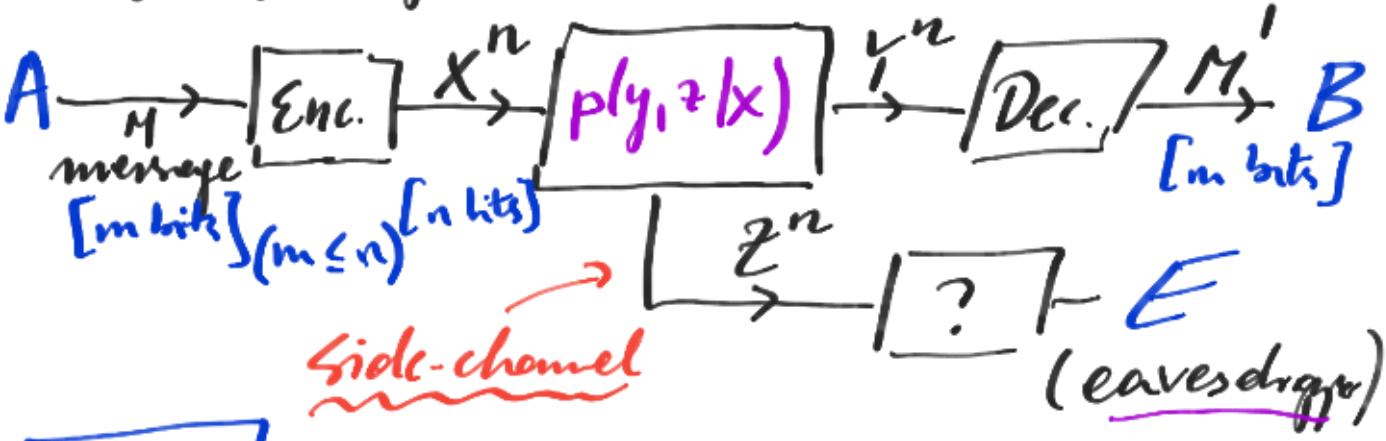
10. Secret channel capacities, EC and PA

(c) Confidential communication: cryptography

(Shannon) Secret Capacity



CLT

Csiszár-Körner Theorem

Secret bit rate R between A & B

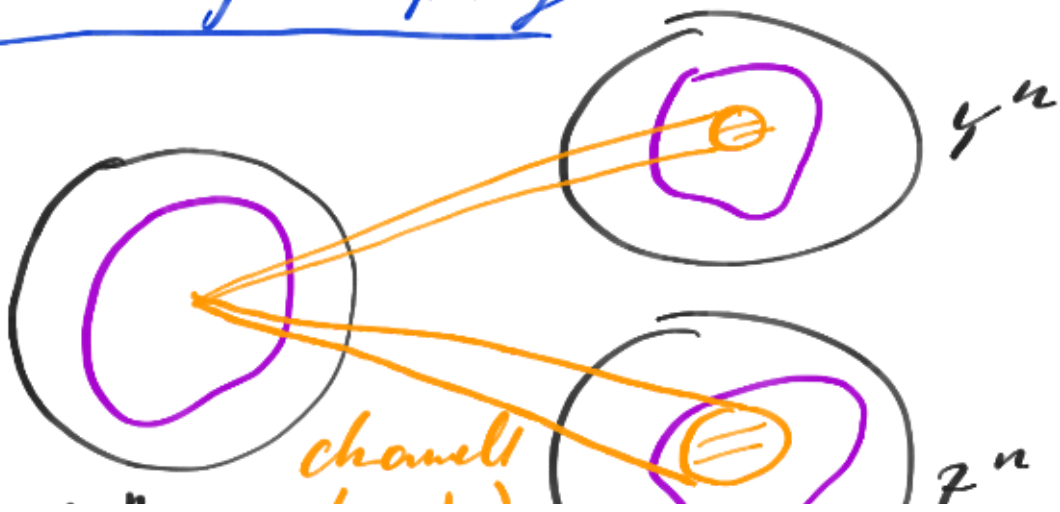
$$R = \lim_{n\to\infty}\left(\frac{n_s}{n}\right) \leq C_s = \max_{p(x)} [I(X:Y) - I(X:Z)]$$

SECRET CAPACITY

N.B.: only possible if

$\exists\, p(x)$ s.t.: $I(X:Y) > I(X:Z)$ (intuitive)

Intuition of the proof



X^n $p(y,z|x)$

note: $X \to Y$ must have larger capacity than $X \to Z$ vs.

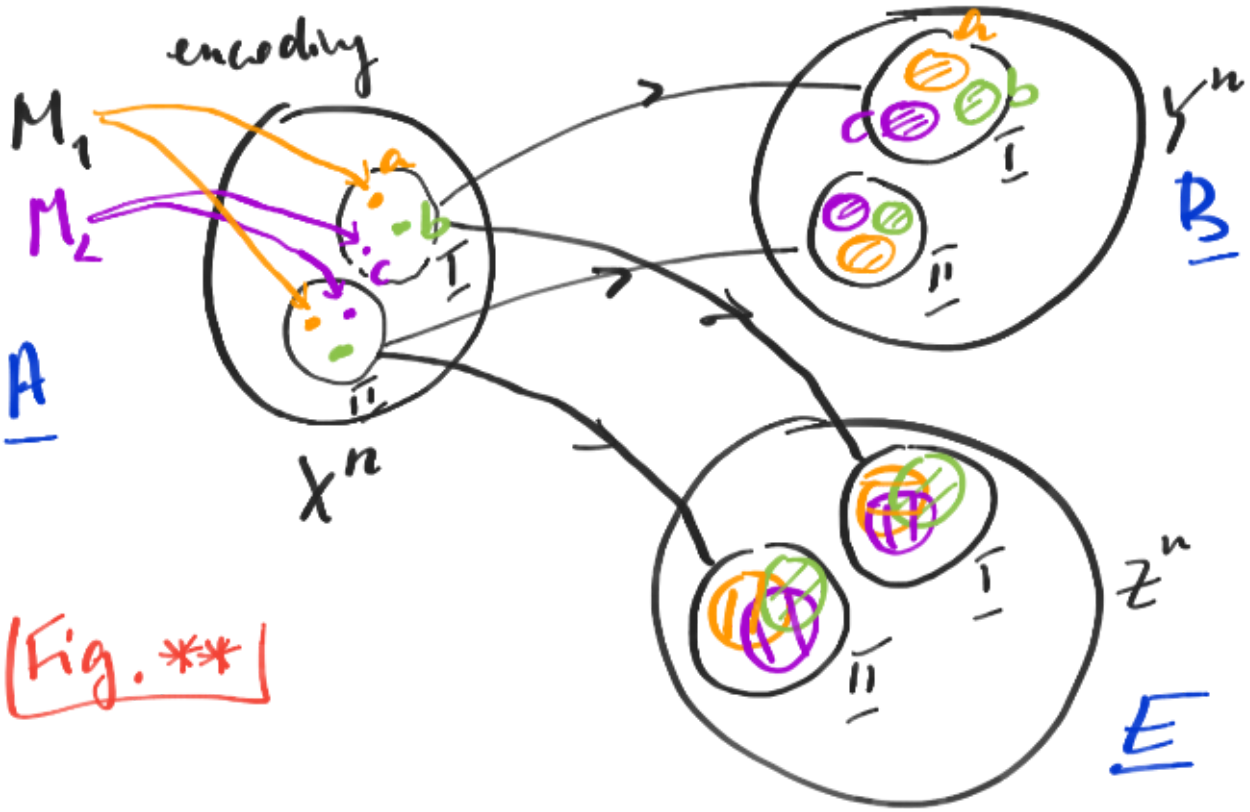


Fig. **

$\{a, b, c, \ldots\}$ → finer structure can be distinguished only by B.

$\{\bar{I}, \bar{II}, \ldots\}$ → coarser structure can still be distinguished by E.

How many messages can be encoded into the finer structure?

$2^{nI(X:Y)}$ ← # messages distinguishable for B

$2^{nI(X:Z)}$ ← # ——— " ——— for E

$$\alpha = 2^{n[I(X:Y)-I(X:Z)]}$$

Cryptography point of view

CKT ⇔ Result of A & B performing:

- error correction [EC]
- privacy amplification [PA]

Motivation:

EC – A & B want to communicate without errors

PA – A & B introduce additional randomness (hash functions) to reduce knowledge of E to zero!

Protocol: (IID! assumption)

A	X:	1	0	0	1	0	0	1	(more ≀)
B	Y:	1	0	1	1	1	0	1	≀ } errors
E	Z:	0	0	1	0	0	1	0	≀ } errors

MOTIVATION (single example)

EC → repetition code (send 3 bits)

encoding: M = 0 ⇝ X = 000

n = 12

X: 1 1 1 | 0 0 0 | 0 0 0 | 1 1 1

Ber. Y: 1 0 1 | 0 0 1 | 0 0 0 | 0 1 1

Z: 0 0 1 | 1 0 1 | 1 0 0 | 1 0 0

$P_{error}(Y) < 1/3$

$P_{error}(Z) > 1/3$

⇒ EC

X': 111 000 000 111

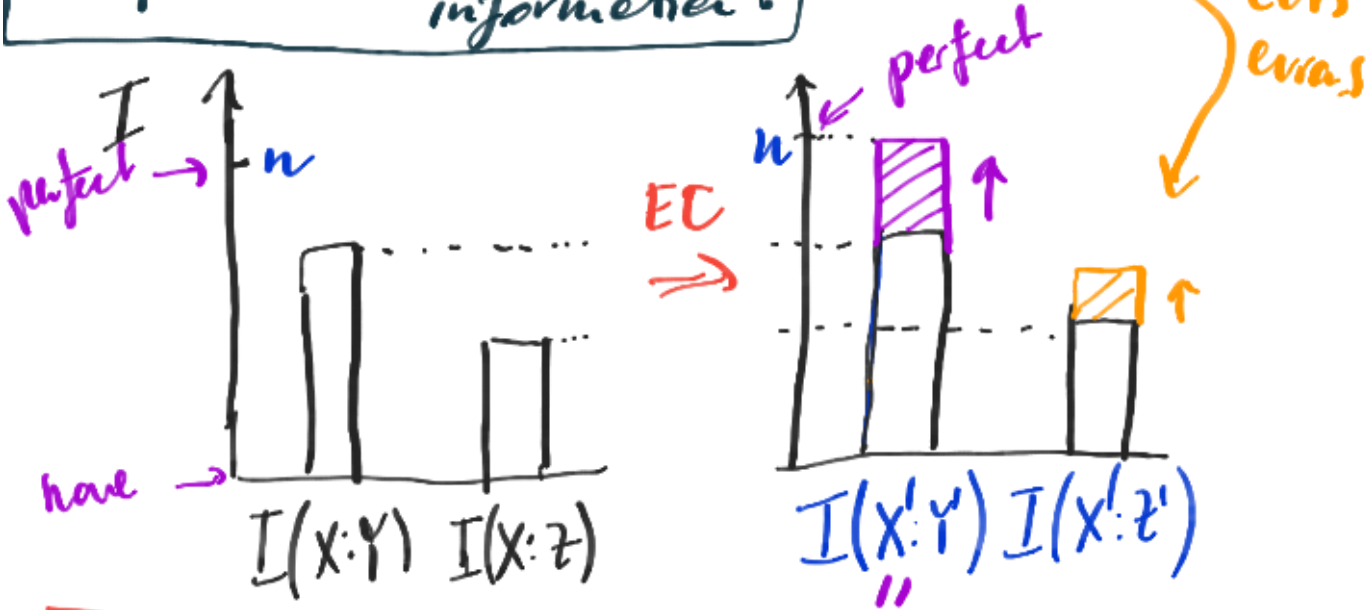
Our Y': 111 000 000 111

Our Z': 000 111 000 000

[take block majority and correct]

less errors

Impact on mutual information:



PA → ① A decides on random permutation and communicates it publicly

② A,B perform XOR op^{n} on every triplet a⊕b⊕c

Permutation: 1,4|2|3,6|5,8|7,10|9,12|11

① X': 111000000111

X'': 010101101010

Y'': 010101101010

Z'': 101000100000

#bits: $n = 12$

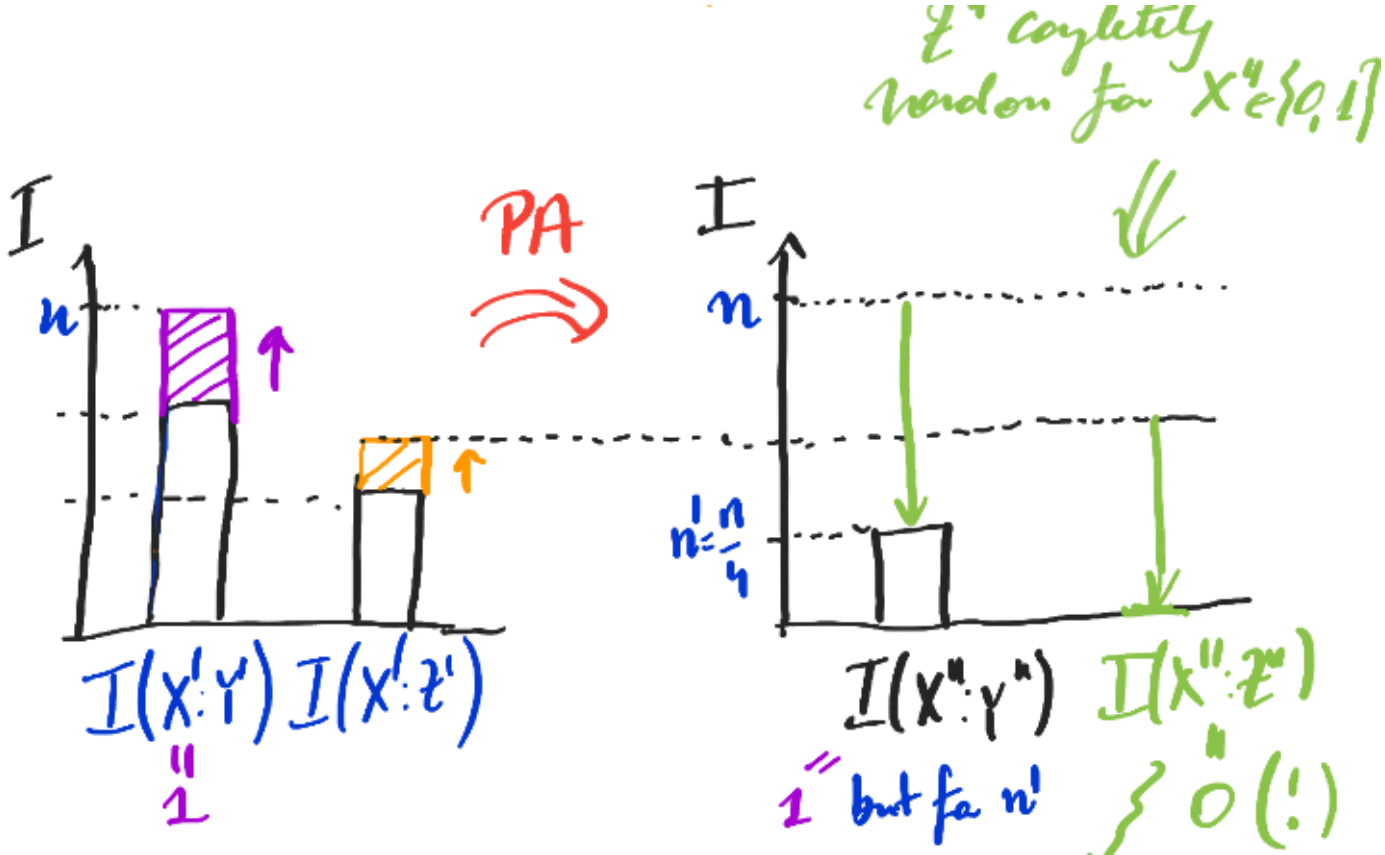
⇓ PA

#bits: $n' = 4$

② X'': 1 0 0 1

Y'': 1 0 0 1 ⇒ $I(X'':Y'')=1$

Z'': 0 0 1 0 ⇒ $I(X'':Z'')=0$



$\Rightarrow$ Ended up with secure!

$$R_S = \frac{n}{n'} = \frac{1}{4}$$

but how to attain (asymptotically)?

$$R_S = \lim_{n\to\infty}\left(\frac{n}{n'}\right) \leq I(X:Y) - I(X:Z)$$

?? "=" ??

EC & PA IN PRACTISE

EC Interactive protocol

1. 1) As & Bs apply same random perm.

(one-way communication $A \to B$)

2) A & B divide their n bits into blocks of length "b".

$n = k \cdot b$ ← block-size

k: # blocks

b:
Such that very little probability > 1 error in a single block.

3) Check parity in each block and communicate (one-way $A \to B$)
⇒ if disagree then bisection {binary search}

⇒ until the error is corrected !

⋮

... over all blocks until all parities agree.

4) Change block-size $b' = b + 1$

⋮

5) until $b = \frac{n}{2}$.

2. Repeat ν times with different random permutations

⇒ probability of obtaining errorless bitstring after

ν bits:

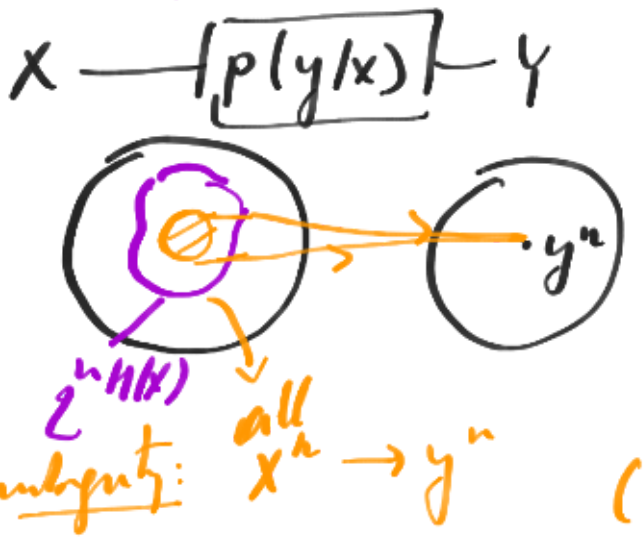
$$P_{\text{"no errors"}} = 1 - 2^{-\nu}$$

$\Rightarrow$ enough to choose eg. $\nu \simeq 20$, $P = 1 - 10^{-6}$

NB. After EC Eve has information that no longer can be regarded as IID $\Rightarrow$ parity checks have introduced correlations between bits.

OK, but how many bits at least must be communicated to correct all the errors?
$\Rightarrow$ Shannon limit!

$I(A:B) := I(X^n : Y^n) = n\, I(X:Y)$ {i.i.d.}



$\#X^n = 2^{nH(X|Y)}$

given Y, what is the randomness in X (how many yield Y=y on aver.?)

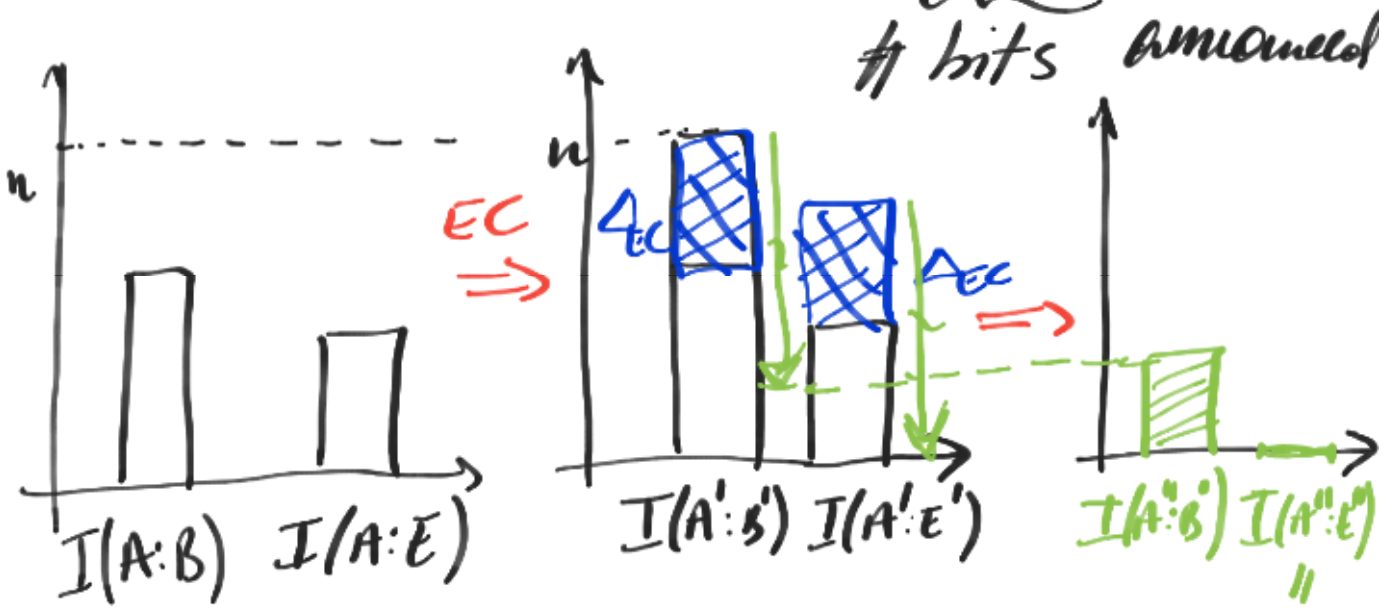
Shannon limit to EC: # bits $= nH(X|Y) = n[H(X) - I(X:Y)]$

Write a program which would allow to verify the efficiency of the above protocol with the Shannon Limit on EC!

- After EC n errorless bits between A:B but the information also given to Eve!!!

$$I(A':E') \leq n\, I(X:Z) + \Delta_{EC}$$

Δ_{EC}: # bits announced



PA ⇒ hashing functions

"Hashing" ⇒ shrink the number of bits to:

$n' = n - I(A':E')$, so that {errors (spread)} of E are uniformly distributed and $I(A'':E'') = 0$, ✓

then:

$$n' = n - [n\, I(X:Z) + n(1 - I(X:Y))]$$
$$= n(I(X:Y) - I(X:Z))$$

CLT

Example:

Random Toeplitz Matrix

$\forall_a : T_{i+a,j+a} = T_{i,j}$

$$\begin{bmatrix} t_1 & t_2 & t_3 & \cdots & t_{n-1} & t_n \\ \tilde{t}_1 & t_1 & t_2 & \ddots & & t_{n-1} \\ \tilde{t}_2 & \ddots & \ddots & \ddots & & \\ \tilde{t}_{m'} & \tilde{t}_2 & t_1 & t_2 & \cdots & t_{n-m'+1} \end{bmatrix}$$

with binary entries $\forall_i : t_i, \tilde{t}_i \in \{0,1\}$

e.g. $3 \to 2$

$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} t_1 & t_2 & t_3 \\ \tilde{t}_1 & t_1 & t_2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} x_1 t_2 \oplus x_2 t_2 \oplus x_3 t_3 \\ x_1 \tilde{t}_1 \oplus x_2 t_1 \oplus x_3 t_2 \end{bmatrix}$$

$$\mathbb{E}[y_1] = \sum_{t_1, \tilde{t}_1} p(t_1, \tilde{t}_1, \ldots) [T\,x]_1 = \tfrac{1}{2}(x_1 \oplus x_2 \oplus x_3)$$

changes if any x_1, x_2, x_3 flipped.

Ⓐ But what about the probability of collision

$\Pr[h(x) = h(x')] = \frac{1}{2^{m'}}$ for universal hashing

N.B.

CLT applies either $A \to B$ or $B \to A$ "one-way" communication:

$$C_S = \max_{p(x)} \max \{ I(X:Y) - I(X:Z),\ I(X:Y) - I(Y:Z) \}$$

(encodings)

ECsPA is done by A or B

$\Rightarrow$ A & B may agree whether it is better to do $A \to B$ or $B \to A$ as they know the form of the channel: $p(y, z|x)$

Last modified: 18:31