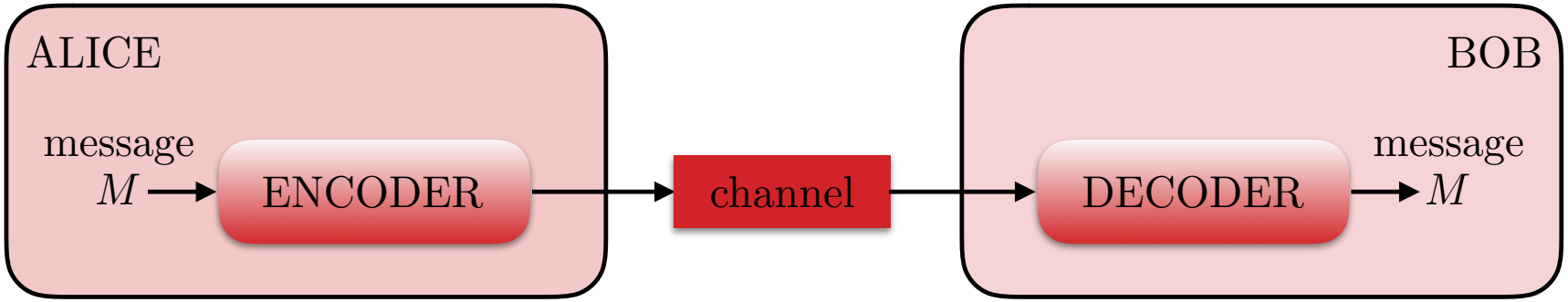
1. Introduction and Overview

Traditional Approach



- Security (e.g. public key encryption) *"on top"*

➠ *Conditional security* only under certain assumptions such as

  - complexity
  - limited computational power of eavesdroppers

Traditional Approach

- Security (e.g. public key encryption) *"on top"*
- *Conditional security* only under certain assumptions such as
  - complexity
  - limited computational power of eavesdroppers

Traditional Approach

- Security (e.g. public key encryption) *"on top"*
- *Conditional security* only under certain assumptions such as
  - complexity
  - limited computational power of eavesdroppers

Traditional Approach

- Security (e.g. public key encryption) *"on top"*

➠ *Conditional security* only under certain assumptions such as

  - complexity
  - limited computational power of eavesdroppers

Cryptographic Security

- Recently, there are huge developments in algorithmic and number theory
  - Public Key Cryptography – **RSA method**:
    Scientific American 1977: secure for 40×10^{15} years!
  - **In 1994 it was demonstrated it takes only 6 months to decrypt the encrypted text!**
  - In 2002 it was shown that the question "*Is a number a prime number or not?*" is easily to answer algorithmically!
  - Recently, the NSA successfully spied on Angela Merkel!
- Unfortunately, algorithmic advances cannot always be compensated by improved hardware
- There is no information available about "*algorithmic knowledge*" of enemies and criminals

➠ Cryptographic security is **technology dependent**!

Paradigm Shift for Future System Design

- *Embedded security:* Integrate protocols on the physical layer for certain specified and guaranteed security

➠ New concept of **physical layer security** / **information theoretic security**

Shannon's Secrecy System

- Roughly speaking, the objective of secure communication is twofold:
  1. Intended receivers should recover the message without errors
  2. **Nobody else should acquire any information**

Formalized by Shannon in 1949 using the model of a secrecy system

Fig. 1. Schematic of a general secrecy system

C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949

Shannon's Secrecy System

- Roughly speaking, the objective of secure communication is twofold:
  1. Intended receivers should recover the message without errors
  2. **Nobody else should acquire any information**

Formalized by Shannon in 1949 using the model of a secrecy system

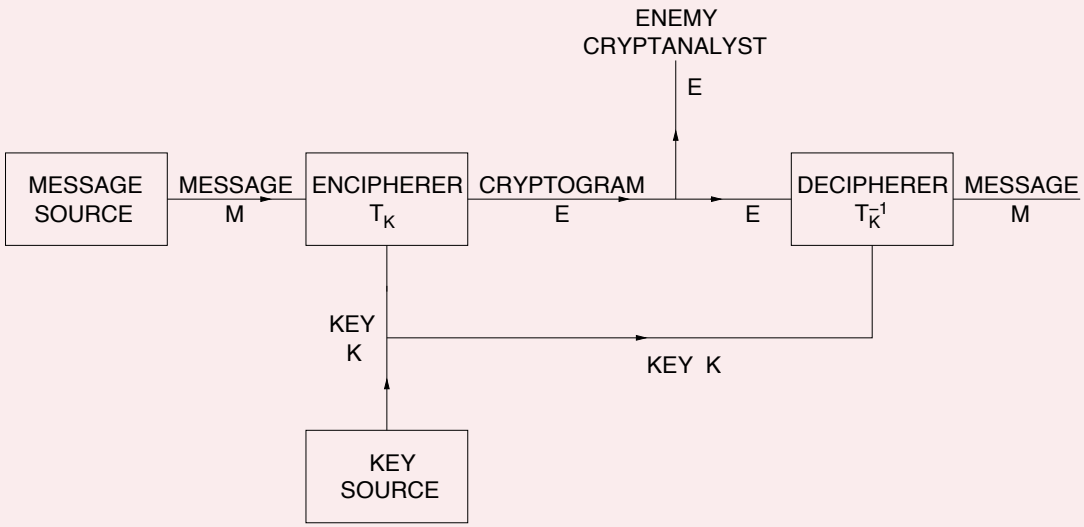
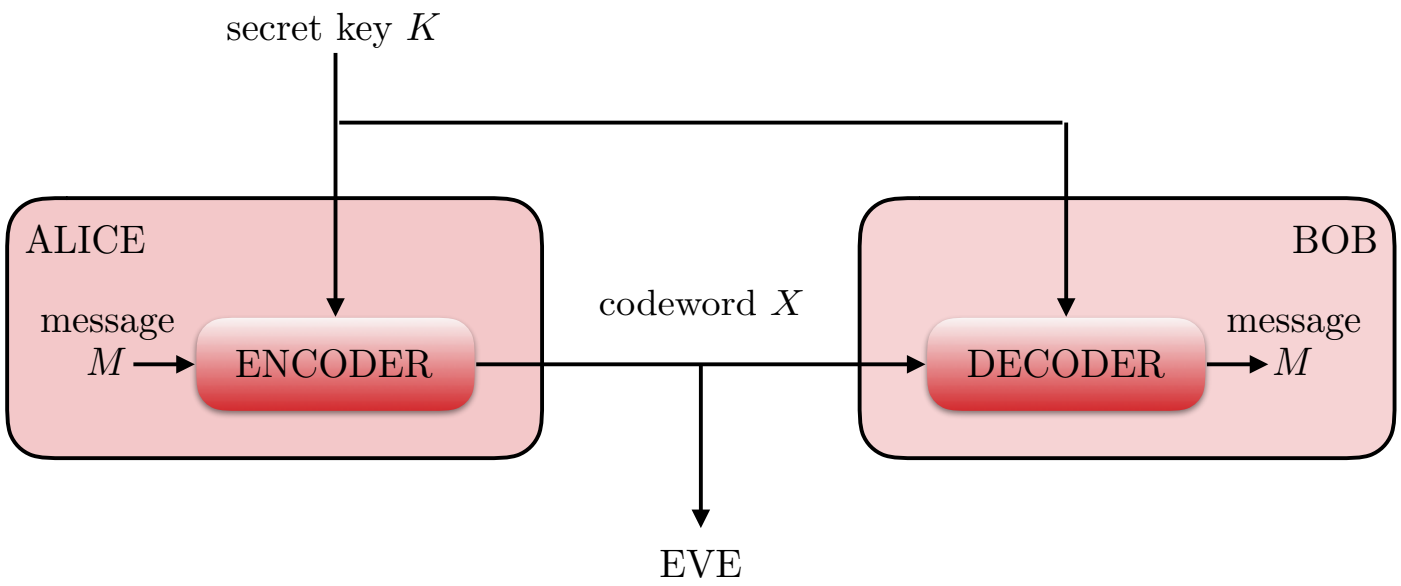


Fig. 1. Schematic of a general secrecy system

C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949

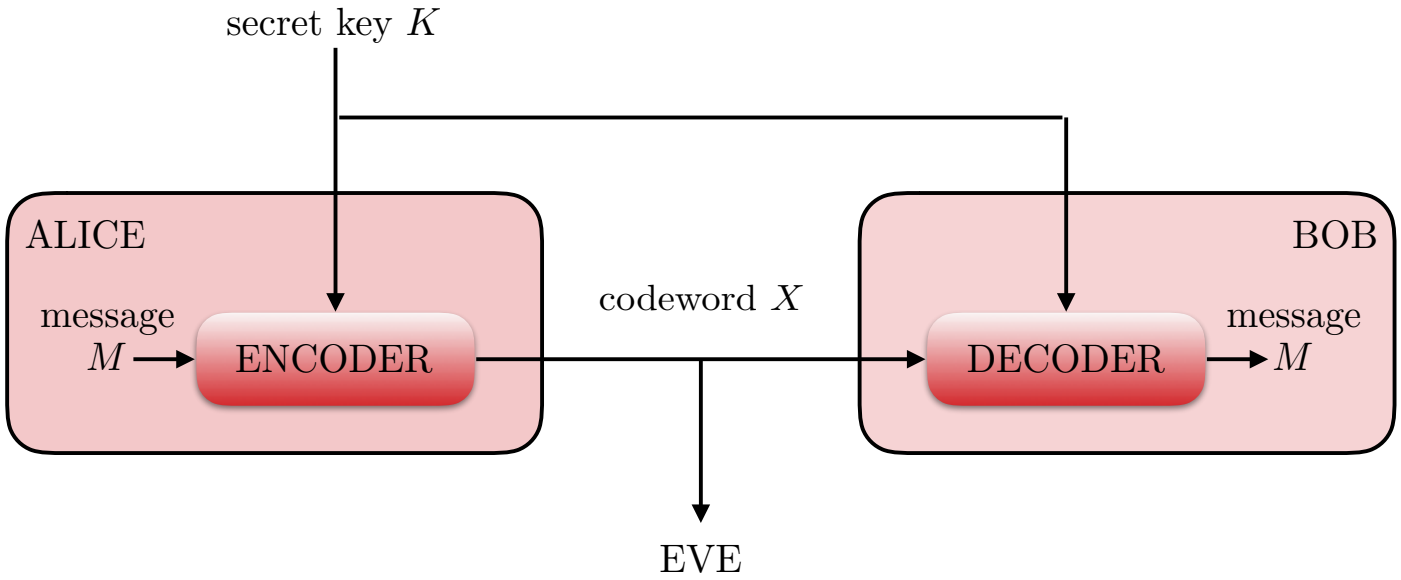
Shannon's Secrecy System



- Transmitter (ALICE) attempts to send message M to a legitimate receiver (BOB) by encoding it into a *codeword* X
- Codeword is observed by an eavesdropper (EVE) without any degradation
  - Worst-case scenario of an error-free communication channel
  - In real systems, this corresponds to the existence of error-correction mechanisms, which allow recovery with arbitrarily small probability of error

➠ BOB must have **some advantage over EVE**, otherwise EVE would be able to **recover M as well**!

Shannon's Secrecy System



- Solution lies in the use a **secret key K known only to ALICE and BOB**

➠ Codeword X is then obtained by computing a function of the message M and the secret key K

Perfect Secrecy

- Shannon formalized the notion of secrecy by quantifying the average uncertainty of the eavesdropper
- In information-theoretic terms
  - message and codewords are treated as random variables
  - secrecy is measured in terms of conditional entropy of the message given the codeword: $H(M|X)$ (also called *equivocation*)

- **Perfect secrecy** is achieved if the eavesdropper's equivocation equals the a-priori uncertainty one could have about the message, i.e.,

$$H(M|X) = H(M)$$

- **Codeword X is statistically independent of the message M.**
- There exists no algorithm that would allow the eavesdropper to extract any information about the message

Perfect Secrecy

- Shannon formalized the notion of secrecy by quantifying the average uncertainty of the eavesdropper
- In information-theoretic terms
  - message and codewords are treated as random variables
  - secrecy is measured in terms of conditional entropy of the message given the codeword: $H(M|X)$ (also called *equivocation*)

➠ **Perfect secrecy** is achieved if the eavesdropper's equivocation equals the a-priori uncertainty one could have about the message, i.e.,

$$\boldsymbol{H(M|X) = H(M)}$$

➠ **Codeword X is statistically independent of the message M.**

➠ There exists no algorithm that would allow the eavesdropper to extract any information about the message

One-Time Pad

- We will see that this is only possible if $\boldsymbol{H(K) \geq H(M)}$, i.e., uncertainty about the key must be at least as large as the uncertainty about the message
- In other words, we must have at least **one secret bit for every bit of information** contained in the message
- From an algorithmic perspective, perfect secrecy can be achieved by means of a simple procedure called *one-time pad*.
- Binary example:

Message	M	0	1	0	1	0	0	0	1	1	0	1
Key	K	1	0	0	1	1	0	0	0	1	0	1
Codeword	$X = M \oplus K$	1	1	0	0	1	0	0	1	0	0	0

- Codeword X is formed by computing the binary addition (XOR) of each message bit M with a separate key bit K, i.e., $X = M \oplus K$
- If the key bits are independent and uniformly distributed, the codeword is statistically independent of the message

One-Time Pad

- We will see that this is only possible if $\boldsymbol{H(K) \geq H(M)}$, i.e., uncertainty about the key must be at least as large as the uncertainty about the message
- In other words, we must have at least **one secret bit for every bit of information** contained in the message

- From an algorithmic perspective, perfect secrecy can be achieved by means of a simple procedure called *one-time pad*.
- Binary example:

Message	M	0	1	0	1	0	0	0	1	1	0	1
Key	K	1	0	0	1	1	0	0	0	1	0	1
Codeword	$X = M \oplus K$	1	1	0	0	1	0	0	1	0	0	0

- Codeword X is formed by computing the binary addition (XOR) of each message bit M with a separate key bit K, i.e., $X = M \oplus K$
- If the key bits are independent and uniformly distributed, the codeword is statistically independent of the message

Drawbacks

- Although the one-time pad can achieve perfect secrecy with low complexity, its application is limited:
  - The legitimate partners must generate and store long keys consisting of random bits
  - Each key can be used only once (otherwise the eavesdropper has a fair chance of discovering the key)
  - The key must be shared over a secure channel
- To overcome this, we could be tempted to generate long pseudo-random sequences using a smaller seed
  - However, information theory shows that the uncertainty of the eavesdropper is upper bounded by the number of random key bits used
  - The smaller the key the greater the probability that the eavesdropper will succeed in extracting some information from the codeword
  - In this case, the only obstacle faced by the eavesdropper is computational complexity, which leads directly to the concept of **computational security**

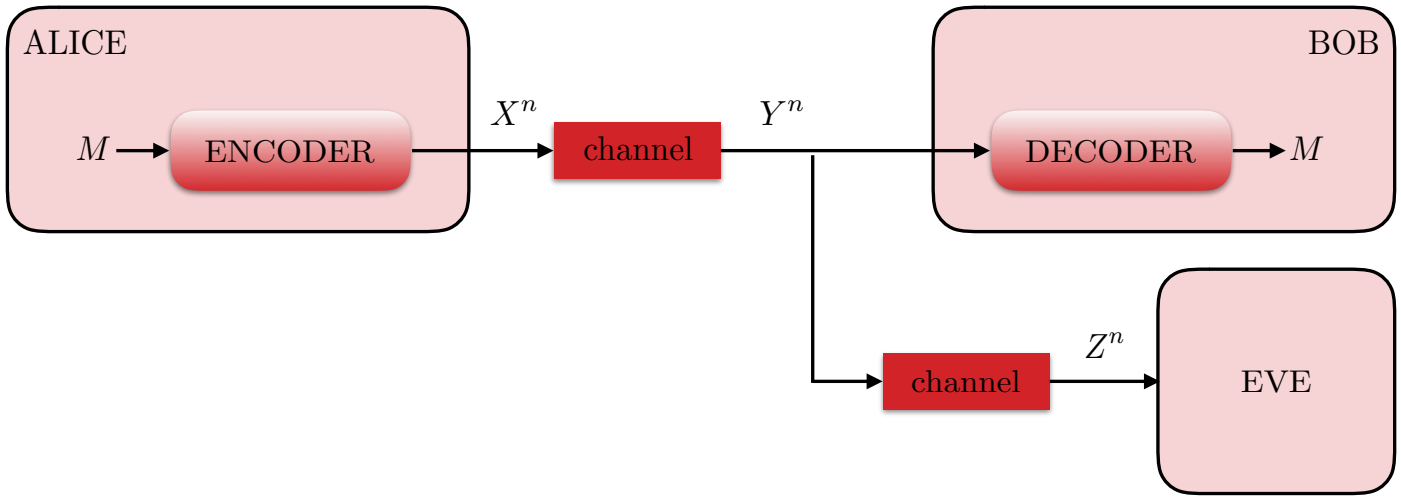
➠ These caveats are responsible for the skepticism with which security practitioners dismiss the usefulness of information-theoretic security

Drawbacks

- Although the one-time pad can achieve perfect secrecy with low complexity, its application is limited:
  - The legitimate partners must generate and store long keys consisting of random bits
  - Each key can be used only once (otherwise the eavesdropper has a fair chance of discovering the key)
  - The key must be shared over a secure channel
- To overcome this, we could be tempted to generate long pseudo-random sequences using a smaller seed
  - However, information theory shows that the uncertainty of the eavesdropper is upper bounded by the number of random key bits used
  - The smaller the key the greater the probability that the eavesdropper will succeed in extracting some information from the codeword
  - In this case, the only obstacle faced by the eavesdropper is computational complexity, which leads directly to the concept of **computational security**

➠ These caveats are responsible for the skepticism with which security practitioners dismiss the usefulness of information-theoretic security

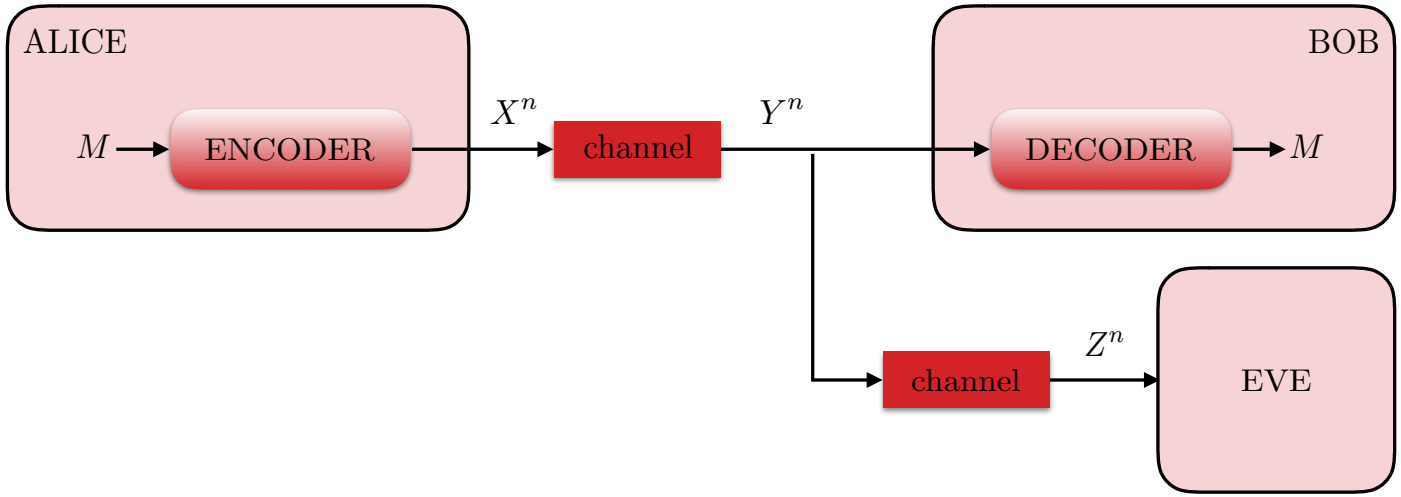
Secure Communication Over Noisy Channels



- Random noise is an intrinsic element of almost all physical communication channels
- To understand its role in the context of secure communications, Wyner introduced in 1975 the *wiretap channel*

A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975

Secure Communication Over Noisy Channels



- Main differences to Shannon's original secrecy system are:
  - The legitimate transmitter encodes a message M into a codeword X^n consisting of n symbols which is sent over a noisy channel to the legitimate receiver
  - The eavesdropper observes a noisy version, denoted by Z^n, of the signal Y^n available at the receiver

A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975

Secure Communication Over Noisy Channels

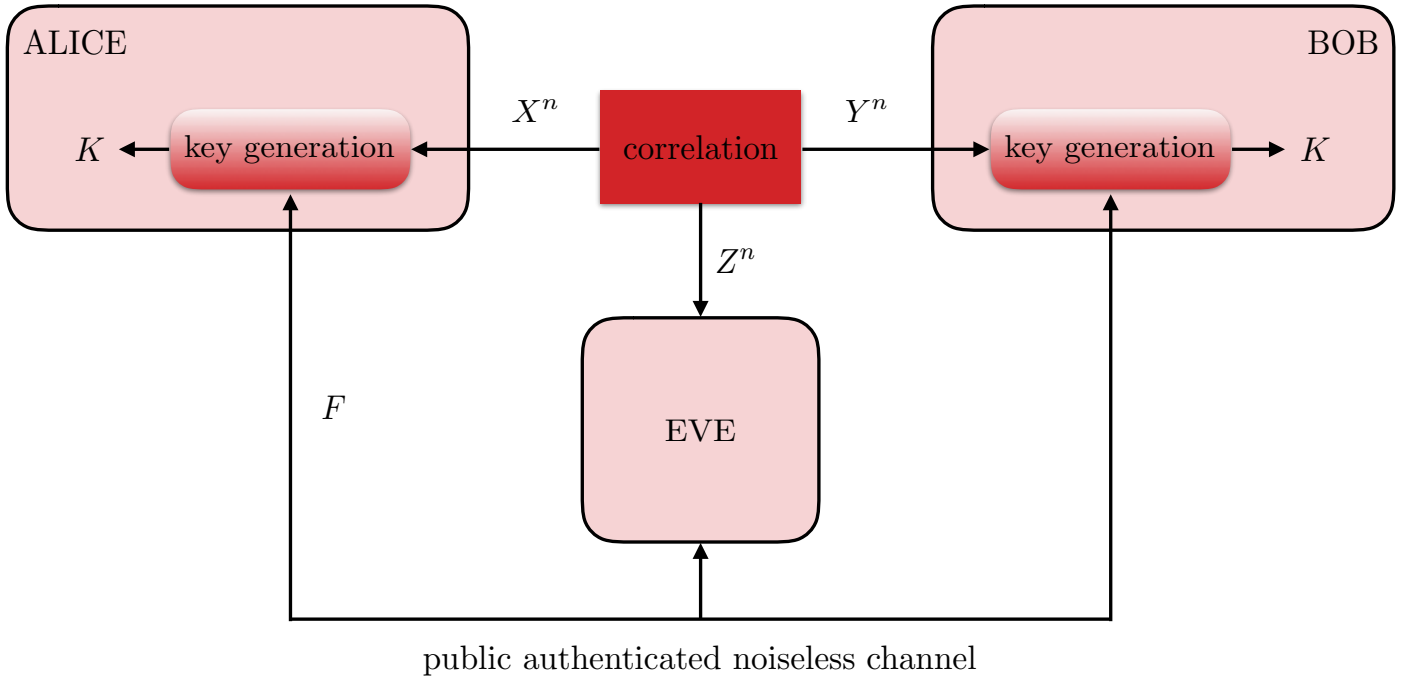
- In addition, Wyner suggested a new definition for the secrecy condition. Instead of requiring the eavesdropper's equivocation to be exactly equal to the entropy of the message, we now ask for the *equivocation rate*

$$\frac{1}{n} H(M|Z^n)$$

  to be arbitrarily close to the entropy rate of the message $\frac{1}{n}H(M)$ for sufficiently large codeword length n

- It can be shown that there exist channel codes (so-called *wiretap codes*) that *asymptotically* guarantee both an arbitrarily small probability of error at the intended receiver and secrecy.
- Maximum transmission rate that is achievable under these premises is called *secrecy capacity*
- It can be shown to be strictly positive whenever the eavesdropper's observation Z^n is "noisier" than Y^n

Secret-Key Agreement From Noisy Observations

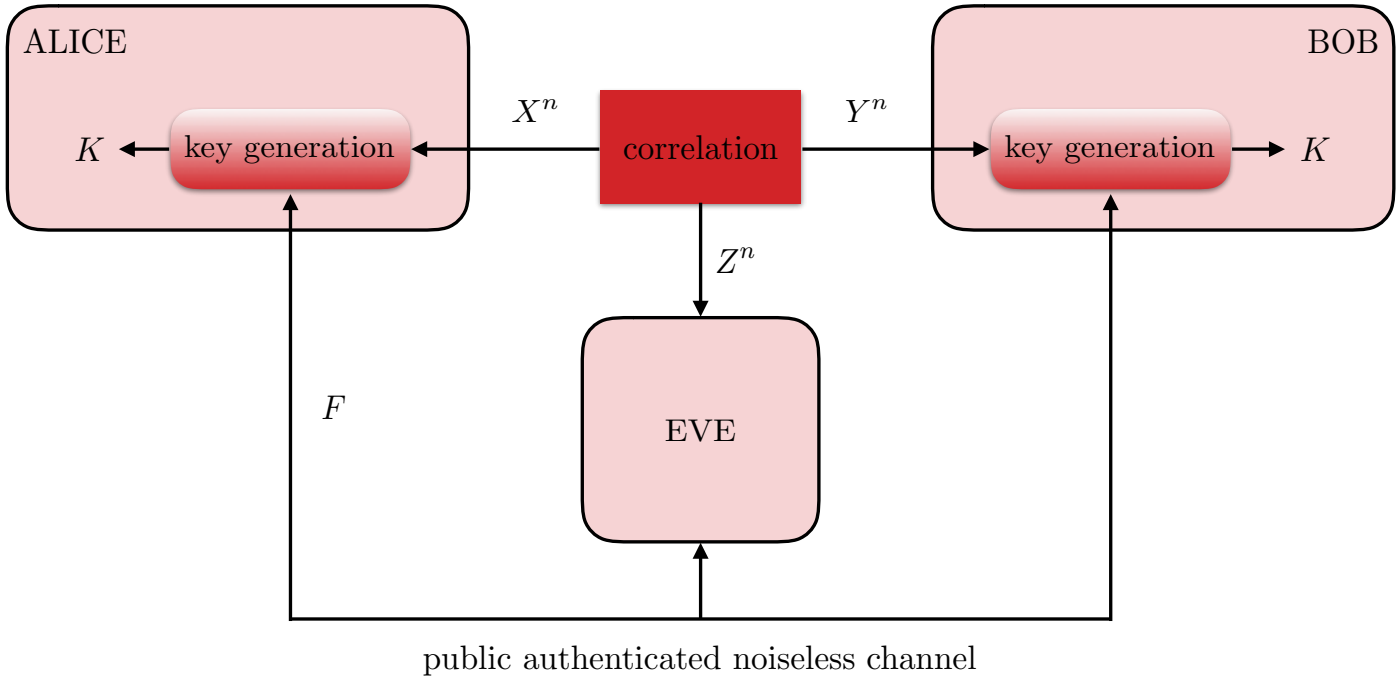


- Instead of communicating a secret message straight away, *ALICE and BOB generate a secret key* instead
- First discussed by Ahlswede/Csiszár and Maurer in 1993

R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography—Part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993

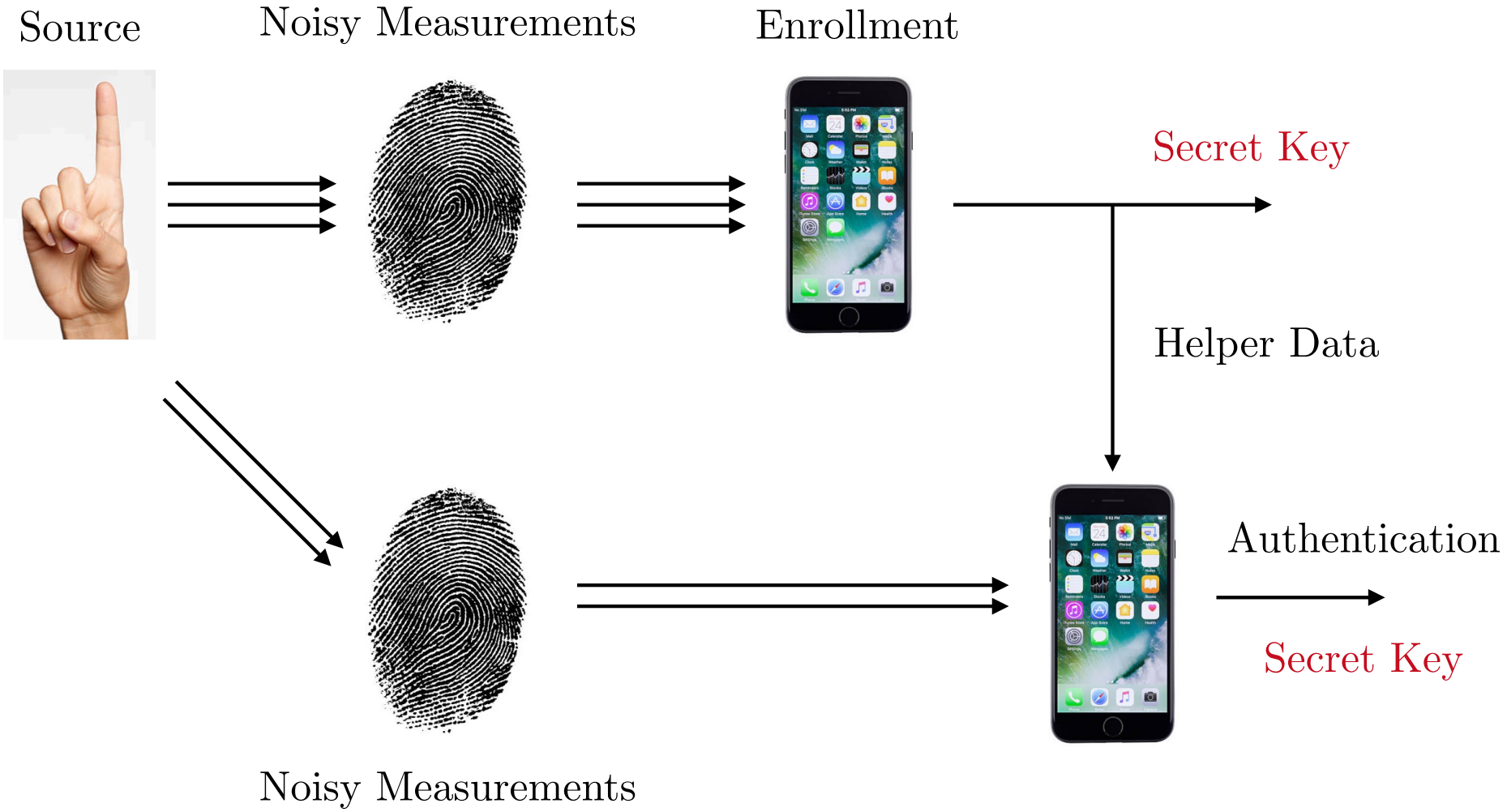
U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993

Secret-Key Agreement From Noisy Observations

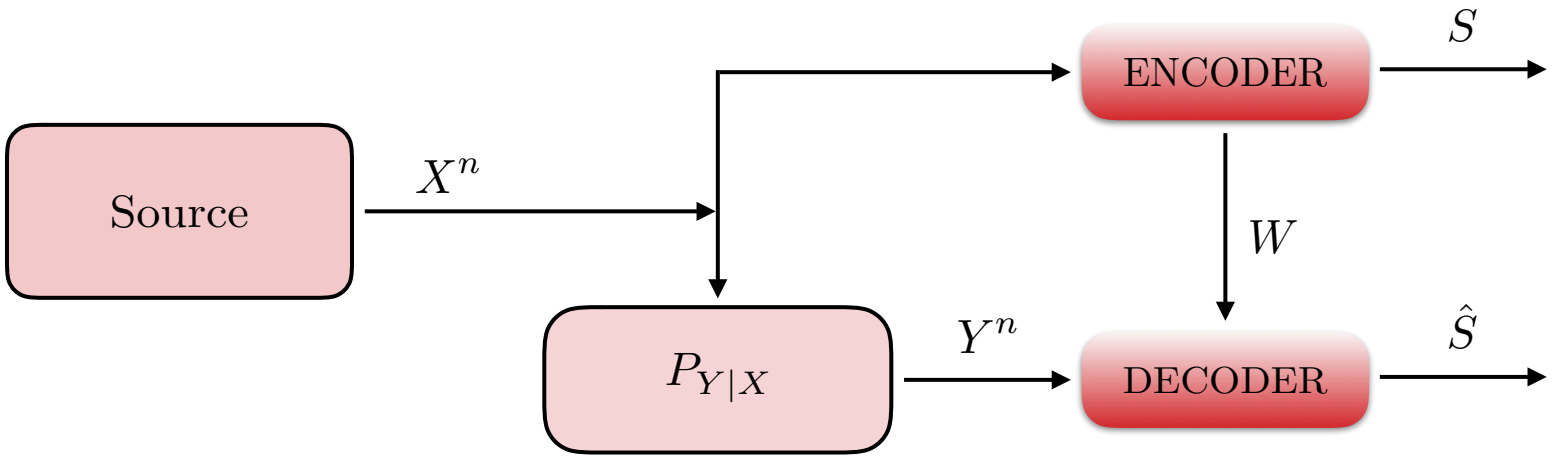


- ALICE, BOB, and EVE obtain correlated observations X^n, Y^n, and Z^n
- ALICE and BOB then generate a key K based on their observations and a set of messages F exchanged over the error-free public channel
- Even if F is available to EVE, key generation is possible such that $H(K|Z^n, F)$ is arbitrarily close to $H(K)$

Biometric Authentication

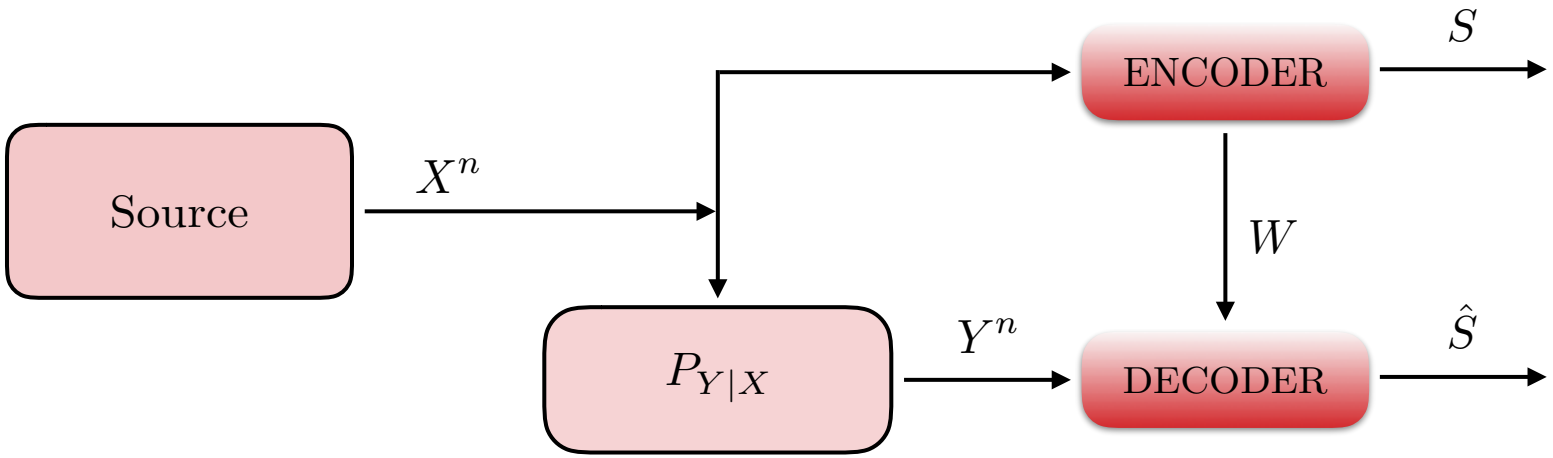


Biometric Authentication



- Secret key with rate R_s
- Public helper data with rate R_w
- Leakage rate $R_l = \frac{1}{n} I(X^n; W)$
- Requirements:
  - *Reliability:* error probability $P_e = \mathbb{P}[\hat{S} \neq S]$ should be **small**
  - *Secrecy:* S should be independent of W and R_s **large**
  - *Privacy:* leakage rate R_l should be **small**
  - *Storage:* storage rate R_w should be **small**

Biometric Authentication



- Secret key with rate R_s
- Public helper data with rate R_w
- Leakage rate $R_l = \frac{1}{n} I(X^n; W)$
- Requirements:
  - *Reliability:* error probability $P_e = \mathbb{P}[\hat{S} \neq S]$ should be **small**
  - *Secrecy:* S should be independent of W and R_s **large**
  - *Privacy:* leakage rate R_l should be **small**
  - *Storage:* storage rate R_w should be **small**

Privacy

INSIDER

Jacob Shamsian, INSIDER

Sep. 17, 2016, 1:11 PM 4,755

Private Information Retrieval (PIR)

Anonymity: hide Alice's identity

PIR: Hide Alice's queries

Alice

Mr. Supreme Leader

Private Information Retrieval (PIR)

"We're using algorithms to protect users privacy when accessing, sharing and searching data in the cloud. Imagine being able to search Google without revealing to Google what you're searching for. It sounds impossible, but it's not."

Salim El Rouayheb, Mar 2017.

Differential Privacy

Aggregate via Differential Privacy

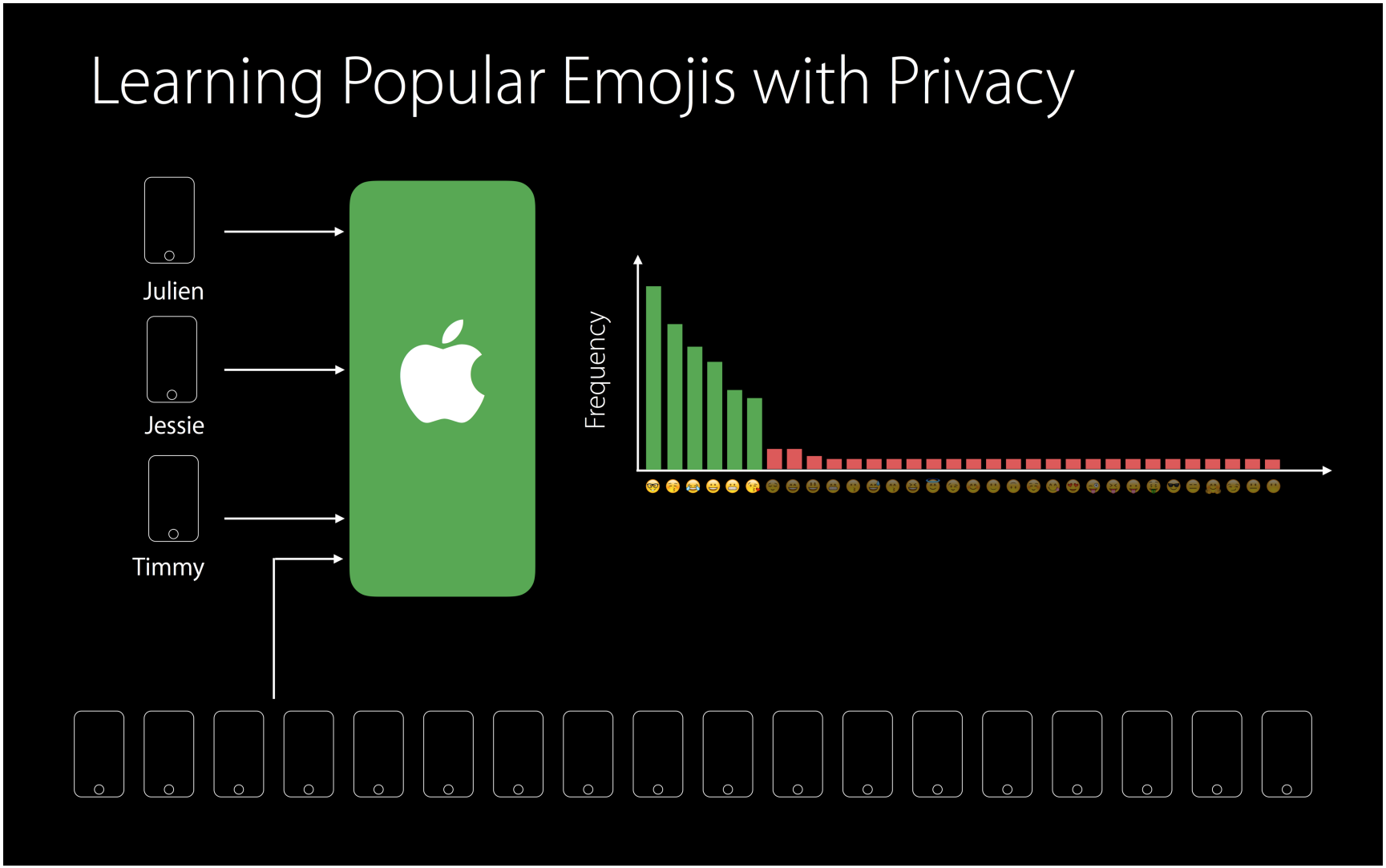
NEW

Learn from crowd while protecting individual privacy

Strong mathematical guarantees

iOS and macOS

Differential Privacy



Differential Privacy

Idea