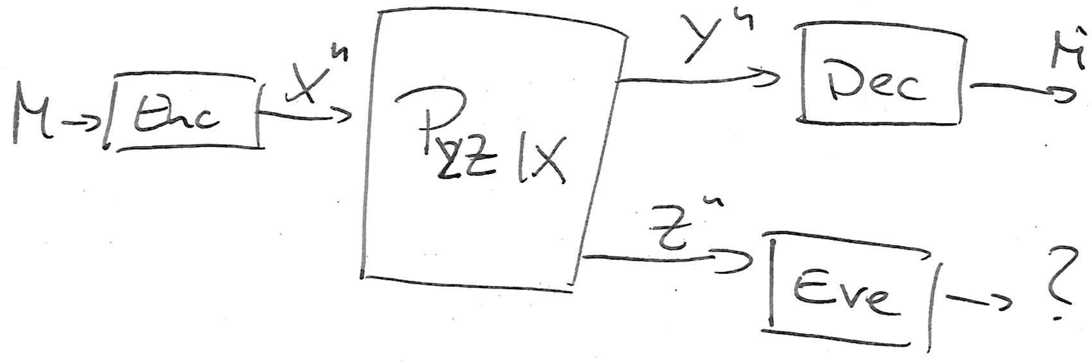
4. SECRECY CRITERION

- We consider a communication scenario of the form



- Last time, in Shannon's Secrecy System, we considered <u>perfect</u> secrecy:

$$I(M;Z^n) = D(P_{MZ} \| P_M P_{Z^n}) \overset{\downarrow}{=} 0$$

This notion is too stringent.

- Replace requirement of <u>exact</u> statistical independence by <u>asymptotic</u> statistical independence as block length n goes to infinity
- In principle, ~~any~~ measure in terms of any distance d defined on joint distribution ~~of~~ P_{MZ^n} possible:

$$\lim_{n\to\infty} d(P_{MZ^n}, P_M P_{Z^n}) = 0$$

There are many different notions on secrecy out there....

1) Weak secrecy

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

2) Strong secrecy:

$$I(M;Z^n) \leq \varepsilon_n$$

3) Effective secrecy / Stealth

$$D(P_{MZ^n} \| P_M Q_{Z^n}) \leq \varepsilon_n$$

4) Semantic security

$$\max_{P_M} I(M;Z^n) \leq \varepsilon_n$$

- Weak secrecy has been first proposed by Wyner in 1975 which has been used without asking about its operational meaning
- Weak secrecy has some considerable drawbacks and has been replaced recently by stronger notions of security.

1) Weak Secrecy

. Definition in terms of "rate"

⇝ equivocation rate $\frac{1}{n} H(M|Z^n) \approx$ information rate $\frac{1}{n} H(M)$

⇝ information leakage rate $\frac{1}{n} I(M; Z^n) \to 0$

Proposition: Weak secrecy ($\frac{1}{n} I(M; Z^n) \leq \varepsilon_n$) implies that the average decoding error at Eve approaches 1.

Proof: From Fano's Inequality we have

$$H(M|Z^n) \leq H(M|\hat{M}) \leq H_2(P_e^{Eve}) + P_e^{Eve} \log|M|$$

so that

$$P_e^{Eve} \geq \frac{H(M|Z^n) - H_2(P_e^{Eve})}{\log|M|}$$

$$= \frac{H(M) - I(M; Z^n) - H_2(P_e^{Eve})}{nR} \qquad (R = \frac{1}{n} \log|M|)$$

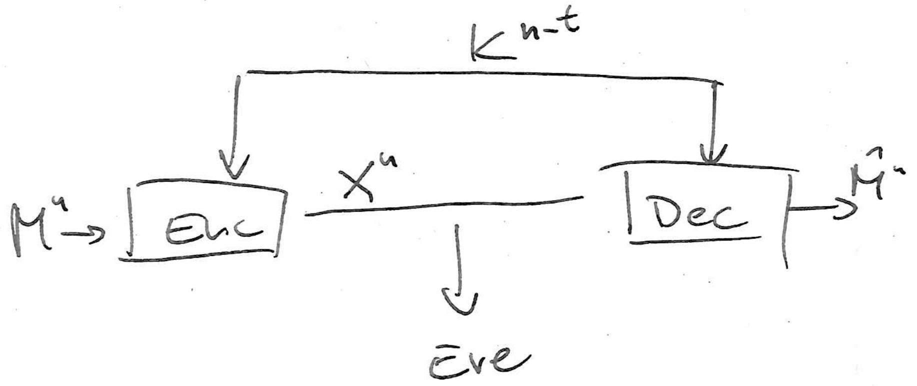
$$= 1 - \underbrace{\frac{1}{n} I(M; Z^n) \frac{1}{R}}_{\to 0 \text{ (weak secrecy)}} - \underbrace{\frac{H_2(P_e^{Eve})}{nR}}_{\to 0}$$

⇝ Asymptotically, Eve cannot decode the transmitted message

⇝ If this is true for weak secrecy, then it also holds for stronger notion of security!

⇝ However, convergence can be arbitrarily slow!

• Consider the following example:



Let $n \geq 1$ and $t = \lfloor \sqrt{n} \rfloor$. Suppose that Alice encodes message bits $M^n \in \{0,1\}^n$ into a code word $X^n \in \{0,1\}^n$ with $n-t$ secret-key bits $K^{n-t} \in \{0,1\}^{n-t}$ as

$$X_i = \begin{cases} M_i \oplus K_i & \text{for } i \in [1, n-t] \\ M_i & \text{for } i \in [n-t+1, n] \end{cases}$$

The key bits K_i for $i \in [1, n-t]$ are assumed i.i.d. according to $\mathcal{B}(0,5)$ and known to Bob. In other words, Alice performs a one-time pad of the first $n-t$ bits of M with the $n-t$ key bits and she appends the remaining t bits unprotected. Eve is assumed to intercept X^n directly.

. Using the crypto lemma, we obtain

$$\forall n \geq 1 \qquad H(M|X^n) = n - t = H(M) - t$$

$\rightsquigarrow I(M; X^n) = t = \lfloor\sqrt{n}\rfloor$

$\rightsquigarrow$ Does not satisfy the strong secrecy criterion
Even worse, the information leaked to Eve grows unbounded with n!

. However, we observe

$$\lim_{n\to\infty} \frac{1}{n} I(M; X^n) = \lim_{n\to\infty} \frac{\lfloor\sqrt{n}\rfloor}{n} = 0$$

$\rightsquigarrow$ This scheme satisfies the weak secrecy criterion!

- One could argue that this has been constructed ad hoc to exhibit flaws (Eve obtains a fraction of message bits without errors
- See Tutorial / Exercise for a more involved example

$\rightsquigarrow$ This does <u>not</u> imply all weakly secure schemes are useless, but suggests that not all measures of asymptotic stat. independence are meaningful

2) Strong Secrecy

- Definition in terms of absolute value instead of rate

$\rightsquigarrow$ "total amount of information leaked to Eve" must be small

$\rightsquigarrow$ $I(M; Z^n) \to 0$

Proposition: For a wiretap code of rate $R = \frac{1}{n}\log|M|$ with strong secrecy $I(M; Z^n) = \varepsilon_n$ and $\varepsilon_n \to 0$ as $n \to \infty$, the decoding error at Eve satisfies

$$P_e^{Eve} \geq 1 - 2^{-nR} - c\sqrt{\varepsilon_n}$$

for any decoding strategy Eve may use.

Proof: See Tutorial / Exercise

Remark:

If we have a code with $I(M; Z)^n \leq 2^{-n\delta}$ with fixed constant $\delta > 0$, then

$$P_e^{Eve} \geq 1 - 2^{-nR} - c\,2^{-n\frac{\delta}{2}}$$

i.e. the average decoding error at Eve approaches 1 exponentially fast!

3) Effective secrecy / stealth

Consider the criterion

$$D(P_{MZ^n} \| P_M Q_Z^n)$$

$$= \sum_{m\in\mathcal{M}} \sum_{z^n\in\mathcal{Z}^n} P_{MZ^n}(m,z^n) \log \frac{P_{MZ}(m,z^n)}{P_M(m)\, Q_Z^n(z^n)} \cdot \frac{P_{Z^n}(z^n)}{P_{Z^n}(z^n)}$$

$$= \sum_{m\in\mathcal{M}} \sum_{z^n\in\mathcal{Z}^n} P_{MZ^n}(m,z^n) \left(\log \frac{P_{MZ^n}(m,z^n)}{P_M(m)\, P_{Z^n}(z^n)} + \log \frac{P_{Z^n}(z^n)}{Q_Z^n(z^n)} \right)$$

$$= \underbrace{I(M;Z^n)}_{\text{strong secrecy}} + \underbrace{D(P_{Z^n} \| Q_Z^n)}_{\text{stealth}}$$

"Effective secrecy = strong secrecy + stealth"

- P_{Z^n} is output distribution when Alice transmits conf. data
- Q_Z^n is output distribution when Alice does not send meaningful information

$$Q_Z^n(z^n) = \sum_{x^n\in\mathcal{X}^n} Q_X^n(x^n)\, P_{Z^n|X^n}(z^n|x^n)$$

"random/garbage" transmit signals

- If $D(P_{MZ^n} \| P_M Q_Z^n)$ is small, this implies that both $I(M; Z^n)$ (strong secrecy) and $D(P_{Z^n} \| Q_Z^n)$ (stealth) are small!

⇝ Stealth allows to control the output distribution at Eve. "You can decide how the received signals at Eve look like"

⇝ Allows you to hide your secure communication to make it look like no communication for ex.

⇝ Eve learns nothing about M and cannot recognize whether Alice is transmitting anything meaningful at all!