ADVANCED INFORMATION, COMPUTATION, COMMUNICATION II

Prof. M. Gastpar

Slides by Prof. M. Gastpar and Prof. em. B. Rimoldi

EPFL

Spring Semester 2025— *Slides Version 1.0*

Outline

AICC-I

- **Computation**
- Algorithms
- Discrete Structures

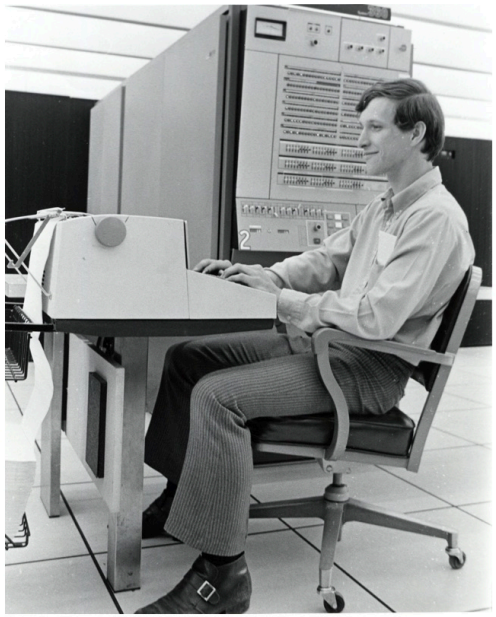
AICC-I

- **Computation**
- Algorithms
- Discrete Structures

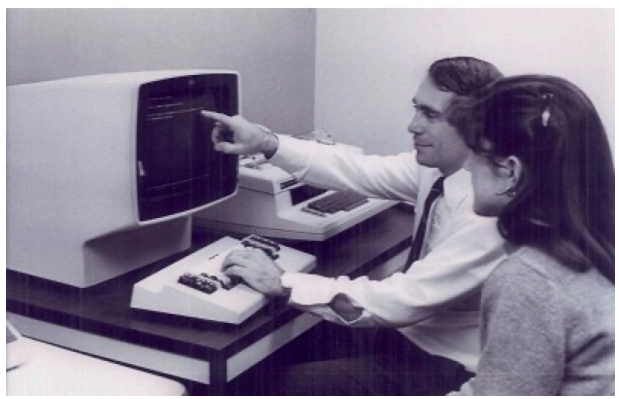
But to have interesting computations, we need data!

AICC-I

- **Computation**
- Algorithms
- Discrete Structures

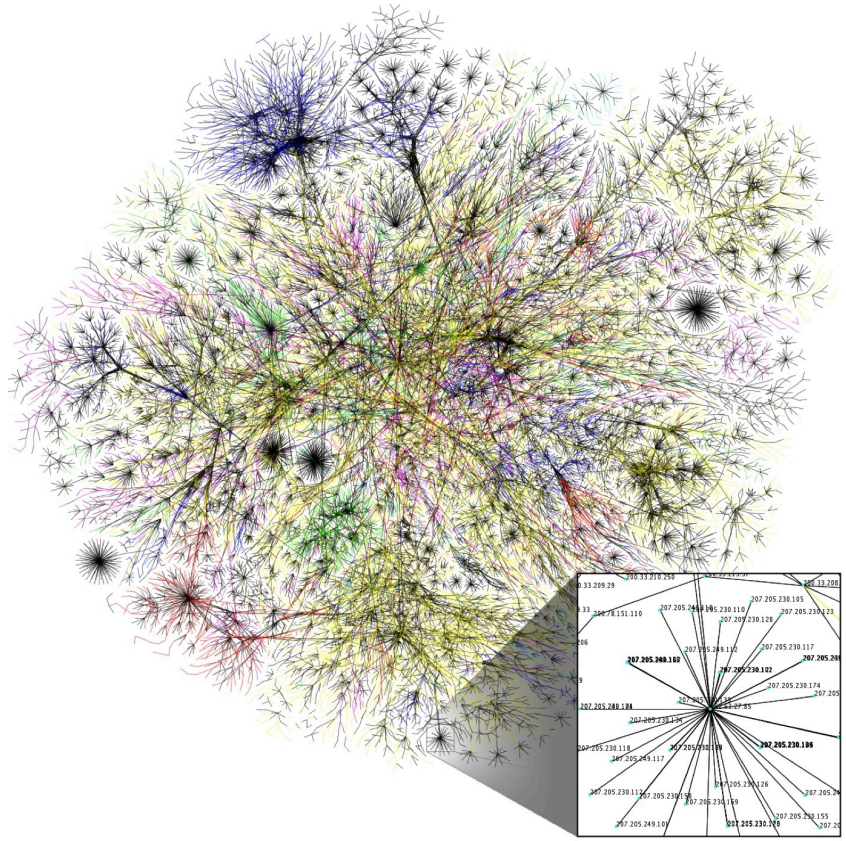


ca. 1980



AICC-I

- **Computation**
- Algorithms
- Discrete Structures



From The Opte Project

AICC-I

- **Computation**
- Algorithms
- Discrete Structures

AICC-II

- **Communication**
- Information and Data Science
- Cryptography, Secrecy, Privacy

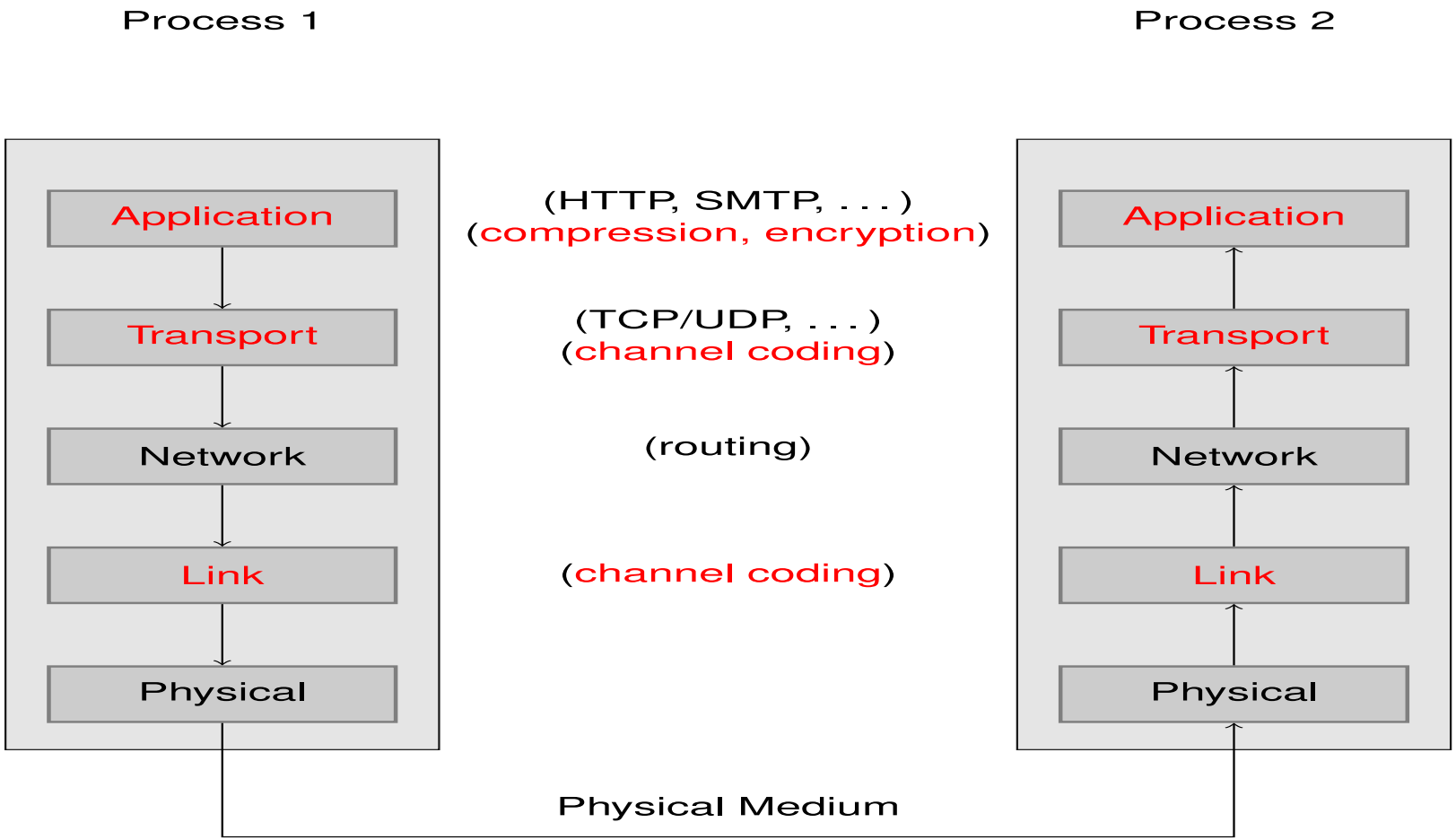
WE STUDY: SOURCE CODING, CRYPTOGRAPHY, CHANNEL CODING

Why these topics?

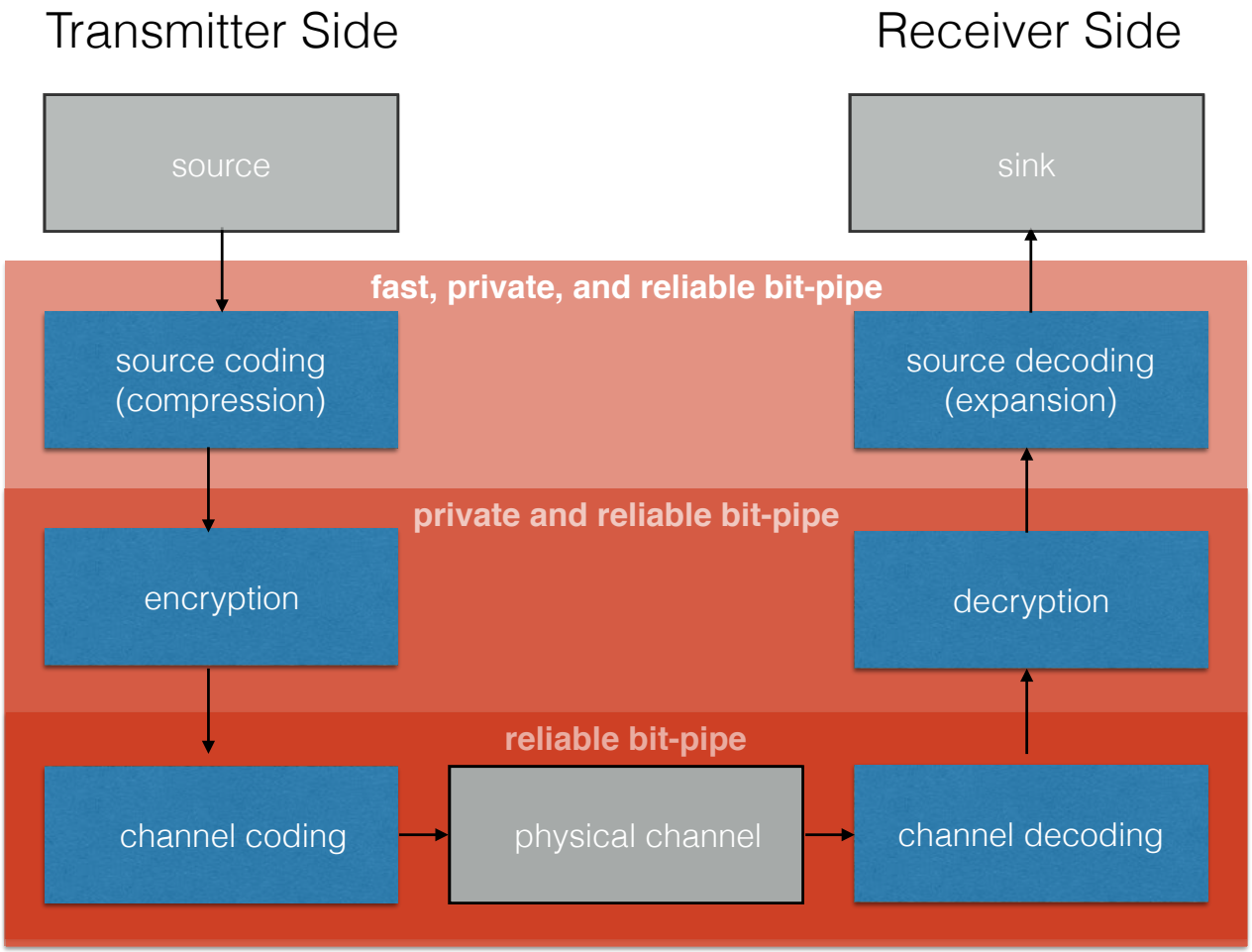
- important building blocks of communication systems
- non-evident topics and the results are often surprising
- intimately related to fundamental concepts (probability theory, linear algebra, number theory)
- have a common root: the notion of entropy
- require/promote rigorous thinking

Digital Communication: The "Big Picture"

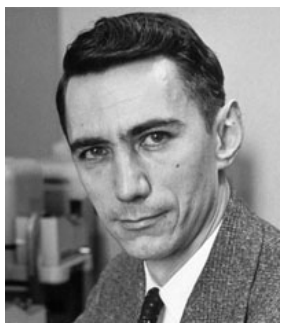
Communication over the Internet



POINT-TO-POINT COMMUNICATION SYSTEM

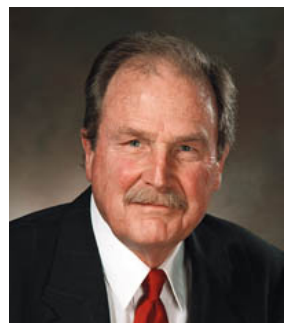


We will rely on **discrete probability theory** and on the work of various people including:



Shannon

Fano



Huffman

SOURCE CODING

1) ENTROPY

$$H_D(S) = -\sum_S p(s) \log_D p(s)$$

$$0 \leq H_D(S^+) \leq \log_D |S|$$

SOURCE CODING

1) ENTROPY

$$H(S) = -\sum_{s} p(s) \log p(s)$$

$$0 \leq H(S) \leq \log |S|$$

2) ENTROPY CONDITIONED ON AN EVENT

$$H(S|Y=y) = -\sum_{s} p(s|Y=y) \log p(s|Y=y)$$

3) CONDITIONAL ENTROPY

$$H(S|Y) = \sum_y p(y)\, H(S|Y=y)$$

$$= -\sum_{s,y} p(s,y) \log p(s|y)$$

3) CONDITIONAL ENTROPY

$$H(S|Y) = \sum_y p(y)\, H(S|Y=y)$$

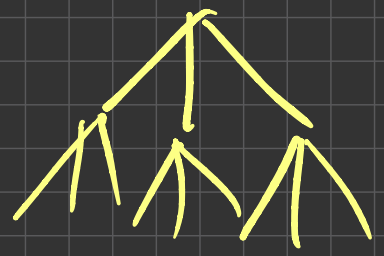
$$= -\sum_{s,y} p(s,y) \log p(s|y)$$

TWO KEY THEOREMS

$$H(S|Y) \leq H(S)$$

$$H(S_1, S_2) = H(S_1) + H(S_2|S_1)$$

4) SOURCE CODING



"UNIQUELY DECODABLE"

"PREFIX-FREE" $\longrightarrow$ **TREE**

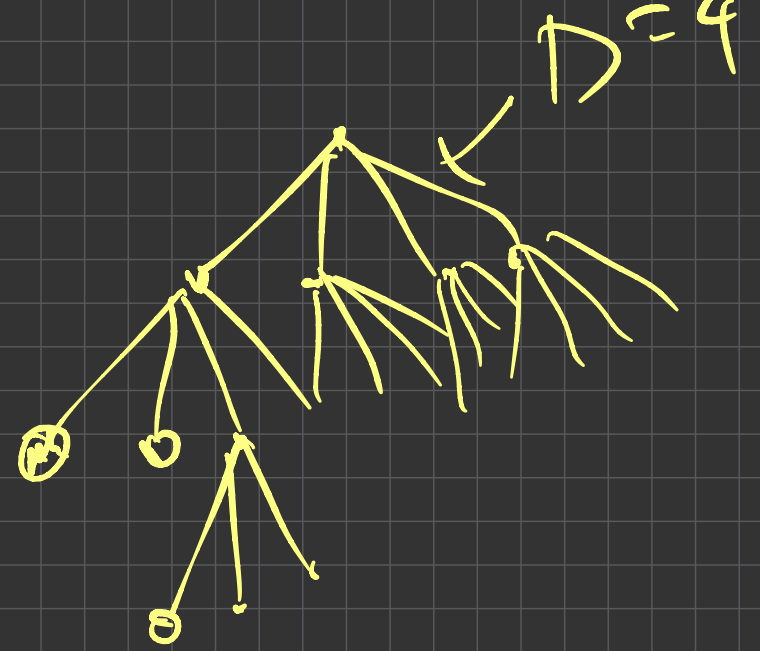
SOURCE ALPHABET $\mathcal{A}$.

$\mathcal{A}$	$\Gamma(s)$	length
a	010	$\ell(a) = 3$
b	0212	$\ell(b) = 4$
c	1210	$\ell(c) = 4$
d		$\vdots$
e		

MAIN THEOREMS:

- There exists a uniquely decodable code with lengths $\{\ell_1, \ell_2, \ldots\}$ <u>if and only if</u> there exists a prefix-free code with the same lengths.

- $$\sum_{s \in A} D^{-\ell(s)} \leq 1$$



SOURCE MODELS:

- 1D SOURCE

SOURCE MODELS:

- IID SOURCE

SHANNON-FANO CODE:

$$\ell(s) = \lceil -\log_D p(s) \rceil$$

SOURCE MODELS:

- IID SOURCE

SHANNON-FANO CODE:

$$\ell(s) = \lceil -\log p(s) \rceil$$

HUFFMAN CODE CONSTRUCTION.

→ IS <u>OPTIMAL</u>.

SOURCE MODELS:

- IID SOURCE

SHANNON-FANO CODE:

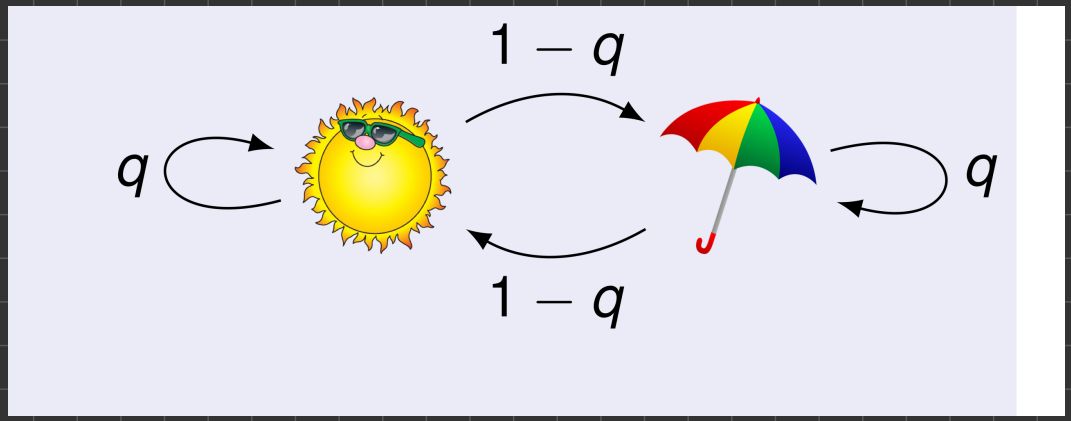
$$\ell(s) = \lceil -\log p(s) \rceil$$

HUFFMAN CODE CONSTRUCTION.

→ IS <u>OPTIMAL</u>.

$$H_D(S) \leq L(S, \Gamma) \leq H_D(S) + 1$$

- "SUNNY – RAINY"



$$H(S_i \mid S_{i-1}, S_{i-2}, \ldots)$$
$$= H(S_i \mid S_{i-1})$$
$$= h_b(q)$$

CROSS-ENTROPY Loss.

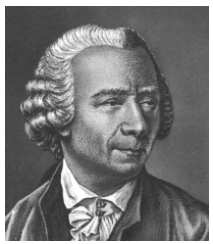
$$L(p(y), q(y)) = -\sum_y p(y) \log q(y)$$

$$\min_{q(y) \in Q} L(p(y), q(y))$$

↑ FOR EXAMPLE, DISTRIBUTIONS THAT CAN BE REPRESENTED BY NEURAL NETS.

Second Topic: Cryptography

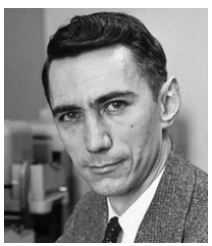
We will rely on **number theory**



Euler

Fermat

as well as on **group theory** and on the work of various people including:



Shannon

Clifford Cocks

Rivest, Shamir, Adleman

1) ONE-TIME PAD.

PLAINTEXT t , $t \in \{0,1\}^n$

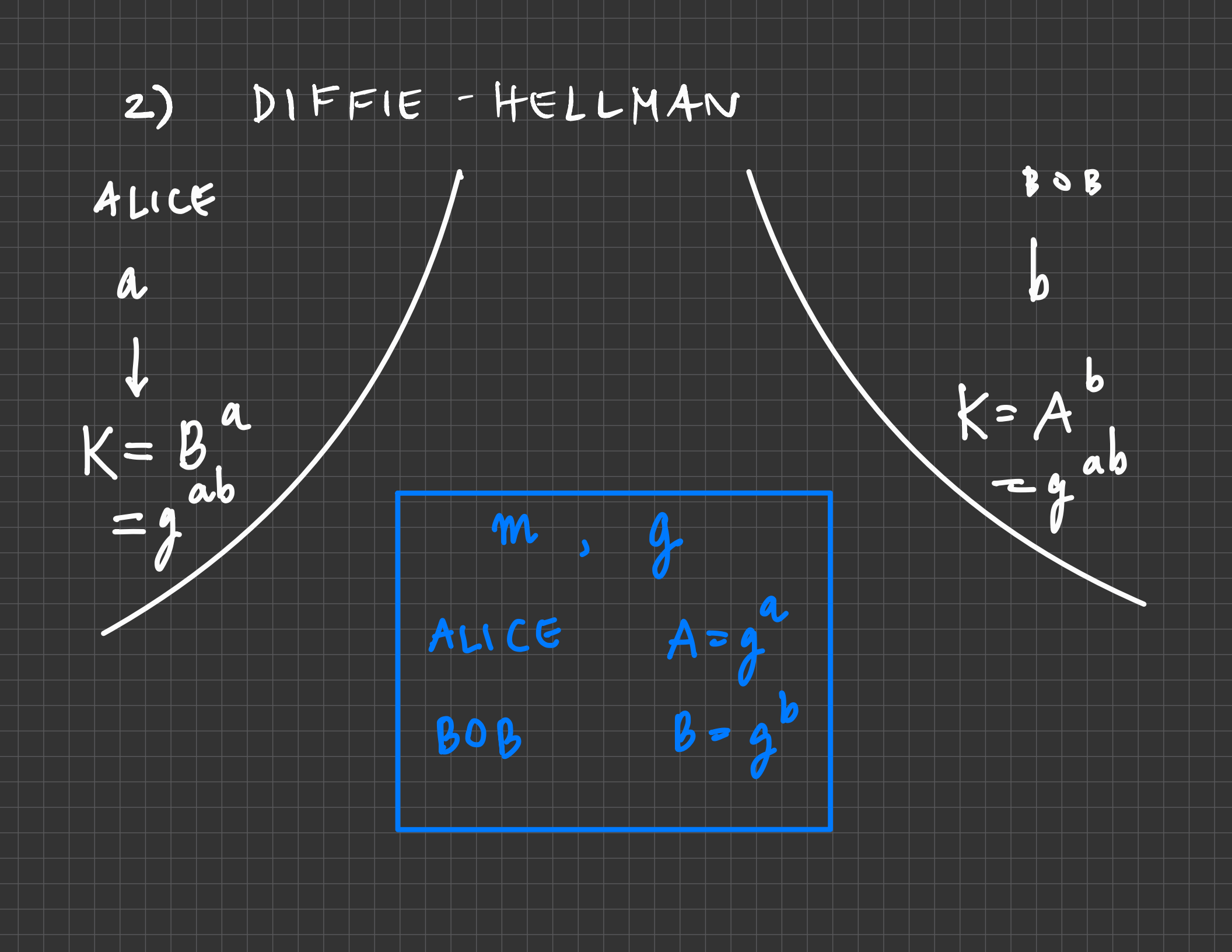
KEY k , $k \in \{0,1\}^n$

$\uparrow$ IID uniform bits

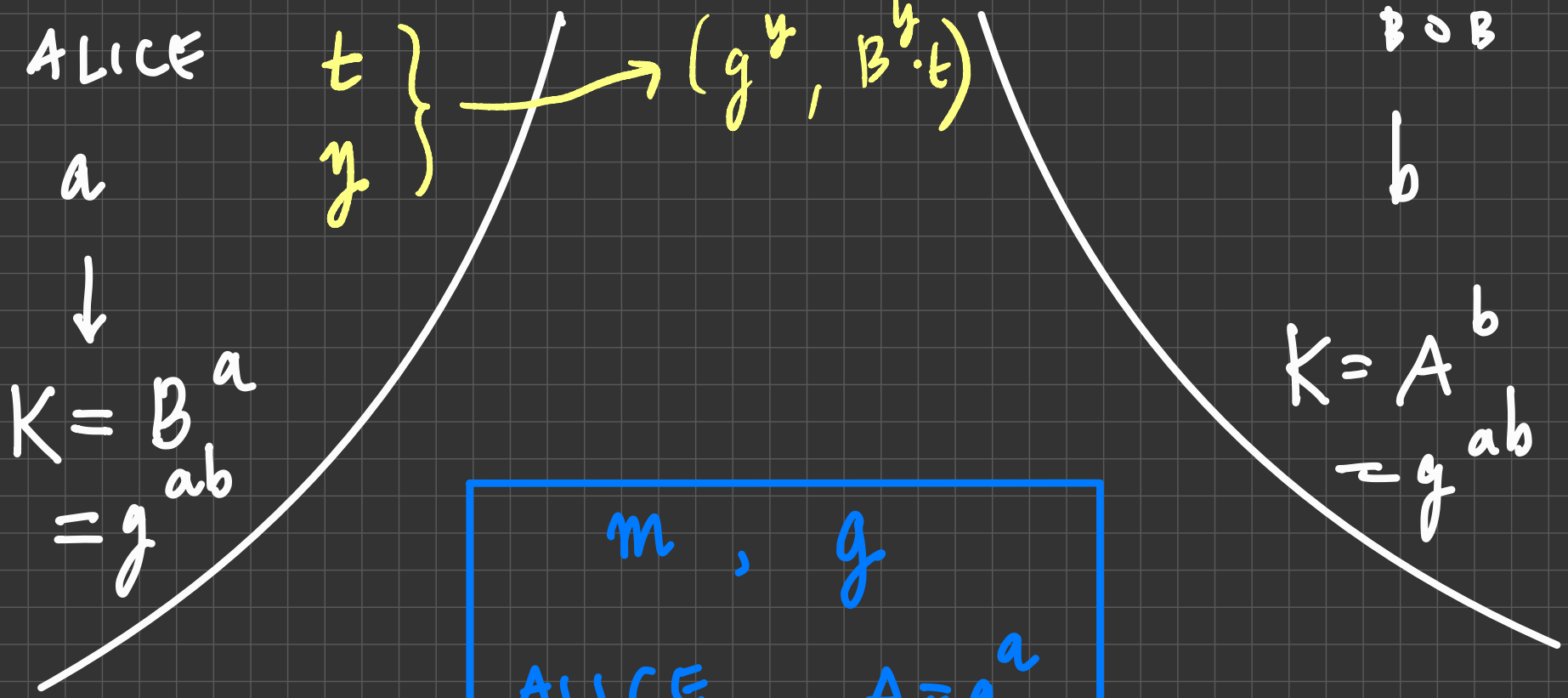
CYPHERTEXT $c = t \oplus k$

THIS IS PERFECTLY SECURE.

2) DIFFIE - HELLMAN



EL GAMAL



m , g

ALICE $A = g^a$

BOB $B = g^b$

3) TOOLBOX

- MODULO - m

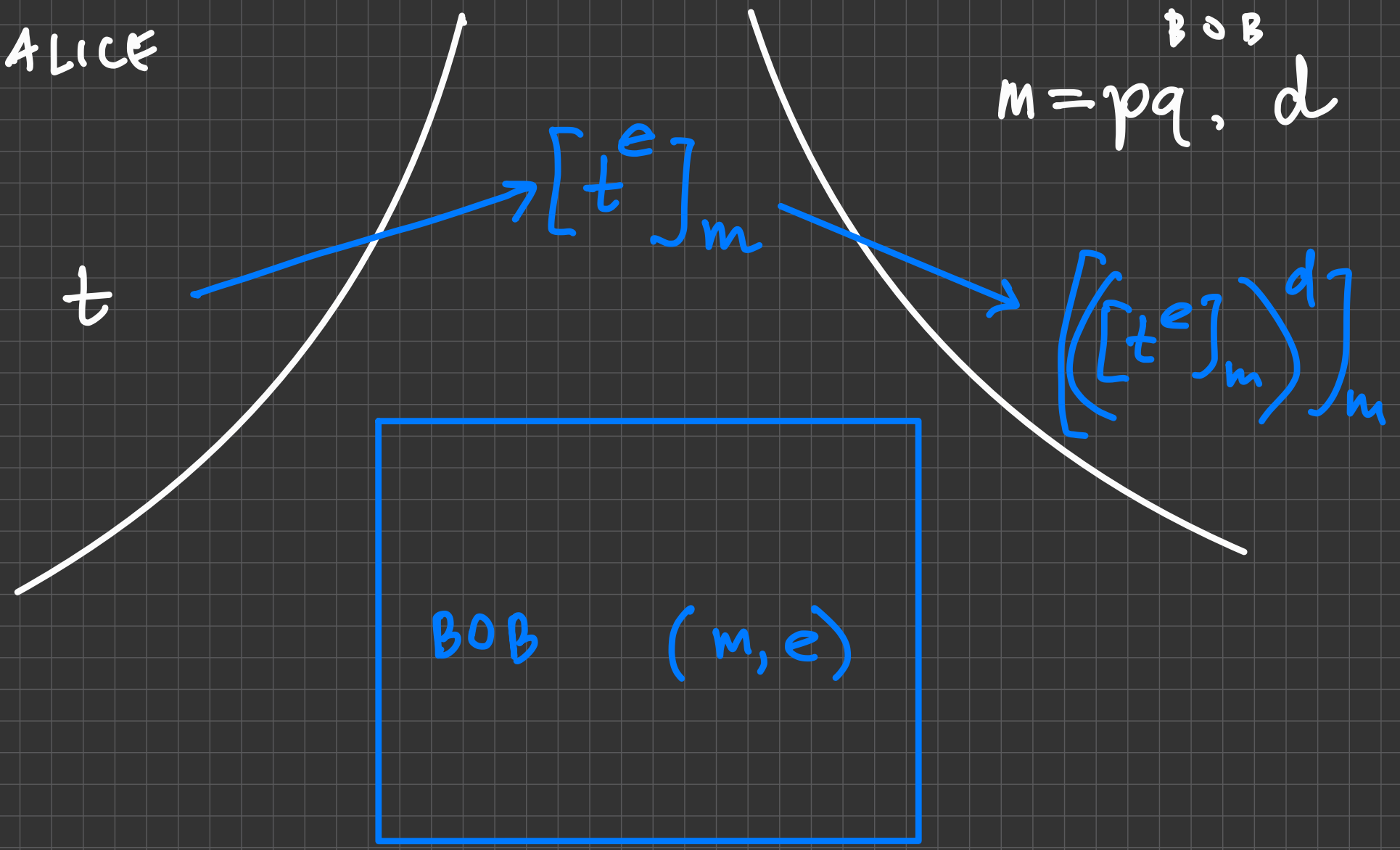
3) TOOLBOX

- MODULO - m
- GROUP $(G, *)$
  - → every element has a unique inverse (w.r.t. $*$)
  - → order of group elements
    - ↳ Lagrange.
- PRODUCT GROUP $(G_1, *_1) \times (G_2, *_2)$

3) TOOLBOX

- MODULO - m
- GROUP $(G, *)$
  - → every element has a unique inverse (w.r.t. $*$)
  - → order of group elements
    - ↳ Lagrange.
- PRODUCT GROUP $(G_1, *_1) \times (G_2, *_2)$
- THE SPECIAL ISOMORPHISM BETWEEN $\mathbb{Z}/m_1 m_2 \mathbb{Z}$ and $\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$
  - ↳ REMAINDER THEOREM.

4) RSA

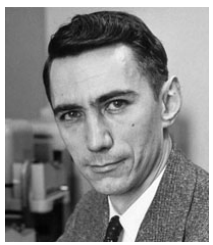


THIRD TOPIC: CHANNEL CODING

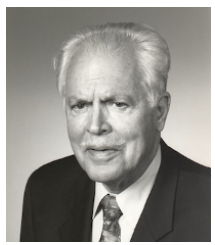
We will rely on **finite fields**

Galois

as well as on **linear algebra** and on the work of various people including:



Shannon

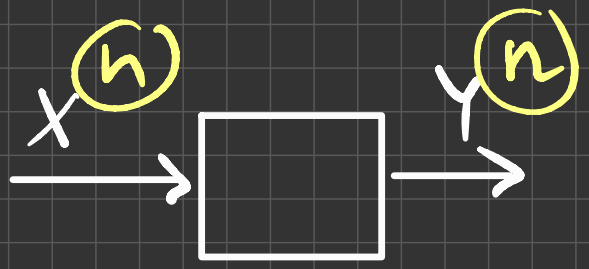


Reed

Solomon

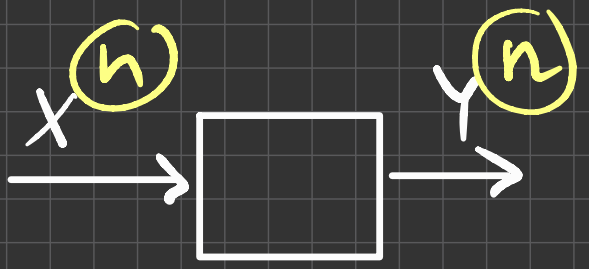
1) CHANNEL MODELING

- ERROR CHANNEL
- ERASURE CHANNEL



1) CHANNEL MODELING

- ERROR CHANNEL
- ERASURE CHANNEL



2) CHANNEL CODING

COULD SEND ANY X^n,

BUT WE RESTRICT TO A SUBSET.

$$\mathcal{C} = \{ \vec{c}_1, \vec{c}_2, \ldots \vec{c}_M \}$$

3) CHANNEL DECODING.

PROPOSAL: MINIMUM DISTANCE.

$$\min_{\vec{c} \in \mathcal{C}} d(\vec{c}, \vec{y})$$

Hence, we are interested in

$$d_{min}(\mathcal{C})$$

SINGLETON:

$$d_{min}(\mathcal{C}) \leq n - k + 1.$$

4) LINEAR CODES. $\mathbb{F}^n$

$$\vec{c} = \vec{u} G$$

↑ ranges over all of $\mathbb{F}^k$, $k \le n$

$$d_{min}(C) = \min_{\vec{c} \neq 0} w(\vec{c})$$

Parity check view:

$$C = \{ \vec{c} : \vec{c} H^T = \vec{0} \}$$

Syndrome $\vec{s} = \vec{y} H^T$

can be used to decode:

$$\vec{x} = \vec{f}(\vec{s})$$

↑ lookup table

5) REED-SOLOMON CODES.

$$\left(p_{\vec{u}}(a_1), p_{\vec{u}}(a_2), \dots, p_{\vec{u}}(a_n) \right)$$

over <u>all</u> polynomials $p_{\vec{u}}(x)$

with $\text{degree}\left(p_{\vec{u}}(x)\right) \leq k-1.$

WHAT'S NEXT

SECOND YEAR

COM-202 SIGNAL PROCESSING

CS-202 COMPUTER SYSTEMS

MATH-232 PROBABILITY & STATISTICS

CS-233 INTRO TO ML

THIRD YEAR

COM-300 STOCHASTIC MODELS

COM-301 COMPUTER SECURITY

COM-302 PRINCIPLES OF DIGITAL COMMUNICATIONS

COM-309 QUANTUM INFORMATION PROCESSING

MATH-310 ALGEBRA

MS PROGRAM

COM-401 CRYPTO & SECURITY

COM-404 INFORMATION THEORY & CODING

COM-406 FOUNDATIONS OF DATA SCIENCE

and many more ... !