Information-Theoretic Security

EE 25N, Science of Information

11/08/2018

Ziv Goldfeld

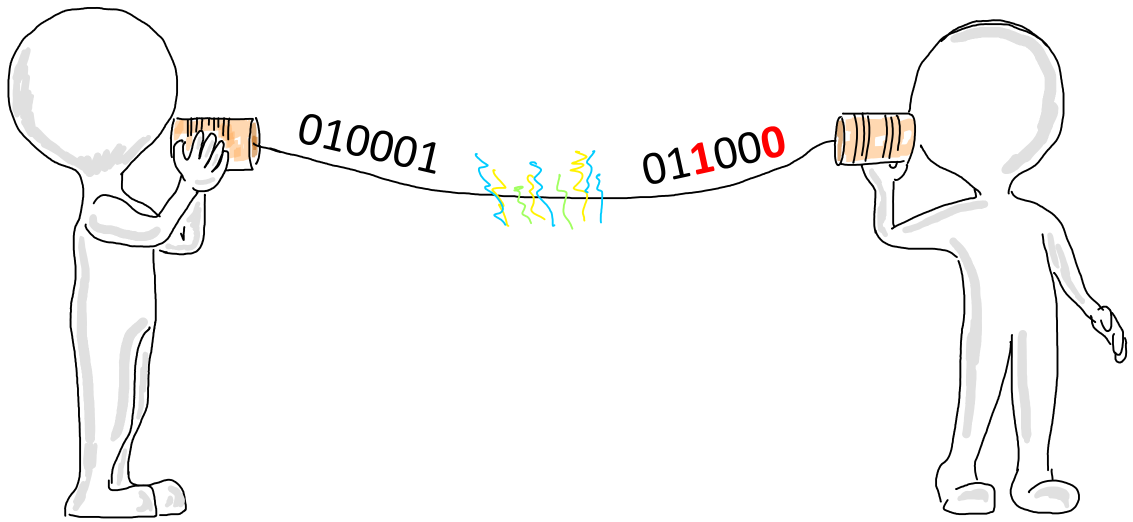
Past Lectures - Communication Despite Noise

- Alice the <u>sender</u> and Bob the <u>receiver</u>
- Communicate a **message** as a strings of 0’s and 1’s (bits)
- Use **longer** bit strings (**codewords**) to protect **message** carrying bits
- Agree on a strategy beforehand:

    1) Set of codewords used

    2) Encoding for Alice

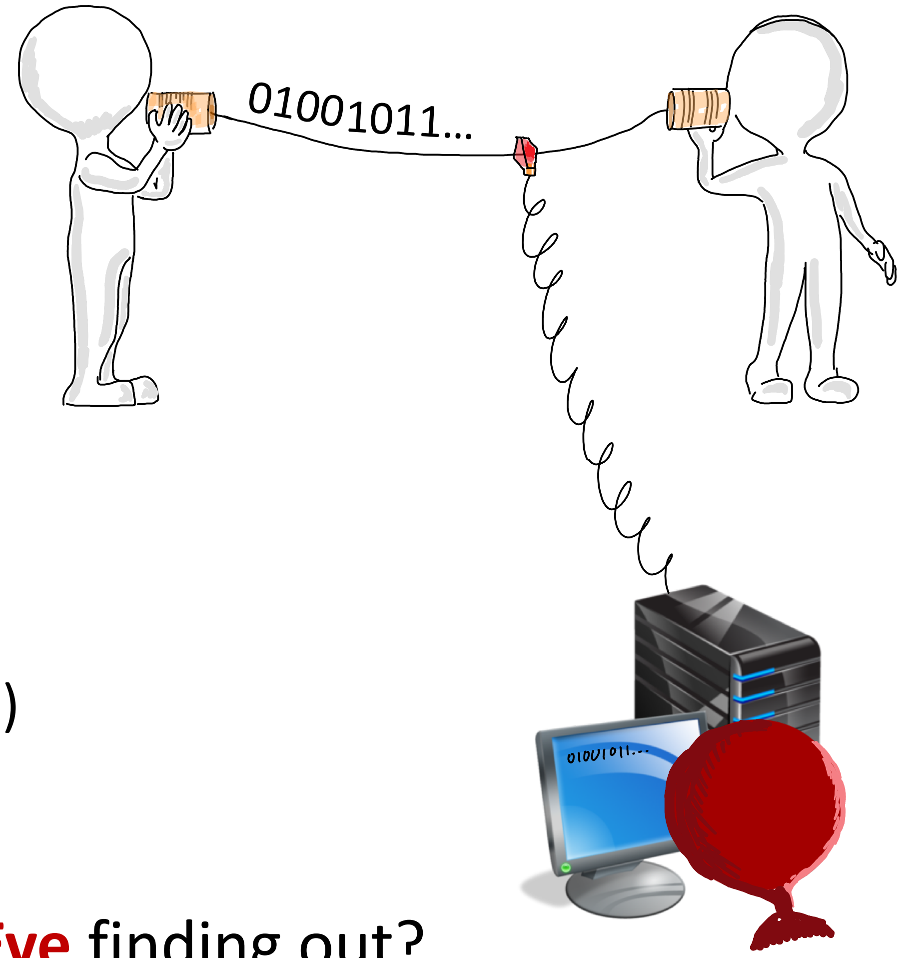
    3) Decoding for Bob



⇒ **Error correcting codes** for reliability

Communication under Eavesdropping

- Alice and bob wish to communicate
- Channel is noiseless
- But Eve taps their line
- They don't want Eve to decipher their chat



- Assumptions on Eve:
  1) She sees their transmitted bit string
  2) She knows their communication strategy (aka code)
  3) She has an extremely powerful computer

Q: Can Alice send Bob a secret message without Eve finding out?

A: Not without an additional recourse!

Resource 1: Pre-Eve Secret

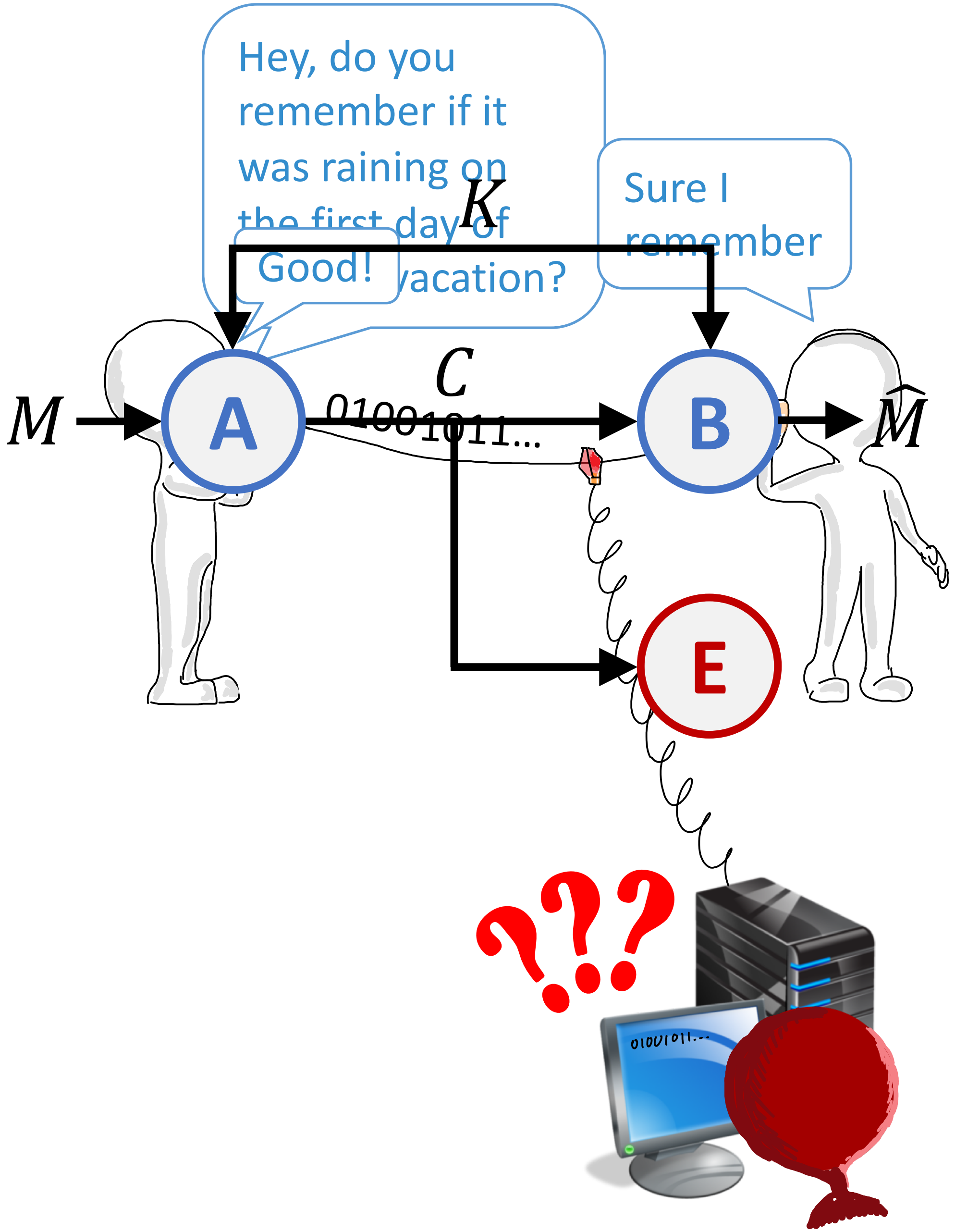
Simple Case Study

- **Alice** sends **Bob** a bit $M \in \{0,1\}$

  Bit probability: $P_M(0) = P_M(1) = \frac{1}{2}$

- They share a secret **Eve** has no access to

$\Rightarrow$ **Resource:** 1 secret bit $K \in \{0,1\}$



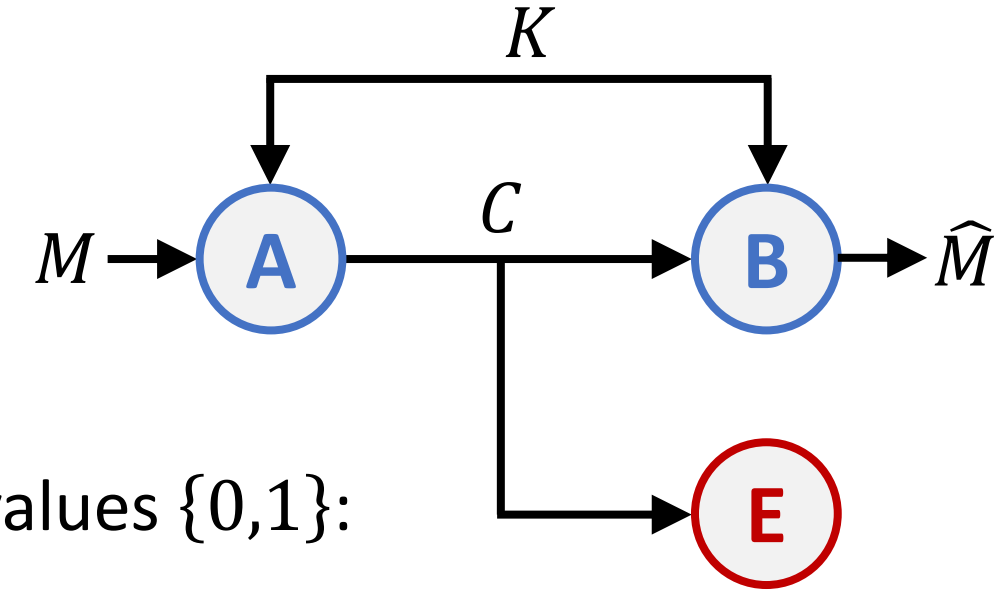
<u>Formally:</u>

Alice: $(M, K) \rightarrow C$

Bob: $(C, K) \rightarrow \hat{M}$

Eve: Intercepts C and tries to figure out M

Simple Case Study – Modeling Eve



Q1: How to model **Eve**'s perception of K?

- Knows K is being used
- Doesn't know its value

$\Rightarrow$ **Eve** has a **guessing probability** over K's values $\{0,1\}$:

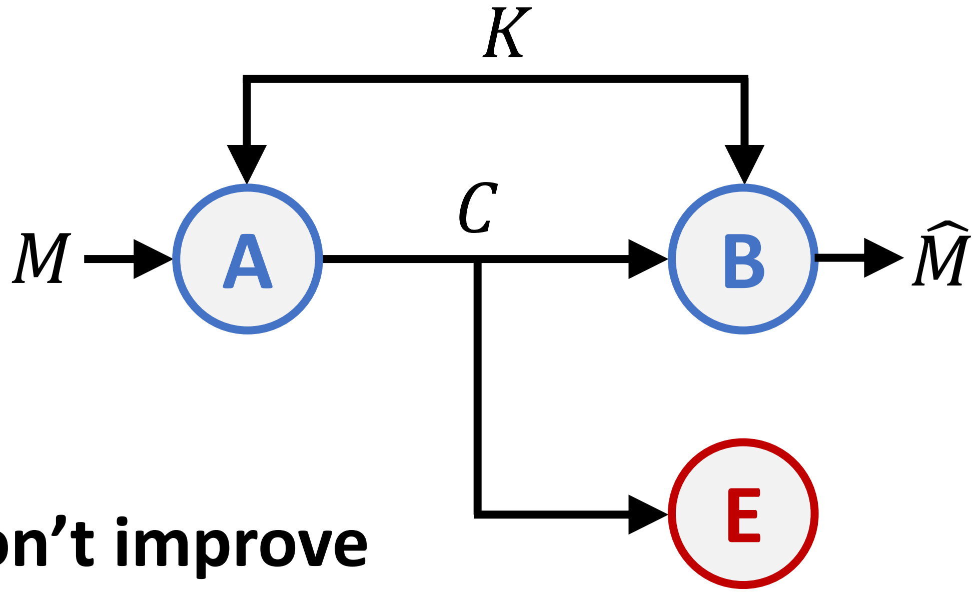
- Doesn't have a clue:
- Knows something:

Q2: Which kind of secret should **Alice** and **Bob** favor?

Simple Case Study – Modeling Security

Q3: What does it mean to secure M?

- Pre-transmission: $P_M(0) = P_M(1) = \frac{1}{2}$
- **Eve** tries to recover M from C



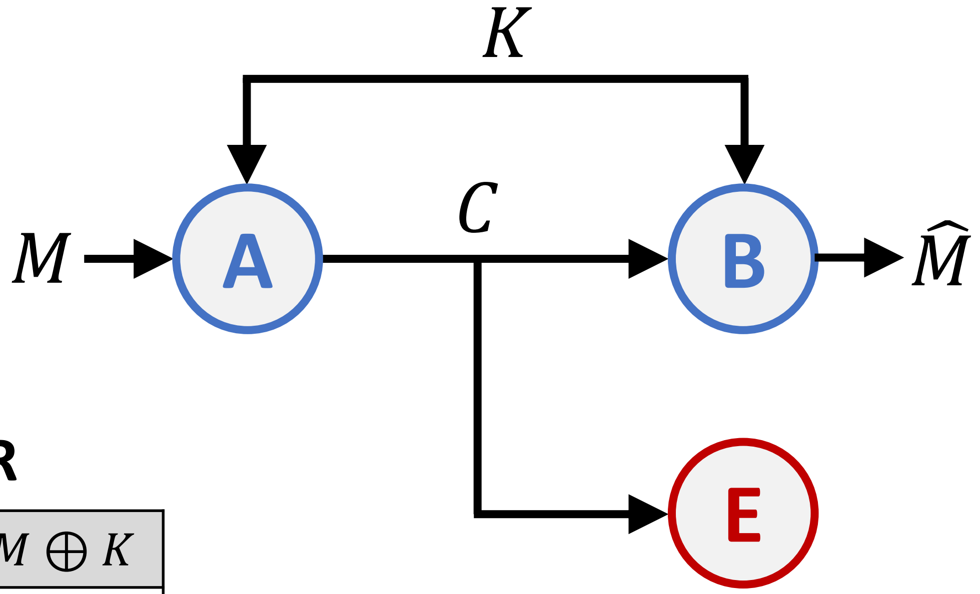
$\Rightarrow$ M is secure if **after** seeing C **Eve**'s odds **don't improve**

<u>Goal:</u> Design functions for **Alice** and **Bob** such that:

- **Bob** can decode M from (C, K)
- **Eve**'s best guess of M **after** seeing C is still 50/50

Simple Case Study – Binary Operations

- Assume M and K are both symmetric (50/50)
- **Alice** gets C via binary operation on (M, K)
- <u>Possible binary operations:</u>



OR

M	K	$M + K$
0	0	0
0	1	1
1	0	1
1	1	1

AND

M	K	$M \cdot K$
0	0	0
0	1	0
1	0	0
1	1	1

XOR

M	K	$M \oplus K$
0	0	0
0	1	1
1	0	1
1	1	0

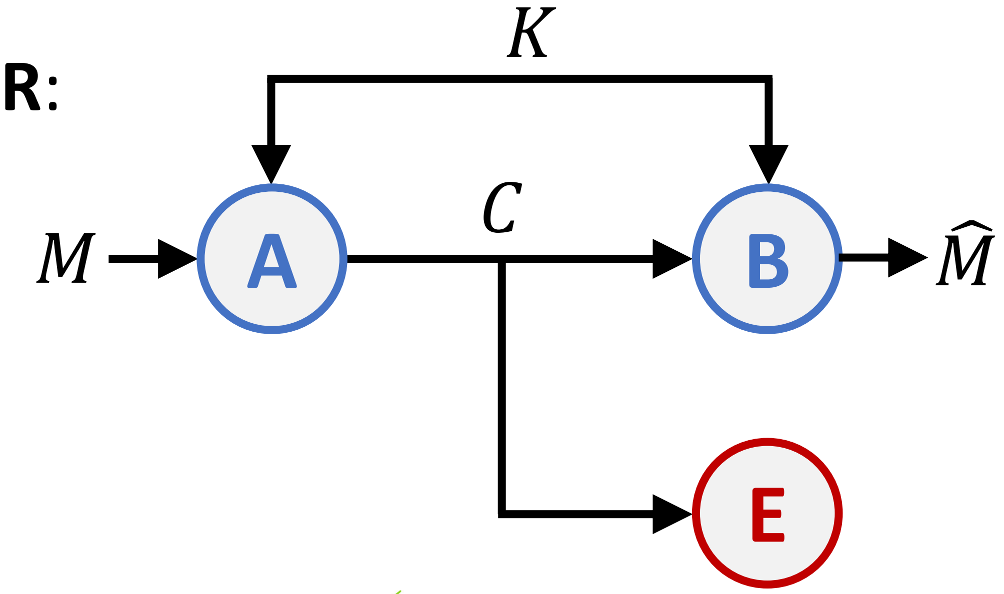
Q4: Which binary operation is better for secrecy?

Simple Case Study – Reliability & Optimality

⇒ Best function for symmetric (M, K) is **XOR**:

- **Eve**'s best guess after seeing C is 50/50
- **Same** odds like **before** seeing C

⇒ Information-theoretic security ✓



Q4: Can **Bob** decode an **XOR**–based transmission? ✓

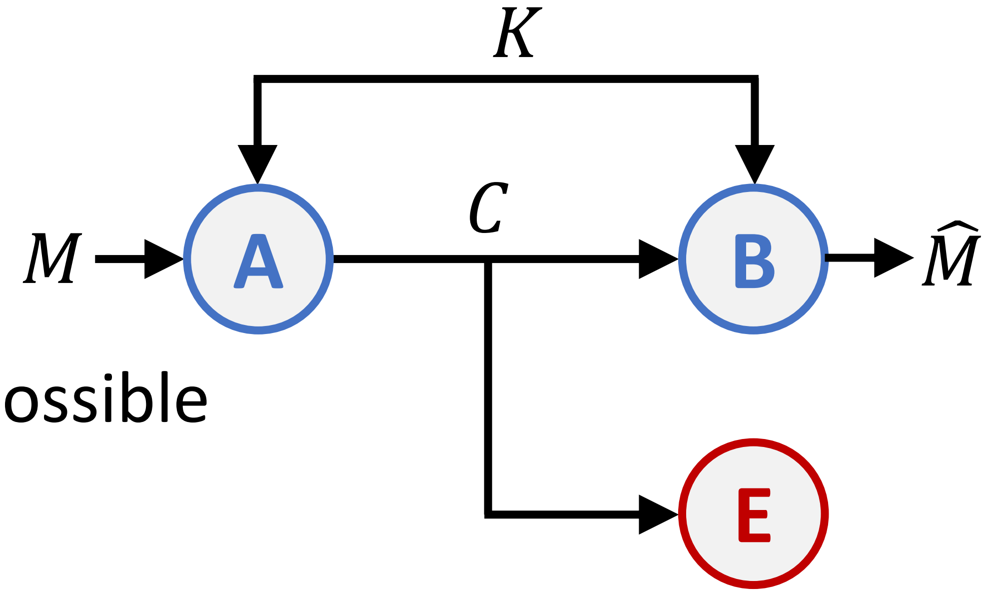
Q5: Can **OR** or **AND** operations be used for communication only? ✗

<u>**Symmetry is Crucial:**</u> Asymmetric keys can't achieve security with **XOR**

Simple Case Study – General Claim

One-Time Pad:

- m messages bits and k key bits
- All bits are equiprobable
- k^* = least k s.t. secure communication is possible



Shannon (1949):

Achieving reliability & information-theoretic security over the OTP is:

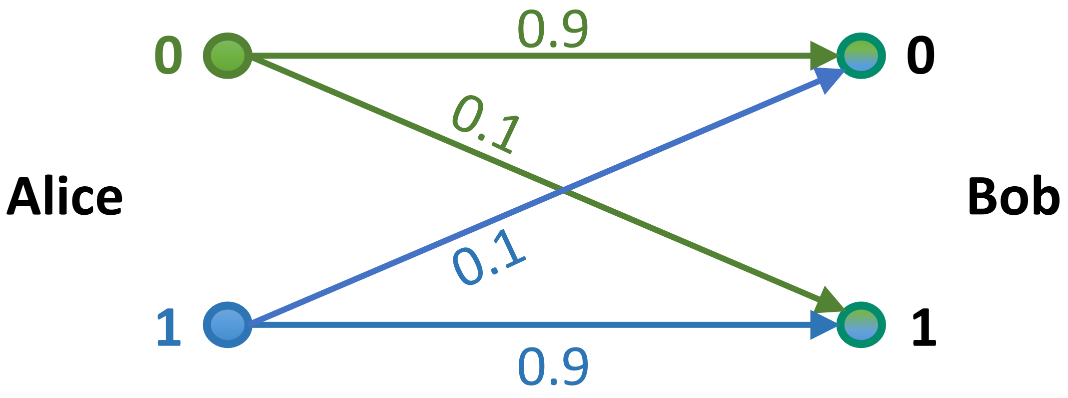
1) **possible** using exactly m key bits
2) **impossible** using less than m key bits

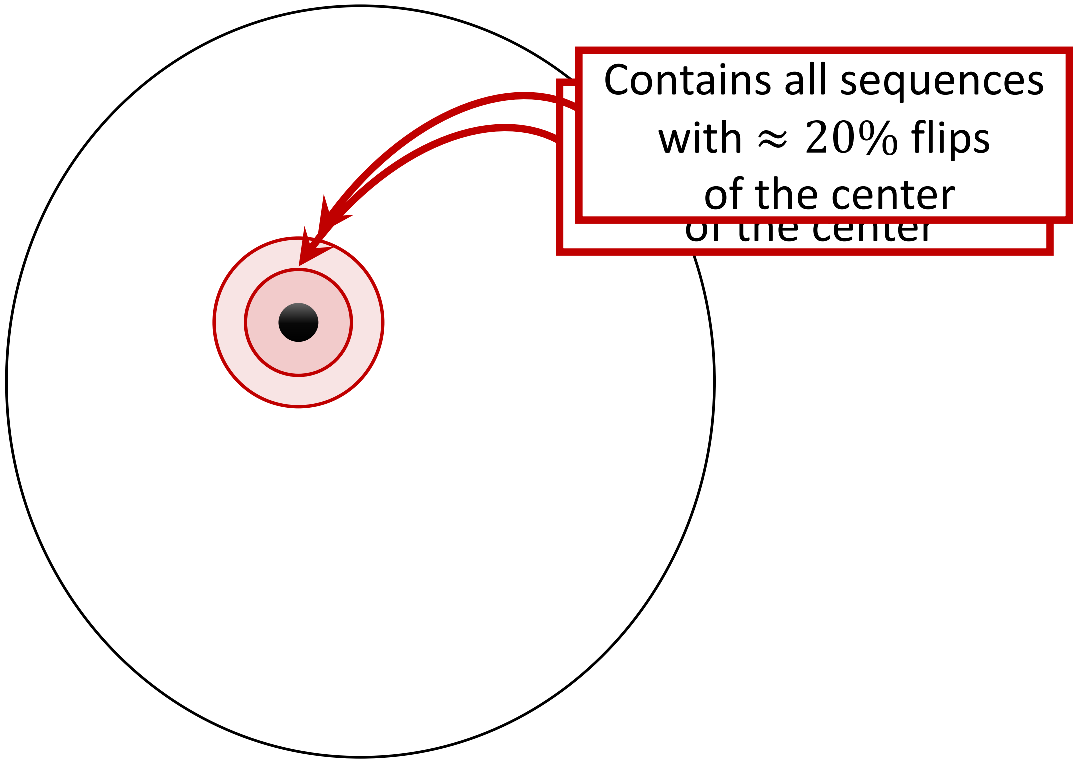
$$\boxed{k^* = m}$$

Resource 2: Noise

Noisy Channel

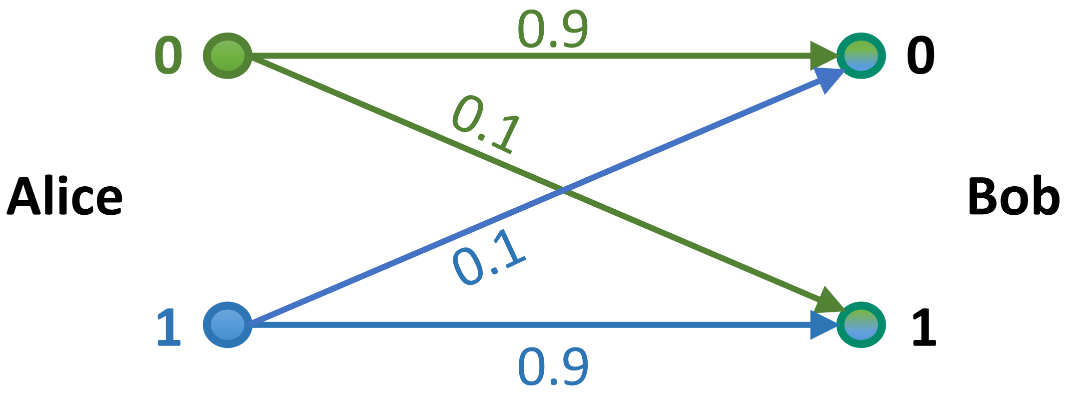
- In most real-world systems we don't exactly know the number of bit flips
- Common mode of operation is to model noise probabilistically

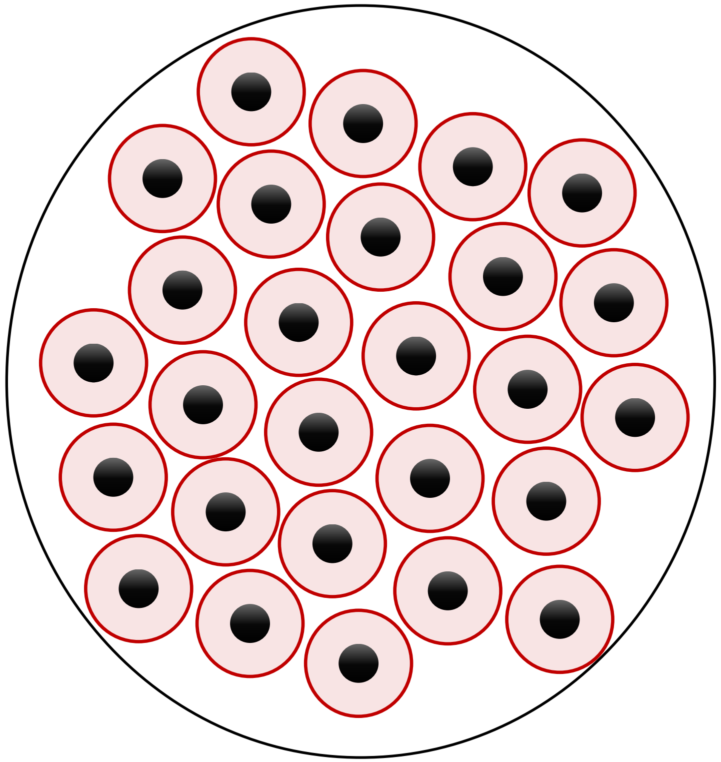




Noisy Channel

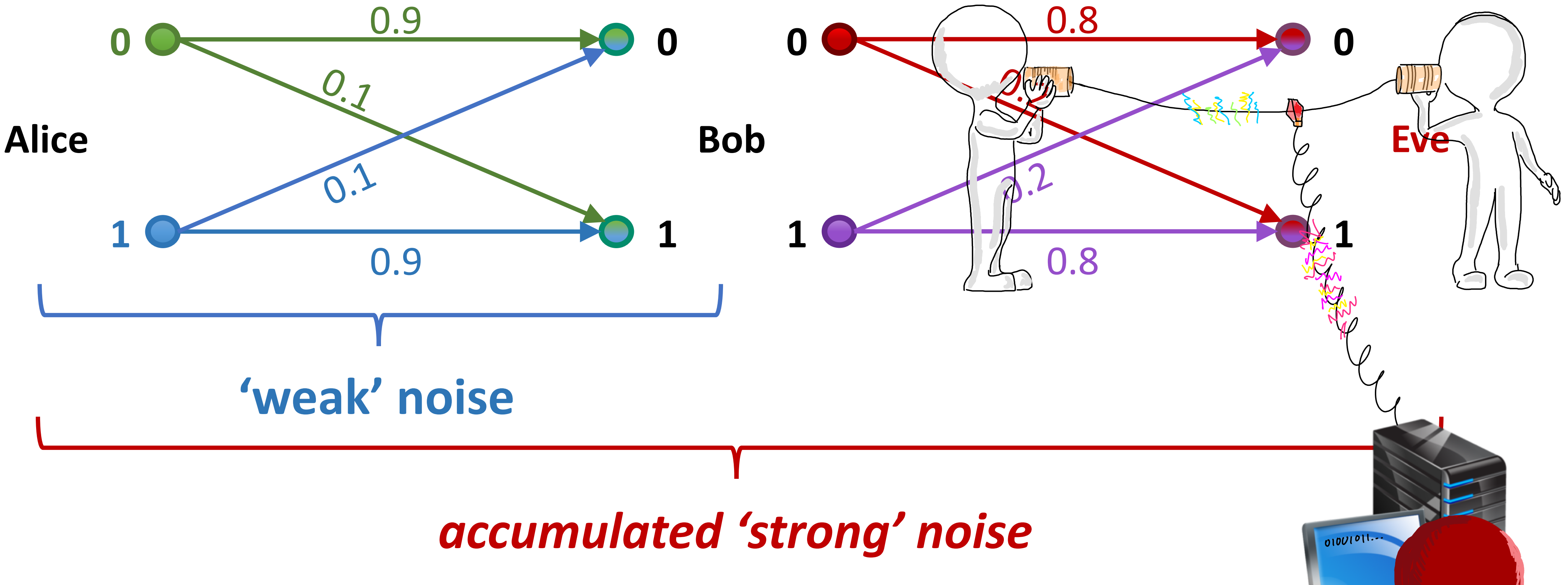
- In most real-world systems we don't exactly know the number of bit flips
- Common mode of operation is to model noise probabilistically





Wiretap Channel

Noisy communication channel with an eavesdropper



⇒ We can exploit **Eve**'s extra noise for securing the transmitted message!

Information-Theoretic Security Research

Many interesting research questions:

1) Key agreement over noisy channels
2) Active Adversaries
   - **Eve** not only overhear the transmission but can influence the channel
   - Has a set of possible actions **Alice** and **Bob** know
   - They don’t know which action is chosen $\Rightarrow$ Ensure security versus all actions!
3) Covert Communication:
   - Communicate without **Eve** noticing
4) Many many many many more…