Information Theoretic Cryptography

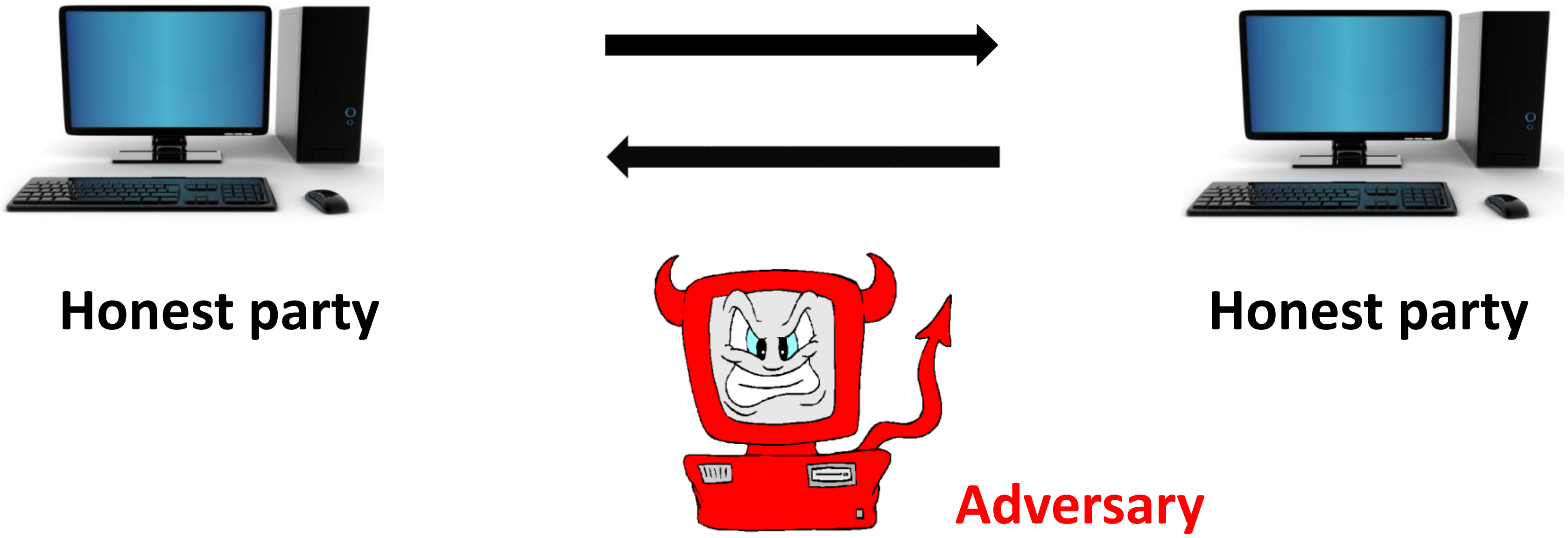
Introduction

Benny Applebaum
Tel Aviv University

BIU Winter-School of Information-Theoretic Cryptography
February 2020

Cryptography

Communication and Computation
in the presence of adversary



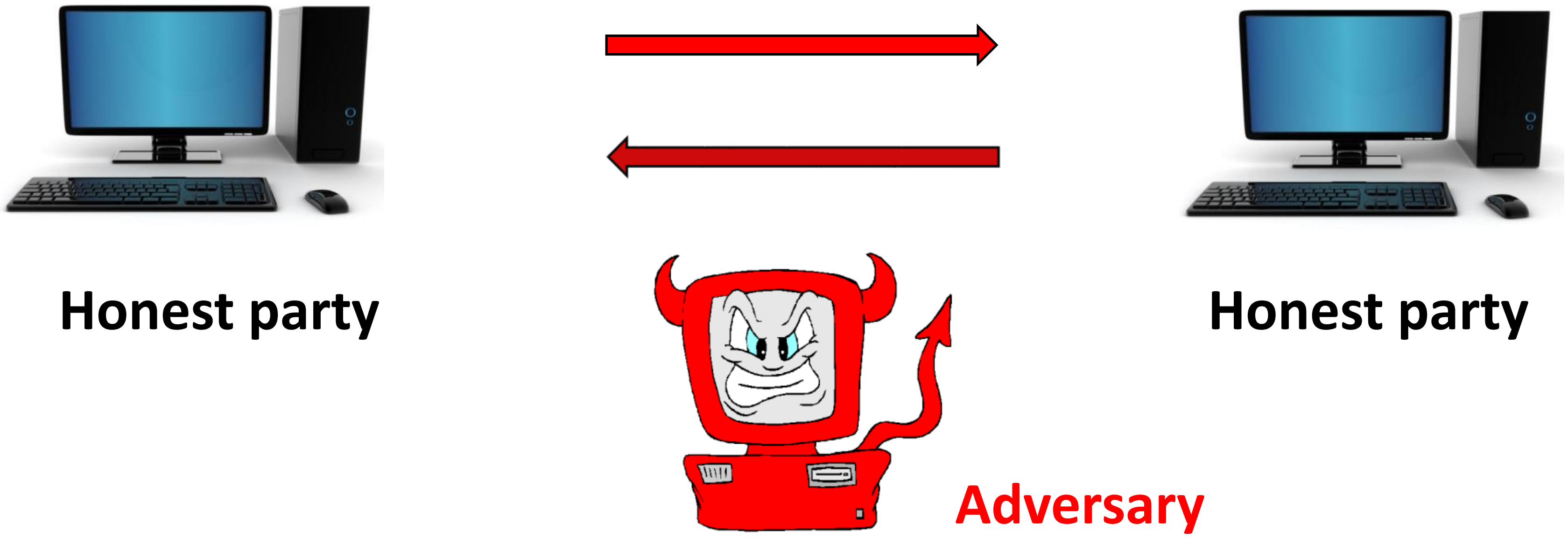
Honest party

Honest party

Adversary

Cryptography

- Encryption
- Authentication



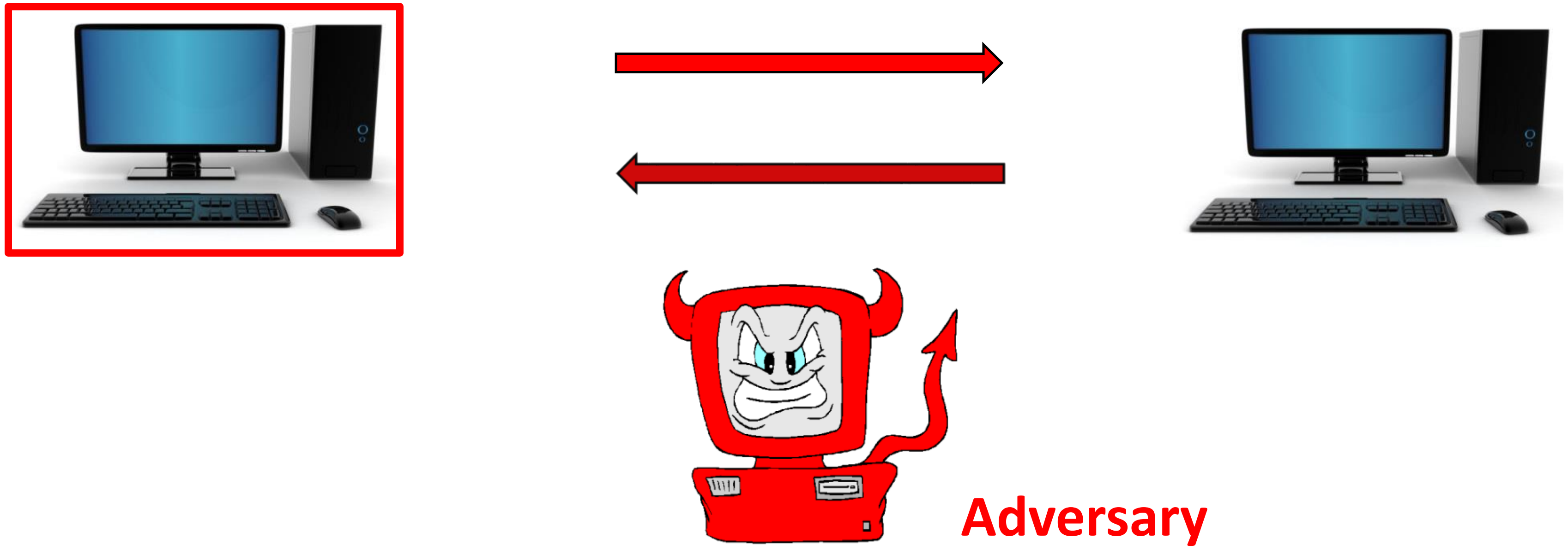
Honest party

Honest party

Adversary

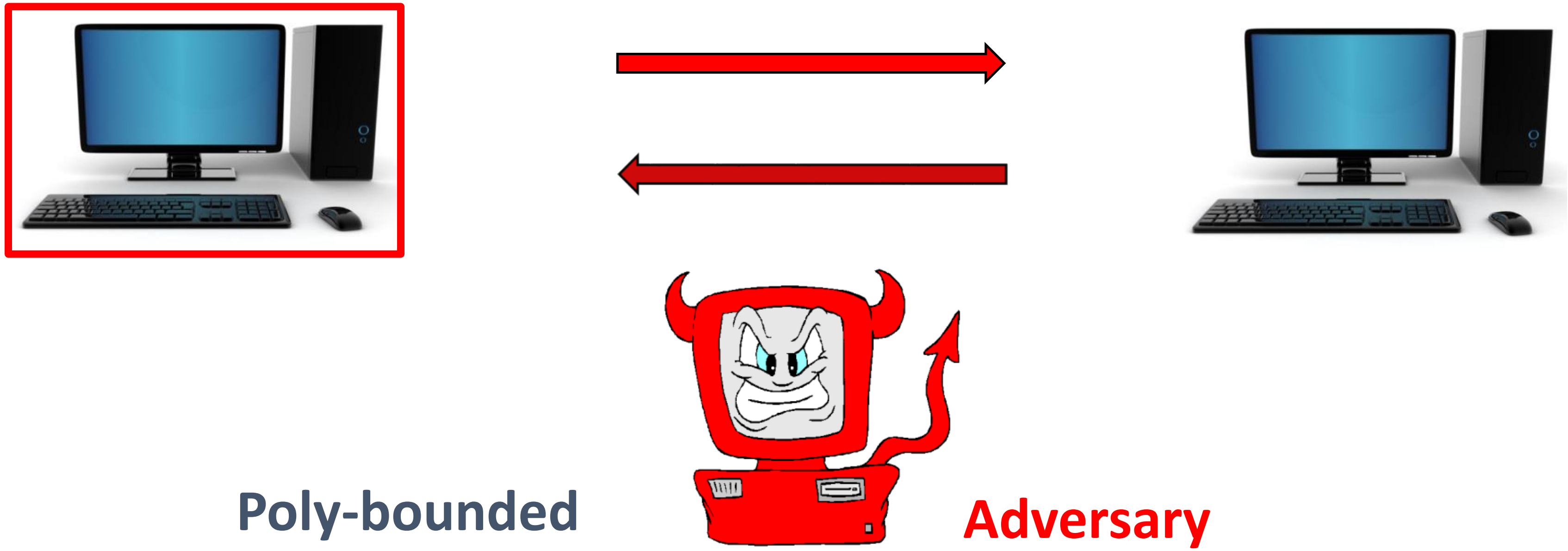
Cryptography

- Commitments
- Coin Tossing
- ZK-Proofs
- Secure Computation



Computational Cryptography

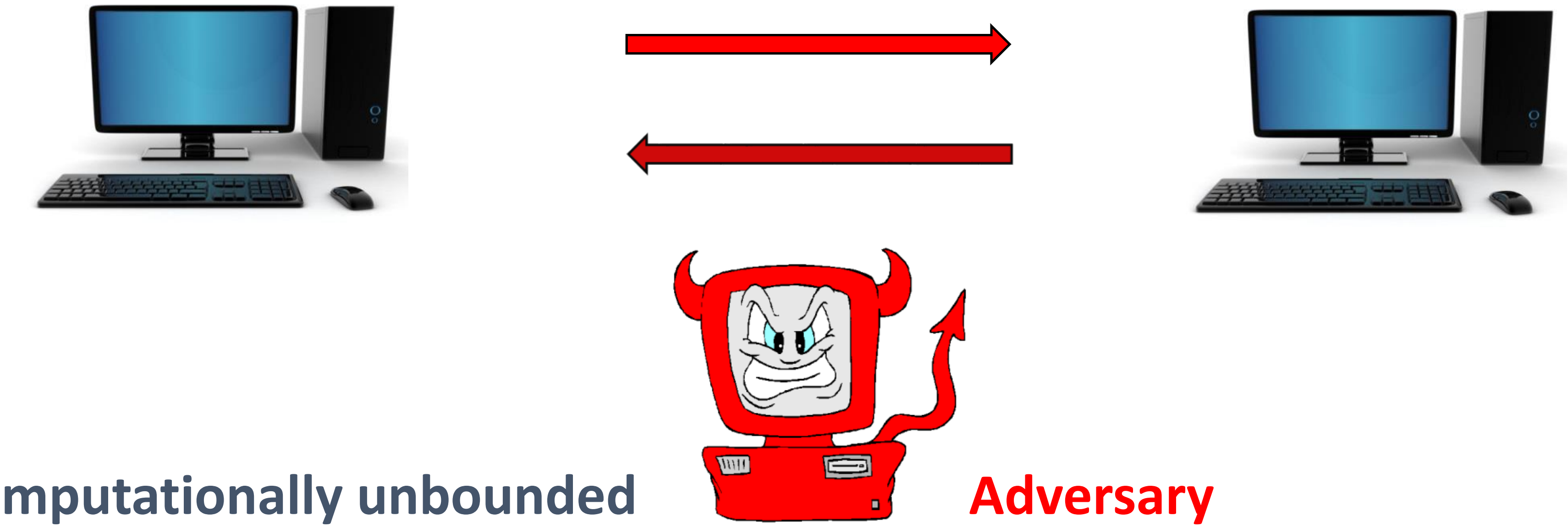
Exploit **computational limitation** to achieve privacy/authenticity/…



Poly-bounded **Adversary**

Information-Theoretic Cryptography

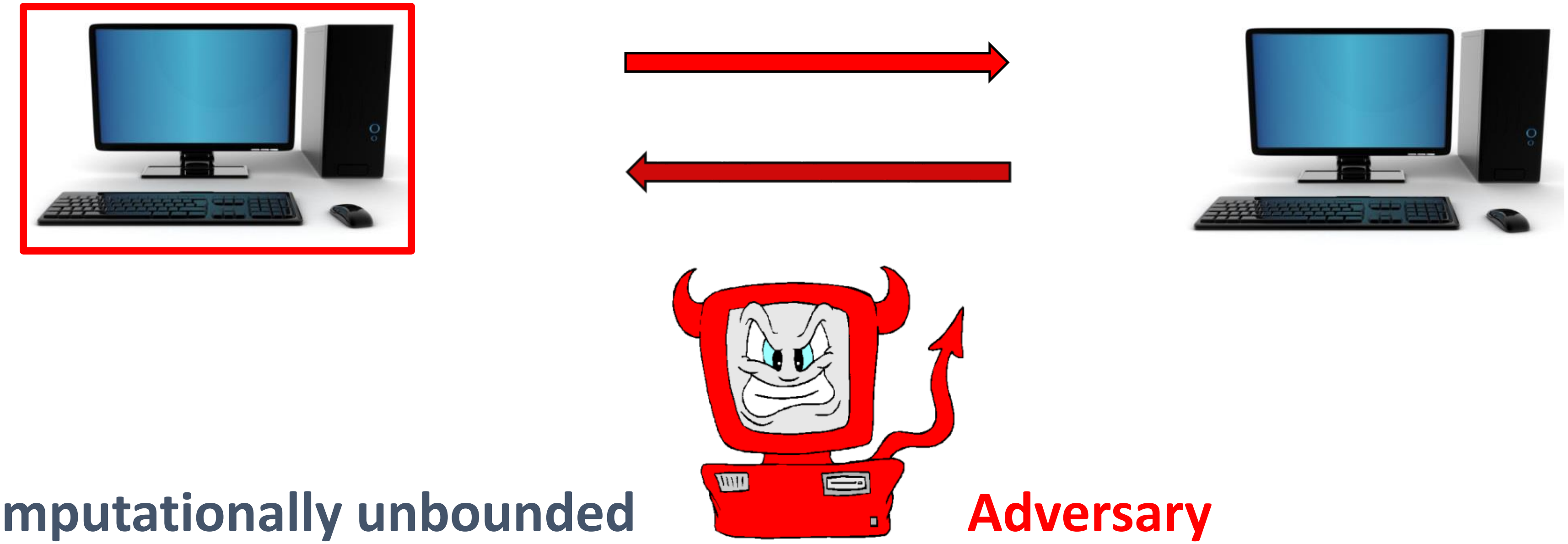
Exploit **information gaps** to achieve privacy/authenticity/…



Computationally unbounded **Adversary**

Information-Theoretic Cryptography

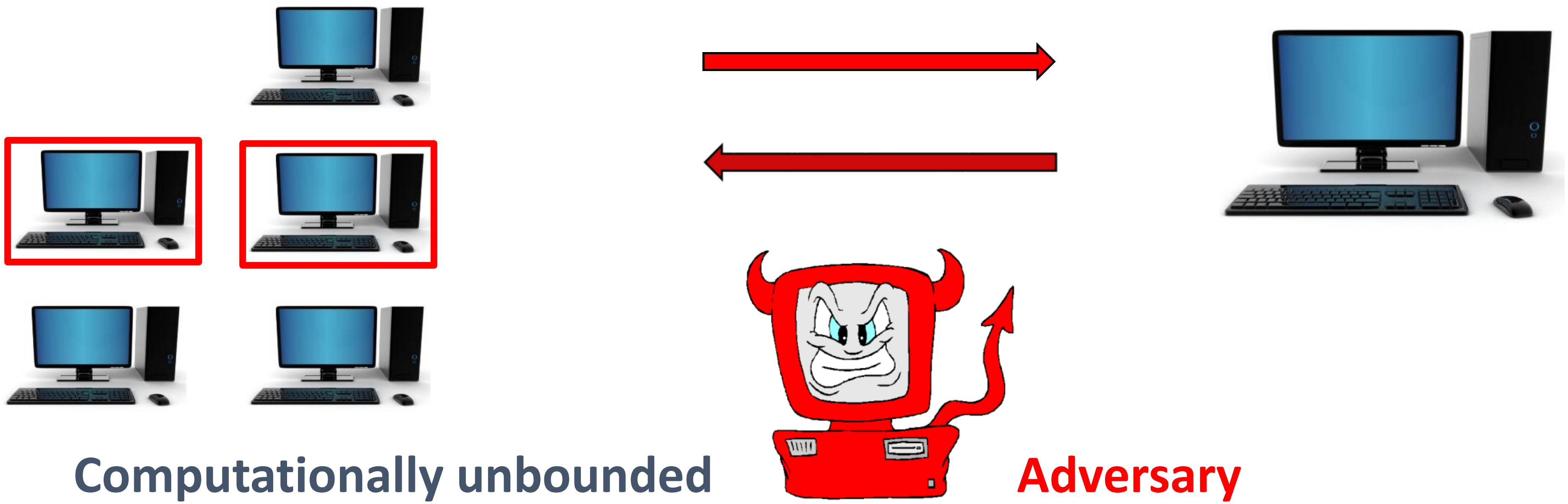
Exploit **information gaps** to achieve privacy/authenticity/…



Computationally unbounded **Adversary**

Information-Theoretic Cryptography

Exploit **information gaps** to achieve privacy/authenticity/…



Computationally unbounded **Adversary**

(Shallow) Comparison

Computational Cryptography	**IT Cryptography**
Comp-limited adversary	Comp-unbounded adversary
Unproven assumptions	Unconditional (no assumptions)
Composability issues	Good closure properties
Complicated def’s	Easy to define and work with (concretely)
Allows magic (PRG/PKC/OT/)	No magic (useless w/o information gaps)
Short keys	Long keys/large communication
May be comp. expensive	Typically fast (for short messages)

The Crypto Tower

Assumption

Obfustopia

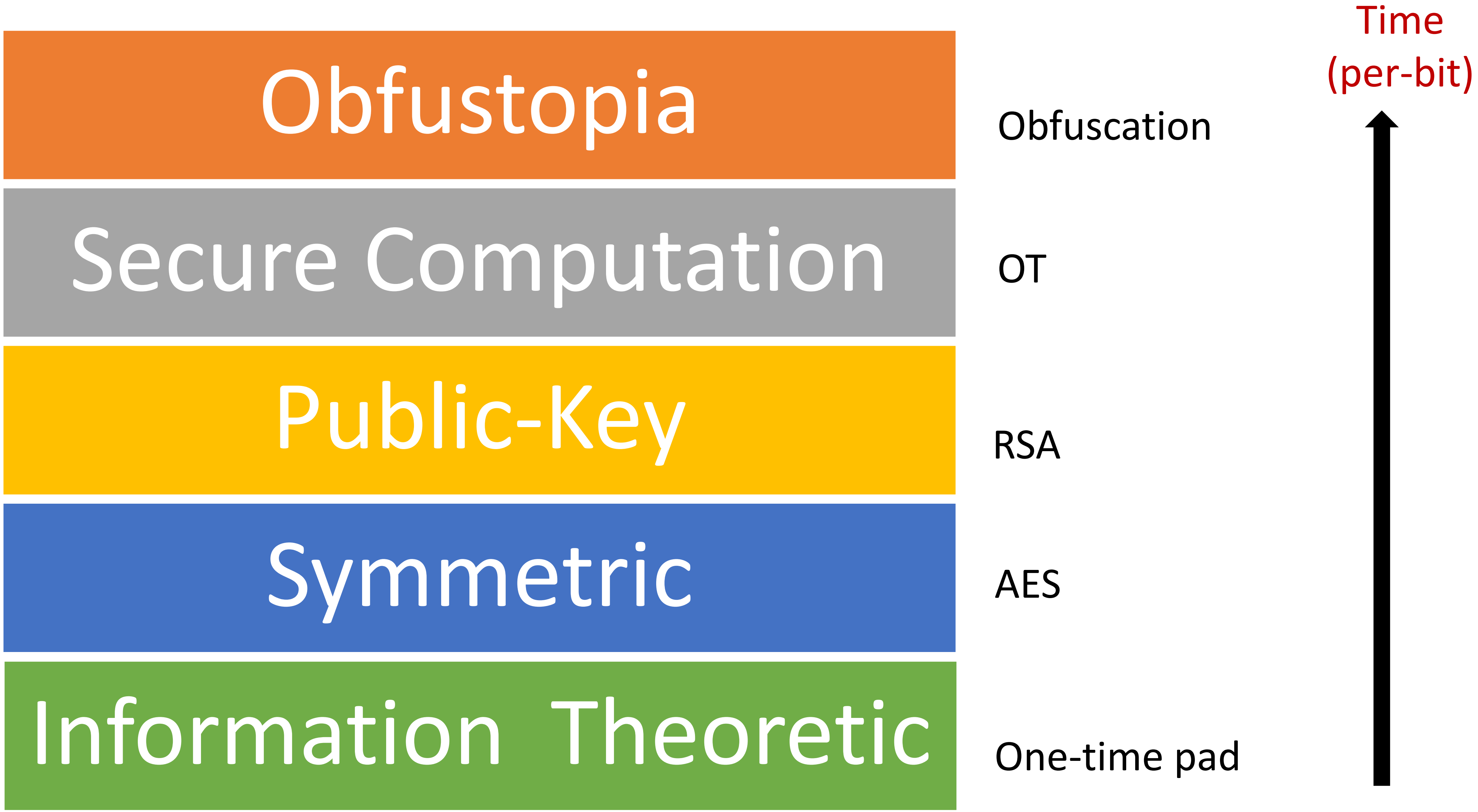
Secure Computation

Public-Key

Symmetric

Information Theoretic

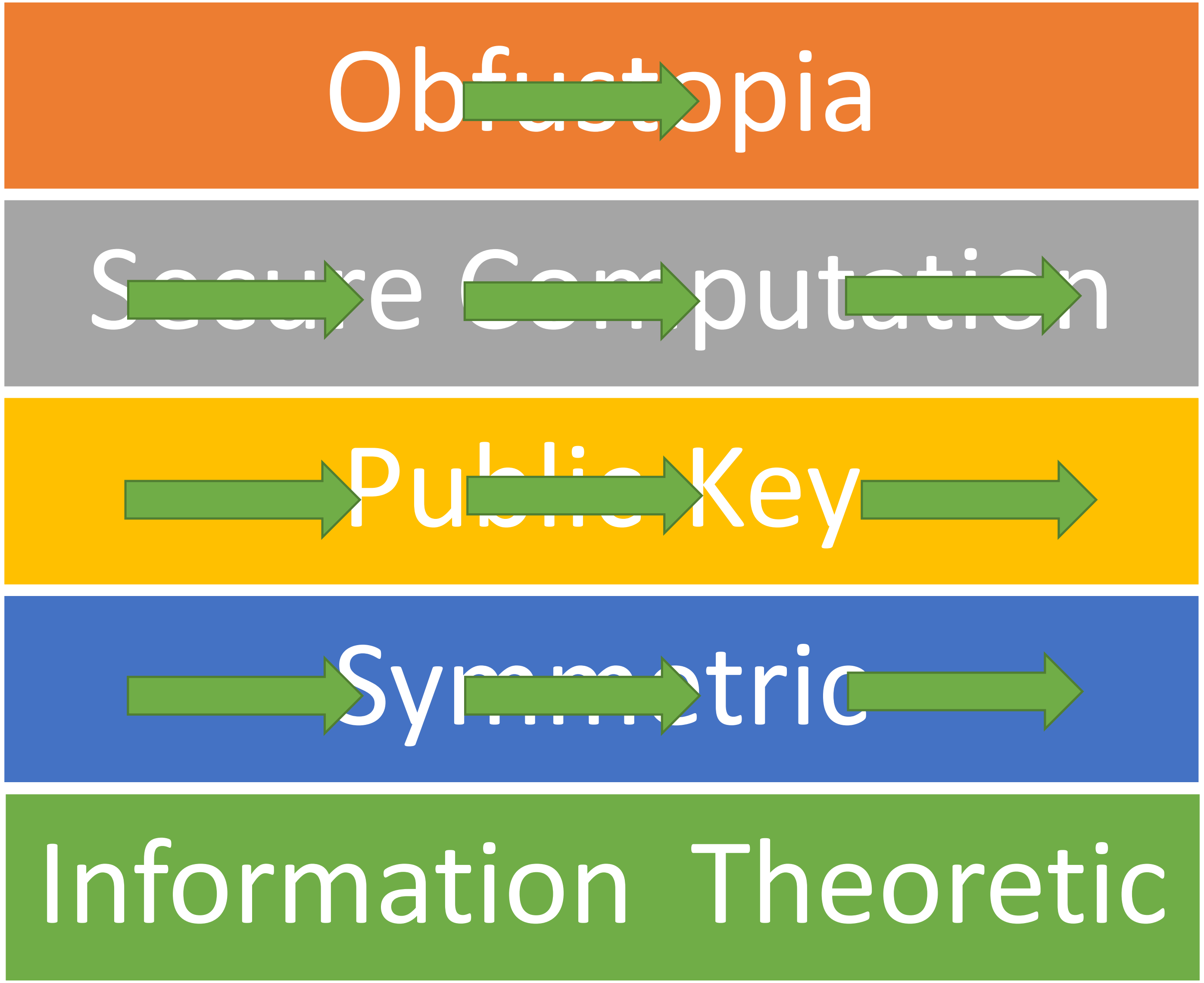
The Crypto Tower



Obfustopia	Obfuscation
Secure Computation	OT
Public-Key	RSA
Symmetric	AES
Information Theoretic	One-time pad

Time (per-bit)

The Crypto Tower: Realistic View



Obfustopia

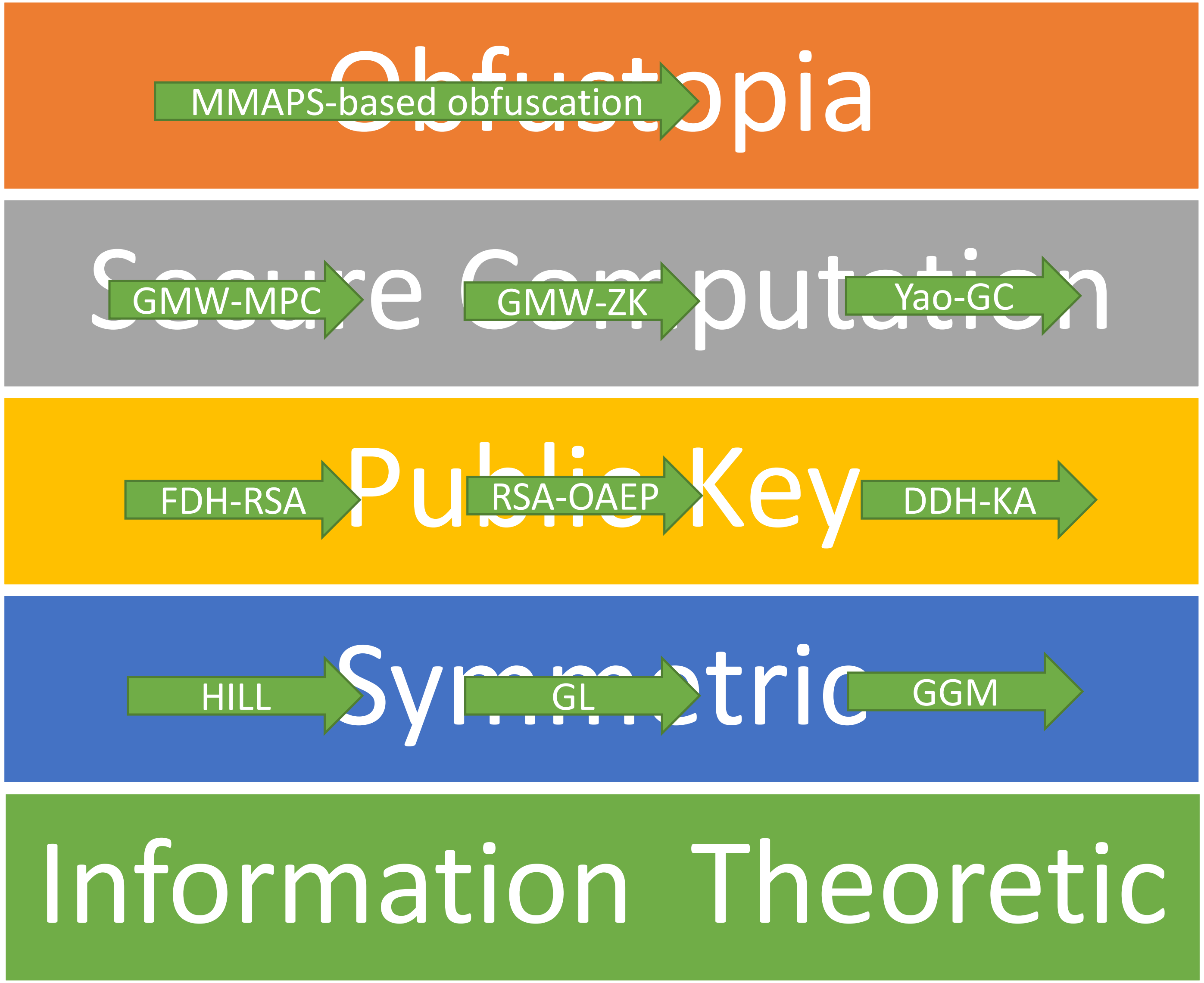
Secure Computation

Public Key

Symmetric

Information Theoretic

The Crypto Tower: Realistic View



Obfustopia

MMAPS-based obfuscation

Secure Computation

GMW-MPC

GMW-ZK

Yao-GC

Public Key

FDH-RSA

RSA-OAEP

DDH-KA

Symmetric

HILL

GL

GGM

Information Theoretic

The best of all worlds

Obfustopia

Secure Computation

Public-Key

Symmetric

Information Theoretic

Problem

The best of all worlds

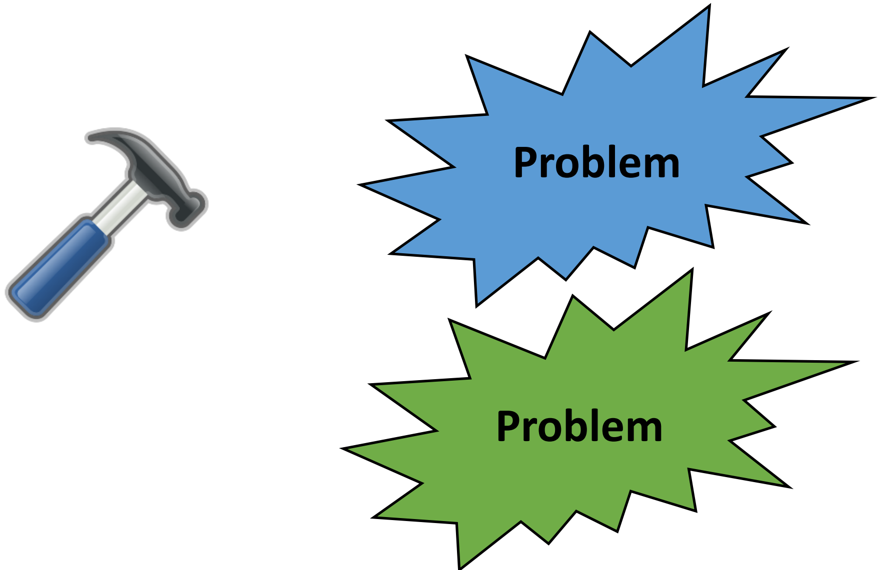
Obfustopia

Secure Computation

Public-Key

Symmetric

Information Theoretic



Two Case Studies:

Perfect Encryption & Error Correcting Codes

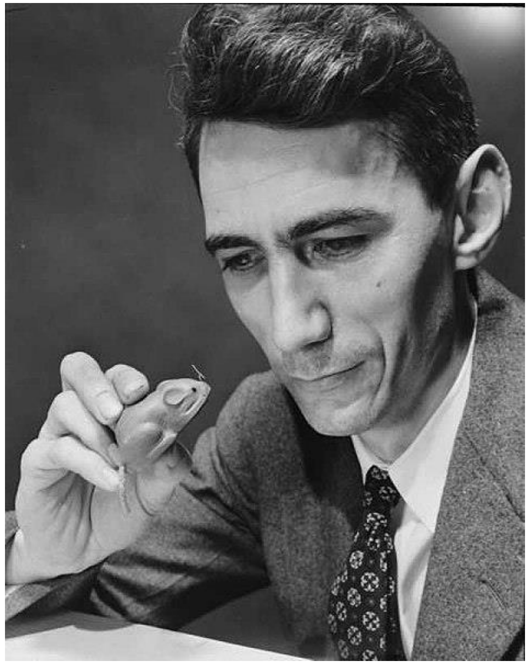
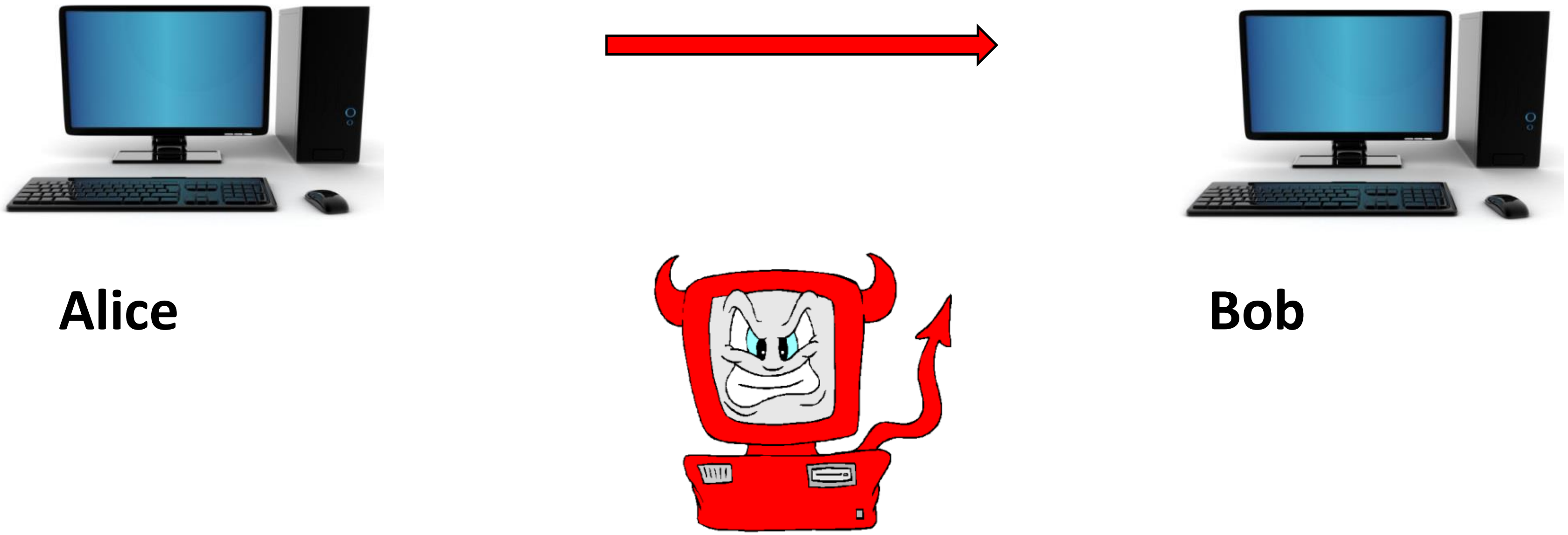


Image credits:
Photo: CC BY SA 4.0, by DobriZheglov, https://commons.wikimedia.org/wiki/File:Claude_Shannon_1776.jpg
Ali Baba's cave: CC BY 2.5, by Dake, https://commons.wikimedia.org/wiki/File:Zkip_alibaba{1,2,3}.png

Case Study 1: Perfect Encryption [Shannon 48]

Message $M \in \{0,1\}^n$



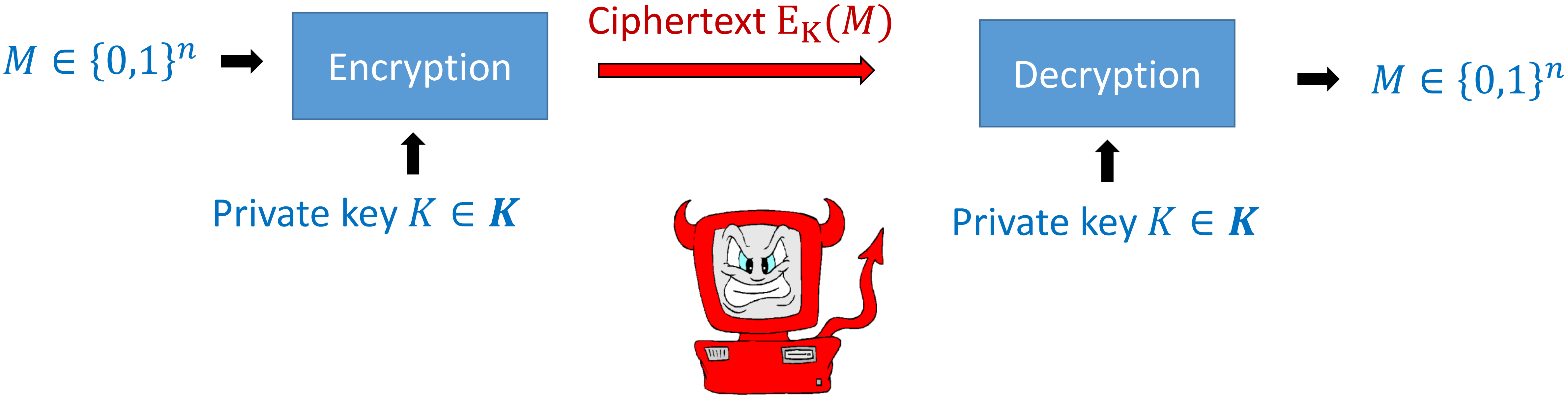
Alice

Bob

Case Study 1: Perfect Encryption [Shannon 48]

Secrecy: For every $X, Y \in \{0,1\}^n$ $\quad \mathrm{E}_{\mathrm{K}}(X) \equiv \mathrm{E}_{\mathrm{K}}(Y)$

where $K \in_R \boldsymbol{K}$



$M \in \{0,1\}^n$ ➡

Encryption

Ciphertext $\mathrm{E}_{\mathrm{K}}(M)$

Decryption

➡ $M \in \{0,1\}^n$

Private key $K \in \boldsymbol{K}$

Private key $K \in \boldsymbol{K}$

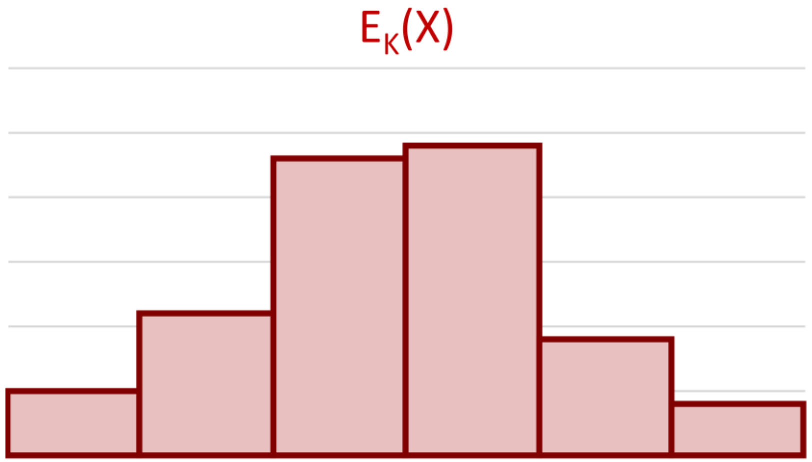
Perfect Secrecy

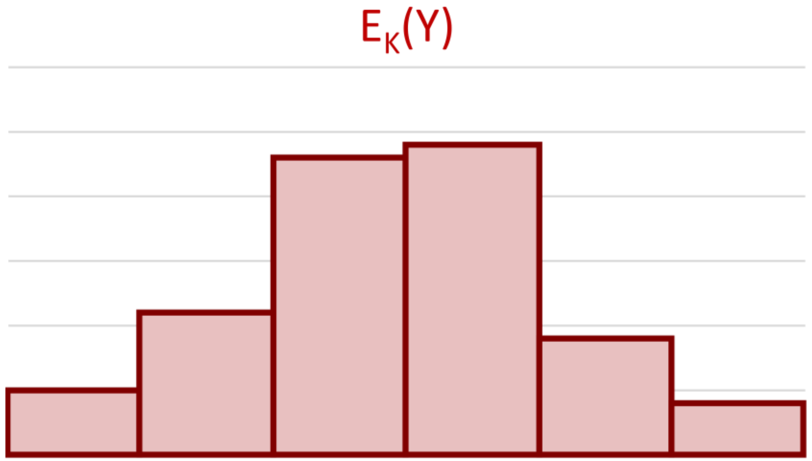
Secrecy: For every $X, Y \in \{0,1\}^n$

where $K \in_R \boldsymbol{K}$

$$\mathrm{E}_{\mathrm{K}}(X) \equiv \mathrm{E}_{\mathrm{K}}(Y)$$

$$\forall\, C, \Pr_K[E_K(X) = C] = \Pr_K[E_K(Y) = C]$$



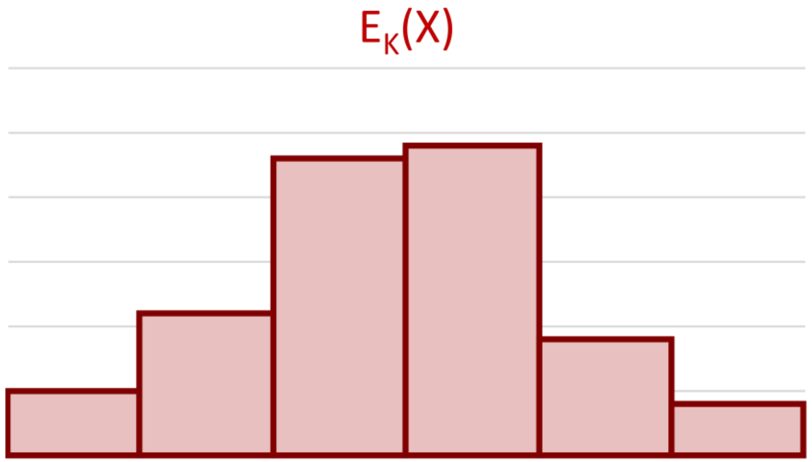


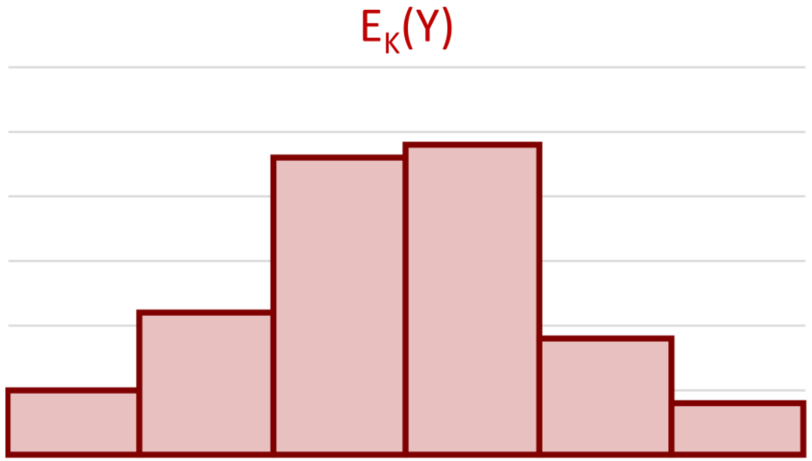
Statistical Secrecy

Secrecy: For every $X, Y \in \{0,1\}^n$
where $K \in_R \boldsymbol{K}$

$$\mathrm{E}_{\mathrm{K}}(X) \approx \mathrm{E}_{\mathrm{K}}(Y)$$

$$\forall \text{ set of ciphertexts } S, \underset{K}{\Pr}[E_K(X) \in S] \approx_\delta \underset{K}{\Pr}[E_K(Y) \in S]$$



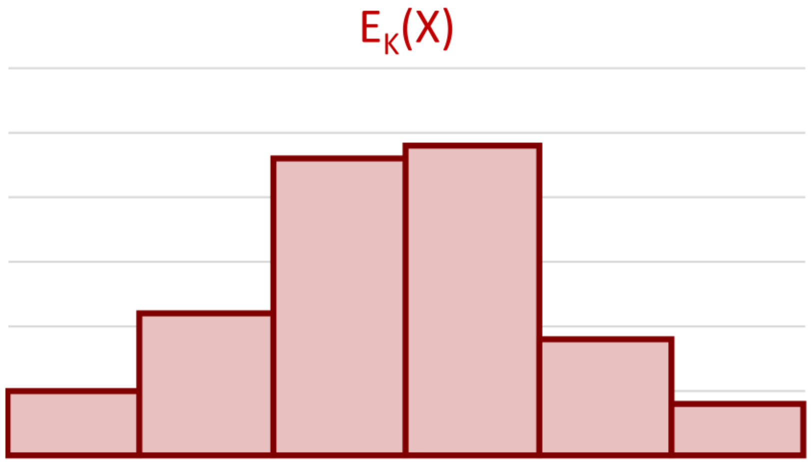


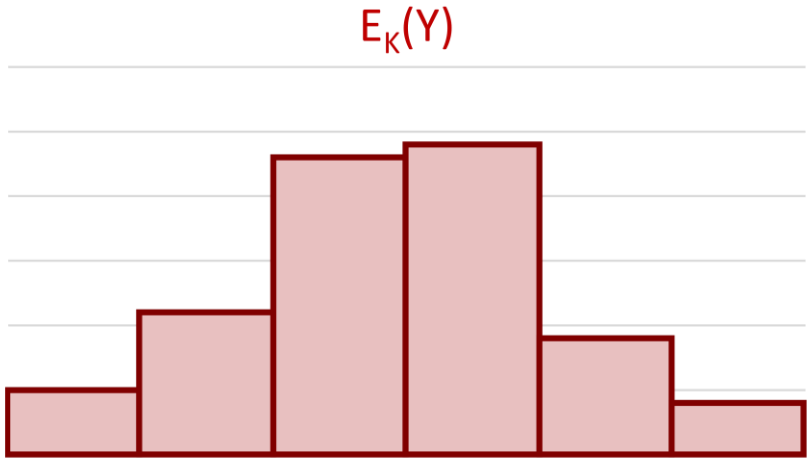
Statistical Secrecy

Secrecy: For every $X, Y \in \{0,1\}^n$
where $K \in_R \boldsymbol{K}$

$$\boxed{\mathrm{E}_{\mathrm{K}}(X) \approx \mathrm{E}_{\mathrm{K}}(Y)}$$

$$\forall \text{ unbounded } Adv, \left|\Pr_{K}\left[Adv\left(E_K(X)\right) = 1\right] - \Pr_{K}\left[Adv\left(E_K(Y)\right) = 1\right]\right| \leq \delta$$



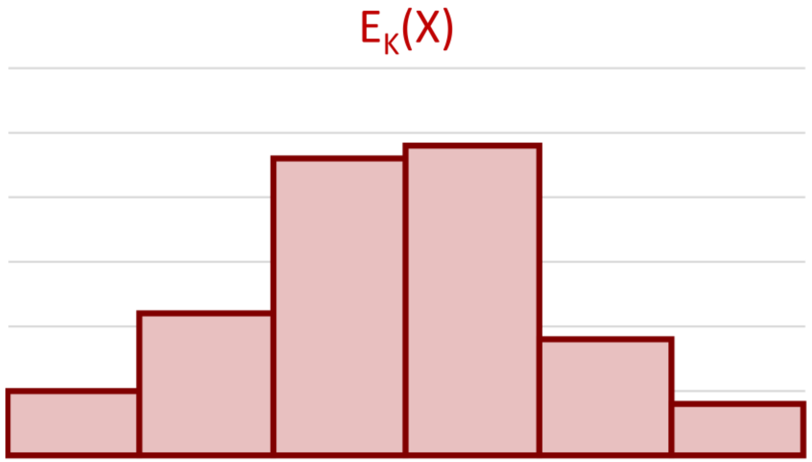


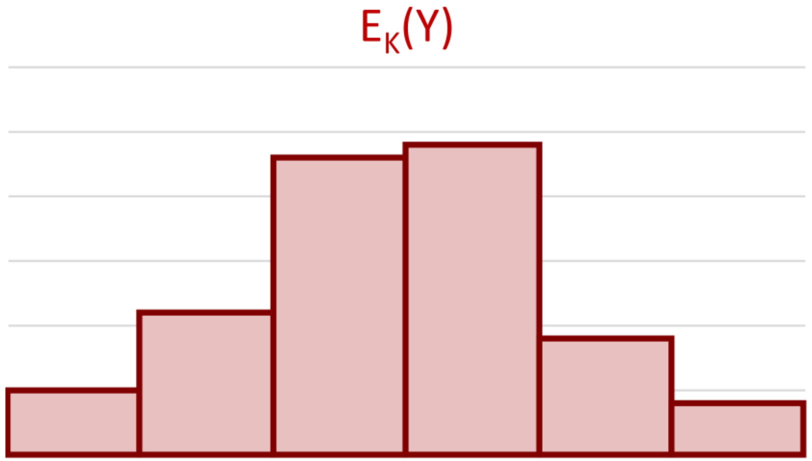
Computational Secrecy [GM'82]

Secrecy: For every $X, Y \in \{0,1\}^n$
where $K \in_R \boldsymbol{K}$

$$\mathrm{E}_{\mathrm{K}}(X) \approx \mathrm{E}_{\mathrm{K}}(Y)$$

$$\forall \text{ comp} - \text{bounded } Adv, \left|\Pr_{K}\left[Adv\left(E_K(X)\right) = 1\right] - \Pr_{K}\left[Adv\left(E_K(Y)\right) = 1\right]\right| \leq \delta$$





One-Time Pad is Perfectly Secure

$$\forall X, Y, \qquad \mathrm{E_K}(X) \equiv \mathrm{E_K}(Y)$$

Message

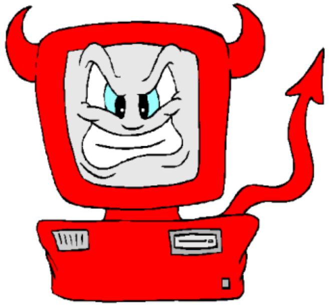
$M \in \quad \boldsymbol{G}$ ➡ Encryption

$\mathrm{E_K}(M) = K + M$ ➡

Decryption ➡ $\mathrm{D_K}(C) = C \ - K$

⬆ Private key $K \in_R \quad \boldsymbol{G}$

⬆ Private key $K \in_R \quad \boldsymbol{G}$



Proof

$$\forall X, Y, \qquad \mathrm{E}_\mathrm{K}(X) \equiv \mathrm{E}_\mathrm{K}(Y)$$

Claim: $\forall\, X, C, \Pr_K[E_K(X) = C] = 1/|G|$

$$\Pr_K[K + M \; = C] = \Pr_K[K = C - M] = 1/|G|$$

Put differently: For every X the mapping

$$K \mapsto E_K(X)$$

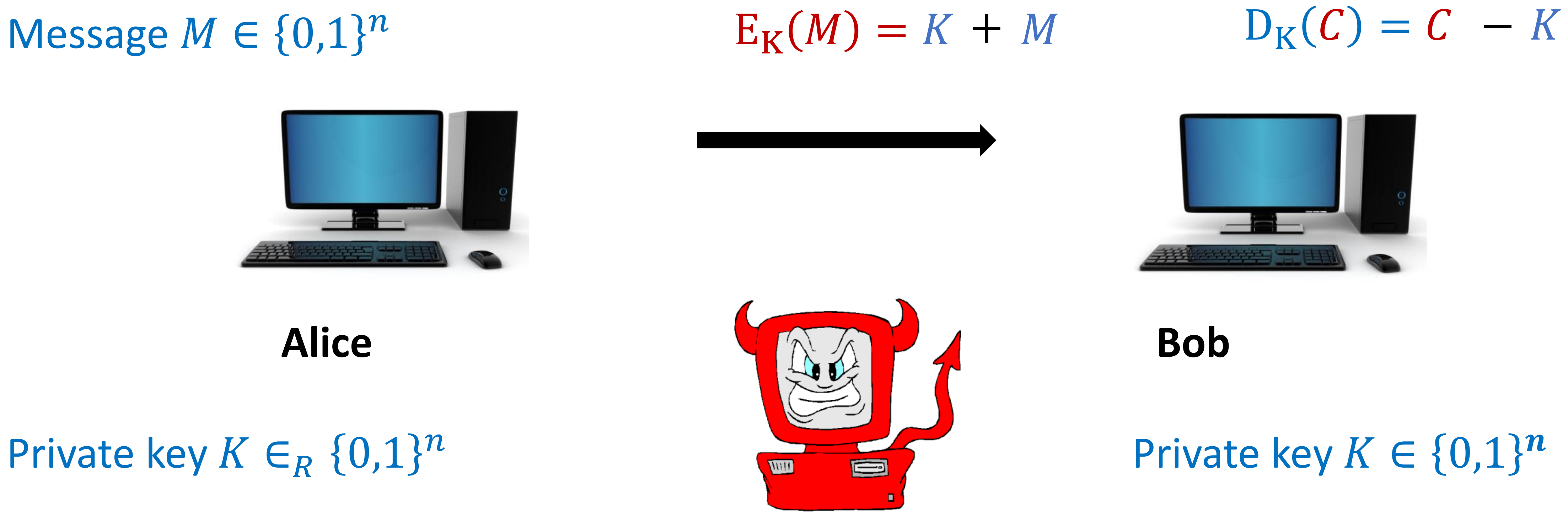
is a bijection from randomness space to ciphertext space

In fact, **non-degenerate linear mapping**

Efficiency Measures

Communication, Randomness, Round complexity

- OTP: Optimal !



Message $M \in \{0,1\}^n$

$\mathrm{E}_{\mathrm{K}}(M) = K + M$

$\mathrm{D}_{\mathrm{K}}(C) = C - K$

Alice

Bob

Private key $K \in_R \{0,1\}^n$

Private key $K \in \{0,1\}^n$

Riddle: Broadcast Encryption [Fiat-Naor94]

Message $M \in \{0,1\}$
Subset S

Alice

Keys $K_1, \dots, K_N$

$\mathrm{E_K}(M, S)$
Subset S

key K_1

Bob1

…

key K_i

Bob $\boldsymbol{i}$

Can decrypt iff
$\boldsymbol{i \in S}$

…

key K_N

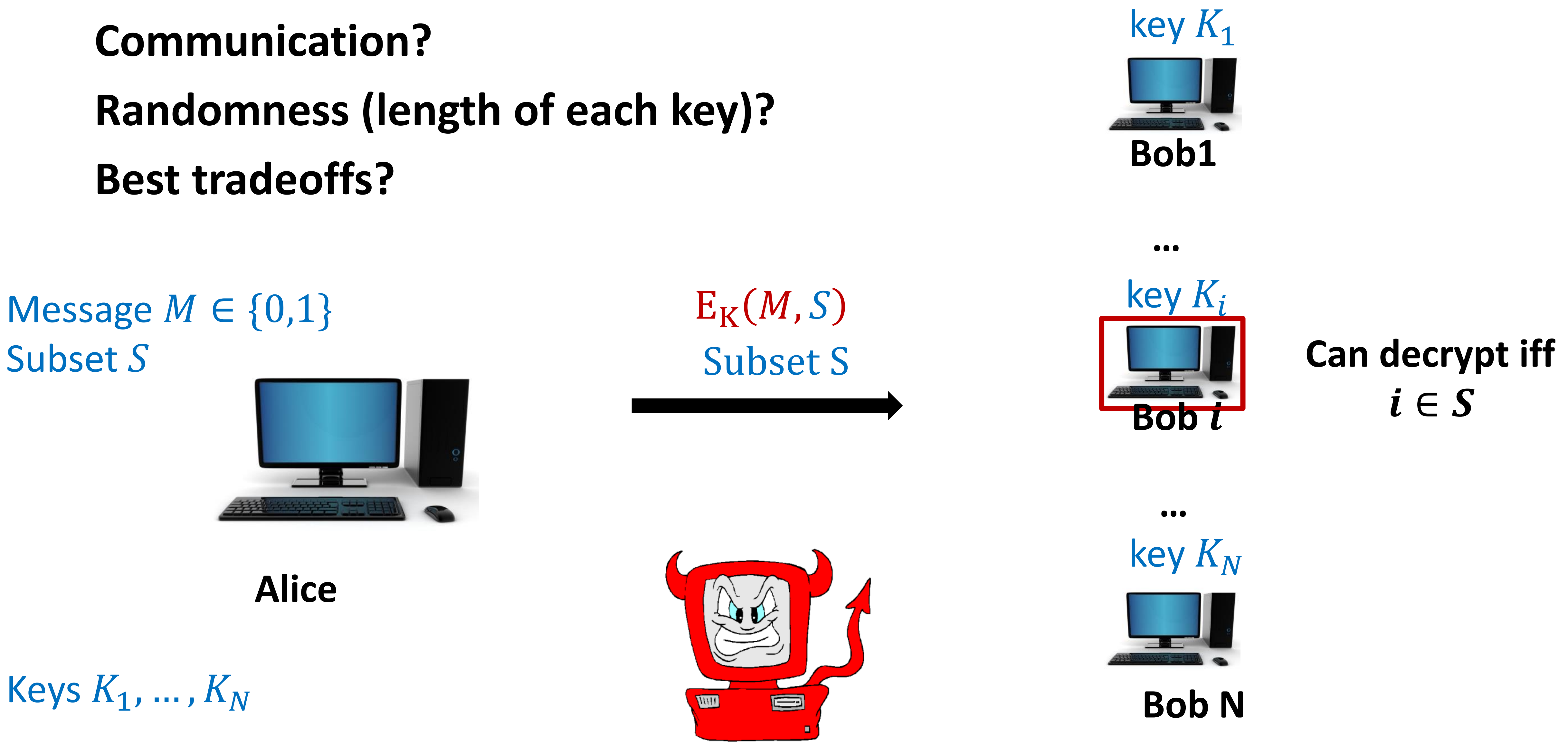
Bob N

Riddle: Broadcast Encryption [Fiat-Naor94]

Communication?

Randomness (length of each key)?

Best tradeoffs?



key K_1

Bob1

…

key K_i

Bob i

Can decrypt iff $i \in S$

…

key K_N

Bob N

Message $M \in \{0,1\}$

Subset S

$\mathrm{E}_{\mathrm{K}}(M, S)$

Subset S

Alice

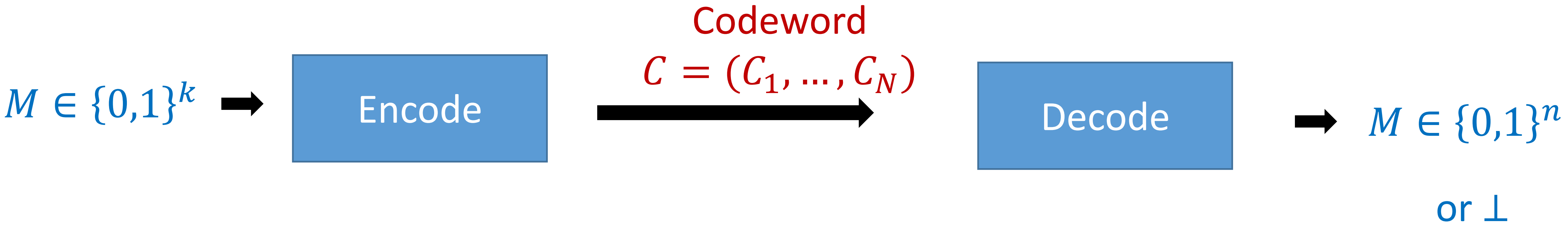
Keys $K_1, \ldots, K_N$

Case Study 2: Error Correction/Detection

[Hamming47, Shannon48]

Shannon: Solutions with optimal communication overhead

- Random linear mapping is optimal [Varshamov]
- Later efficient constructions



$M \in \{0,1\}^k$ ➡ Encode

Codeword

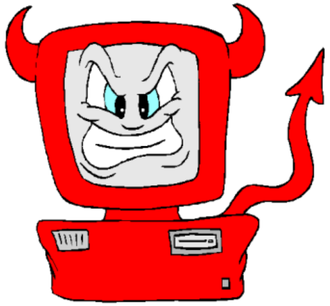
$C = (C_1, \ldots, C_N)$

Decode ➡ $M \in \{0,1\}^n$

or ⊥

Can tamper (erase/corrupt)

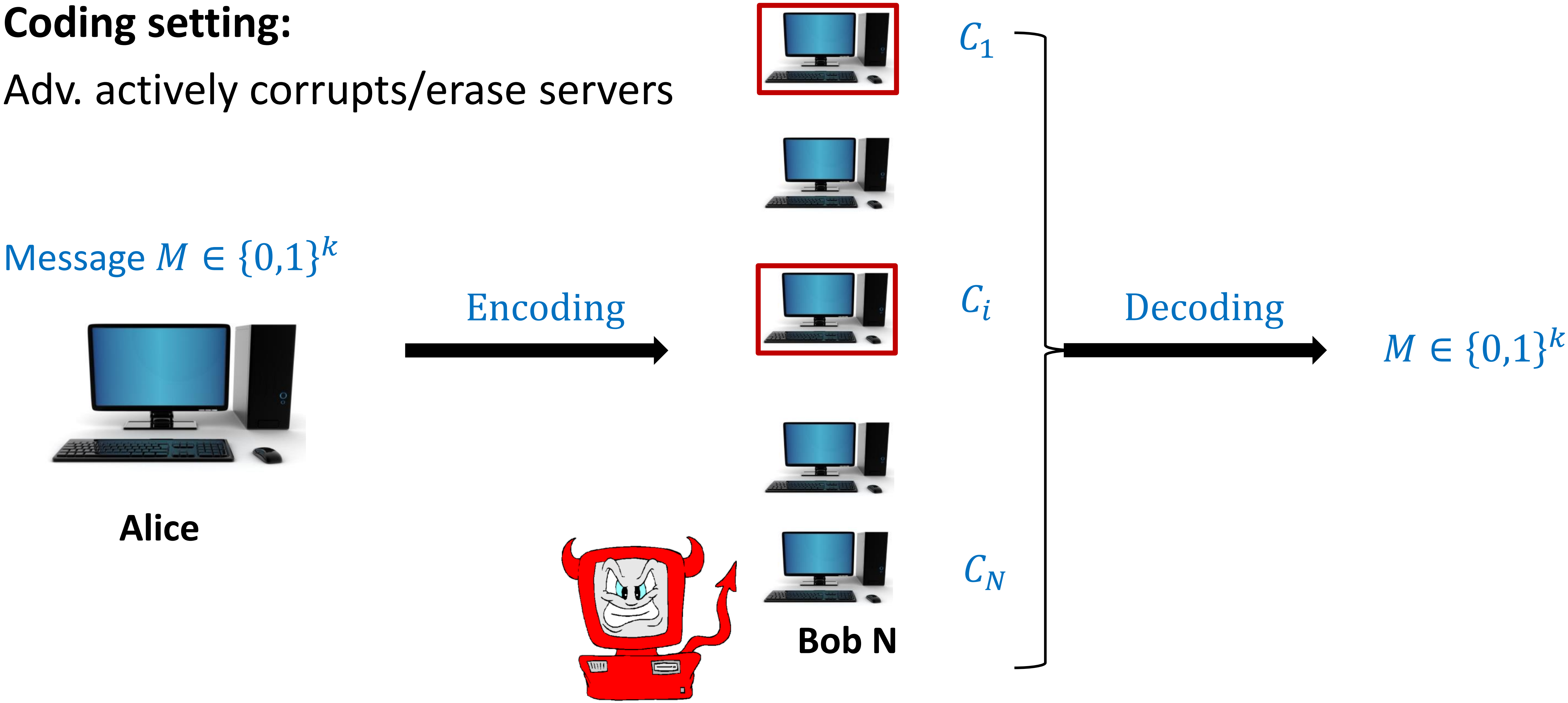
up to δ-fraction of symbols



Unified view: Distributed Storage

Coding setting:

Adv. actively corrupts/erase servers



Message $M \in \{0,1\}^k$

Encoding

C_1

C_i

C_N

Decoding

$M \in \{0,1\}^k$

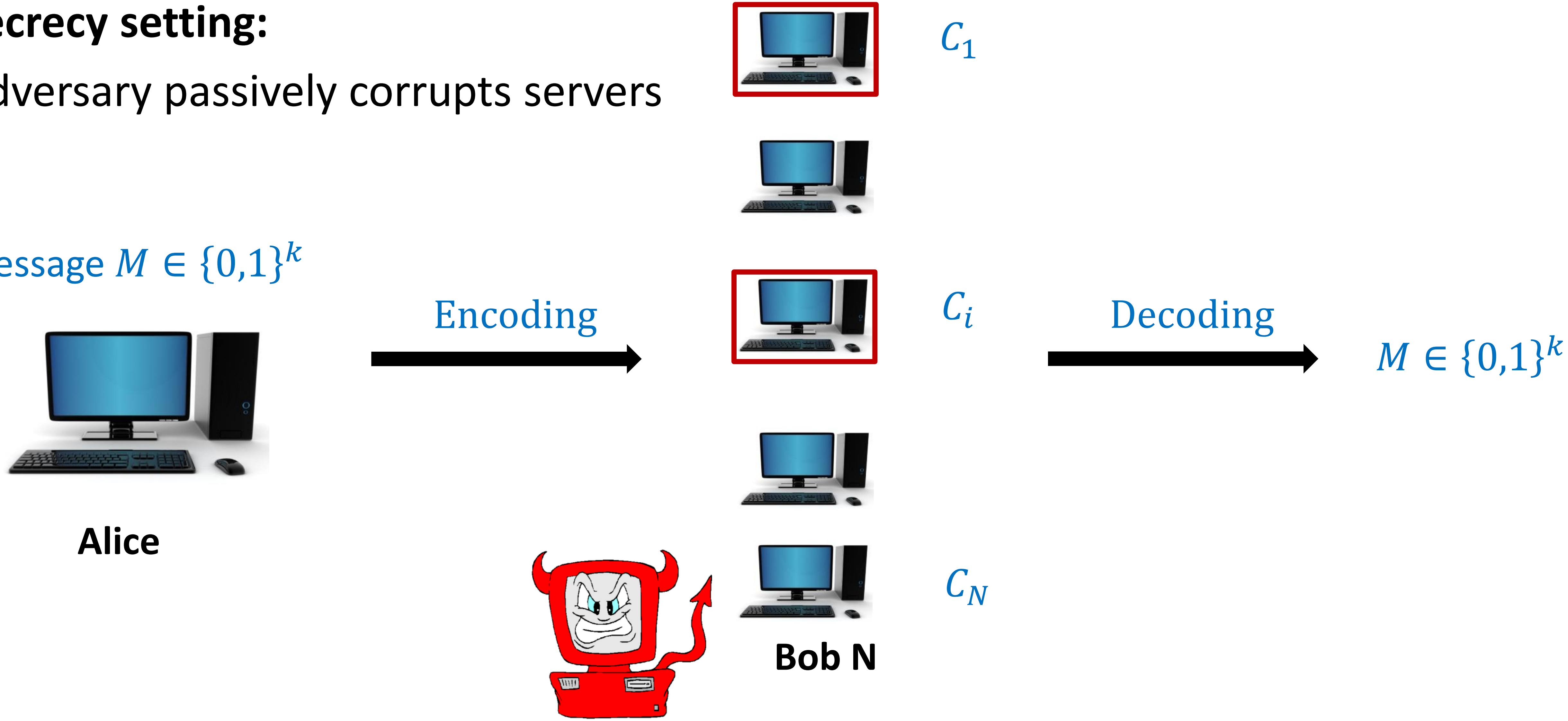
Alice

Bob N

Unified view: Distributed Storage

Secrecy setting:

Adversary passively corrupts servers



Message $M \in \{0,1\}^k$

Alice

Encoding

C_1

C_i

C_N

Bob N

Decoding

$M \in \{0,1\}^k$

Unified view: Distributed Storage

Secrecy setting:

Adversary passively corrupts servers

K

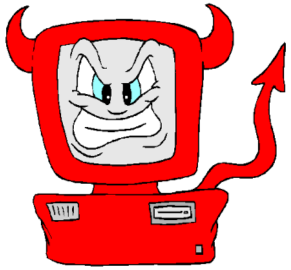
Message $M \in \{0,1\}^k$

Encoding

Decoding

$M \in \{0,1\}^k$

Alice

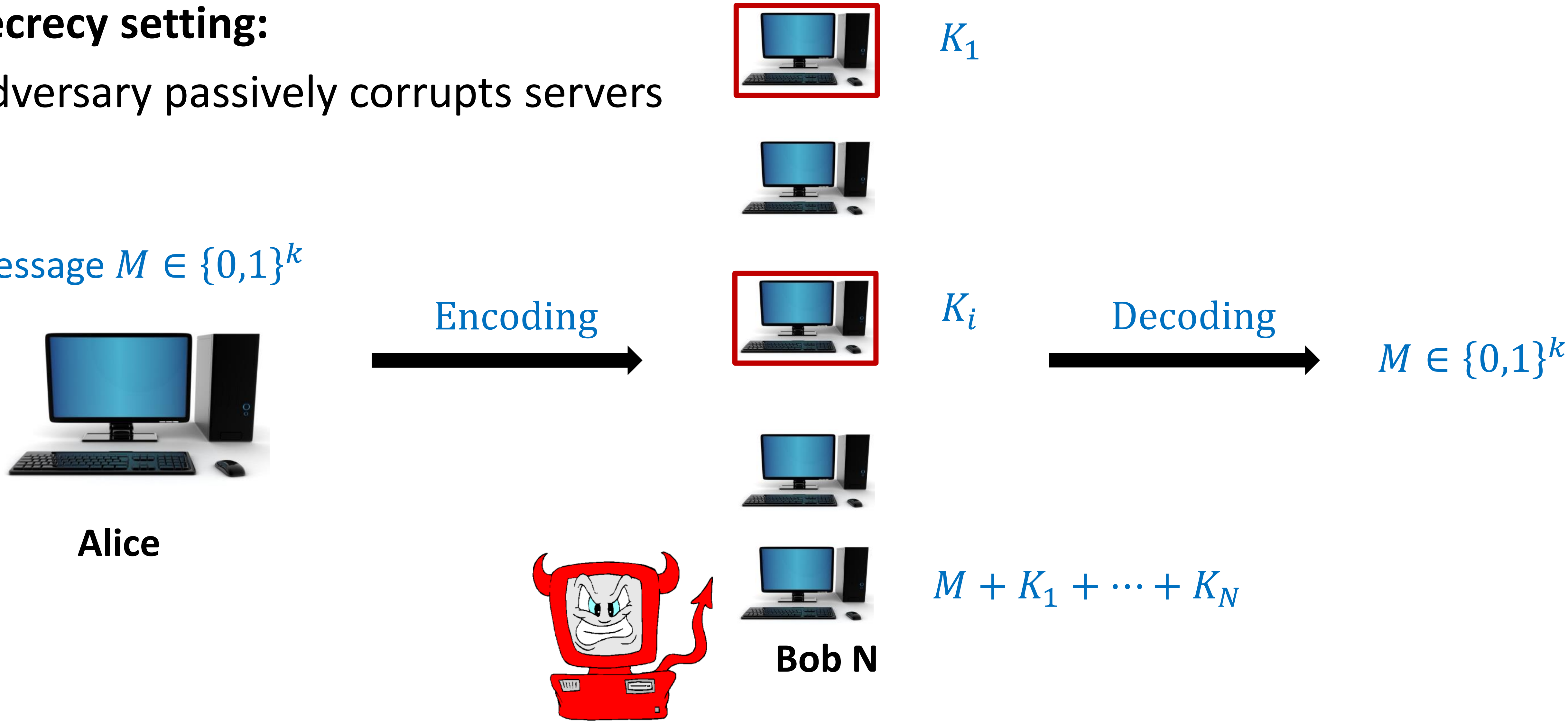


$E_K(M) = K + M$

Unified view: Distributed Storage

Secrecy setting:

Adversary passively corrupts servers



Message $M \in \{0,1\}^k$

Encoding

K_1

K_i

Decoding

$M \in \{0,1\}^k$

$M + K_1 + \cdots + K_N$

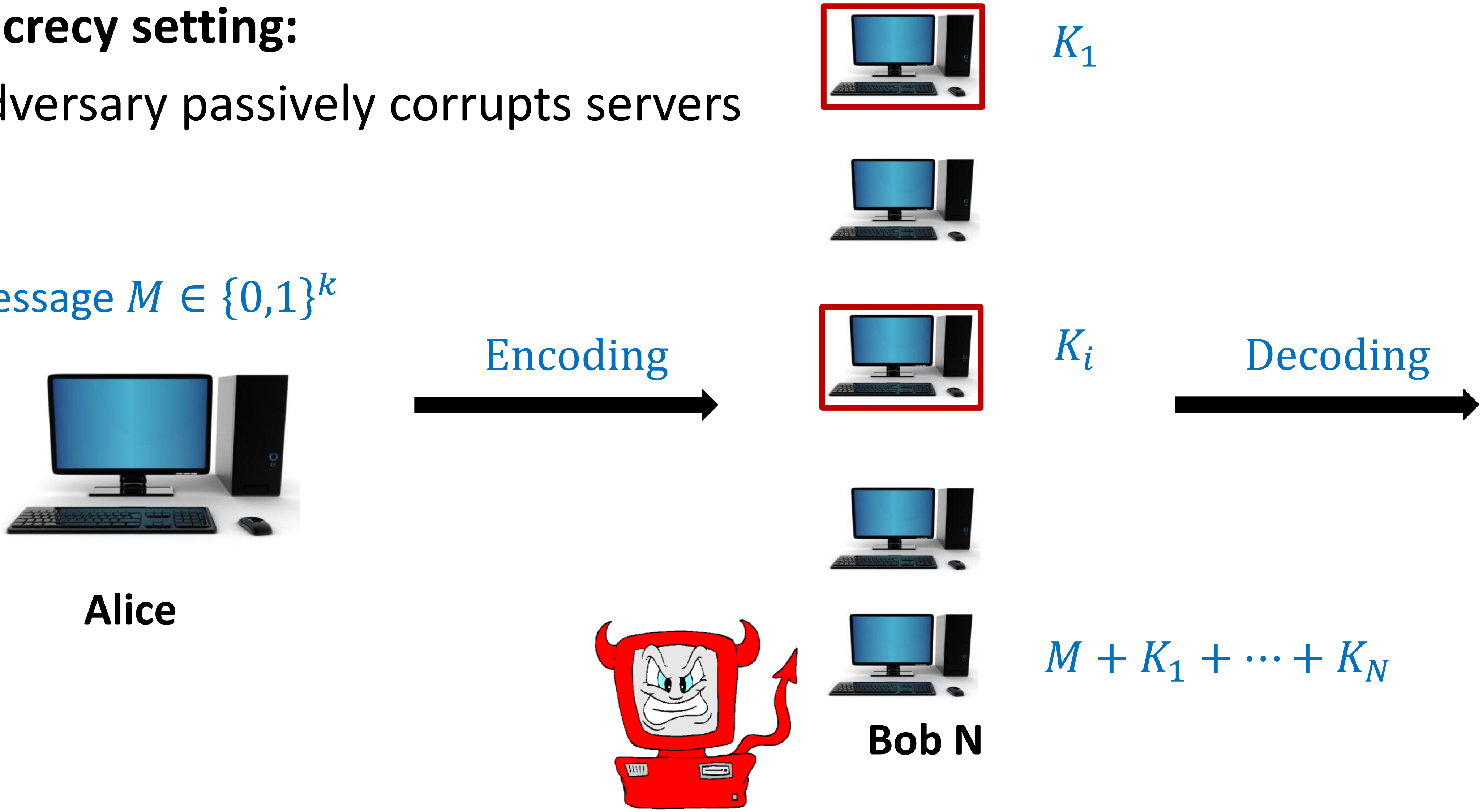
Alice

Bob N

Can we achieve privacy & resiliency?

Secrecy setting:

Adversary passively corrupts servers



K_1

Message $M \in \{0,1\}^k$

Encoding

K_i

Decoding

$M \in \{0,1\}^k$

Alice

$M + K_1 + \cdots + K_N$

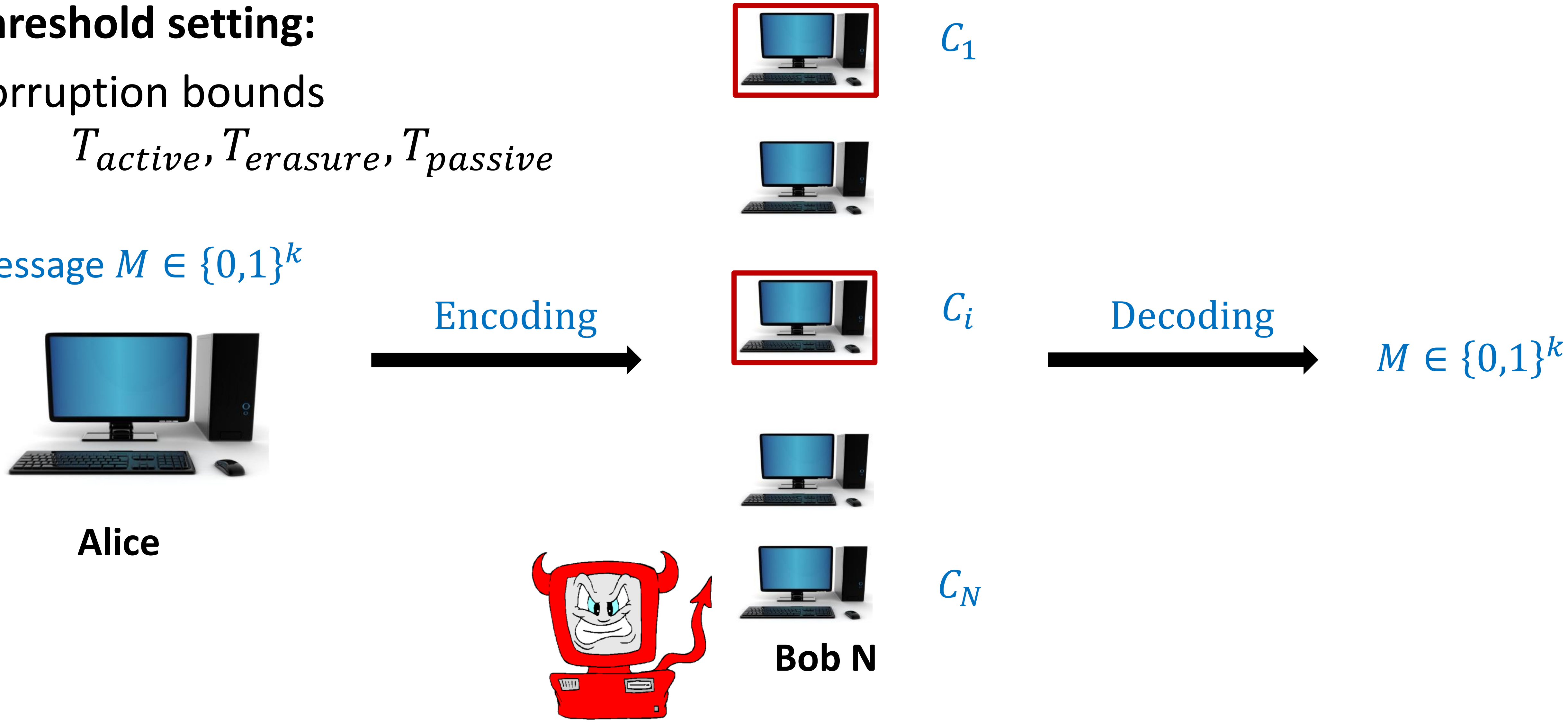
Bob N

Secret-Sharing (Gilad’s talk)

Threshold setting:

Corruption bounds

$$T_{active}, T_{erasure}, T_{passive}$$



Message $M \in \{0,1\}^k$

Encoding

C_1

C_i

Decoding

$M \in \{0,1\}^k$

Alice

C_N

Bob N

Secret-Sharing (Gilad’s talk)

Threshold setting:

Corruption bounds

$$T_{active}, T_{erasure}, T_{passive}$$

Message $M \in \{0,1\}^k$

Alice

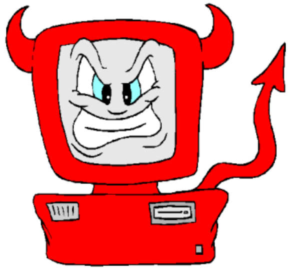
Encoding

C_1

C_i

Decoding

$M \in \{0,1\}^k$



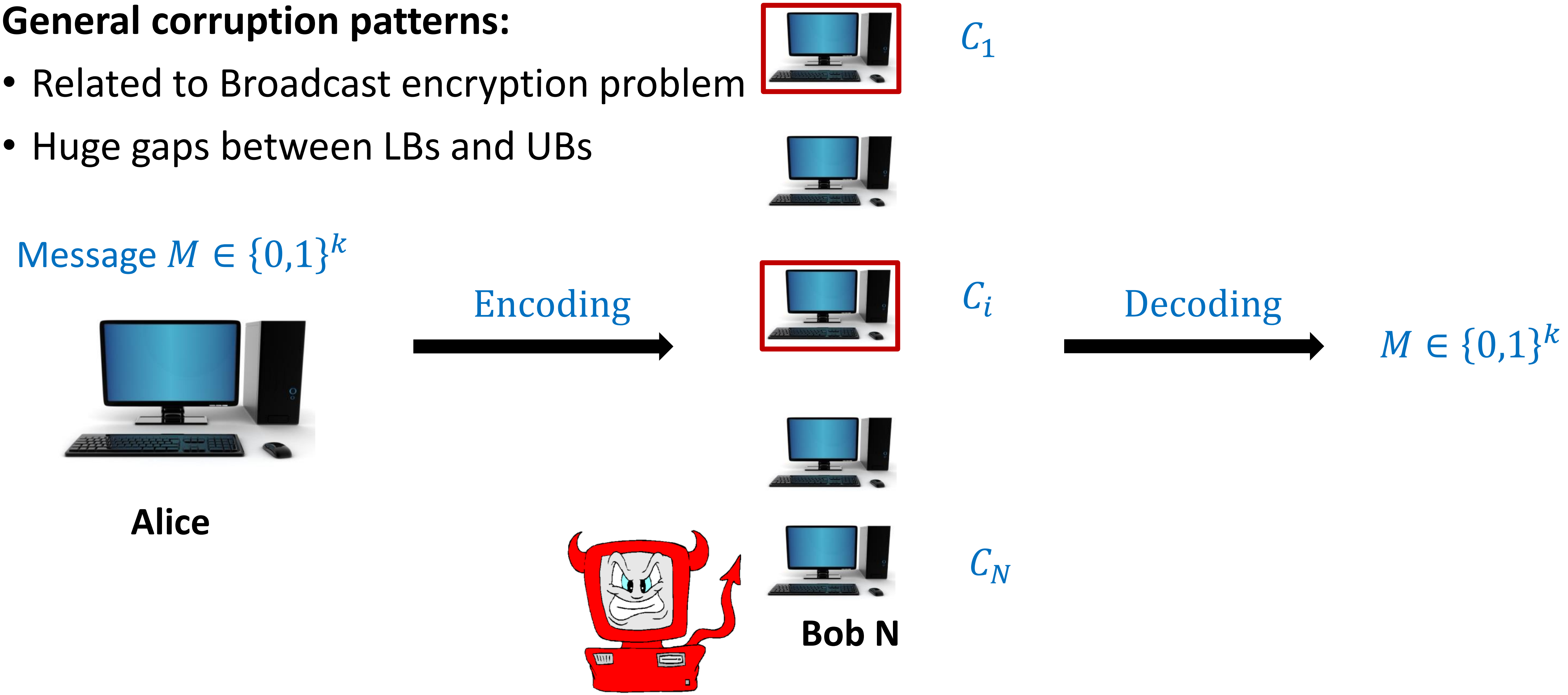
Bob N

C_N

General Secret-Sharing (Benny’s talk)

General corruption patterns:

- Related to Broadcast encryption problem
- Huge gaps between LBs and UBs



Message $M \in \{0,1\}^k$

Encoding

C_1

C_i

C_N

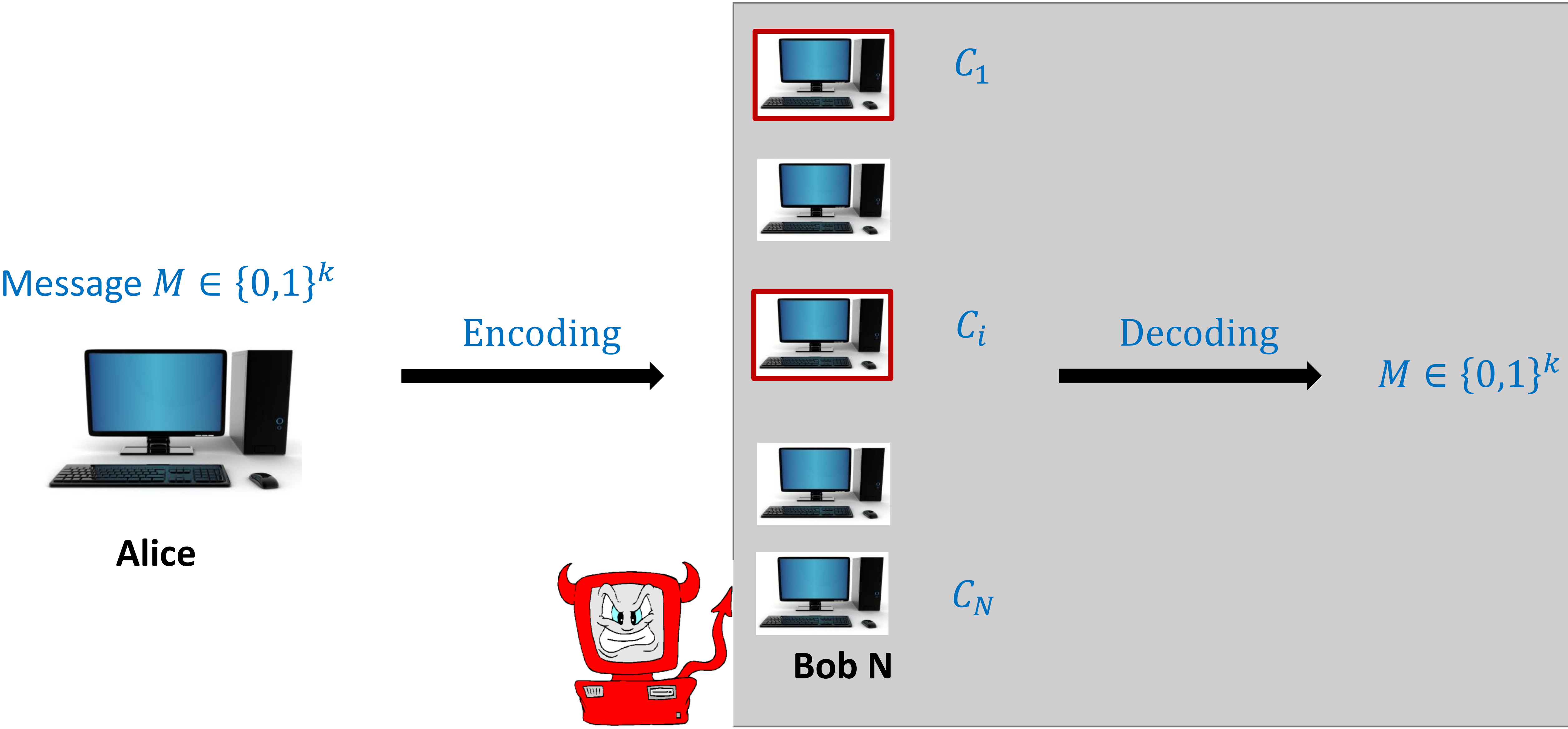
Decoding

$M \in \{0,1\}^k$

Alice

Bob N

Private Information **Retrieval** (Yuval+Klim)



Message $M \in \{0,1\}^k$

Alice

Encoding

C_1

C_i

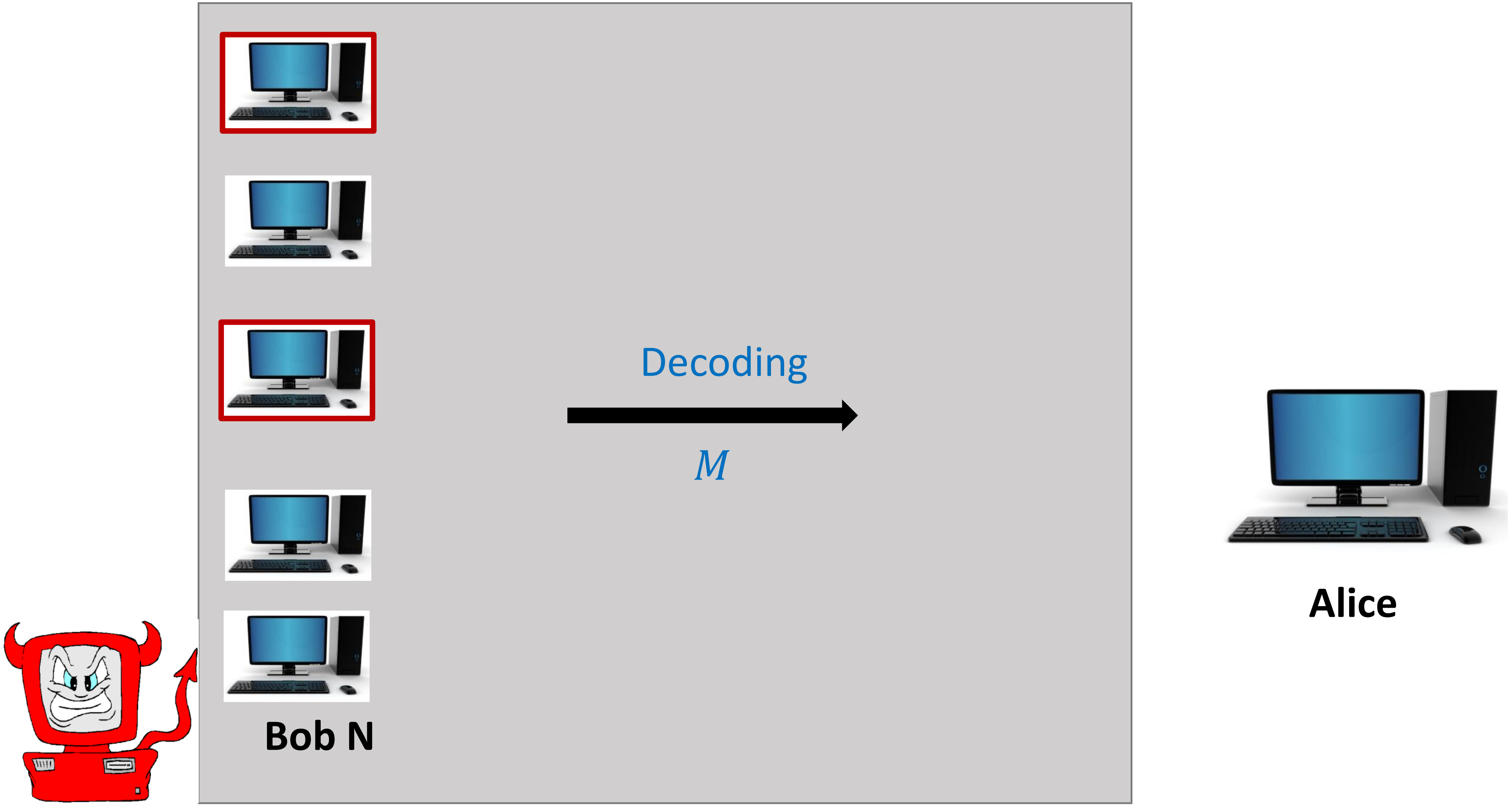
C_N

Bob N

Decoding

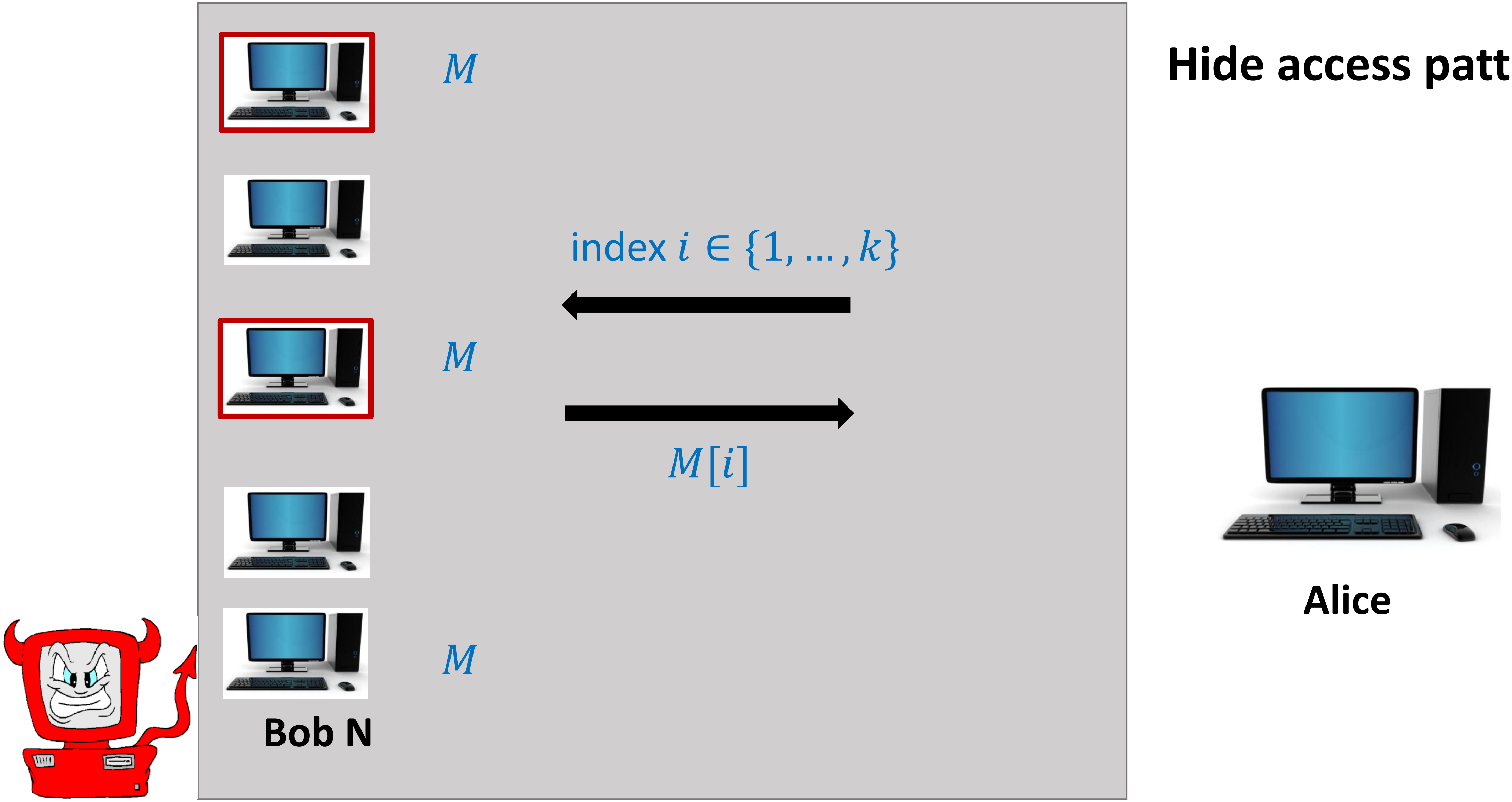
$M \in \{0,1\}^k$

Private Information **Retrieval** (Yuval+Klim)



Private Information **Retrieval** (Yuval+Klim)

Hide access pattern $\mathbf{i}$



M

index $i \in \{1, \ldots, k\}$

M

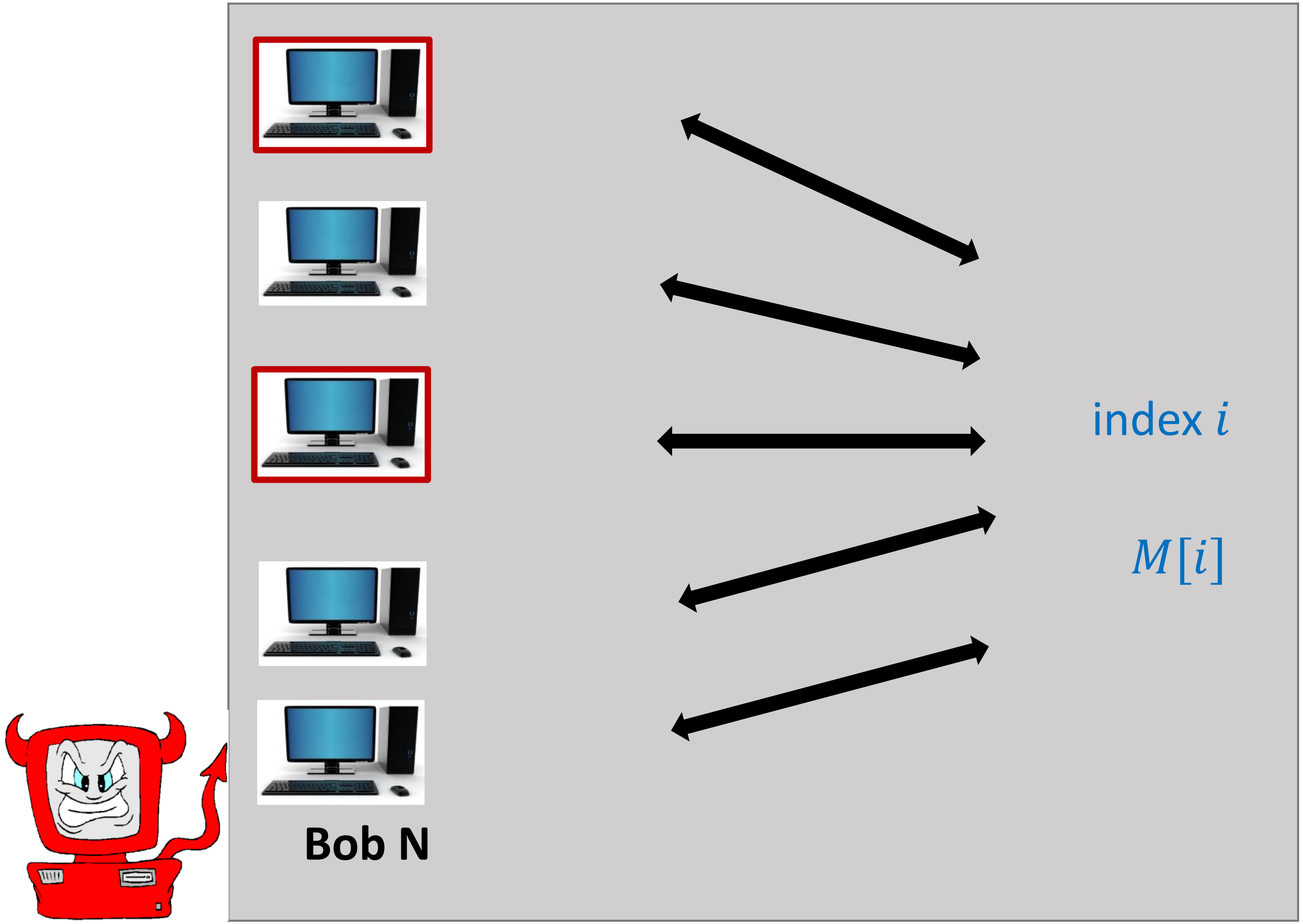
$M[i]$

M

Bob N

Alice

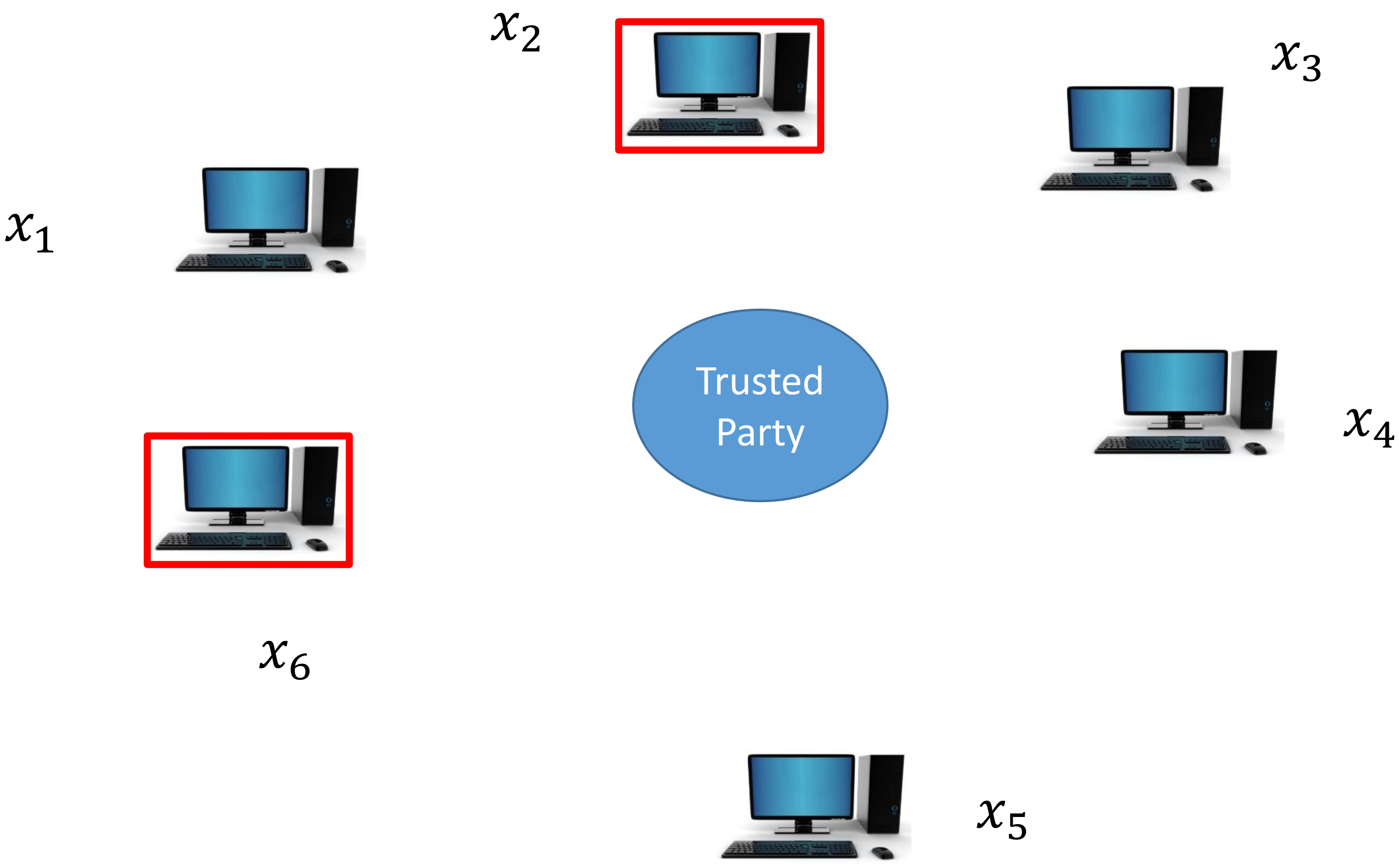
Private Information **Retrieval** (Yuval+Klim)



Hide access pattern i

- Power of non-linearity
- Huge gaps between LBs and UPs

Computation: Beyond Storage



x_2

x_3

x_1

Trusted Party

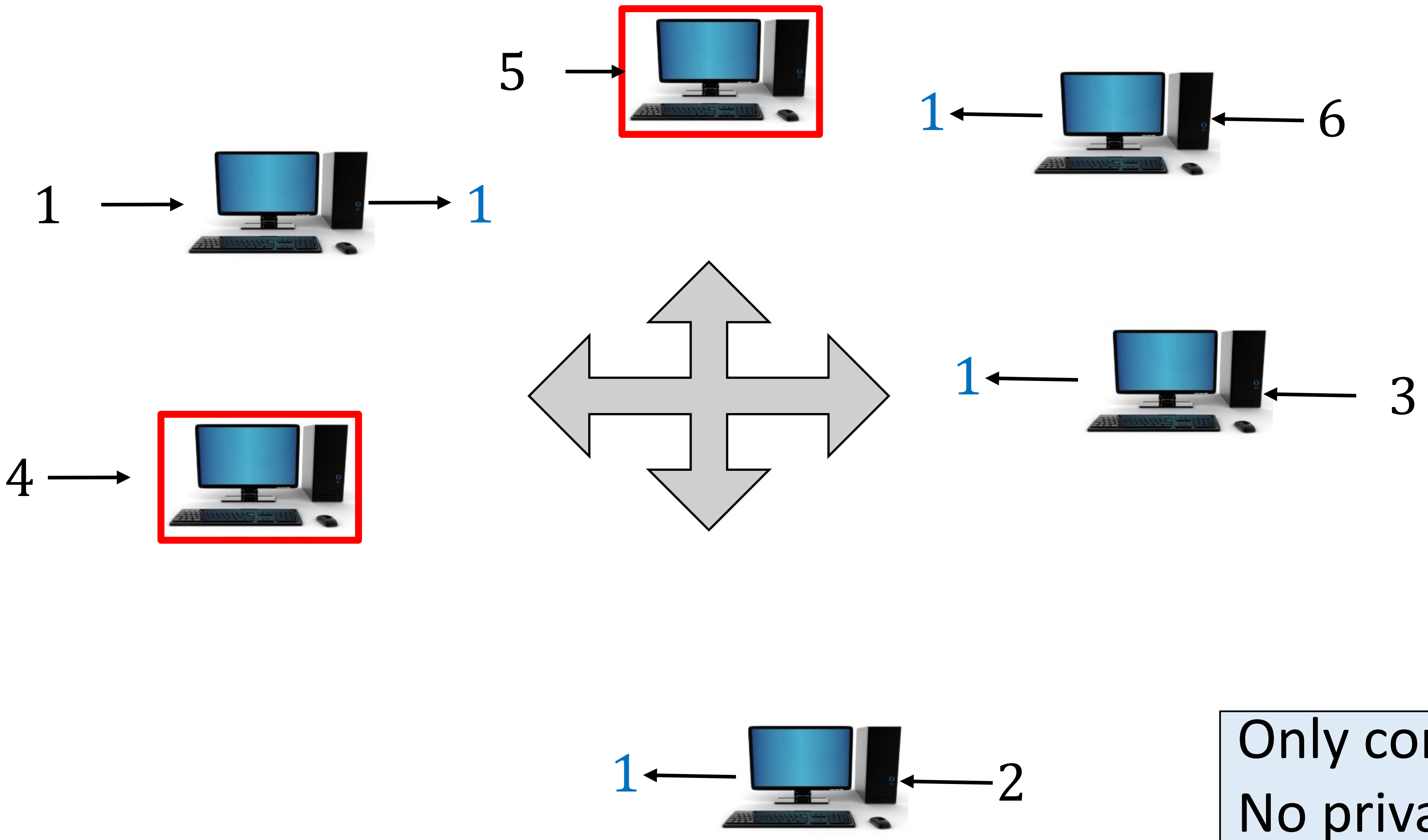
x_4

x_6

x_5

Consensus (Ittai’s talk)

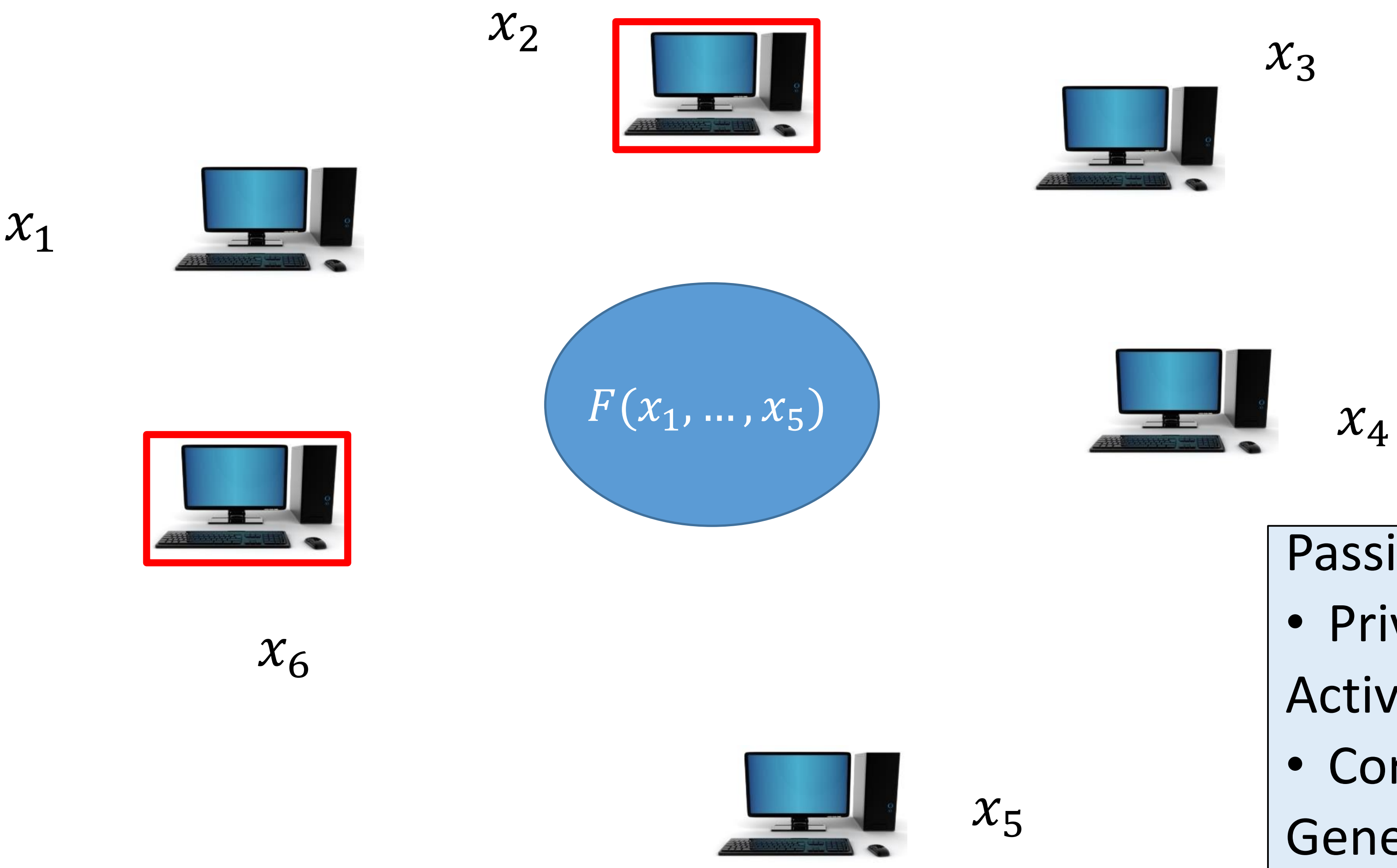
Achieving Agreement at the presence of failures/corruptions/delays



Only correctness requirement
No privacy requirements

General Secure Computation (Yuval's talk)

Compute joint function of the parties inputs



Passive adversaries

- Privacy

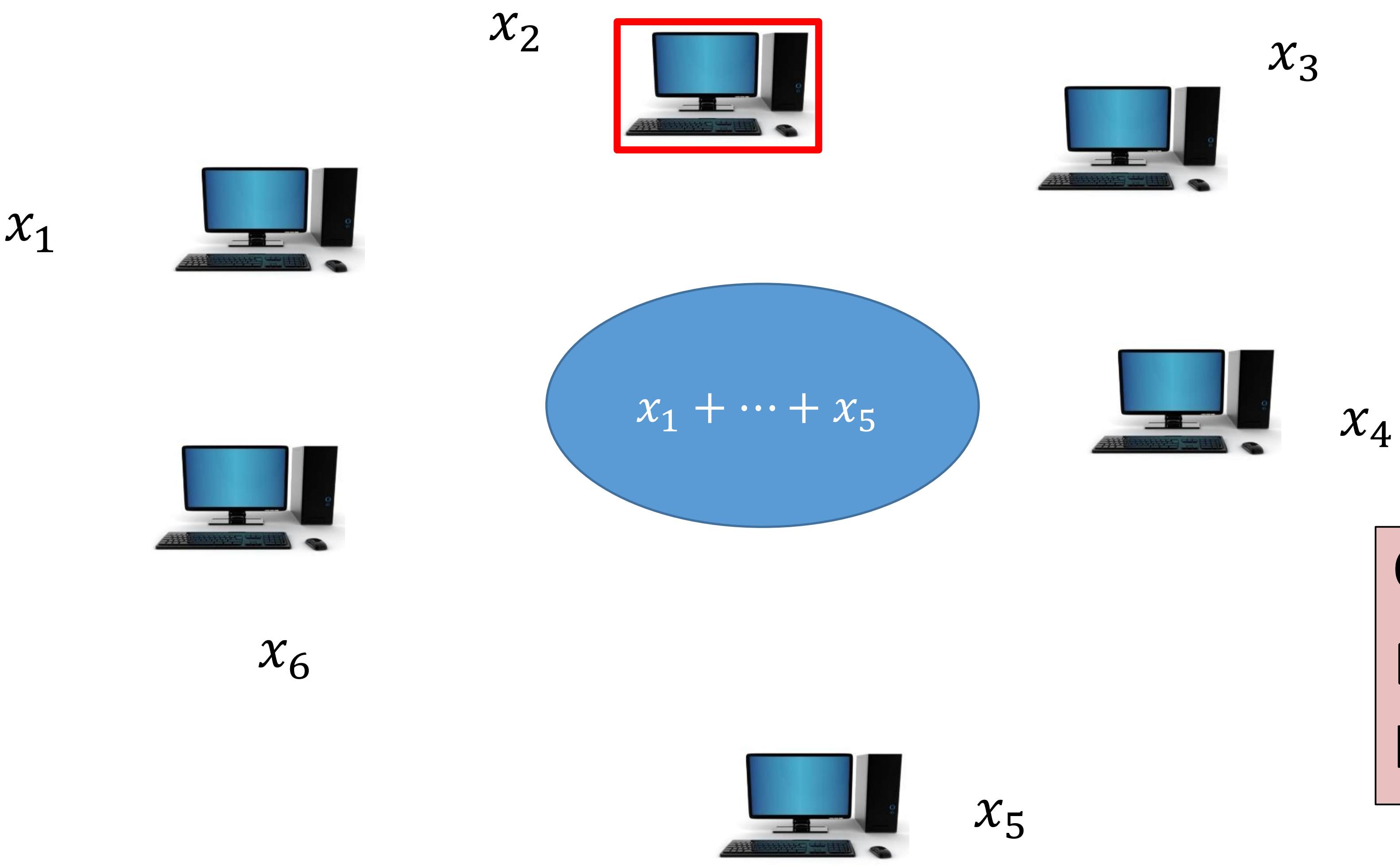
Active adversaries

- Correctness & Privacy

General Functions

General Secure Computation (Yuval's talk)

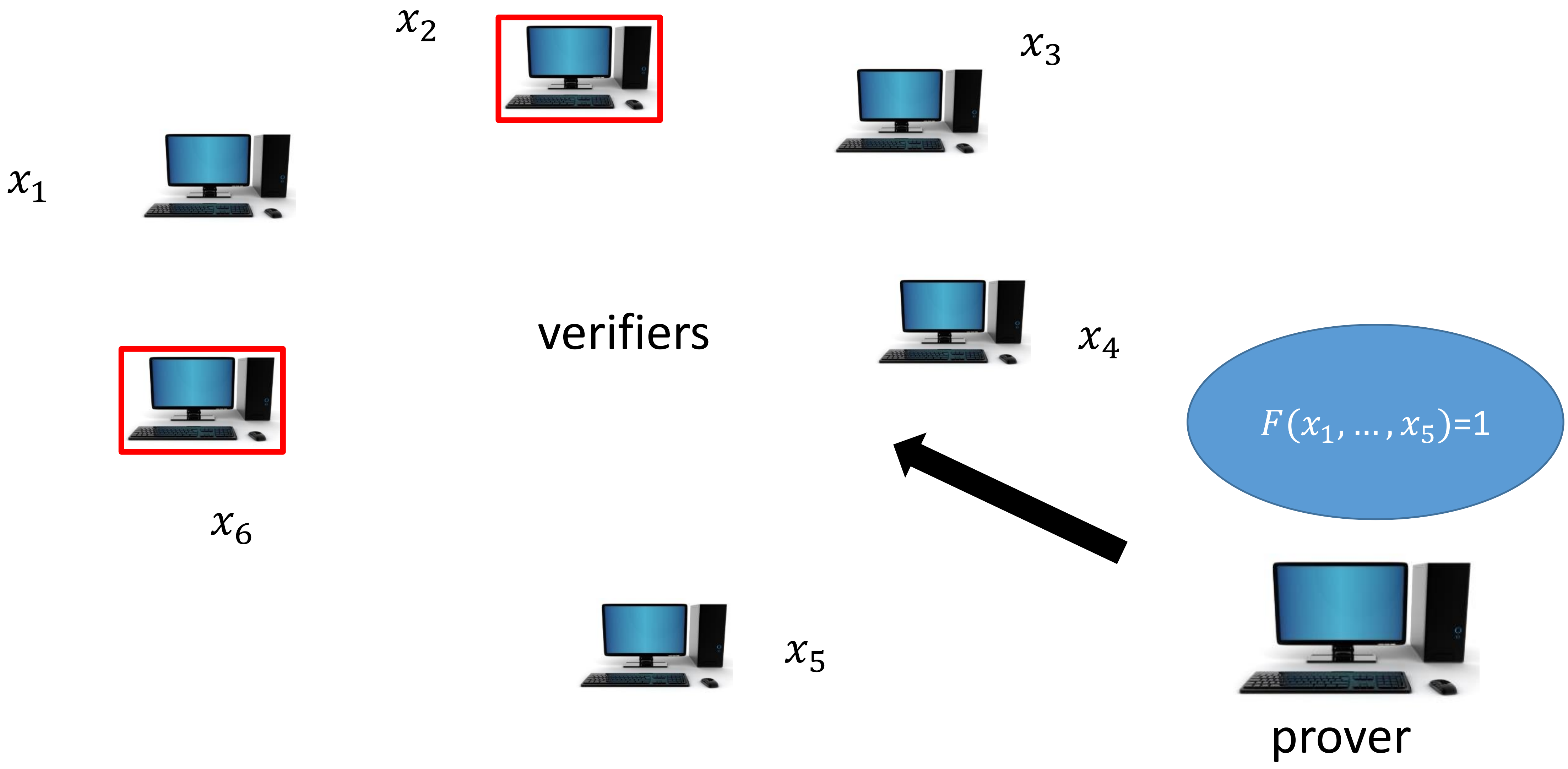
Compute joint function of the parties inputs



Challenge:

Design 1-private protocol for sum over **G**

Proofs in Non-Interactive Setting (Niv's Talk)



x_2

x_3

x_1

verifiers

x_4

$F(x_1, \dots, x_5)$=1

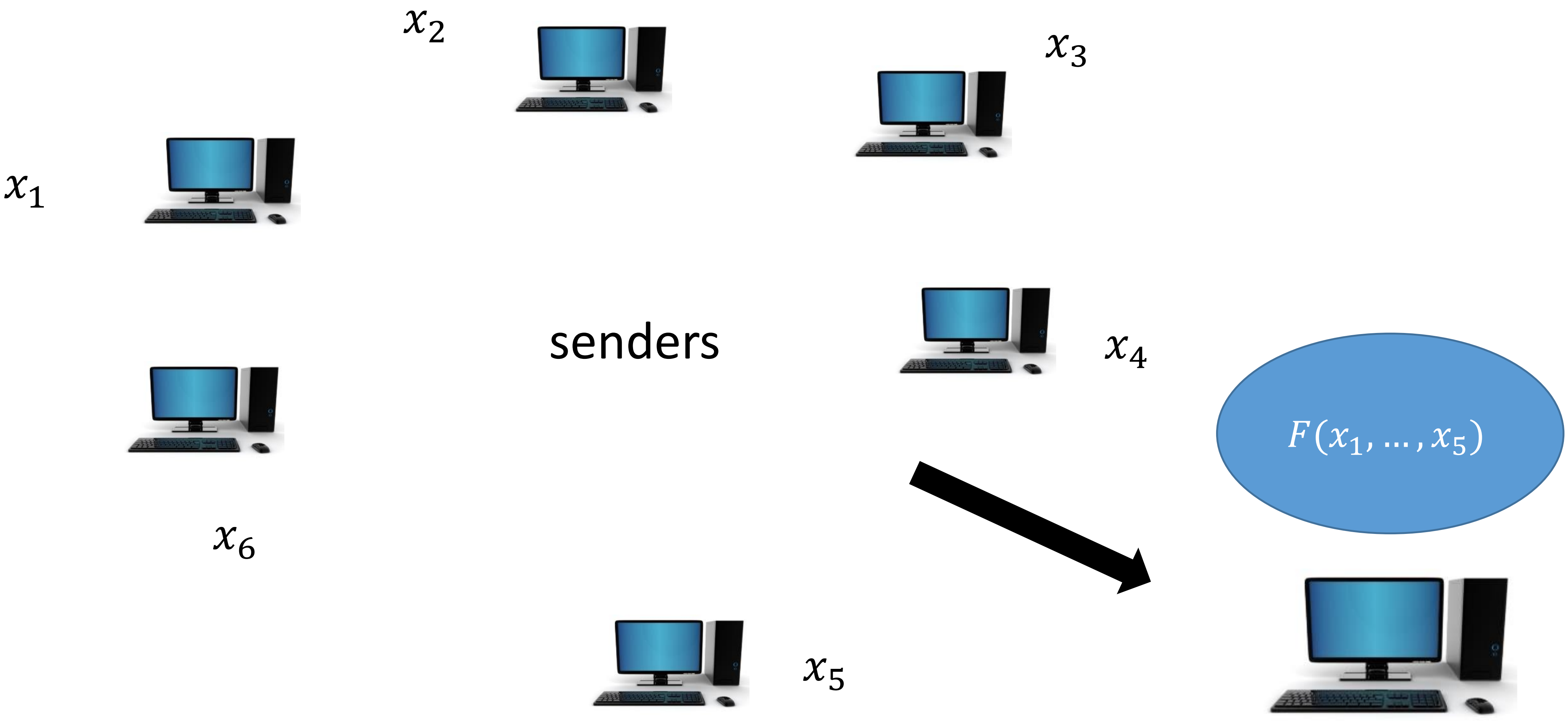
x_6

x_5

prover

Randomized Encoding & Constant-Round MPC

(Benny's Talk)



x_2

x_3

x_1

senders

x_4

$F(x_1, \ldots, x_5)$

x_6

x_5

receiver

Summary: Information Theoretic Cryptography

- Cool questions
- Exciting connections with
  - Coding, Information-theory, Communication Complexity, Computational complexity, Theory of Computation
- Relevant to computational crypto as well
- Many open problems
- New conference: ITC 2020, June 17-19, 2020 in Boston
  - PC: Daniel Wichs, General Chairs: Adam Smith & Yael Kalai

Have a Good Time!