C) - \cancel{H(M|KC)}^{\,0} = H(M)$$

Theorem: If $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$ then a protocol (f, g) is reliable & secure iff both of the following hold:

(i) $\forall (m, c) \in \mathcal{M} \times \mathcal{C} \quad \exists! k \in \mathcal{K}, \quad c = f(m, k)$

(ii) $P_{\mathcal{K}} = \text{Unif}(\mathcal{K})$

item (i) visualized



Corollary: Let $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}^n$, $M, K \sim \text{Unif}(\{0,1\}^n)$ and independent. Consider the n-fold extension of the XOR scheme from before:

$$f(m, k) = m \oplus_2^n k$$

$$g(c, k) = c \oplus_2 k$$

then (f, g) protocol is reliable and secure and in fact optimal (one-time pad)

$$I_{avg}\left(C_n, \mathrm{Unif}(\mathcal{M}_n)\right) = I_Q^{(C_n)}(M; Z^n)$$

$$I_{max}(C_n) \le \max_{m \in \mathcal{M}_n} D_{KL}\left(Q_{Z^n|M}^{(C_n)}(\cdot|m) \,\|\, P_Z^{\otimes n}\right) \xrightarrow[n\to\infty]{} 0$$

Any Z !! messaging!

To be proved