Cryptography for the quantum internet

Elements of a “quantum TLS”

Christian Majenz

Colloquium

Informatics Institute, University of Amsterdam

QuSoft
Research Center for Quantum Software

CWI
Centrum Wiskunde & Informatica

Quantum computers

Quantum computers

- Accelerating effort to build a quantum computer

Quantum computers

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

QUTech
Google
IBM
nationale wetenschaps agenda
intel
Microsoft
QUANTUM FLAGSHIP

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
  - …

Quantum computers

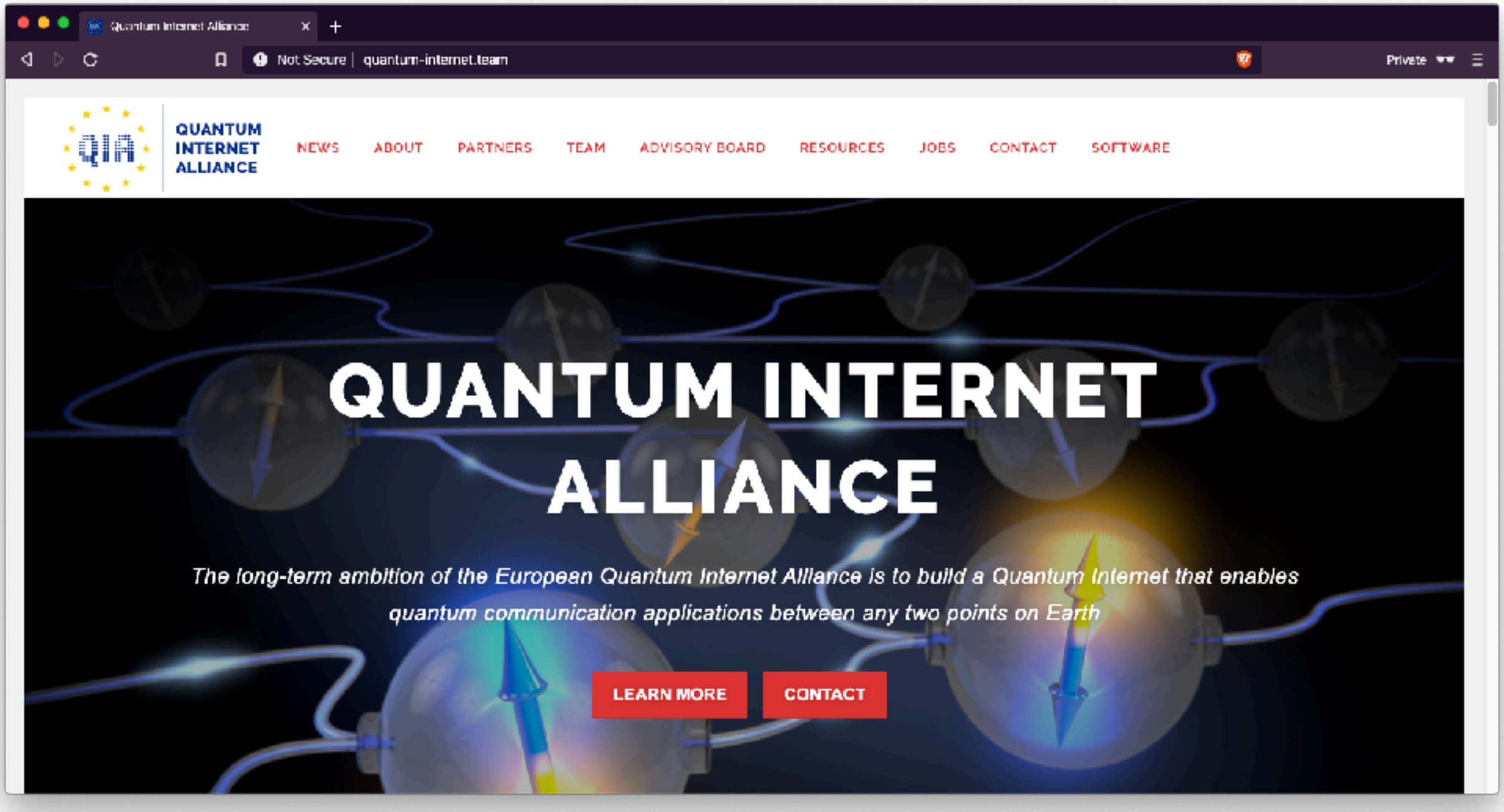
- Accelerating effort to build a quantum computer
- Major investments:



- 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



Quantum internet

Quantum internet

Quantum internet

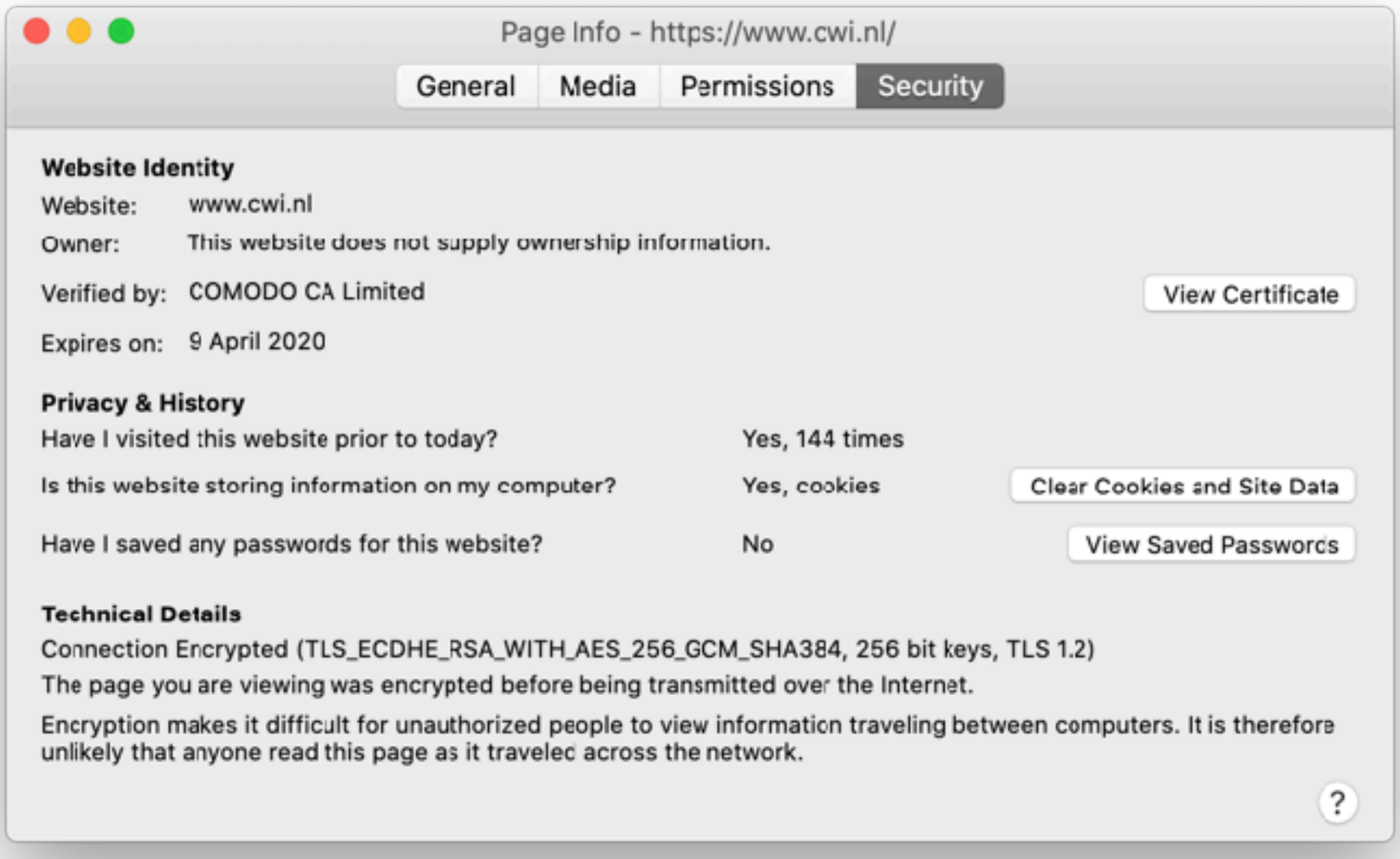
How can we secure the Quantum internet?

Internet crypto

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

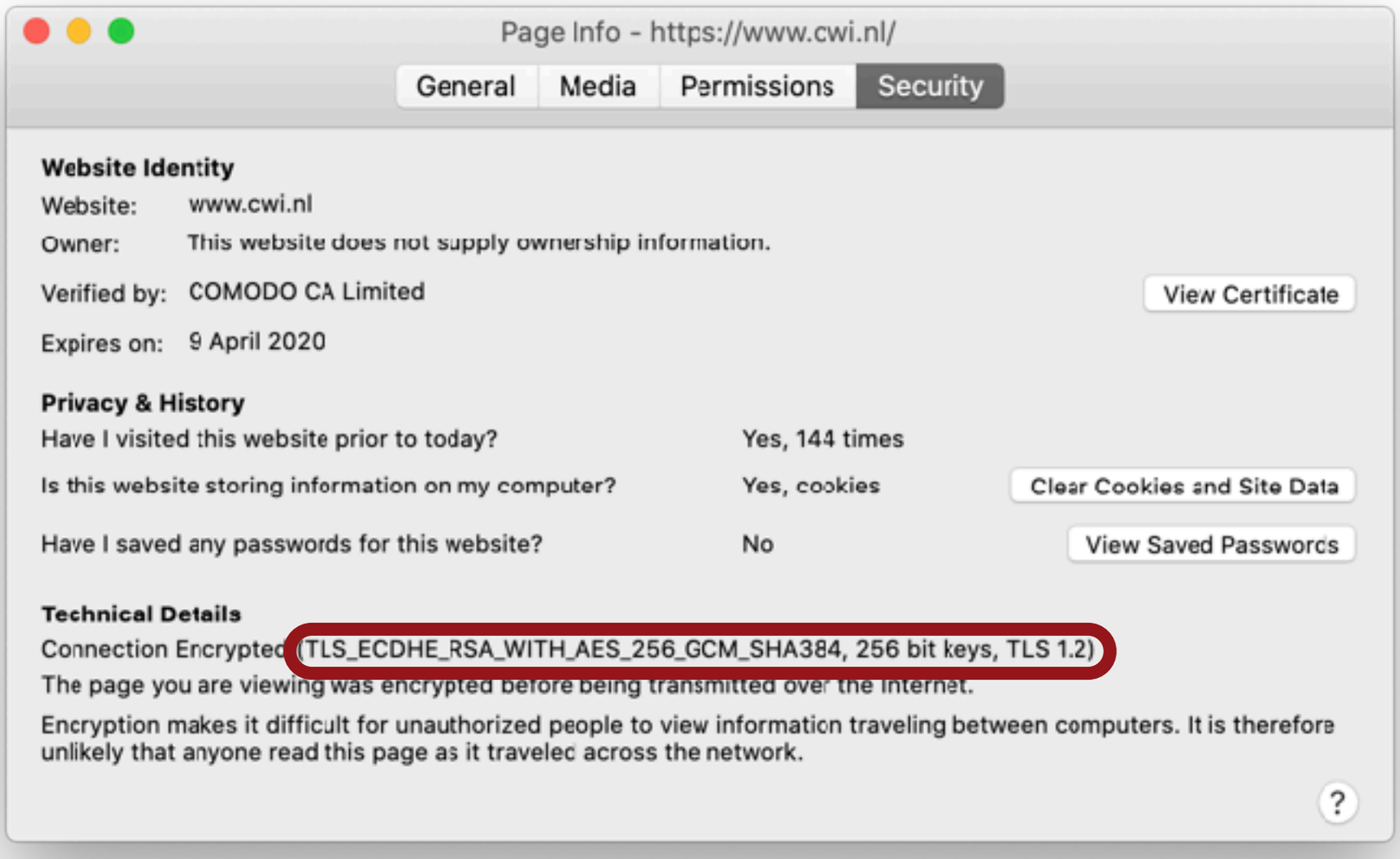
Internet crypto

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

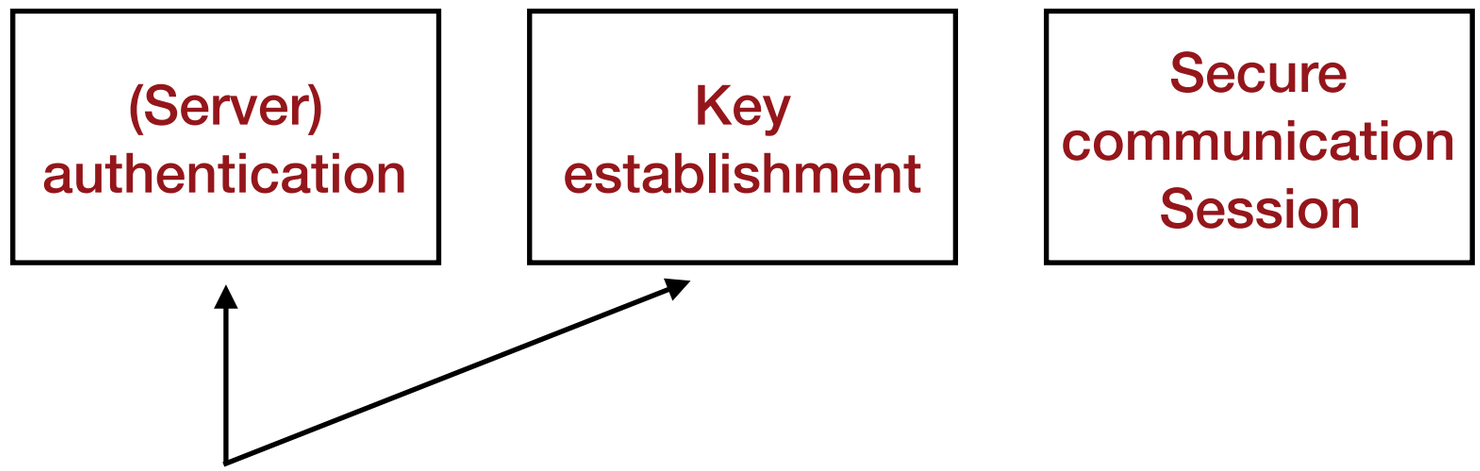
The TLS protocol

Functionalities

- (Server) authentication
- Key establishment
- Secure communication Session

The TLS protocol

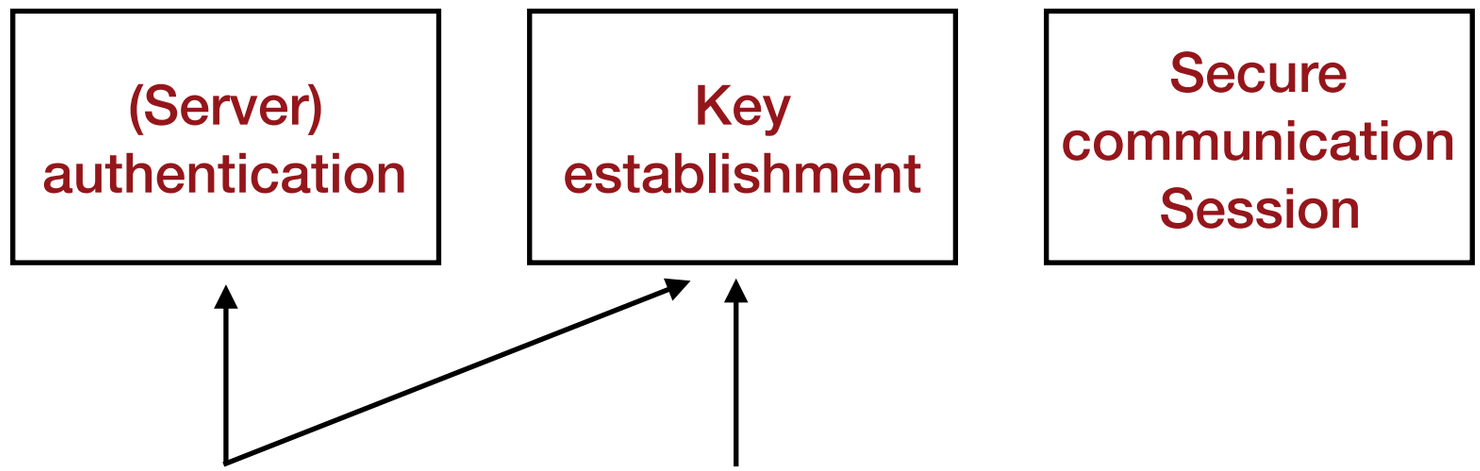
Functionalities



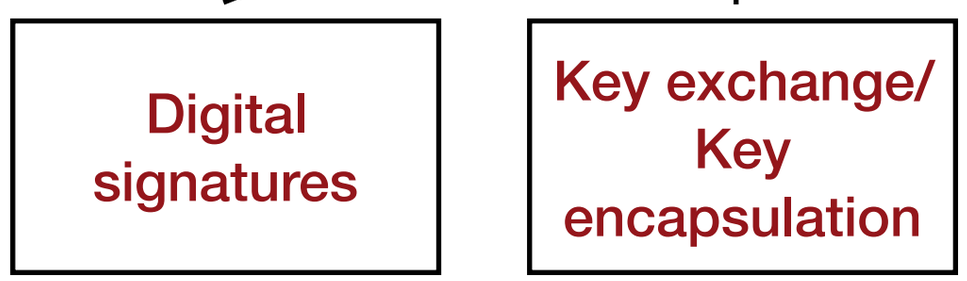
Protocols

The TLS protocol

Functionalities

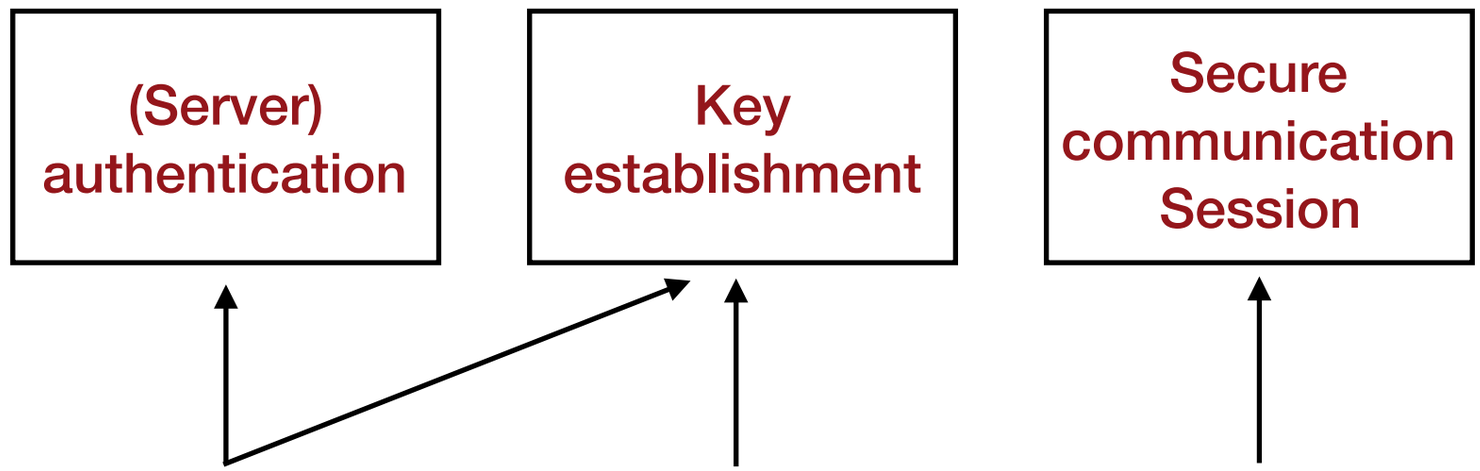


Protocols

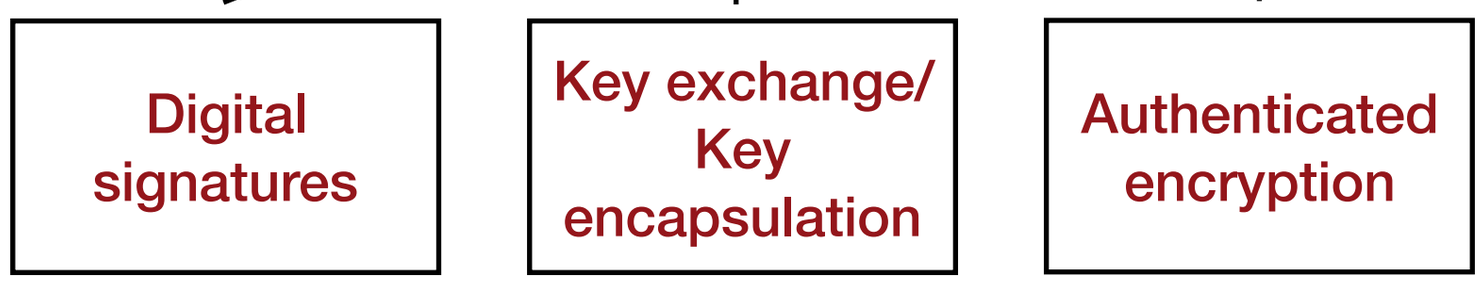


The TLS protocol

Functionalities



Protocols

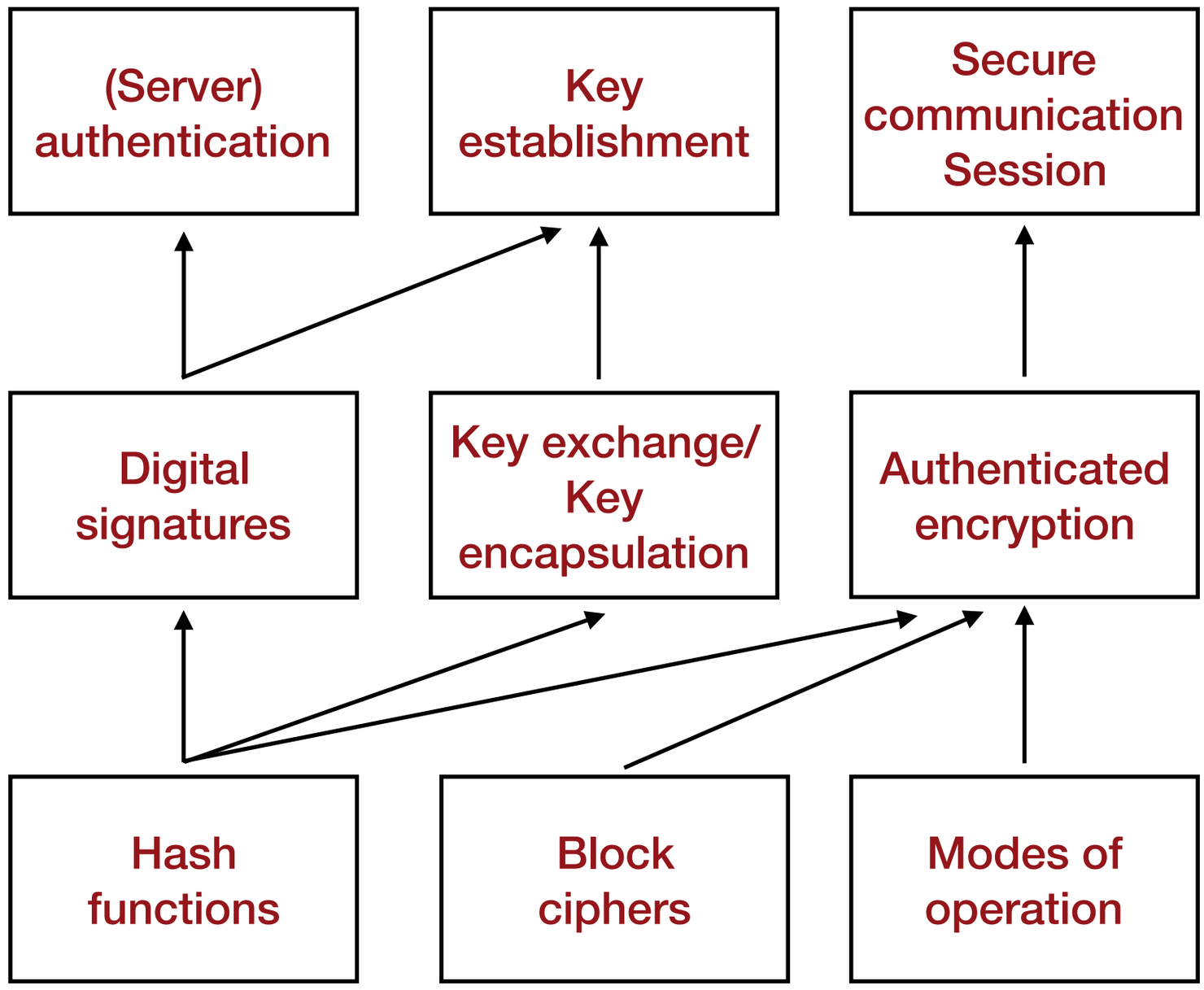


The TLS protocol

Functionalities

Protocols

Cryptographic Ingredients



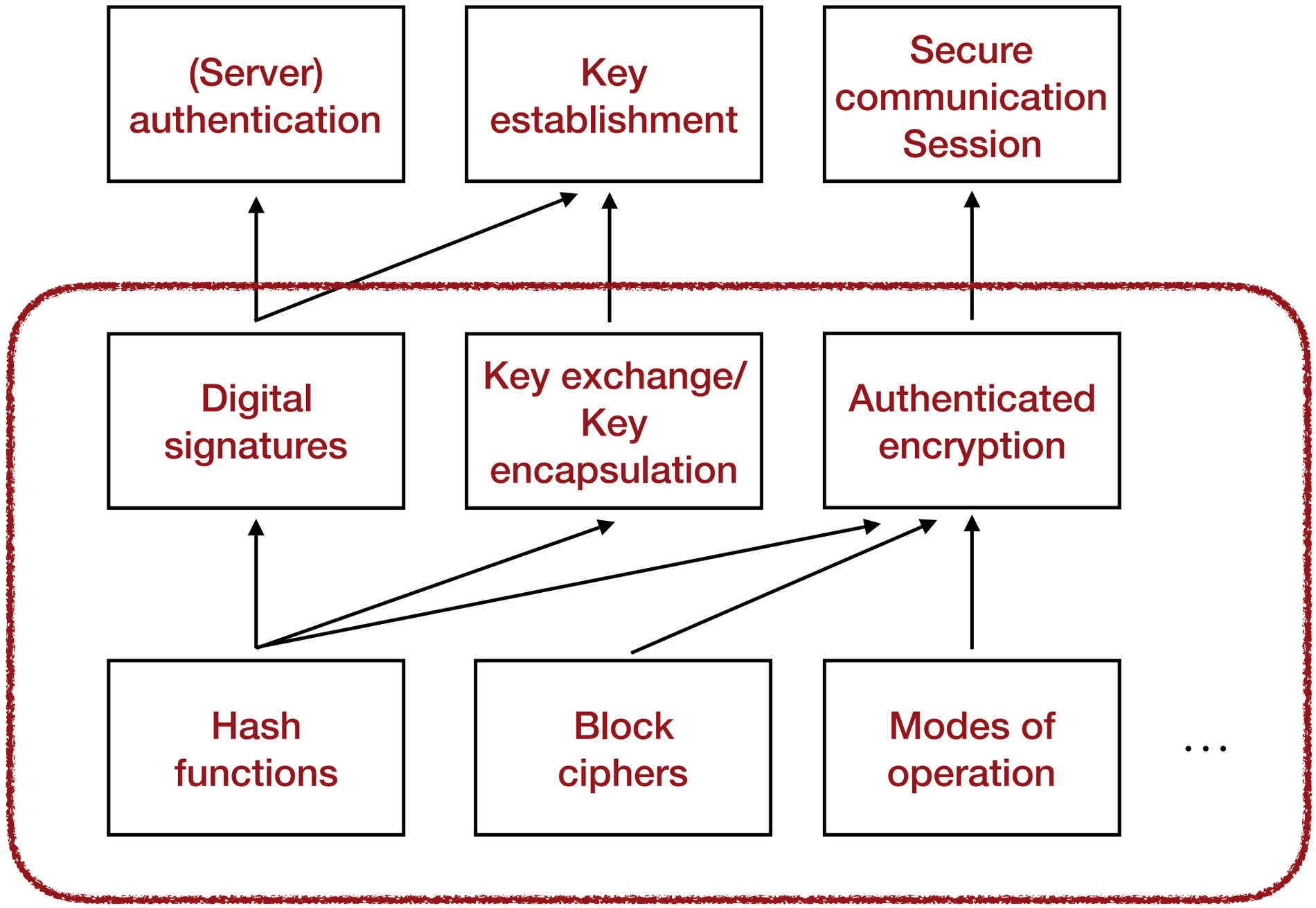
The TLS protocol

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

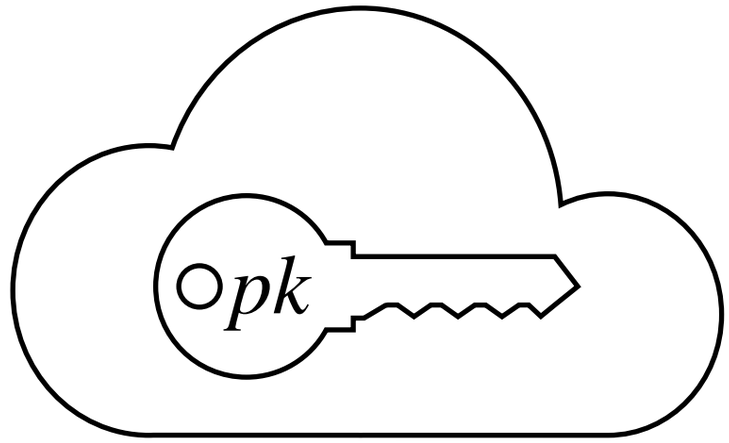
Bob

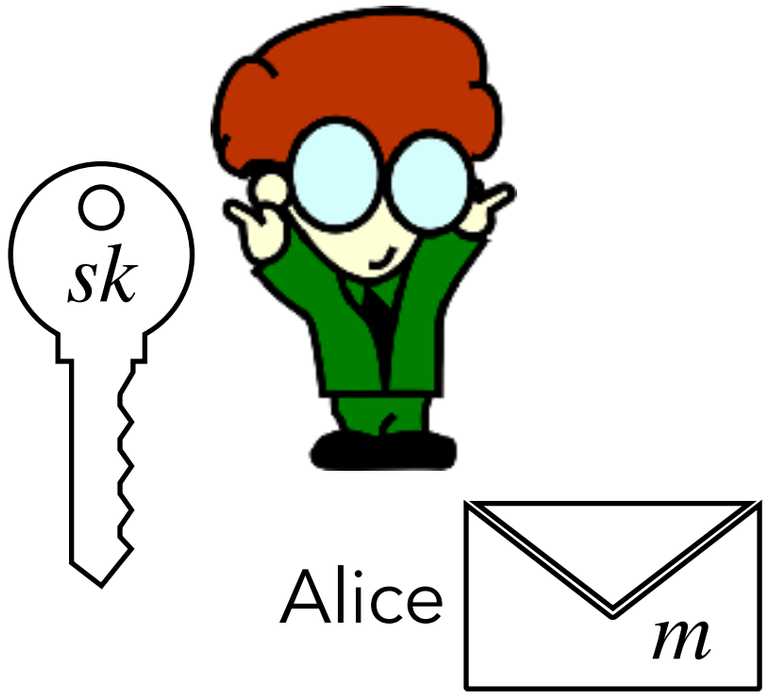
Digital signatures

Alice

Bob

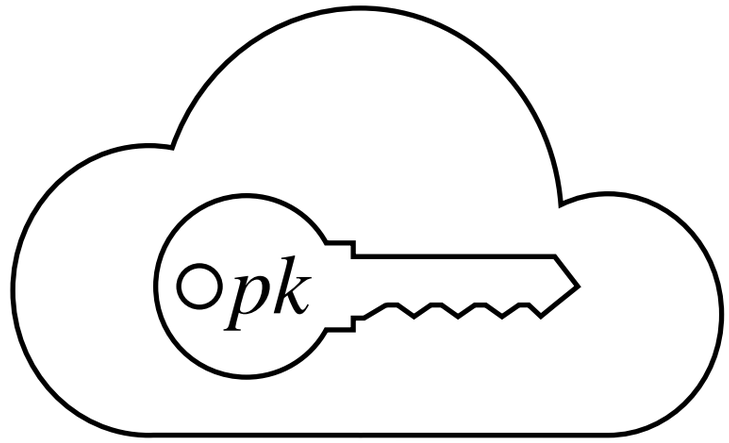
Digital signatures

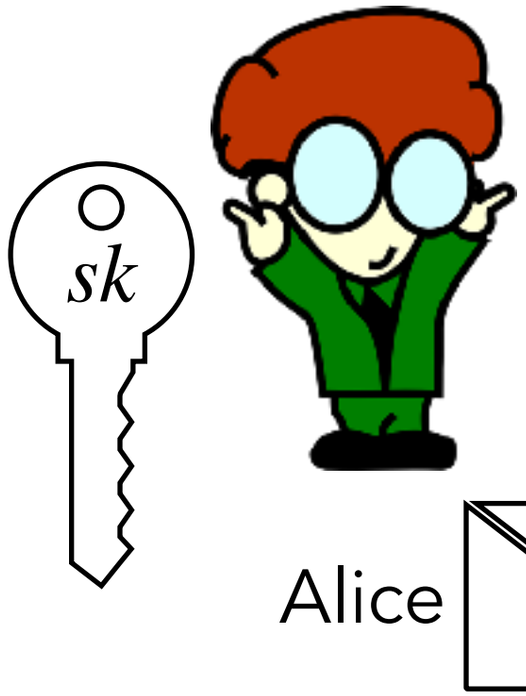




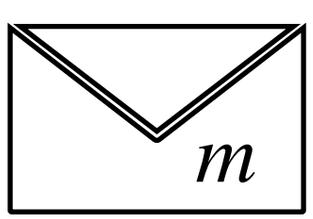
Bob

Digital signatures





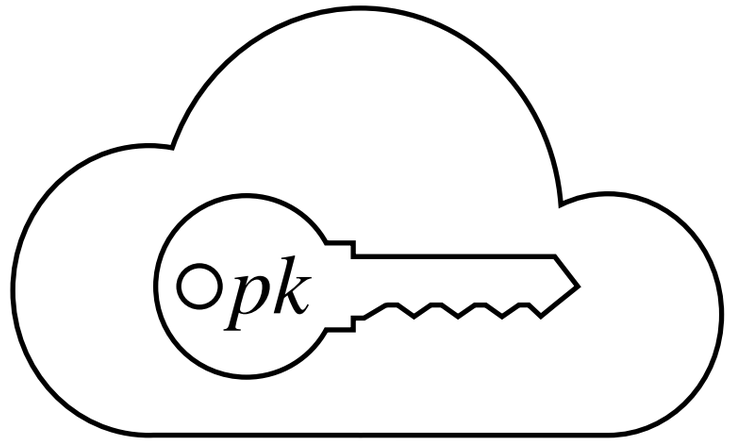
Alice

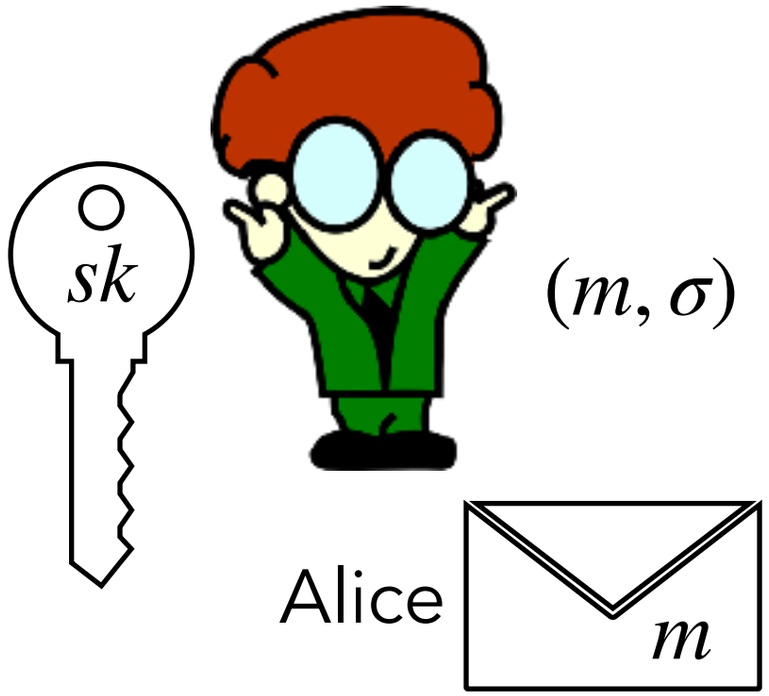


Bob

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

Digital signatures

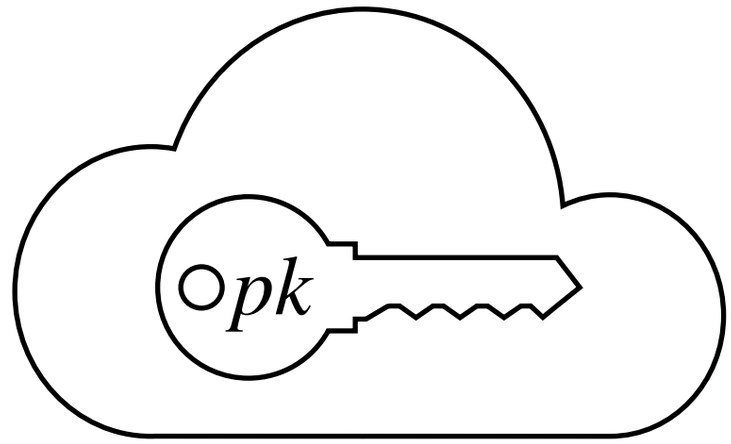


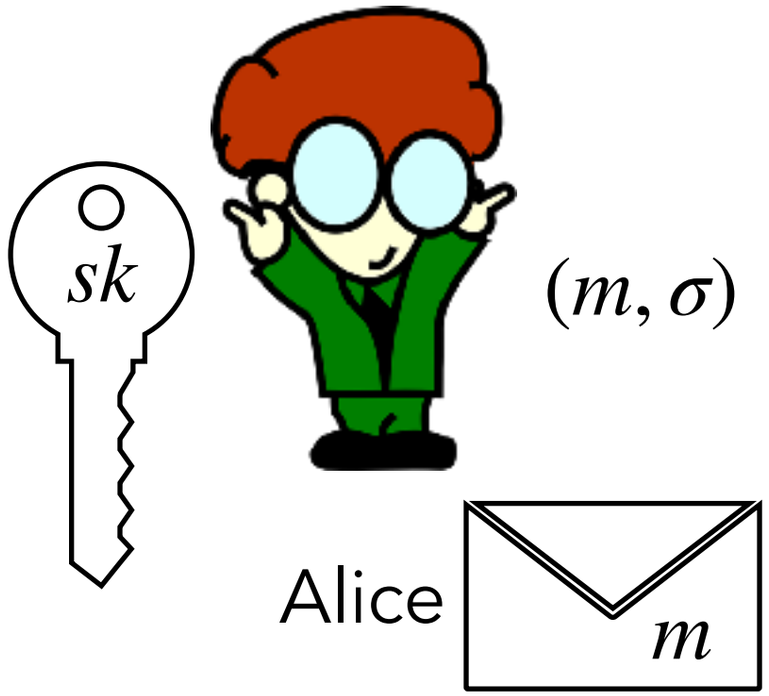


Bob

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

Digital signatures



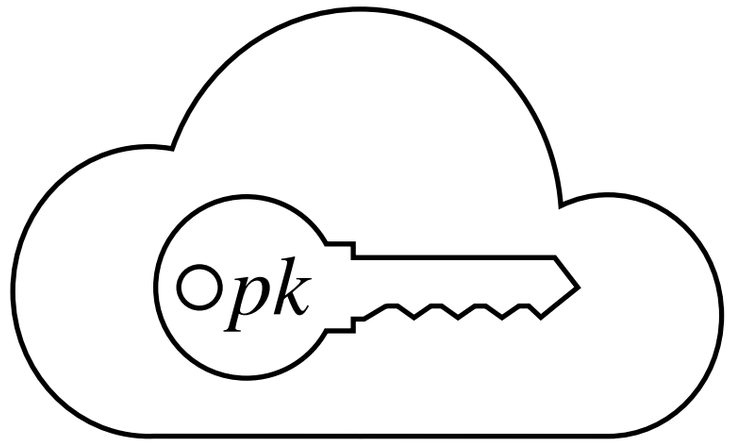


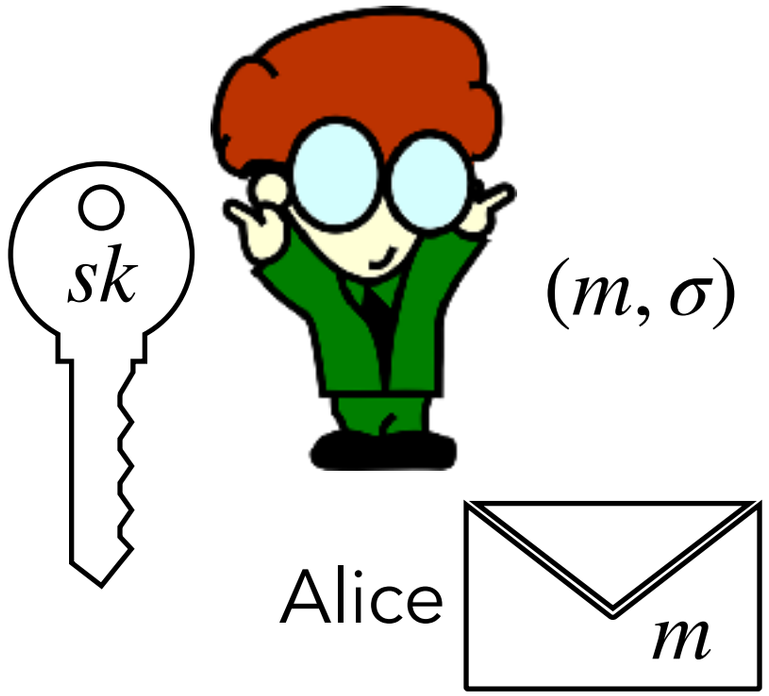
Bob

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

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

Digital signatures





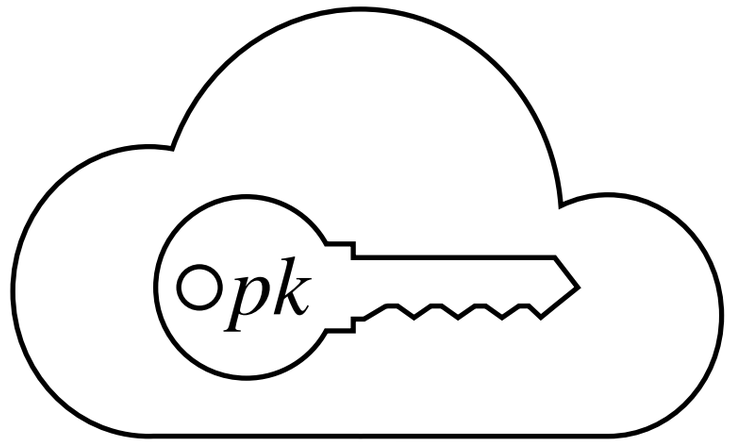
Bob

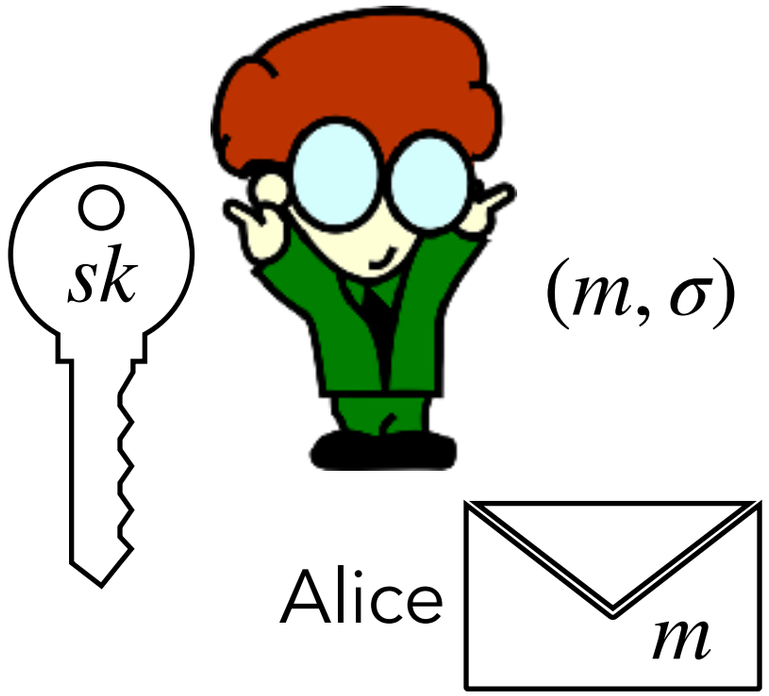
$\sigma = \mathrm{Sign}_{sk}(m)$

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

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

Digital signatures





Bob

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

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

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

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”?

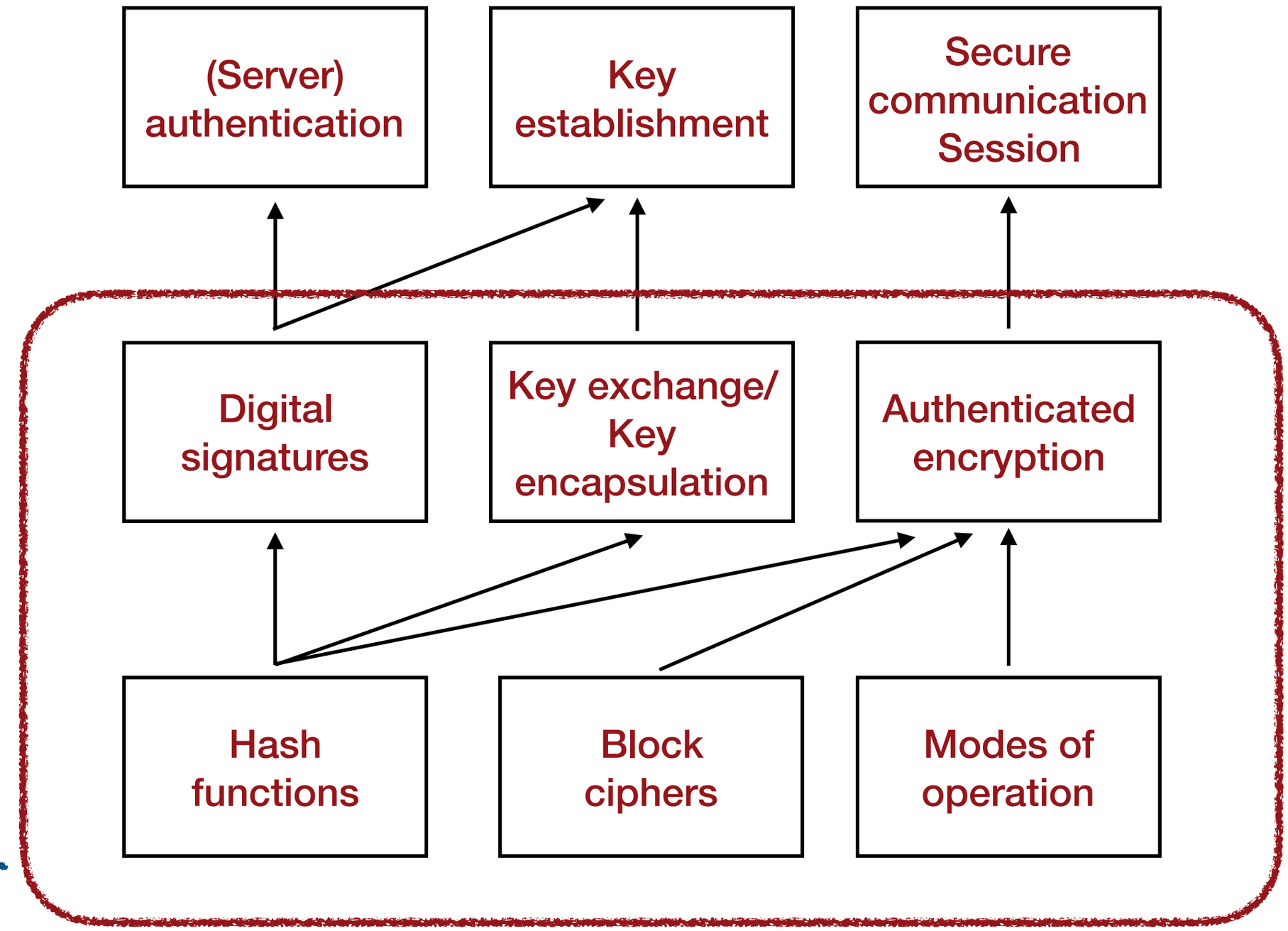
The TLS protocol

Functionalities

Protocols

Cryptographic Ingredients

Quantum-ready?



The TLS protocol

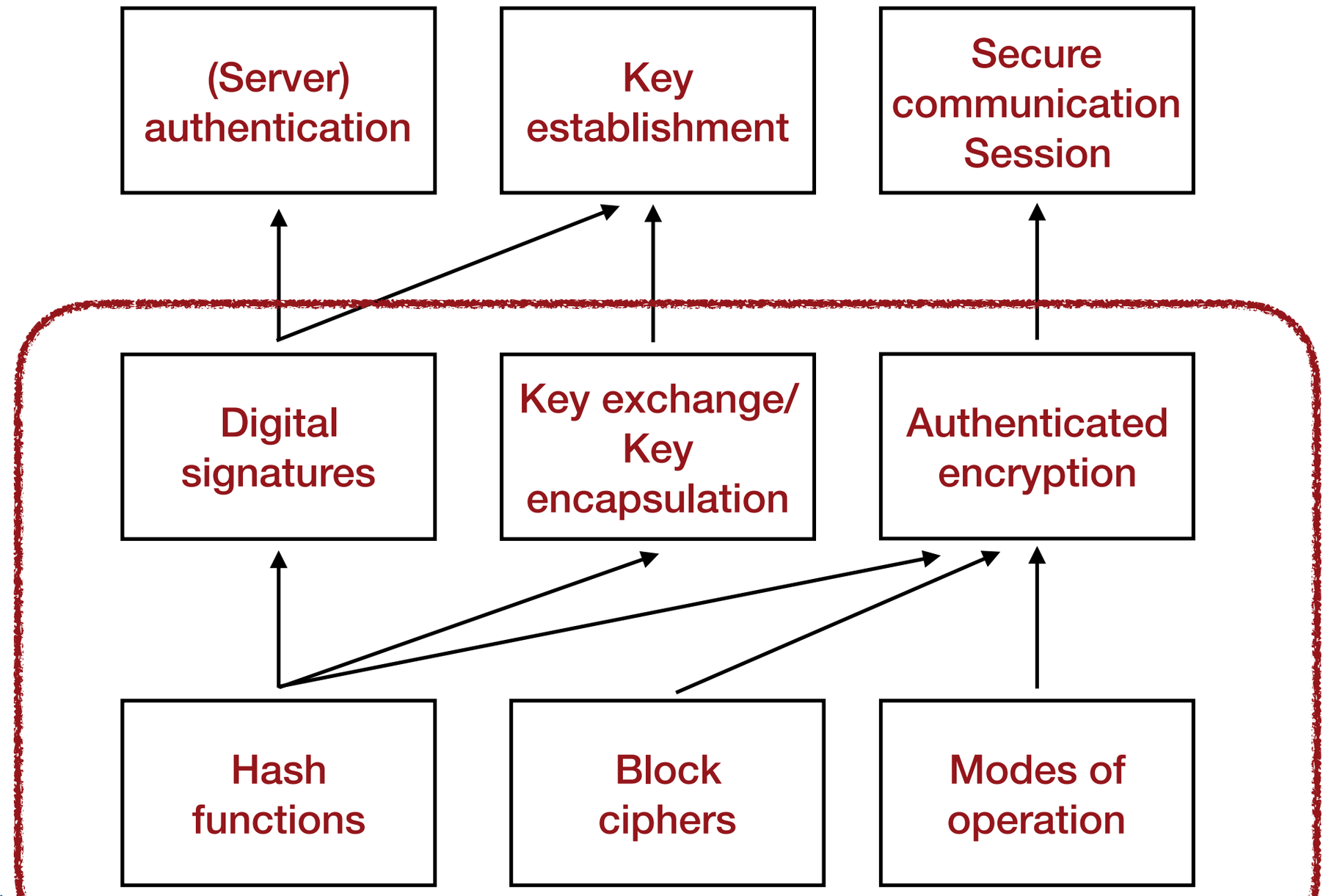
Quantum

Functionalities

Protocols

Cryptographic Ingredients

Quantum-ready?



The TLS protocol

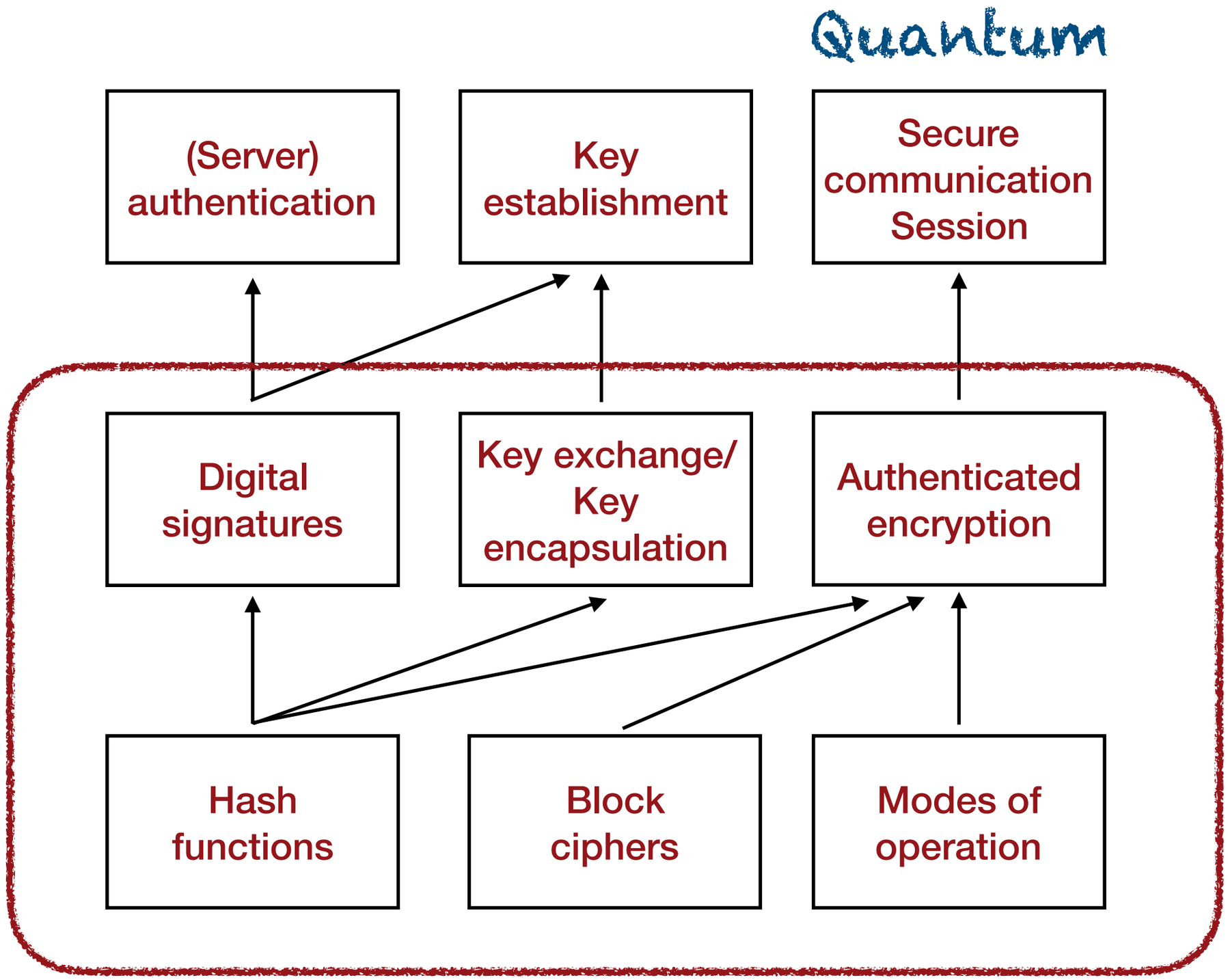
Quantum

Functionalities

Protocols

Cryptographic Ingredients

Quantum-ready?



The TLS protocol

Quantum

"post-quantum"

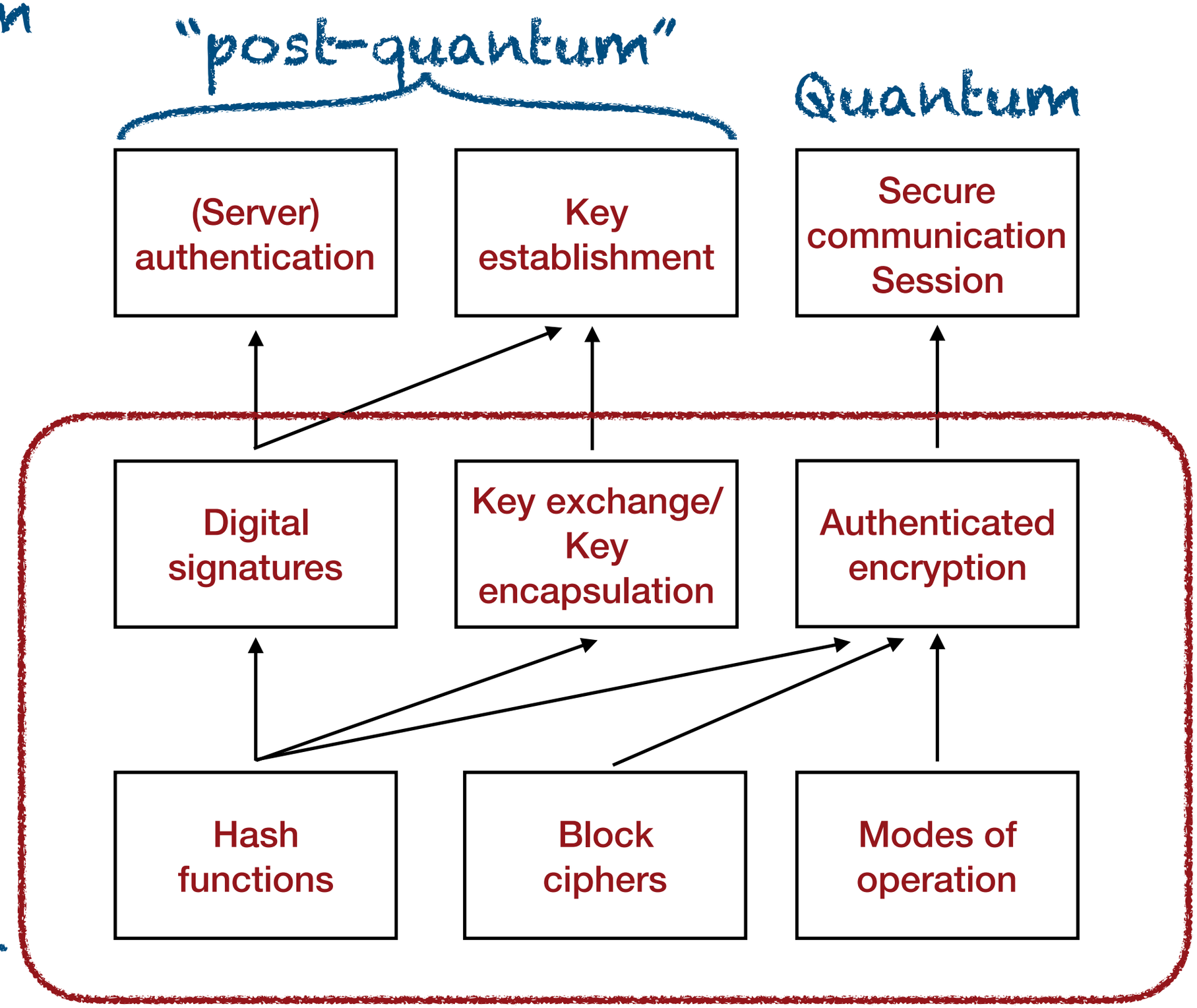
Quantum

Functionalities

Protocols

Cryptographic Ingredients

Quantum-ready?



The TLS protocol

Quantum

"post-quantum"

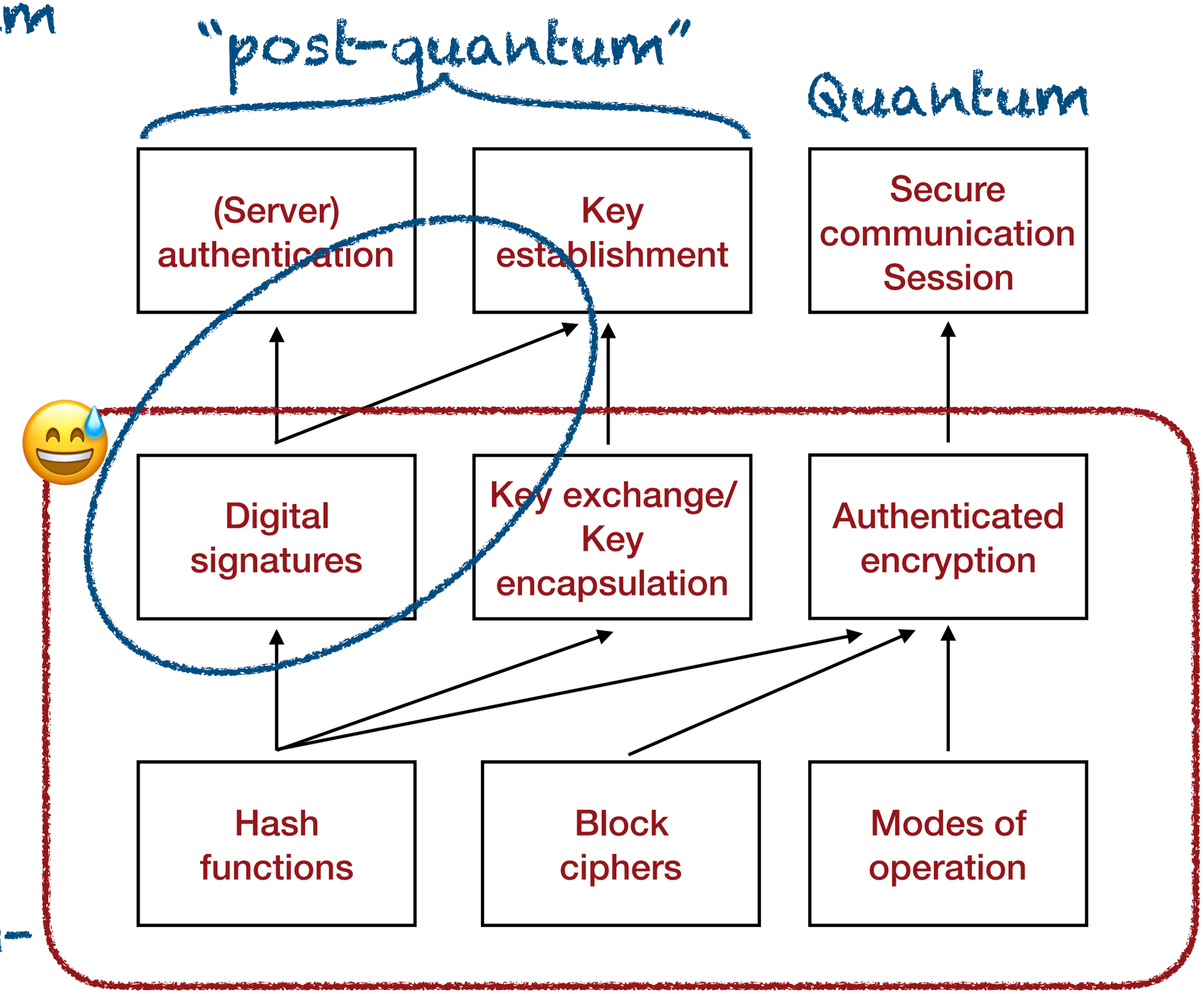
Quantum

Functionalities

Protocols

Cryptographic Ingredients

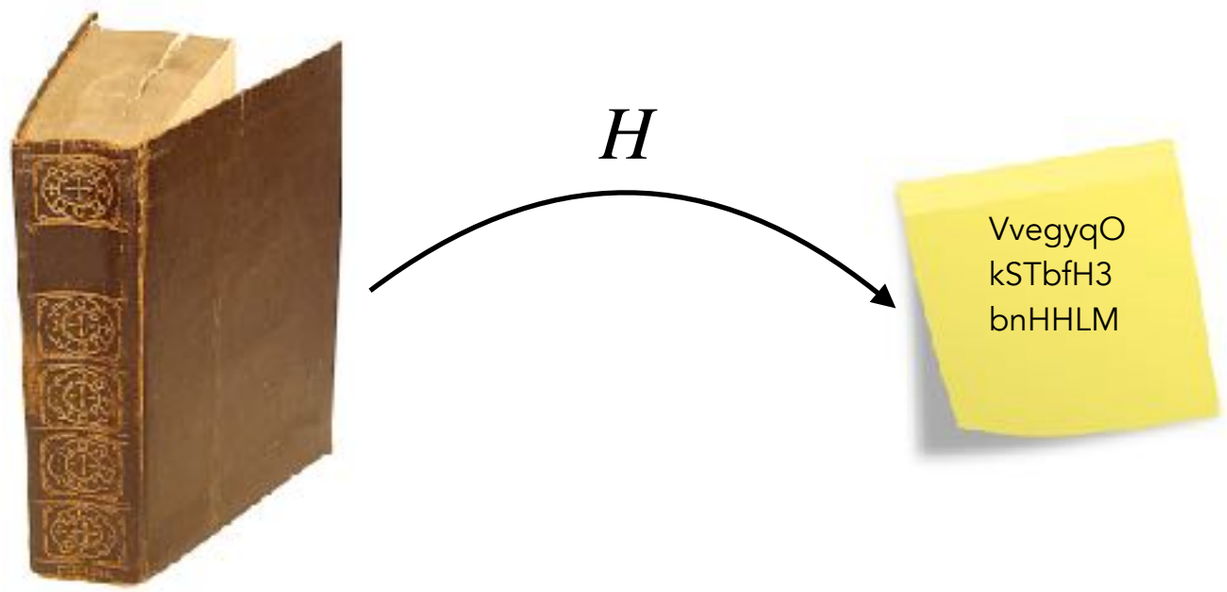
Quantum-ready?



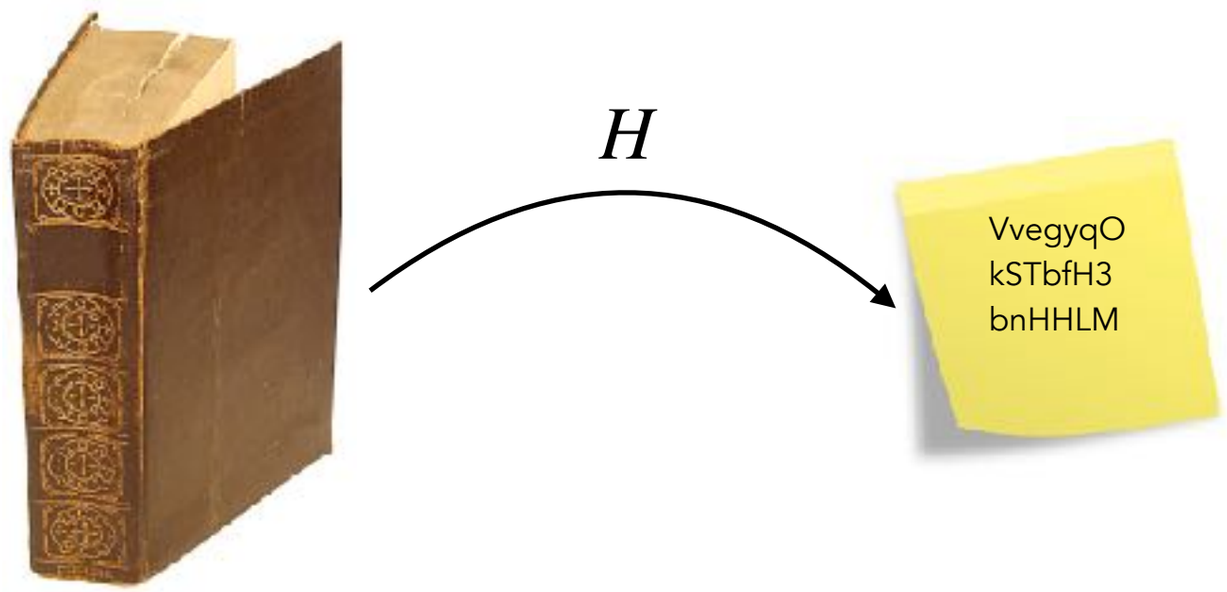
Are we ready for encrypting the quantum internet?

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…

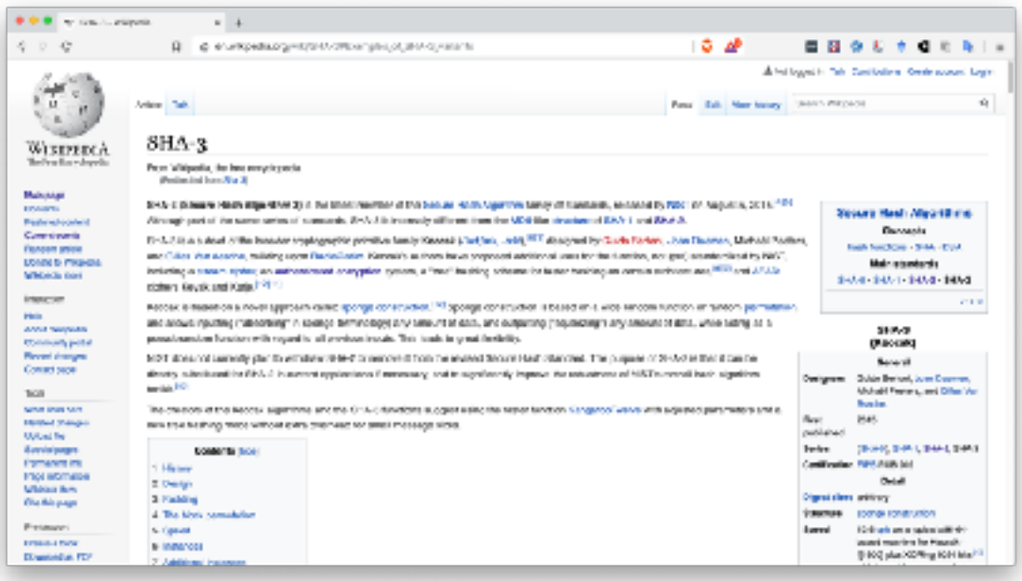
$\Longrightarrow$ just model H as random, “Random Oracle Model” (ROM)

Hash function security

Output should look random! Formalization difficult…

$\Longrightarrow$ just model H as random, “Random Oracle Model” (ROM)

Reality

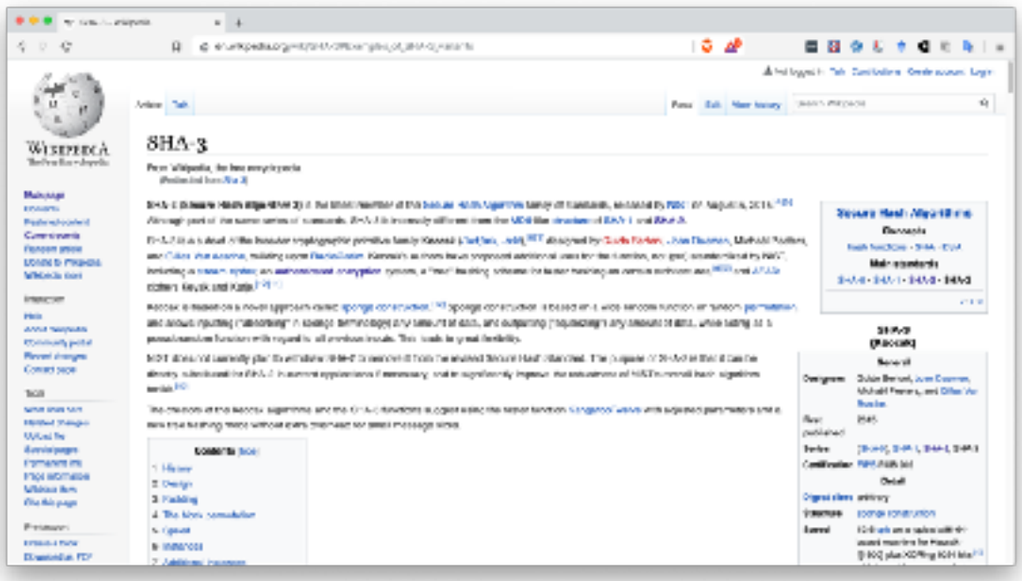


Hash function security

Output should look random! Formalization difficult…

$\Longrightarrow$ just model H as random, "Random Oracle Model" (ROM)

Reality



Model

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

Uniformly random

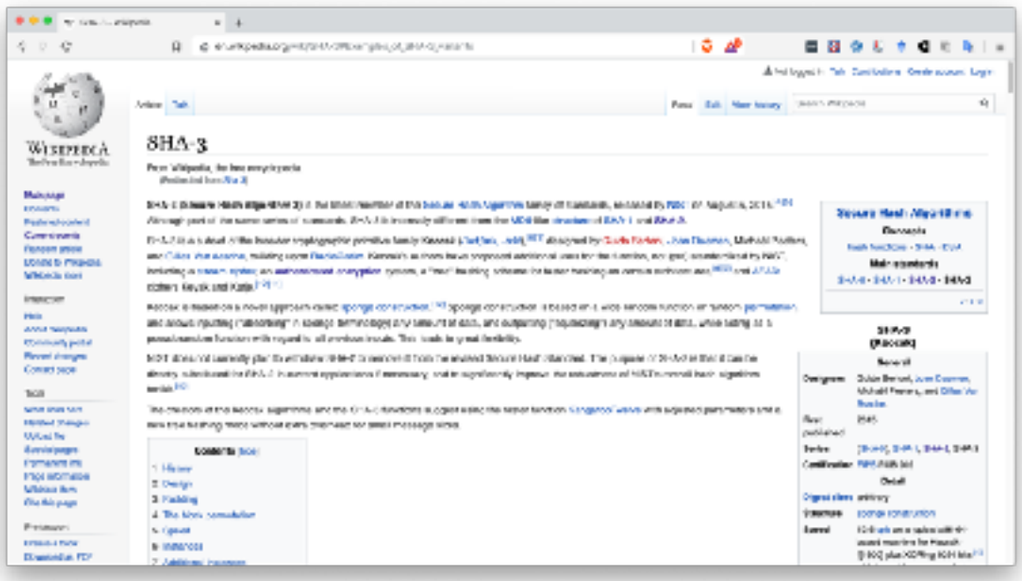
All agents have oracle access to H

Hash function security

Output should look random! Formalization difficult…

$\Longrightarrow$ just model H as random, “Random Oracle Model” (ROM)

Reality



Model

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

Uniformly random

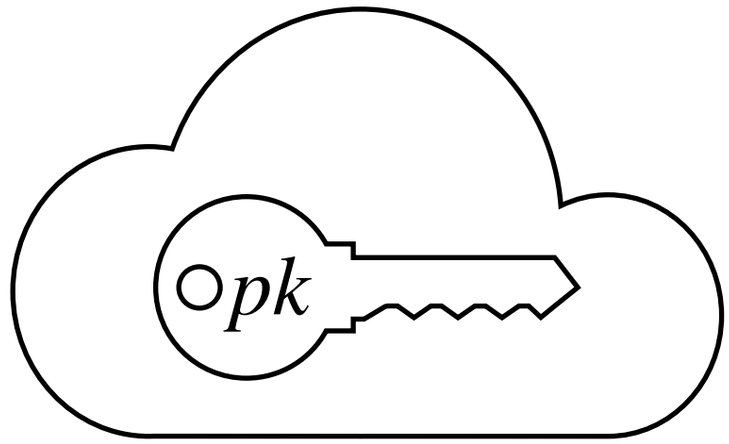
All agents have quantum oracle access to H

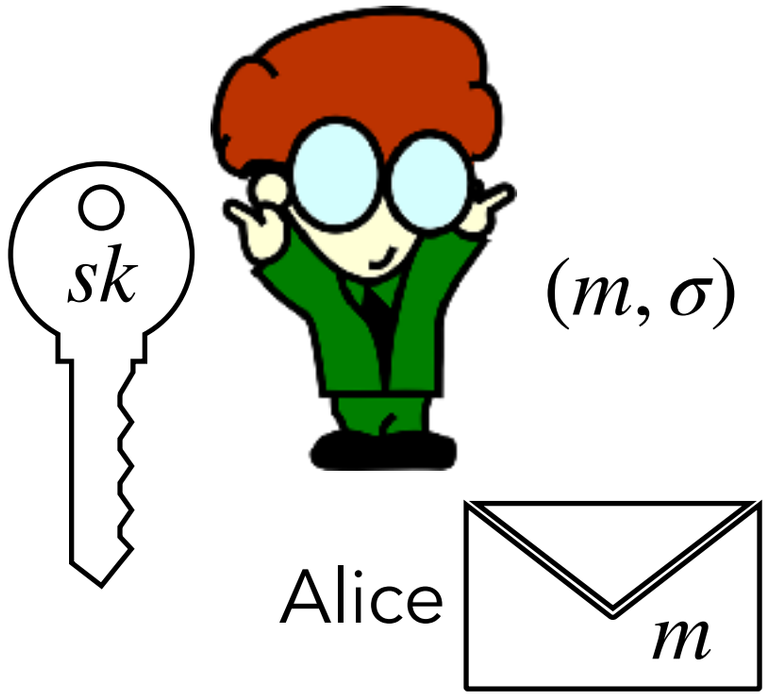
Quantum Random Oracle Model (Boneh et al. ’10)

Are we ready for encrypting the quantum internet?

Digital Signatures II

Digital signatures





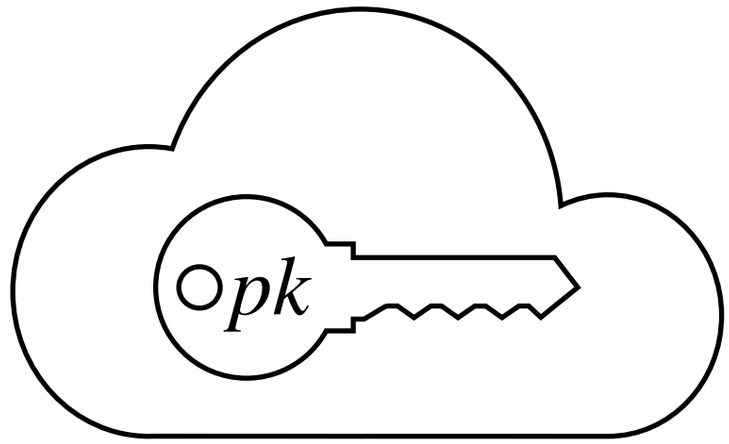
Bob

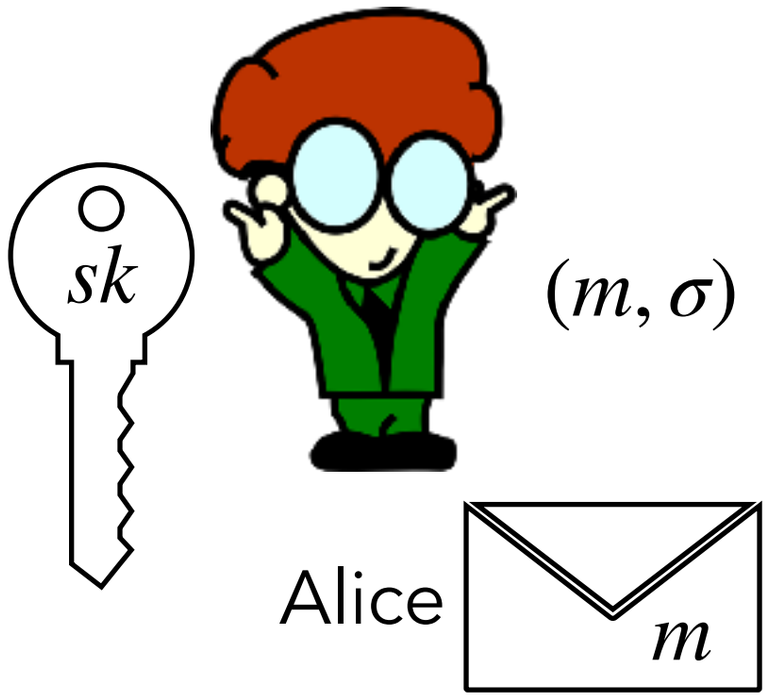
$\sigma = \mathrm{Sign}_{sk}(m)$

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

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

Digital signatures





(m, σ)

Bob

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

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

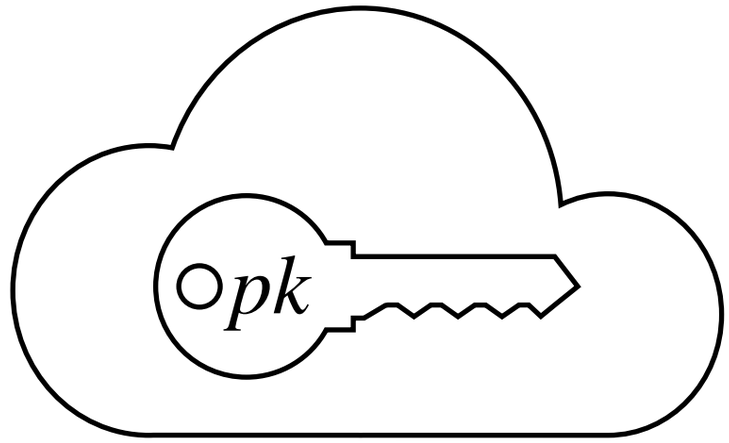
Computed in polynomial time

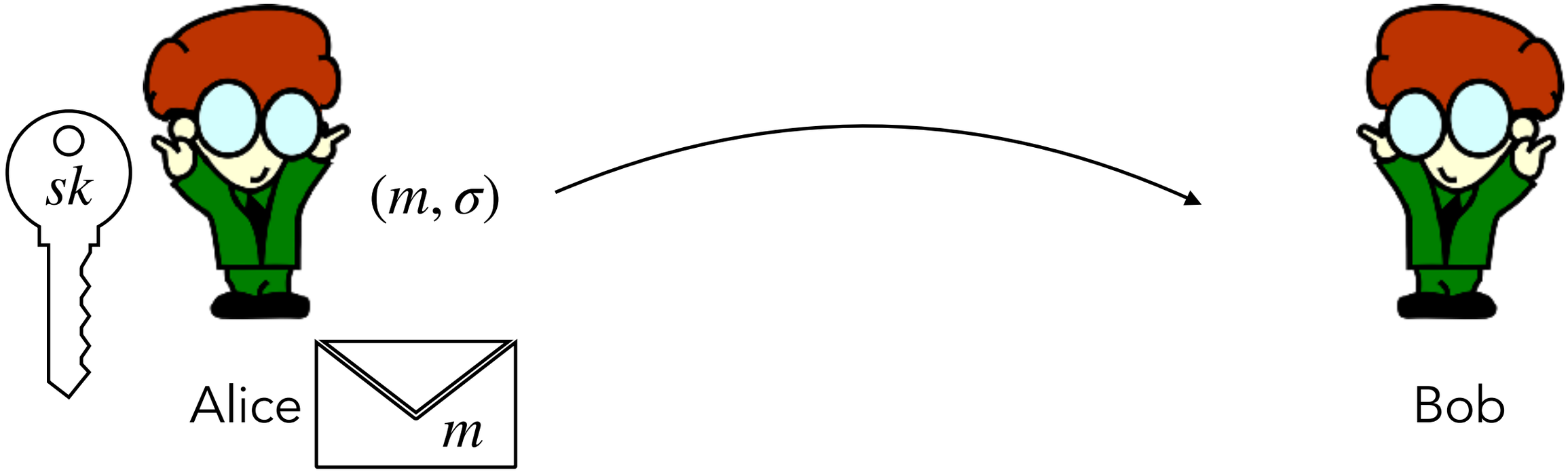
Security: If (m', σ') was ~~produced~~ from (m, σ) without using sk, then

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

Digital signatures

post-quantum





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

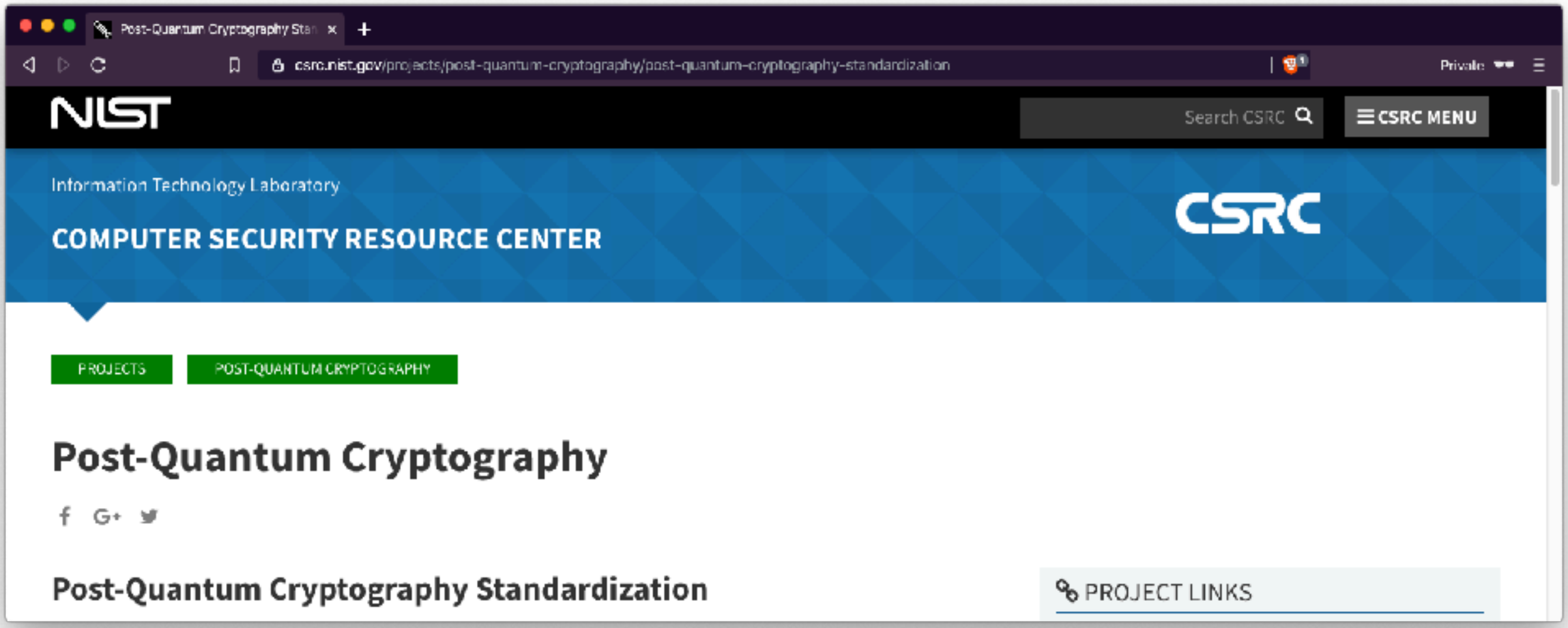
$\mathrm{Ver}_{pk}(m, \sigma) = \mathrm{accept}$

Computed in quantum polynomial time

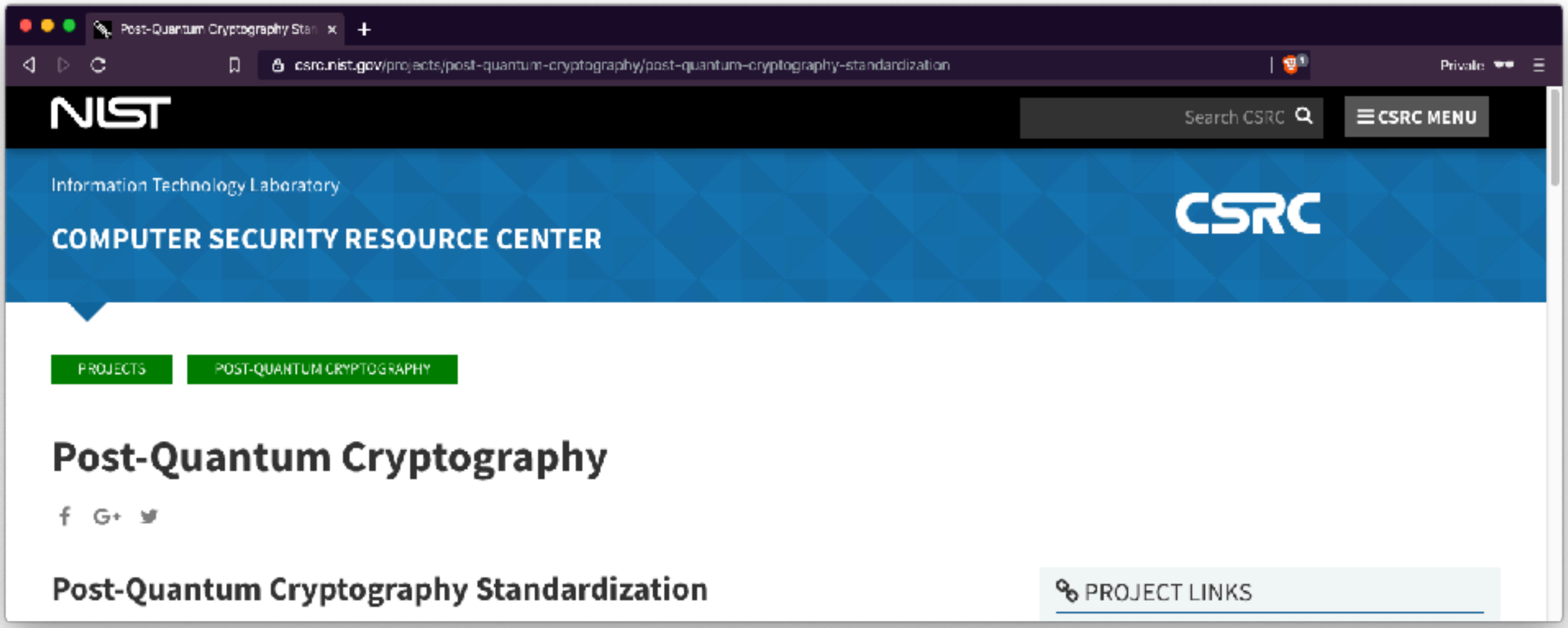
Security: If (m', σ') was ~~produced~~ from (m, σ) without using sk, then

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

NIST competition

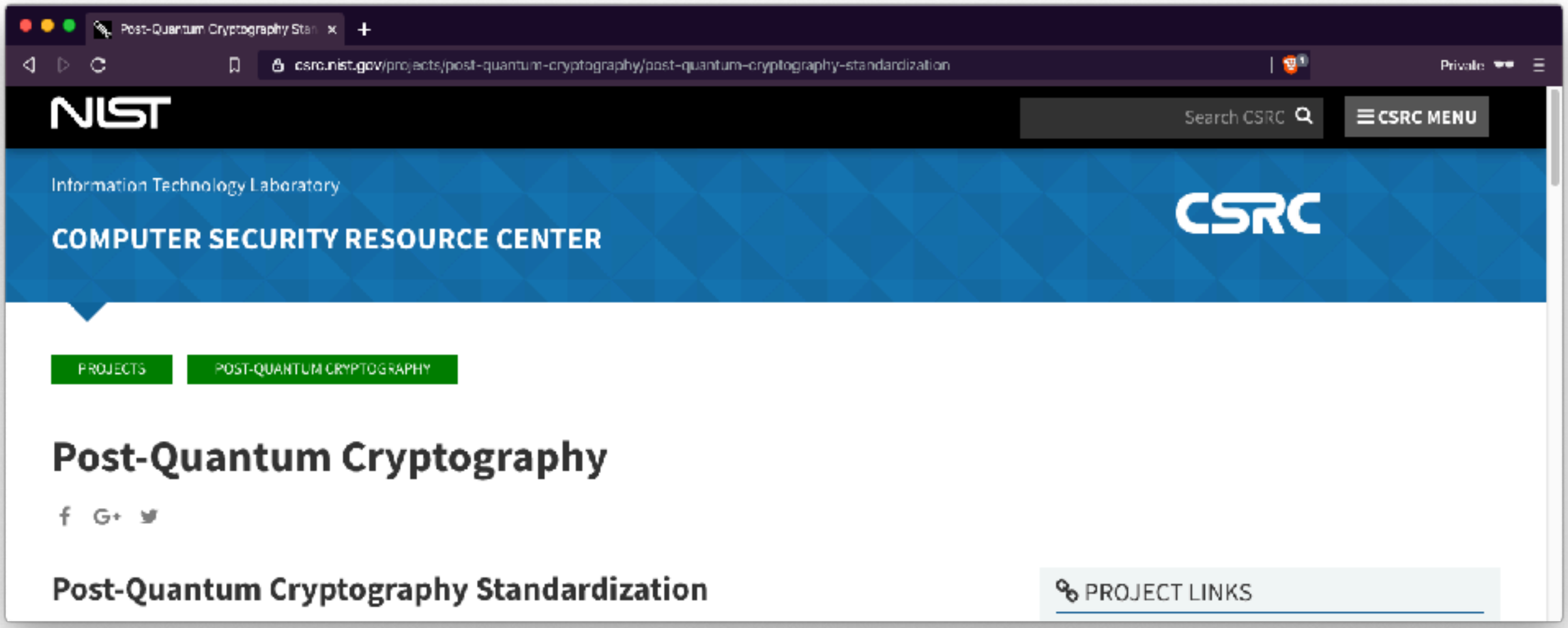


NIST competition



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 $\Longrightarrow$ Digital signature scheme

Fiat Shamir transformation

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

Well-known: Security in the Random Oracle Model

Fiat Shamir transformation

Removes interaction from *identification schemes* using hash functions $\Longrightarrow$ 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 $\Longrightarrow$ 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 $\Longrightarrow$ 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 $\Longrightarrow$ 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 $\Longrightarrow$ 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!*

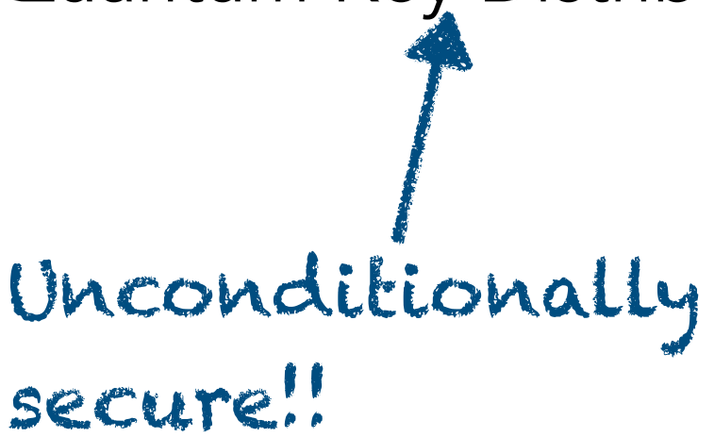
Post-quantum key exchange

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

Alternative: post-quantum secure Key Encapsulation

Post-quantum key exchange

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



Alternative: post-quantum secure Key Encapsulation

+Classical $\Longrightarrow$ more efficient

Post-quantum key exchange

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

Alternative: post-quantum secure Key Encapsulation

+ Classical $\Longrightarrow$ 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"

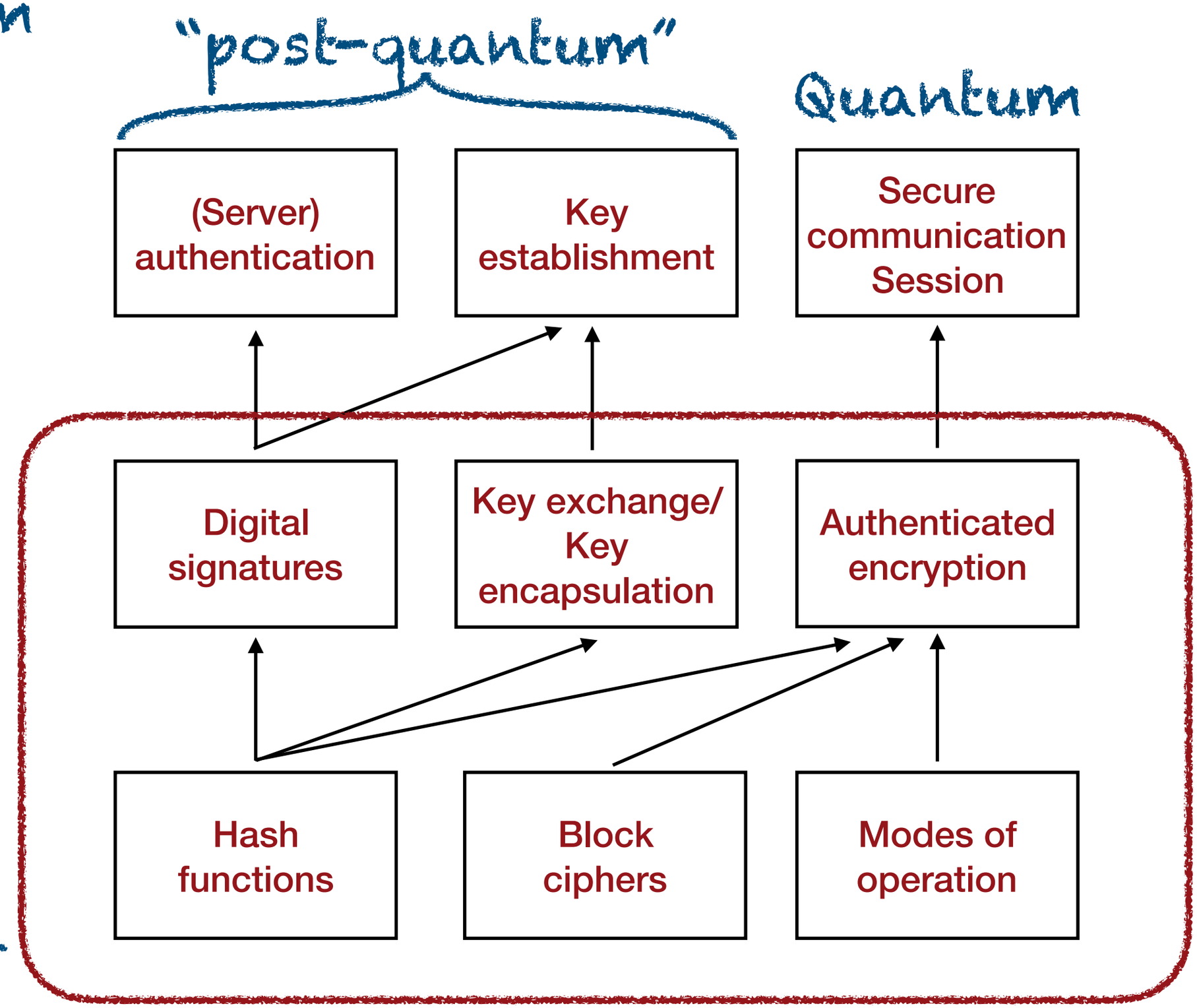
Quantum

Functionalities

Protocols

Cryptographic Ingredients

Quantum-ready?



The TLS protocol

Quantum

"post-quantum"

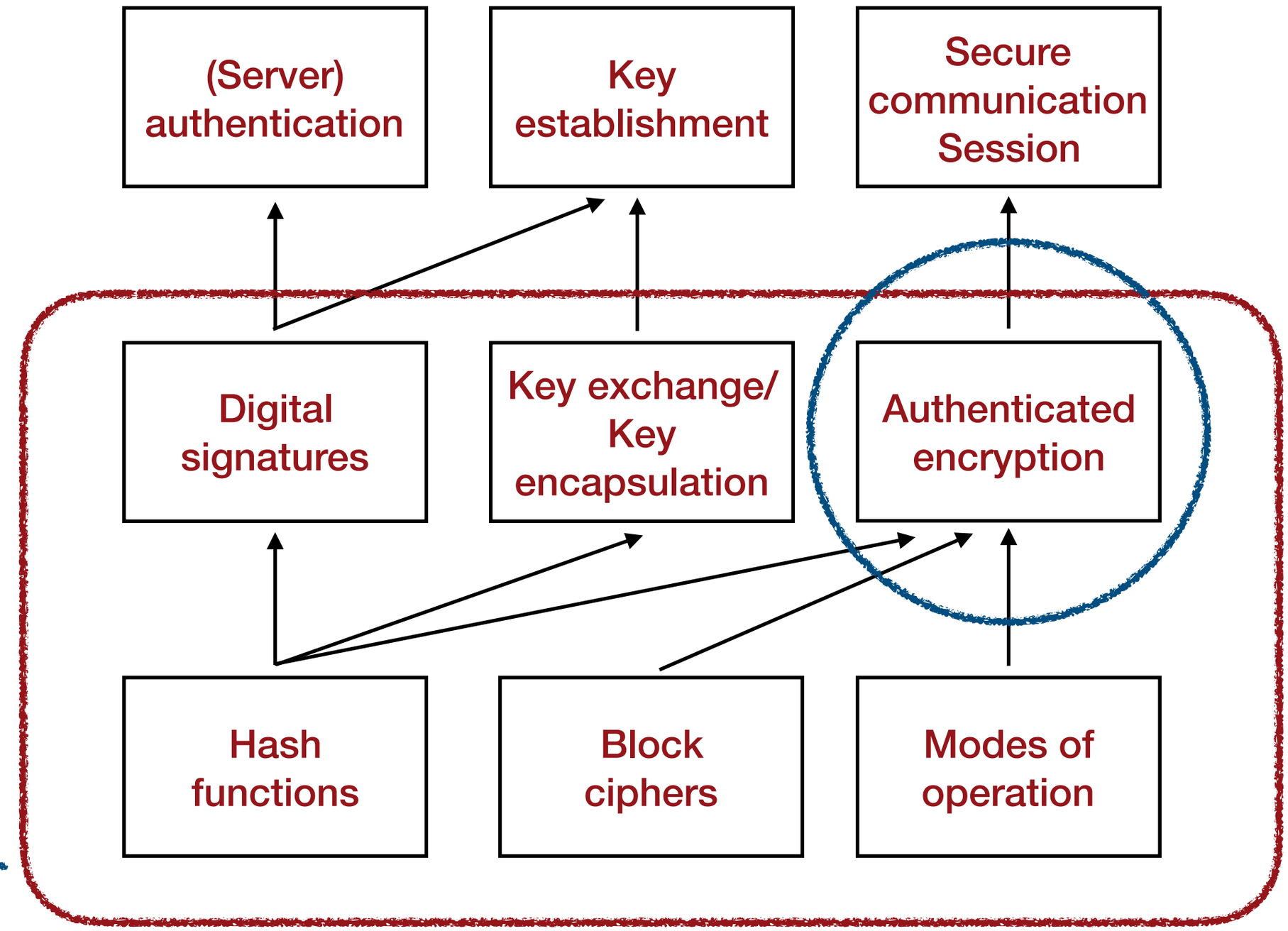
Quantum

Functionalities

Protocols

Cryptographic Ingredients

Quantum-ready?



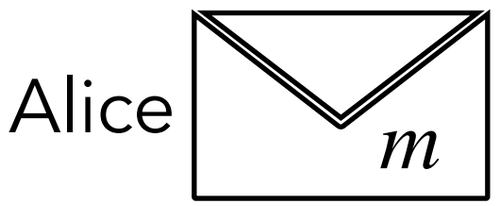
Authenticated Encryption

Authenticated Encryption

Alice

Bob

Authenticated Encryption



Alice

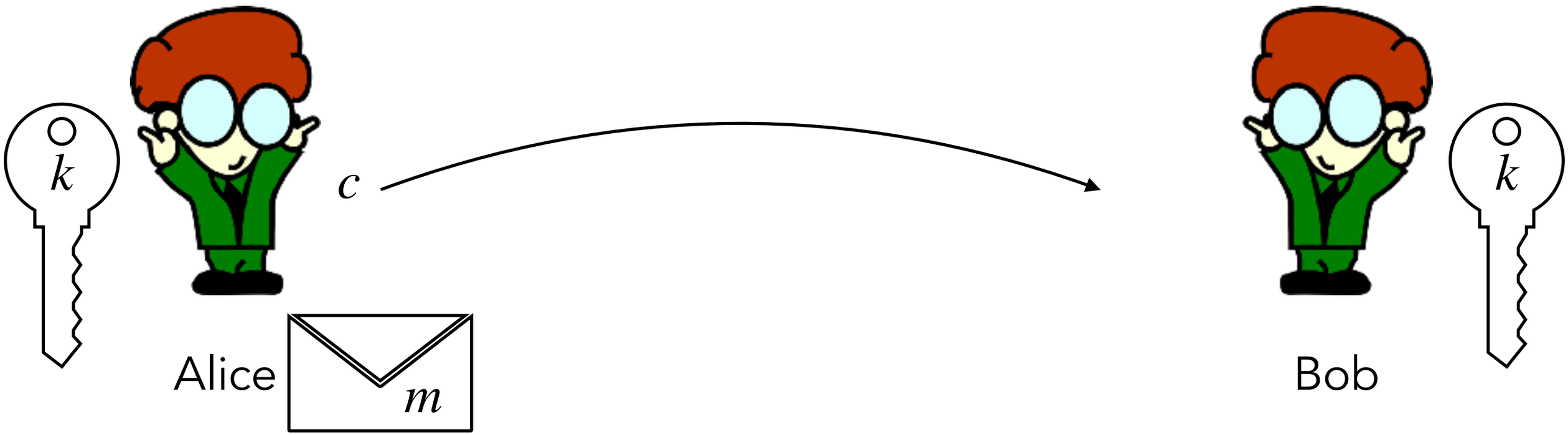
Bob

Authenticated Encryption

Authenticated Encryption

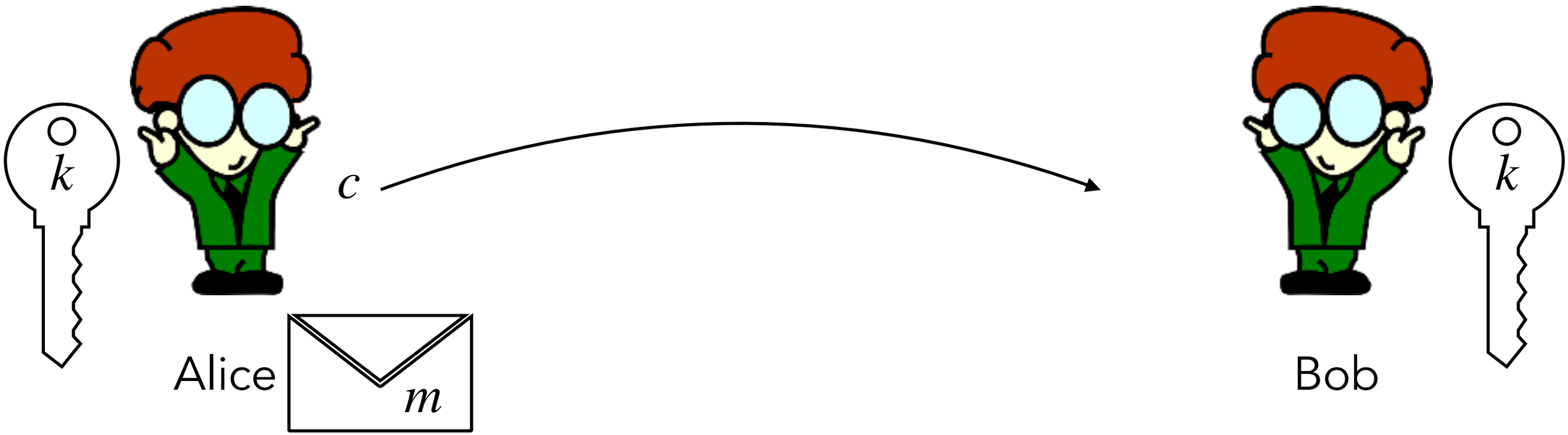
$$c = \mathrm{Enc}_k(m)$$

Authenticated Encryption



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

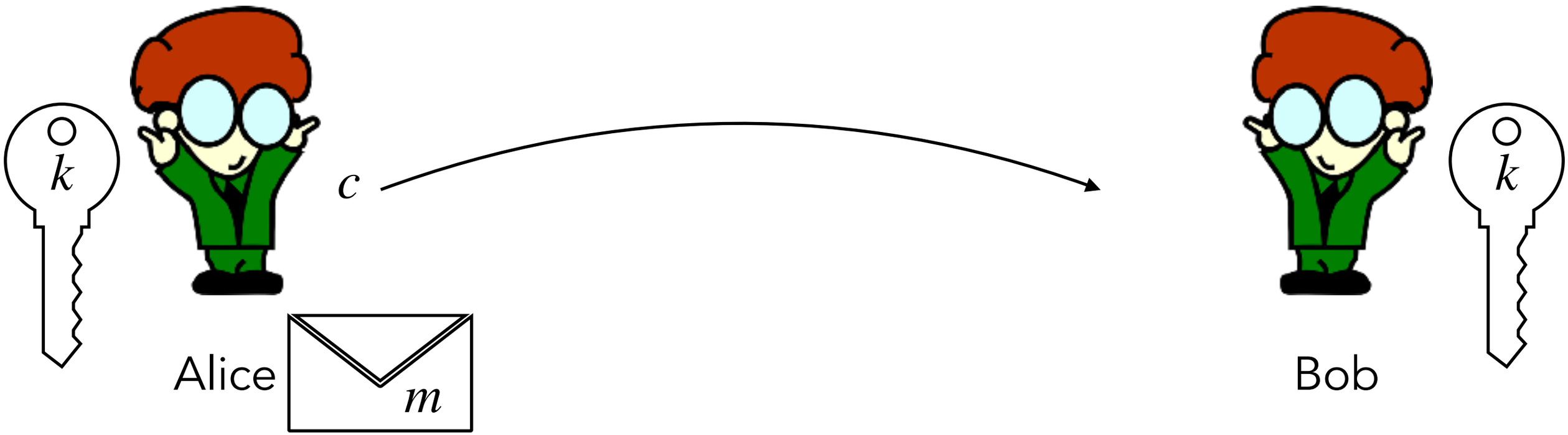
Authenticated Encryption



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

$\mathrm{Dec}_k(c) = m$

Authenticated Encryption

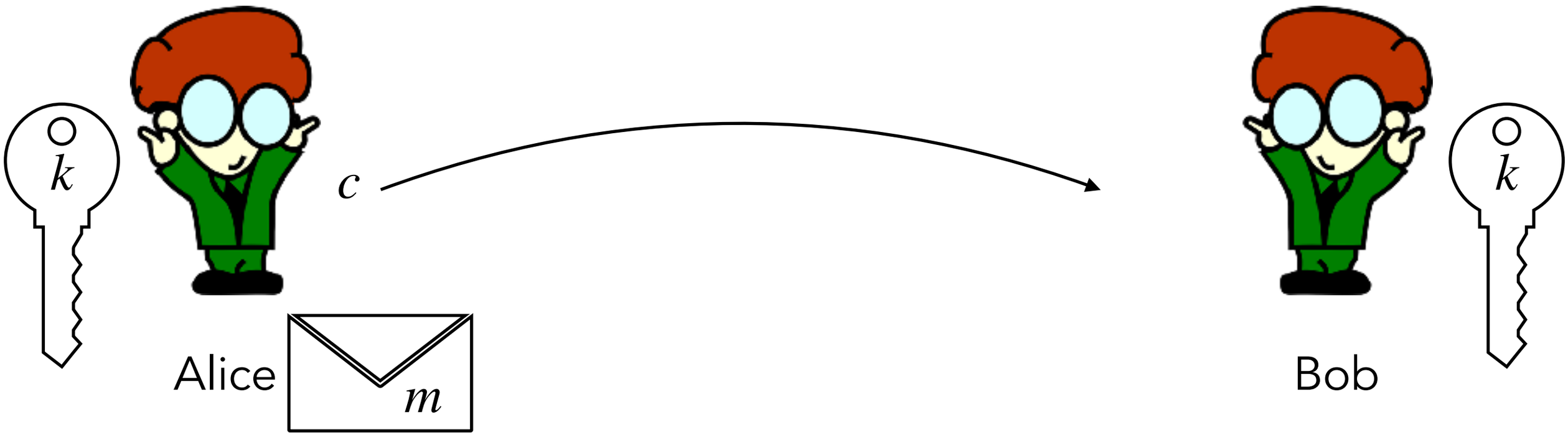


$$c = \mathrm{Enc}_k(m)$$

$$\mathrm{Dec}_k(c) = m$$

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

Authenticated Encryption



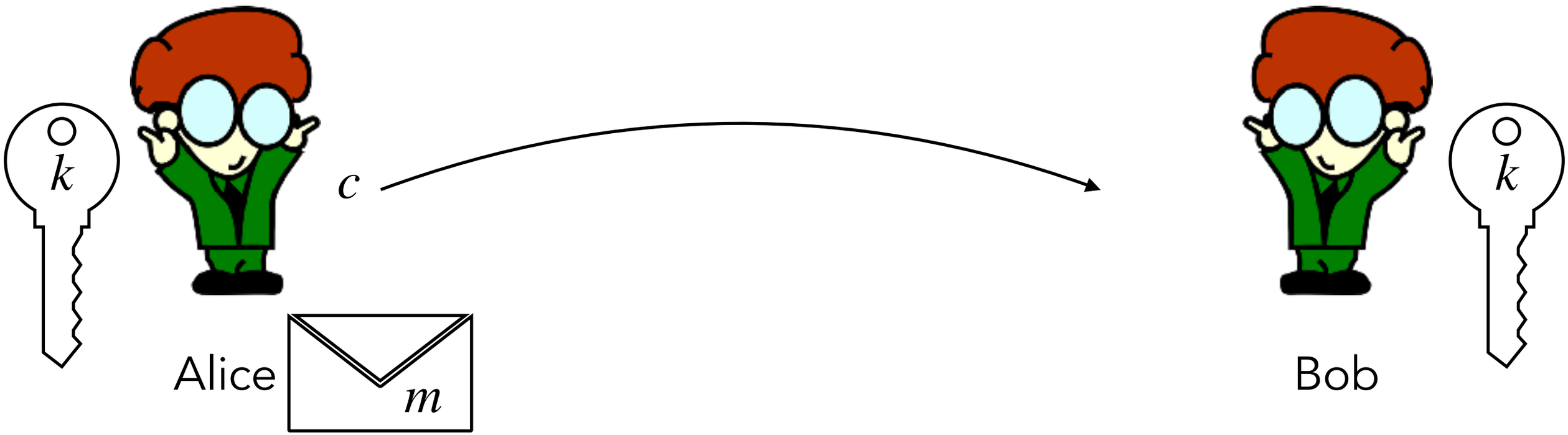
$c = \mathrm{Enc}_k(m)$

$\mathrm{Dec}_k(c) = m$

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

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

Authenticated Encryption



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

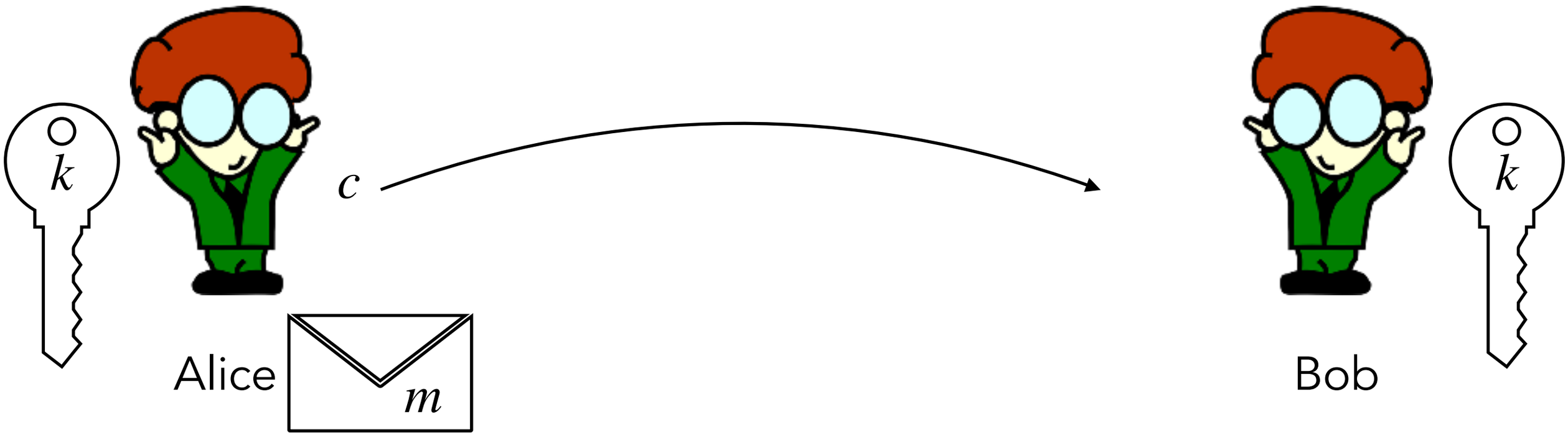
$\mathrm{Dec}_k(c) = m$

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

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

Slightly simplified...

Authenticated Encryption



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

$\mathrm{Dec}_k(c) = m$

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

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

Confidentiality+Integrity=Authenticated encryption

Real vs. Ideal

Alternative characterization (Shrimpton ’04):

Real vs. Ideal

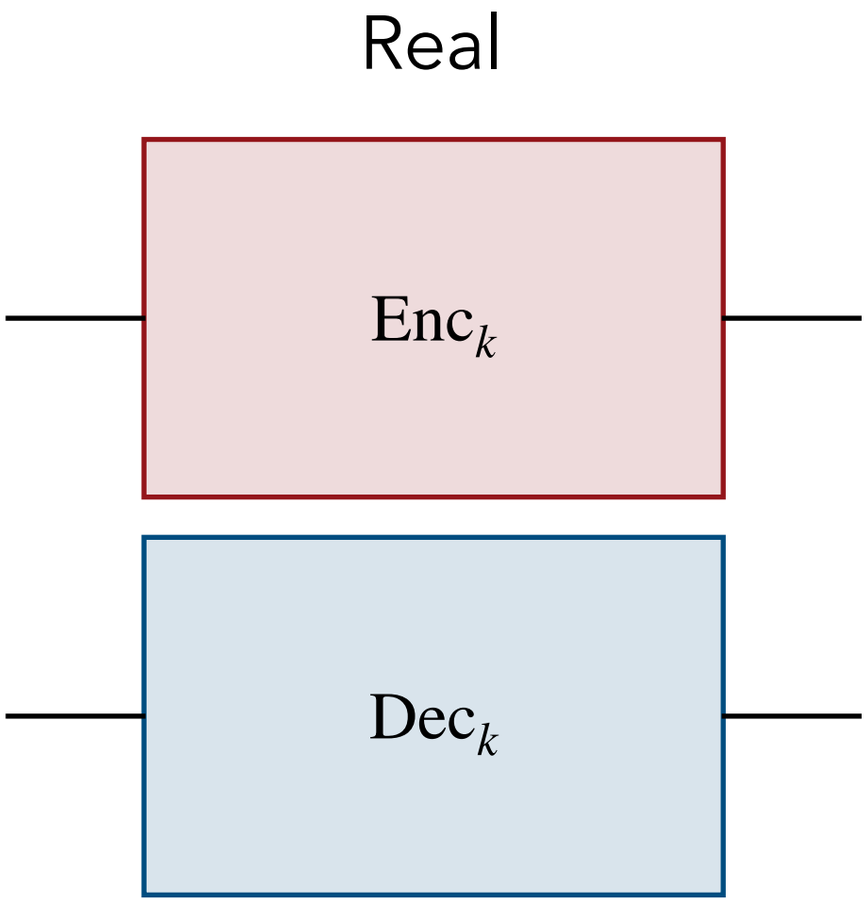
Alternative characterization (Shrimpton ’04):

Real

Ideal

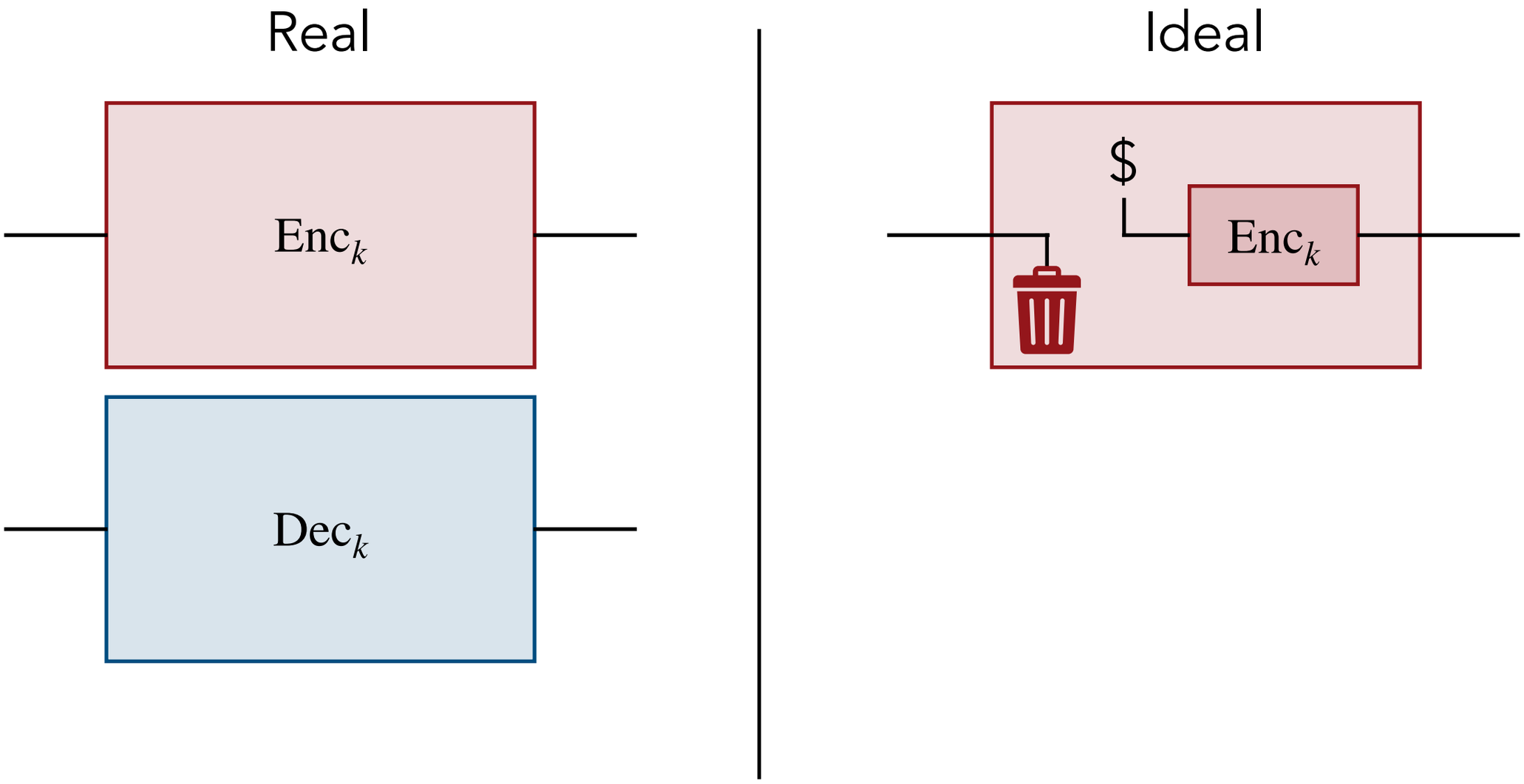
Real vs. Ideal

Alternative characterization (Shrimpton '04):



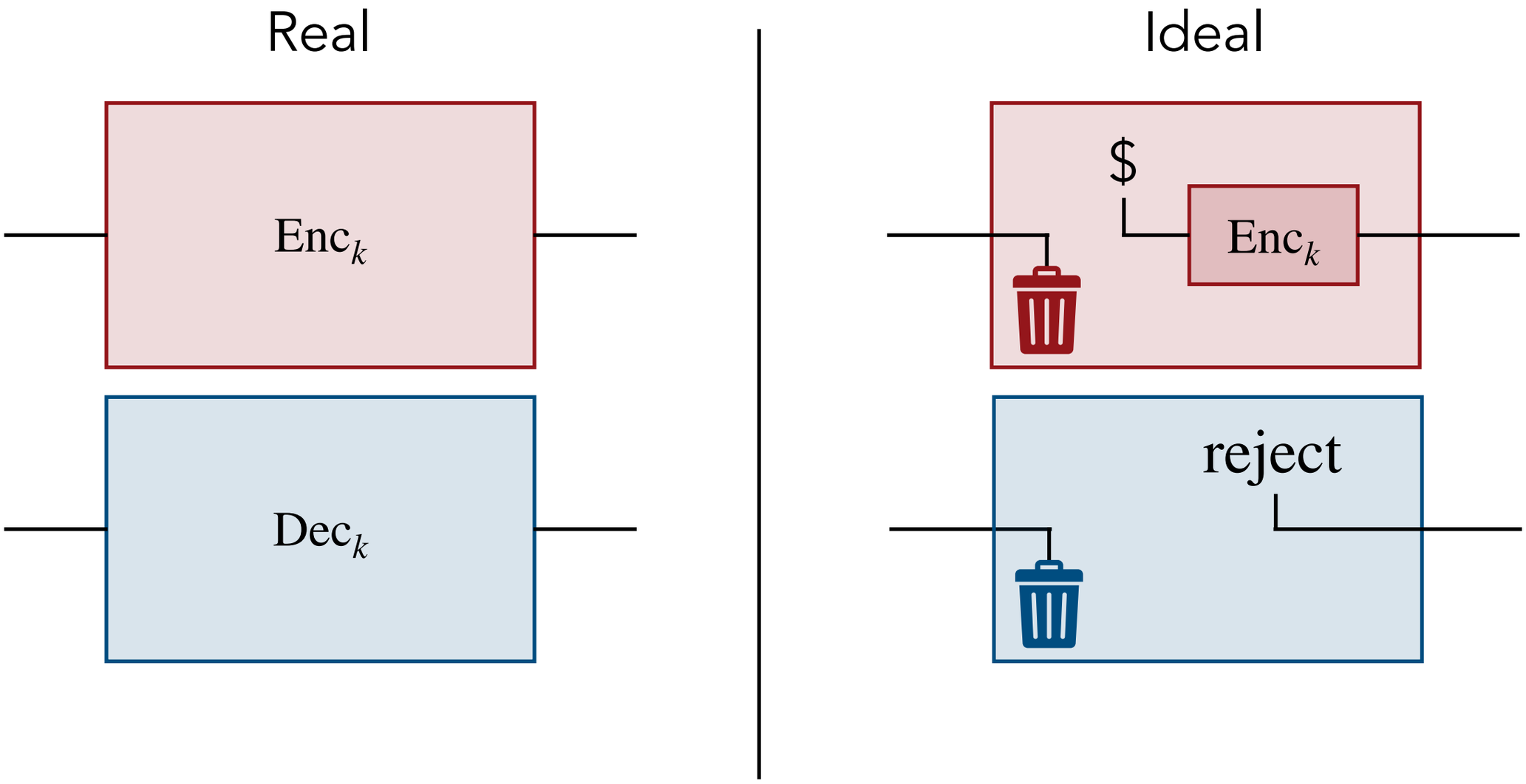
Real vs. Ideal

Alternative characterization (Shrimpton '04):



Real vs. Ideal

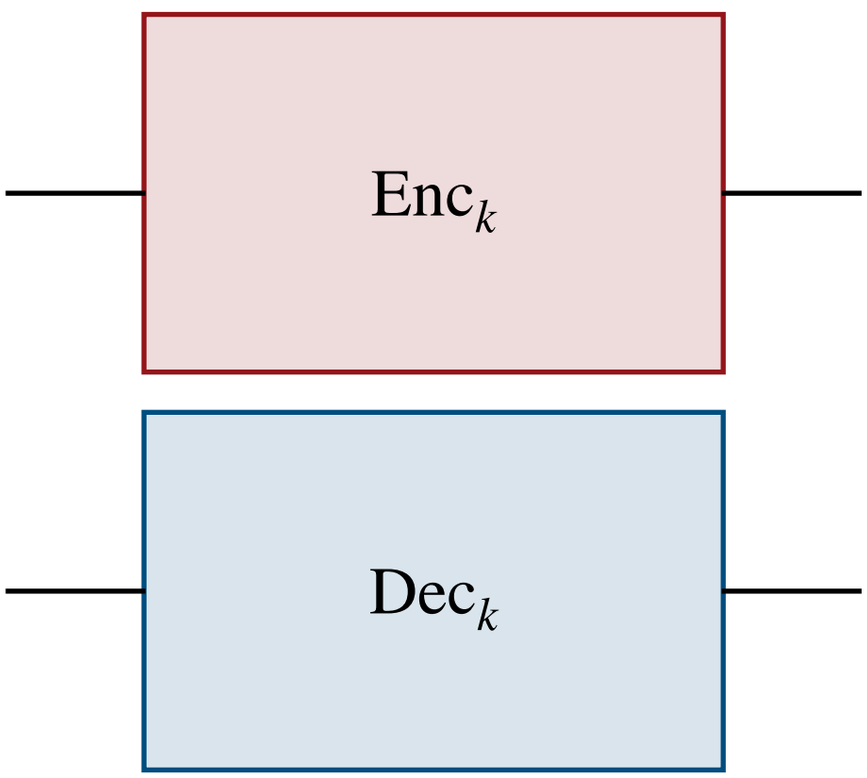
Alternative characterization (Shrimpton '04):



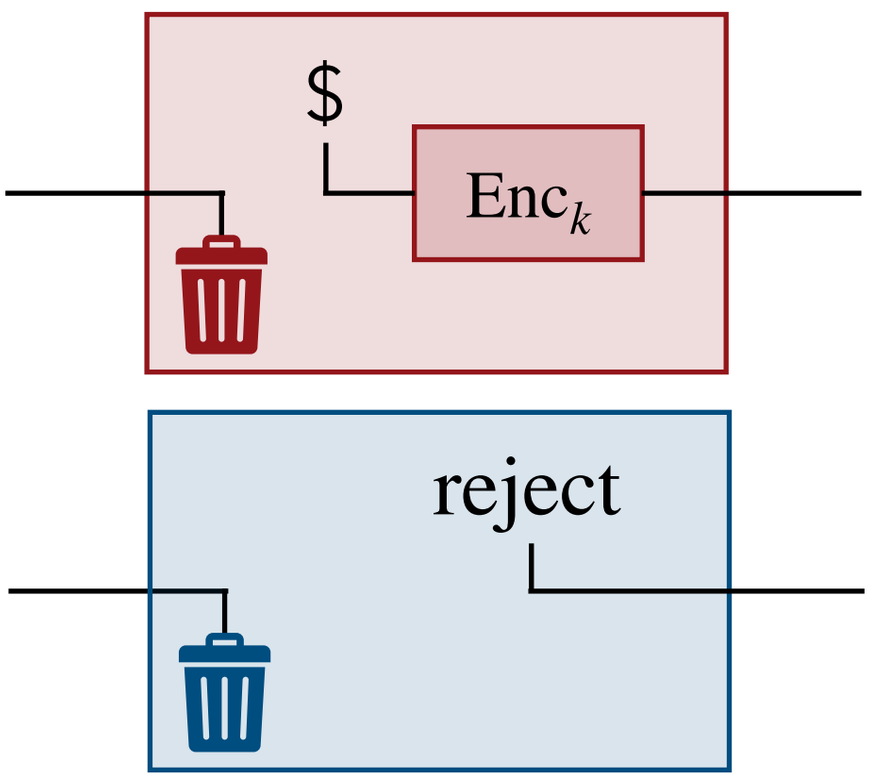
Real vs. Ideal

Alternative characterization (Shrimpton '04):

Real



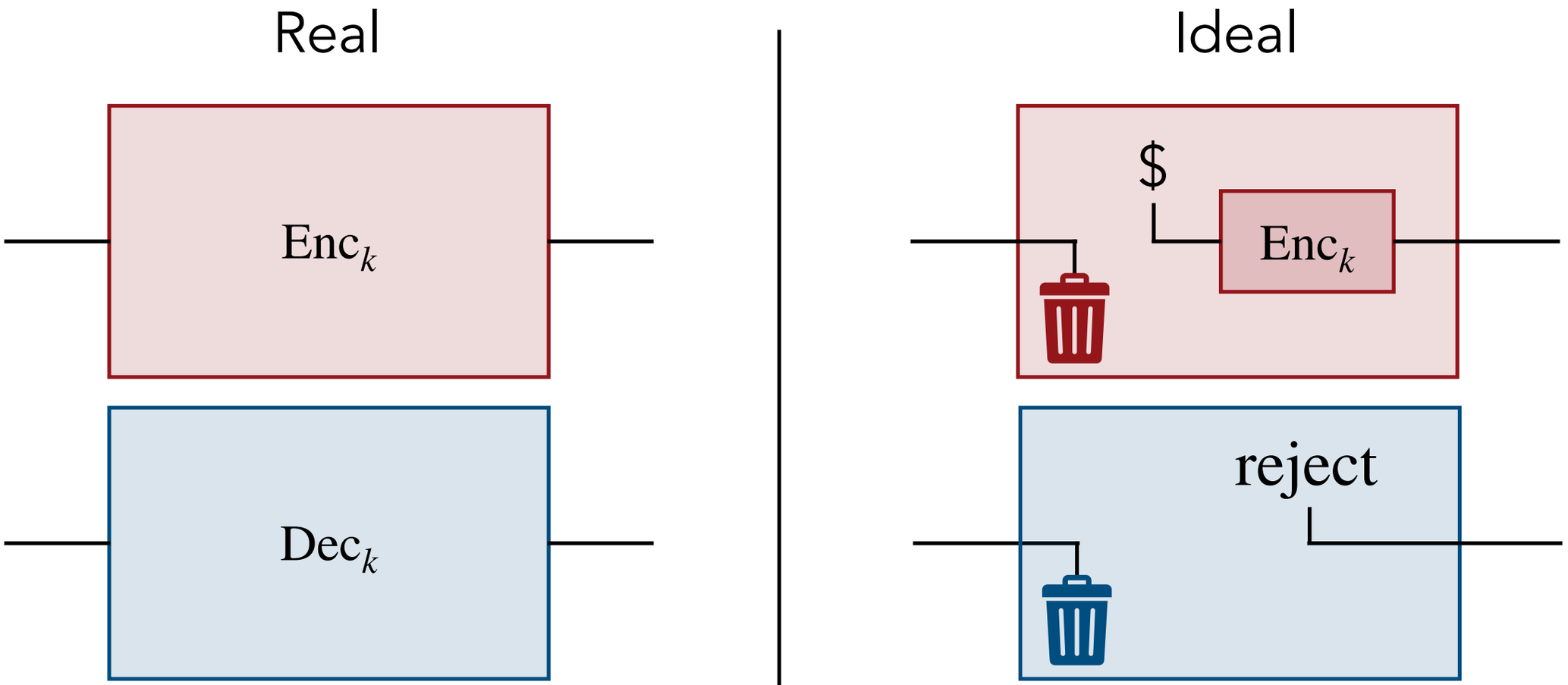
Ideal



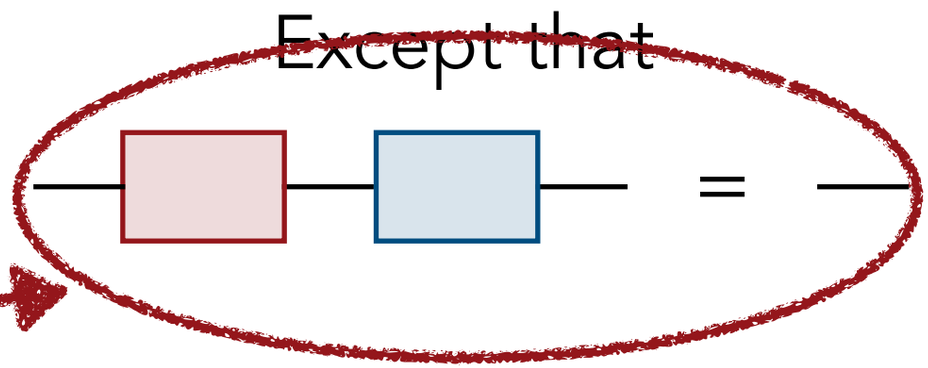
Except that

Real vs. Ideal

Alternative characterization (Shrimpton '04):



Except that



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

Quantum authenticated encryption

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"

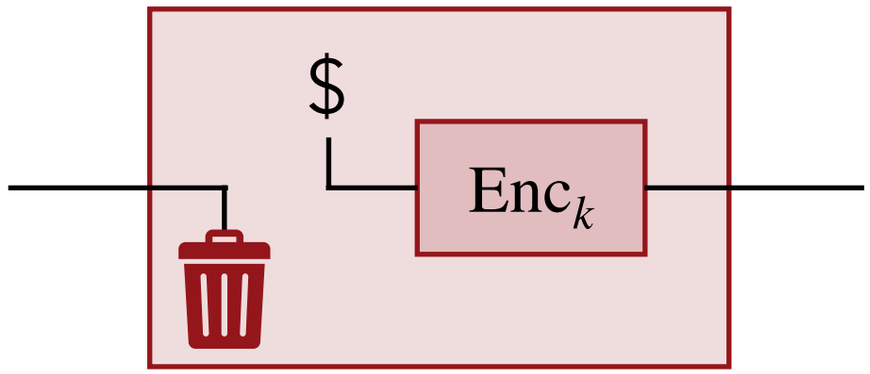
Problem 2: Measurement disturbance

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 purpuse

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 purpuse
  - 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 purpuse
  - 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 purpuse
  - 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 purpuse
  - 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 purpuse
  - 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 purpuse
  - 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 purpuse
  - 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?

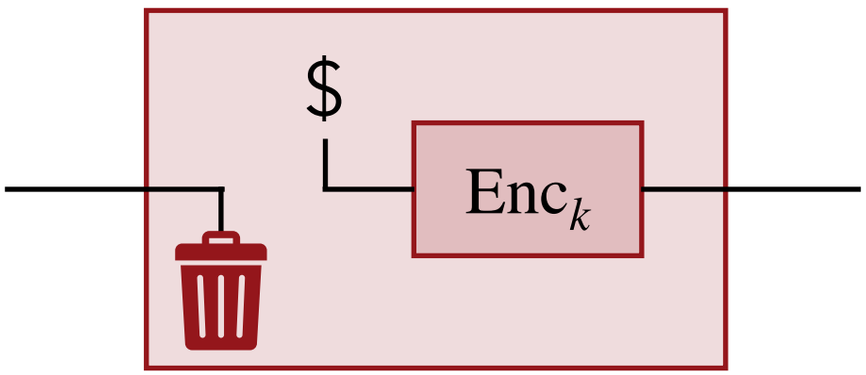
Summary and open problems

- Are we ready for encrypting the quantum internet?

  To some extent:

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