
Lecture 1: Course Overview

-COMP 6712 Advanced Security and Privacy

Haiyang Xue

haiyang.xue@polyu.edu.hk

2022/1/10

COMP 6712 Advanced Security and Privacy

- Hello
- It is the first time this course is taught at PolyU.
- Of course, it is also my first time to teach this course.
- I believe it is also your first time to take
- In the following 4 months, hope we will learn together....

Communication

- haiyang.xue@polyu.edu.hk find the instructor Haiyang XUE
- TA: Mengling LIU, 22117804r@connect.polyu.hk
- TA: Xun LIU, compxun.liu@connect.polyu.hk
- **Blackboard**
 - We will use **Blackboard** for announcements
 - Use this to reach all course staff and students
- Zoom: the link and password posted in Blackboard

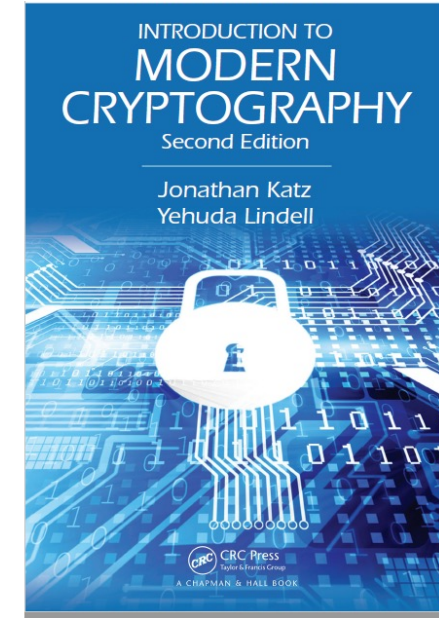
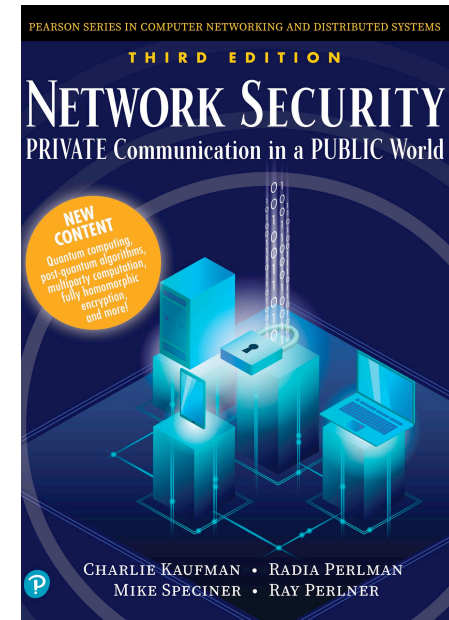
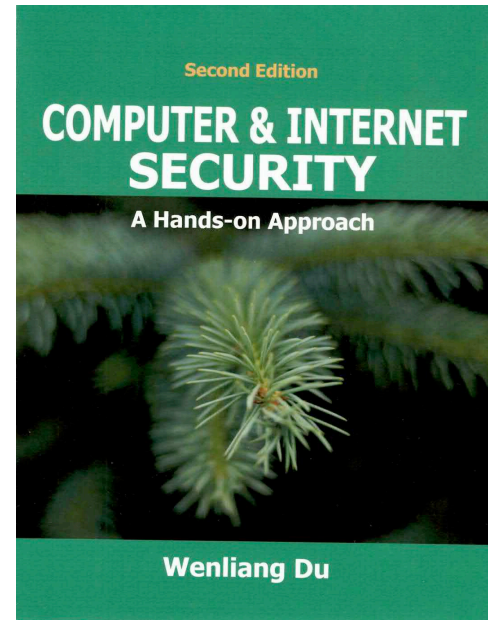
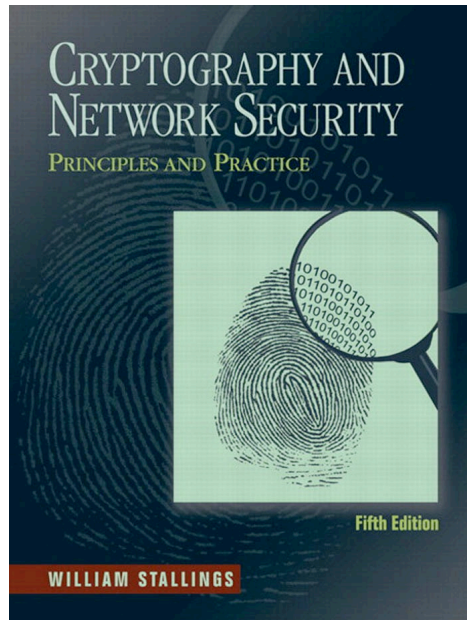
Course website

- <https://haiyangxc.github.io/hyxue/teaching/comp6712-23.html>
- Almost everything: syllabus, grading, final exam...
- I will continuously update slides/lecture notes/readings on the website

2022/23 Semester 2 Department of Computing, PolyU				
General Information				
<ul style="list-style-type: none">• Venue: BC302• Time: Tuesday, 18:30-21:20, week 1-13• Instructor: Haiyang Xue, haiyang.xue@polyu.edu.hk• TA:				
Outline				
This course will cover the most important features of security and privacy issues. The topics include network security, computer security and privacy-preserving computation (aka secure computation), and relevant knowledge in basic cryptography and advanced privacy-enhancing technologies. Two case studies of security and privacy in Blockchain and AI are also included. Refer to the syllabus for details.				
Updating Announcements				
Syllabus				
The syllabus is subject to change, and I will continuously update it as the semester progresses.				
Date	Topics/slides	Outline	Readings	Lecture notes
Week 1: Jan 10	Course Overview	course plan, reading materials, grading, brief introduction to every topic	[Sta] William Stallings, Cryptography and Network Security: Principles and Practice [Du] Wenliang Du, Computer Security: A Hands-on Approach [KPS] Charlie Kaufman, Radia Perlman, and Mike Speciner, Network Security: Private Communication in a Public World [KL] Jonathan Katz, and Yehuda Lindell, Introduction to Modern Cryptography	
Week 2: Jan 17	Basic Cryptography 1: Symmetric-key cryptography	symmetric encryption, one-time pad, blockcipher, hash function, MAC, authenticated encryption.		
Week 3: Jan 31	Basic Cryptography 2: Public-key cryptography	RSA, Diffie-Hellman, public key encryption, Digital signature		
		authenticated key exchange, PKI, and		

Course Materials: text books

- [Sta] William Stallings, **Cryptography and Network Security: Principles and Practice**
- [Du] Wenliang Du, **Computer Security: A Hands-on Approach**
- [KPS] Charlie Kaufman, Radia Perlman, and Mike Speciner, **Network Security: Private Communication in a Public World**
- [KL] Jonathan Katz, and Yehuda Lindell, **Introduction to Modern Cryptography**



Course Materials: lecture notes

- Google

- [Security and privacy](#) + lecture notes or course or subject
- [Cybersecurity](#) + lecture notes or course or subject
- [Computer security](#) + ...
- [cryptography](#)+

- You may find

- Jonathan Katz, Computer and Network Security
- Ronald Rivest, Network and Computer Security
- Etc.

Course Materials

- Some of my slides are also based on the lecture notes:
 - Jonathan Katz, Computer and Network Security
 - Yoshi Kohno, Computer Security
 - Dan Boneh and John Mitchell, Computer and Network Security
 - etc....
- Thanks to Yoshi Kohno, Dan Boneh, Jonathan Katz, Håkon Jacobsen, and many others for sample slides and materials ...
- Please feel free to use and distribute my slides.

What is Security?

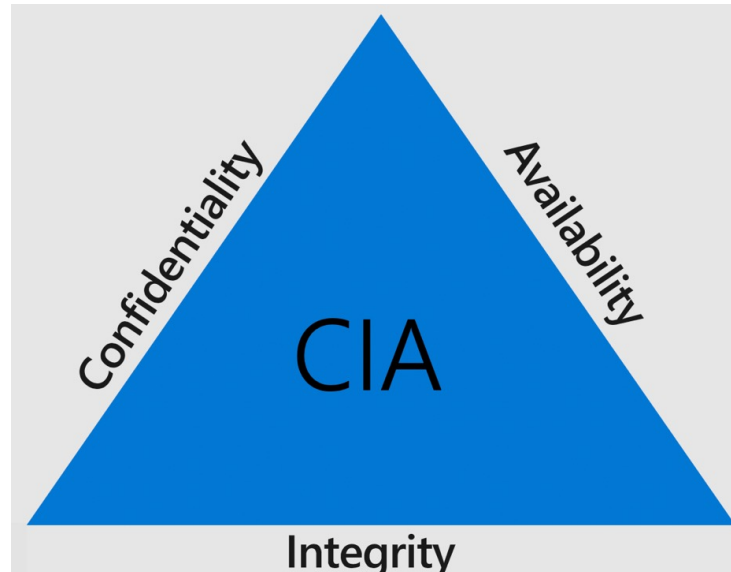
- System Correctness
 - Good input/behavior \Rightarrow Desired output
 - It is better to have more features

- Security
 - Bad input/behaviors $\not\Rightarrow$ Bad output
 - Even attacker supplies unexpected input, system does not fail in certain ways
 - More features \Rightarrow a higher chance of attacks

What is Security?

- **Basic Goals (CIA)**

- **Confidentiality**: Information only available to authorized parties
- **Integrity**: Information is precise, accurate, modified only in acceptable ways, consistent, meaningful, and usable
- **Availability**: Services provide timely response, fair allocation of resources, quality of service



What is Security?



<https://www.bicyclelaw.com/bicycle-safety/how-to-lock-your-bike/>

What is Privacy?

- Generally, security concerns on protecting data from internal and external attackers,
- While privacy focuses on the use and governance of (personal) data
 - Data is shared and used properly



<https://www.varonis.com/blog/data-privacy>

What is Privacy?

- Assume Alice is a millionaire; Bob is also rich
- Security
 - Who want to steal my money? And how
 - Who want to destroy my money? And how
 - How to protect the money?
- Privacy
 - They want to know who is richer,
 - but do not want to leak how much money they have (i.e., x , y)



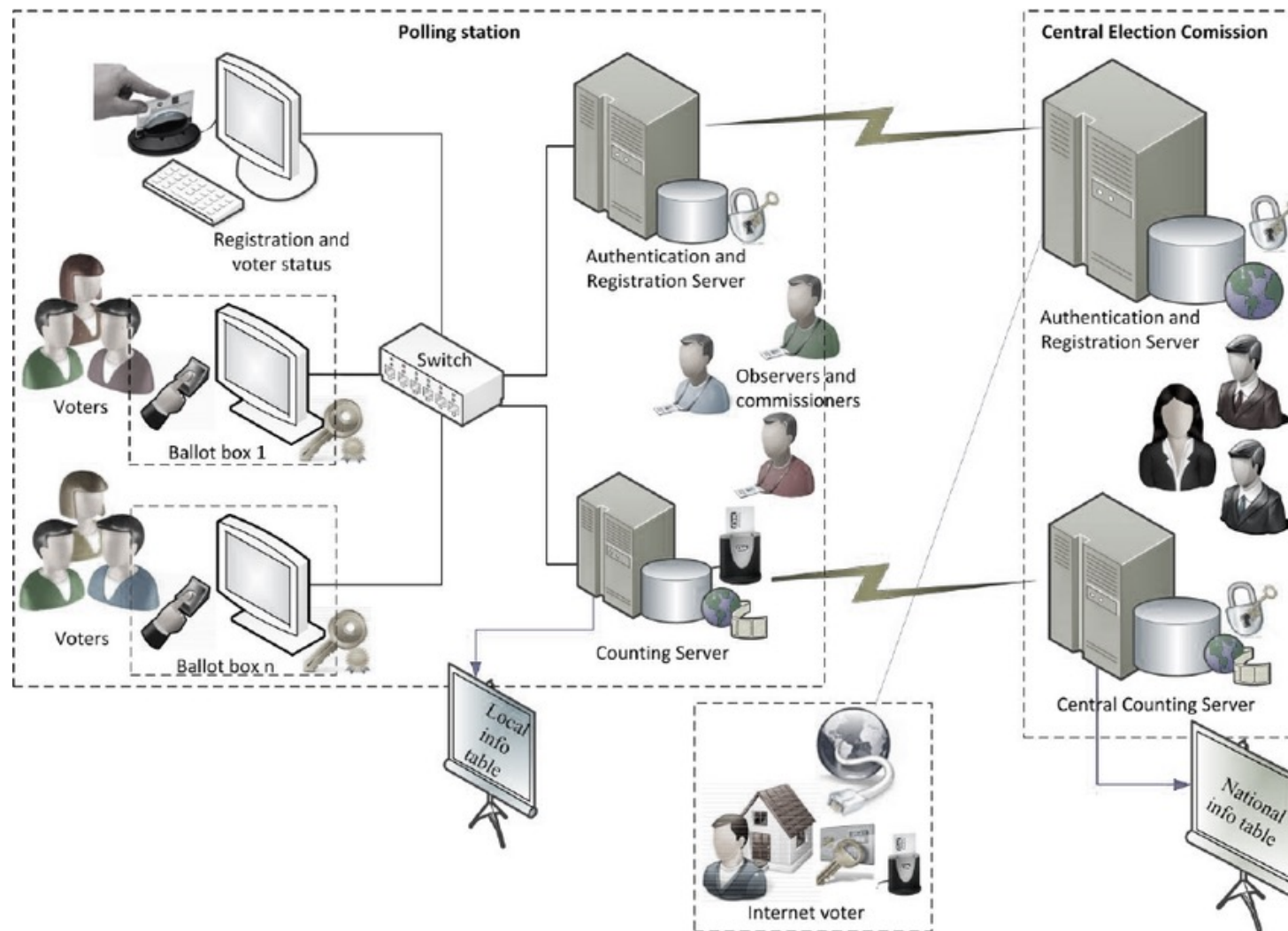
Whose value is greater?



Security and Privacy

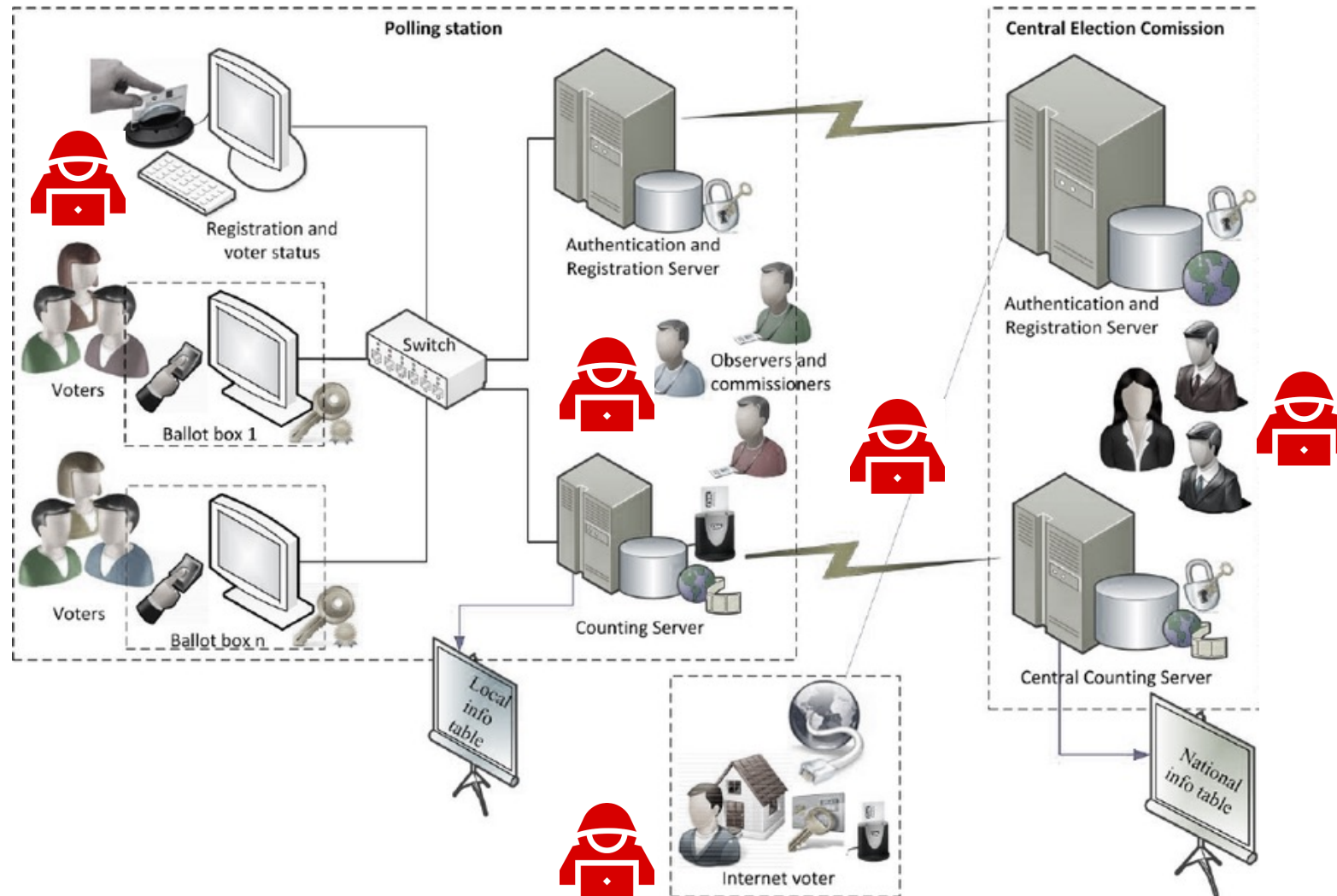
- Privacy and security are generally intertwined
- Security problem usually results in the leakage of data
 - Login in your Facebook, WeChat, WhatsApp account ---> (person info)
 - hack in your iphone ---> (private communication)
 - etc....
- Weakness of privacy may lead to efficient attacks
 - Face/fingerprint recognition ---> login iphone
 - Birthday, family number, ID ---> password of bank account

An Example: Electronic Voting (e-voting)



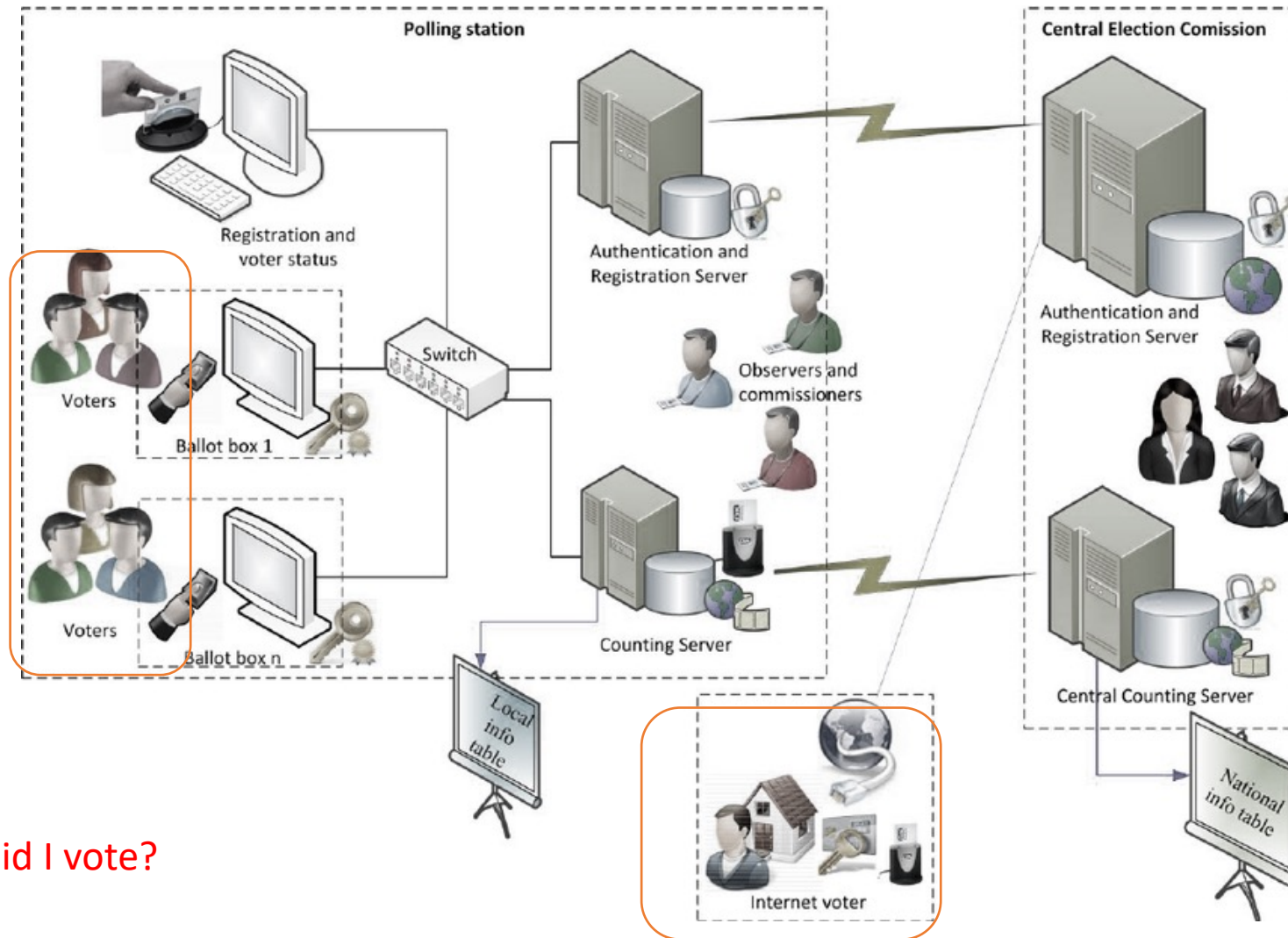
An Example: Electronic Voting (e-voting)

- Security



An Example: Electronic Voting (e-voting)

- Privacy



Who did I vote?

What this course is **NOT** about

- **NOT** a comprehensive course on security and privacy
 - security and privacy are broad topics.
 - Impossible to cover everything in a course
 - Encouraged to present a new topic
- **NOT** about all the latest attacks
 - We do not catch the latest attacks in this lecture
 - Encouraged to present new and great attacks
- **NOT** about ethical, legal, or economic issues

What this course is about

- Introduction to security and privacy
 - Basic tools and recent development to achieve security and privacy
- focus on “big-picture” principles and ideas
 - Basic cryptography
 - and network security
 - Advanced privacy-enhancing technologies
- Security and privacy problems in Blockchain and AI
 - The hot topics in Blockchain and AI

Course Plan

- Lectures
 - Lectures do not follow any textbooks
 - Include recent development
- Two Guest Lectures (**planned**)
 - One is on the topic of security and privacy in the Blockchain
 - The other is on security and privacy in AI
- Your final presentation
 - Every student gives a 20-minute presentation on any paper about S & P

Grading

- Assignments (20%)
 - I will post two assignments throughout the course
- Projects: (45%)
 - lecture notes and final presentation
- Final exam (35%)
 - ;) I will post a summary of what you should know about this on the website

Projects

- Final presentation

- Give a 20-minute presentation for any paper from IEEE S&P 18-22, ACM CCS 18-22, USENIX 18-22, NDSS 18-22, CRYPTO 18-22, or EUROCRYPT 18-22
- Send your choice to the TA on or before Mar 27
- The presentation schedule will be given on Mar 28

- Lecture notes

- Every 2~3 students, as a team, should choose and write one lecture note. (16/7)
- I will give an example for week 2. I will also provide readings as a reference.
- Lecture notes for week x should be submitted to TA and me on or before Tuesday of week $x+4$, $x \in \{3,4,5,6,7,8,9\}$
- Revisions may be required.

Course syllabus

Date	Topics	Lecture notes
Week 1: Jan 10	Course Overview	N/A
Week 2: Jan 17	Basic Cryptography 1: Symmetric-key cryptography	Haiyang Xue
Week 3: Jan 31	Basic Cryptography 2: Public-key cryptography	??
Week 4: Feb 7	Network Security Principles	??
Week 5: Feb 14	Network Security in Practice	??
Week 6: Feb 21	Authentication	??
Week 7: Feb 28	Privacy-Enhancing technologies 1	??
Week 8: Mar 7	Privacy-Enhancing technologies 2	??
Week 9: Mar 14	Privacy-Enhancing technologies 3	??
Week 10: Mar 21	Security and Privacy in Practice 1	N/A
Week 11: Mar 28	Security and Privacy in Practice 2	N/A
Week 12: Apr 4	Final presentation 1	N/A
Week 13: Apr 11	Final presentation 2	N/A

Before giving a brief intro to each topic,
I would like to give several helpful resources

Other Resources for learning security and privacy

- Top-tier conferences

- IEEE Security & Privacy, ACM CCS, USENIX, NDSS
- CRYPTO, EUROCRYPT, ASIACRYPT

- eprint

- <https://eprint.iacr.org/>

- GitHub

- <https://github.com/sbilly/awesome-security>
- <https://github.com/qazbnm456/awesome-web-security>
- <https://github.com/matter-labs/awesome-zero-knowledge-proofs>

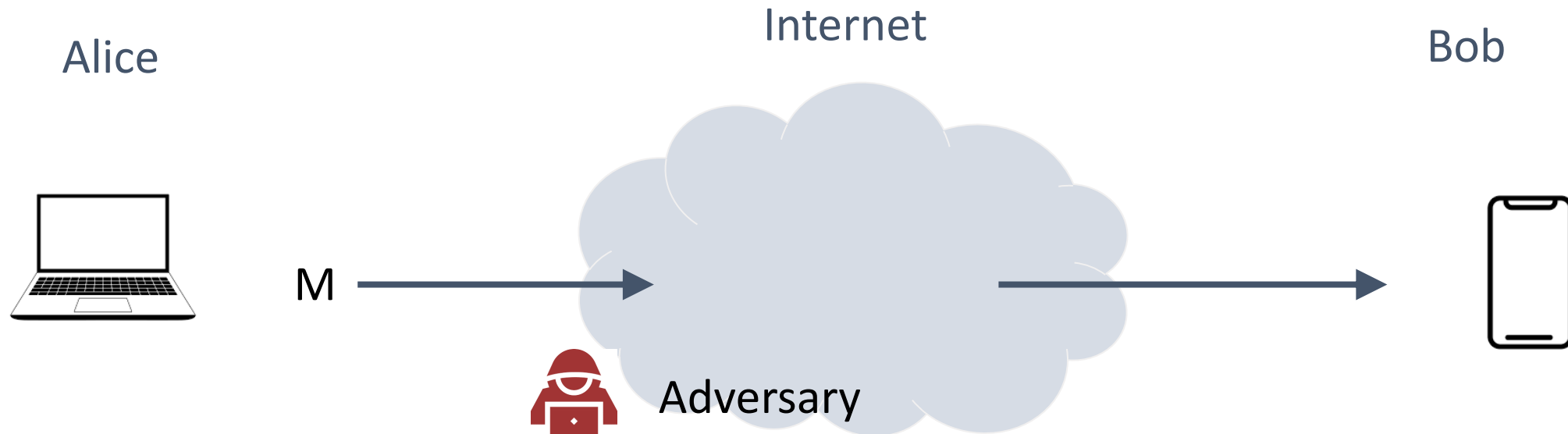
In the rest of this lecture
I will give a brief intro to each topic one by one

Please find which topic(s) you are interested in

Basic Cryptography 1: Symmetric-key cryptography

Date	Topics	Outline (tentative)	Lecture notes
Week 1: Jan 10	Course Overview	course plan, reading materials, grading, brief introduction to every topic	N/A
Week 2: Jan 17	Basic Cryptography 1: Symmetric-key cryptography	symmetric encryption, one-time pad, blockcipher, hash function, MAC, authenticated encryption.	Haiyang Xue
Week 3: Jan 31	Basic Cryptography 2: Public-key cryptography	RSA, Diffie-Hellman, public key encryption, Digital signature	??
Week 4: Feb 7	Network Security Principles	authenticated key exchange, PKI, and certification authorities	??
Week 5: Feb 14	Network Security in Practice	secure sockets layer (SSL), internet protocol security (IPSec), internet key exchange (IKE), virtual private network (VPN)	??
Week 6: Feb 21	Authentication	access control, password authentication, biometric authentication	??
Week 7: Feb 28	Privacy-Enhancing technologies 1	post-quantum cryptography; Fully-homomorphic encryption and applications	??
Week 8: Mar 7	Privacy-Enhancing technologies 2	commitment, zero-knowledge proofs;	??
Week 9: Mar 14	Privacy-Enhancing technologies 3	secure multiparty computation	??
Week 10: Mar 21	Security and Privacy in Practice 1	security and privacy in Blockchain	N/A
Week 11: Mar 28	Security and Privacy in Practice 2	security and privacy for AI, machine learning	N/A
Week 12: Apr 4	Final presentation 1	papers from S&P, CCS, USENIX, NDSS, CRYPTO, or EUROCRYPT	N/A
Week 13: Apr 11	Final presentation 2	papers from S&P, CCS, USENIX, NDSS, CRYPTO, or EUROCRYPT	N/A

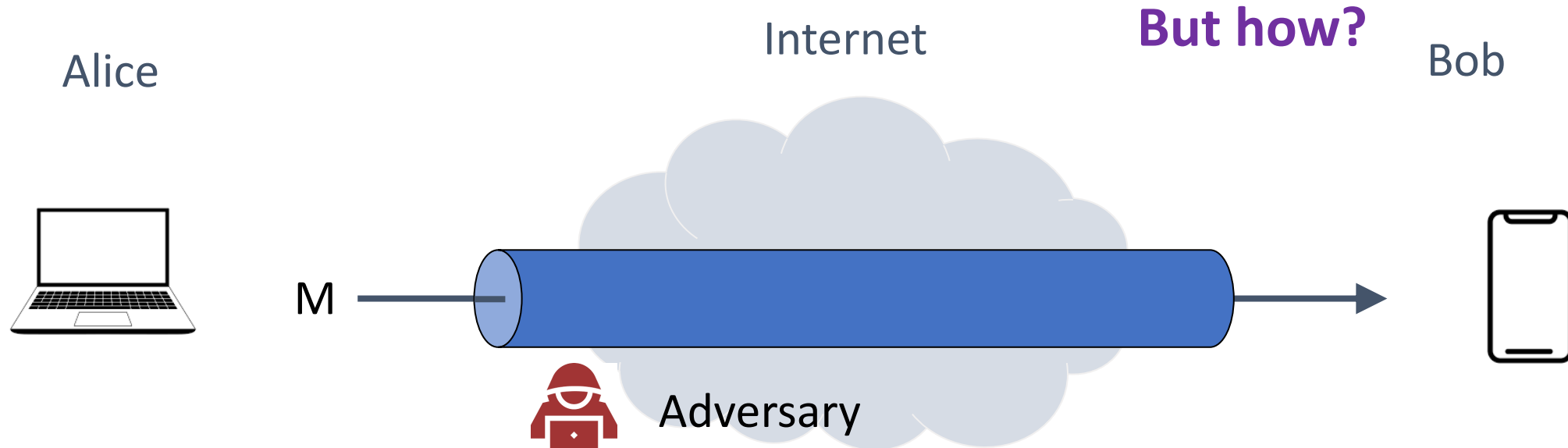
Lecture 2: Symmetric-key cryptography



Security goals:

- **Confidential:** adversary should not be able to read message M
- **Integrity:** adversary should not be able to modify message M
- **Authenticated:** message M really originated from Alice

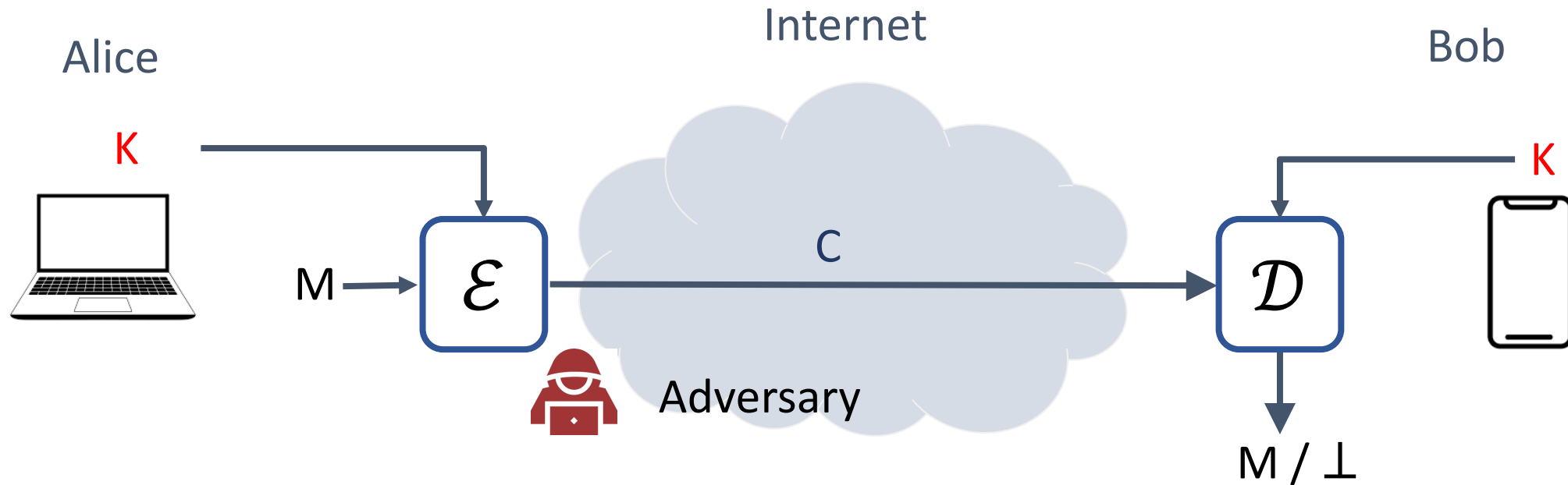
Build secure channels



Security goals:

- **Confidential:** adversary should not be able to read message M
- **Integrity:** adversary should not be able to modify message M
- **Authenticated:** message M really originated from Alice

Lecture 2: Symmetric-key cryptography



\mathcal{E} : encryption algorithm (public)

\mathcal{D} : decryption algorithm (public)

K : shared key between Alice and Bob

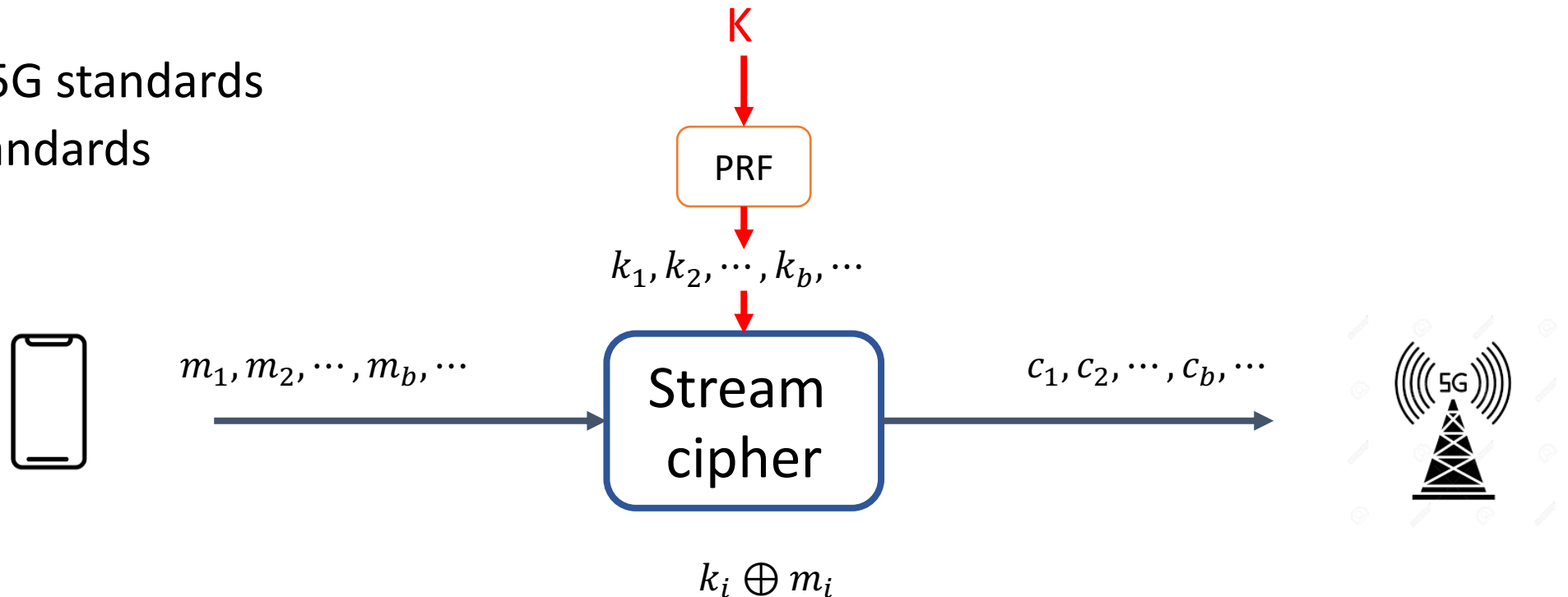
Ignore for now: How to achieve this??

Symmetric-key cryptography Stack

- Stream cipher
 - one-time pad
 - RC5; SNOW; ZUC
- Block cipher
 - 3DES, AES
- Hash function
- Message Authenticated Code (MAC)

Stream cipher

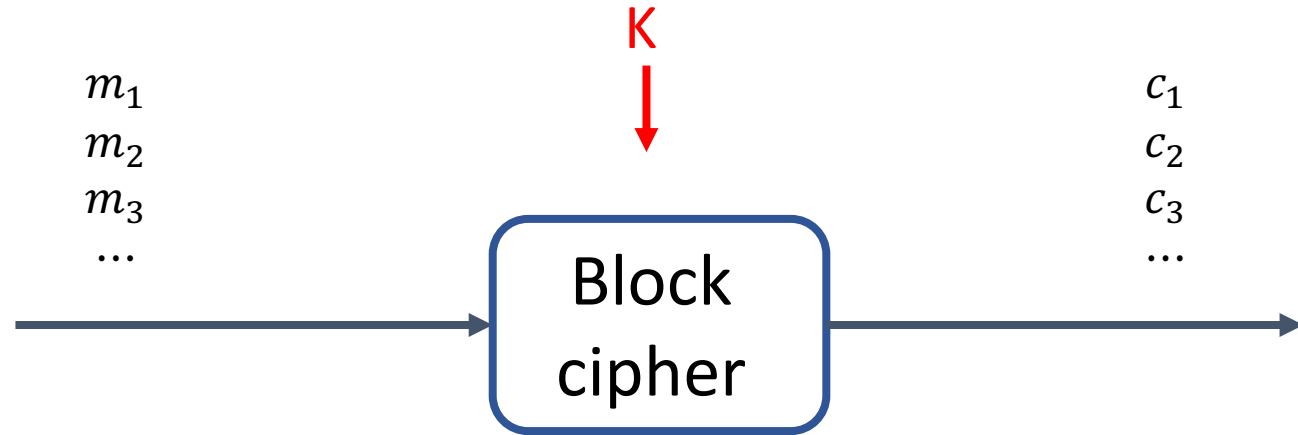
- Stream cipher
 - one-time pad
 - RC4: skype
 - SNOW 3G: 5G standards
 - ZUC: 5G standards
 - ...



<https://en.wikipedia.org/wiki/SNOW>

Block cipher

- Block cipher
 - 3DES, AES-XXX



- Visit any https website

Security overview

This page is secure (valid HTTPS).

- Certificate - **valid and trusted**
The connection to this site is using a valid, trusted server certificate issued by ESET SSL Filter CA.
[View certificate](#)
- Connection - **secure connection settings**
The connection to this site is encrypted and authenticated using TLS 1.3, X25519, and AES_128_GCM.
- Resources - **all served securely**
All resources on this page are served securely.

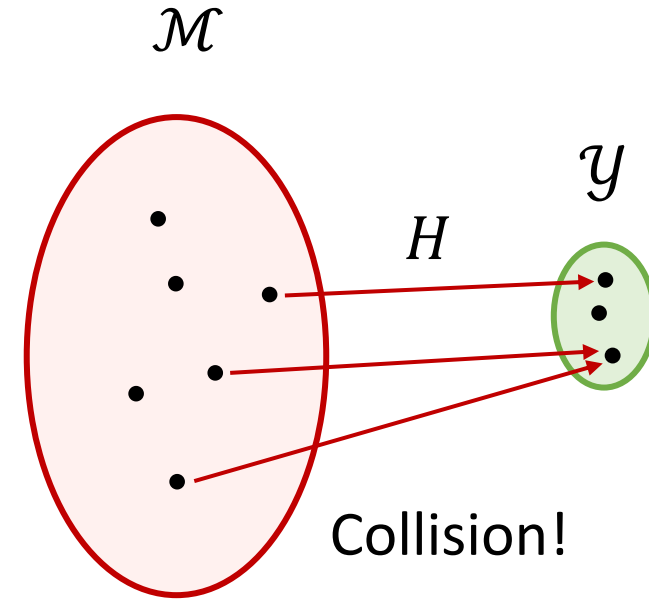
Hash functions

$$H : \mathcal{M} \rightarrow \mathcal{Y}$$

Keyless function

$$|\mathcal{M}| \gg |\mathcal{Y}|$$

Compressing



- SHA1 *: $\{0,1\}^{<2^{64}} \rightarrow \{0,1\}^{160}$
- SHA2-256 : $\{0,1\}^{<2^{64}} \rightarrow \{0,1\}^{256}$
- SHA3-512 : $\{0,1\}^{<2^{128}} \rightarrow \{0,1\}^{512}$

Collision Resistant

One way

Hash functions

- Store password in computer

- Blockchain Mining

- SHA-256
- $<2^{224}$

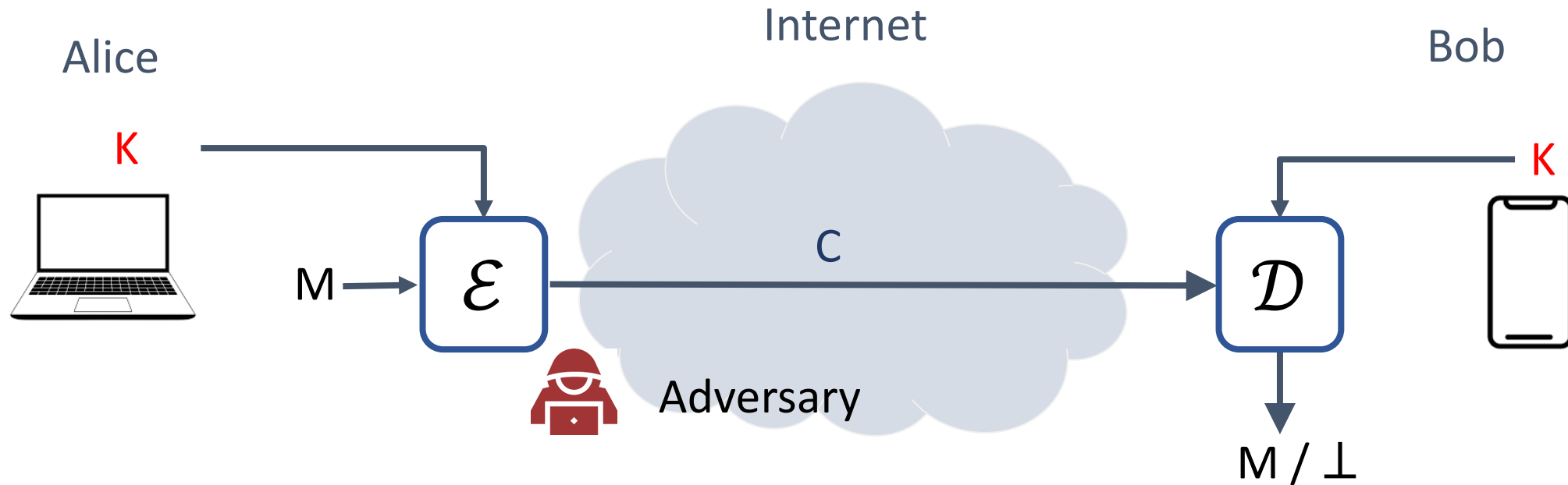
```
Block hash:  
c5aa3150f61b752c8fb39525f911981e2f9982c8b9bc907c73914585ad2ef12b  
Target:  
0x00000000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF  
Is the block hash less than the target?  
False
```

- CA/APP fingerprint etc. example in CA

Symmetric-key cryptography Stack

- Stream cipher
 - one-time pad
 - RC5; SNOW; ZUC
- Block cipher
 - 3DES, AES
- Hash function
- Message Authenticated Code (MAC)

Challenge: Symmetric-key cryptography



\mathcal{E} : encryption algorithm (public)

\mathcal{D} : decryption algorithm (public)

K : shared key between Alice and Bob

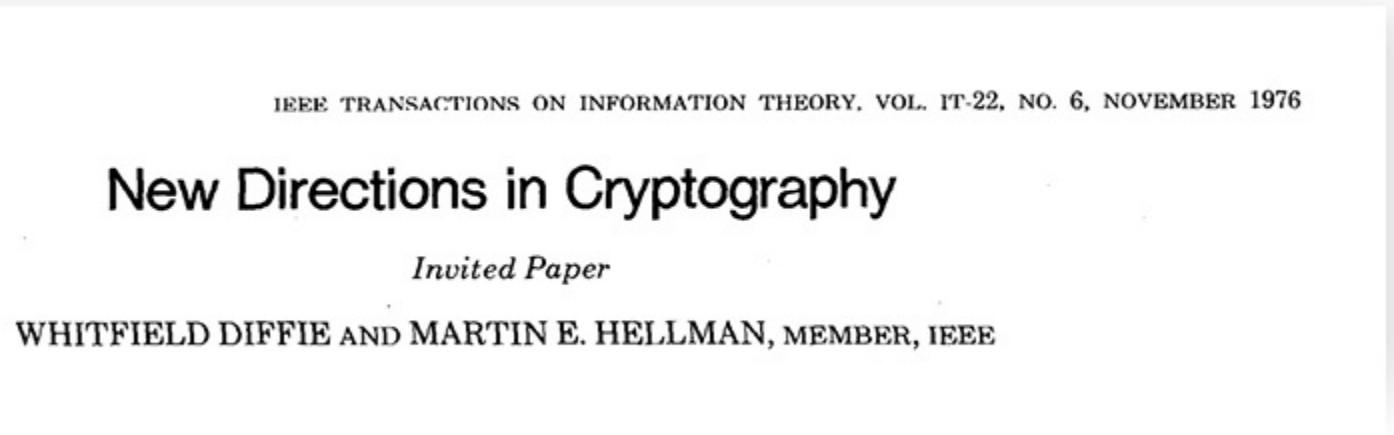
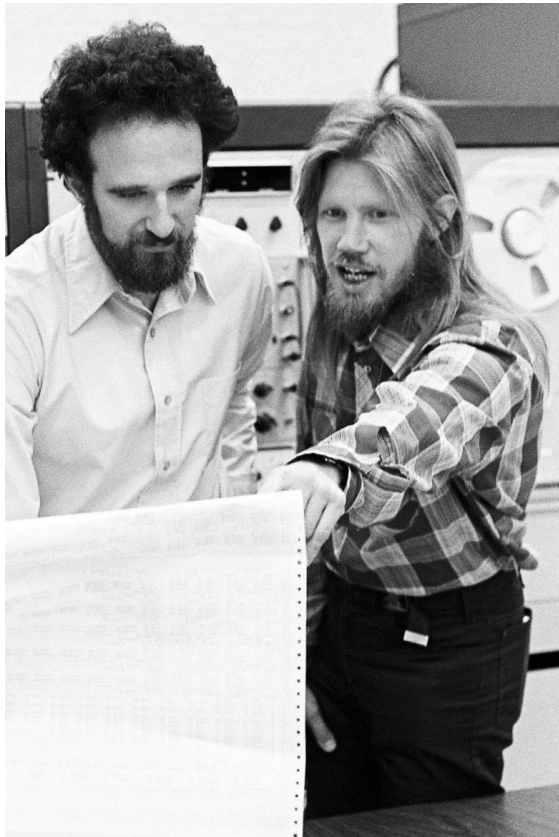
Challenge: How do they privately share a key?

Basic Cryptography 2: Public-key cryptography

Date	Topics	Outline (tentative)	Lecture notes
Week 1: Jan 10	Course Overview	course plan, reading materials, grading, brief introduction to every topic	N/A
Week 2: Jan 17	Basic Cryptography 1: Symmetric-key cryptography	symmetric encryption, one-time pad, blockcipher, hash function, MAC, authenticated encryption.	Haiyang Xue
Week 3: Jan 31	Basic Cryptography 2: Public-key cryptography	RSA, Diffie-Hellman, public key encryption, Digital signature	??
Week 4: Feb 7	Network Security Principles	authenticated key exchange, PKI, and certification authorities	??
Week 5: Feb 14	Network Security in Practice	secure sockets layer (SSL), internet protocol security (IPSec), internet key exchange (IKE), virtual private network (VPN)	??
Week 6: Feb 21	Authentication	access control, password authentication, biometric authentication	??
Week 7: Feb 28	Privacy-Enhancing technologies 1	post-quantum cryptography; Fully-homomorphic encryption and applications	??
Week 8: Mar 7	Privacy-Enhancing technologies 2	commitment, zero-knowledge proofs;	??
Week 9: Mar 14	Privacy-Enhancing technologies 3	secure multiparty computation	??
Week 10: Mar 21	Security and Privacy in Practice 1	security and privacy in Blockchain	N/A
Week 11: Mar 28	Security and Privacy in Practice 2	security and privacy for AI, machine learning	N/A
Week 12: Apr 4	Final presentation 1	papers from S&P, CCS, USENIX, NDSS, CRYPTO, or EUROCRYPT	N/A
Week 13: Apr 11	Final presentation 2	papers from S&P, CCS, USENIX, NDSS, CRYPTO, or EUROCRYPT	N/A

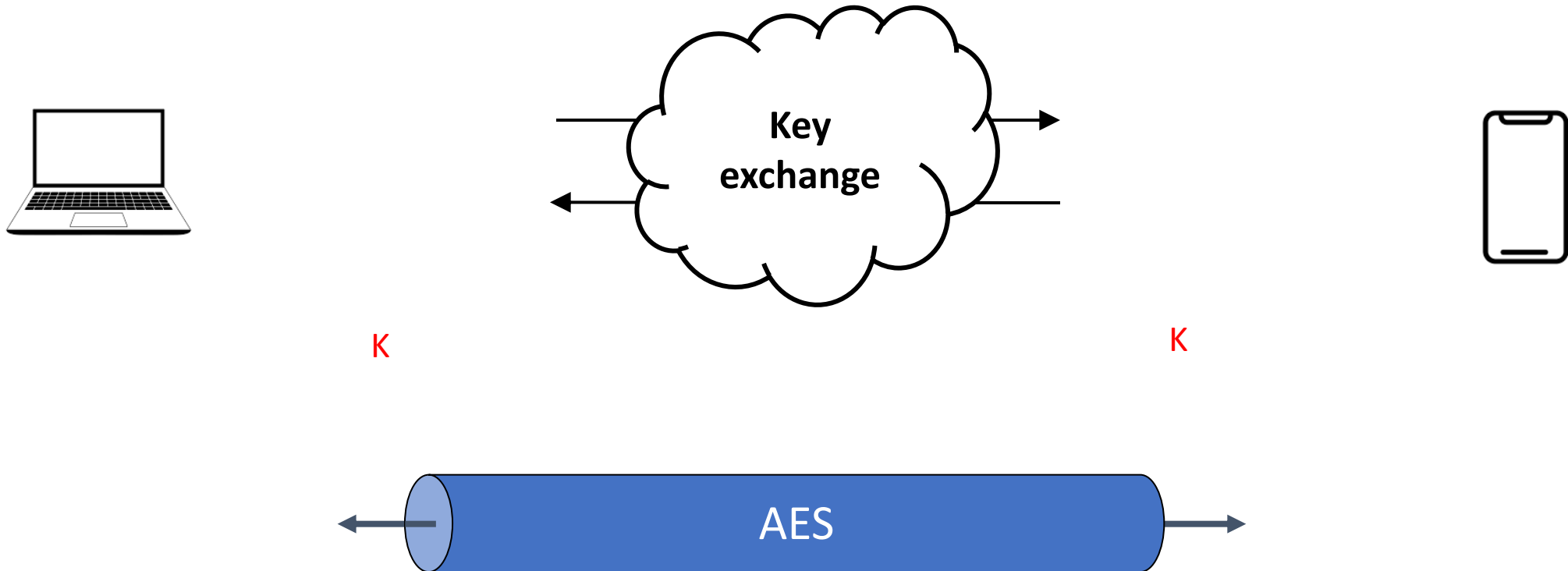
Lecture 3: Public-key cryptography

- Diffie-Hellman 1976 [New Directions in Cryptography](#)

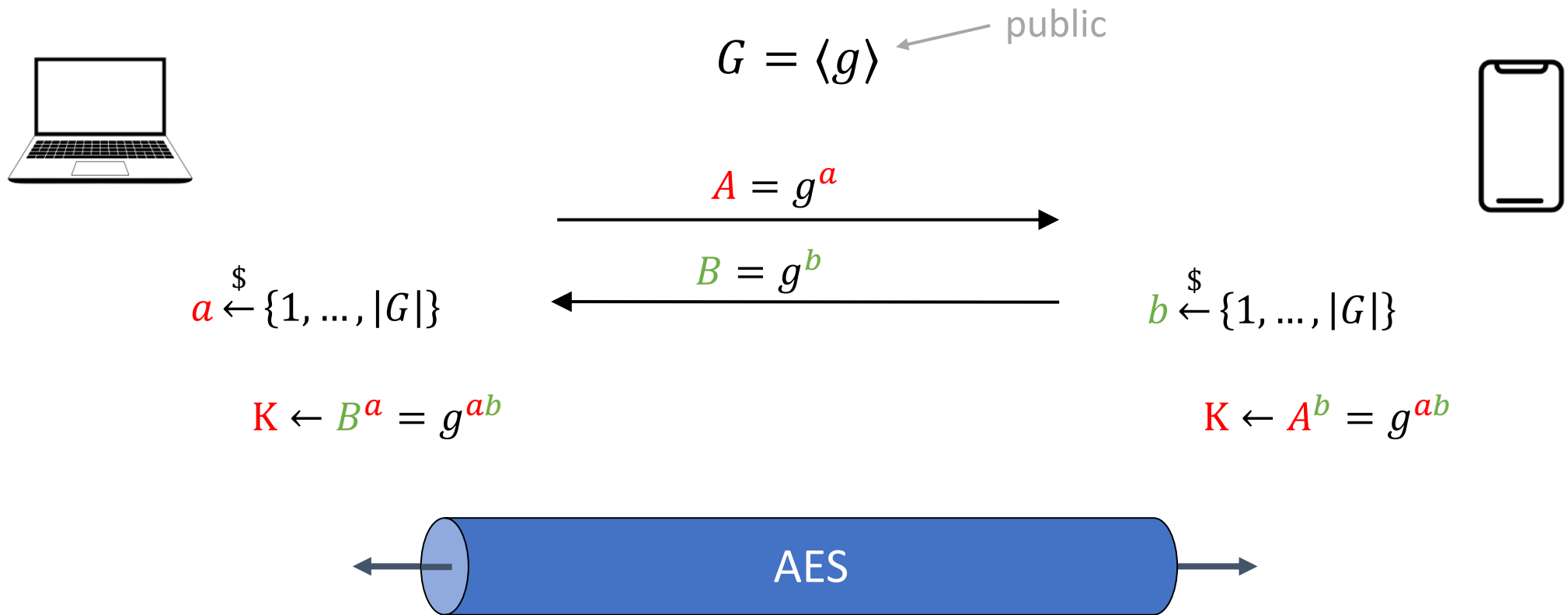


Lecture 3: Public-key cryptography

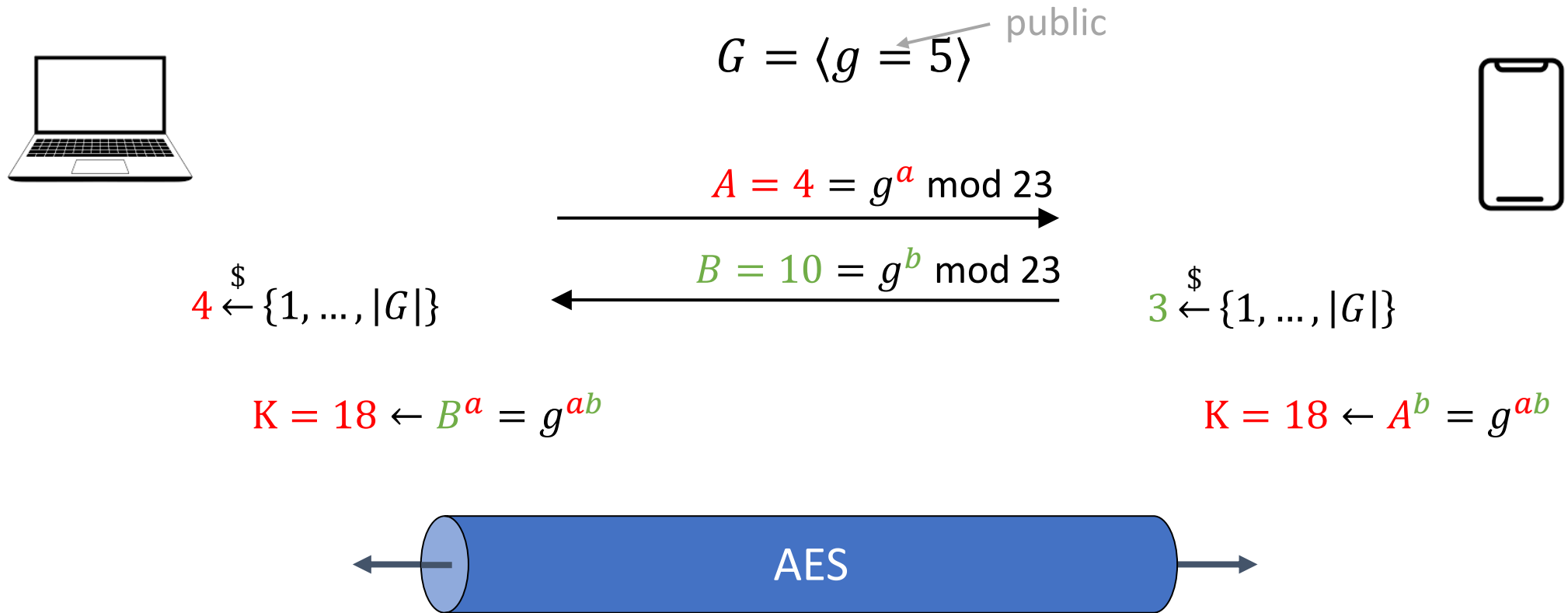
- DH key exchange



Diffie-Hellman Key Exchange



Diffie-Hellman Key Exchange

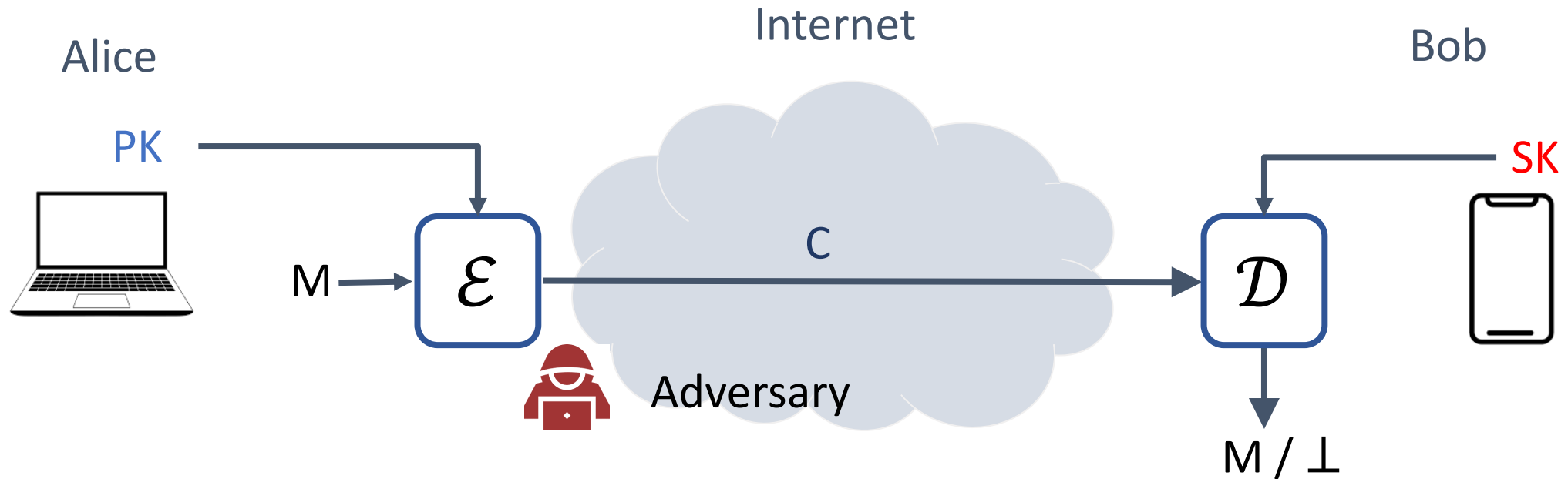


Insecure Exp. $G = (\mathbf{Z}_p^*, \cdot), p = 23, g = 5$

To be secure: length $p > 2048$

<https://www.rfc-editor.org/rfc/rfc2409#section-6.2>; [rfc3526#page-3](https://www.rfc-editor.org/rfc/rfc3526#page-3)

Is public-key cryptography possible???



\mathcal{E} : encryption algorithm (public)

PK : public key of Bob (public)

\mathcal{D} : decryption algorithm (public)

SK : secret key (secret)

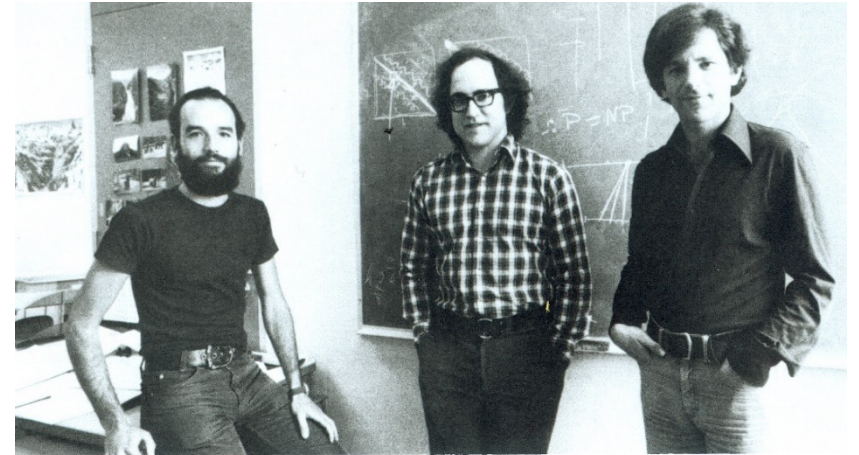
RSA said yes in 1977

- The RSA encryption scheme

$$c = E(m) = m^e \pmod{N}$$
$$m = D(c) = c^d \pmod{N}$$

PK: $N = pq, e$

SK: $d = e^{-1} \pmod{\phi(N)}$



Adi Shamir

Ron Rivest

Leonard Adleman

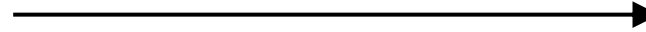
Digital Signature

Alice



$$G = \langle g \rangle$$

$$A = g^a$$



Why should I believe **A** comes from Alice?

Most likely NO

Digital Signature



$$G = \langle g \rangle$$

$$A = g^a$$



Why should I believe **A** comes from Alice?

Well, YES

Digital Signature

- ECDSA

- Digital Signature Standard using Elliptic Curve Cryptography
- Widely deployed in cryptocurrency, such as Bitcoin etc.
- Standardized by NIST

- RSA Enc with hash

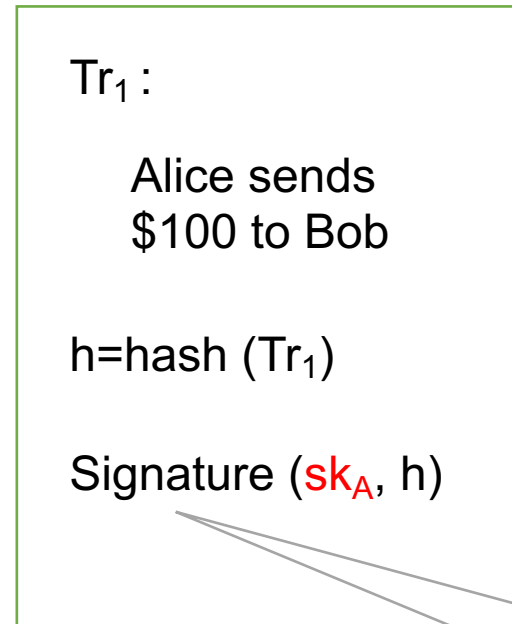
- Roughly, the decryption is the signature
- Roughly, the encryption is the verification

- Schnorr, etc

Digital Signature

- HTTPS / TLS certificates (any https)
- Software installation
- Bitcoin

A transaction in bitcoin looks like



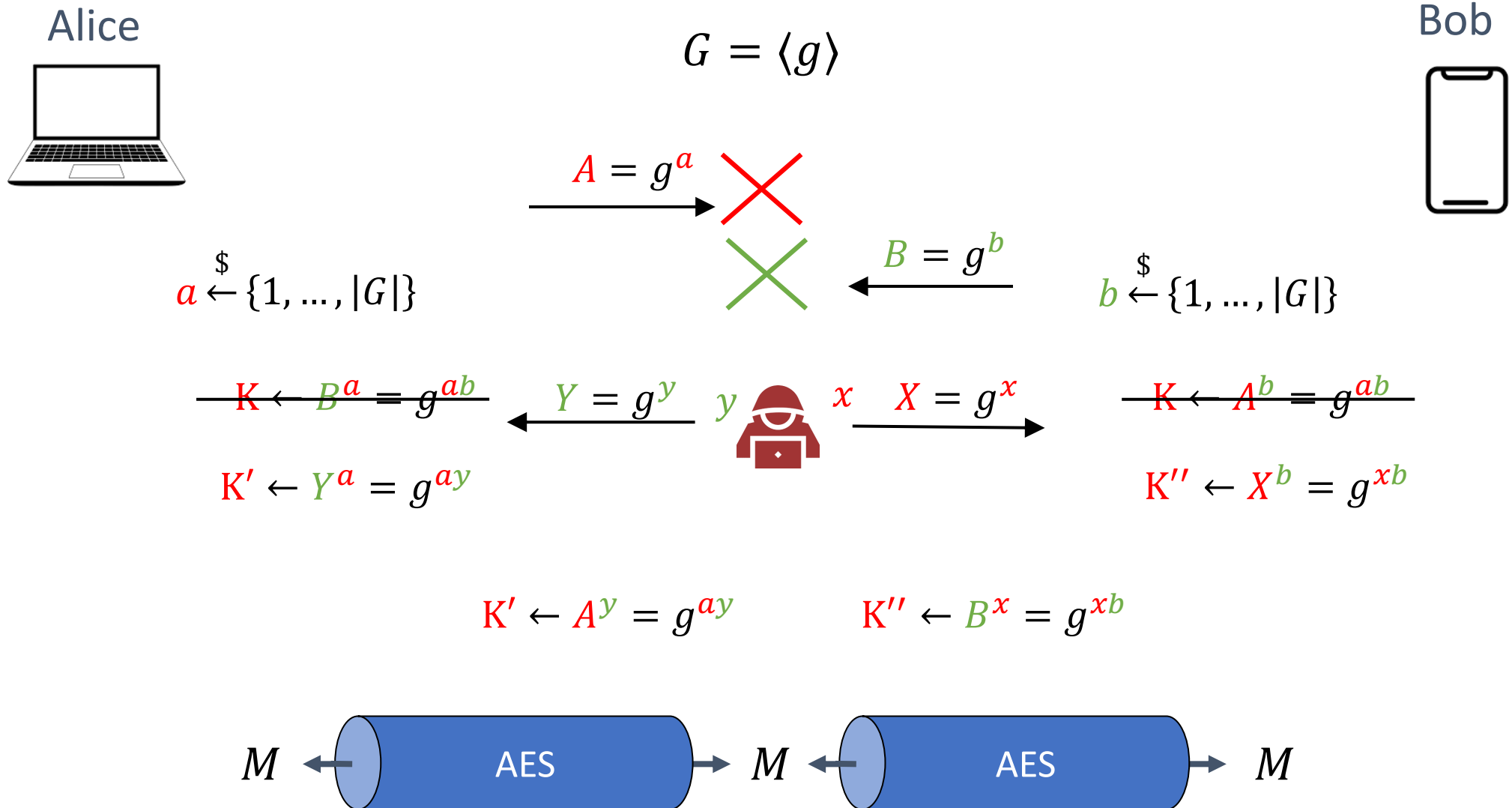
Signature is the standard ECDSA proposed by NIST

Lecture 3: Public-key cryptography

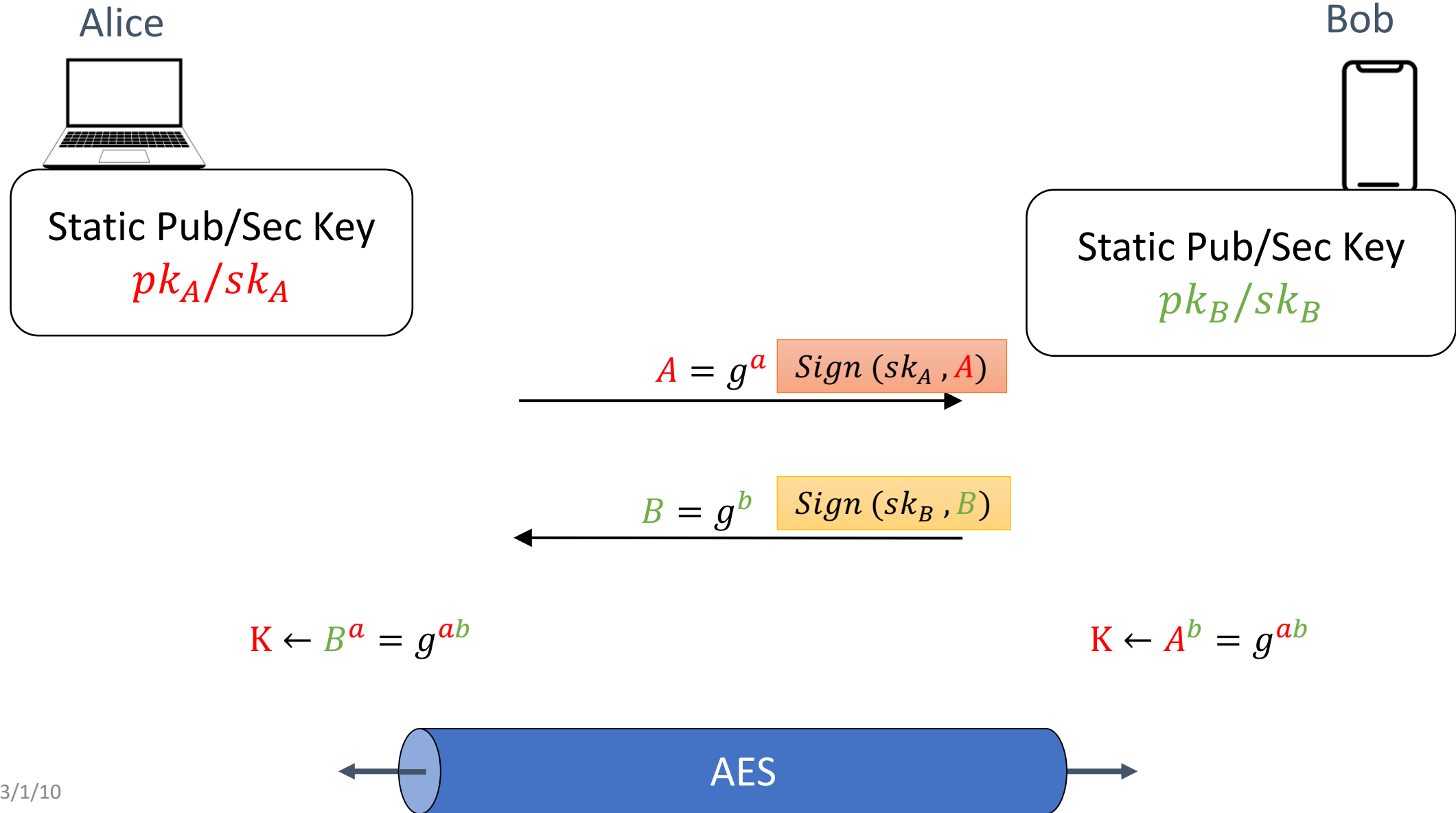
- Diffie-Hellman key exchange
- PKE:
 - RSA
- Signature:
 - RSA, ECDSA, Shnorr
- Applications:
 - https, etc

Date	Topics	Outline (tentative)	Lecture notes
Week 1: Jan 10	Course Overview	course plan, reading materials, grading, brief introduction to every topic	N/A
Week 2: Jan 17	Basic Cryptography 1: Symmetric-key cryptography	symmetric encryption, one-time pad, blockcipher, hash function, MAC, authenticated encryption.	Haiyang Xue
Week 3: Jan 31	Basic Cryptography 2: Public-key cryptography	RSA, Diffie-Hellman, public key encryption, Digital signature	??
Week 4: Feb 7	Network Security Principles	authenticated key exchange, PKI, and certification authorities	??
Week 5: Feb 14	Network Security in Practice	secure sockets layer (SSL), internet protocol security (IPSec), internet key exchange (IKE), virtual private network (VPN)	??
Week 6: Feb 21	Authentication	access control, password authentication, biometric authentication	??
Week 7: Feb 28	Privacy-Enhancing technologies 1	post-quantum cryptography; Fully-homomorphic encryption and applications	??
Week 8: Mar 7	Privacy-Enhancing technologies 2	commitment, zero-knowledge proofs;	??
Week 9: Mar 14	Privacy-Enhancing technologies 3	secure multiparty computation	??
Week 10: Mar 21	Security and Privacy in Practice 1	security and privacy in Blockchain	N/A
Week 11: Mar 28	Security and Privacy in Practice 2	security and privacy for AI, machine learning	N/A
Week 12: Apr 4	Final presentation 1	papers from S&P, CCS, USENIX, NDSS, CRYPTO, or EUROCRYPT	N/A
Week 13: Apr 11	Final presentation 2	papers from S&P, CCS, USENIX, NDSS, CRYPTO, or EUROCRYPT	N/A

Diffie-Hellman: man-in-the-middle attack



Ideal: **Authenticated** Key Exchange



Ideal: Authenticated Key Exchange

Alice



Static Pub/Sec Key

pk_A/sk_A

There are many Alice's

Why should we believe pk_A belongs to Alice?

Need to **bind** public keys to entities

Public-key infrastructure (PKI)

Alice



Static Pub/Sec Key

pk_A/sk_A

Alice

pk_A

Sign(by Google)

Why do we believe
pk_google is Google's pk (or
verification key)?

Google

pk_google

Sign(by the **ROOT**)

A few Roots need to be trust

Certificate authority (CA)

- A way of binding a public key to an entity
- CA consists of:
 - The public key of the entity
 - A bunch of information identifying the entity
 - Name
 - Address
 - Occupation
 - URL
 - ...

Certificate authority (CA)

Certificate

www.google.com	ESET SSL Filter CA
Subject Name	
Common Name	www.google.com
Issuer Name	
Common Name	ESET SSL Filter CA
Organization	ESET, spol. s r. o.
Country	SK
Validity	
Not Before	Mon, 28 Nov 2022 08:19:01 GMT
Not After	Mon, 20 Feb 2023 08:19:00 GMT
Subject Alt Names	
DNS Name	www.google.com
Public Key Info	
Algorithm	Elliptic Curve
Key Size	256
Curve	P-256
Public Value	04:7E:F5:D4:A3:E7:83:25:34:E6:A8:96:FE:A8:14:F0:7A:4C:69:5B:D7:FB:48:5D:4D:01:4...
Miscellaneous	
Serial Number	5B:C8:4B:3F:65:E6:5F:09:6A:40:A8:B6:AF:DF:C1:34

CA examples in chrome, safari, firefox

- Wiki, ECDSA Signature with SHA-384
- Polyu, PKCS #1 RSA Encryption
- Google,

Lecture 4: Network Security Principles

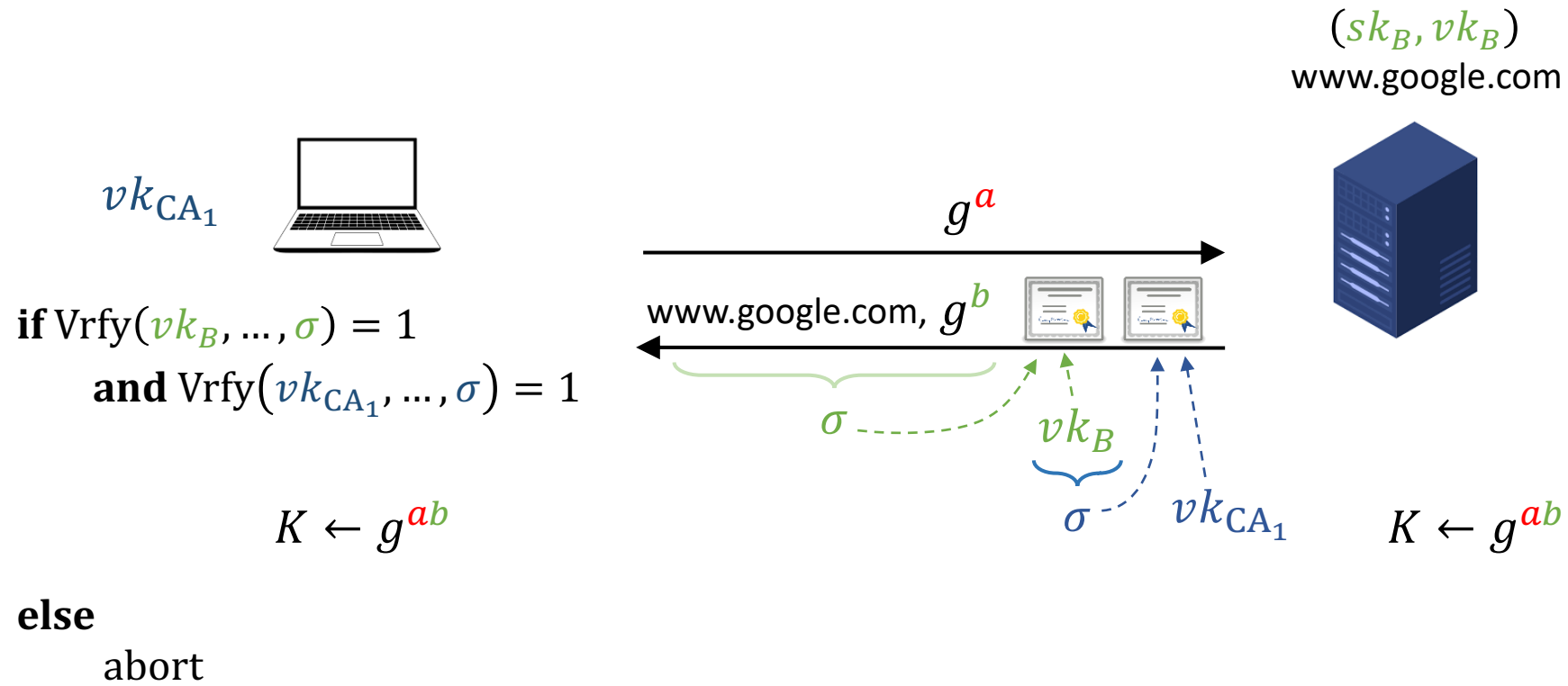
- Authenticated Key Exchange
- Public Key Infrastructure
- Certificate authority

Network Security in Practice

Date	Topics	Outline (tentative)	Lecture notes
Week 1: Jan 10	Course Overview	course plan, reading materials, grading, brief introduction to every topic	N/A
Week 2: Jan 17	Basic Cryptography 1: Symmetric-key cryptography	symmetric encryption, one-time pad, blockcipher, hash function, MAC, authenticated encryption.	Haiyang Xue
Week 3: Jan 31	Basic Cryptography 2: Public-key cryptography	RSA, Diffie-Hellman, public key encryption, Digital signature	??
Week 4: Feb 7	Network Security Principles	authenticated key exchange, PKI, and certification authorities	??
Week 5: Feb 14	Network Security in Practice	secure sockets layer (SSL), internet protocol security (IPSec), internet key exchange (IKE), virtual private network (VPN)	??
Week 6: Feb 21	Authentication	access control, password authentication, biometric authentication	??
Week 7: Feb 28	Privacy-Enhancing technologies 1	post-quantum cryptography; Fully-homomorphic encryption and applications	??
Week 8: Mar 7	Privacy-Enhancing technologies 2	commitment, zero-knowledge proofs;	??
Week 9: Mar 14	Privacy-Enhancing technologies 3	secure multiparty computation	??
Week 10: Mar 21	Security and Privacy in Practice 1	security and privacy in Blockchain	N/A
Week 11: Mar 28	Security and Privacy in Practice 2	security and privacy for AI, machine learning	N/A
Week 12: Apr 4	Final presentation 1	papers from S&P, CCS, USENIX, NDSS, CRYPTO, or EUROCRYPT	N/A
Week 13: Apr 11	Final presentation 2	papers from S&P, CCS, USENIX, NDSS, CRYPTO, or EUROCRYPT	N/A

Lecture 5: Network Security in Practice

- HTTPS / TLS + PKI

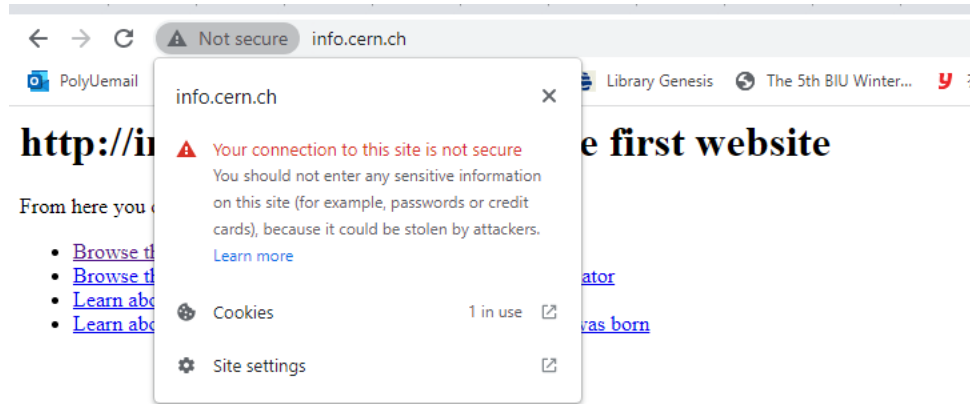


From Håkon Jacobsen

HTTPS



`http://info.cern.ch/`

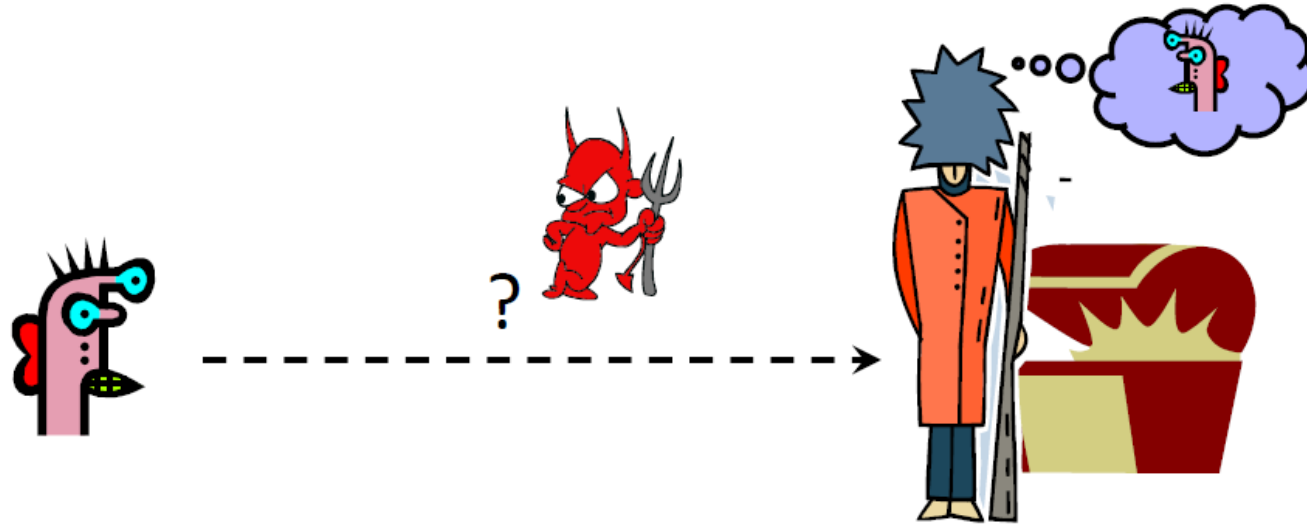


Web/Software Security

Date	Topics	Outline (tentative)	Lecture notes
Week 1: Jan 10	Course Overview	course plan, reading materials, grading, brief introduction to every topic	N/A
Week 2: Jan 17	Basic Cryptography 1: Symmetric-key cryptography	symmetric encryption, one-time pad, blockcipher, hash function, MAC, authenticated encryption.	Haiyang Xue
Week 3: Jan 31	Basic Cryptography 2: Public-key cryptography	RSA, Diffie-Hellman, public key encryption, Digital signature	??
Week 4: Feb 7	Network Security Principles	authenticated key exchange, PKI, and certification authorities	??
Week 5: Feb 14	Network Security in Practice	secure sockets layer (SSL), internet protocol security (IPSec), internet key exchange (IKE), virtual private network (VPN)	??
Week 6: Feb 21	Authentication	access control, password authentication, biometric authentication	??
Week 7: Feb 28	Privacy-Enhancing technologies 1	post-quantum cryptography; Fully-homomorphic encryption and applications	??
Week 8: Mar 7	Privacy-Enhancing technologies 2	commitment, zero-knowledge proofs;	??
Week 9: Mar 14	Privacy-Enhancing technologies 3	secure multiparty computation	??
Week 10: Mar 21	Security and Privacy in Practice 1	security and privacy in Blockchain	N/A
Week 11: Mar 28	Security and Privacy in Practice 2	security and privacy for AI, machine learning	N/A
Week 12: Apr 4	Final presentation 1	papers from S&P, CCS, USENIX, NDSS, CRYPTO, or EUROCRYPT	N/A
Week 13: Apr 11	Final presentation 2	papers from S&P, CCS, USENIX, NDSS, CRYPTO, or EUROCRYPT	N/A

Lecture 6: Authentication

- Basic problem



How do you prove to someone you are who you claimed?

This needs to be solved for any access control system

Prove who you are

- What you know
 - Passwords
 - Answers to questions
- Where you are
 - IP address
- What you are
 - Biometrics
- What you have
 - Secure tokens, mobile devices

Password

- Authentication (& Identification)
 - Establishes that the user is who they say they are.
- Authorization
 - The process used to decide if the authenticated person is allowed to access specific information or functions.
- Access Control
 - Restriction of access (includes authentication & authorization)

How Can Passwords Be Stored?

- Filing System
- 🔓 • Clear text
- Encrypted
- 🔓 • Password + Encryption ?
- Hashed
- 🔓 • Password + Hash function ?
- Salted Hash
- 🔓 🔓 • (Username + Salt + Password) + Hash ?



Weak
Password

What About Biometrics?

- Authentication: **What you are**
- Unique identifying characteristics to authenticate user or create
 - Biological and physiological: Fingerprints, face scan
- Advantages:
 - Do not need to remember
 - Can't share (generally)

Attacking Biometrics

- An adversary might try to steal biometric info
 - Malicious fingerprint reader
 - Consider when biometric is used to derive a cryptographic key
 - Copy fingerprint on a glass
- Continuous news about trying to compromise biometrics

iPhone 6 vulnerable to TouchID fingerprint hack

By Allie Coyne
Sep 24 2014
9:03AM

1 Comment



RELATED ARTICLES

Rackspace customer data taken in 'PLAY' ransomware attack

But researcher not worried about attacks.

Apple's just-released iPhone 6 is vulnerable to the same **TouchID fingerprint sensor attack** as its iPhone 5s predecessor, a researcher who detailed the first security hole has found.

Principal researcher from security firm Lookout, Marc Rogers, followed the **Chaos Computer Club biometrics hacking team** late last year to demonstrate how the TouchID sensor in the iPhone 5s could be fooled by a **fake set of fingerprints** created by using household items.

Rogers this week decided to check whether Apple had



Authentication

Date	Topics	Outline (tentative)	Lecture notes
Week 1: Jan 10	Course Overview	course plan, reading materials, grading, brief introduction to every topic	N/A
Week 2: Jan 17	Basic Cryptography 1: Symmetric-key cryptography	symmetric encryption, one-time pad, blockcipher, hash function, MAC, authenticated encryption.	Haiyang Xue
Week 3: Jan 31	Basic Cryptography 2: Public-key cryptography	RSA, Diffie-Hellman, public key encryption, Digital signature	??
Week 4: Feb 7	Network Security Principles	authenticated key exchange, PKI, and certification authorities	??
Week 5: Feb 14	Network Security in Practice	secure sockets layer (SSL), internet protocol security (IPSec), internet key exchange (IKE), virtual private network (VPN)	??
Week 6: Feb 21	Authentication	access control, password authentication, biometric authentication	??
Week 7: Feb 28	Privacy-Enhancing technologies 1	post-quantum cryptography; Fully-homomorphic encryption and applications	??
Week 8: Mar 7	Privacy-Enhancing technologies 2	commitment, zero-knowledge proofs;	??
Week 9: Mar 14	Privacy-Enhancing technologies 3	secure multiparty computation	??
Week 10: Mar 21	Security and Privacy in Practice 1	security and privacy in Blockchain	N/A
Week 11: Mar 28	Security and Privacy in Practice 2	security and privacy for AI, machine learning	N/A
Week 12: Apr 4	Final presentation 1	papers from S&P, CCS, USENIX, NDSS, CRYPTO, or EUROCRYPT	N/A
Week 13: Apr 11	Final presentation 2	papers from S&P, CCS, USENIX, NDSS, CRYPTO, or EUROCRYPT	N/A

Shor's algorithm

1994

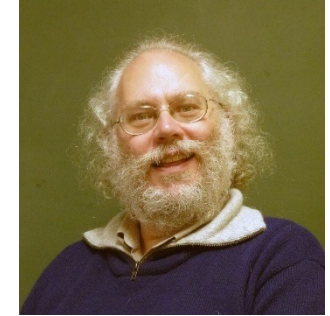
Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor[†]

Abstract

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

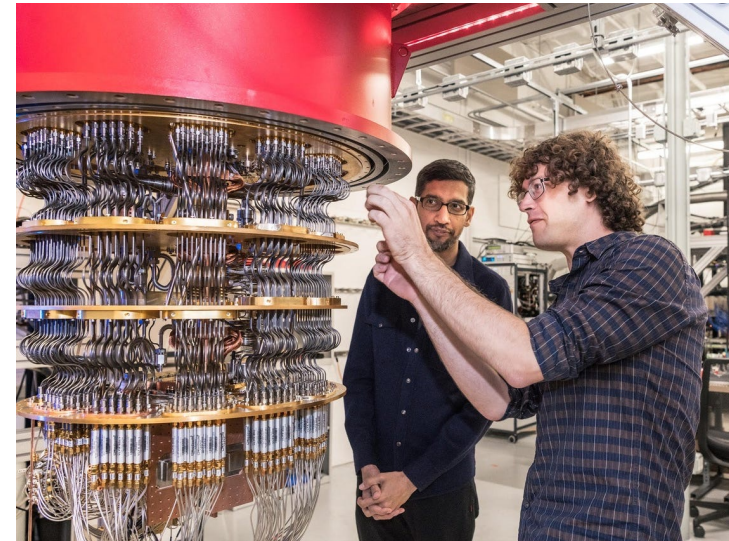
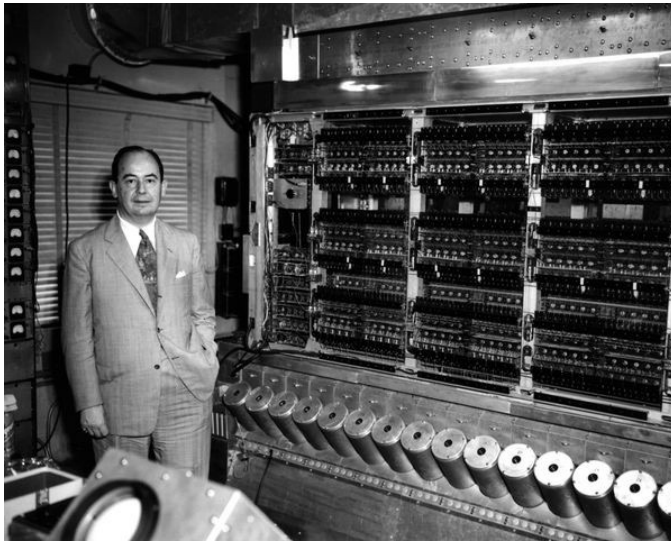
Keywords: algorithmic number theory, prime factorization, discrete logarithms, Church's thesis, quantum computers, foundations of quantum mechanics, spin systems, Fourier transforms



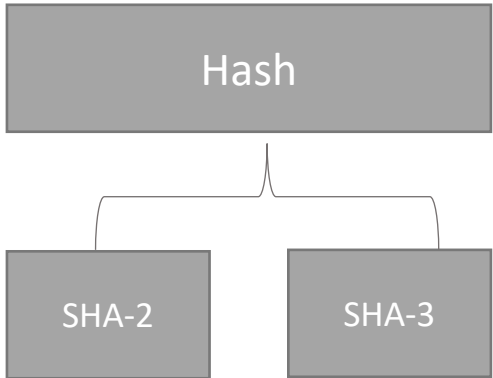
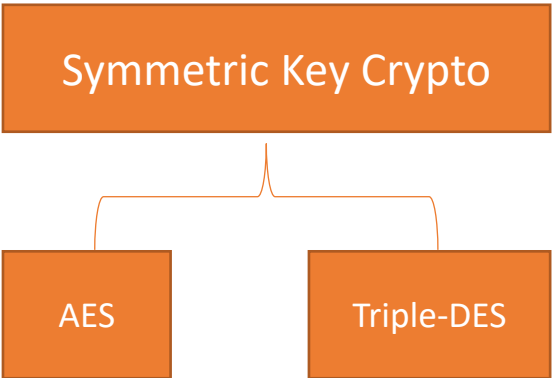
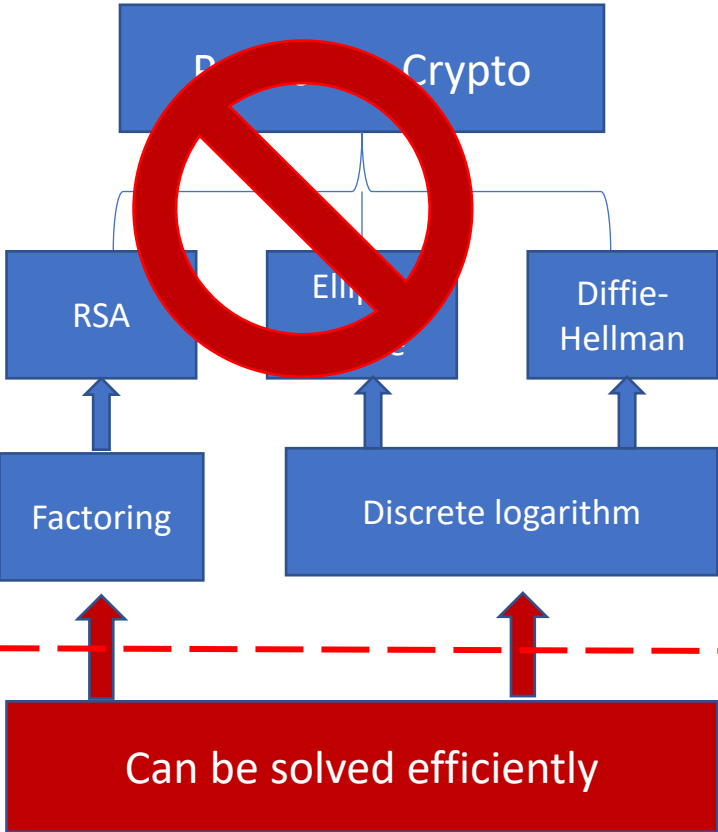
Quantum computer

While it is not sure when large-scale quantum computer could be built
experts estimate it is possible in two decades*

*Quantum Threat Timeline Report: Global Risk Institute



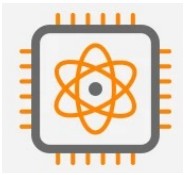
Contemporary cryptography



Larger Keys

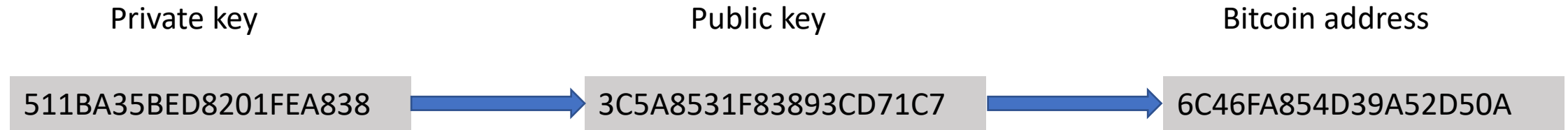
Longer Outputs

Quantum Computing



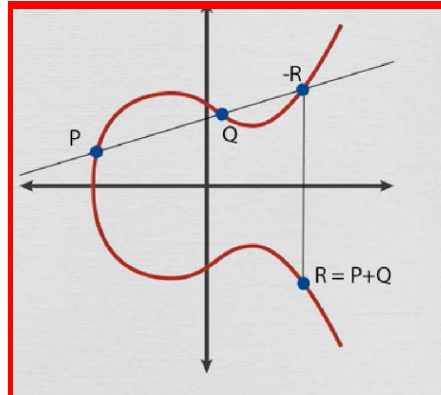
Quantum threats on Blockchain

Secret key vulnerability → financial loss



The private key is secret.
But the public key is public.

Elliptic Curve Digital
Signature (ECDSA)



ECDSA is vulnerable to quantum computer,
i.e., quantum adversary could steal your money.

National Institute of Standards and Technology (NIST)

NIST

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

PROJECTS

Post-Quantum Cryptography PQC



Overview

The [Candidates to be Standardized](#) and [Round 4 Submissions](#) were announced July 5, 2022. [NISTIR 8413](#), Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process is now available.



NIST PQC process

Hard problems believed to be quantum-resistant

Hash-based

- Signature

Code-based

- McEliece

Multivariate

Lattice-based

- NTRU
- LWE
- RLWE

Isogenies

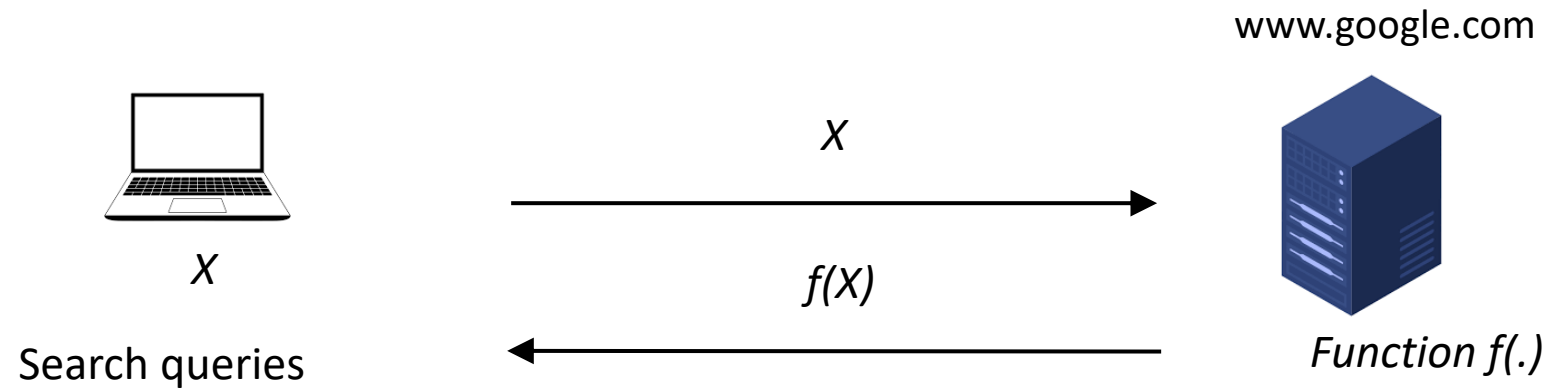
- Supersingular Isogeny (CSIDH)

Fully-homomorphic encryption (FHE)



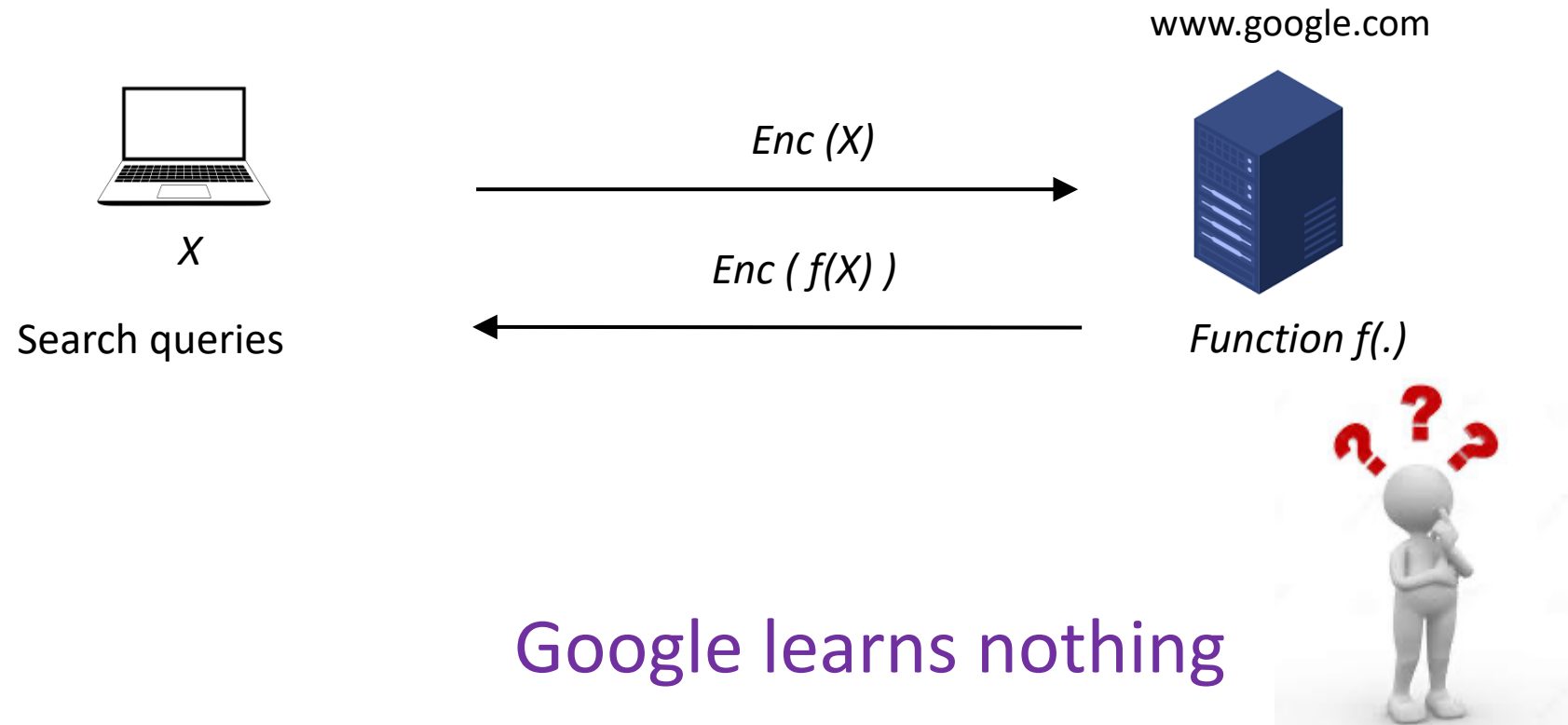
Fully-homomorphic encryption

What can we do with encrypted data, anyway?



WANT PRIVACY!

What can we do with encrypted data, anyway?



Some people noted the algebraic structure in RSA...

- RSA encryption E

$$E(m_1) = m_1^e \quad E(m_2) = m_2^e$$

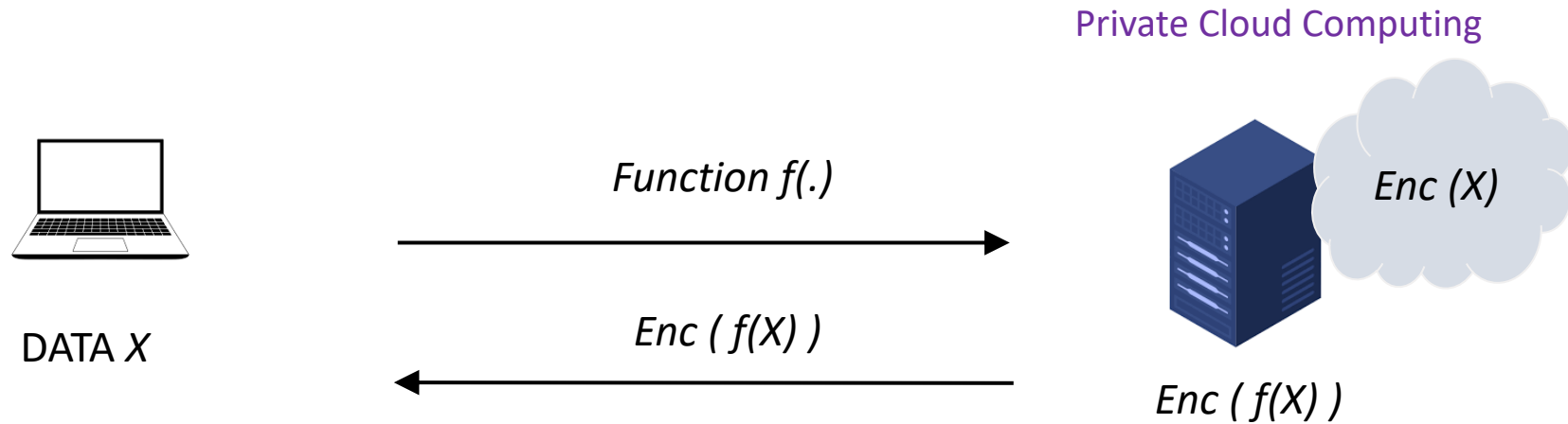
$$\begin{aligned} E(m_1) \times E(m_2) &= m_1^e \times m_2^e \\ &= (m_1 \times m_2)^e \\ &= E(m_1 \times m_2) \end{aligned}$$

f=Multiplication

$$E(m_1) \times E(m_2) = E(m_1 \times m_2)$$

What if f is any poly-time function?

$f = \text{arbitrary}$

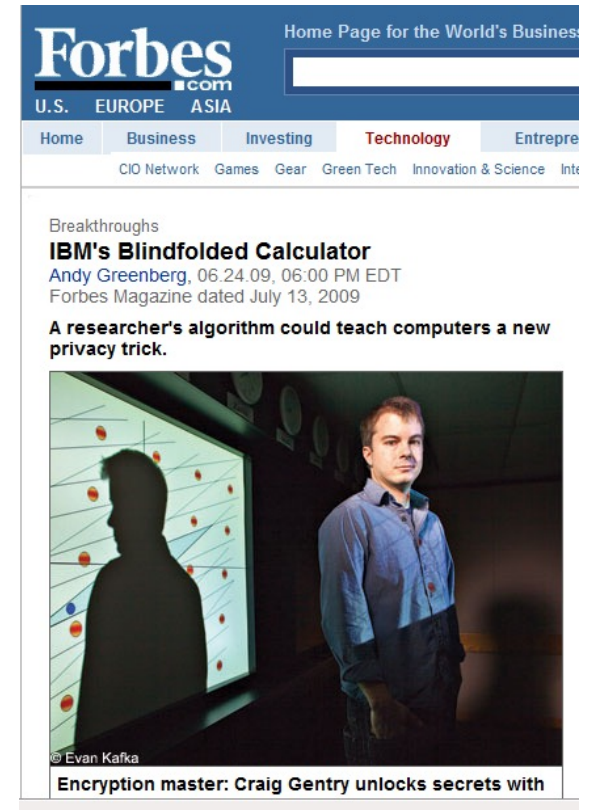


What if f is any poly-time function?

... until, in October 2008 ...

... **Gentry** came up with the first
fully homomorphic encryption scheme ...

... from Lattice...



Fully-homomorphic encryption

How does it work?

What is the magic?

Privacy-Enhancing technologies 1: PQC and FHE

Date	Topics	Outline (tentative)	Lecture notes
Week 1: Jan 10	Course Overview	course plan, reading materials, grading, brief introduction to every topic	N/A
Week 2: Jan 17	Basic Cryptography 1: Symmetric-key cryptography	symmetric encryption, one-time pad, blockcipher, hash function, MAC, authenticated encryption.	Haiyang Xue
Week 3: Jan 31	Basic Cryptography 2: Public-key cryptography	RSA, Diffie-Hellman, public key encryption, Digital signature	??
Week 4: Feb 7	Network Security Principles	authenticated key exchange, PKI, and certification authorities	??
Week 5: Feb 14	Network Security in Practice	secure sockets layer (SSL), internet protocol security (IPSec), internet key exchange (IKE), virtual private network (VPN)	??
Week 6: Feb 21	Authentication	access control, password authentication, biometric authentication	??
Week 7: Feb 28	Privacy-Enhancing technologies 1	post-quantum cryptography; Fully-homomorphic encryption and applications	??
Week 8: Mar 7	Privacy-Enhancing technologies 2	commitment, zero-knowledge proofs;	??
Week 9: Mar 14	Privacy-Enhancing technologies 3	secure multiparty computation	??
Week 10: Mar 21	Security and Privacy in Practice 1	security and privacy in Blockchain	N/A
Week 11: Mar 28	Security and Privacy in Practice 2	security and privacy for AI, machine learning	N/A
Week 12: Apr 4	Final presentation 1	papers from S&P, CCS, USENIX, NDSS, CRYPTO, or EUROCRYPT	N/A
Week 13: Apr 11	Final presentation 2	papers from S&P, CCS, USENIX, NDSS, CRYPTO, or EUROCRYPT	N/A

Lecture 9: Privacy-Enhancing technologies 2: ZKP



Diffie



Rivest



Rivest



Yao



Goldwasser



Hellman



Shamir



Adelman



Adelman



Dertouzos



Micali



Rackoff

1976

**New
directions**

1977

RSA

1978

Homomorphic Enc

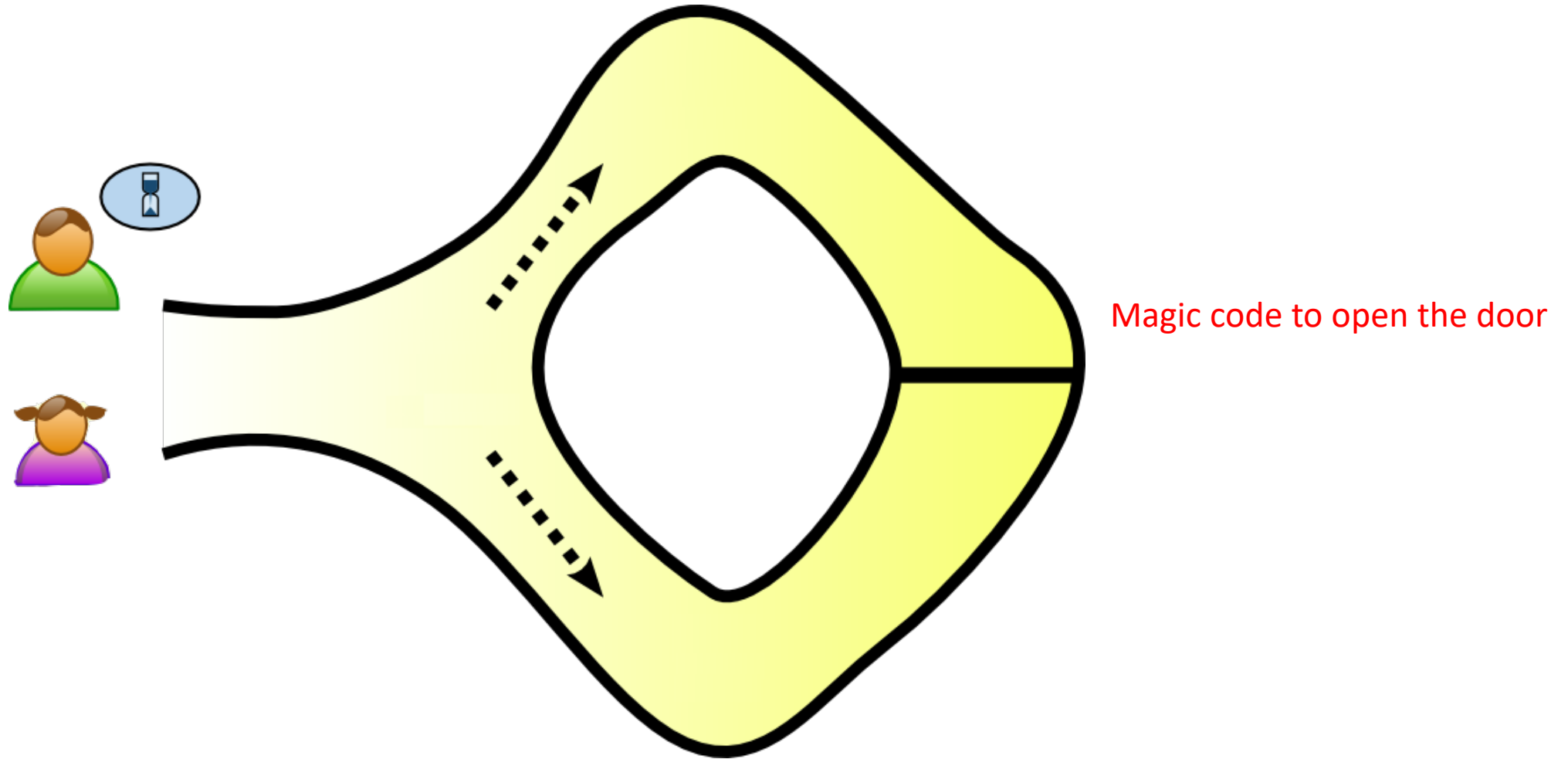
1982

MPC

1985

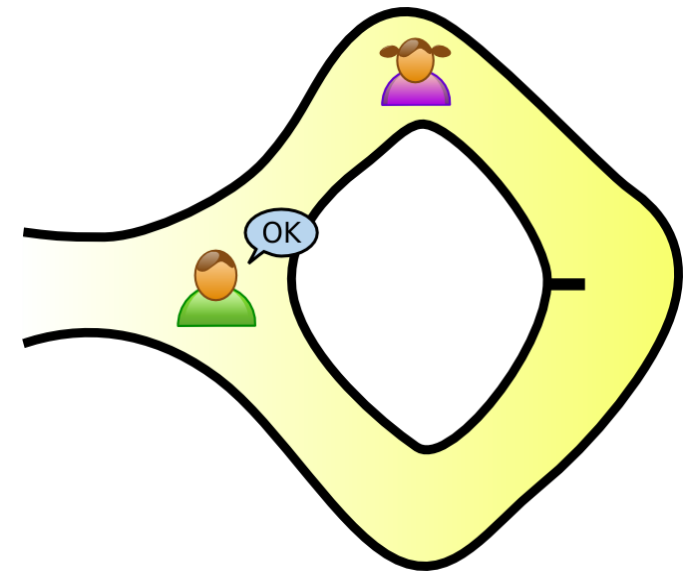
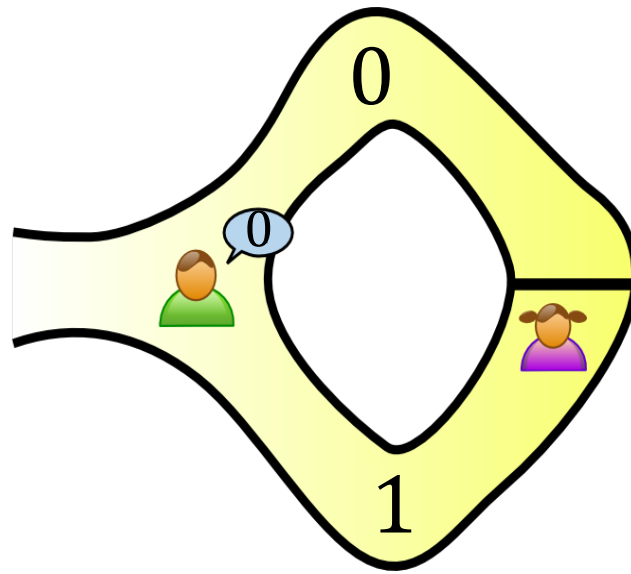
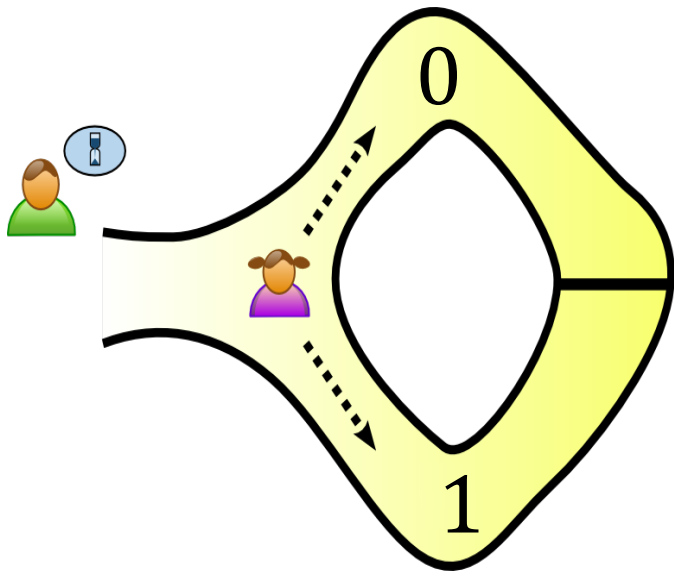
Zero Knowledge

Zero Knowledge Proof

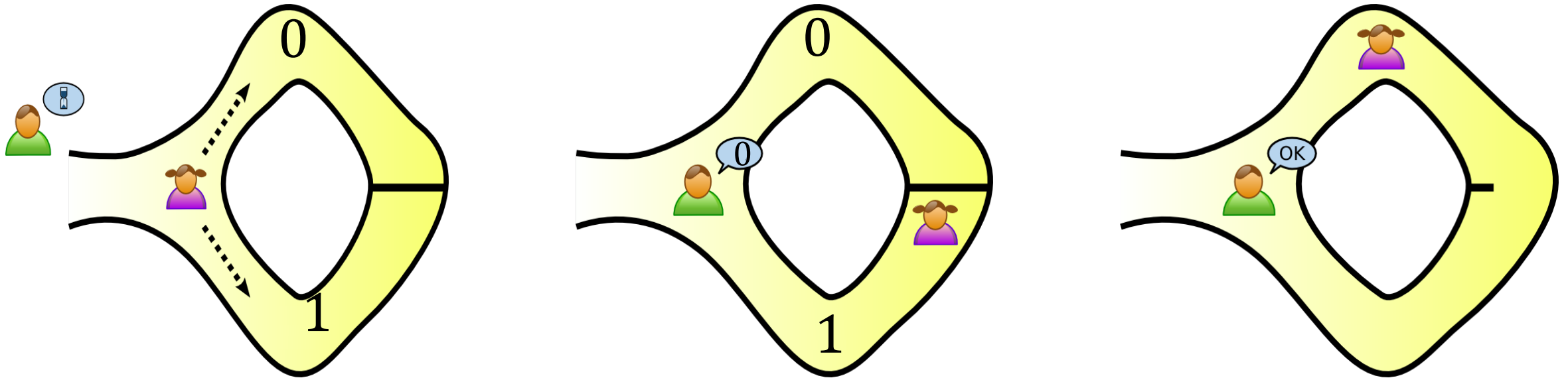




Goldwasser, Micali, Rackoff: The Knowledge Complexity of Interactive Proof-Systems (Extended Abstract)

Alibaba Cave

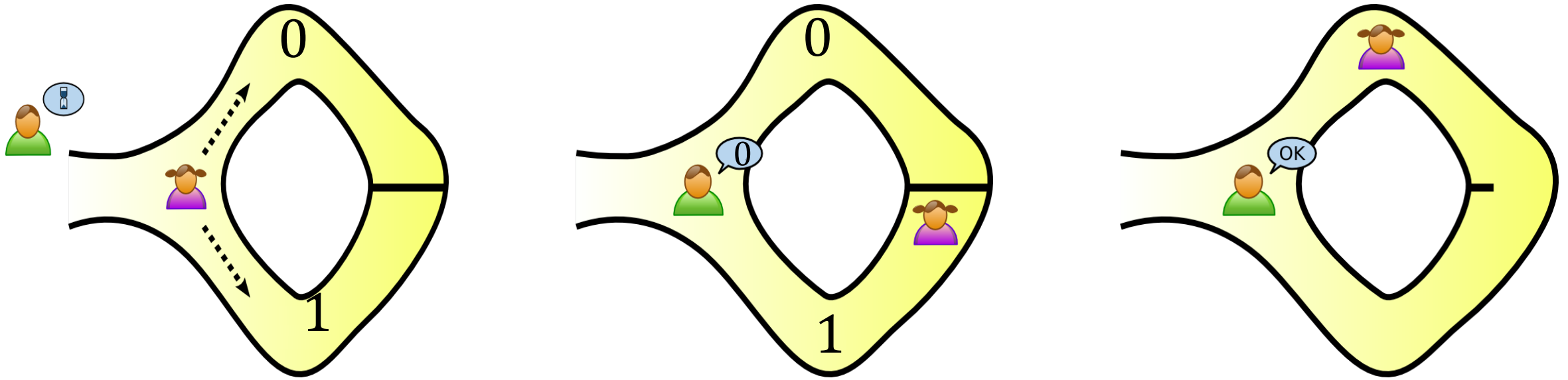




Alibaba Cave



-  doesn't know the key, the proof was accepted with 1/2.
-  learns nothing about the magic code

Repeat the game n times



- if  doesn't know the key, the proof was accepted with $\frac{1}{2^n}$.
-  learns nothing about the magic code

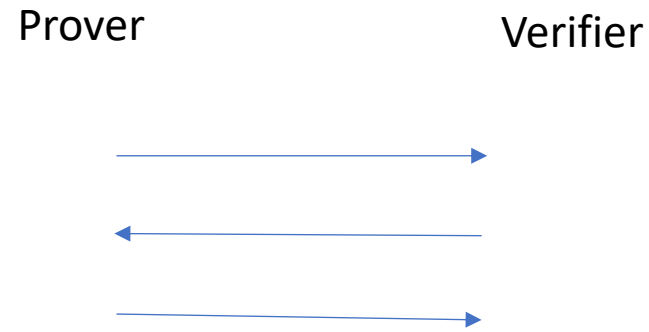
Zero Knowledge Proof for NP language

$x \in L$ if there exists a witness w s.t. $R(x, w) = 1$

$$L := \{x | \exists w \text{ s.t. } R(x, w) = 1\}$$

Zero Knowledge Proof for NP

- Prover with input (x, w) wants to prove that $x \in L$



- if $x \in L$, verifier accept
- if $x \notin L$, for any (PPT) prover, the verifier will reject
- Zero-knowledge: verifier learns nothing about w

Zero Knowledge Proof (ZKP) for NP

Theorem [GMW86]

Commitment \implies ZKP for all of NP

Theorem [GMW86]

One-way function \implies ZKP for all of NP

zk-SNARK/STARK

- Consider the complexity of the Verifier.
- Could it be less than computing $R(x, w)$?????
- This is motivated by the applications in Blockchain.

YES!!!!

PCP Theorem [AS,ALMSS,Dinur]:

NP statements have polynomial-size PCPs in which the verifier reads only $O(1)$ bits.

- Can be made ZK with small overhead [KPT97,IW04]

Lecture 9: Privacy-Enhancing technologies 2: ZKP

- ZKP various applications
 - outsource verifiable computing;
 - Honest behaviors

Zero Knowledge Proof

How does it work?

How to build efficient (and succinct) ZKP?

Privacy-Enhancing technologies 2: ZKP and MPC

Date	Topics	Outline (tentative)	Lecture notes
Week 1: Jan 10	Course Overview	course plan, reading materials, grading, brief introduction to every topic	N/A
Week 2: Jan 17	Basic Cryptography 1: Symmetric-key cryptography	symmetric encryption, one-time pad, blockcipher, hash function, MAC, authenticated encryption.	Haiyang Xue
Week 3: Jan 31	Basic Cryptography 2: Public-key cryptography	RSA, Diffie-Hellman, public key encryption, Digital signature	??
Week 4: Feb 7	Network Security Principles	authenticated key exchange, PKI, and certification authorities	??
Week 5: Feb 14	Network Security in Practice	secure sockets layer (SSL), internet protocol security (IPSec), internet key exchange (IKE), virtual private network (VPN)	??
Week 6: Feb 21	Authentication	access control, password authentication, biometric authentication	??
Week 7: Feb 28	Privacy-Enhancing technologies 1	post-quantum cryptography; Fully-homomorphic encryption and applications	??
Week 8: Mar 7	Privacy-Enhancing technologies 2	commitment, zero-knowledge proofs;	??
Week 9: Mar 14	Privacy-Enhancing technologies 3	secure multiparty computation	??
Week 10: Mar 21	Security and Privacy in Practice 1	security and privacy in Blockchain	N/A
Week 11: Mar 28	Security and Privacy in Practice 2	security and privacy for AI, machine learning	N/A
Week 12: Apr 4	Final presentation 1	papers from S&P, CCS, USENIX, NDSS, CRYPTO, or EUROCRYPT	N/A
Week 13: Apr 11	Final presentation 2	papers from S&P, CCS, USENIX, NDSS, CRYPTO, or EUROCRYPT	N/A

Lecture 9: Privacy-Enhancing technologies 3: MPC



Diffie



Rivest



Rivest



Yao



Goldwasser



Hellman



Shamir



Adelman



Adelman



Dertouzos



Micali



Rackoff

1976

**New
directions**

1977

RSA

1978

Homomorphic Ene

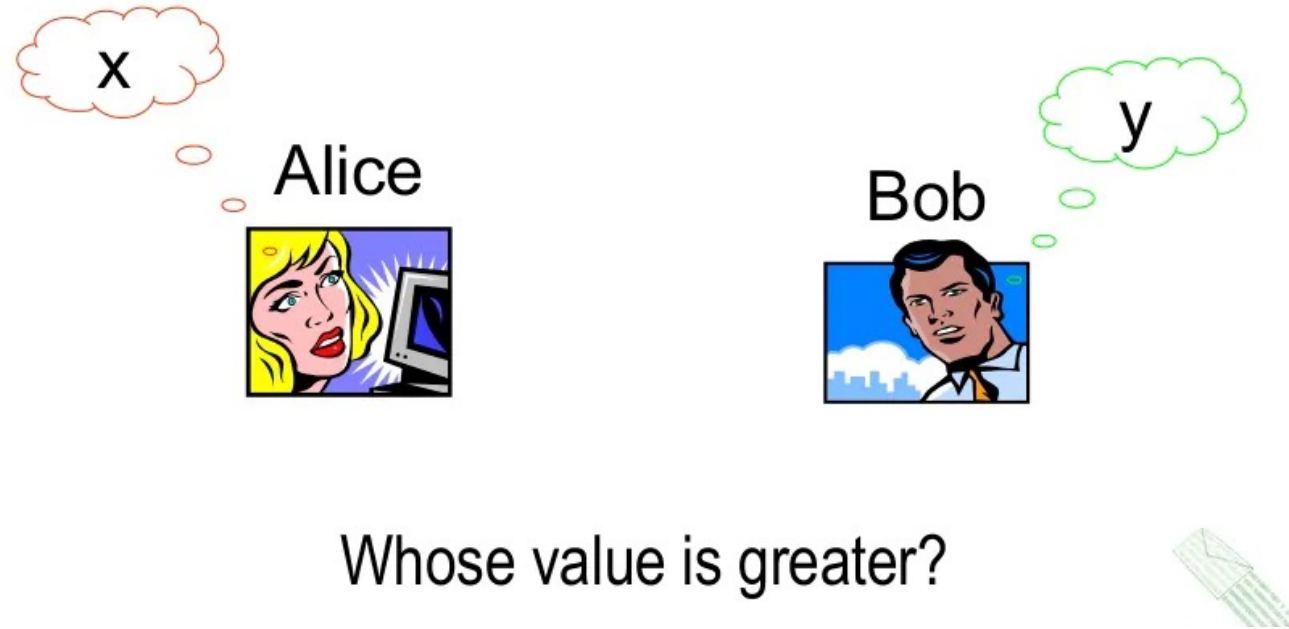
1982

MPC

1985

Zero Knowledge

Yao's Millionaires' Problem



Yao's Millionaires' Problem

$$F(x, y) = \begin{cases} (0, 1), & x < y \\ (1, 0), & x \geq y \end{cases}$$

Two-party computation

- x is Alice's input, a is her output
- y is Bob's input, b is his output

$$F(x, y) = (a, b)$$

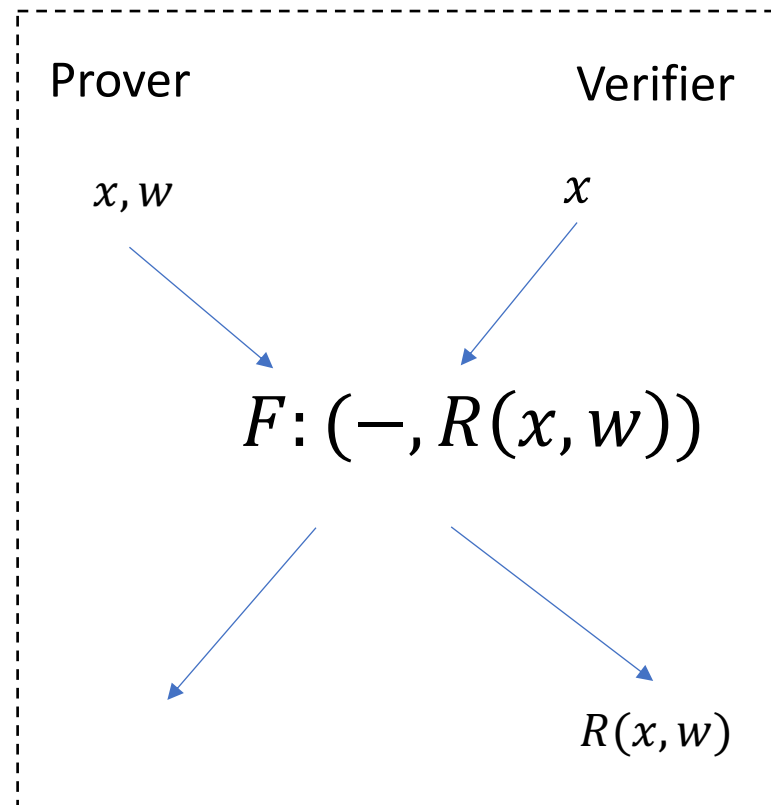
Zero-knowledge proof

$$F(x, y) = (a, b)$$

$$F((x, w), x) = (-, b), b = 1 \text{ if } x \in L$$

Zero-knowledge proof

$$F((x, w), x) = (-, b), b = R(x, w)$$



Multiparty Computation

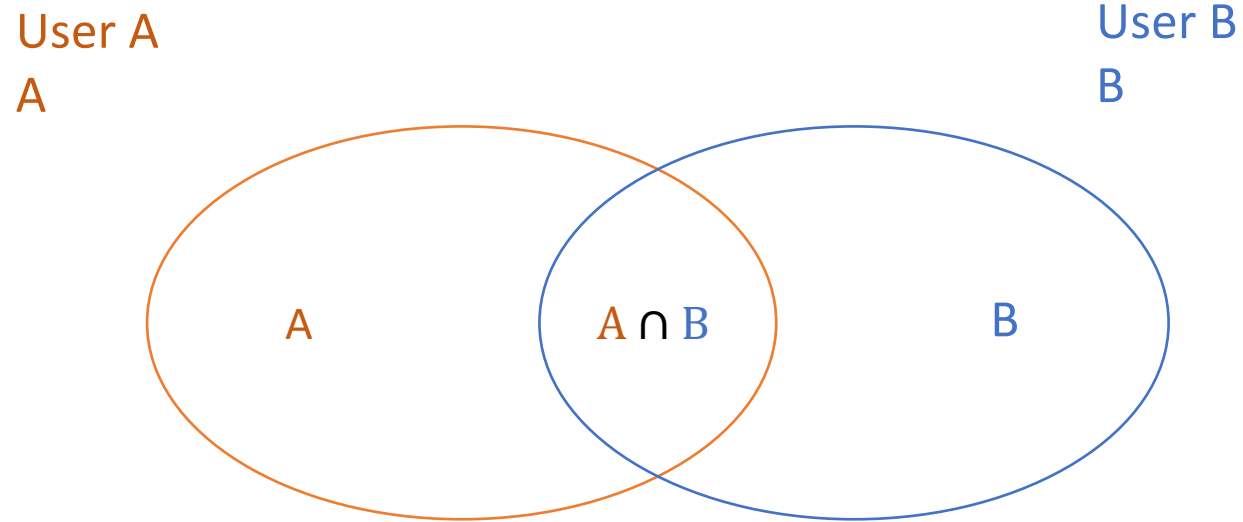
$$F(x_1, x_2, \dots, x_n) = (y_1, y_2, \dots, y_n)$$

- Electronic voting
- Bidding
- Etc.

Multiparty Computation

Two or more parties want to perform some joint computation,
While guaranteeing “security” against “adversary behavior”

Example: Private set intersection



Chrome: [password checkup](#)

A is the set of your **Autofill** passwords, and B is the database of leaked accounts

How does it work?

How to build efficient MPC?

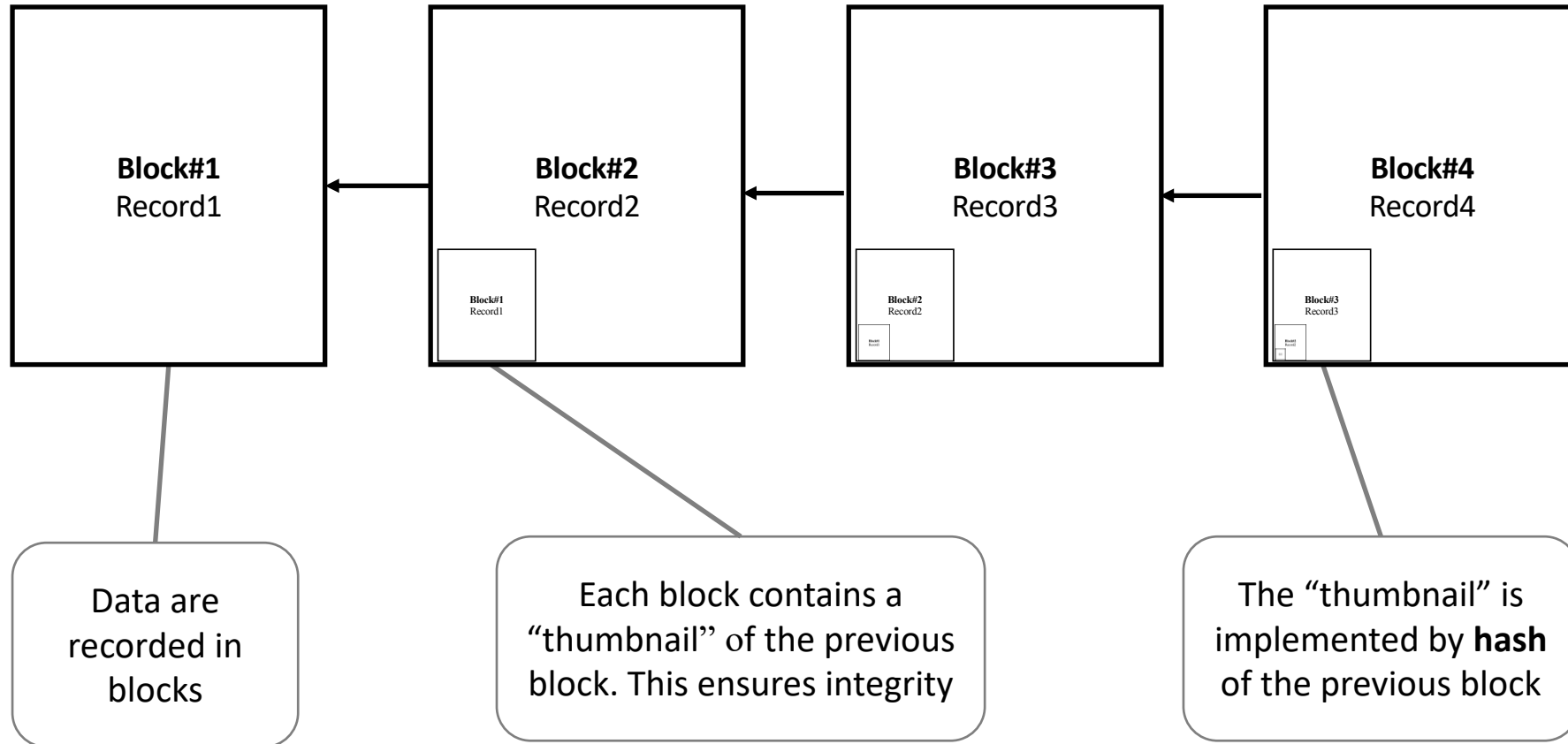
Case Studies 1: Blockchain

Date	Topics	Outline (tentative)	Lecture notes
Week 1: Jan 10	Course Overview	course plan, reading materials, grading, brief introduction to every topic	N/A
Week 2: Jan 17	Basic Cryptography 1: Symmetric-key cryptography	symmetric encryption, one-time pad, blockcipher, hash function, MAC, authenticated encryption.	Haiyang Xue
Week 3: Jan 31	Basic Cryptography 2: Public-key cryptography	RSA, Diffie-Hellman, public key encryption, Digital signature	??
Week 4: Feb 7	Network Security Principles	authenticated key exchange, PKI, and certification authorities	??
Week 5: Feb 14	Network Security in Practice	secure sockets layer (SSL), internet protocol security (IPSec), internet key exchange (IKE), virtual private network (VPN)	??
Week 6: Feb 21	Authentication	access control, password authentication, biometric authentication	??
Week 7: Feb 28	Privacy-Enhancing technologies 1	post-quantum cryptography; Fully-homomorphic encryption and applications	??
Week 8: Mar 7	Privacy-Enhancing technologies 2	commitment, zero-knowledge proofs;	??
Week 9: Mar 14	Privacy-Enhancing technologies 3	secure multiparty computation	??
Week 10: Mar 21	Security and Privacy in Practice 1	security and privacy in Blockchain	N/A
Week 11: Mar 28	Security and Privacy in Practice 2	security and privacy for AI, machine learning	N/A
Week 12: Apr 4	Final presentation 1	papers from S&P, CCS, USENIX, NDSS, CRYPTO, or EUROCRYPT	N/A
Week 13: Apr 11	Final presentation 2	papers from S&P, CCS, USENIX, NDSS, CRYPTO, or EUROCRYPT	N/A

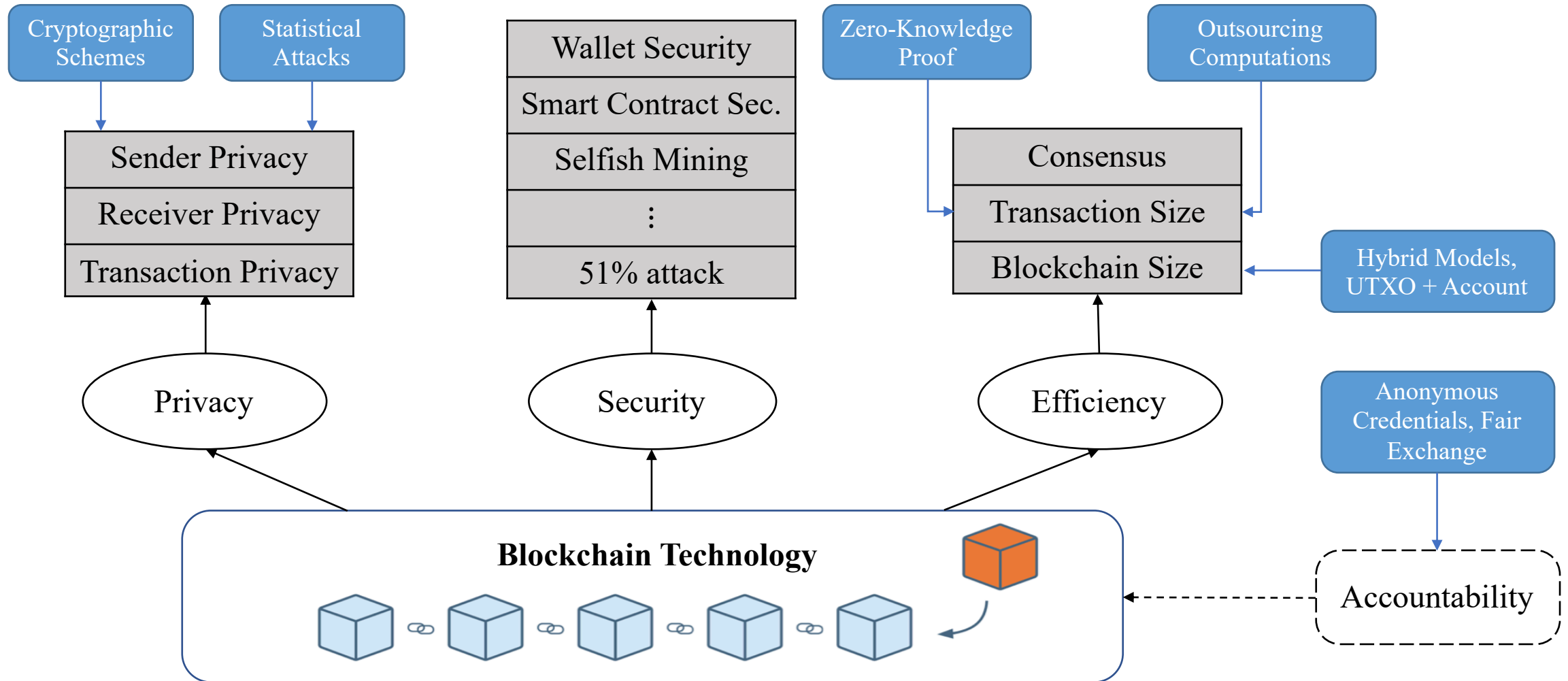
Lecture 11: Case Studies 1: Blockchain

- What is Blockchain
- Security in blockchain
 - Ex. Wallet security
- Privacy in blockchain
 - Ex. private tx,

Blockchain: A public ledger



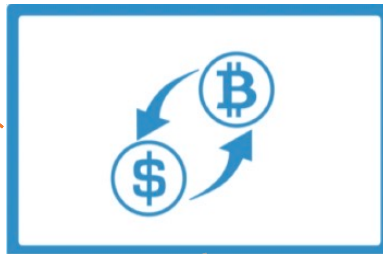
Security and privacy issues



Blockchain-based Cryptocurrency

>\$ 381 B

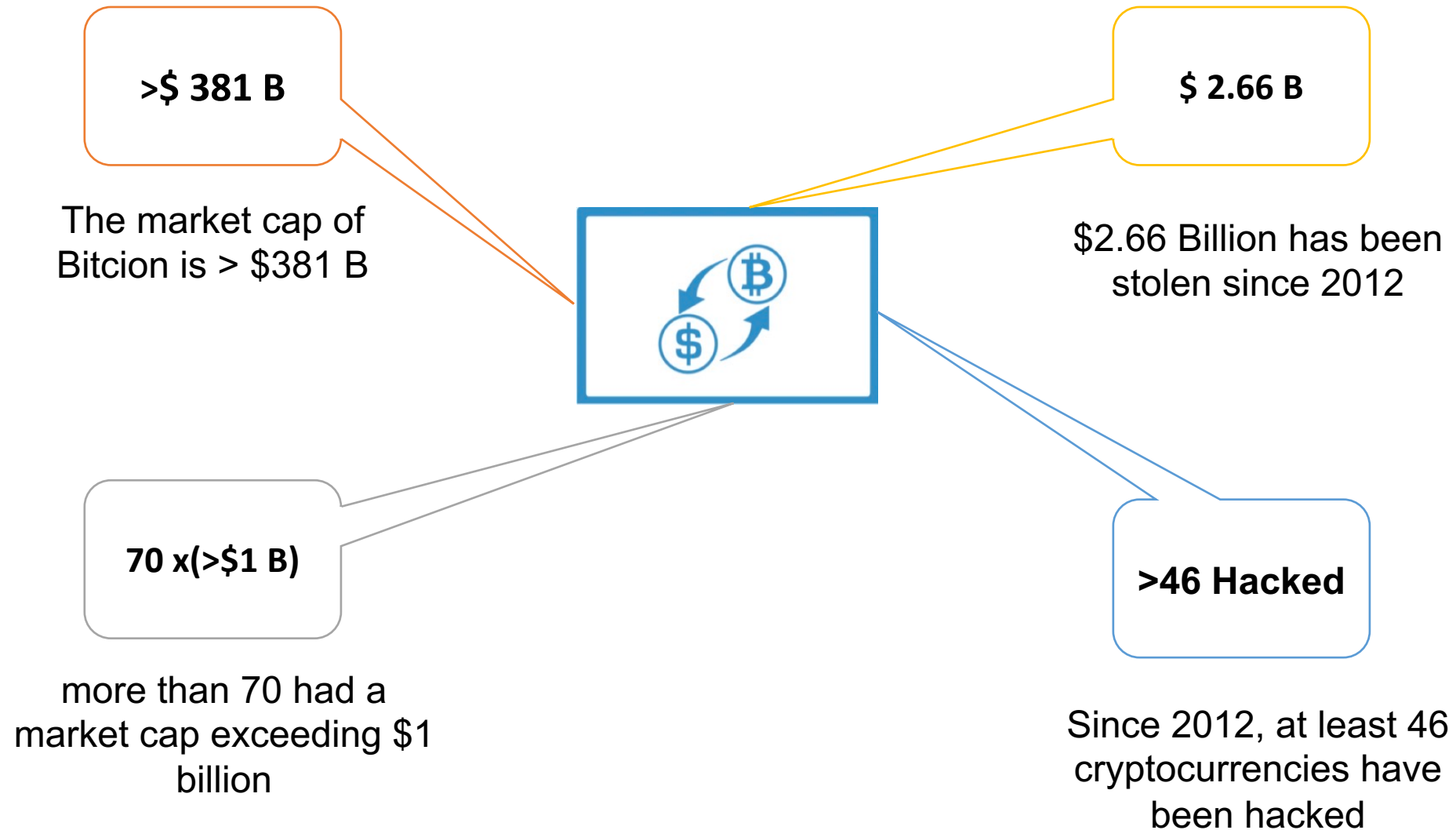
The market capitalization of Bitcoin is > \$381 B



9000
70 x(>\$1 B)

more than 70 had a market cap exceeding \$1 billion

Cryptocurrency (wallet) security



List of Hacked Cryptocurrencies

Bitcoin's Biggest loss

At the beginning of 2014, Mt Gox was handling 70% of Bitcoin's transactions.

In Feb. 2014, Mt. Gox lost about 740,000 bitcoins (6% of all bitcoin in existence at the time) due to a "leak" in the wallet.

DATE	EXCHANGE	CAUSE OF HACK	AMOUNT STOLEN (USD)
2022, January 17	Crypto.com	Unknown	\$34 million
2021, December 11	AscendEX	Obtained access to hot wallet	\$80 million
2021, December 5	BitMart	Obtained access to hot wallet	\$150 million
2021, August 19	Liquid	Obtained access to hot wallet	\$97 million
2021, April 29	Hotbit	Obtained access to hot wallet	Nil
2020, December 23	Livecoin	Compromised system/servers	Unknown
2020, December 21	EXMO	Obtained access to hot wallet	\$4 million
2020, December 1	BTC Markets	Internal staff error/mistake	270,000 user's private details
2020, September 25	KuCoin	Data leak	\$275 million
2020, July 11	Cashaa	Malware	\$3.1 million
2020, June 29	Balancer	Vulnerability in protocol	\$500,000
2020, April 19	Lendf.me	Bugs and Re-entrancy attack	\$24.5 million
2020, April 19	Uniswap	Bugs and Re-entrancy	\$500,000

<https://cryptosec.info/exchange-hacks/>

<https://www.hedgewithcrypto.com/cryptocurrency-exchange-hacks/>

2023/1/10

113/129

Loss of key = loss of money



A transaction in bitcoin looks like

Tr_1 :
Alice sends
\$100 to Bob

 $h = \text{hash}(Tr_1)$

Signature (sk_A, h)

The private key sk_A is the only
secret that Alice uses to
generate this transaction

Signature is the
standard ECDSA
proposed by NIST

Lessons Learned

In cryptocurrency, we need to protect the private key

- **Cold Wallet:** a hardware wallet only stores and protects your **private key**.



- **Threshold Cryptography:** Distribute the trust

Blockchain: The need of privacy

- Supply chain privacy
 - A car company does not want to reveal how much it pays to its supplier

- Payment Privacy
 - A company wants to keep its employee's salaries private

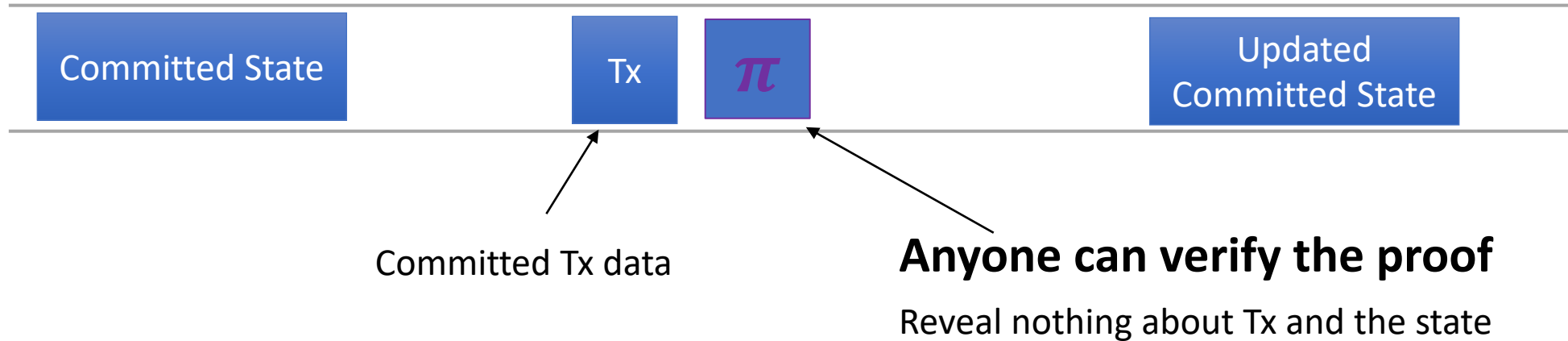
Blockchain: The need of privacy

Can we have private transactions over a public blockchain?

- Seems impossible
 - Universal verifiability --- > transaction data must be public
 - Otherwise, how can we verify the Tx
- Crypto magic
 - Crypto --- > Private Tx on a publicly verifiable blockchain

Blockchain: The need of privacy

Public Blockchain



- **Committed data** : short (hiding) commitment of data
- **Proof π** : short zero-knowledge proof that
 - Committed Tx data is consistent with the committed state
 - The updated committed state is correct

Date	Topics	Outline (tentative)	Lecture notes
Week 1: Jan 10	Course Overview	course plan, reading materials, grading, brief introduction to every topic	N/A
Week 2: Jan 17	Basic Cryptography 1: Symmetric-key cryptography	symmetric encryption, one-time pad, blockcipher, hash function, MAC, authenticated encryption.	Haiyang Xue
Week 3: Jan 31	Basic Cryptography 2: Public-key cryptography	RSA, Diffie-Hellman, public key encryption, Digital signature	??
Week 4: Feb 7	Network Security Principles	authenticated key exchange, PKI, and certification authorities	??
Week 5: Feb 14	Network Security in Practice	secure sockets layer (SSL), internet protocol security (IPSec), internet key exchange (IKE), virtual private network (VPN)	??
Week 6: Feb 21	Authentication	access control, password authentication, biometric authentication	??
Week 7: Feb 28	Privacy-Enhancing technologies 1	post-quantum cryptography; Fully-homomorphic encryption and applications	??
Week 8: Mar 7	Privacy-Enhancing technologies 2	commitment, zero-knowledge proofs;	??
Week 9: Mar 14	Privacy-Enhancing technologies 3	secure multiparty computation	??
Week 10: Mar 21	Security and Privacy in Practice 1	security and privacy in Blockchain	N/A
Week 11: Mar 28	Security and Privacy in Practice 2	security and privacy for AI, machine learning	N/A
Week 12: Apr 4	Final presentation 1	papers from S&P, CCS, USENIX, NDSS, CRYPTO, or EUROCRYPT	N/A
Week 13: Apr 11	Final presentation 2	papers from S&P, CCS, USENIX, NDSS, CRYPTO, or EUROCRYPT	N/A

Case studies 2: Privacy problem with AI?

- Artificial Intelligence: uses machine learning (ML) algorithms to make predictions
 - Input: **your data** & **ML parameters**
 - Output: some recommendation, decision, or classification
- Privacy problem:
 - you have to input **your data** in order to get the valuable prediction!
 - AI server provides **parameters**, and earns money

Case studies 2: Privacy problem with AI?

- Privacy problem:
 - you have to input **your data** in order to get the valuable prediction!
 - AI server provides **parameters**, and earns money

- Could FHE and MPC help us to achieve
- keeping privacy of both **your data** and AI's **parameters**?



Lecture 12-13 Final presentation

Date	Topics	Lecture notes
Week 1: Jan 10	Course Overview	N/A
Week 2: Jan 17	Basic Cryptography 1: Symmetric-key cryptography	Haiyang Xue
Week 3: Jan 31	Basic Cryptography 2: Public-key cryptography	??
Week 4: Feb 7	Network Security Principles	??
Week 5: Feb 14	Network Security in Practice	??
Week 6: Feb 21	Authentication	??
Week 7: Feb 28	Privacy-Enhancing technologies 1	??
Week 8: Mar 7	Privacy-Enhancing technologies 2	??
Week 9: Mar 14	Privacy-Enhancing technologies 3	??
Week 10: Mar 21	Security and Privacy in Practice 1	N/A
Week 11: Mar 28	Security and Privacy in Practice 2	N/A
Week 12: Apr 4	Final presentation 1	N/A
Week 13: Apr 11	Final presentation 2	N/A

Lecture notes

Date	Topics	Lecture notes
Week 1: Jan 10	Course Overview	N/A
Week 2: Jan 17	Basic Cryptography 1: Symmetric-key cryptography	Haiyang Xue
Week 3: Jan 31	Basic Cryptography 2: Public-key cryptography	??
Week 4: Feb 7	Network Security Principles	??
Week 5: Feb 14	Network Security in Practice	??
Week 6: Feb 21	Authentication	??
Week 7: Feb 28	Privacy-Enhancing technologies 1	??
Week 8: Mar 7	Privacy-Enhancing technologies 2	??
Week 9: Mar 14	Privacy-Enhancing technologies 3	??
Week 10: Mar 21	Security and Privacy in Practice 1	N/A
Week 11: Mar 28	Security and Privacy in Practice 2	N/A
Week 12: Apr 4	Final presentation 1	N/A
Week 13: Apr 11	Final presentation 2	N/A

Choose lecture

Thank you
and two more examples

Security Examples



<https://kentonbrothers.com/generalinfo/1984/>

An example from Yoshi Kohno

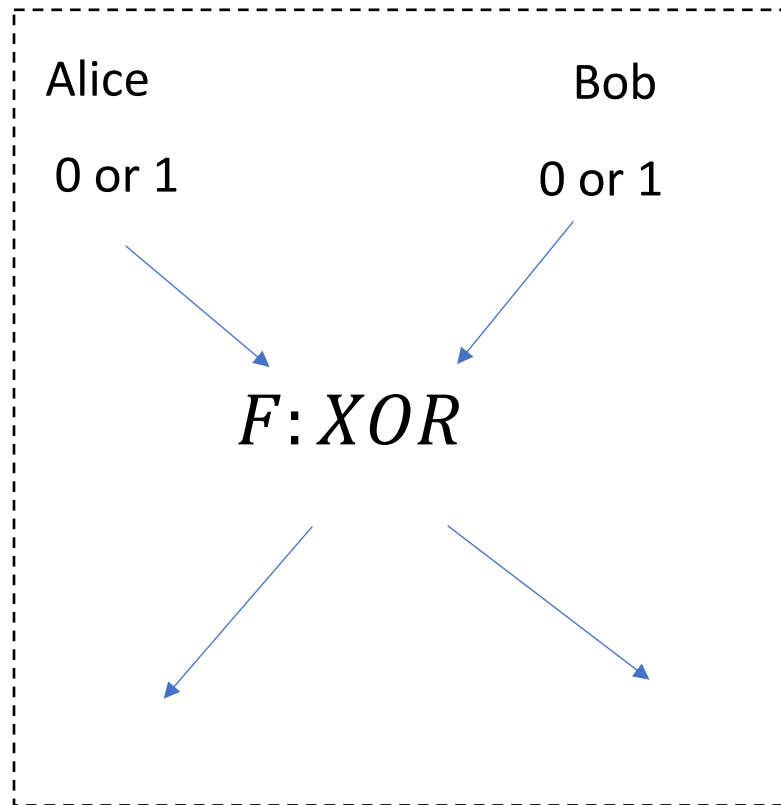
A fun privacy problem

- Bob and Alice want to check if they are interested in dating
 - If both are yes, the output is yes
 - If one is no, the output is no
- If Bob says NO, the output is always NO, no matter whether Alice said YES or NO.
 - Alice does not lose face.



<Pride and Prejudice>

A fun privacy problem



<Pride and Prejudice>

Lecture 3: Public-key cryptography

- Case studies

- WhatsApp



Public Key Types

- **Identity Key Pair** – A long-term Curve25519 key pair, generated at install time.
- **Signed Pre Key** – A medium-term Curve25519 key pair, generated at install time, signed by the **Identity Key**, and rotated on a periodic timed basis.
- **One-Time Pre Keys** – A queue of Curve25519 key pairs for one time use, generated at install time, and replenished as needed.

Session Key Types

- **Root Key** – A 32-byte value that is used to create **Chain Keys**.
- **Chain Key** – A 32-byte value that is used to create **Message Keys**.
- **Message Key** – An 80-byte value that is used to encrypt message contents. 32 bytes are used for an AES-256 key, 32 bytes for a HMAC-SHA256 key, and 16 bytes for an IV.