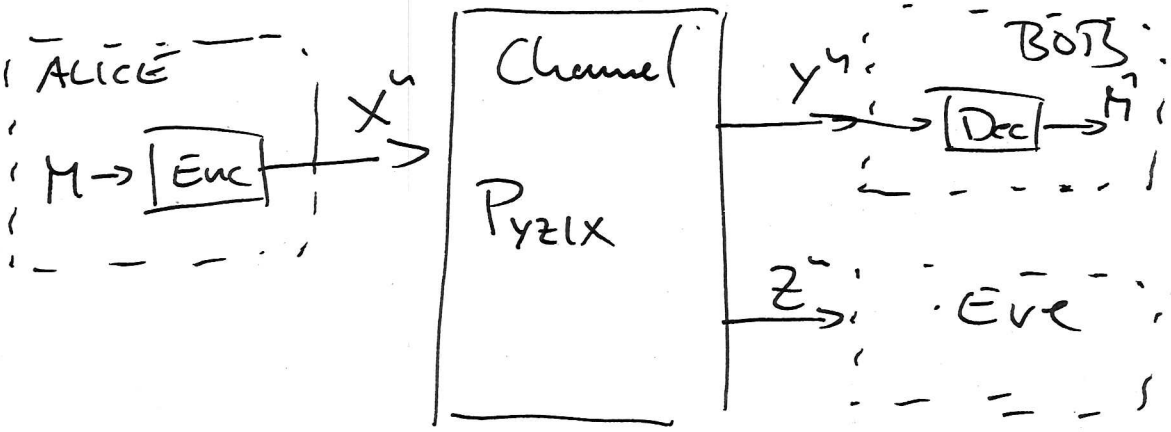
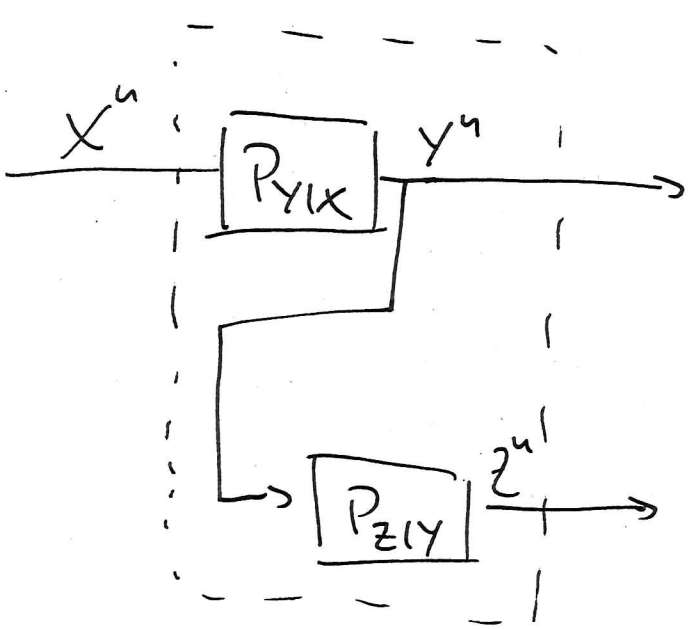
WIRETAP CHANNEL

. Wiretap channel is the simplest building block of secure communication (reliability + secrecy)



. We only look at the special case of degraded channels, i.e. $X-Y-Z$ is a Markov chain:



→ Bob's channel is strictly better than Eve's.

→ Goal: Transmit a message reliably to Bob while keeping it secure from Eve!

Definition: (Code)

A code for the wiretap channel consists of a stochastic encoder

$$E : \mathcal{M} \to \mathcal{X}^n$$

with message set $\mathcal{M} = \{1, \ldots, M_n\}$ and a decoder

$$\varphi : \mathcal{Y}^n \to \mathcal{M}$$

Remark:

A stochastic encoder is a stochastic matrix such that for each $m \in \mathcal{M}$

$E(x^n|m)$ is the probability that message m is encoded into the codeword x^n.

A deterministic encoder is a special case

$$f(x^n|m) = \begin{cases} 1 & x^n = x_m^n \\ 0 & \text{else} \end{cases}$$

- without secrecy requirement deterministic encoding is sufficient, with secrecy we necessarily need a stochastic encoder! (see problem set)

Definition (Achievable rate)

A rate $R>0$ is called achievable if for every $\tau>0$, there exists an $n_0 = n_0(\tau)$ such that for every $n \geq n_0$ there is a code with

i) $P[\hat{M} \neq M] \leq \varepsilon_n$ (average prob of error)

ii) $\frac{1}{n} I(M; Z^n) \leq \delta_n$ (weak secrecy)

iii) $\frac{1}{n} \log |\mathcal{M}| \geq R - \tau$

with $\varepsilon_n, \delta_n \to 0$ as $n \to \infty$.

The secrecy capacity C_S is the maximum of all achievable rates R.

Theorem:

The secrecy capacity C_S of the degraded (X-Y-Z) wiretap channel is

$$C_S = \max_{P_X} \left(I(X;Y) - I(X;Z) \right)$$

Proof:

As usual:

1) Achievability

2) Converse

Achievability

- We have to show that for given input distr. P_X, the rate $R_S = I(X;Y) - I(X;Z)$ is achievable

→ Idea: stochastic encoder allows multiple codewords for each message ⇝ to confuse Eve

- for every P_X, we generate $2^{n(R_S+\tilde{R})}$ codewords $x^n \in \mathcal{X}^n$ according to $P_X^n(x^n) = \prod_{i=1}^{n} P_X(x_i)$
- We label the codewords

$$x^n_{me}$$

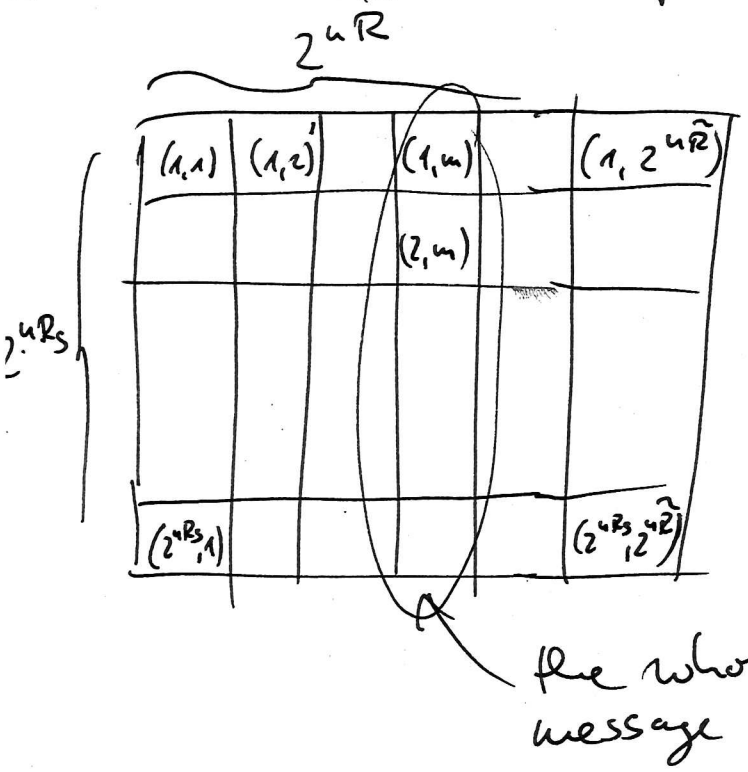
with

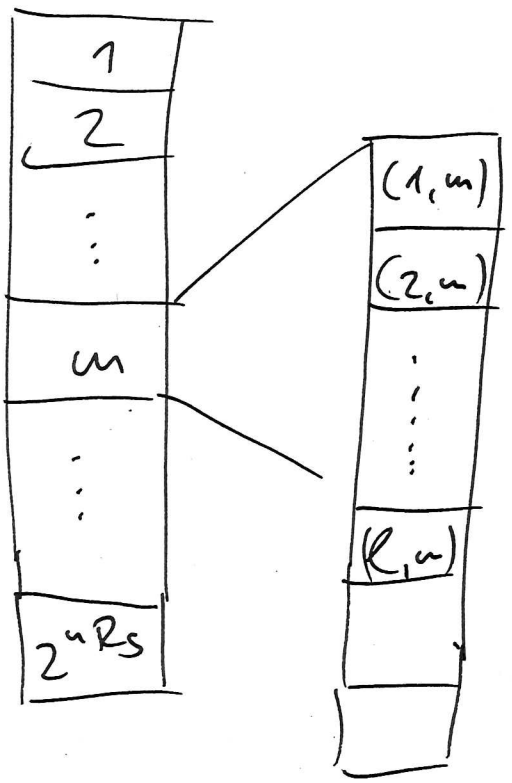
$m \in \mathcal{M} = \{1, \dots, 2^{nR_S}\}$ conf. message

$l \in \mathcal{L} = \{1, \dots, 2^{n\tilde{R}}\}$ dummy message without information

→ the task of the "dummy" message is to protect the confidential message

→ codebook has the following structure





$$\rightarrow \quad R_S = I(X;Y) - I(X;Z)$$

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

- to send message $m \in \mathcal{M}$, choose randomly index $l \in \mathcal{L} = \{1, \dots, 2^{n\tilde{R}}\}$ uniformly at random and transmit $x^n_{m,l} \in \mathcal{X}^n$.

→ Bob decodes both message m and index l by using a joint typicality decoder, i.e.

$$(X^n_{\hat{m},\hat{l}}, Y^n) \in T^n_\varepsilon(X,Y)$$

- Bob can decode both m and l if

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

which follows from the classical P2P channel. (without secrecy)

- (Note that l is decoded although not needed)

→ The important question is how much resources are needed to "confuse" Eve.

- It is sufficient to choose

$$\tilde{R} = I(X;Z) \qquad \text{(give } M\text{, Eve could decode } L\text{)}$$

to have weak secrecy $\frac{1}{n} I(M; Z^n) \in \mathcal{J}_n$

· Consider the "information leakage rate" to Eve

$$\frac{1}{n} I(M; Z^n)$$

$$= \frac{1}{n} I(M, L; Z^n) - \frac{1}{n} I(L; Z^n | M)$$

$$= \frac{1}{n} I(X^n; Z^n) - \frac{1}{n} H(L|M) + \frac{1}{n} H(L|Z^n M)$$

$$= \underbrace{\frac{1}{n} I(X^n; Z^n)}_{\text{Information leakage not controllable}} \underbrace{- \frac{1}{n} H(L) + \frac{1}{n} H(L|Z^n M)}_{\text{have to be choose to compensate first term}}$$

(I) (II) (III)

(II) By construction, all codewords are equiprobable

$$\frac{1}{n} H(L) = \frac{1}{n} \log \lceil 2^{n\tilde{R}} \rceil \geq \tilde{R}$$

(III) $\frac{1}{n} H(L|Z^n M) = \frac{1}{n} H(X^n | Z^n M)$

$$\leq \frac{1}{n} (P_e \log \lceil 2^{n\tilde{R}} \rceil + H_2(P_e)) \quad \text{(Fano)}$$

$$\leq \frac{1}{n} (P_e \cdot \tilde{R} + 1)$$

$$\to \delta_n \to 0$$

(I) $\frac{1}{n} I(X^n; Z^n) = I(X; Z)$

since X^n, Z^n are i.i.d. $\sim P_{XZ}$

(I) (III) $\rightsquigarrow$

$$\frac{1}{n} I(M; Z^n) \leq I(X; Z) - \widetilde{R} + \delta_n$$

with $\widehat{R} \doteq I(X; Z)$ $\quad (\widehat{R} = I(X; Z) - \delta_n)$

we get

$$\frac{1}{n} I(M; Z^n) \leq \delta_n \to 0$$

Converse

Fano's inequality

$$H(M|Y^n) \leq P_e \cdot \log|\mathcal{M}| + H_2(P_e) = n \cdot \varepsilon_n$$

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

We know that we have a "good" code that achieves the secrecy capacity

$\rightsquigarrow$ in particular secrecy is satisfied

$$\frac{1}{n} I(M; Z^n) \leq \delta_n \to 0$$

· We get for the rate

$$
\begin{aligned}
nR_S &= H(M) \\
&= I(M;Y^n) + H(M|Y^n) \\
&\le I(M;Y^n) + n\varepsilon_n \qquad \text{(Fano)} \\
&= I(M;Y^n) - I(M;Z^n) + I(M;Z^n) + n\varepsilon_n \\
&\le I(M;Y^n) - I(M;Z^n) \quad n(\delta_n + \varepsilon_n) \qquad \text{(secrecy)} \\
&= I(M;Y^n|Z^n) + n\tilde{\varepsilon} \qquad \text{(since } M\text{-}X\text{-}Y\text{-}Z \text{ Markov chain)} \\
&\le I(X^n;Y^n|Z^n) + n\tilde{\varepsilon} \qquad \text{(data processing inequality)} \\
&\le nI(X;Y|Z) + n\tilde{\varepsilon} \\
&= n\big(I(X;Y) - I(X;Z)\big| + n\tilde{\varepsilon} \qquad \text{(Markov chain } X\text{-}Y\text{-}Z\text{,}
\end{aligned}
$$

□