

Cryptography for the quantum internet

Elements of a “quantum TLS”

Christian Majenz

Colloquium

Informatics Institute, University of Amsterdam



Quantum computers

Quantum computers

- ▶ Accelerating effort to build a quantum computer

Quantum computers

- ▶ Accelerating effort to build a quantum computer
- ▶ Major investments:



Microsoft



QUANTUM
FLAGSHIP

Quantum computers

- ▶ Accelerating effort to build a quantum computer
- ▶ Major investments:



QUANTUM
FLAGSHIP

- ▶ Many applications! (In theory)

- Quantum chemistry
- Quantum Key Distribution
- Quantum Money
- Cryptanalysis
- Machine learning
- Distributed quantum computing
- Multiparty quantum computation
- ...

Quantum computers

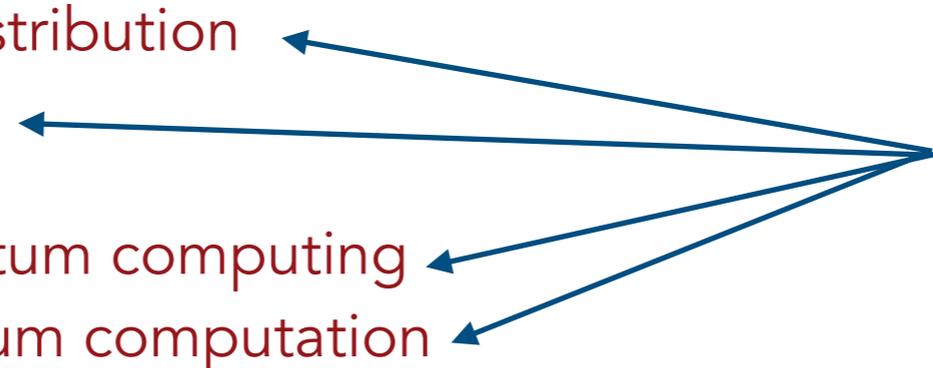
- ▶ Accelerating effort to build a quantum computer
- ▶ Major investments:



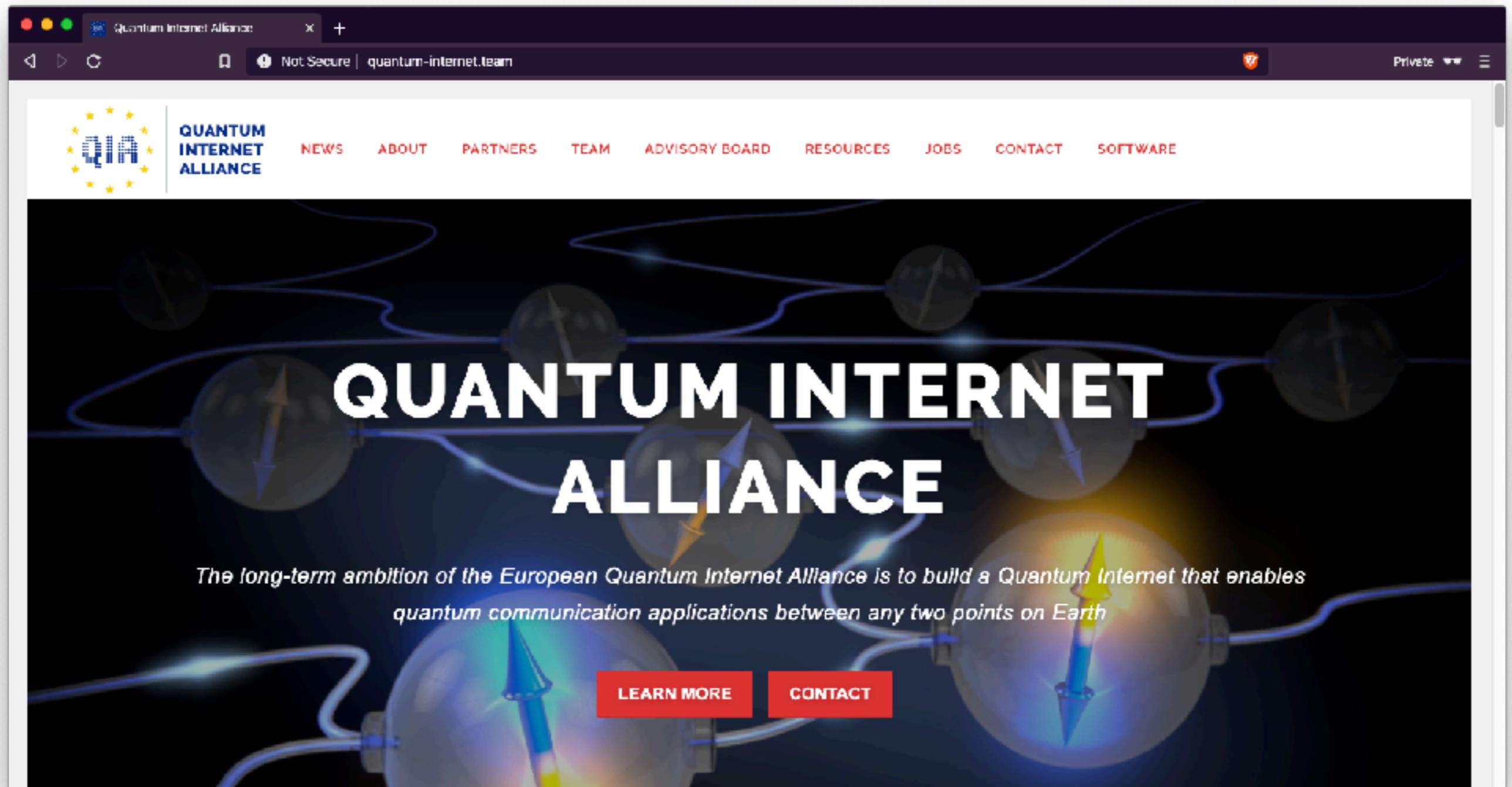
- ▶ Many applications! (In theory)

- Quantum chemistry
- Quantum Key Distribution
- Quantum Money
- Cryptanalysis
- Machine learning
- Distributed quantum computing
- Multiparty quantum computation
- ...

Need a quantum network!



Quantum internet



The image shows a browser window displaying the homepage of the Quantum Internet Alliance. The browser's address bar shows the URL "quantum-internet.team" and a "Not Secure" warning. The website header features the QIA logo, which consists of the letters "QIA" in a stylized font surrounded by yellow stars, and the text "QUANTUM INTERNET ALLIANCE" to its right. A navigation menu in red text includes links for "NEWS", "ABOUT", "PARTNERS", "TEAM", "ADVISORY BOARD", "RESOURCES", "JOBS", "CONTACT", and "SOFTWARE". The main content area has a dark background with glowing blue and yellow lines and spheres. The title "QUANTUM INTERNET ALLIANCE" is written in large, bold, white capital letters. Below the title, a paragraph of text reads: "The long-term ambition of the European Quantum Internet Alliance is to build a Quantum Internet that enables quantum communication applications between any two points on Earth". At the bottom of this section, there are two red buttons with white text: "LEARN MORE" and "CONTACT".

Quantum Internet Alliance

NEWS ABOUT PARTNERS TEAM ADVISORY BOARD RESOURCES JOBS CONTACT SOFTWARE

QUANTUM INTERNET ALLIANCE

The long-term ambition of the European Quantum Internet Alliance is to build a Quantum Internet that enables quantum communication applications between any two points on Earth

LEARN MORE CONTACT

Quantum internet



Quantum internet



Quantum internet



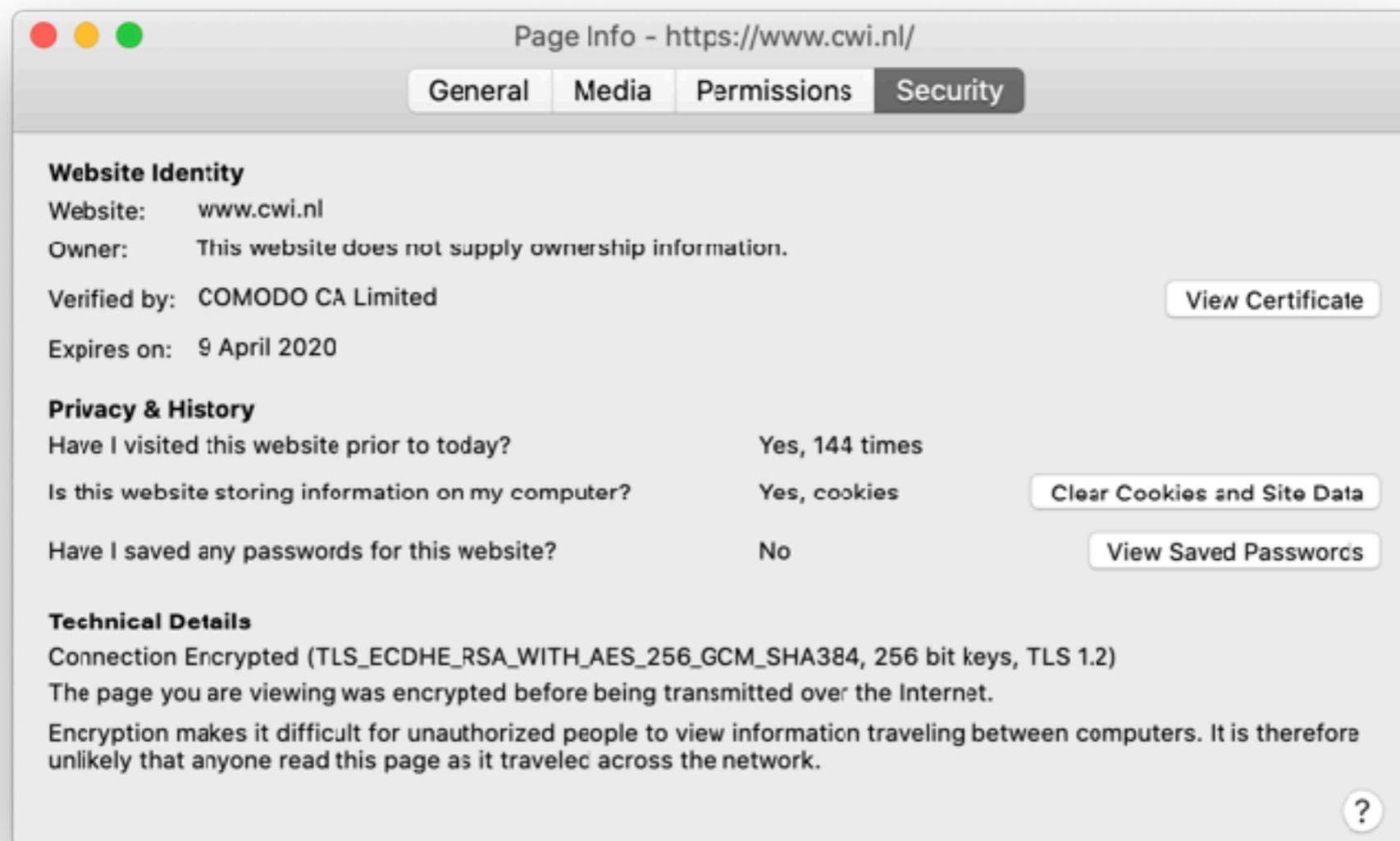
How can we secure the
Quantum internet?

Internet crypto

Let's have a look how the classical internet is secured.

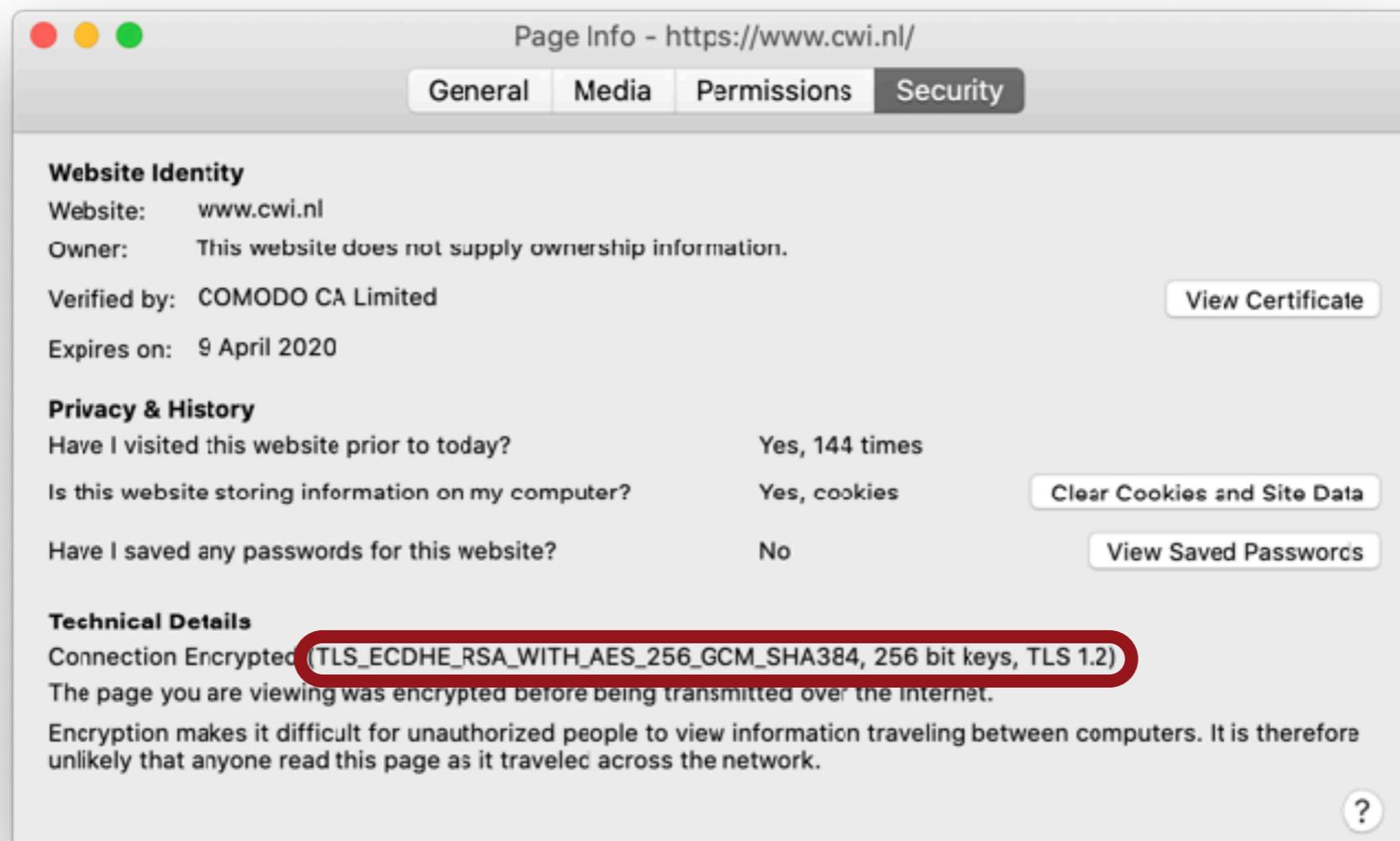
Internet crypto

Let's have a look how the classical internet is secured.



Internet crypto

Let's have a look how the classical internet is secured.



The TLS protocol

The TLS protocol

Functionalities

The TLS protocol

Functionalities

(Server)
authentication

The TLS protocol

Functionalities

(Server)
authentication

Key
establishment

The TLS protocol

Functionalities

**(Server)
authentication**

**Key
establishment**

**Secure
communication
Session**

The TLS protocol

Functionalities

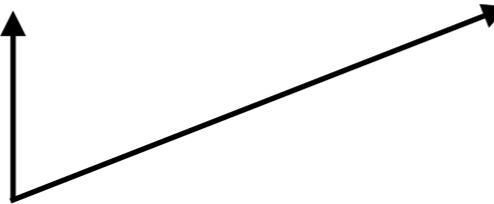
**(Server)
authentication**

**Key
establishment**

**Secure
communication
Session**

Protocols

**Digital
signatures**



The TLS protocol

Functionalities

**(Server)
authentication**

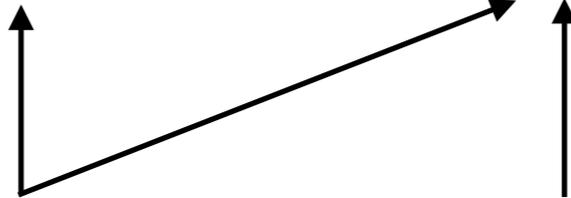
**Key
establishment**

**Secure
communication
Session**

Protocols

**Digital
signatures**

**Key exchange/
Key
encapsulation**



The TLS protocol

Functionalities

**(Server)
authentication**

**Key
establishment**

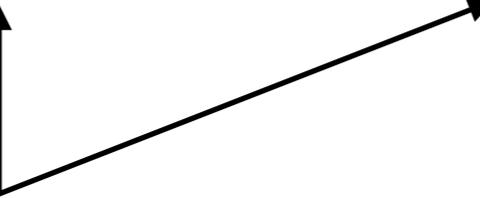
**Secure
communication
Session**

Protocols

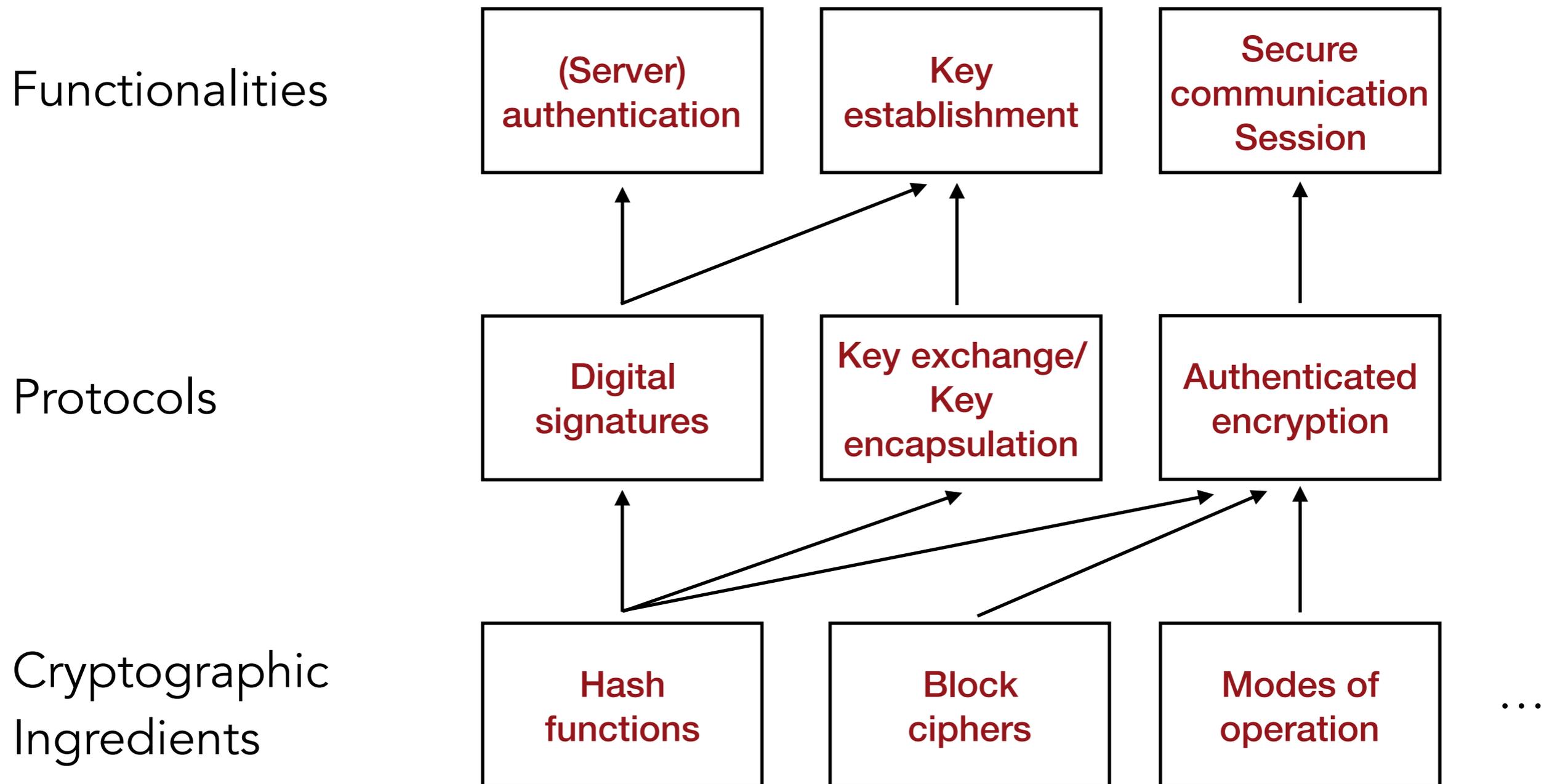
**Digital
signatures**

**Key exchange/
Key
encapsulation**

**Authenticated
encryption**



The TLS protocol



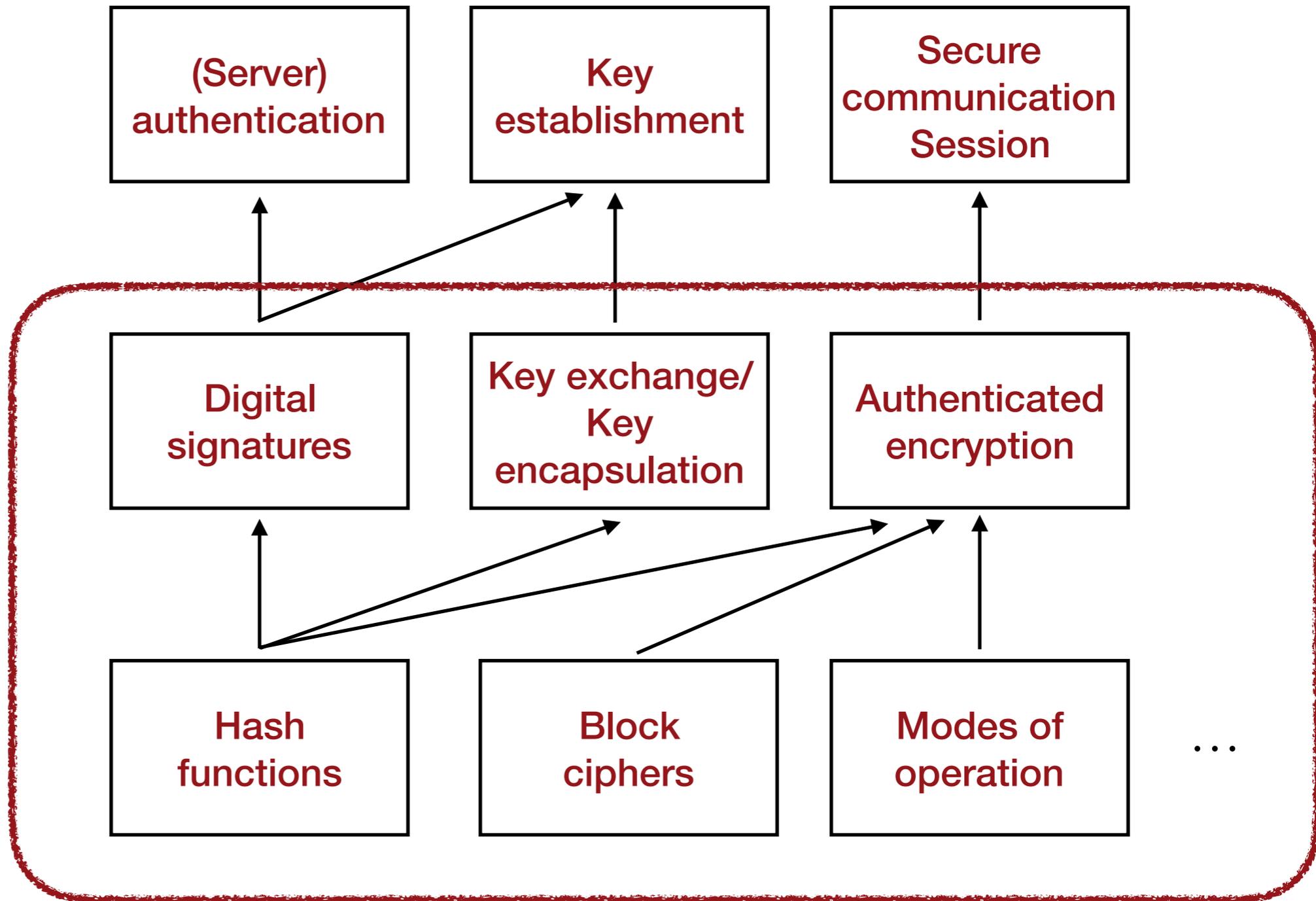
The TLS protocol

Functionalities

Protocols

Cryptographic
Ingredients

Quantum-
ready?



Outline

- ▶ Are we ready for encrypting the quantum internet?
 - Digital signatures I
 - Hash functions
 - Digital signatures II
 - Key exchange/key encapsulation
 - Authenticated Encryption
- ▶ Summary and open problems

Are we ready for encrypting the quantum internet?

Digital Signatures I



Digital signatures

Digital signatures



Alice

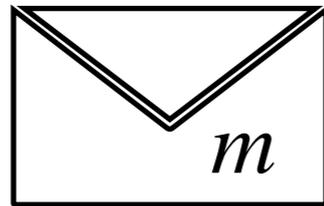


Bob

Digital signatures

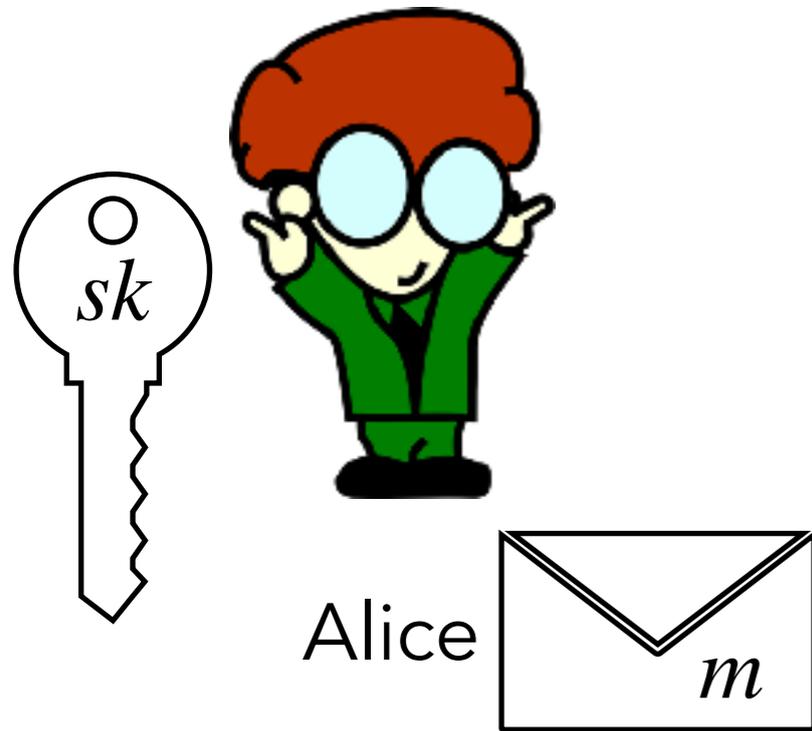
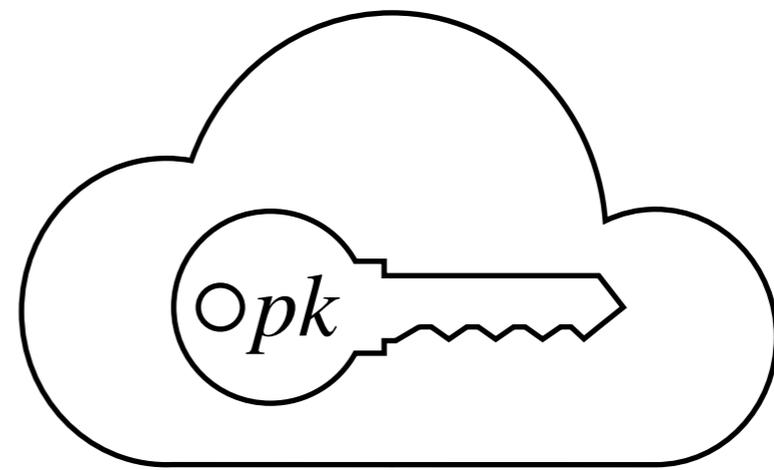


Alice

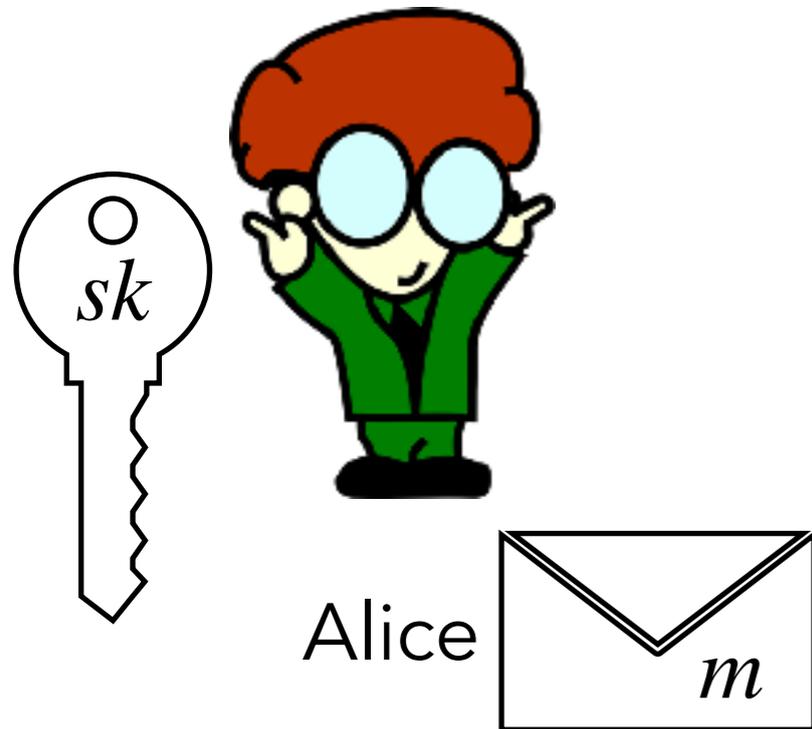
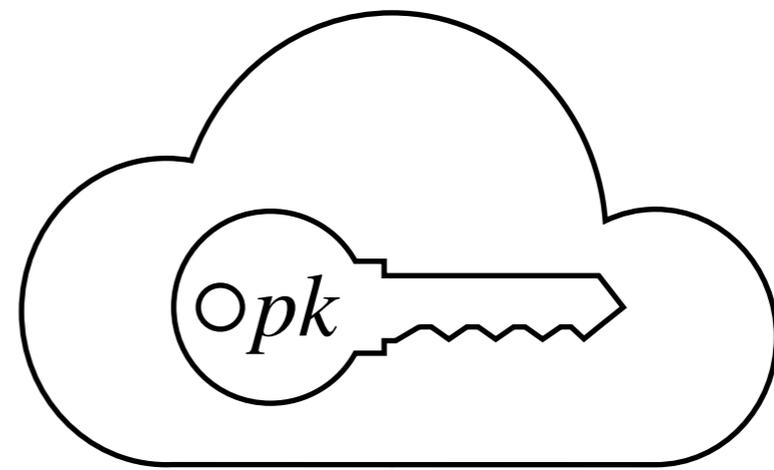


Bob

Digital signatures



Digital signatures

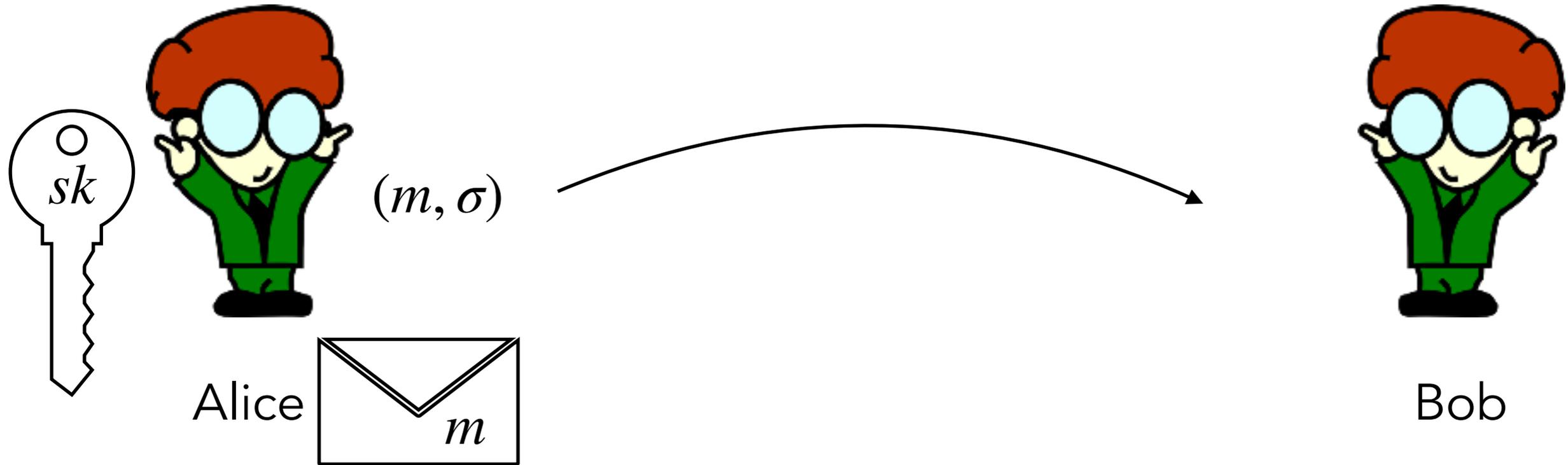
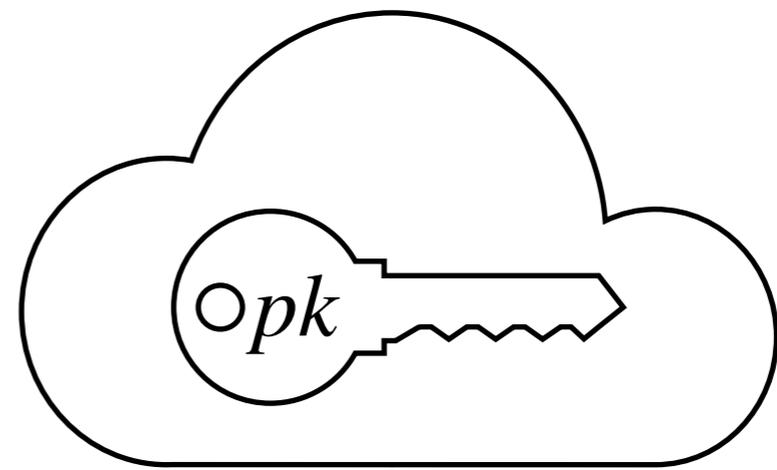


$$\sigma = \text{Sign}_{sk}(m)$$



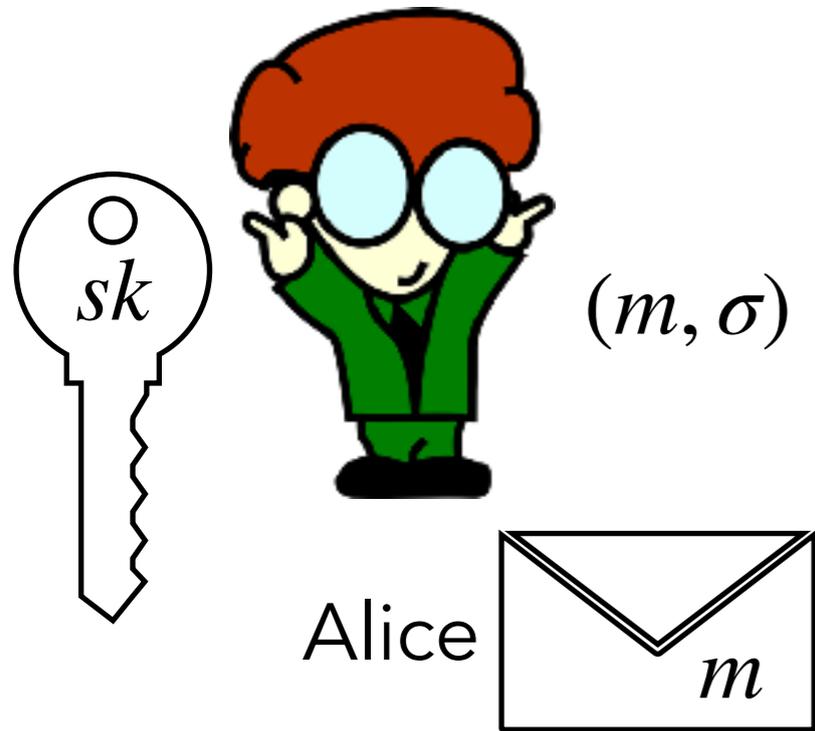
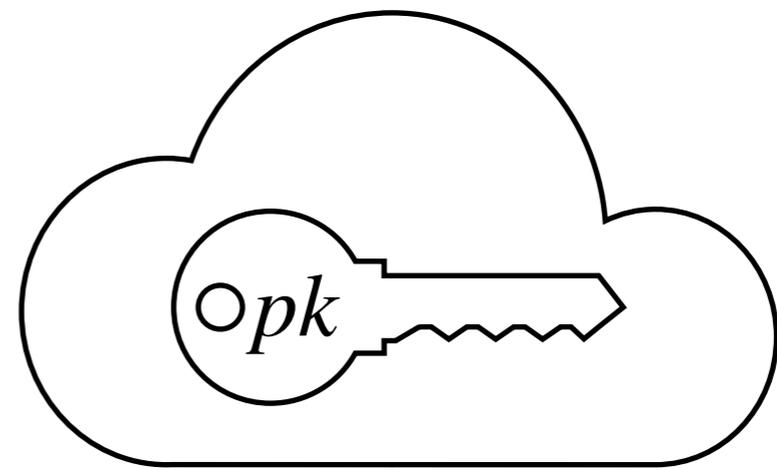
Bob

Digital signatures



$$\sigma = \text{Sign}_{sk}(m)$$

Digital signatures



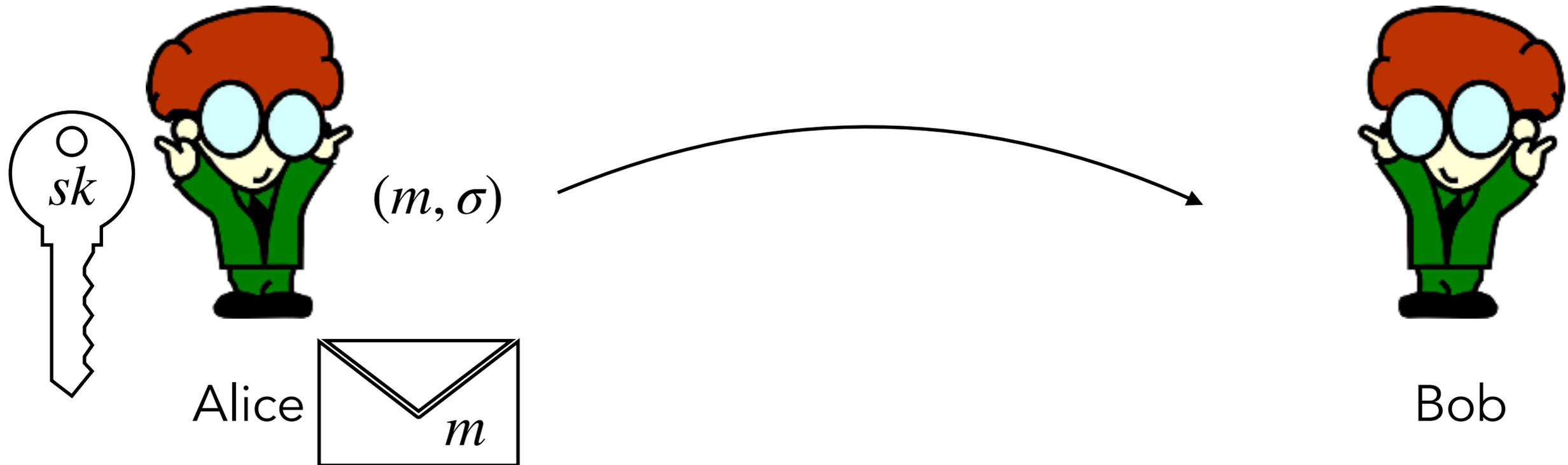
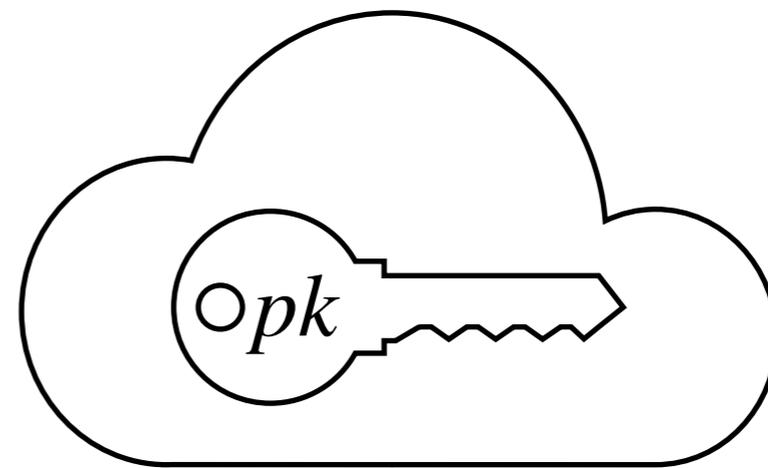
$$\sigma = \text{Sign}_{sk}(m)$$



Bob

$$\text{Ver}_{pk}(m, \sigma) = \text{accept}$$

Digital signatures

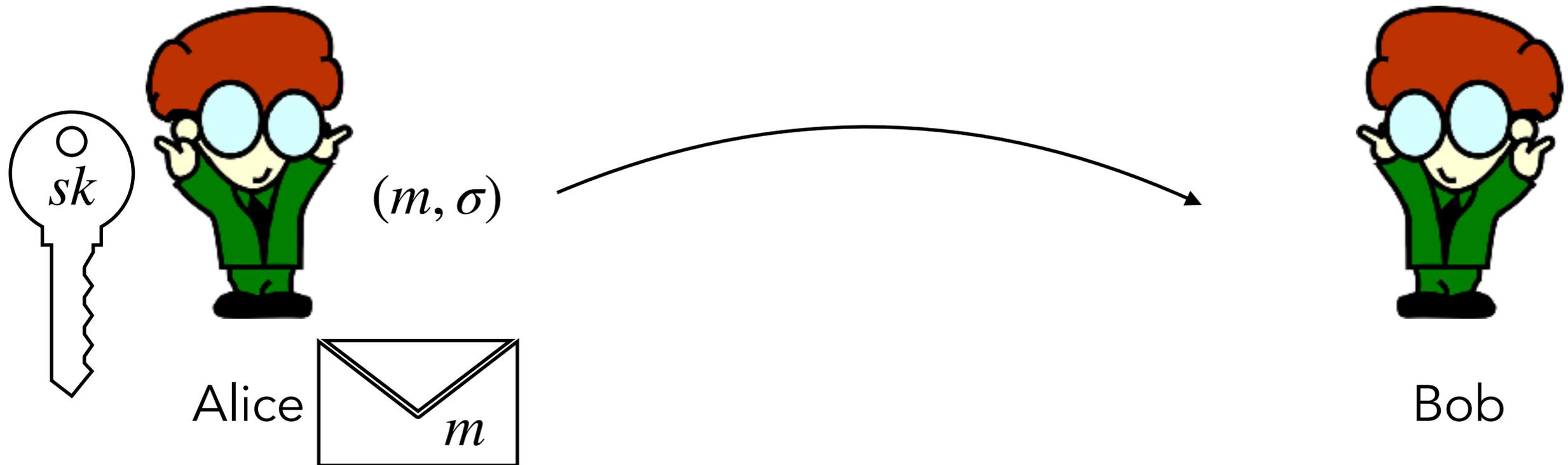
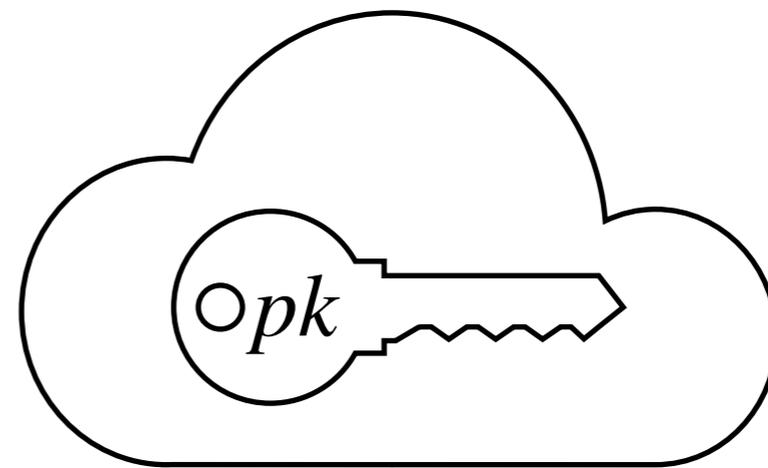


$$\sigma = \text{Sign}_{sk}(m)$$

$$\text{Ver}_{pk}(m, \sigma) = \text{accept}$$

Security: If (m', σ') was produced from (m, σ) without using sk , then $\text{Ver}_{pk}(m', \sigma') = \text{reject}$

Digital signatures



$$\sigma = \text{Sign}_{sk}(m)$$

$$\text{Ver}_{pk}(m, \sigma) = \text{accept}$$

Security: If (m', σ') was produced from (m, σ) without using sk , then $\text{Ver}_{pk}(m', \sigma') = \text{reject}$

Slightly simplified...

Quantum digital signatures

What about signatures for quantum messages?

Quantum digital signatures

What about signatures for quantum messages?

Theorem (Barnum et al. '02; Alagic, Gagliardoni, M '18):
Quantum information cannot be signed.

Quantum digital signatures

What about signatures for quantum messages?

Theorem (Barnum et al. '02; Alagic, Gagliardoni, M '18):
Quantum information cannot be signed.

Consequence of linearity of quantum theory, uses tools like
"Channel Uhlman" (Kretschman '06)

Quantum digital signatures

What about signatures for quantum messages?

Theorem (Barnum et al. '02; Alagic, Gagliardoni, M '18):
Quantum information cannot be signed.

Consequence of linearity of quantum theory, uses tools like
"Channel Uhlman" (Kretschman '06)

Is this the end of "Project
Quantum TLS"?

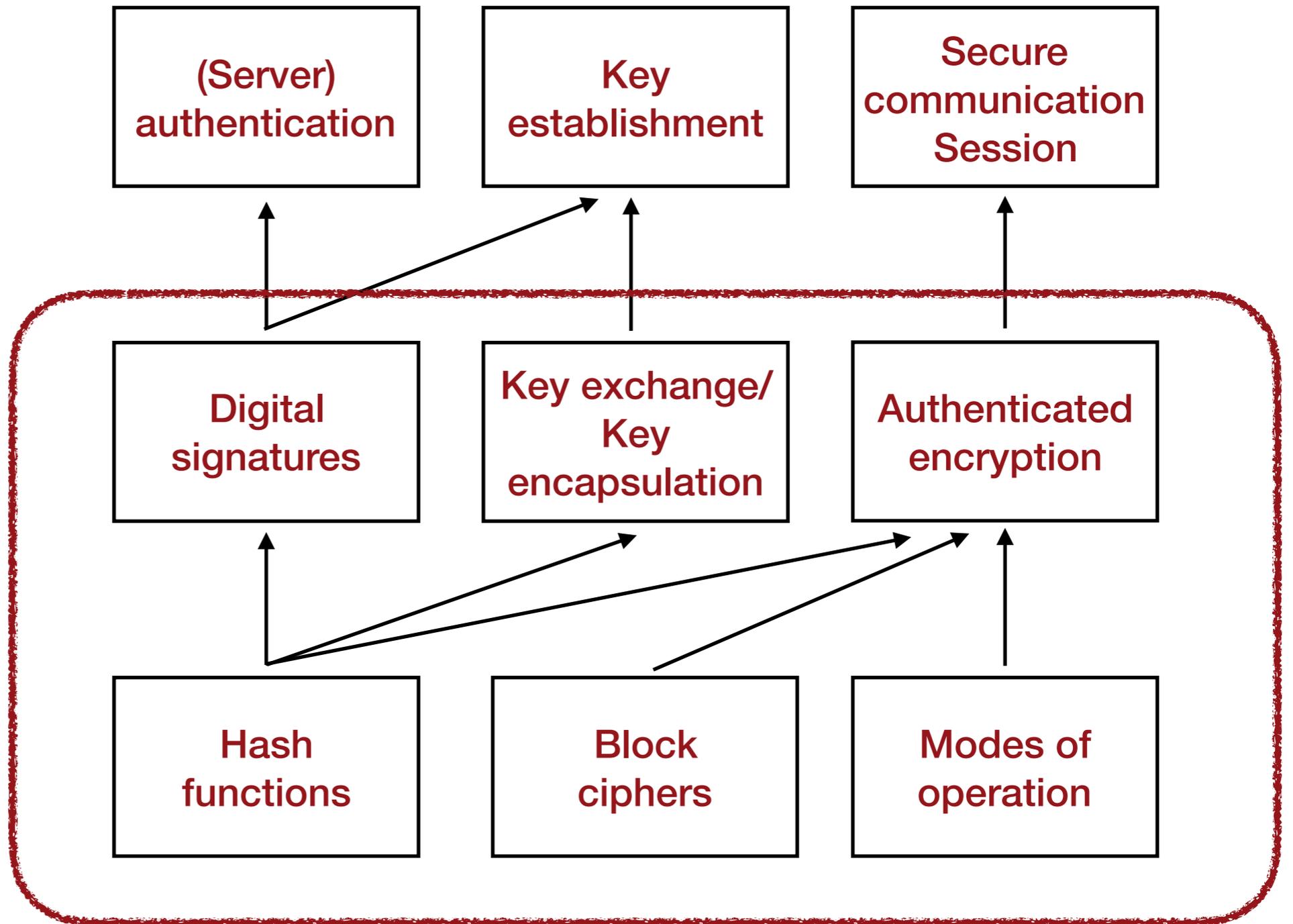
The TLS protocol

Functionalities

Protocols

Cryptographic
Ingredients

*Quantum-
ready?*



The TLS protocol

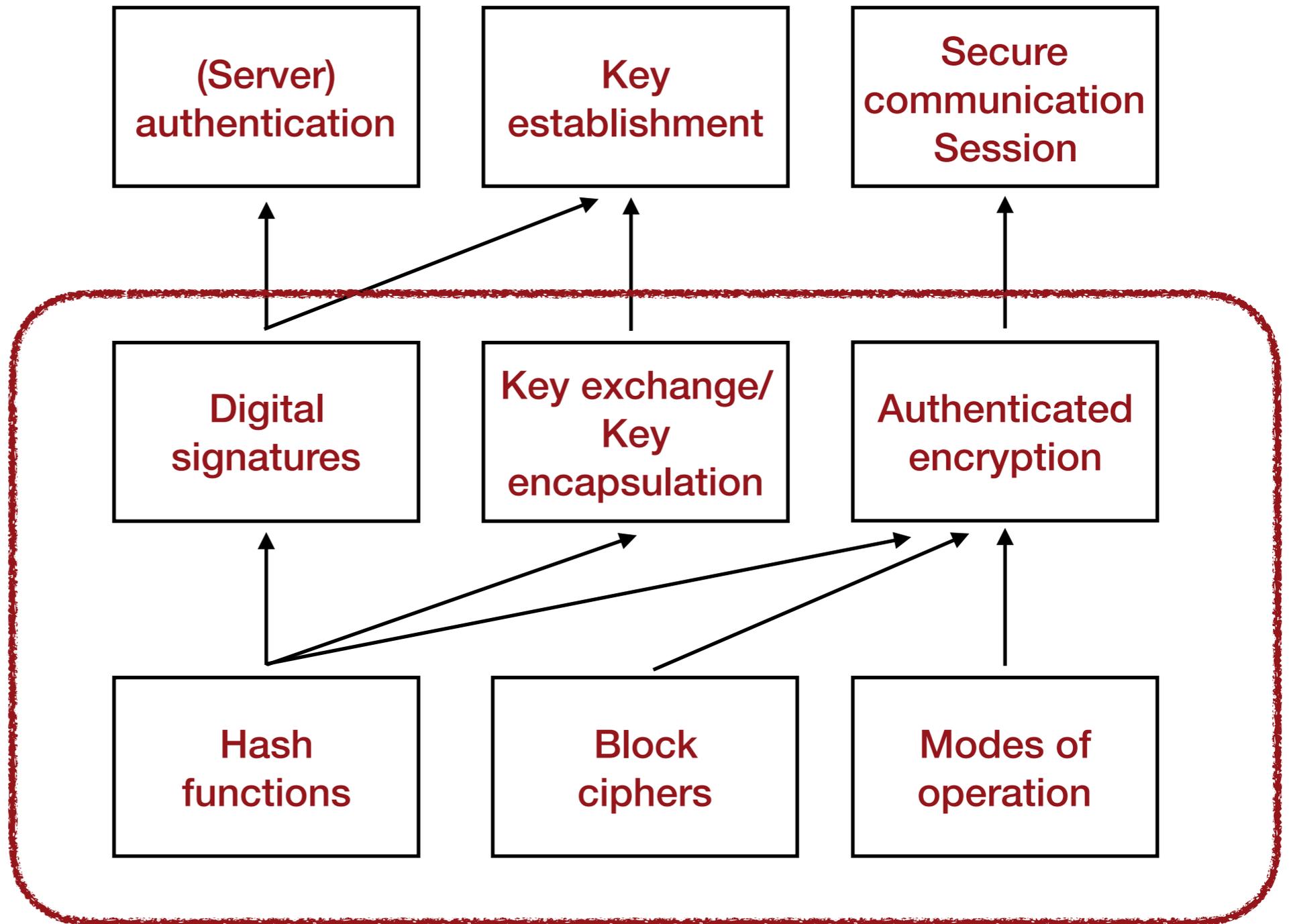
Quantum

Functionalities

Protocols

Cryptographic
Ingredients

Quantum-
ready?



The TLS protocol

Quantum

Functionalities

(Server)
authentication

Key
establishment

Secure
communication
Session

Protocols

Digital
signatures

Key exchange/
Key
encapsulation

Authenticated
encryption

Cryptographic
Ingredients

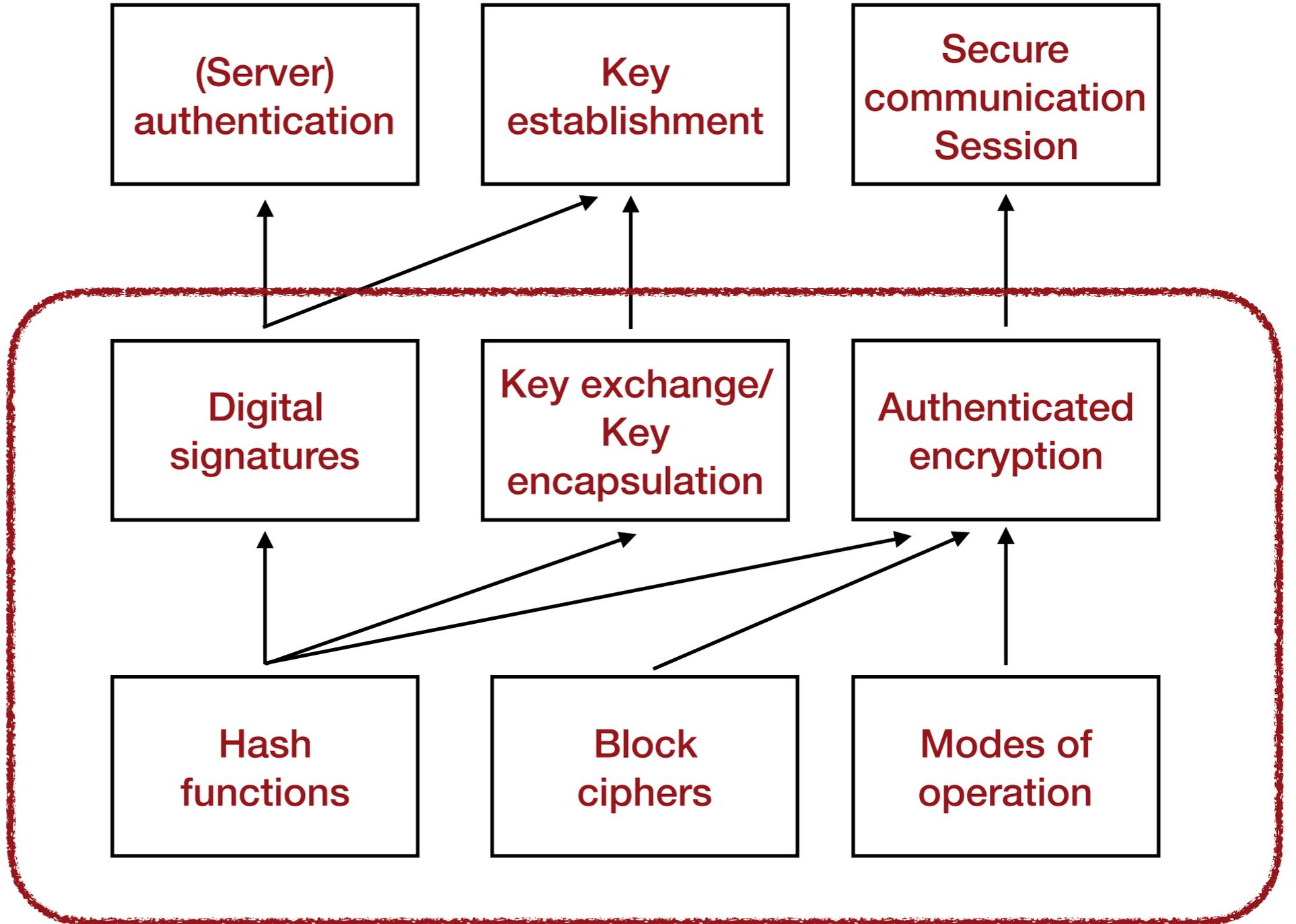
Hash
functions

Block
ciphers

Modes of
operation

Quantum

Quantum-
ready?



The TLS protocol

Quantum

"post-quantum"

Quantum

Functionalities

(Server)
authentication

Key
establishment

Secure
communication
Session

Protocols

Digital
signatures

Key exchange/
Key
encapsulation

Authenticated
encryption

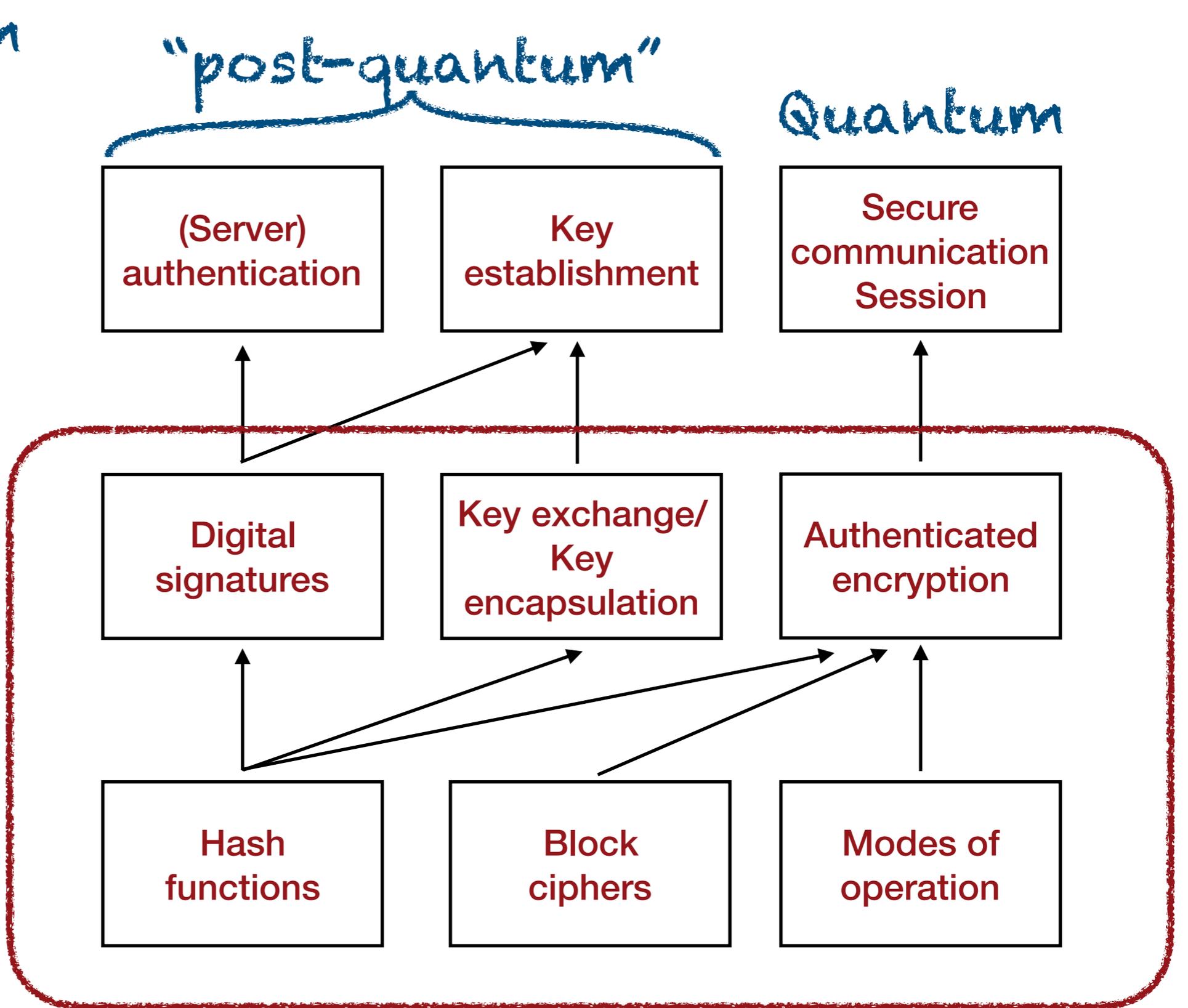
Cryptographic
Ingredients

Hash
functions

Block
ciphers

Modes of
operation

Quantum-
ready?



The TLS protocol

Quantum

"post-quantum"

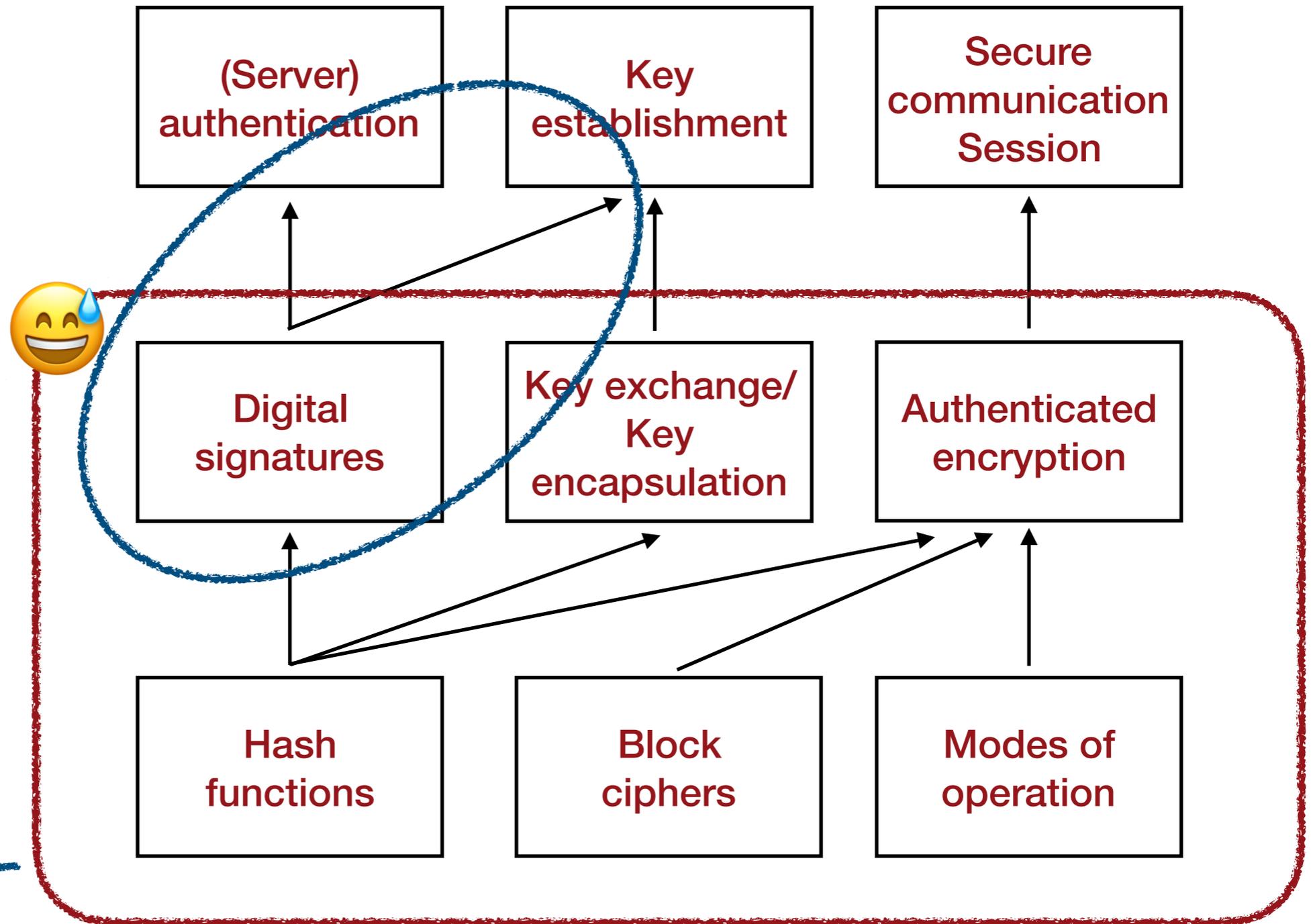
Quantum

Functionalities

Protocols

Cryptographic
Ingredients

Quantum-
ready?

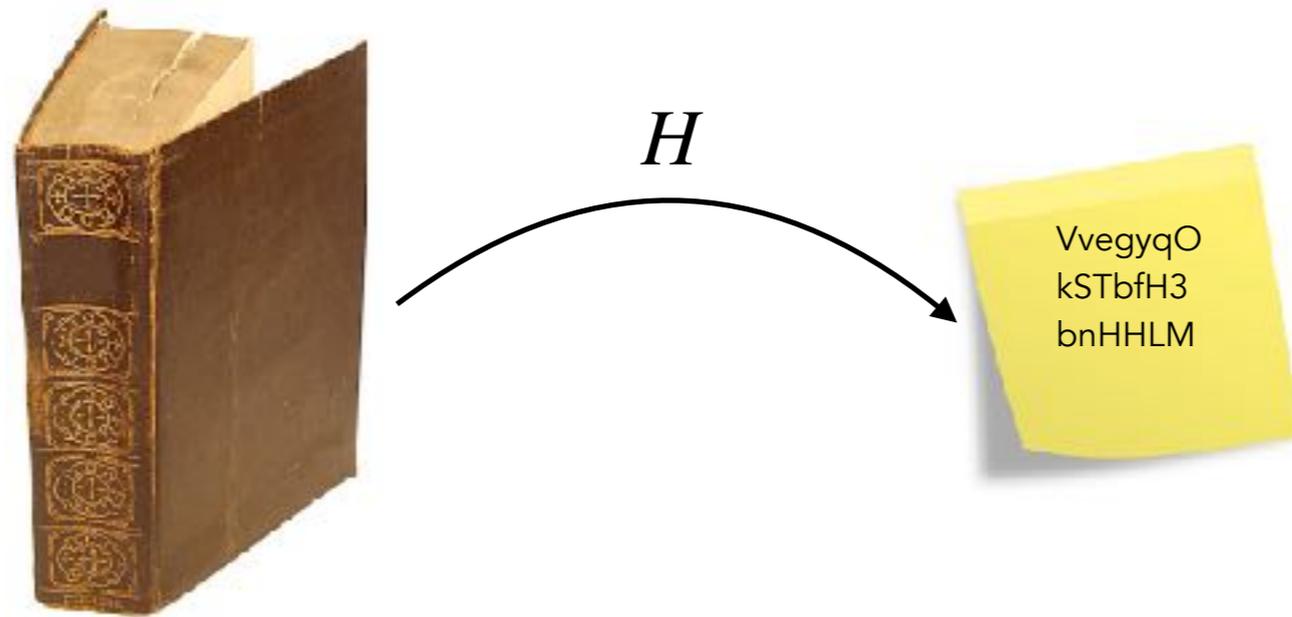


Are we ready for encrypting the quantum internet?

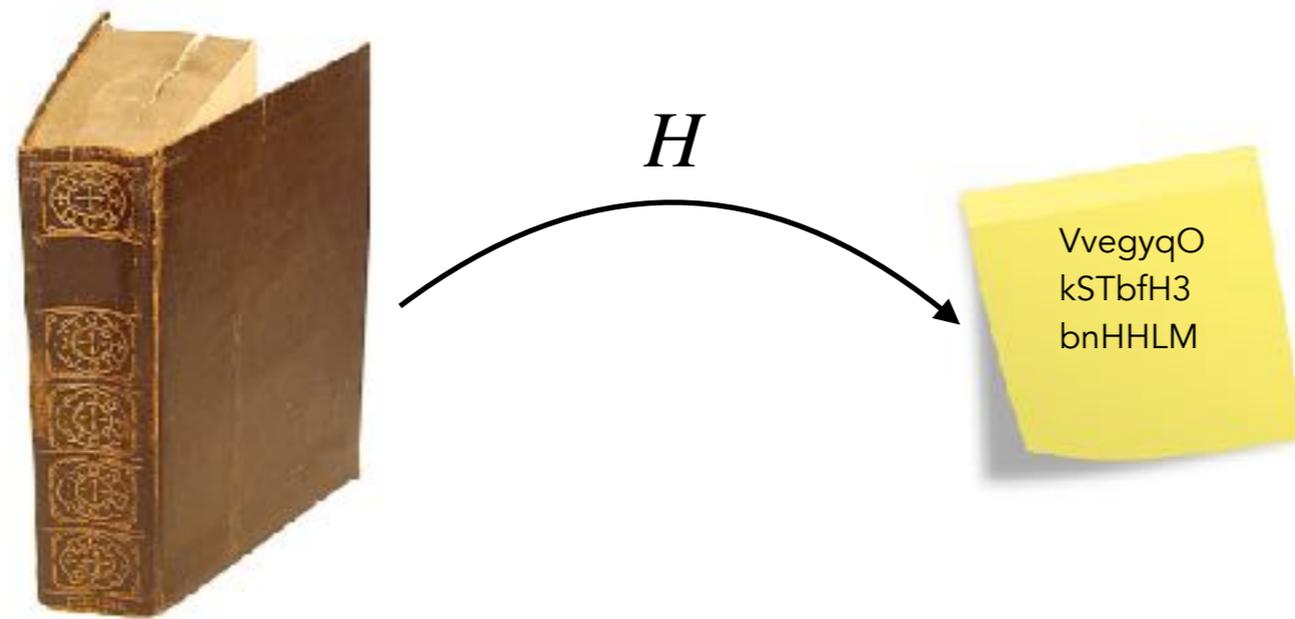
Hash Functions



Hash functions



Hash functions



Ubiquitous in cryptography. Examples:

- ▶ Key encapsulation mechanisms
- ▶ Digital signatures
- ▶ Message authentication codes
- ▶ ...

Hash function security

Hash function security

Output should look random! Formalization difficult...

Hash function security

Output should look random! Formalization difficult...

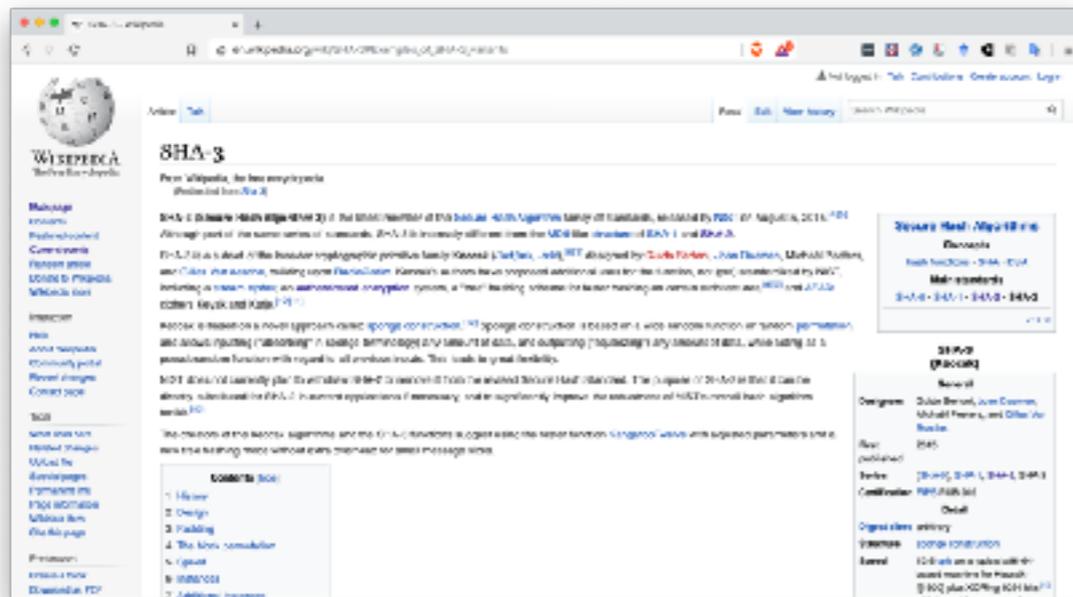
⇒ just model H as random, "Random Oracle Model" (ROM)

Hash function security

Output should look random! Formalization difficult...

⇒ just model H as random, "Random Oracle Model" (ROM)

Reality

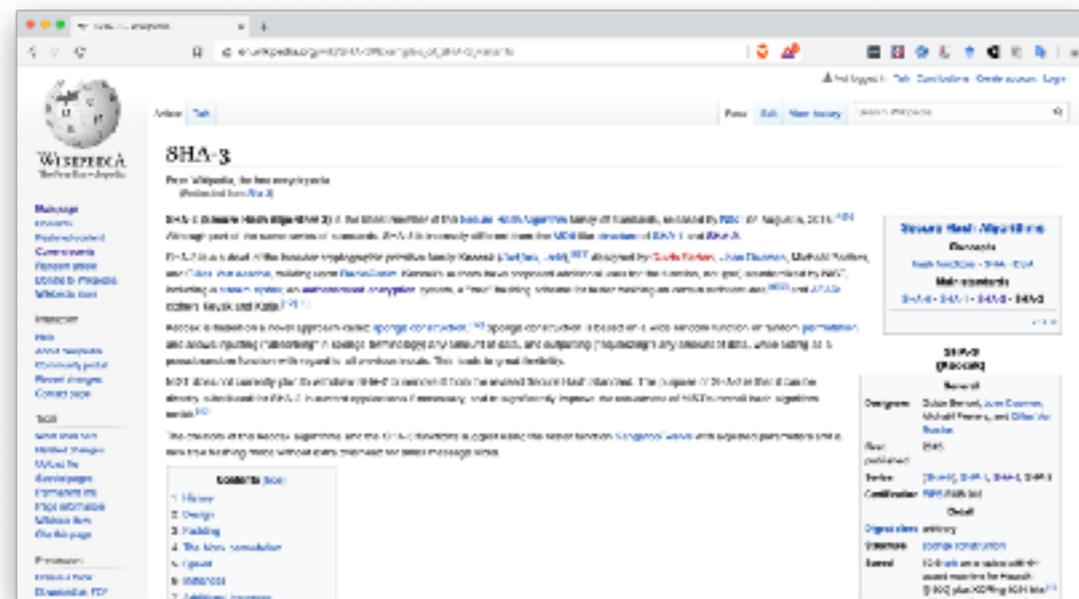


Hash function security

Output should look random! Formalization difficult...

⇒ just model H as random, "Random Oracle Model" (ROM)

Reality



Model

$$H : \{0,1\}^* \rightarrow \{0,1\}^n$$

Uniformly random

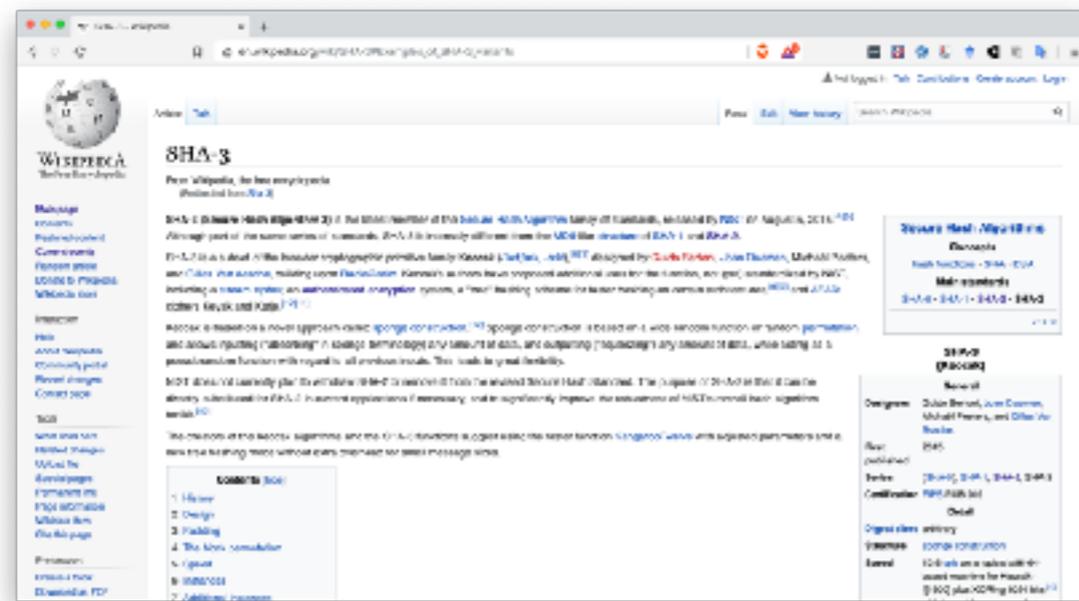
All agents have oracle access to H

Hash function security

Output should look random! Formalization difficult...

⇒ just model H as random, "Random Oracle Model" (ROM)

Reality



Model

$$H : \{0,1\}^* \rightarrow \{0,1\}^n$$

Uniformly random

All agents have quantum oracle access to H

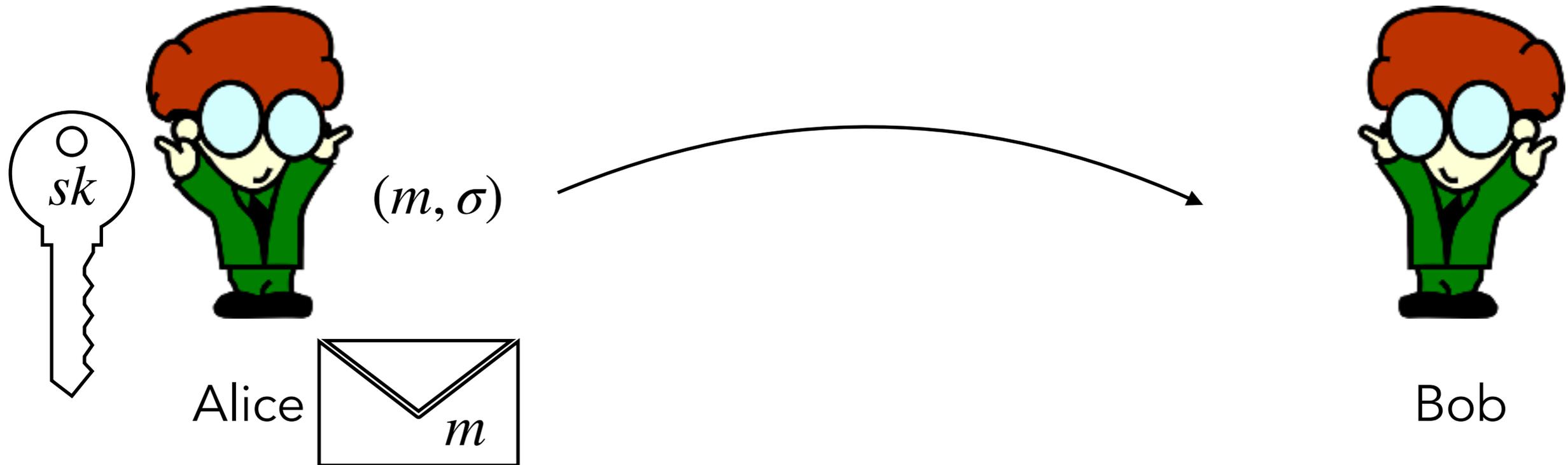
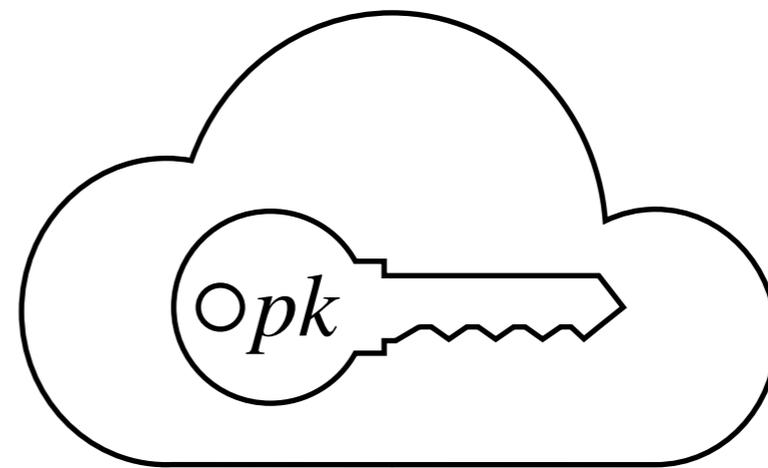
Quantum Random Oracle Model (Boneh et al. '10)

Are we ready for encrypting the quantum internet?

Digital Signatures II



Digital signatures

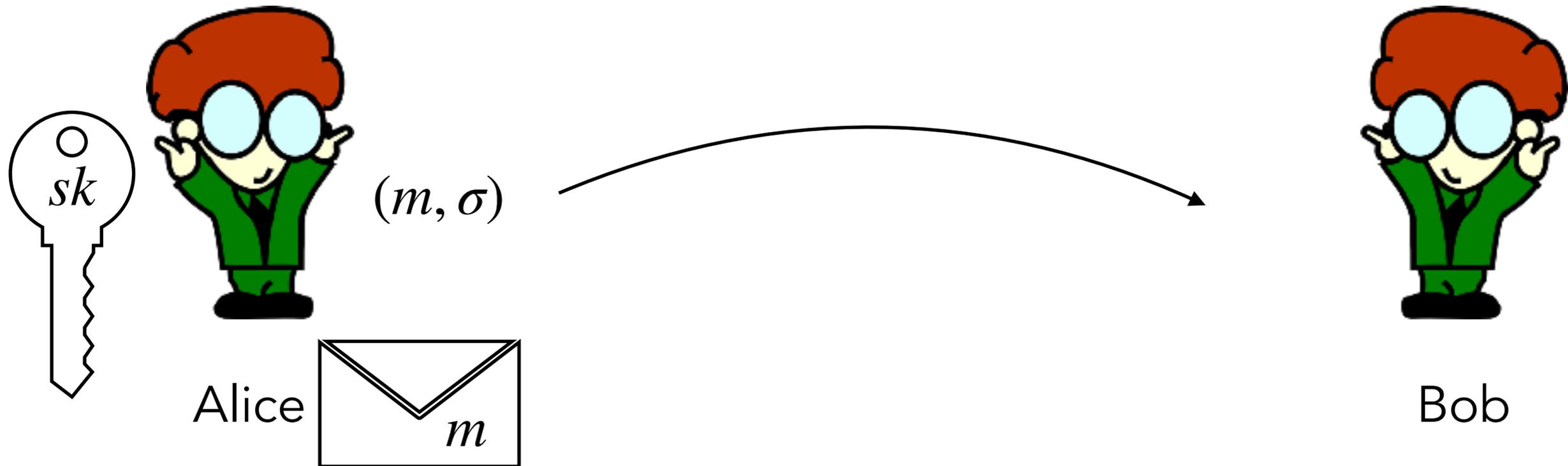
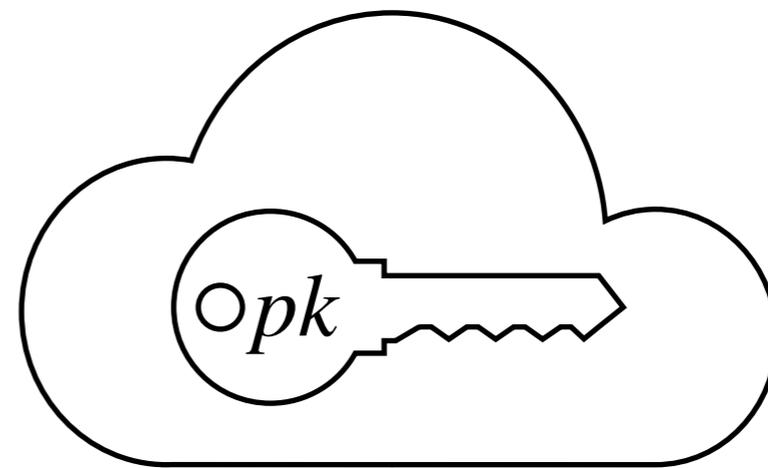


$$\sigma = \text{Sign}_{sk}(m)$$

$$\text{Ver}_{pk}(m, \sigma) = \text{accept}$$

Security: If (m', σ') was produced from (m, σ) without using sk , then $\text{Ver}_{pk}(m', \sigma') = \text{reject}$

Digital signatures



$$\sigma = \text{Sign}_{sk}(m)$$

$$\text{Ver}_{pk}(m, \sigma) = \text{accept}$$

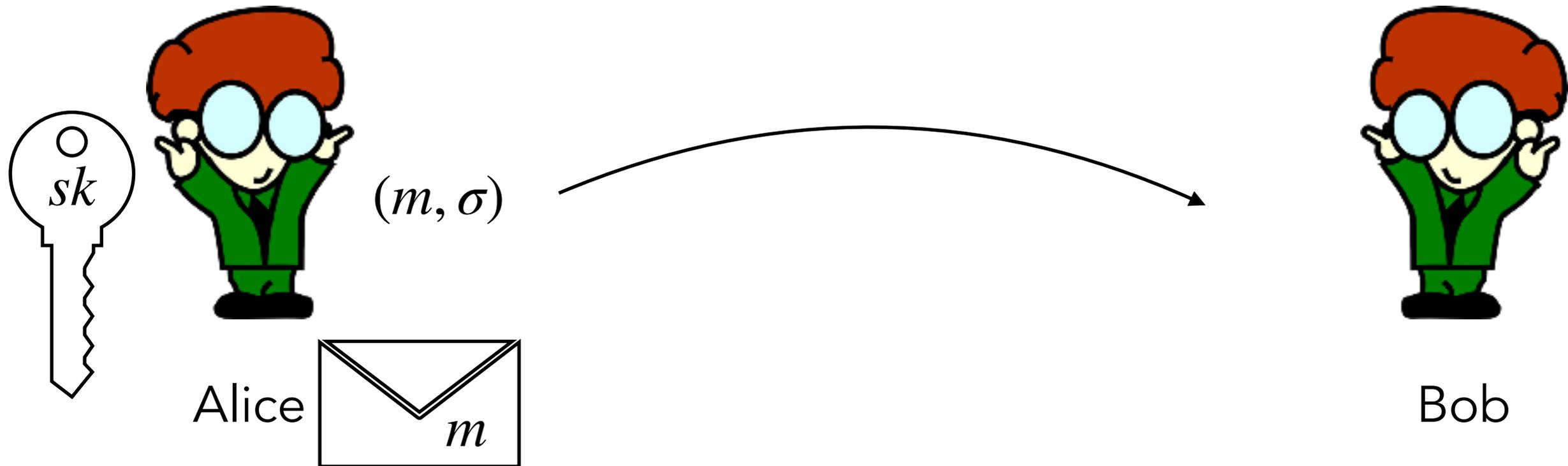
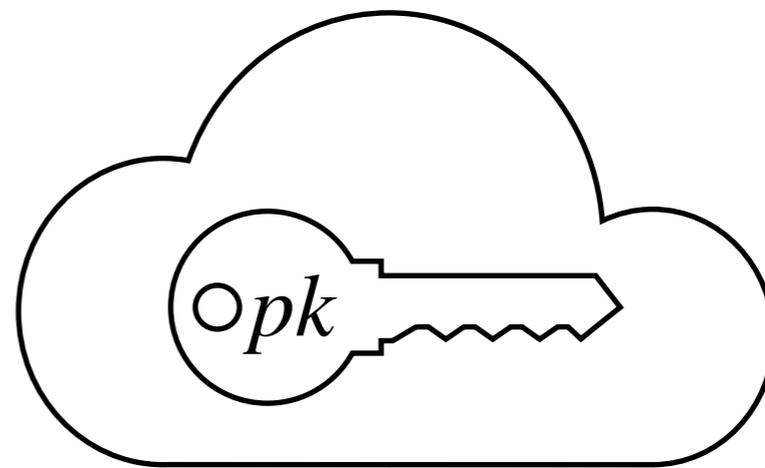
Computed in
polynomial time

Security: If (m', σ') was ~~produced~~ from (m, σ) without using sk , then

$$\text{Ver}_{pk}(m', \sigma') = \text{reject}$$

Digital signatures

post-quantum



$$\sigma = \text{Sign}_{sk}(m)$$

$$\text{Ver}_{pk}(m, \sigma) = \text{accept}$$

Computed in quantum polynomial time

Security: If (m', σ') was ~~produced~~ from (m, σ) without using sk , then

$$\text{Ver}_{pk}(m', \sigma') = \text{reject}$$

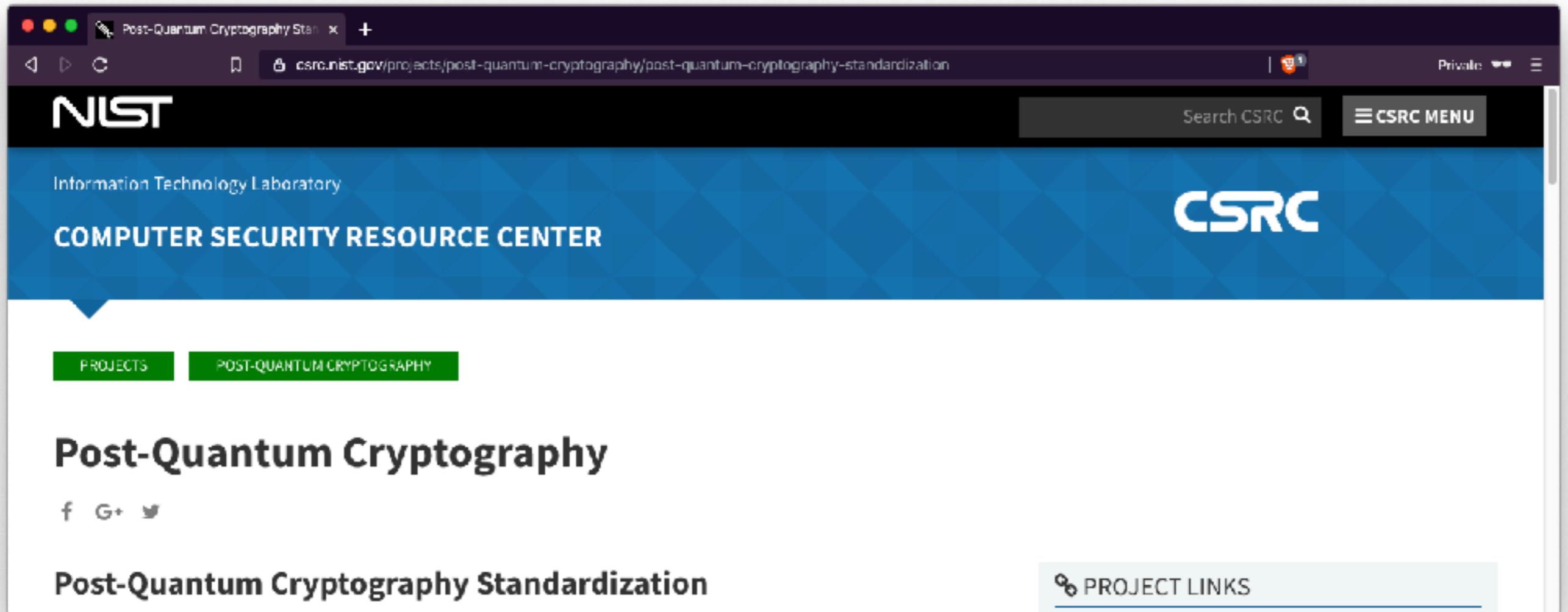
NIST competition

The image shows a browser window displaying the NIST CSRC website. The browser's address bar shows the URL: `csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization`. The page features the NIST logo in the top left and the CSRC logo in the top right. Below the logos, the text "Information Technology Laboratory" and "COMPUTER SECURITY RESOURCE CENTER" is visible. A navigation bar contains "PROJECTS" and "POST-QUANTUM CRYPTOGRAPHY" buttons. The main heading is "Post-Quantum Cryptography", followed by social media icons for Facebook, Google+, and Twitter. The sub-heading is "Post-Quantum Cryptography Standardization". A "PROJECT LINKS" button is located in the bottom right corner.

Post-Quantum Cryptography Standardization

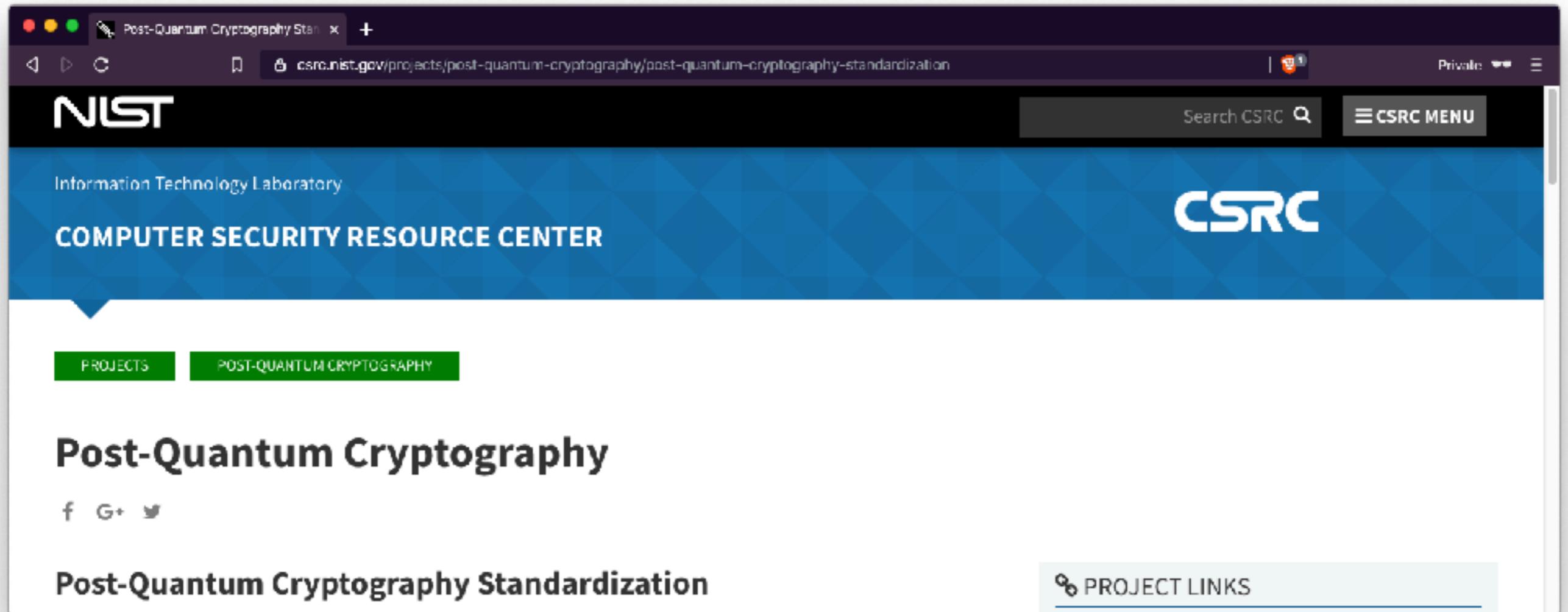
PROJECT LINKS

NIST competition



Goal: Standardize post-quantum secure signatures and key encapsulation mechanisms.

NIST competition



Goal: Standardize post-quantum secure signatures and key encapsulation mechanisms.

4/9 round 2 signature schemes use *Fiat Shamir transformation*

Fiat Shamir transformation

Removes interaction from *identification schemes* using hash functions



Like signature but
with interactive verification

Fiat Shamir transformation

Removes interaction from *identification schemes* using hash functions \implies Digital signature scheme

Fiat Shamir transformation

Removes interaction from *identification schemes* using hash functions \implies Digital signature scheme

Well-known: Security in the Random Oracle Model

Fiat Shamir transformation

Removes interaction from *identification schemes* using hash functions \implies Digital signature scheme

Well-known: Security in the Random Oracle Model

How about the **Quantum** Random Oracle Model (QROM)?

Fiat Shamir transformation

Removes interaction from *identification schemes* using hash functions \implies Digital signature scheme

Well-known: Security in the Random Oracle Model

How about the **Quantum** Random Oracle Model (QROM)?

Theorem (Don, Fehr, M, Schaffner '19):

Fiat Shamir signatures are secure in the QROM.

Fiat Shamir transformation

Removes interaction from *identification schemes* using hash functions \implies Digital signature scheme

Well-known: Security in the Random Oracle Model

How about the **Quantum** Random Oracle Model (QROM)?

Theorem (Don, Fehr, M, Schaffner '19):
Fiat Shamir signatures are secure in the QROM.

Also proven concurrently by Liu, Zhandry. Less tight reduction.

Fiat Shamir transformation

Removes interaction from *identification schemes* using hash functions \implies Digital signature scheme

Well-known: Security in the Random Oracle Model

How about the **Quantum** Random Oracle Model (QROM)?

Theorem (Don, Fehr, M, Schaffner '19):
Fiat Shamir signatures are secure in the QROM.

Also proven concurrently by Liu, Zhandry. Less tight reduction.

More efficient NIST candidate signature schemes!!!

Fiat Shamir transformation

Removes interaction from *identification schemes* using hash functions \implies Digital signature scheme

Well-known: Security in the Random Oracle Model

How about the **Quantum** Random Oracle Model (QROM)?

Theorem (Don, Fehr, M, Schaffner '19):
Fiat Shamir signatures are secure in the QROM.

Also proven concurrently by Liu, Zhandry. Less tight reduction.

More efficient NIST candidate signature schemes!!!



Are we ready for encrypting the quantum internet?

Key Exchange



Post-quantum key exchange

This is what Quantum Key Distribution (QKD) can do!*

Post-quantum key exchange

This is what Quantum Key Distribution (QKD) can do!*

Unconditionally
secure!!



Post-quantum key exchange

This is what Quantum Key Distribution (QKD) can do!*

Unconditionally
secure!!



Alternative: post-quantum secure Key Encapsulation

Post-quantum key exchange

This is what Quantum Key Distribution (QKD) can do!*

Unconditionally
secure!!



Alternative: post-quantum secure Key Encapsulation

+ Classical \implies more efficient

Post-quantum key exchange

This is what Quantum Key Distribution (QKD) can do!*

Unconditionally
secure!!



Alternative: post-quantum secure Key Encapsulation

- + Classical \implies more efficient
- Computational assumptions (similar to signatures, current internet crypto...)

Are we ready for encrypting the quantum internet?

Authenticated Encryption



The TLS protocol

Quantum

"post-quantum"

Quantum

Functionalities

(Server)
authentication

Key
establishment

Secure
communication
Session

Protocols

Digital
signatures

Key exchange/
Key
encapsulation

Authenticated
encryption

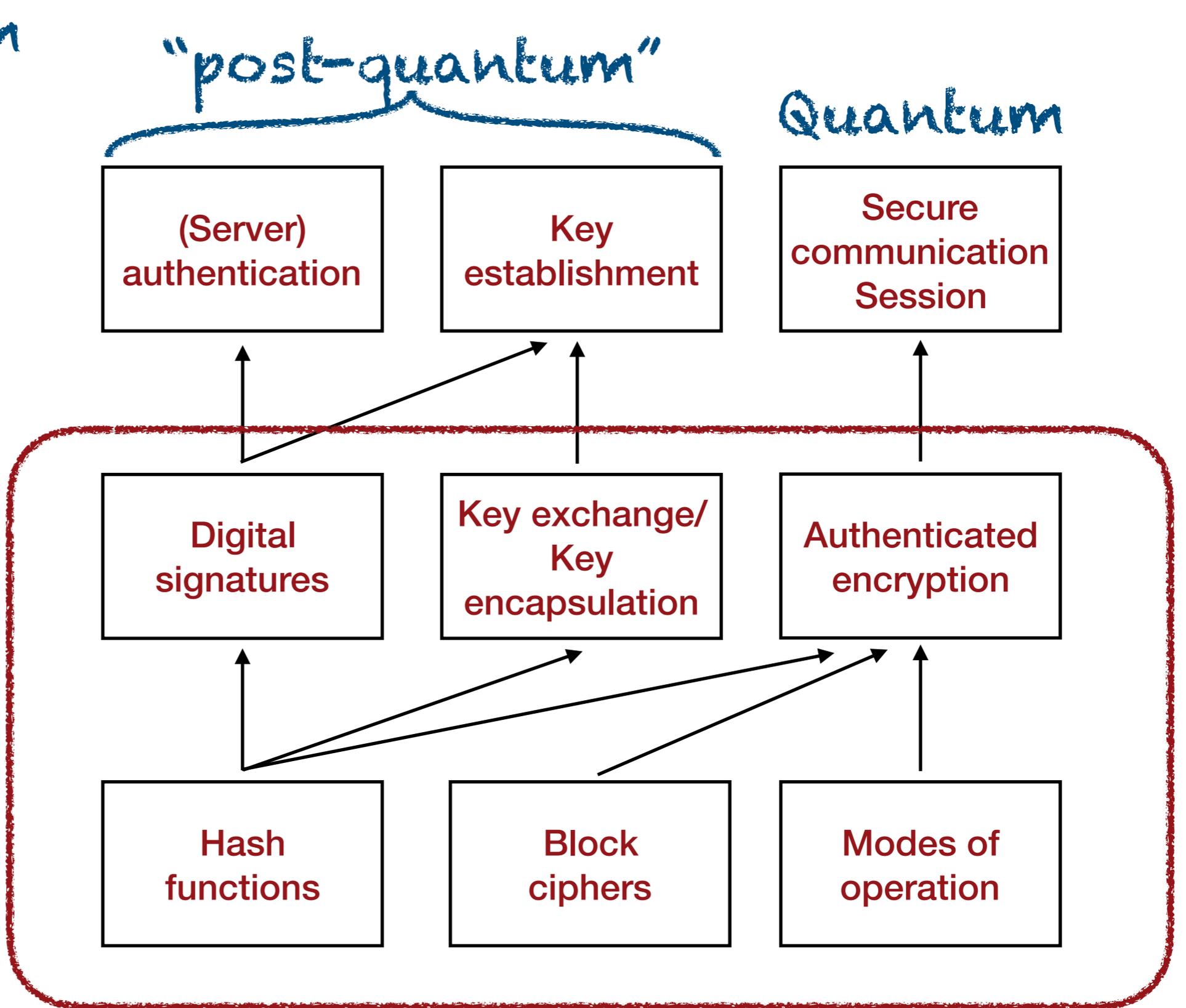
Cryptographic
Ingredients

Hash
functions

Block
ciphers

Modes of
operation

Quantum-
ready?



The TLS protocol

Quantum

"post-quantum"

Quantum

Functionalities

(Server)
authentication

Key
establishment

Secure
communication
Session

Protocols

Digital
signatures

Key exchange/
Key
encapsulation

Authenticated
encryption

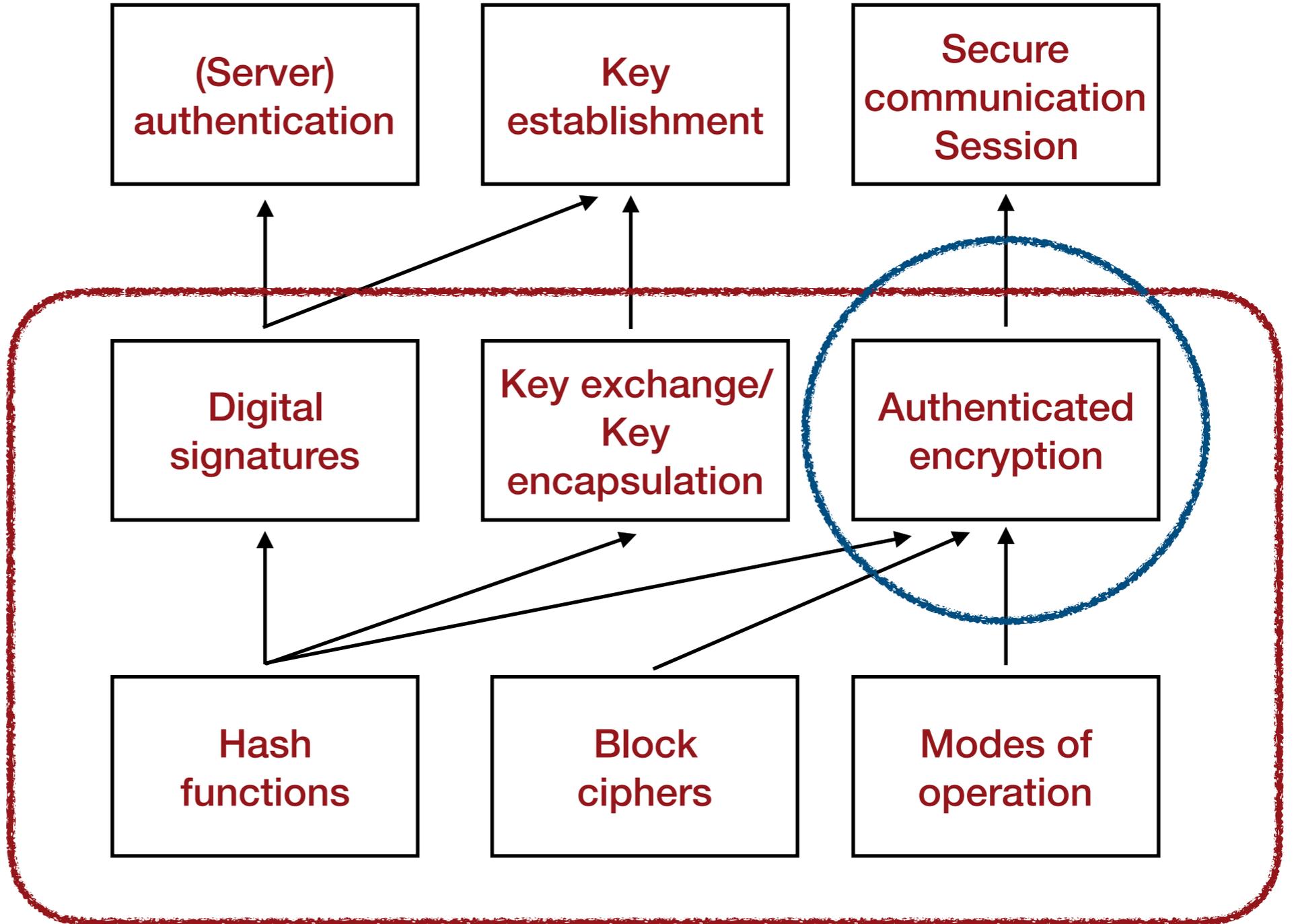
Cryptographic
Ingredients

Hash
functions

Block
ciphers

Modes of
operation

Quantum-
ready?



Authenticated Encryption

Authenticated Encryption



Alice

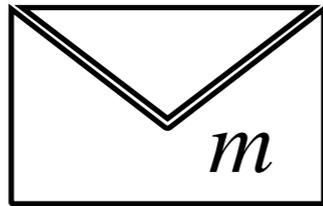


Bob

Authenticated Encryption

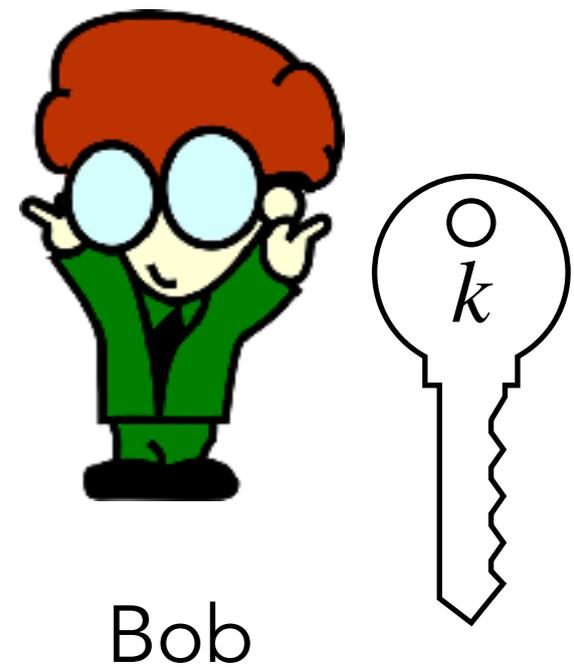
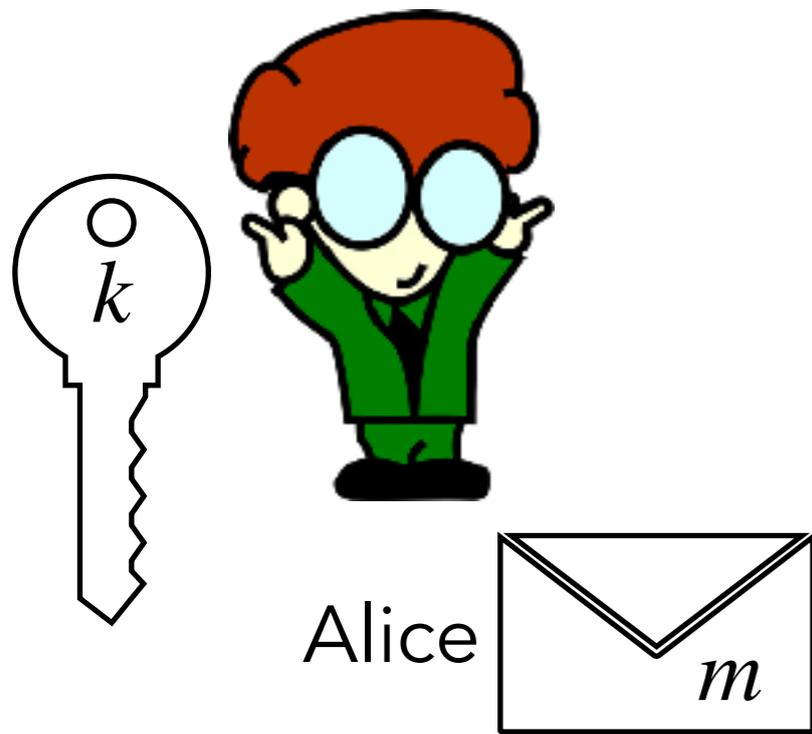


Alice

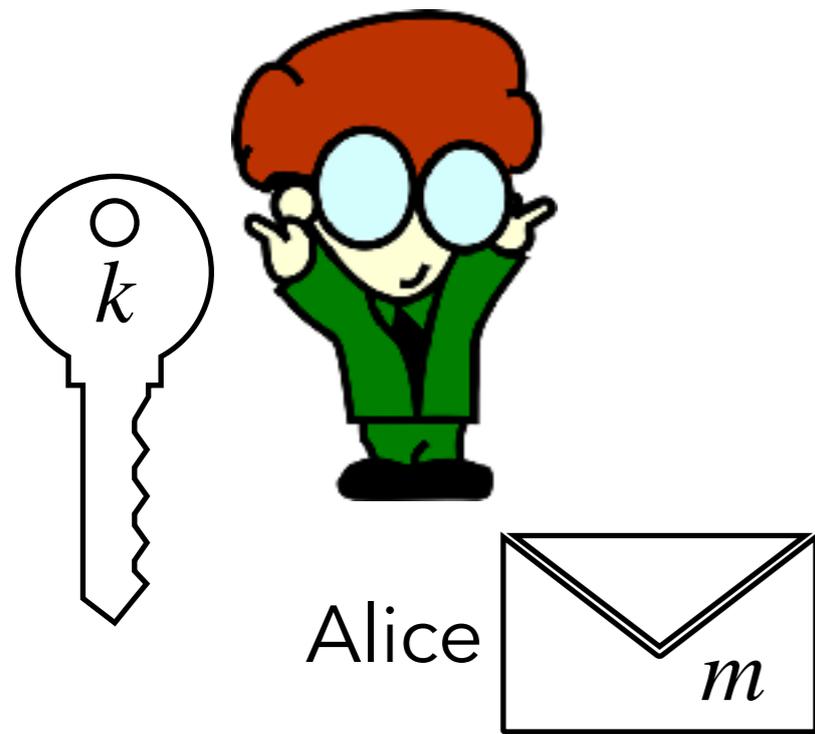


Bob

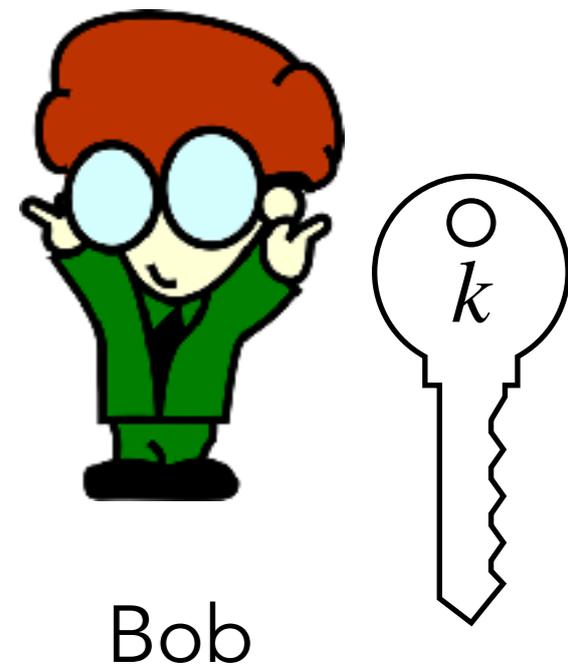
Authenticated Encryption



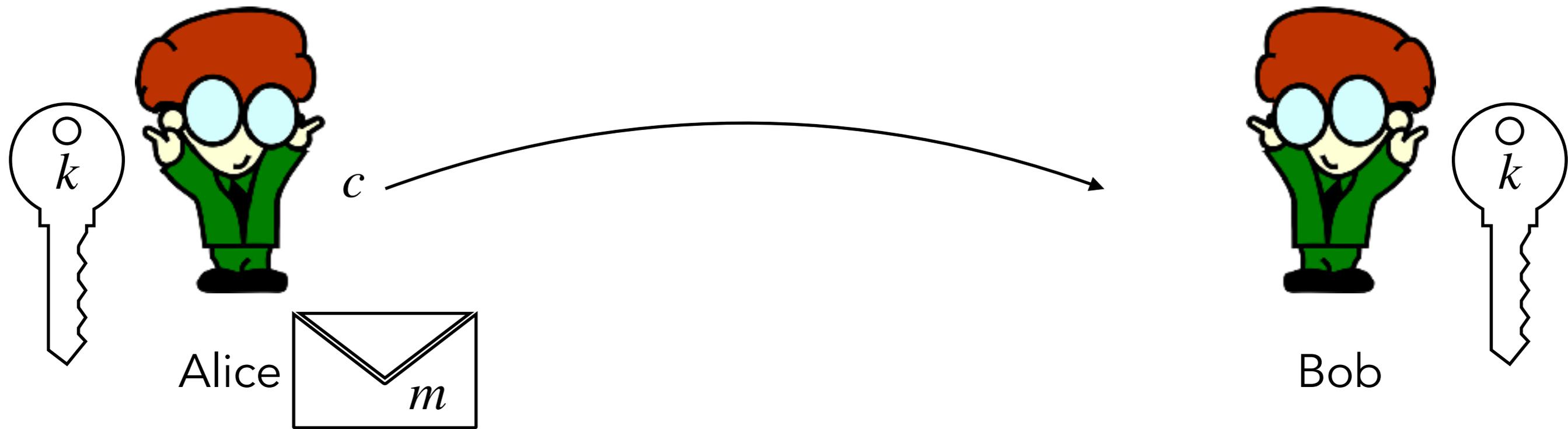
Authenticated Encryption



$$c = \text{Enc}_k(m)$$

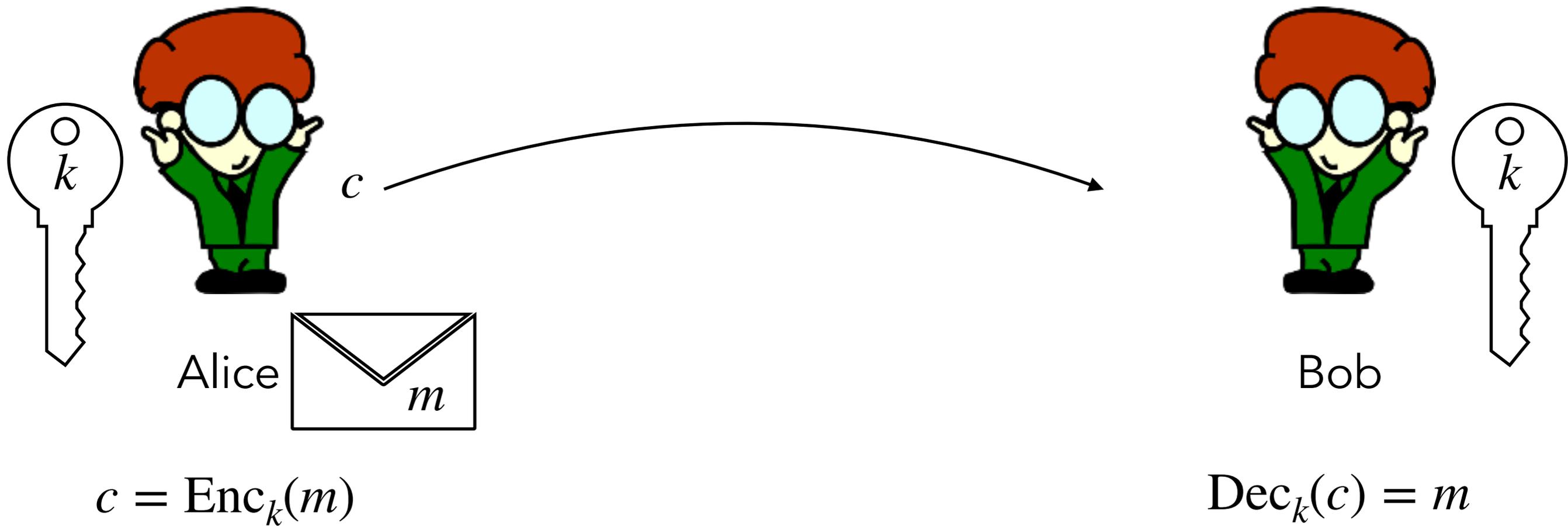


Authenticated Encryption

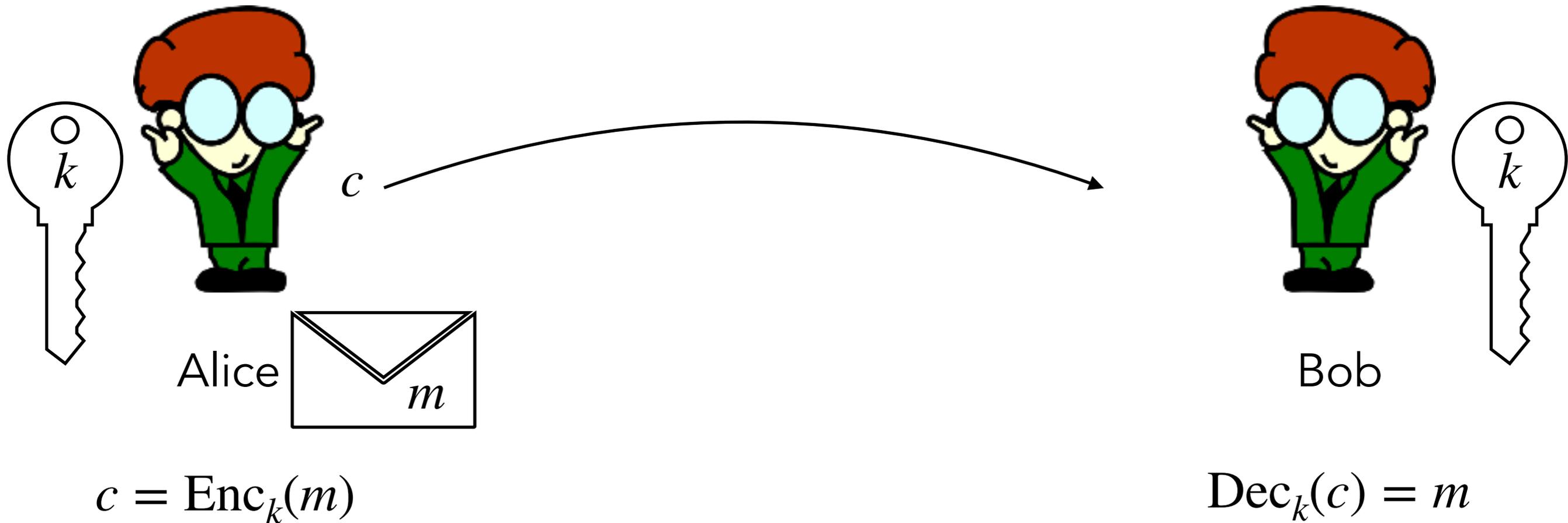


$$c = \text{Enc}_k(m)$$

Authenticated Encryption

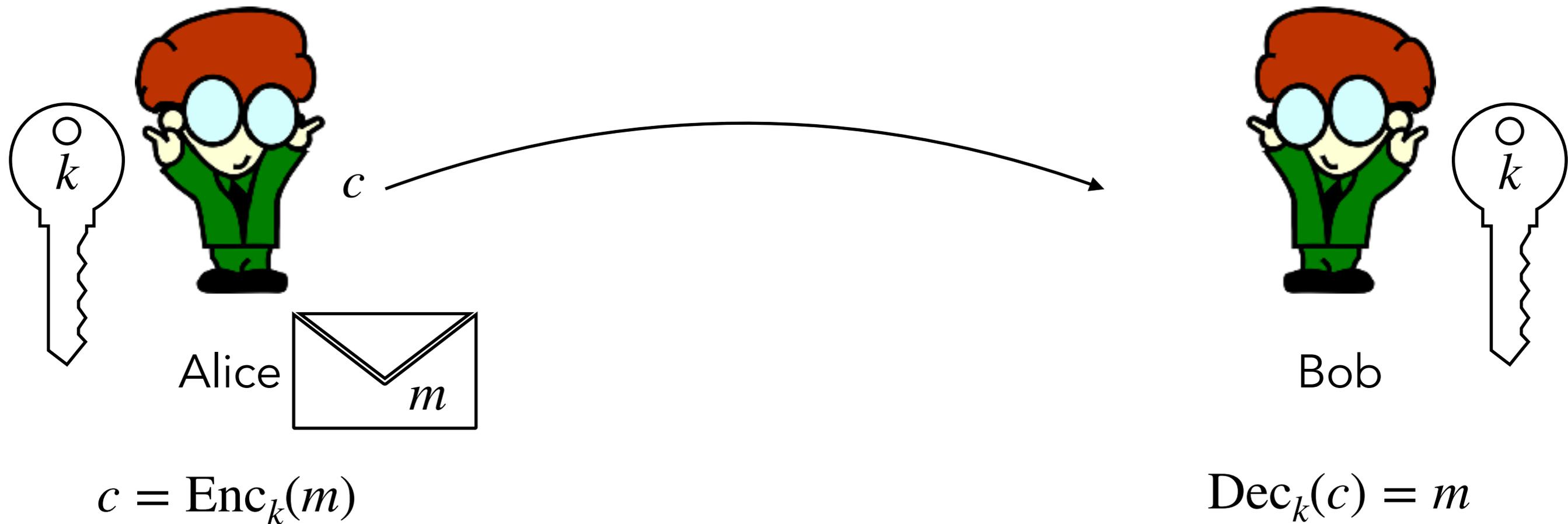


Authenticated Encryption



Confidentiality: c doesn't tell you anything about m .

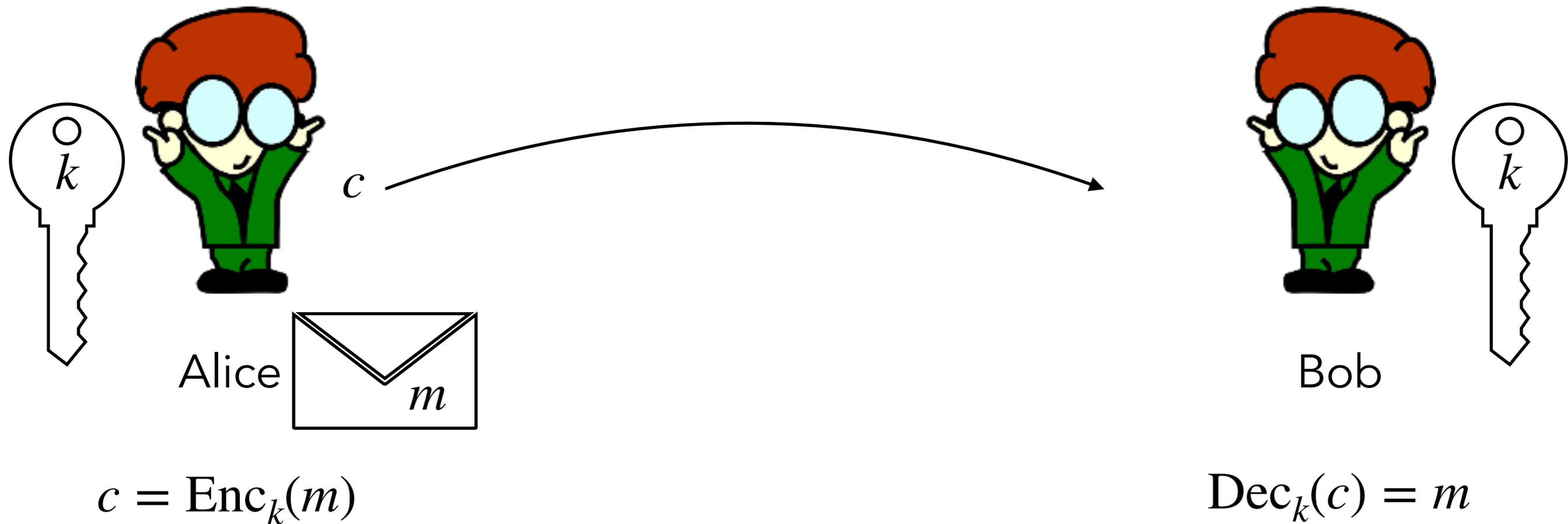
Authenticated Encryption



Confidentiality: c doesn't tell you anything about m .

Integrity: If c' was produced from c without using k , then $\text{Dec}_k(c') = \text{reject}$

Authenticated Encryption

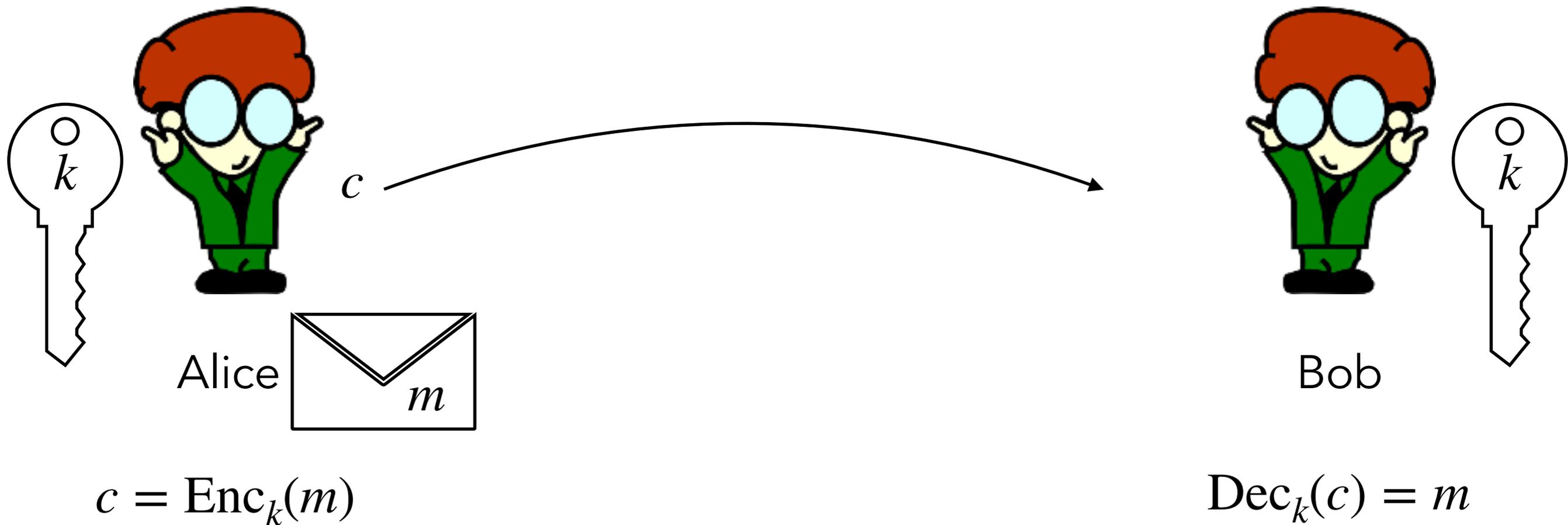


Confidentiality: c doesn't tell you anything about m .

Integrity: If c' was produced from c without using k , then $\text{Dec}_k(c') = \text{reject}$

Slightly simplified...

Authenticated Encryption



Confidentiality: c doesn't tell you anything about m .

Integrity: If c' was produced from c without using k , then $\text{Dec}_k(c') = \text{reject}$

Confidentiality+Integrity=Authenticated encryption

Real vs. Ideal

Alternative characterization (Shrimpton '04):

Real vs. Ideal

Alternative characterization (Shrimpton '04):

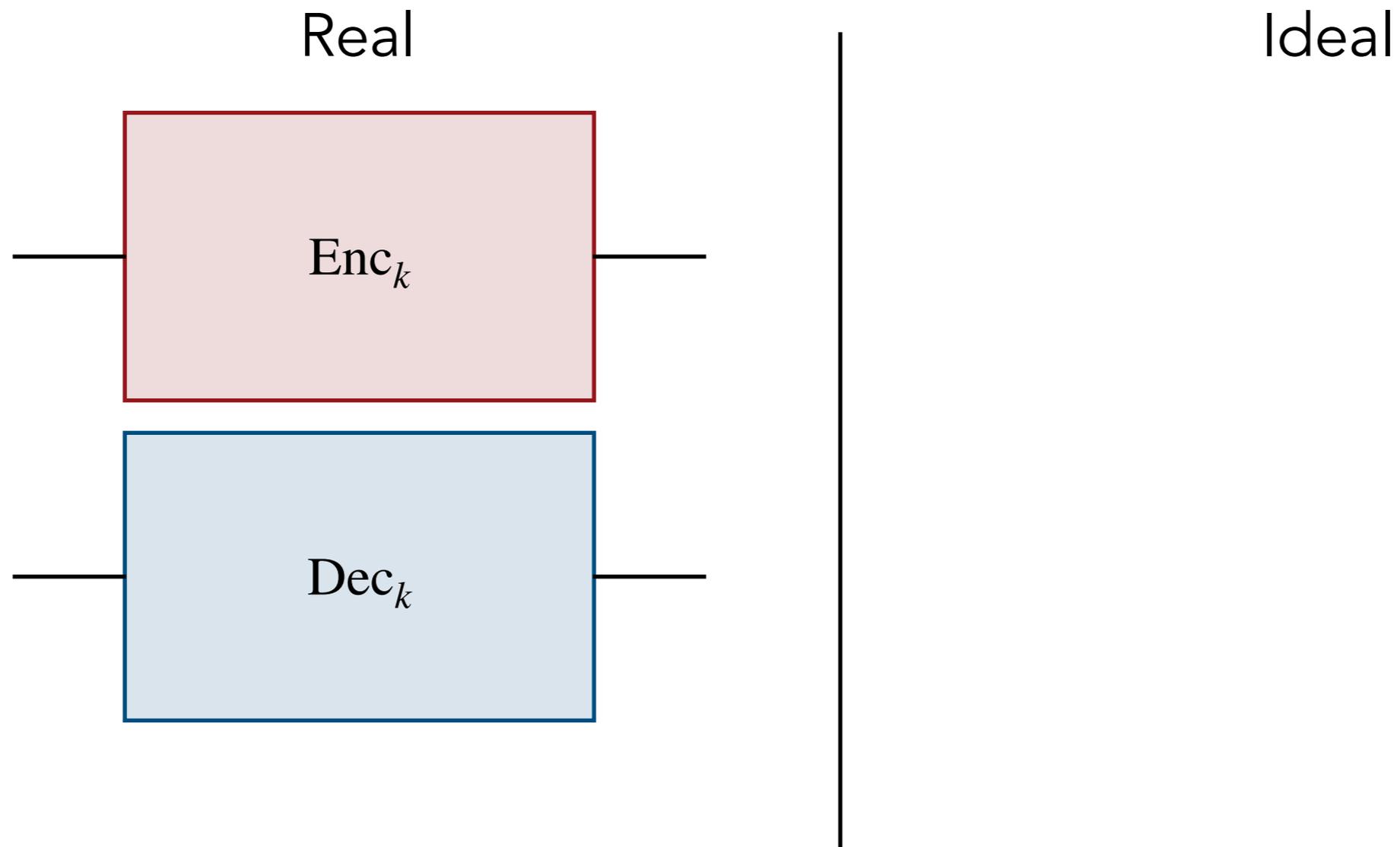
Real

Ideal



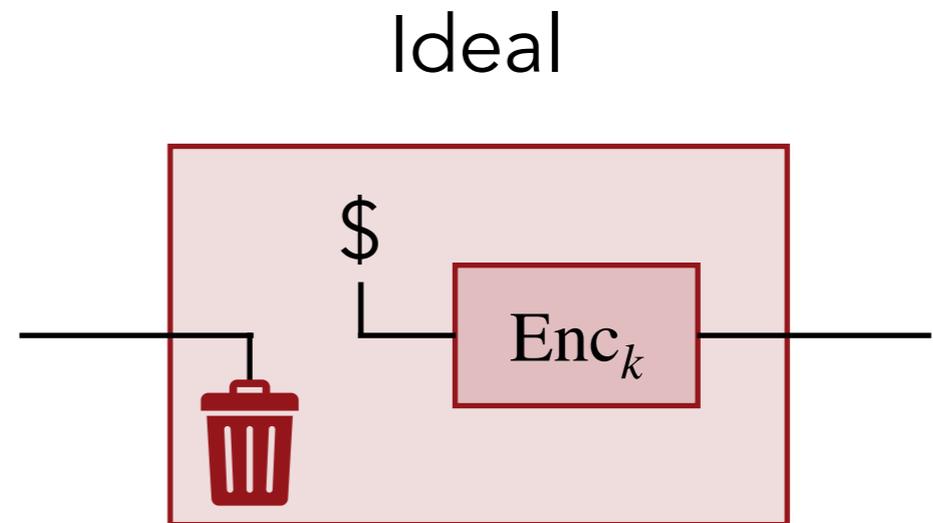
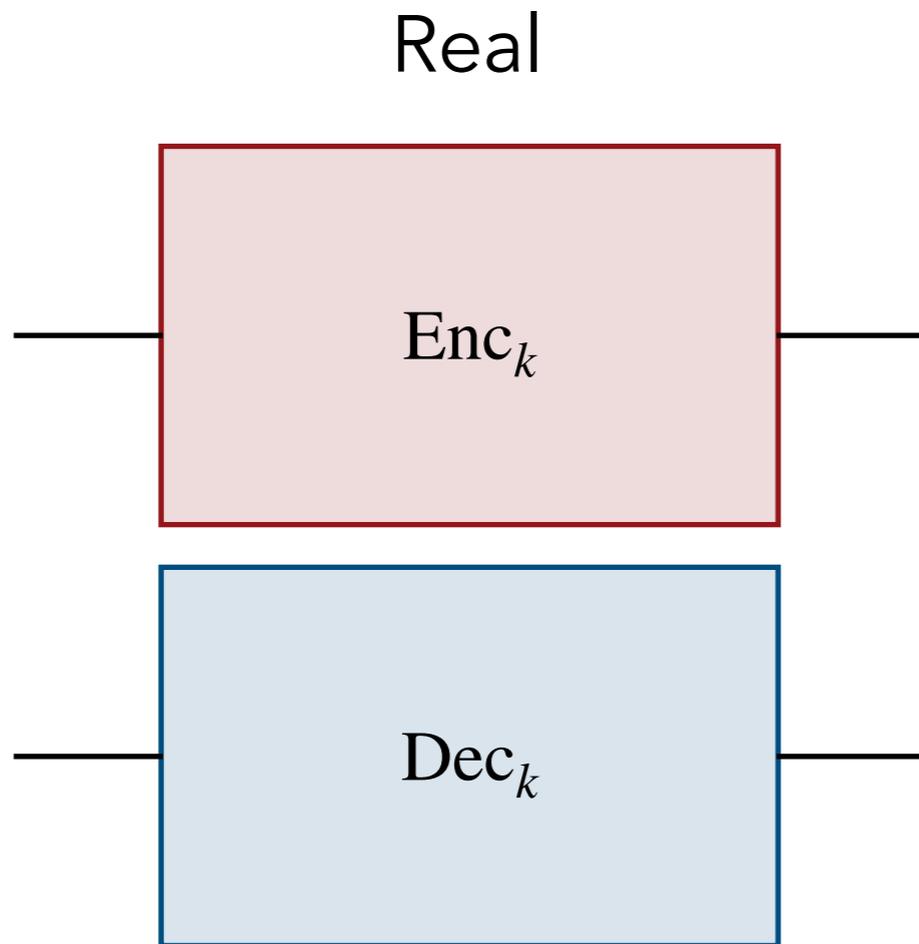
Real vs. Ideal

Alternative characterization (Shrimpton '04):



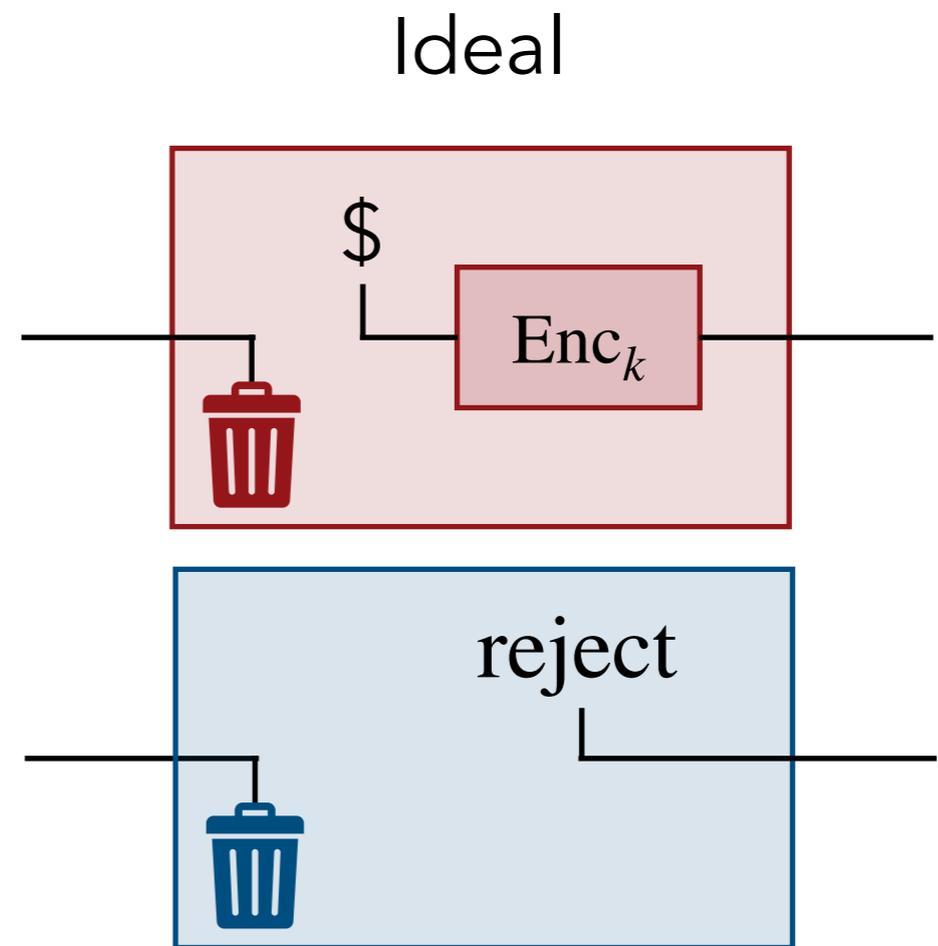
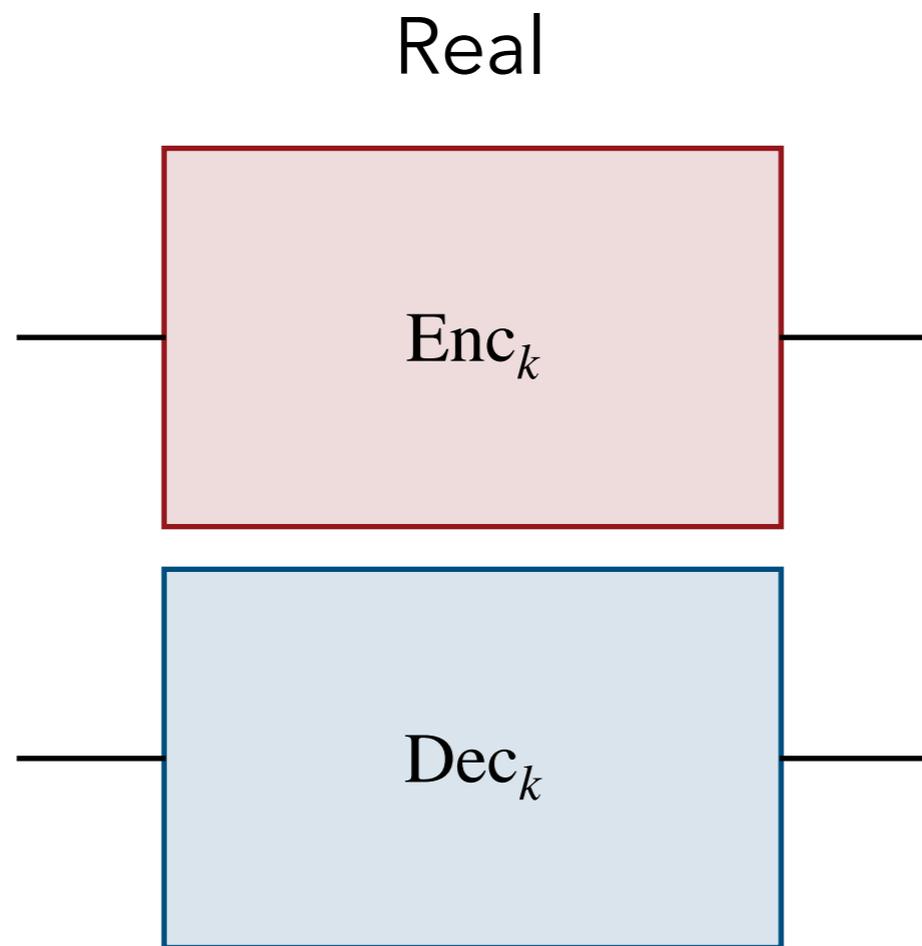
Real vs. Ideal

Alternative characterization (Shrimpton '04):



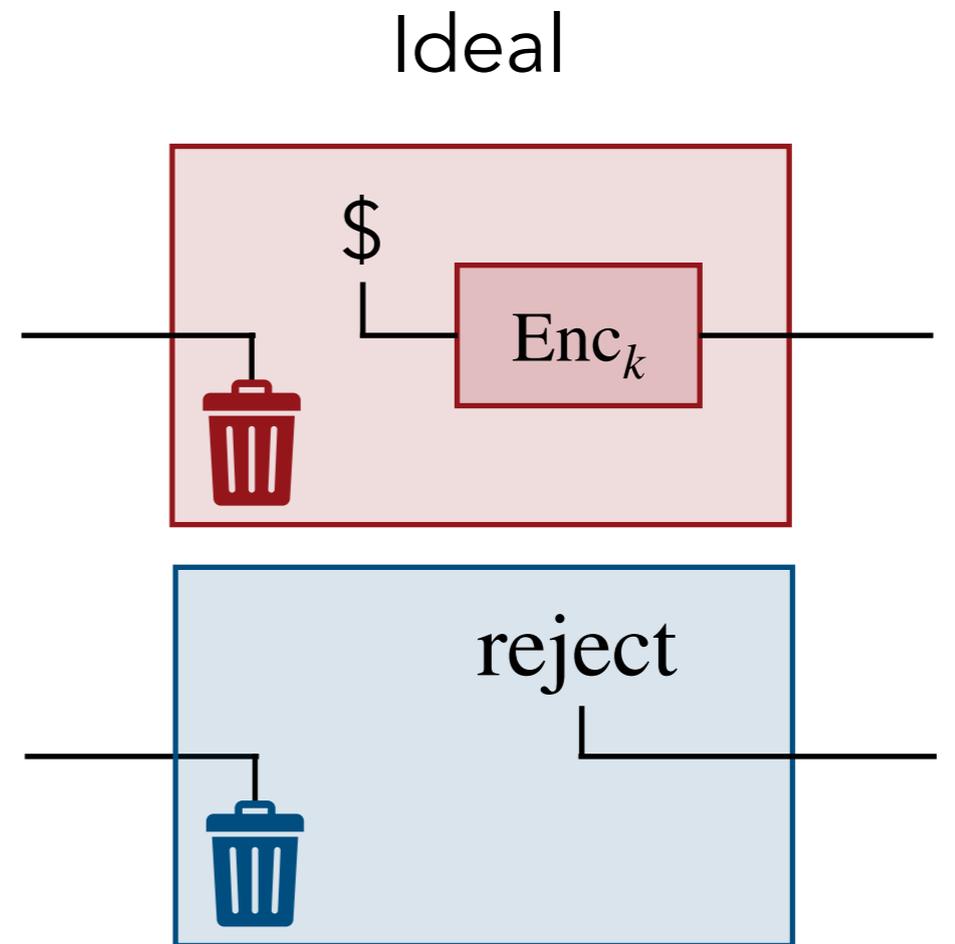
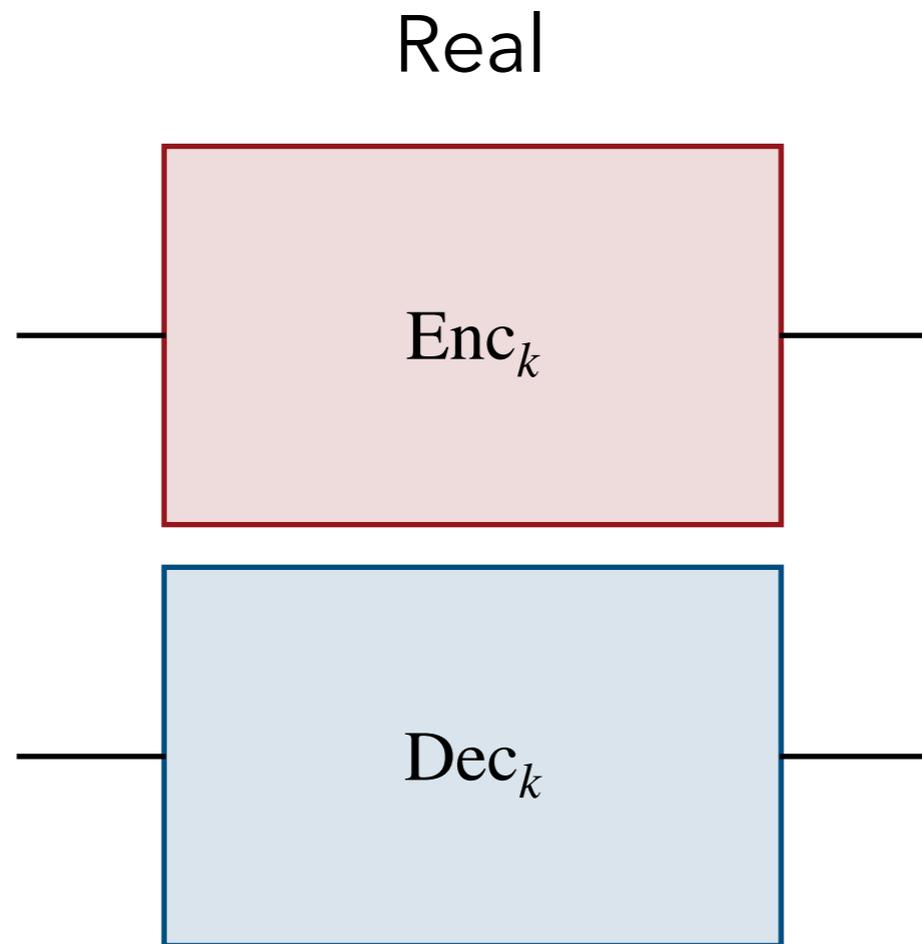
Real vs. Ideal

Alternative characterization (Shrimpton '04):

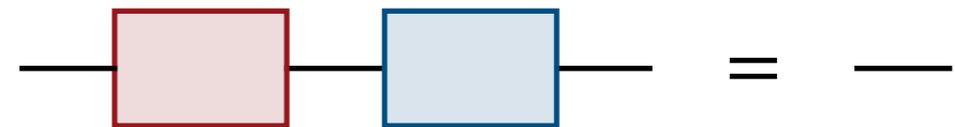


Real vs. Ideal

Alternative characterization (Shrimpton '04):

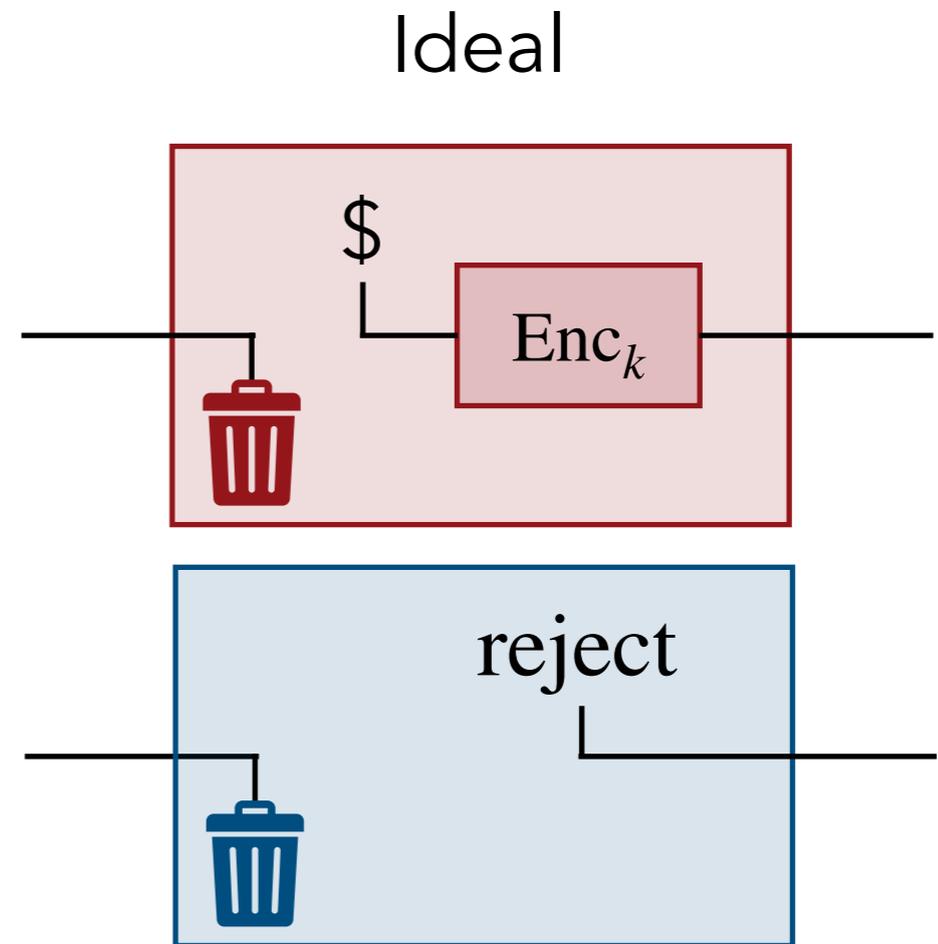
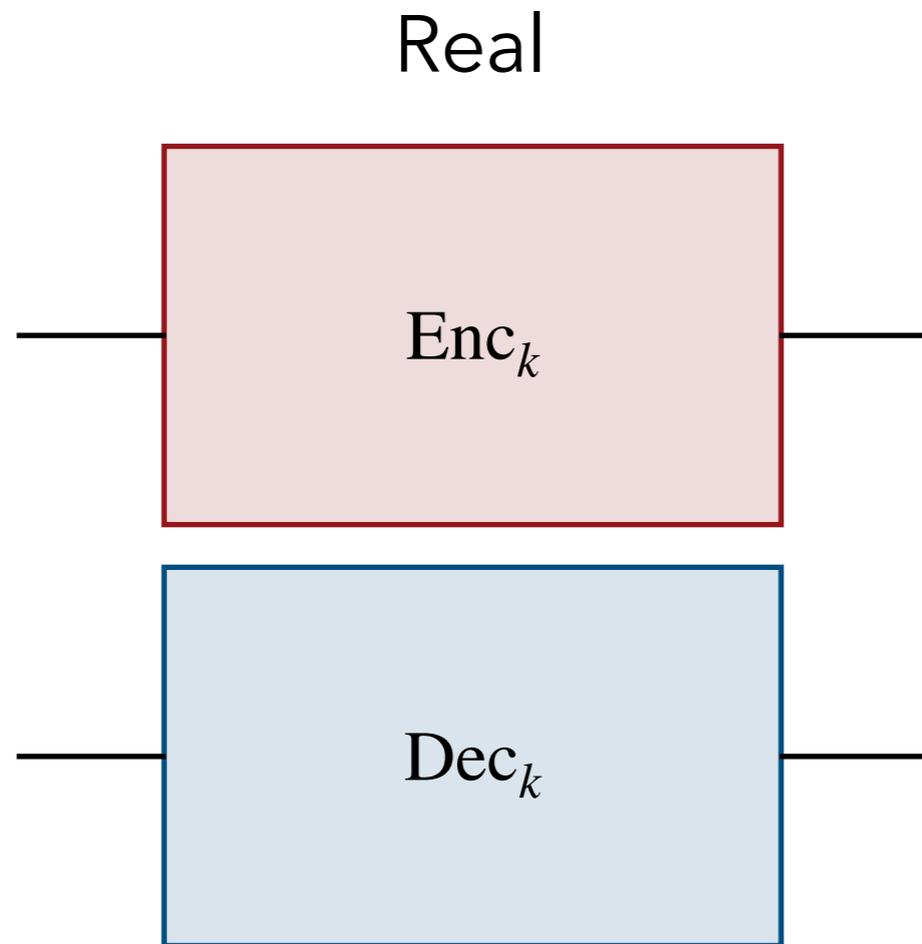


Except that

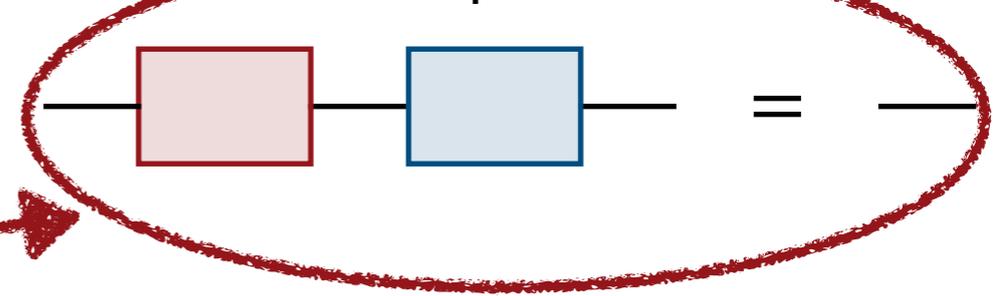


Real vs. Ideal

Alternative characterization (Shrimpton '04):



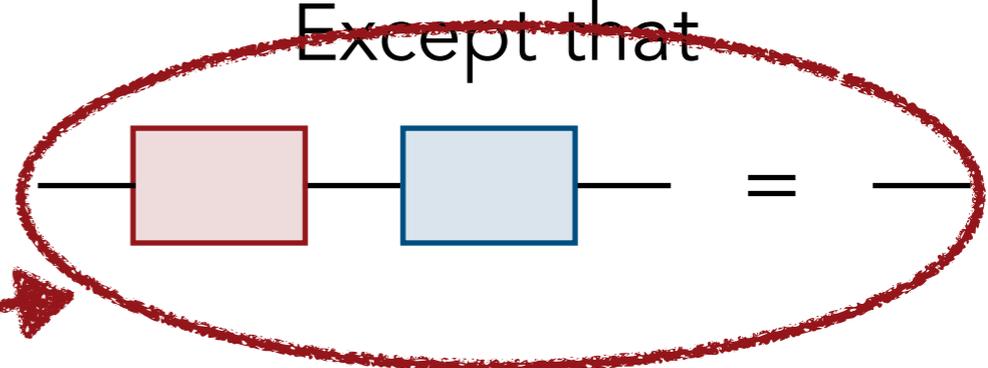
Except that



Enforced by keeping a list
of input-output-pairs
of 

Quantum authenticated encryption

Except that



Enforced by keeping a list
of input-output-pairs
of 

Quantum authenticated encryption

Problem 1: requires copying quantum ciphertexts...

Quantum authenticated encryption

Problem 1: requires copying quantum ciphertexts...
forbidden by *quantum no-cloning theorem!*

Quantum authenticated encryption

Problem 1: requires copying quantum ciphertexts...

forbidden by *quantum no-cloning theorem!*

"Recording Barrier"

Quantum authenticated encryption

Problem 1: requires copying quantum ciphertexts...

forbidden by *quantum no-cloning theorem!*

"Recording Barrier"

Problem 2: Measurement disturbance

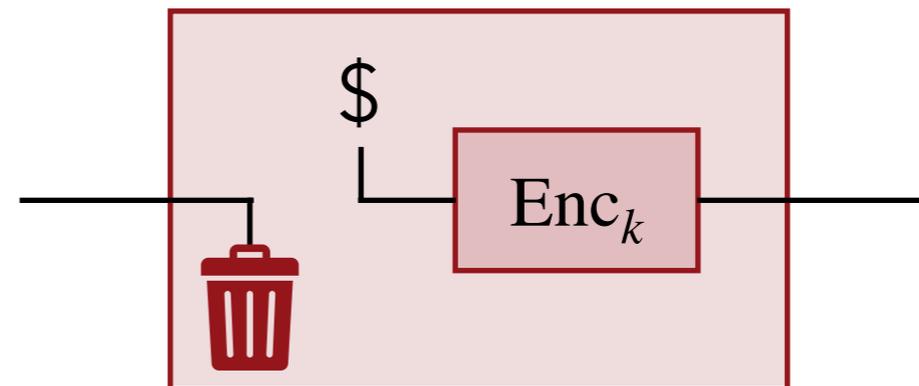
Quantum authenticated encryption

Problem 1: requires copying quantum ciphertexts...
forbidden by *quantum no-cloning theorem!*

"Recording Barrier"

Problem 2: Measurement disturbance

Solution 1: Purify "\$"



Quantum authenticated encryption

Problem 1: requires copying quantum ciphertexts...
forbidden by *quantum no-cloning theorem!*

"Recording Barrier"

Problem 2: Measurement disturbance

Solution 1: Purify "\$"

Solution 2: Even CPA-secure encryption is randomized... record the randomness!

Quantum authenticated encryption

Problem 1: requires copying quantum ciphertexts...
forbidden by *quantum no-cloning theorem!*

"Recording Barrier"

Problem 2: Measurement disturbance

Solution 1: Purify "\$"

Solution 2: Even CPA-secure encryption is randomized... record the randomness!

Alagic, Gagliardoni, M '18: Definition of quantum authenticated encryption

- ▶ Reduces to authenticated encryption for classical schemes
- ▶ Can be satisfied with simple hybrid encryption

Summary and open problems

Summary and open problems

- ▶ Are we ready for encrypting the quantum internet?

Summary and open problems

- ▶ Are we ready for encrypting the quantum internet?

To some extent:

Summary and open problems

- ▶ Are we ready for encrypting the quantum internet?

To some extent:

- Quantum digital signatures are impossible, but not needed for this purpose

Summary and open problems

- ▶ Are we ready for encrypting the quantum internet?

To some extent:

- Quantum digital signatures are impossible, but not needed for this purpose
- We have efficient quantum-secure digital signatures

Summary and open problems

- ▶ Are we ready for encrypting the quantum internet?

To some extent:

- Quantum digital signatures are impossible, but not needed for this purpose
- We have efficient quantum-secure digital signatures
- Quantum Authenticated Encryption can be defined and constructed

Summary and open problems

- ▶ Are we ready for encrypting the quantum internet?

To some extent:

- Quantum digital signatures are impossible, but not needed for this purpose
 - We have efficient quantum-secure digital signatures
 - Quantum Authenticated Encryption can be defined and constructed
- ▶ This is just the beginning, many interesting questions:

Summary and open problems

- ▶ Are we ready for encrypting the quantum internet?

To some extent:

- Quantum digital signatures are impossible, but not needed for this purpose
 - We have efficient quantum-secure digital signatures
 - Quantum Authenticated Encryption can be defined and constructed
- ▶ This is just the beginning, many interesting questions:
 - Ongoing work: is quantum communication provably necessary for unconditional security à la QKD?

Summary and open problems

- ▶ Are we ready for encrypting the quantum internet?

To some extent:

- Quantum digital signatures are impossible, but not needed for this purpose
 - We have efficient quantum-secure digital signatures
 - Quantum Authenticated Encryption can be defined and constructed
- ▶ This is just the beginning, many interesting questions:
 - Ongoing work: is quantum communication provably necessary for unconditional security à la QKD?
 - Signatures are used everywhere. Ramifications of impossibility?

Summary and open problems

- ▶ Are we ready for encrypting the quantum internet?

To some extent:

- Quantum digital signatures are impossible, but not needed for this purpose
 - We have efficient quantum-secure digital signatures
 - Quantum Authenticated Encryption can be defined and constructed
- ▶ This is just the beginning, many interesting questions:
 - Ongoing work: is quantum communication provably necessary for unconditional security à la QKD?
 - Signatures are used everywhere. Ramifications of impossibility?
 - Can we have more efficient quantum authenticated encryption from “quantum block ciphers”

Summary and open problems

- ▶ Are we ready for encrypting the quantum internet?

To some extent:

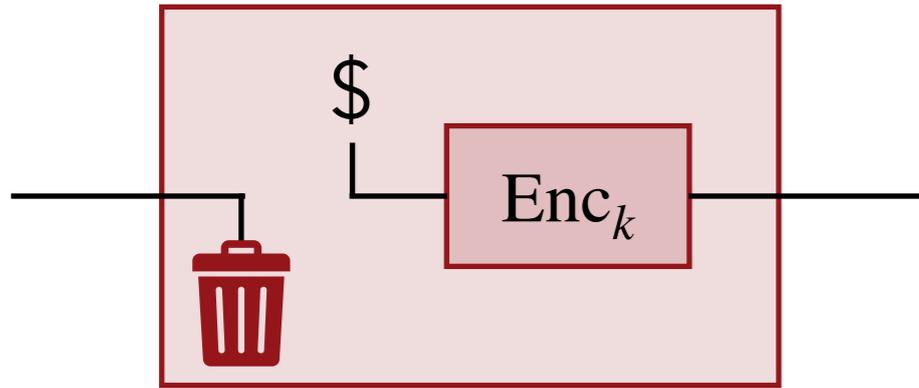
- Quantum digital signatures are impossible, but not needed for this purpose
 - We have efficient quantum-secure digital signatures
 - Quantum Authenticated Encryption can be defined and constructed
- ▶ This is just the beginning, many interesting questions:
 - Ongoing work: is quantum communication provably necessary for unconditional security à la QKD?
 - Signatures are used everywhere. Ramifications of impossibility?
 - Can we have more efficient quantum authenticated encryption from “quantum block ciphers”
 - Do “quantum block ciphers” exist?

Summary and open problems

- ▶ Are we ready for encrypting the quantum internet?

To some extent:

- Quantum digital signatures are impossible, but not needed for this purpose
 - We have efficient quantum-secure digital signatures
 - Quantum Authenticated Encryption can be defined and constructed
- ▶ This is just the beginning, many interesting questions:
 - Ongoing work: is quantum communication provably necessary for unconditional security à la QKD?
 - Signatures are used everywhere. Ramifications of impossibility?
 - Can we have more efficient quantum authenticated encryption from “quantum block ciphers”
 - Do “quantum block ciphers” exist?
 - Noninteractive verification of quantum computation...



Thank you very much for your attention!

