

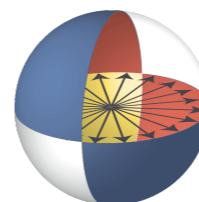
# Unforgeable quantum encryption

Christian Majenz

Joint work with Gorjan Alagic and Tommaso Gagliardoni

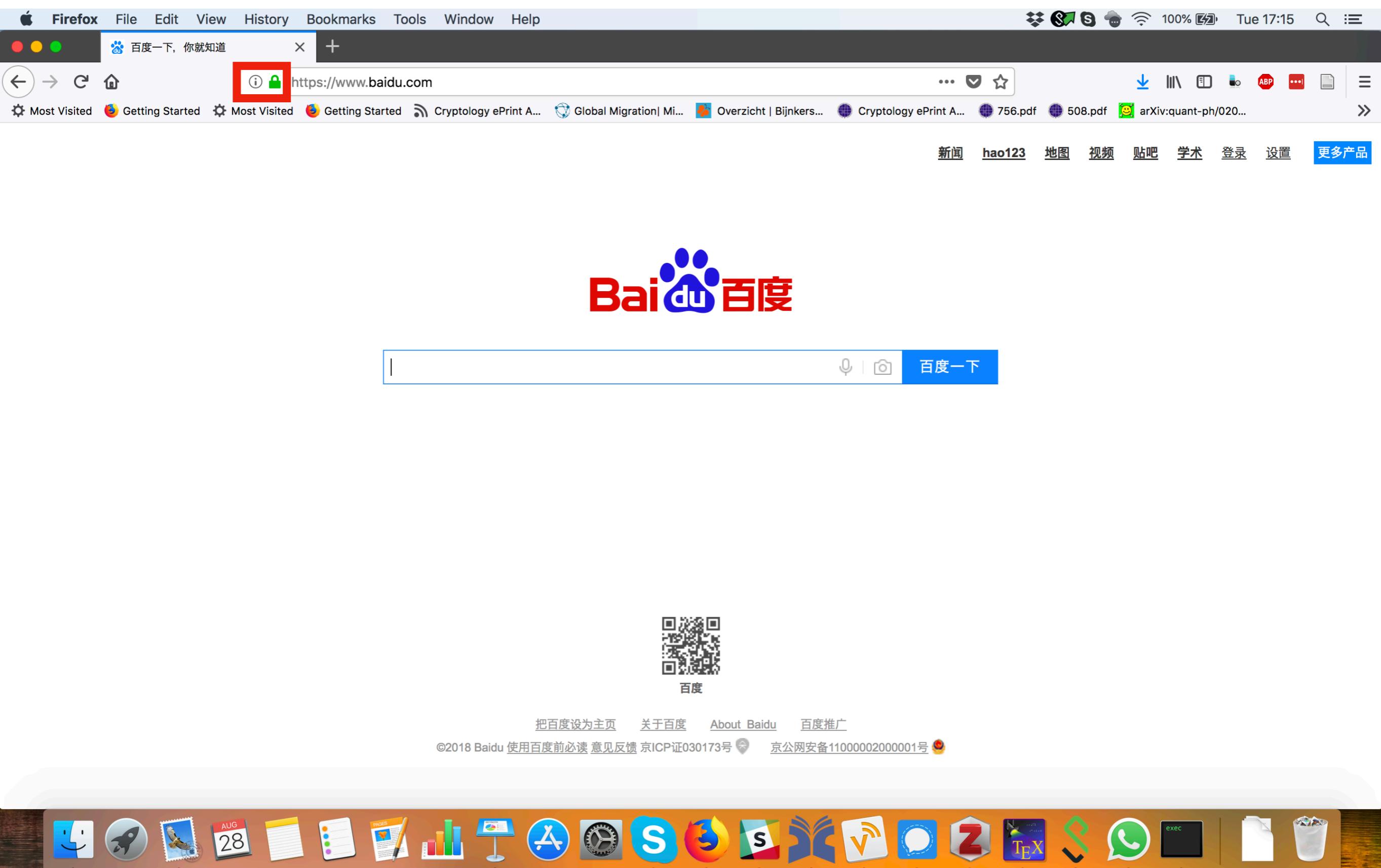


Research Center for Quantum Software



JOINT CENTER FOR  
QUANTUM INFORMATION  
AND COMPUTER SCIENCE

IBM Research | Zurich



Firefox File Edit View History Bookmarks Tools Window Help

百度一下，你就知道

https://www.baidu.com

www.baidu.com  
Secure Connection  
Firefox has blocked parts of this page that are not secure.

Permissions  
You have not granted this site any special permissions.

Baidu 百度

百度一下

把百度设为主页 关于百度 About Baidu 百度推广

©2018 Baidu 使用百度前必读 意见反馈 京ICP证030173号 京公网安备11000002000001号

The image shows a Firefox browser window on a Mac OS X desktop. The title bar says "Firefox". The address bar shows "https://www.baidu.com". A sidebar message from Firefox states: "www.baidu.com Secure Connection Firefox has blocked parts of this page that are not secure." Below this, another message says: "Permissions You have not granted this site any special permissions." A red box highlights the first message. The main content area shows the Baidu logo and a search bar with the placeholder "百度一下". At the bottom, there's a footer with links like "把百度设为主页", "关于百度", "About Baidu", and "百度推广". Copyright information for 2018 Baidu is also present. The bottom of the screen features the Mac OS X Dock with icons for various applications like Mail, Calendar, and Finder.

Firefox File Edit View History Bookmarks Tools Window Help

百度一下，你就知道

https://www.baidu.com

Site Security

www.baidu.com  
Secure Connection

Verified by: GlobalSign nv-sa

Firefox has blocked parts of this page that are not secure. [Learn More](#)

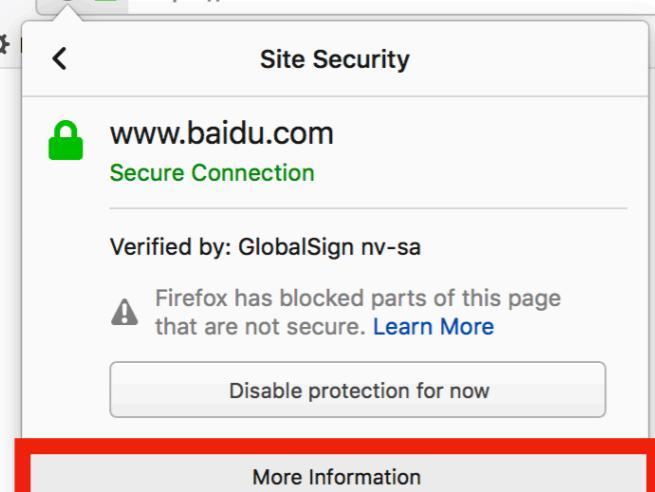
Disable protection for now

More Information

Baidu 百度

新闻 hao123 地图 视频 贴吧 学术 登录 设置 更多产品

百度一下



百度

[把百度设为主页](#) [关于百度](#) [About Baidu](#) [百度推广](#)

©2018 Baidu 使用百度前必读 意见反馈 京ICP证030173号 京公网安备11000002000001号



### Website Identity

Website: [www.baidu.com](https://www.baidu.com/)  
Owner: This website does not supply ownership information.  
Verified by: GlobalSign nv-sa  
Expires on: 26 May 2019

[View Certificate](#)

### Privacy & History

Have I visited this website prior to today?

No

Is this website storing information on my computer?

Yes, cookies

[Clear Cookies and Site Data](#)

Have I saved any passwords for this website?

No

[View Saved Passwords](#)

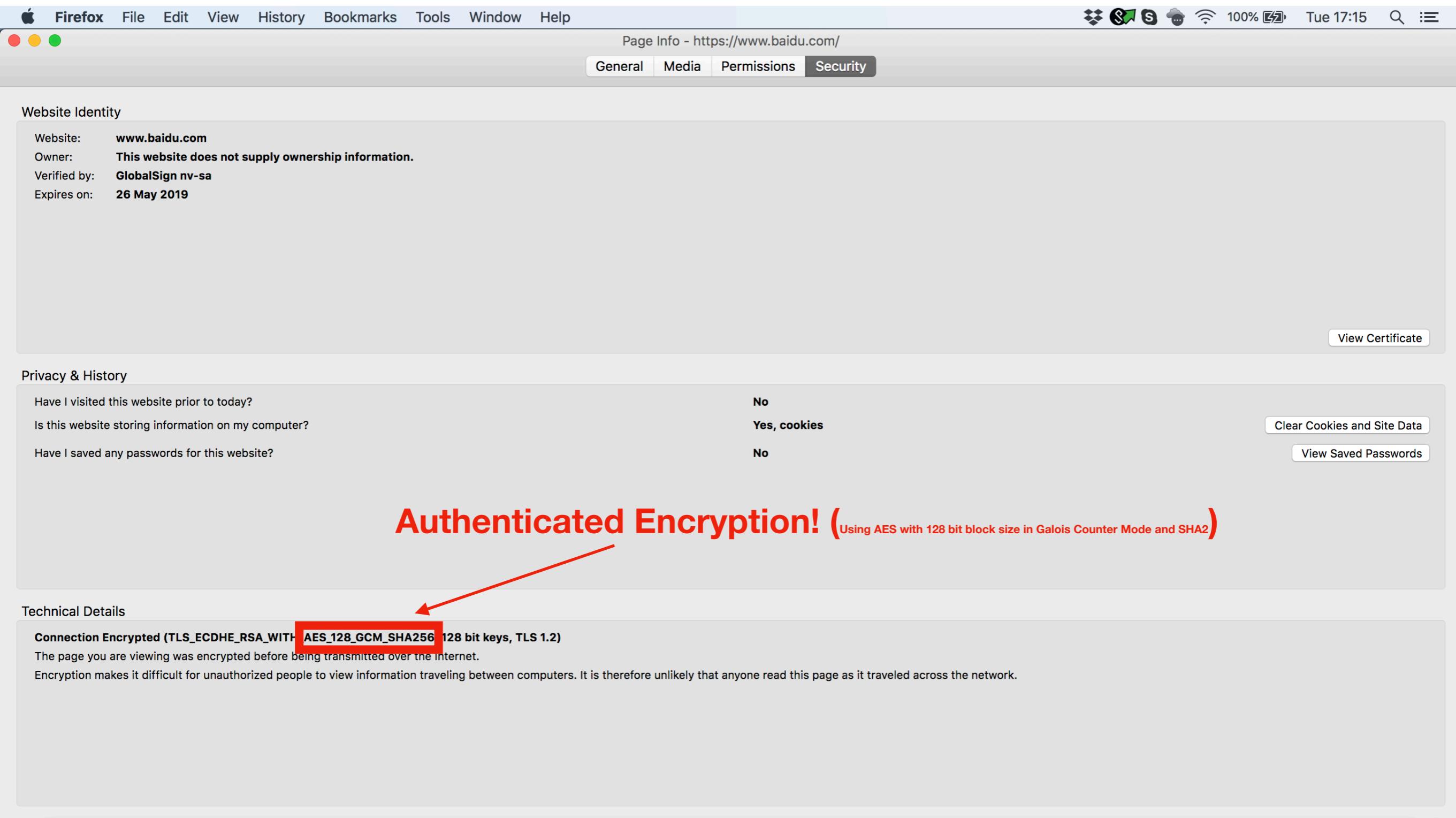
### Technical Details

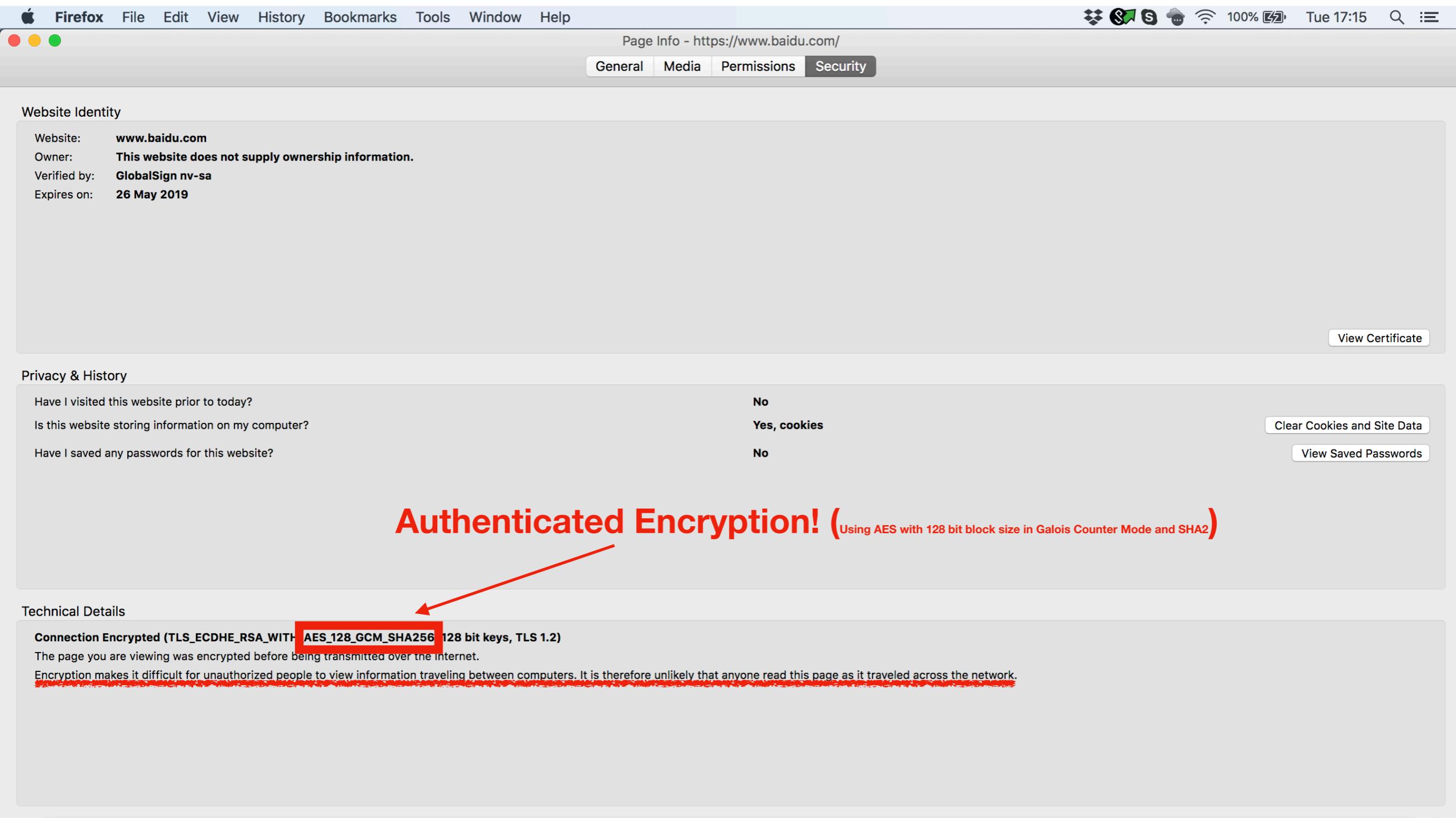
**Connection Encrypted (TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256, 128 bit keys, TLS 1.2)**

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.







# **Taxonomy of security**

# Taxonomy of security

secrecy

# Taxonomy of security

authenticity,  
Integrity

secrecy

# Taxonomy of security

authenticity,  
Integrity

secrecy

Indistinguishability of ciphertexts  
under chosen plaintext attacks  
(IND-CPA)

# Taxonomy of security

authenticity,  
Integrity

secrecy

Indistinguishability of ciphertexts  
under nonadaptive chosen ciphertext attacks  
(IND-CCA1)

→ = implication

↓  
Indistinguishability of ciphertexts  
under chosen plaintext attacks  
(IND-CPA)

# Taxonomy of security

authenticity,  
Integrity

secrecy

Indistinguishability of ciphertexts  
under adaptive chosen ciphertext attacks  
(IND-CCA2)



Indistinguishability of ciphertexts  
under nonadaptive chosen ciphertext attacks  
(IND-CCA1)



Indistinguishability of ciphertexts  
under chosen plaintext attacks  
(IND-CPA)

→ = implication

# Taxonomy of security

authenticity,  
Integrity

secrecy

Integrity of ciphertexts  
(INT-CTXT)  
( $\approx$  EUF-CMA for encryption  
schemes)

Indistinguishability of ciphertexts  
under adaptive chosen ciphertext attacks  
(IND-CCA2)



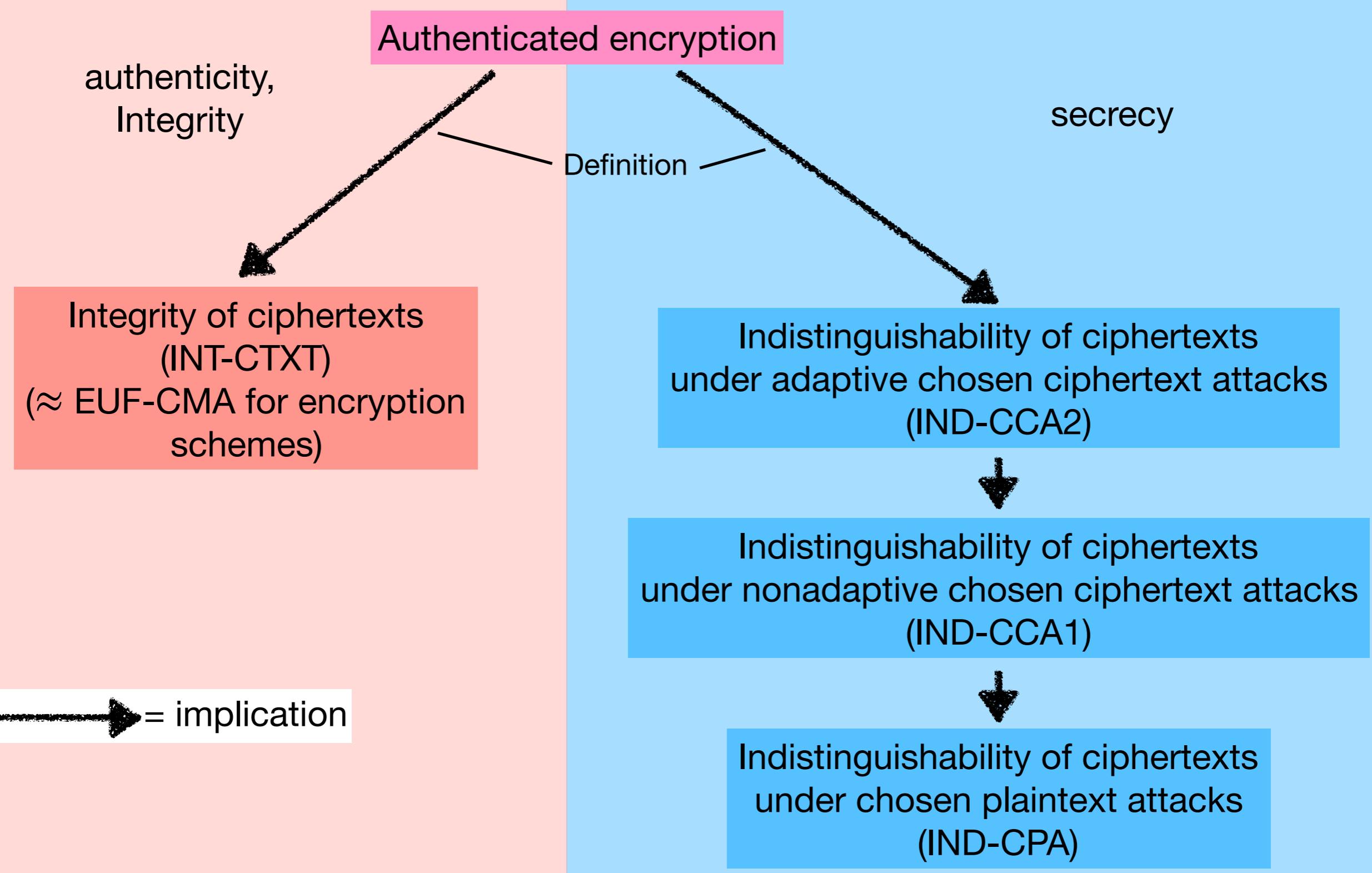
Indistinguishability of ciphertexts  
under nonadaptive chosen ciphertext attacks  
(IND-CCA1)



Indistinguishability of ciphertexts  
under chosen plaintext attacks  
(IND-CPA)

→ = implication

# Taxonomy of security



# Taxonomy of security

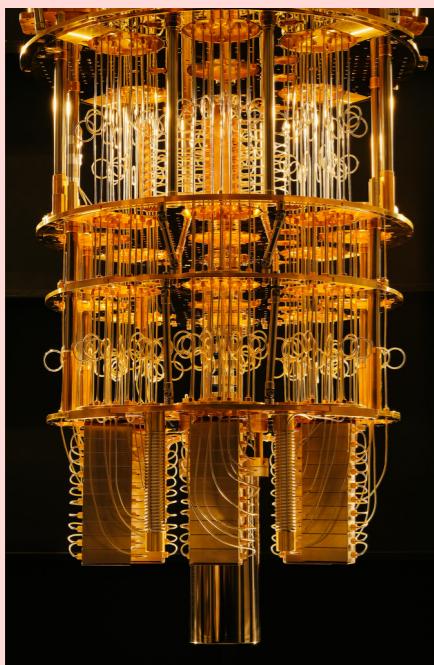
authenticity,  
Integrity

Authenticated encryption

secrecy

Integrity of ciphertexts  
(INT-CTXT)  
( $\approx$  EUF-CMA for encryption  
schemes)

Indistinguishability of ciphertexts  
under adaptive chosen ciphertext attacks  
(IND-CCA2)



Broadbent and Jeffery, Crypto 2015  
Alagic et al., ICITS 2016

Indistinguishability of ciphertexts  
under nonadaptive chosen ciphertext attacks  
(IND-CCA1)

Indistinguishability of ciphertexts  
under chosen plaintext attacks  
(IND-CPA)

# Taxonomy of security

authenticity,  
Integrity

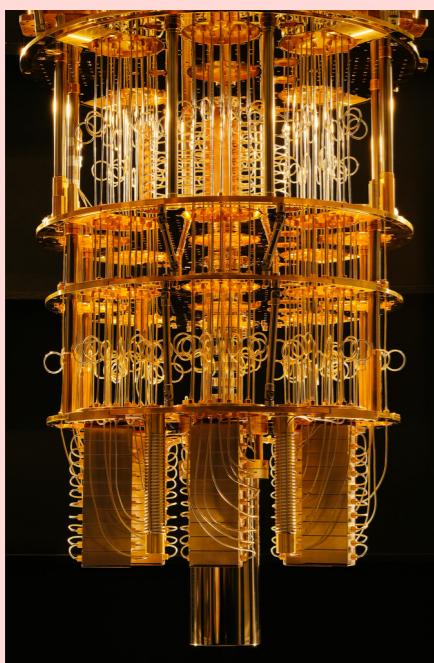
Authenticated encryption

secrecy

No quantum version!!!  
Why not, what is the difficulty?

Integrity of ciphertexts  
(INT-CTXT)  
( $\approx$  EUF-CMA for encryption  
schemes)

Indistinguishability of ciphertexts  
under adaptive chosen ciphertext attacks  
(IND-CCA2)



Indistinguishability of ciphertexts  
under nonadaptive chosen ciphertext attacks  
(IND-CCA1)

Broadbent and Jeffery, Crypto 2015  
Alagic et al., ICITS 2016

Indistinguishability of ciphertexts  
under chosen plaintext attacks  
(IND-CPA)

# Integrity of ciphertexts

An encryption scheme  $(\text{KeyGen}, \text{Enc}, \text{Dec})$  has integrity of ciphertexts, if no successfull ciphertext-forging adversary exists:

# Integrity of ciphertexts

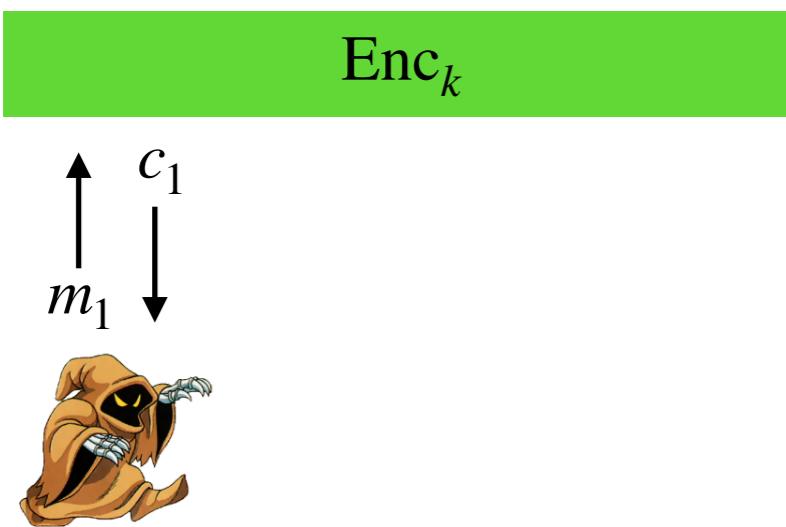
An encryption scheme  $(\text{KeyGen}, \text{Enc}, \text{Dec})$  has integrity of ciphertexts, if no successfull ciphertext-forging adversary exists:

$\text{Enc}_k$



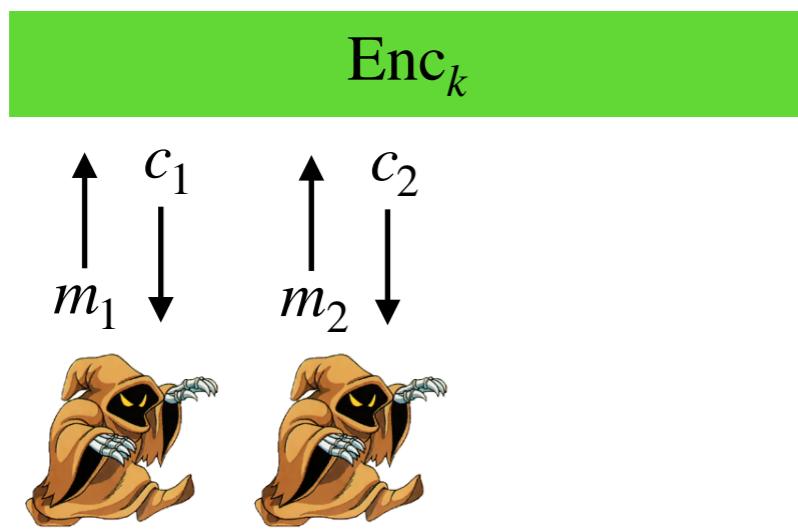
# Integrity of ciphertexts

An encryption scheme  $(\text{KeyGen}, \text{Enc}, \text{Dec})$  has integrity of ciphertexts, if no successfull ciphertext-forging adversary exists:



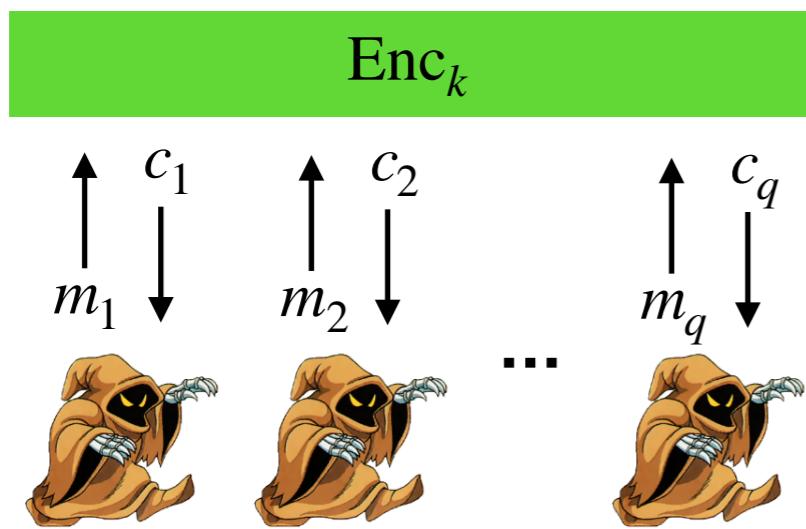
# Integrity of ciphertexts

An encryption scheme  $(\text{KeyGen}, \text{Enc}, \text{Dec})$  has integrity of ciphertexts, if no successfull ciphertext-forging adversary exists:



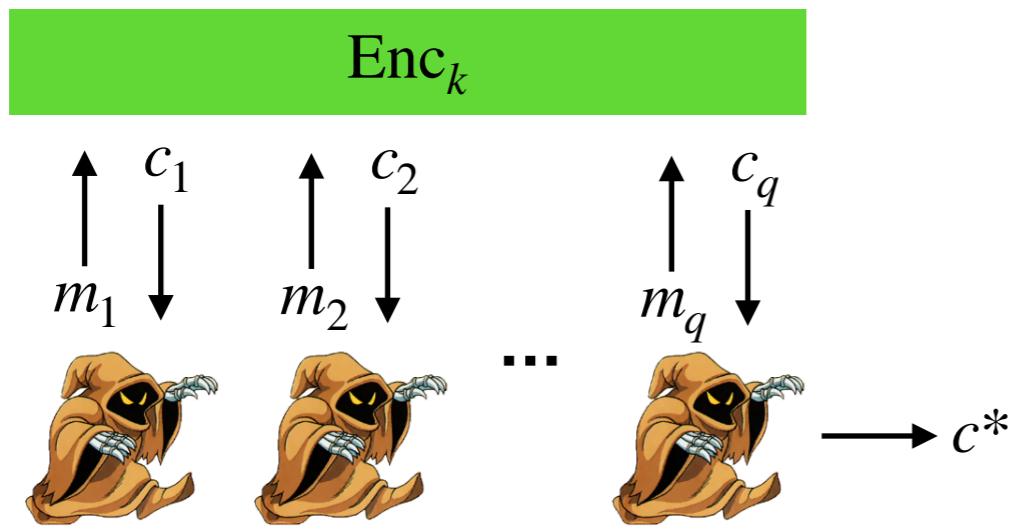
# Integrity of ciphertexts

An encryption scheme  $(\text{KeyGen}, \text{Enc}, \text{Dec})$  has integrity of ciphertexts, if no successfull ciphertext-forging adversary exists:



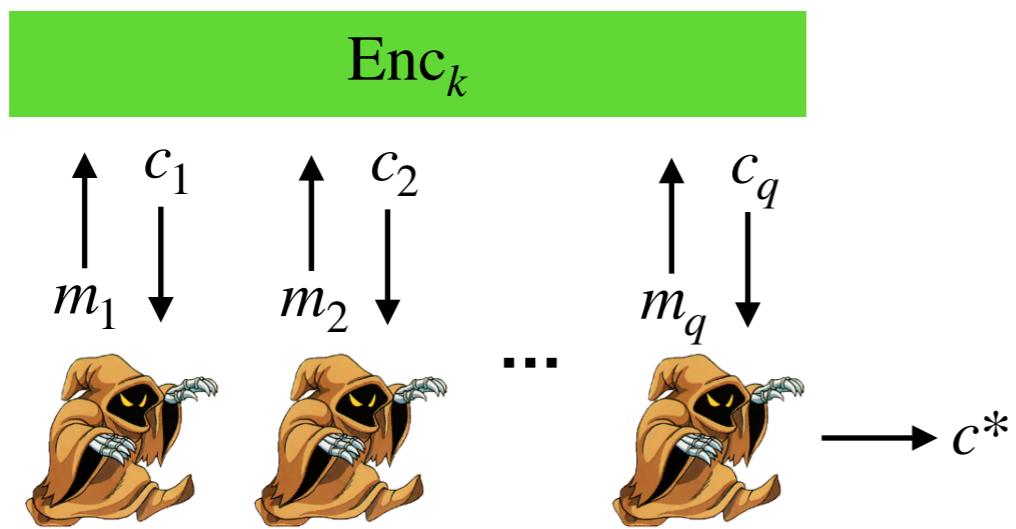
# Integrity of ciphertexts

An encryption scheme  $(\text{KeyGen}, \text{Enc}, \text{Dec})$  has integrity of ciphertexts, if no successfull ciphertext-forging adversary exists:



# Integrity of ciphertexts

An encryption scheme  $(\text{KeyGen}, \text{Enc}, \text{Dec})$  has integrity of ciphertexts, if no successfull ciphertext-forging adversary exists:

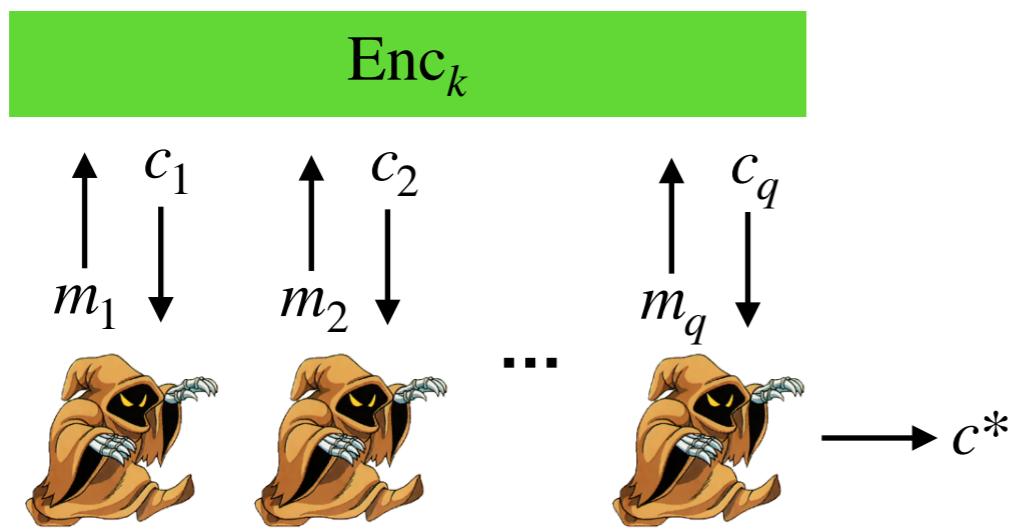


**Success:**

- i)  $c^* \neq c_i$  for all  $i = 1, \dots, q$
- ii)  $\text{Dec}_k(c^*) \neq \perp$

# Integrity of ciphertexts

An encryption scheme  $(\text{KeyGen}, \text{Enc}, \text{Dec})$  has integrity of ciphertexts, if no successfull ciphertext-forging adversary exists:



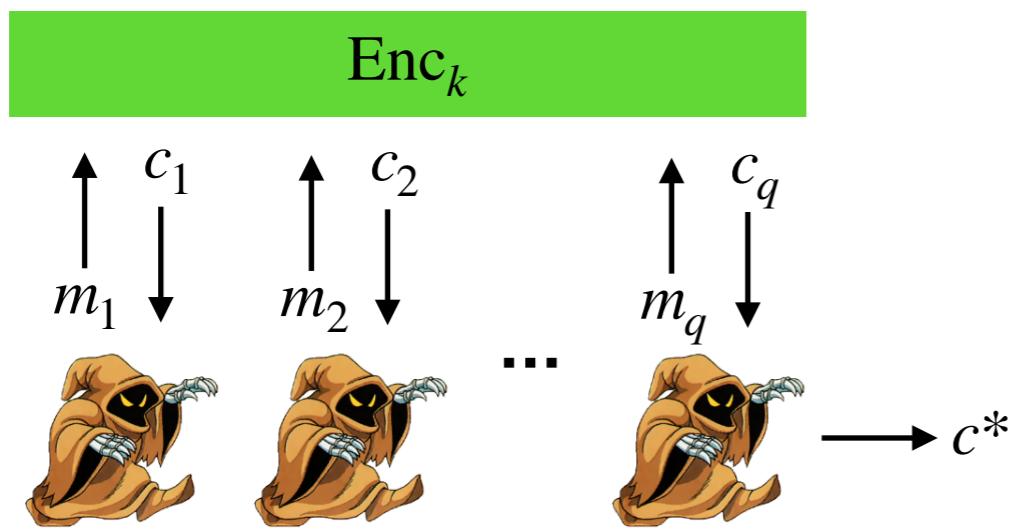
**Success:**

- i)  $c^* \neq c_i$  for all  $i = 1, \dots, q$
- ii)  $\text{Dec}_k(c^*) \neq \perp$

What about encryption of quantum data?

# Quantum integrity of ciphertexts (attempt)

An encryption scheme  $(\text{KeyGen}, \text{Enc}, \text{Dec})$  has integrity of ciphertexts, if no successfull ciphertext-forging adversary exists:



Success:

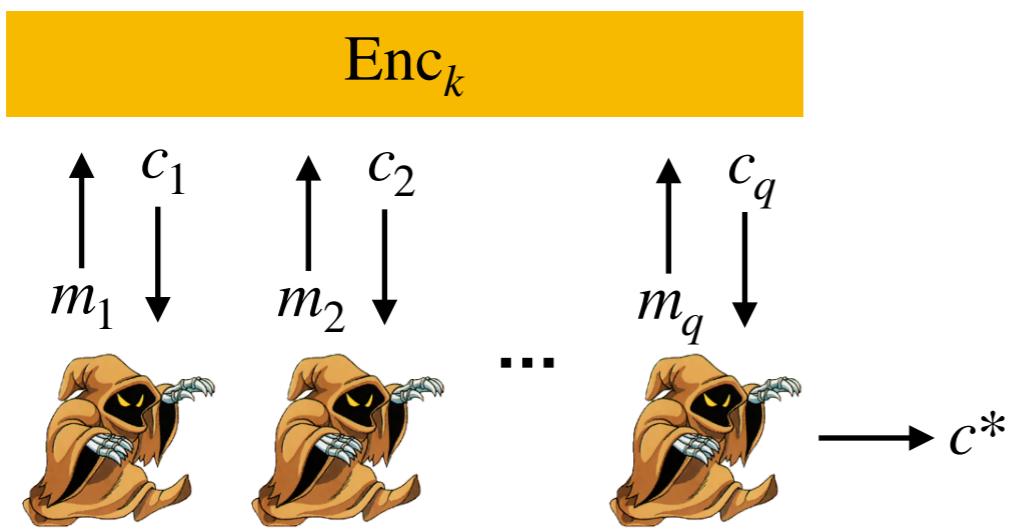
- i)  $c^* \neq c_i$  for all  $i = 1, \dots, q$
- ii)  $\text{Dec}_k(c^*) \neq \perp$

What about encryption of quantum data?

# Quantum integrity of ciphertexts (attempt)

Quantum

An encryption scheme  $(\text{KeyGen}, \text{Enc}, \text{Dec})$  has integrity of ciphertexts, if no successfull ciphertext-forging adversary exists:



Success:

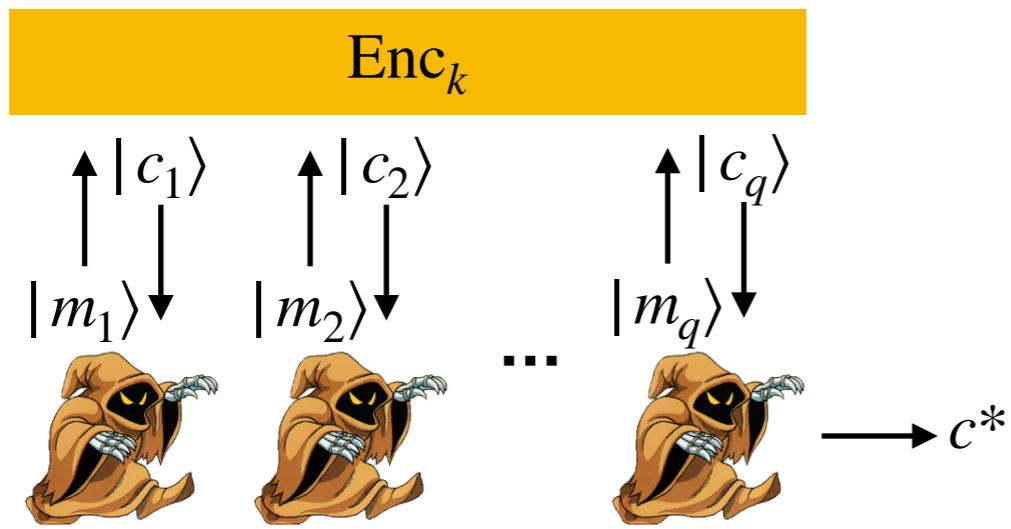
- i)  $c^* \neq c_i$  for all  $i = 1, \dots, q$
- ii)  $\text{Dec}_k(c^*) \neq \perp$

What about encryption of quantum data?

# Quantum integrity of ciphertexts (attempt)

Quantum

An encryption scheme  $(\text{KeyGen}, \text{Enc}, \text{Dec})$  has integrity of ciphertexts, if no successfull ciphertext-forging adversary exists:



Success:

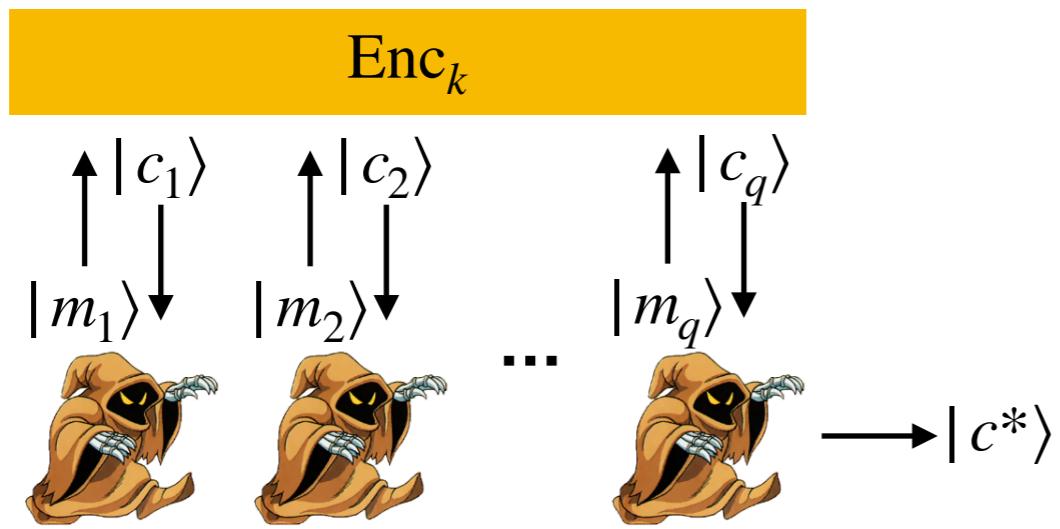
- i)  $c^* \neq c_i$  for all  $i = 1, \dots, q$
- ii)  $\text{Dec}_k(c^*) \neq \perp$

What about encryption of quantum data?

# Quantum integrity of ciphertexts (attempt)

Quantum

An encryption scheme  $(\text{KeyGen}, \text{Enc}, \text{Dec})$  has integrity of ciphertexts, if no successfull ciphertext-forging adversary exists:



Success:

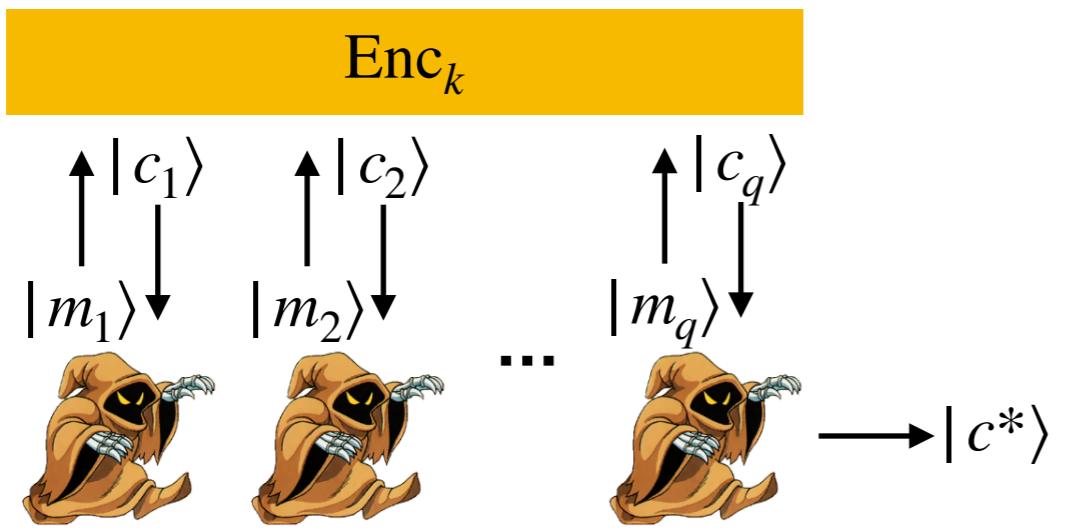
- i)  $c^* \neq c_i$  for all  $i = 1, \dots, q$
- ii)  $\text{Dec}_k(c^*) \neq \perp$

What about encryption of quantum data?

# Quantum integrity of ciphertexts (attempt)

Quantum

An encryption scheme  $(\text{KeyGen}, \text{Enc}, \text{Dec})$  has integrity of ciphertexts, if no successfull ciphertext-forging adversary exists:



Success:

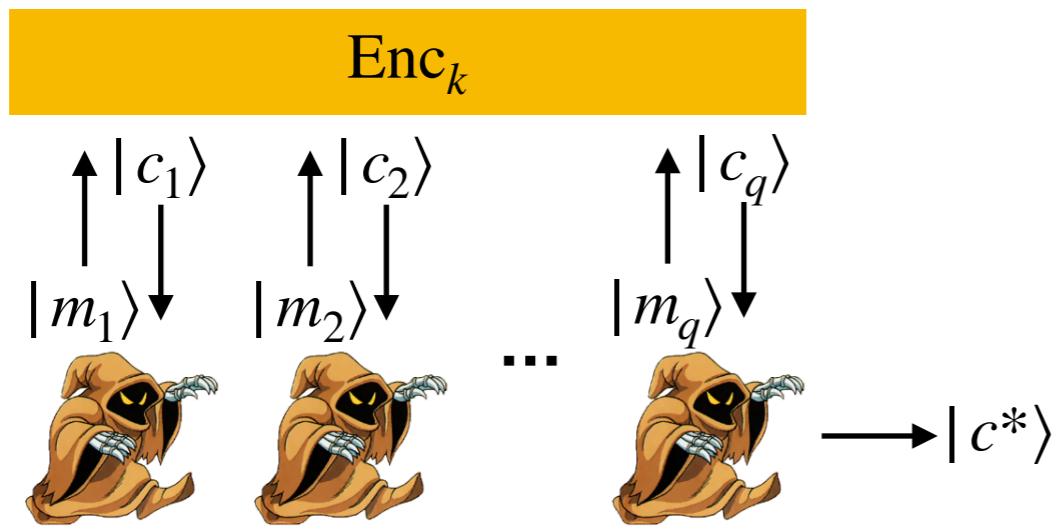
- i) ??????????????
- ii)  $\text{Dec}_k(|c^*\rangle) \neq |\perp\rangle$

What about encryption of quantum data?

# Quantum integrity of ciphertexts (attempt)

## Quantum

An encryption scheme  $(\text{KeyGen}, \text{Enc}, \text{Dec})$  has integrity of ciphertexts, if no successfull ciphertext-forging adversary exists:



Success:

- i) ??????????????
- ii) Dec<sub>k</sub>(|c\*⟩) ≠ |⊥⟩

What about encryption of quantum data?

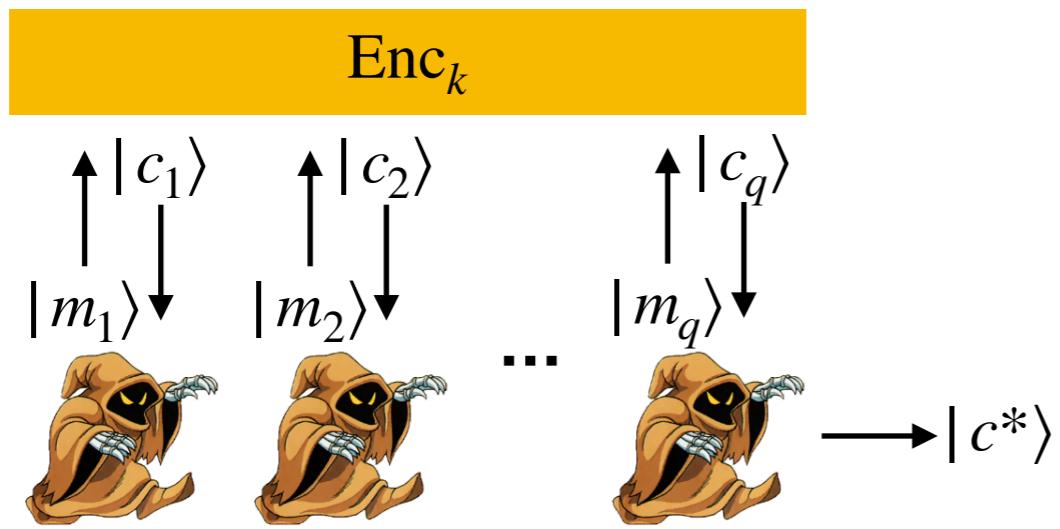
Unsurmountable problems arise:

- no-cloning: can't copy |c<sub>i</sub>⟩ for later comparison with |c\*⟩
- destructive nature of quantum measurement: even assuming we had coexisting copies of |c<sub>i</sub>⟩ and |c\*⟩, can't compare them without destroying |c\*⟩.

# Quantum integrity of ciphertexts (attempt)

## Quantum

An encryption scheme  $(\text{KeyGen}, \text{Enc}, \text{Dec})$  has integrity of ciphertexts, if no successfull ciphertext-forging adversary exists:



Success:

- i) ??????????????
- ii)  $\text{Dec}_k(|c^*\rangle) \neq |\perp\rangle$

What about encryption of quantum data?

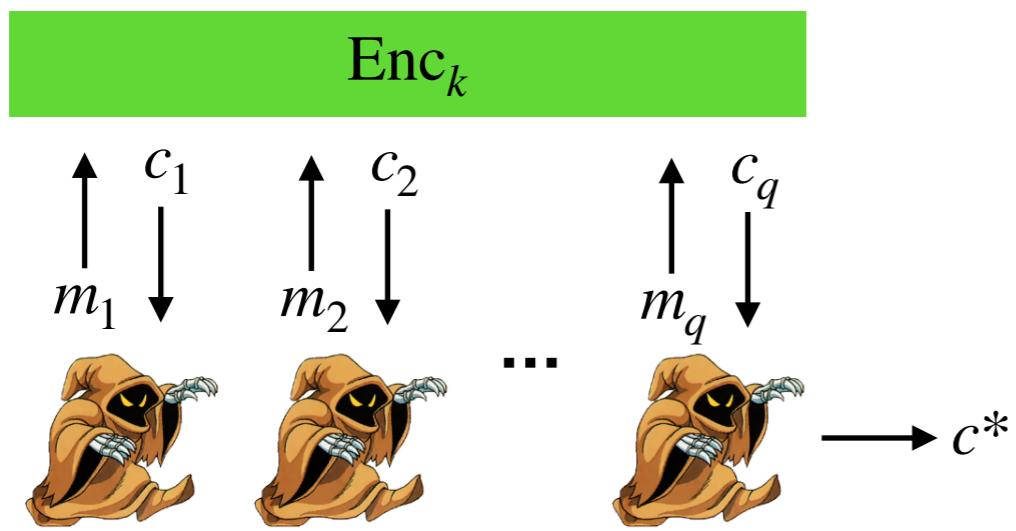
Unsurmountable problems arise:

- no-cloning: can't copy  $|c_i\rangle$  for later comparison with  $|c^*\rangle$
- destructive nature of quantum measurement: even assuming we had coexisting copies of  $|c_i\rangle$  and  $|c^*\rangle$ , can't compare them without destroying  $|c^*\rangle$ .

IND-CCA2: Adversary gets decryption oracle after the challenge phase, but can't decrypt the challenge.  $\implies$  Similar problem

# Quantum (plaintext) unforgeability – Setup

For simplicity of exposition, let's try to generalize plaintext unforgeability to quantum

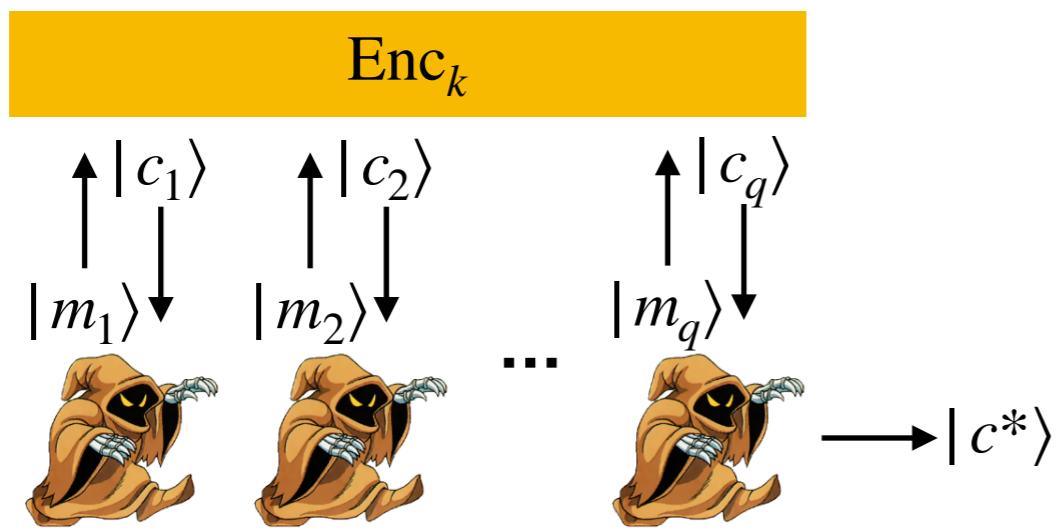


Success:

- i)  $m^* := \text{Dec}_k(c^*) \neq m_i$  for all  $i = 1, \dots, q$
- ii)  $\text{Dec}_k(c^*) \neq \perp$

# Quantum (plaintext) unforgeability – Setup

For simplicity of exposition, let's try to generalize plaintext unforgeability to quantum

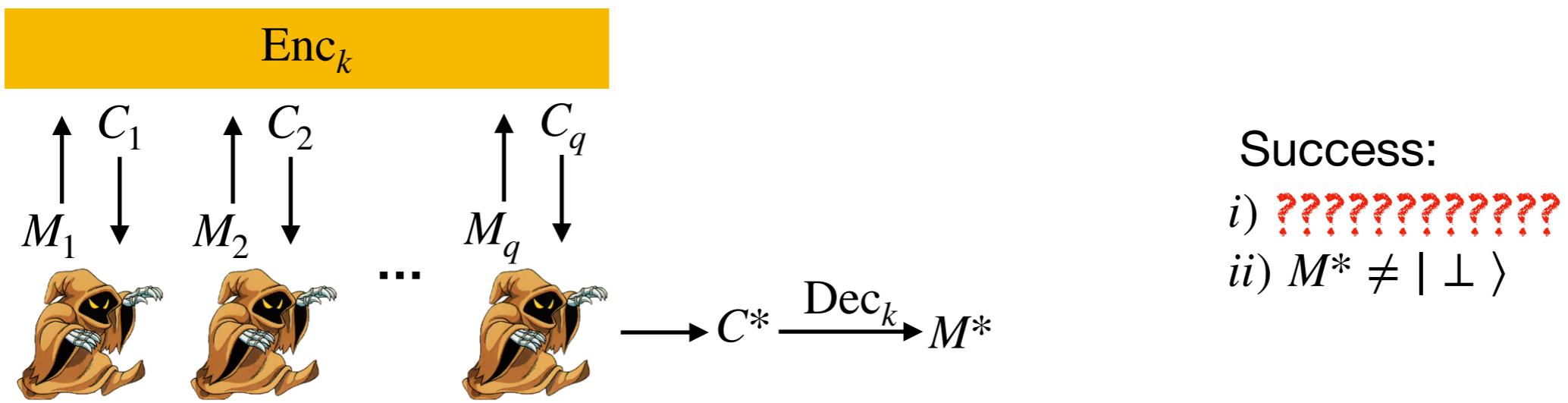


Success:

- i) ??????????????
- ii)  $\text{Dec}_k(|c^*\rangle) \neq |\perp\rangle$

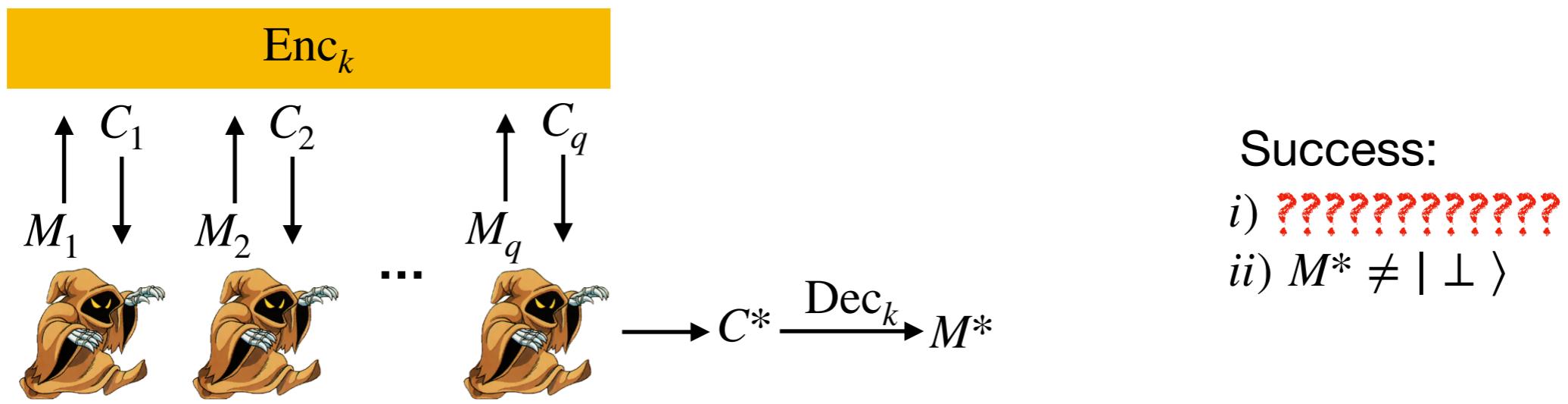
# Quantum (plaintext) unforgeability – Setup

For simplicity of exposition, let's try to generalize plaintext unforgeability to quantum



# Quantum (plaintext) unforgeability – Setup

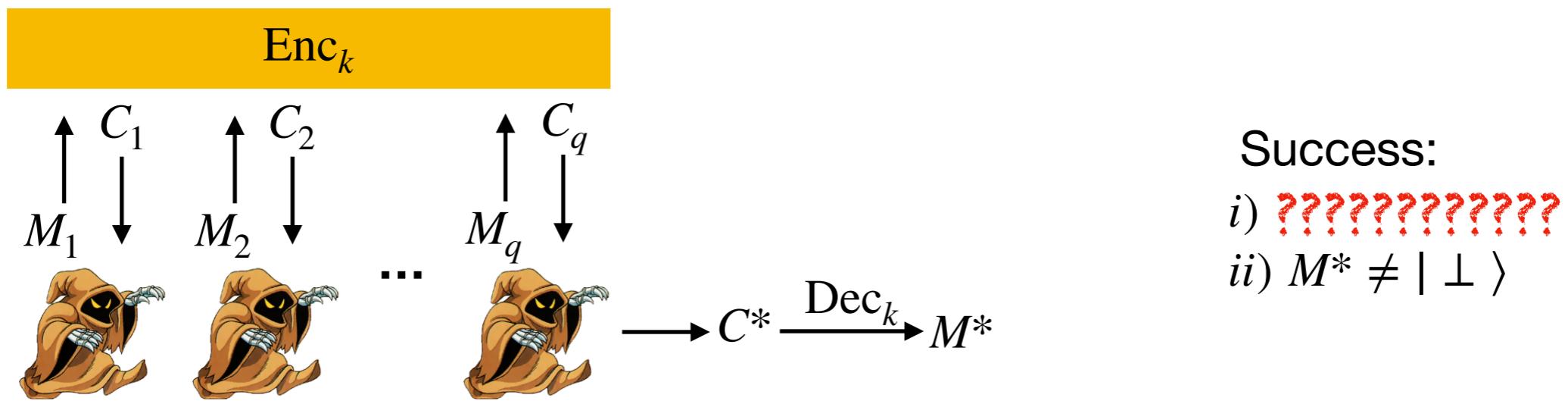
For simplicity of exposition, let's try to generalize plaintext unforgeability to quantum



Problem:  $M_i$  and  $M^*$  don't coexist. Ideas

# Quantum (plaintext) unforgeability – Setup

For simplicity of exposition, let's try to generalize plaintext unforgeability to quantum

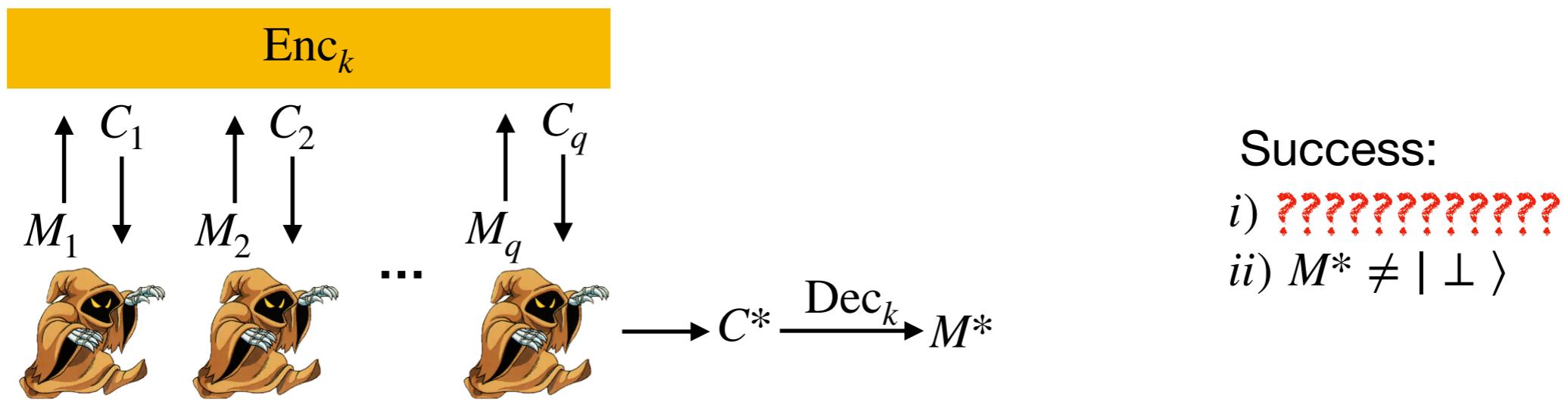


Problem:  $M_i$  and  $M^*$  don't coexist. Ideas

- look at the channels with input  $M_i$  and output  $M^*$

# Quantum (plaintext) unforgeability – Setup

For simplicity of exposition, let's try to generalize plaintext unforgeability to quantum

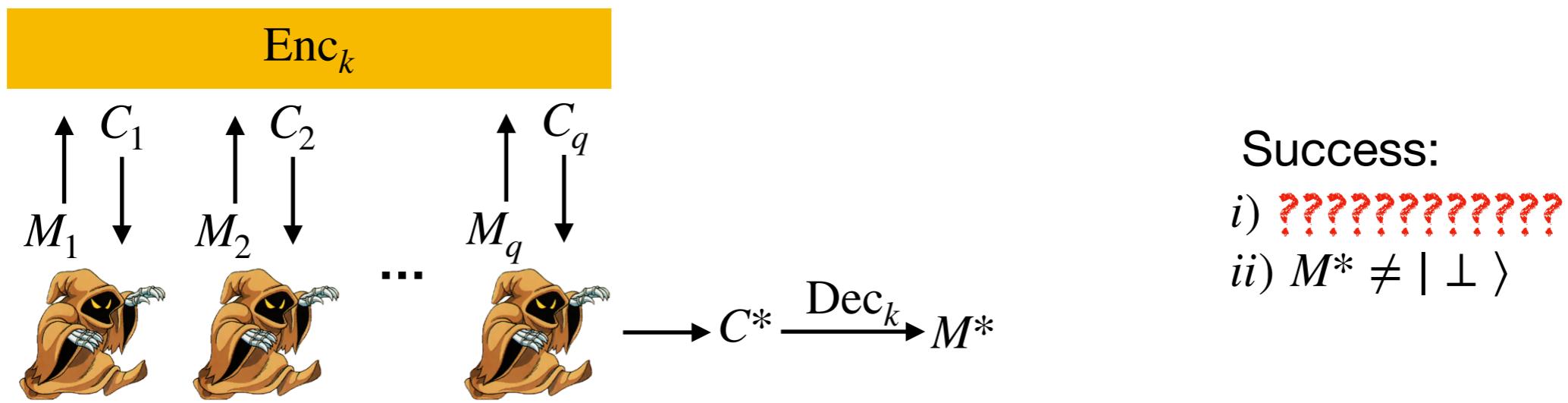


Problem:  $M_i$  and  $M^*$  don't coexist. Ideas

- look at the channels with input  $M_i$  and output  $M^*$
- compare two games, one testing whether any of these channels is the identity, one testing validity of output

# Quantum (plaintext) unforgeability – Setup

For simplicity of exposition, let's try to generalize plaintext unforgeability to quantum



Problem:  $M_i$  and  $M^*$  don't coexist. Ideas

- look at the channels with input  $M_i$  and output  $M^*$
- compare two games, one testing whether any of these channels is the identity, one testing validity of output
- efficiency needed for reduction proofs

# Identity test

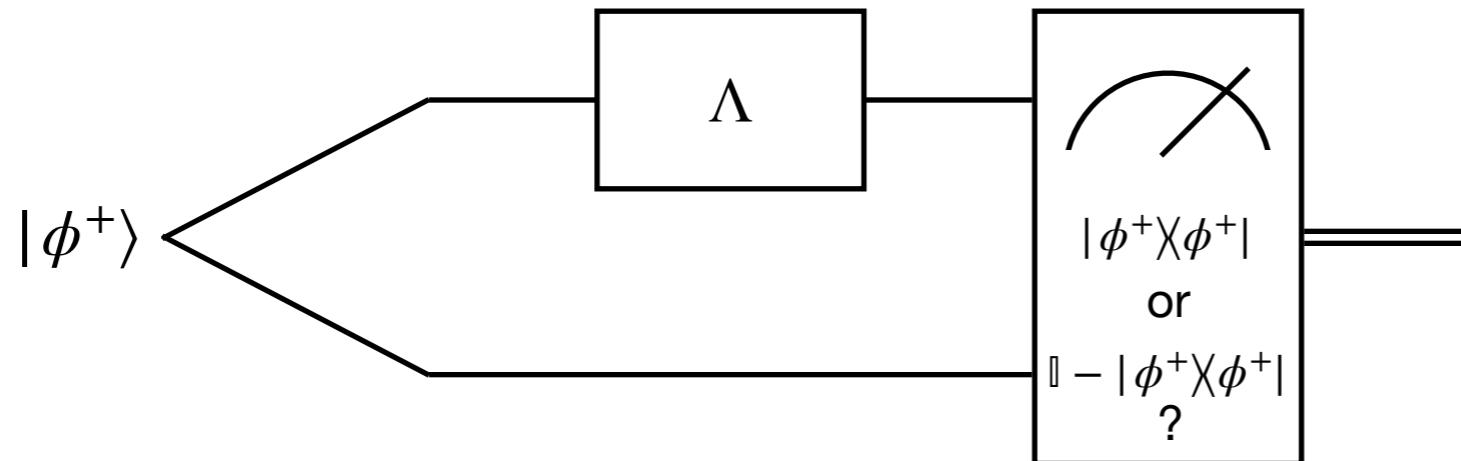
How do we test whether a quantum channel is the identity?



# Identity test

How do we test whether a quantum channel is the identity?

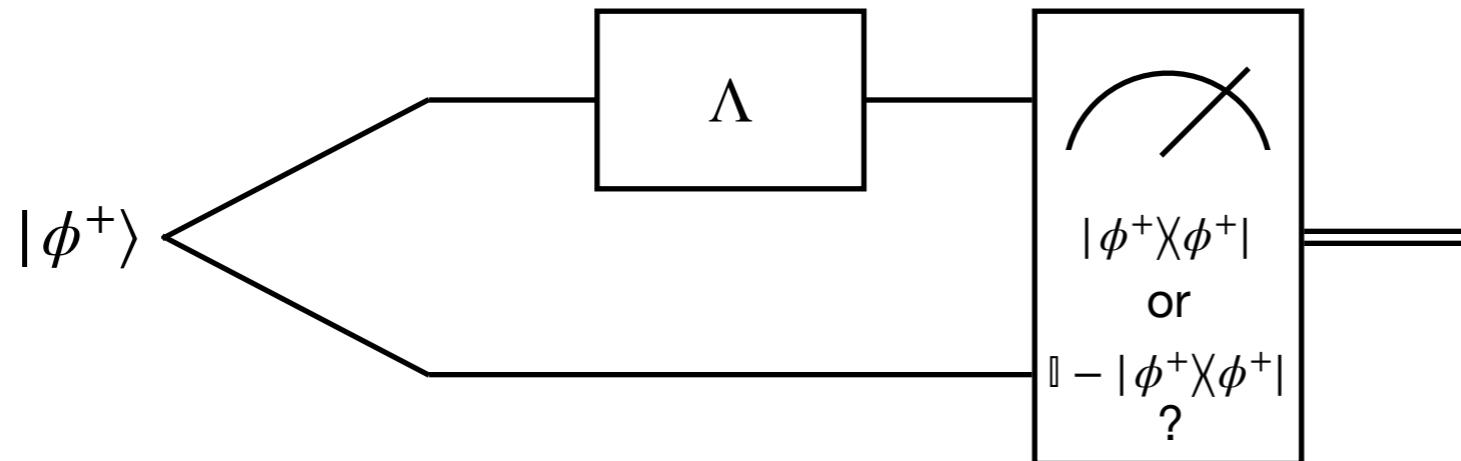
one efficient solution (Broadbent & Waynewright ICITS 2016):



# Identity test

How do we test whether a quantum channel is the identity?

one efficient solution (Broadbent & Waynewright ICITS 2016):



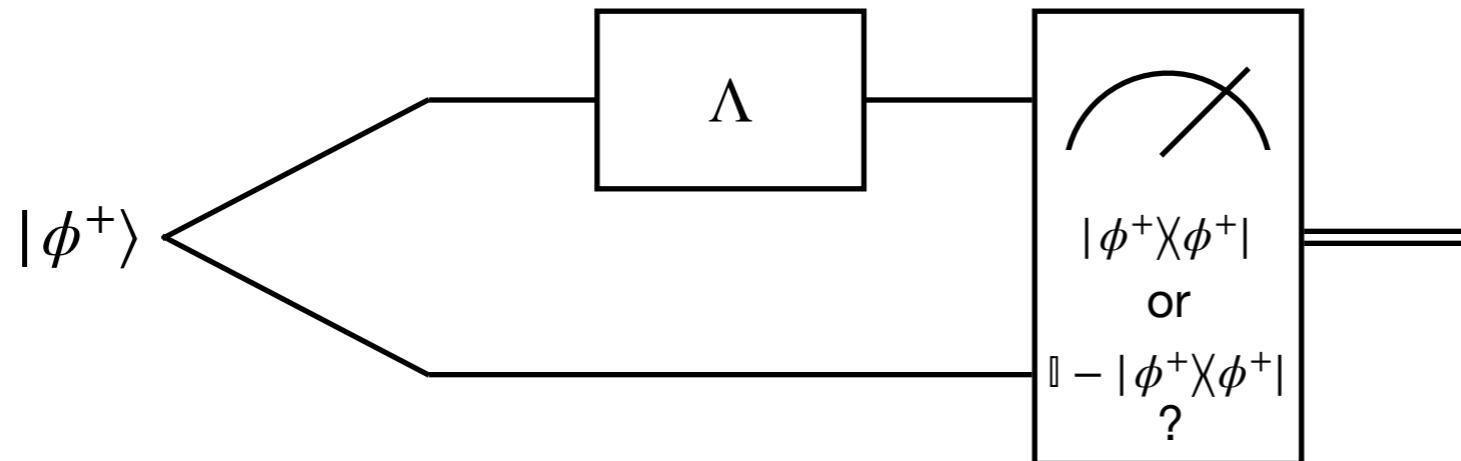
inner product in the Choi-Jamiołkowski picture



# Identity test

How do we test whether a quantum channel is the identity?

one efficient solution (Broadbent & Waynewright ICITS 2016):



inner product in the Choi-Jamiołkowski picture

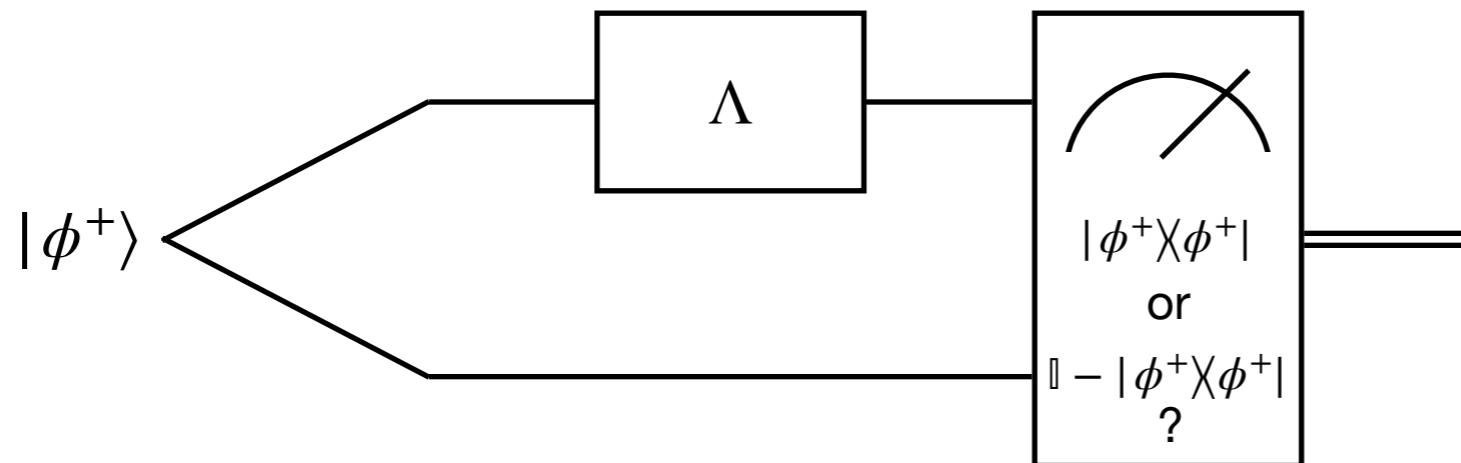
other identity tests possible that don't need entanglement....



# Identity test

How do we test whether a quantum channel is the identity?

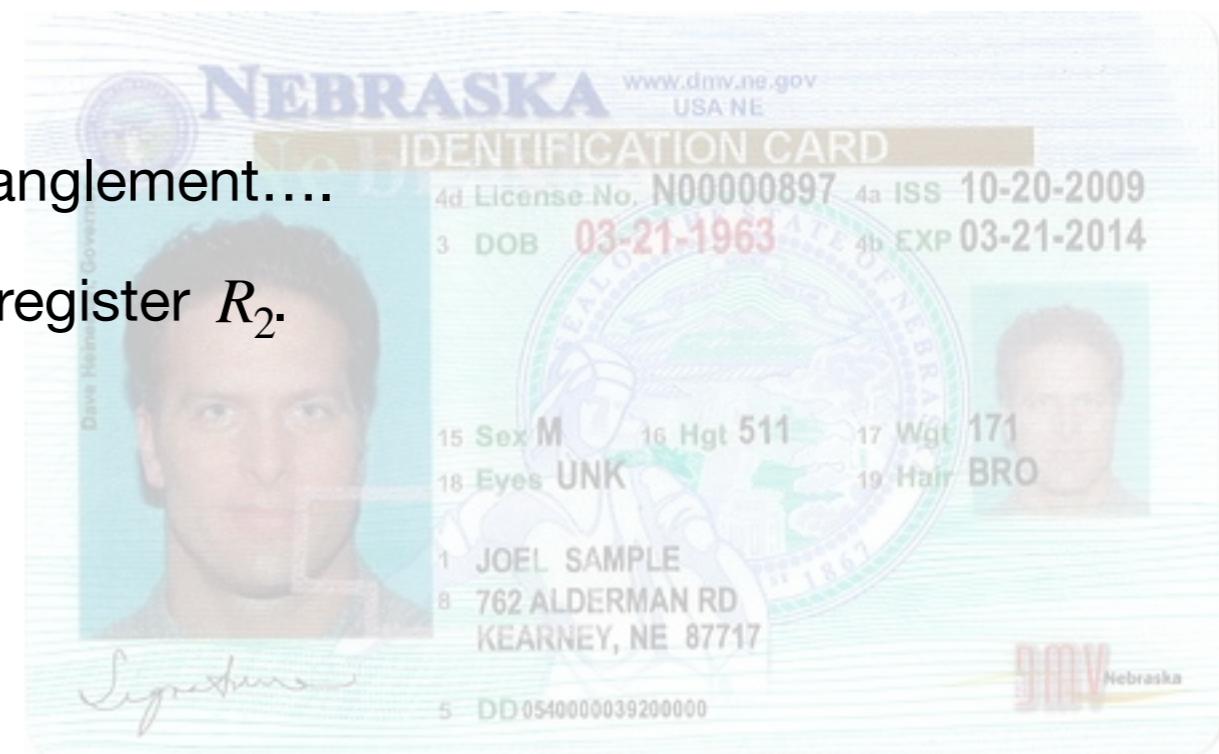
one efficient solution (Broadbent & Waynewright ICITS 2016):



inner product in the Choi-Jamiołkowski picture

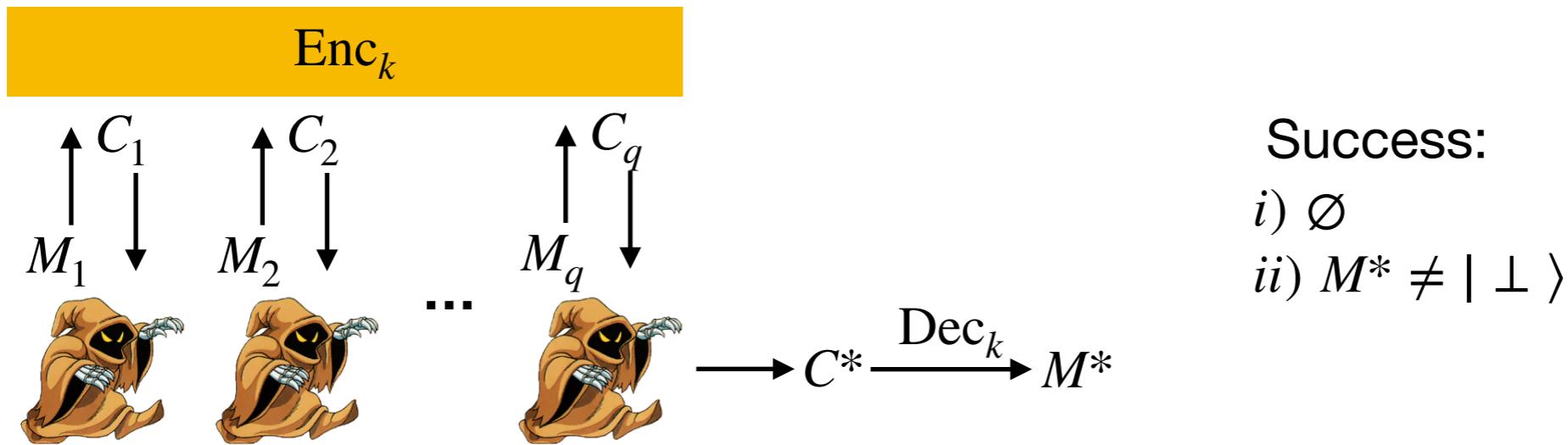
other identity tests possible that don't need entanglement....

Let  $\text{Id}_{R_1 R_2}$  be the identity test from register  $R_1$  to register  $R_2$ .



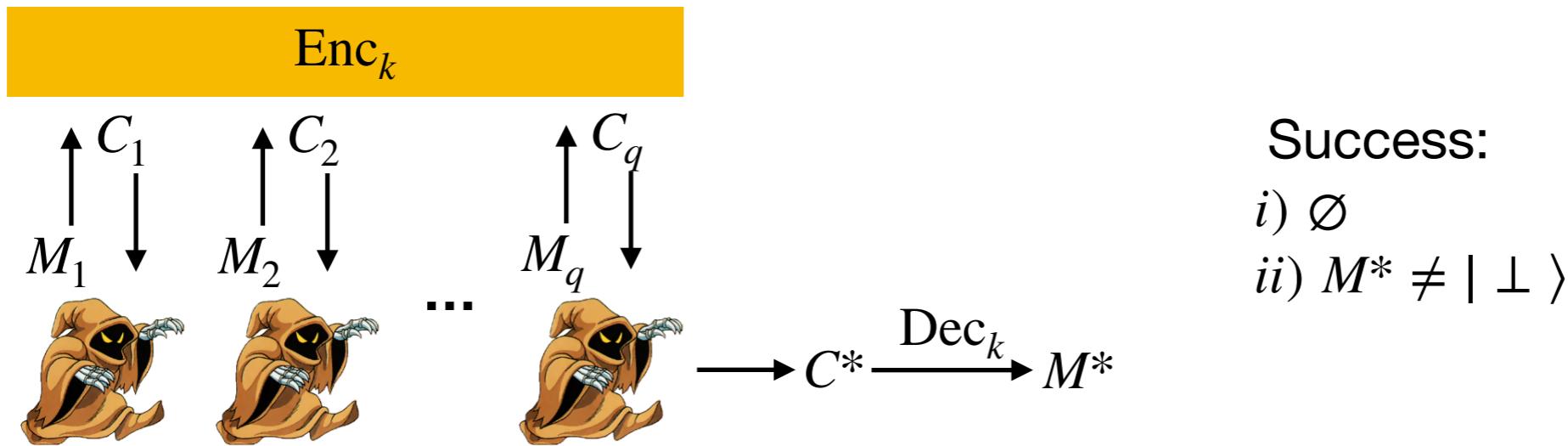
# Two games

QUF-Forge game



# Two games

QUF-Forge game



Success:

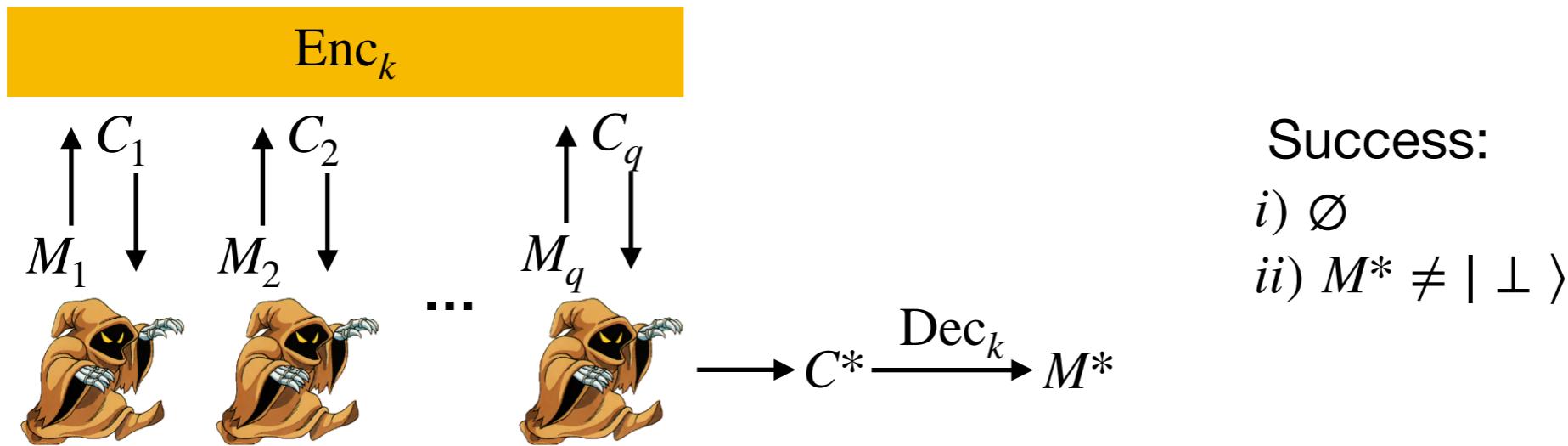
- i)  $\emptyset$
- ii)  $M^* \neq |\perp\rangle$

QUF-Test game



# Two games

QUF-Forge game

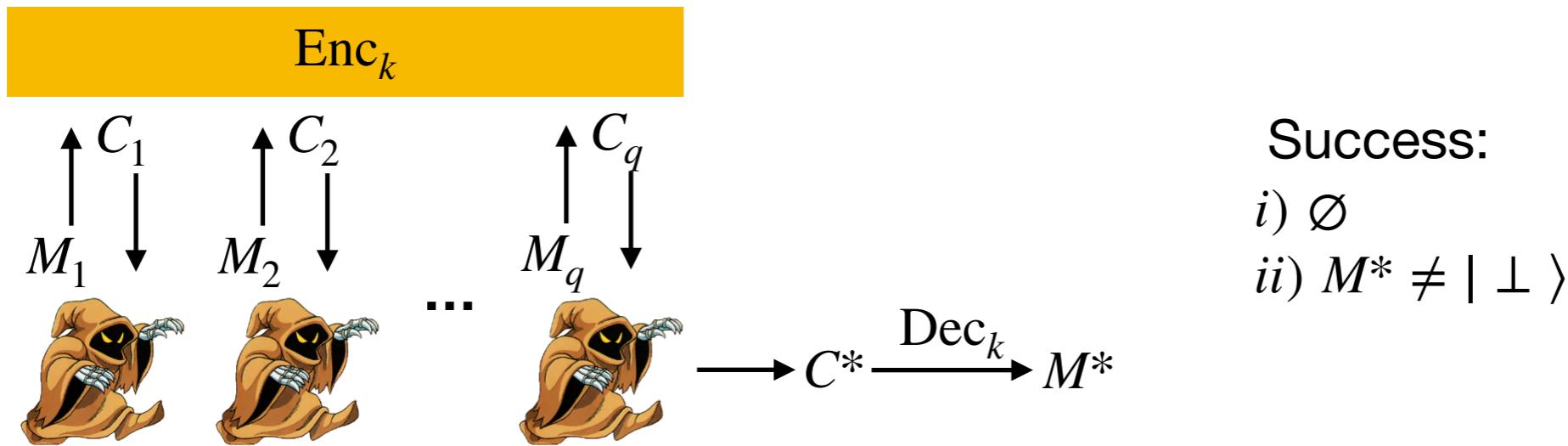


QUF-Test game

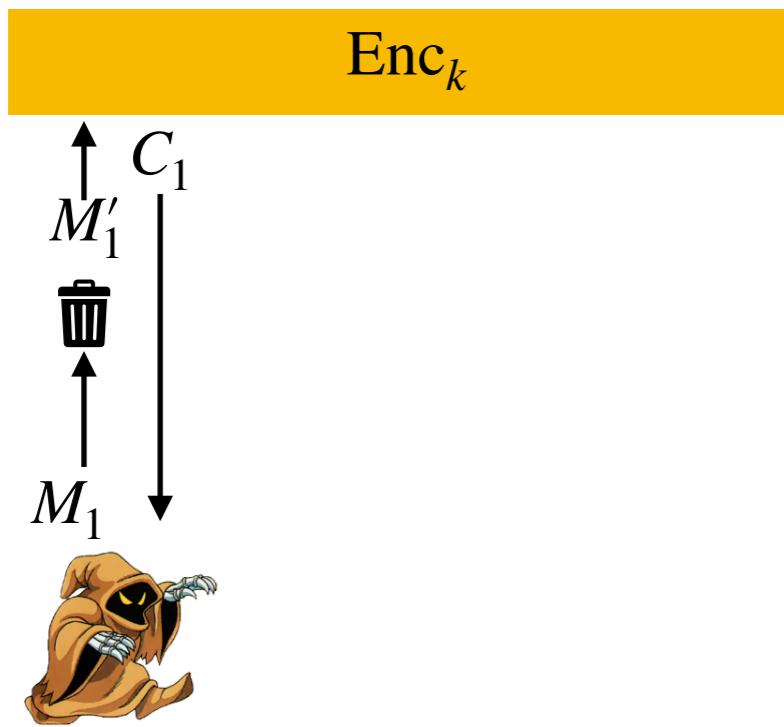


# Two games

QUF-Forge game

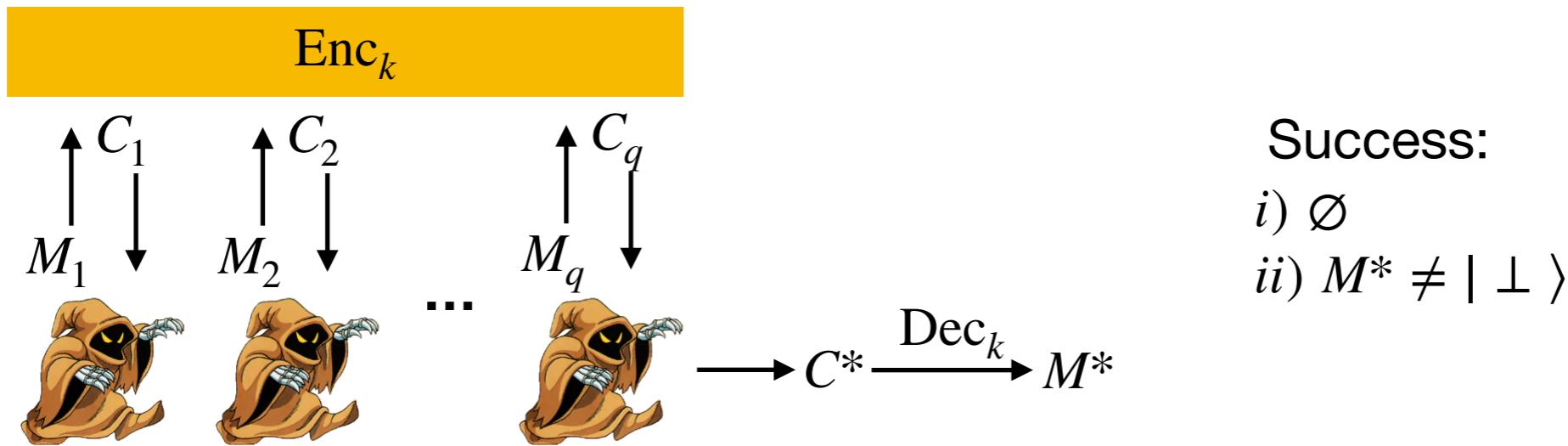


QUF-Test game

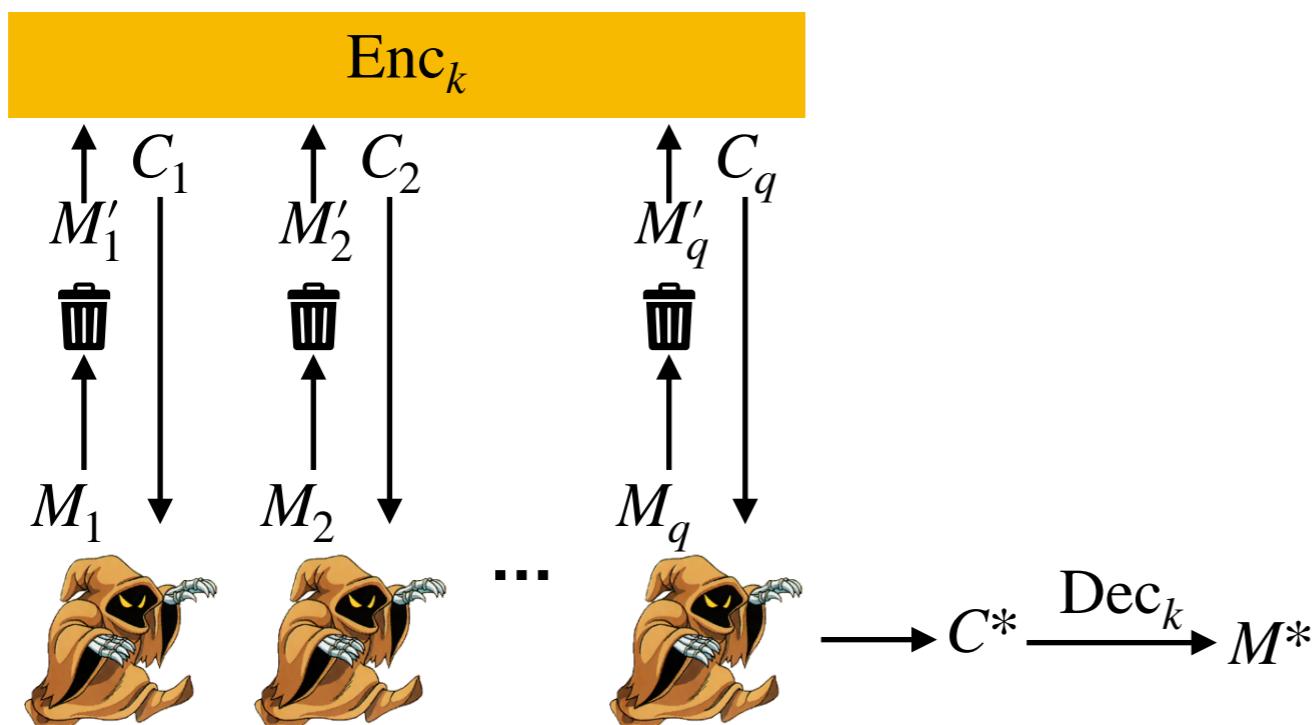


# Two games

QUF-Forge game

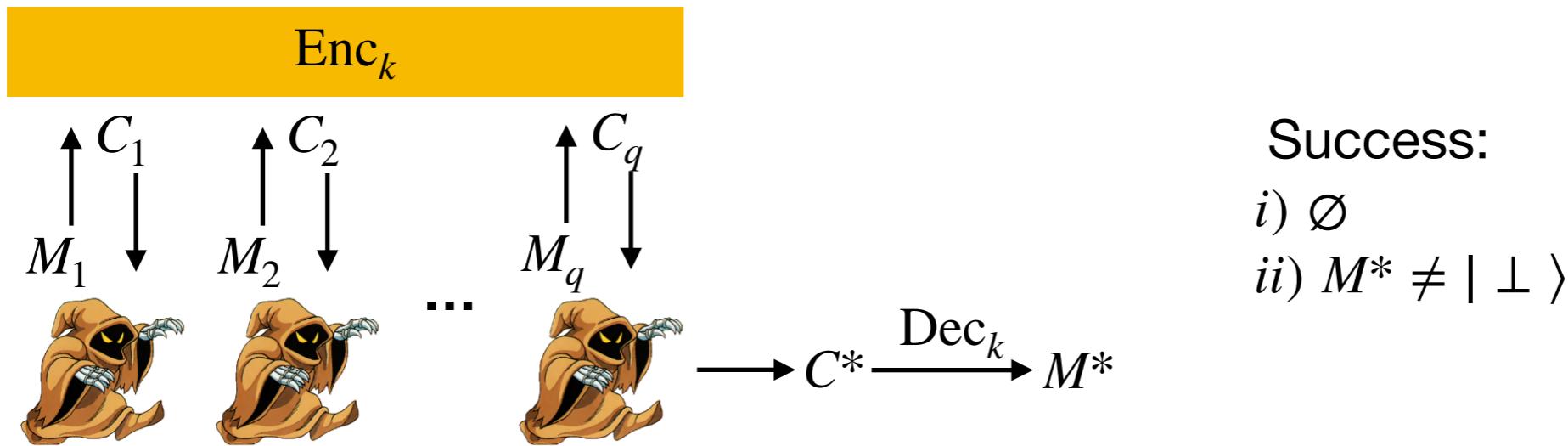


QUF-Test game

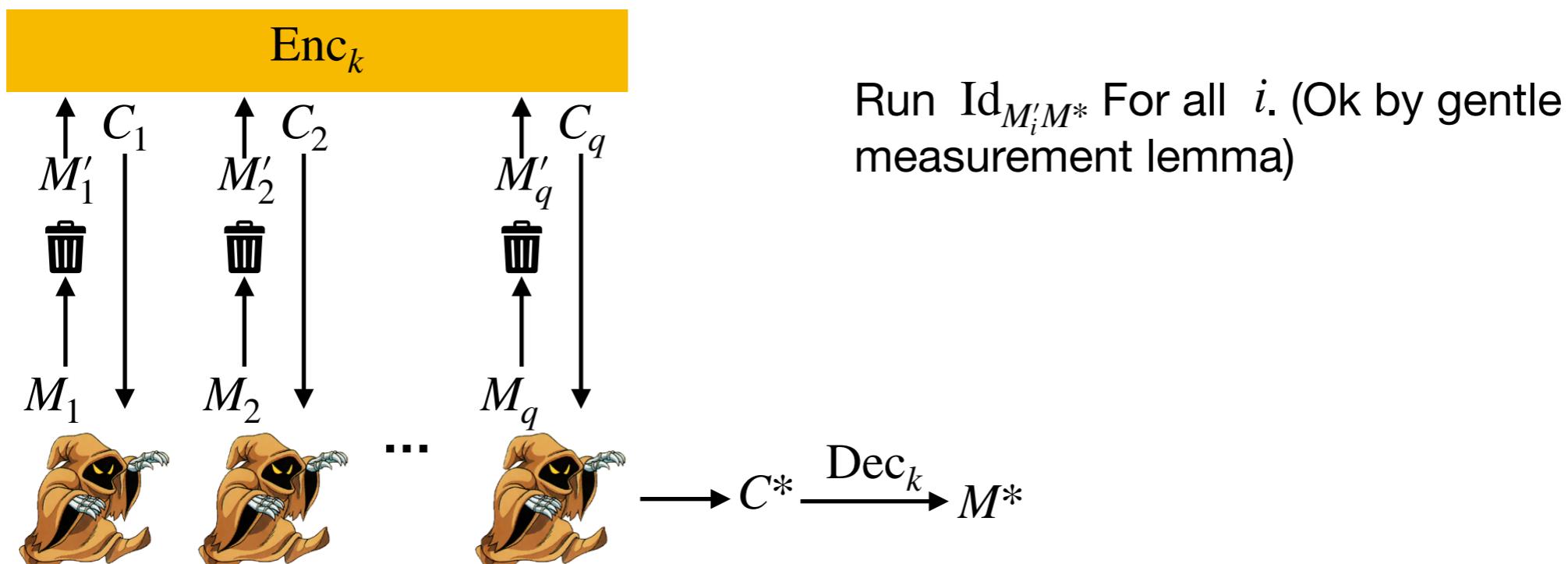


# Two games

QUF-Forge game

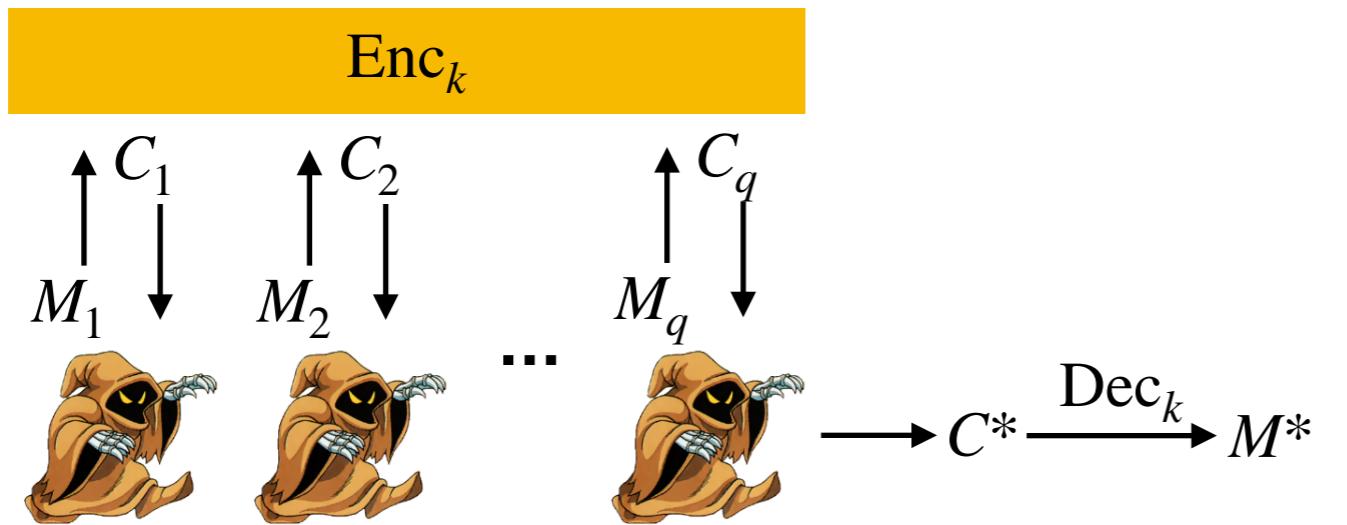


QUF-Test game

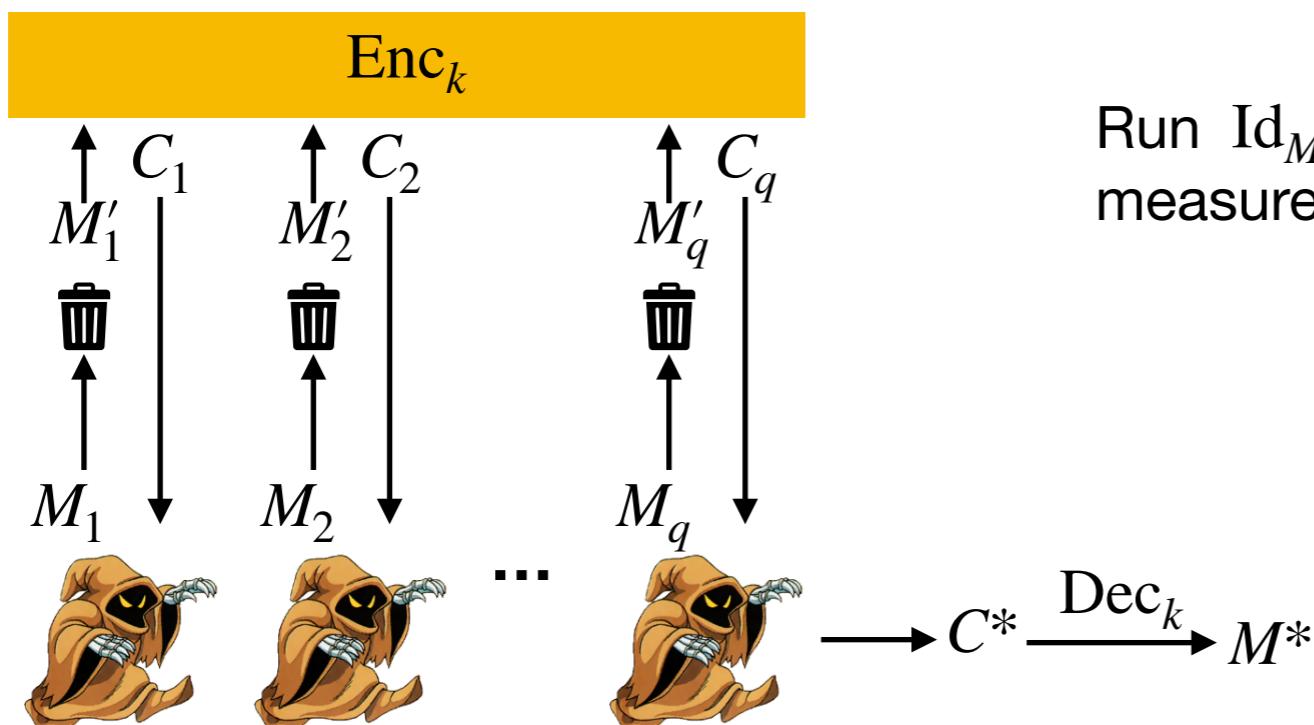


# Two games

QUF-Forge game



QUF-Test game



# Quantum (plaintext) unforgeability – Definition

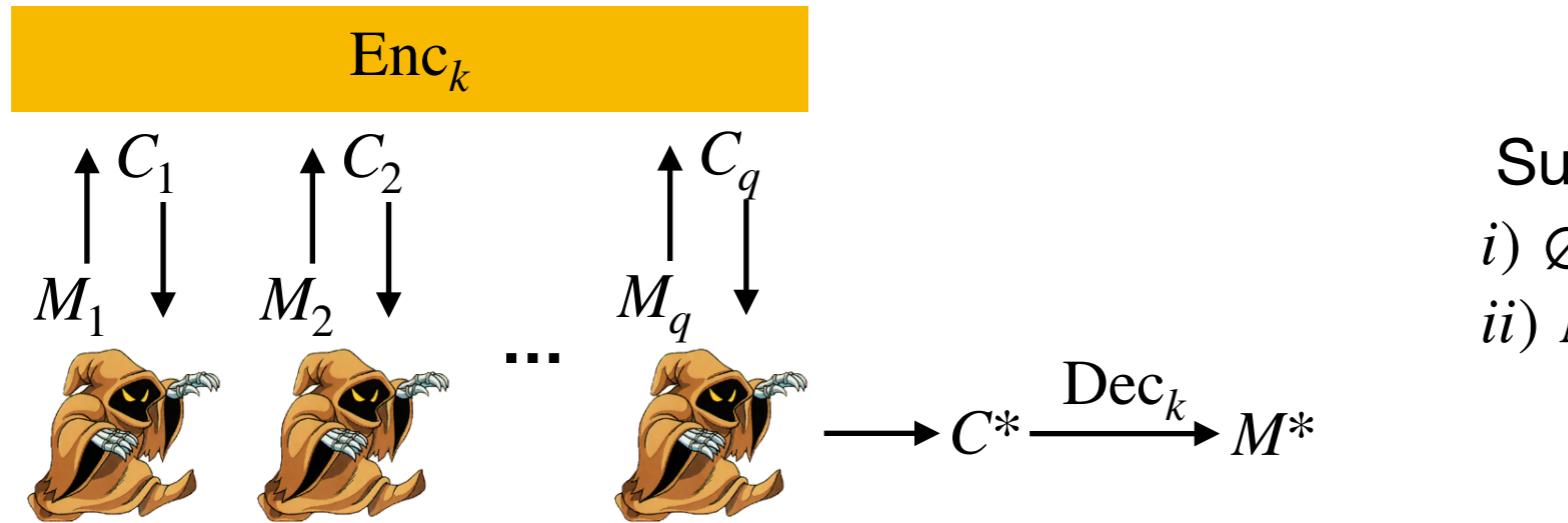
**Definition** (Quantum plaintext unforgeability):

A quantum encryption scheme  $(\text{KeyGen}, \text{Enc}, \text{Dec})$  has unforgeable plaintexts, if for all QPT adversaries  $\mathcal{A}$  it holds that

$$\left| \mathbb{P} [\mathcal{A} \text{ wins QUF - forge}] - \mathbb{P} [\mathcal{A} \text{ wins QUF - test}] \right| \leq \text{negl}(n)$$

# Quantum (plaintext) unforgeability – Definition

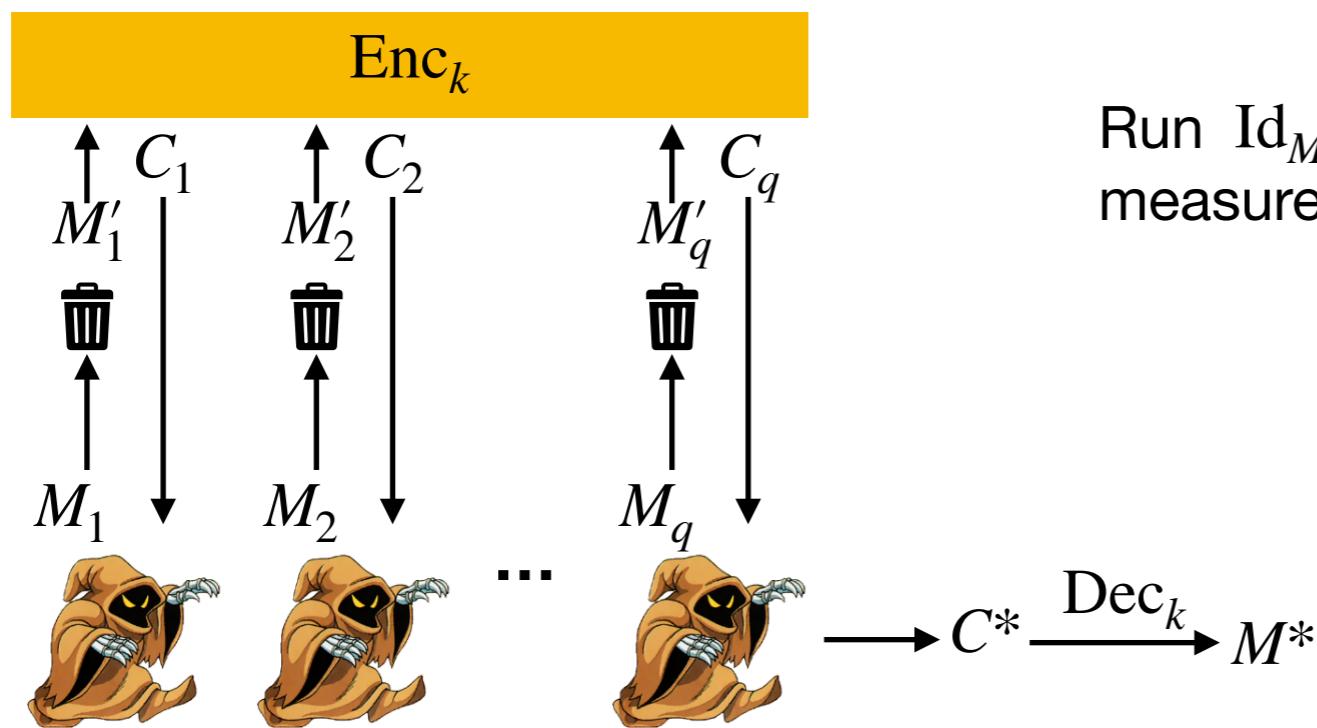
QUF-Forge game



Success:

- i)  $\emptyset$
- ii)  $M^* \neq |\perp\rangle$

QUF-Test game



Run  $\text{Id}_{M'_i M^*}$  For all  $i$ . (Ok by gentle measurement lemma)

Cheat (=“Success”):

- i)  $\text{Id}_{M'_i M^*}$  succeeds for at least one  $i$
- ii)  $\emptyset$

# Quantum (plaintext) unforgeability – Definition

**Definition** (Quantum plaintext unforgeability):

A quantum encryption scheme  $(\text{KeyGen}, \text{Enc}, \text{Dec})$  has unforgeable plaintexts, if for all QPT adversaries  $\mathcal{A}$  it holds that

$$\left| \mathbb{P} [\mathcal{A} \text{ wins QUF - forge}] - \mathbb{P} [\mathcal{A} \text{ wins QUF - test}] \right| \leq \text{negl}(n)$$

# Quantum (plaintext) unforgeability – Definition

**Definition** (Quantum plaintext unforgeability):

A quantum encryption scheme  $(\text{KeyGen}, \text{Enc}, \text{Dec})$  has unforgeable plaintexts, if for all QPT adversaries  $\mathcal{A}$  it holds that

$$\left| \mathbb{P} [\mathcal{A} \text{ wins QUF - forge}] - \mathbb{P} [\mathcal{A} \text{ wins QUF - test}] \right| \leq \text{negl}(n)$$

- implies IND-CPA, ok because authentication  $\Rightarrow$  encryption (Barnum et al. 2002).

# Quantum (plaintext) unforgeability – Definition

**Definition** (Quantum plaintext unforgeability):

A quantum encryption scheme  $(\text{KeyGen}, \text{Enc}, \text{Dec})$  has unforgeable plaintexts, if for all QPT adversaries  $\mathcal{A}$  it holds that

$$\left| \mathbb{P} [\mathcal{A} \text{ wins QUF - forge}] - \mathbb{P} [\mathcal{A} \text{ wins QUF - test}] \right| \leq \text{negl}(n)$$

- implies IND-CPA, ok because authentication  $\implies$  encryption (Barnum et al. 2002).
- classical restriction is equivalent to authenticated encryption

# Quantum (plaintext) unforgeability – Definition

**Definition** (Quantum plaintext unforgeability):

A quantum encryption scheme  $(\text{KeyGen}, \text{Enc}, \text{Dec})$  has unforgeable plaintexts, if for all QPT adversaries  $\mathcal{A}$  it holds that

$$\left| \mathbb{P} [\mathcal{A} \text{ wins QUF - forge}] - \mathbb{P} [\mathcal{A} \text{ wins QUF - test}] \right| \leq \text{negl}(n)$$

- implies IND-CPA, ok because authentication  $\implies$  encryption (Barnum et al. 2002).
- classical restriction is equivalent to authenticated encryption
- can be upgraded to quantum ciphertext authentication:

# Quantum (plaintext) unforgeability – Definition

**Definition** (Quantum plaintext unforgeability):

A quantum encryption scheme  $(\text{KeyGen}, \text{Enc}, \text{Dec})$  has unforgeable plaintexts, if for all QPT adversaries  $\mathcal{A}$  it holds that

$$\left| \mathbb{P} [\mathcal{A} \text{ wins QUF - forge}] - \mathbb{P} [\mathcal{A} \text{ wins QUF - test}] \right| \leq \text{negl}(n)$$

- implies IND-CPA, ok because authentication  $\implies$  encryption (Barnum et al. 2002).
- classical restriction is equivalent to authenticated encryption
- can be upgraded to quantum ciphertext authentication:
  - \* possible via lemma: any quantum encryption function can be implemented by classical sampling and unitary transformation

# Quantum (plaintext) unforgeability – Definition

**Definition** (Quantum plaintext unforgeability):

A quantum encryption scheme  $(\text{KeyGen}, \text{Enc}, \text{Dec})$  has unforgeable plaintexts, if for all QPT adversaries  $\mathcal{A}$  it holds that

$$\left| \mathbb{P} [\mathcal{A} \text{ wins QUF - forge}] - \mathbb{P} [\mathcal{A} \text{ wins QUF - test}] \right| \leq \text{negl}(n)$$

- implies IND-CPA, ok because authentication  $\implies$  encryption (Barnum et al. 2002).
- classical restriction is equivalent to authenticated encryption
- can be upgraded to quantum ciphertext authentication:
  - \* possible via lemma: any quantum encryption function can be implemented by classical sampling and unitary transformation
  - \* use identity test for quantum part and save a copy of classical randomness

**What I couldn't explain in 17 min...**

# What I couldn't explain in 17 min...

QIND-CCA2: Use identity test to detect challenge decryption, again by comparing two games

# What I couldn't explain in 17 min...

QIND-CCA2: Use identity test to detect challenge decryption, again by comparing two games

quantum authenticated encryption? Could define as QUF+QIND-CCA2, but...

# What I couldn't explain in 17 min...

QIND-CCA2: Use identity test to detect challenge decryption, again by comparing two games

quantum authenticated encryption? Could define as QUF+QIND-CCA2, but...

...alternative real vs. ideal characterization (Shrimpton, 2004) is *made* for the identity testing technique!

# What I couldn't explain in 17 min...

QIND-CCA2: Use identity test to detect challenge decryption, again by comparing two games

quantum authenticated encryption? Could define as QUF+QIND-CCA2, but...

...alternative real vs. ideal characterization (Shrimpton, 2004) is *made* for the identity testing technique!

⇒ separate definition: QAE

# What I couldn't explain in 17 min...

QIND-CCA2: Use identity test to detect challenge decryption, again by comparing two games

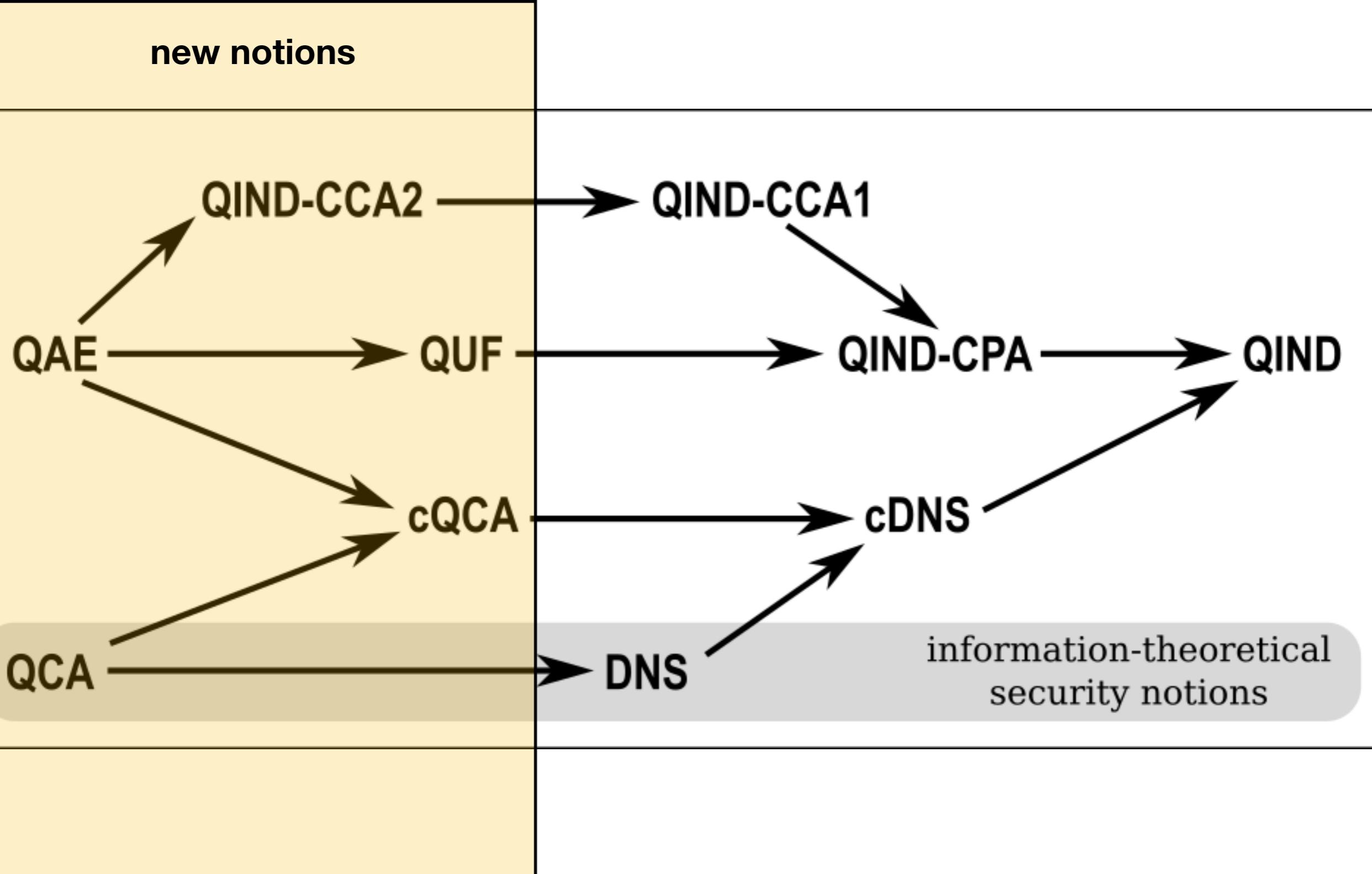
quantum authenticated encryption? Could define as QUF+QIND-CCA2, but...

...alternative real vs. ideal characterization (Shrimpton, 2004) is *made* for the identity testing technique!

⇒ separate definition: QAE

simple construction from pseudorandom functions and unitary 2-designs

# Taxonomy of quantum security



# Conclusion

- Generalizing authenticity and integrity security notions (and adaptive CCA security) to quantum is complicated by the fact that states from different stages of an algorithm cannot be compared
- Divide and conquer! If it is impossible to check two properties in one game, use two (indistinguishable) games!
- That way we get quantum versions of the integrity notions used in modern crypto.
- They can be fulfilled and have nice relationships.

## What's left to do?

- Is QAE=QUF+QIND-CCA2?
- Relationship to quantum world notions?