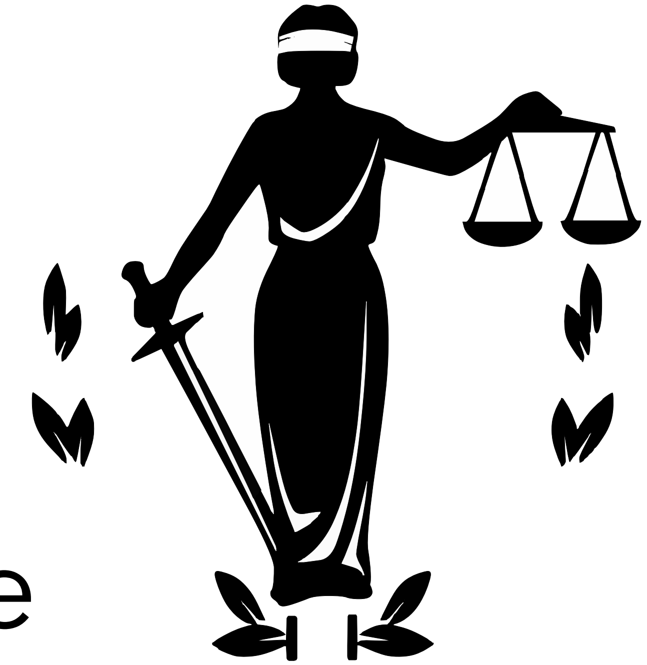


# Quantum-secure message authentication via blind-unforgeability

Gorjan Alagic, Christian Majenz, Alexander Russell and Fang Song

Eurocrypt 2020, in Cyberspace

QuSoft
Research Center for Quantum Software

UCONN

Texas A&M University 1876

Joint Center for Quantum Information and Computer Science

# Introduction

# Integrity and authenticity

# Integrity and authenticity

- "It says X on the bottom, but is this letter really from them?"

# Integrity and authenticity

- “It says X on the bottom, but is this letter really from them?”
- “The letter probably took 5 days to get here, offering plenty of opportunities for somebody to change it.”

# Integrity and authenticity

- "It says X on the bottom, but is this letter really from them?"
- "The letter probably took 5 days to get here, offering plenty of opportunities for somebody to change it."

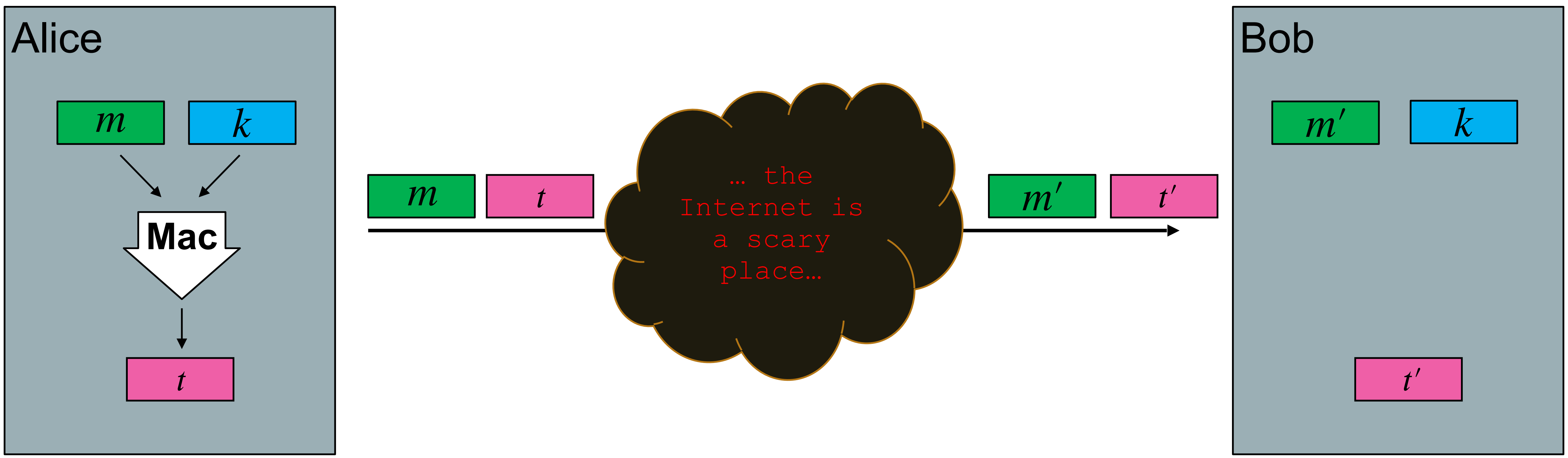
Nowadays: digital signature schemes, message authentication codes (MACs).

# Message authentication

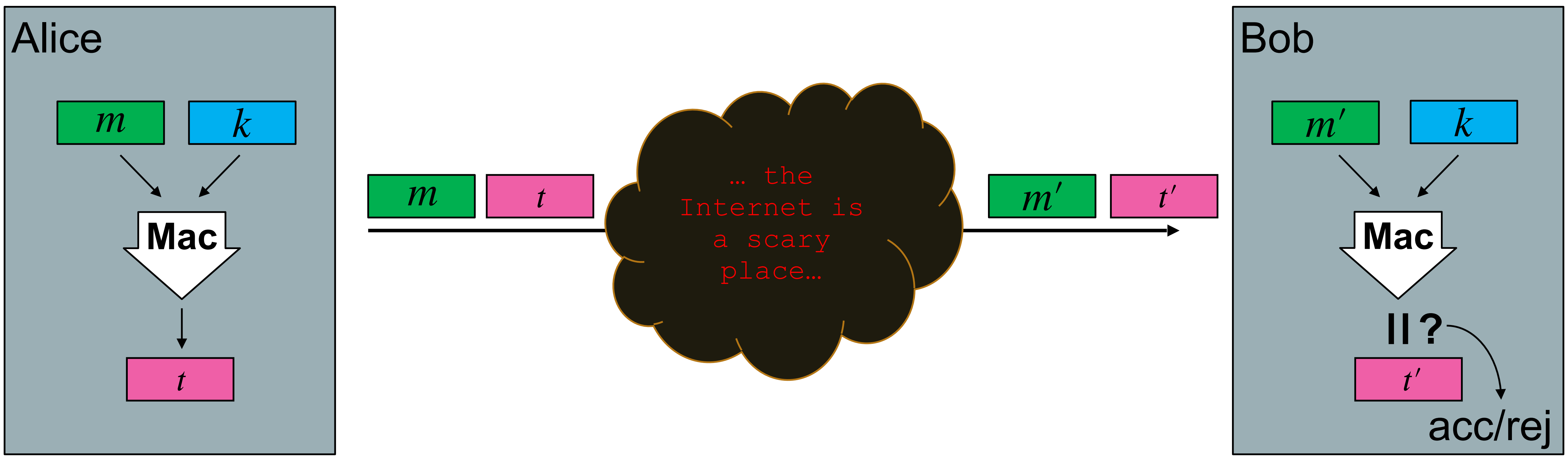
# Message authentication

# Message authentication

# Message authentication



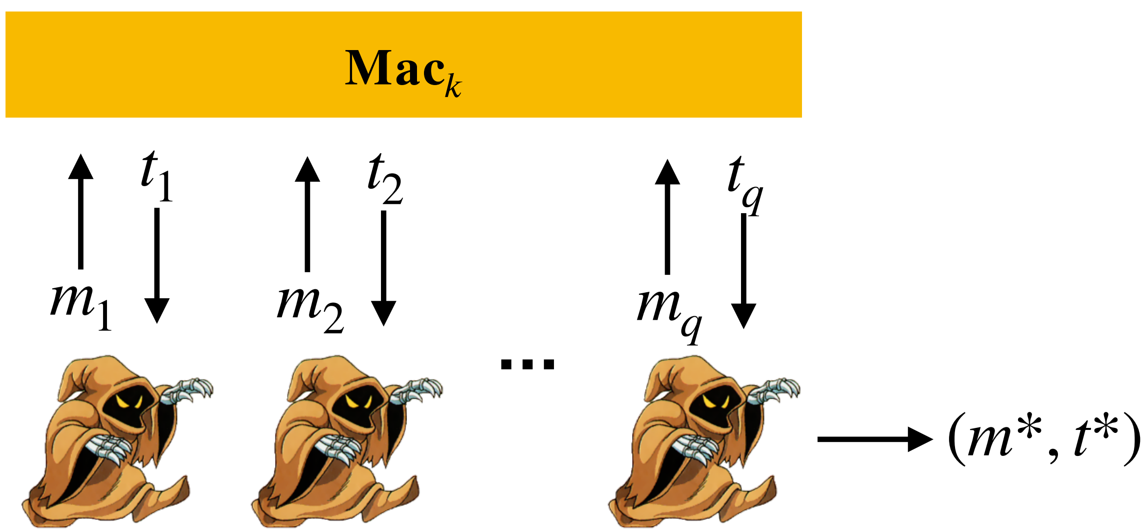
# Message authentication



# Security: UF-CMA

Definition: Unforgeability under chosen message attacks (**UF-CMA)**

A message authentication code is secure, if no successful forger exists:




Success:

$i)$ $m^* \neq m_i$ for all $i = 1, \ldots, q$

$ii)$ $\mathbf{Mac}_k(m^*) = t^*$

# Quantum Access Security

Stronger security model: quantum oracle access to $\mathbf{Mac}_k$:

$$|m\rangle|t\rangle \mapsto |m\rangle|t \oplus \mathrm{Mac}_k(m)\rangle$$

# Quantum Access Security

Stronger security model: quantum oracle access to $\mathbf{Mac}_k$:

$$|m\rangle|t\rangle \mapsto |m\rangle|t \oplus \mathrm{Mac}_k(m)\rangle$$

Why?

# Quantum Access Security

Stronger security model: quantum oracle access to $\mathbf{Mac}_k$:

$$|m\rangle|t\rangle \mapsto |m\rangle|t \oplus \mathrm{Mac}_k(m)\rangle$$

Why?

- As-strong-as-possible security

# Quantum Access Security

Stronger security model: quantum oracle access to $\mathbf{Mac}_k$:

$$|m\rangle|t\rangle \mapsto |m\rangle|t \oplus \mathrm{Mac}_k(m)\rangle$$

Why?

- As-strong-as-possible security
- Post-quantum Composability

# Quantum Access Security

Stronger security model: quantum oracle access to $\mathbf{Mac}_k$:

$$|m\rangle|t\rangle \mapsto |m\rangle|t \oplus \mathrm{Mac}_k(m)\rangle$$

Why?

- As-strong-as-possible security
- Post-quantum Composability
- Physics?

# Quantum Access Security

Stronger security model: quantum oracle access to $\mathbf{Mac}_k$:

$$|m\rangle|t\rangle \mapsto |m\rangle|t \oplus \mathrm{Mac}_k(m)\rangle$$

Why?

- As-strong-as-possible security
- Post-quantum Composability
- Physics?

Let's try **UF-"QCMA"**

# Quantum Access Security

Stronger security model: quantum oracle access to $\mathbf{Mac}_k$:

$$|m\rangle|t\rangle \mapsto |m\rangle|t \oplus \mathrm{Mac}_k(m)\rangle$$

Why?

- As-strong-as-possible security
- Post-quantum Composability
- Physics?

Let's try **UF-"QCMA"**

Example:

i) Query $|m_1\rangle = \sum_{m\in\{0,1\}^n} |m\rangle|0\rangle$ to obtain $\sum_{m\in\{0,1\}^n} |m\rangle|\mathrm{Mac}_k(m)\rangle$

ii) Measure in the computational basis to obtain $(m, \mathbf{Mac}_k(m))$ for random $m$

iii) Output $(m, \mathbf{Mac}_k(m))$

# Quantum Access Security

Stronger security model: quantum oracle access to $\mathbf{Mac}_k$:

$$|m\rangle|t\rangle \mapsto |m\rangle|t \oplus \mathrm{Mac}_k(m)\rangle$$

Why?

- As-strong-as-possible security
- Post-quantum Composability
- Physics?

Let's try **UF-"QCMA"**

Example:

i) Query $|m_1\rangle = \sum_{m\in\{0,1\}^n} |m\rangle|0\rangle$ to obtain $\sum_{m\in\{0,1\}^n} |m\rangle|\mathrm{Mac}_k(m)\rangle$

ii) Measure in the computational basis to obtain $(m, \mathbf{Mac}_k(m))$ for random $m$

iii) Output $(m, \mathbf{Mac}_k(m))$

**UF-CMA** doesn't make sense anymore…

# Quantum chosen message attacks

What does it mean for a function to be unpredictable against quantum?

What is a successful forging adversary?

# Quantum chosen message attacks

What does it mean for a function to be unpredictable against quantum?

What is a successful forging adversary?

We shouldn't be worried about:

i) Query $m_1 = \sum_{m \in \{0,1\}^n} |m\rangle|0\rangle$ to obtain $\sum_{m \in \{0,1\}^n} |m\rangle|\mathrm{Mac}_k(m)\rangle$

ii) Measure in the computational basis to obtain $(m, \mathbf{Mac}_k(m))$ for random $m$

iii) Output $(m, \mathbf{Mac}_k(m))$

# Quantum chosen message attacks

What does it mean for a function to be unpredictable against quantum?

What is a successful forging adversary?

We shouldn't be worried about:

i) Query $m_1 = \sum_{m \in \{0,1\}^n} |m\rangle|0\rangle$ to obtain $\sum_{m \in \{0,1\}^n} |m\rangle|\mathrm{Mac}_k(m)\rangle$

ii) Measure in the computational basis to obtain $(m, \mathbf{Mac}_k(m))$ for random $m$

iii) Output $(m, \mathbf{Mac}_k(m))$

We should be worried about:

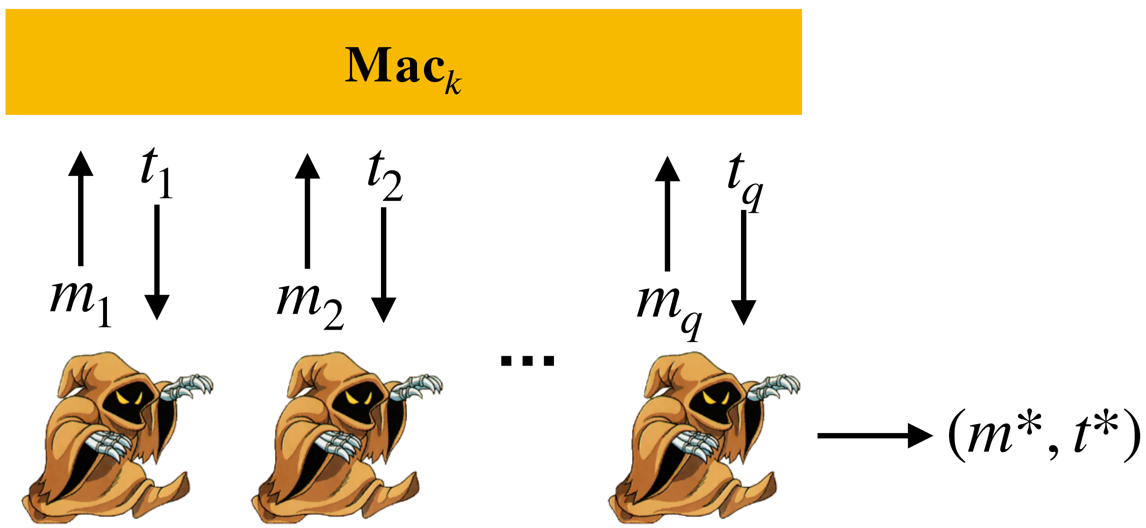
key $k$ specifies a random periodic function $f_k$ with period $p_k$

$\mathbf{Mac}_k(p_k) = 0$ , and $\mathbf{Mac}_k(x) = f_k(x)\ \forall x \neq p_k$

i) run period finding (a subroutine of Shor's algorithm) to find $p_k$

ii) output $(p_k, 0)$

# Quantum problems

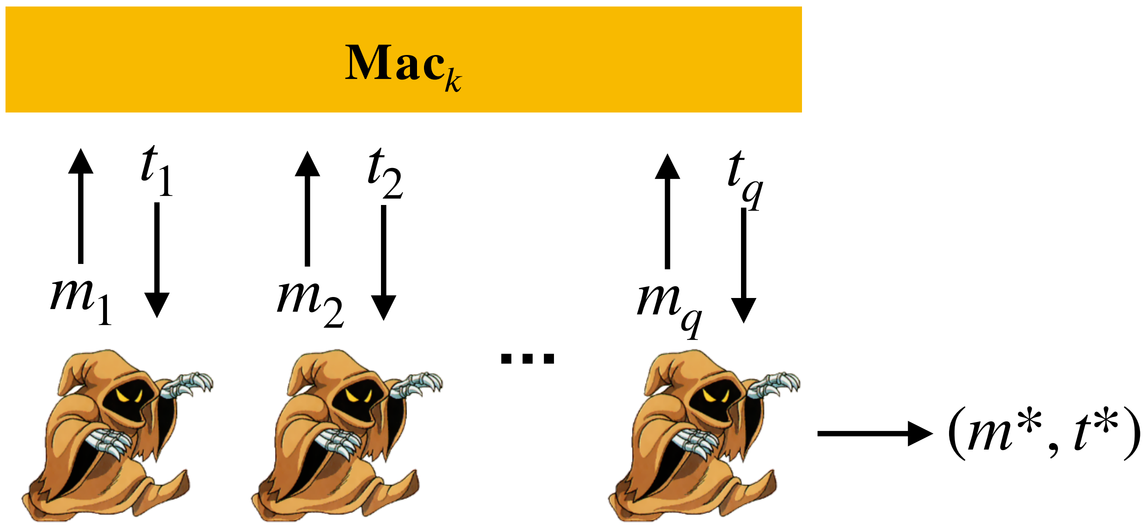



Success:

*i*) $m^* \neq m_i$ for all $i = 1,\ldots,q$

*ii*) $\mathbf{Mac}_k(m^*) = t^*$

# Quantum problems




Success:

$i)\ m^* \neq m_i$ for all $i = 1,\ldots,q$

$ii)\ \mathbf{Mac}_k(m^*) = t^*$

- No-cloning principle: can't keep a transcript
- Measurement causes disturbance!

# Results

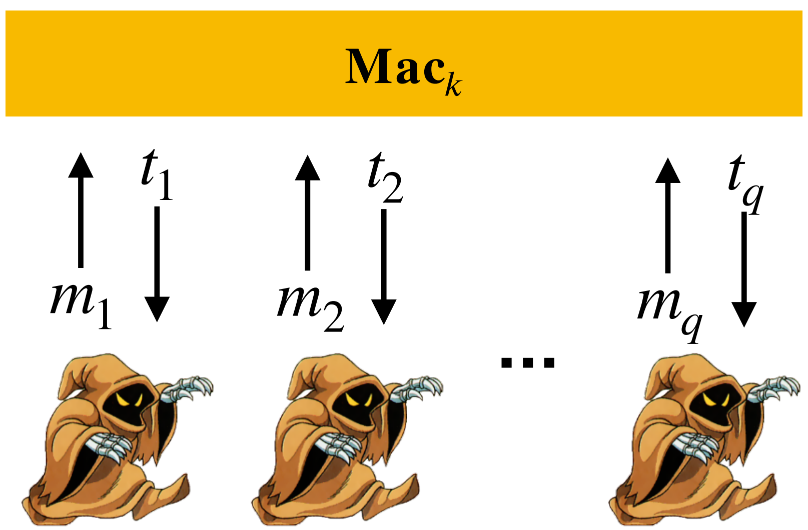
# Our results

- We study unforgeability under **quantum** chosen message attacks
- We propose a new security definition: **blind unforgeability (BU)**
- We exhibit a MAC that is secure under a previous definition by Boneh and Zhandry (Eurocrypt 2013) but clearly broken, and BU-insecure
- We characterize BU
  - It implies the previous definition
  - Random functions, Lamport signatures are BU secure
  - Hash-and-Mac/Hash-and-Sign preserves BU security for appropriate hash functions

# Boneh Zhandry unforgeability

Boneh and Zhandry (Eurocrypt 2013) propose:

Ask $q+1$ forgeries for $q$ queries!




$$\longrightarrow (m_1^*, t_1^*), (m_2^*, t_2^*), \ldots, (m_{q+1}^*, t_{q+1}^*)$$

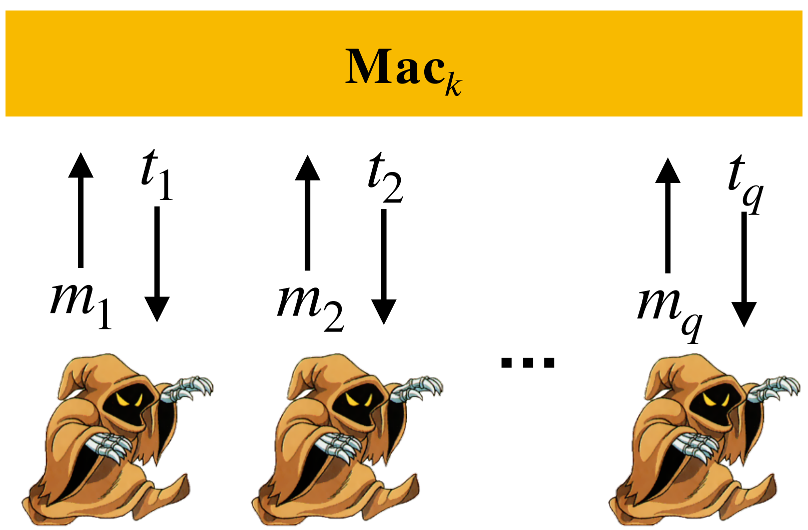
Success:

$$\mathbf{Mac}_k(m_i^*) = t_i^* \ \forall i = 1, \ldots, q+1$$

# Boneh Zhandry unforgeability

Boneh and Zhandry (Eurocrypt 2013) propose:

Ask $q+1$ forgeries for $q$ queries!




$\longrightarrow (m_1^*, t_1^*), (m_2^*, t_2^*), \ldots, (m_{q+1}^*, t_{q+1}^*)$

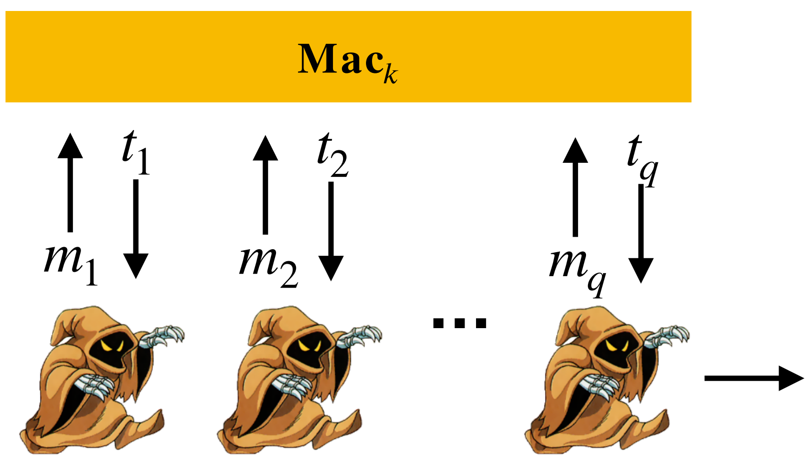
Success:

$\mathbf{Mac}_k(m_i^*) = t_i^* \ \forall i = 1,\ldots,q+1$

Has some nice properties:

- Equivalent to **UF-CMA** for classical oracle
- A random oracle is BZ-unforgeable (BZ '13)

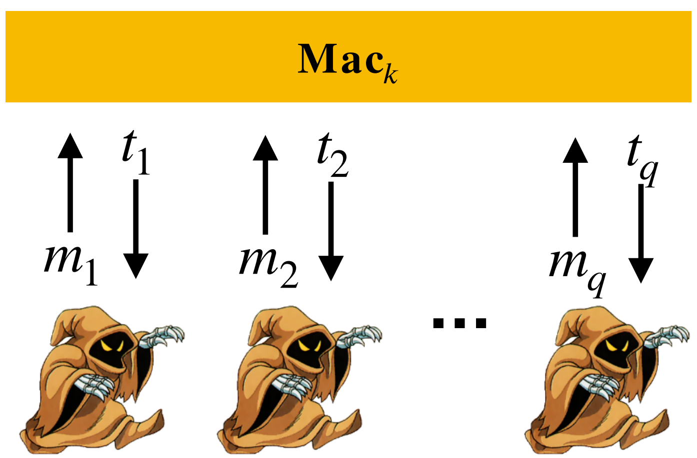
# The right definition?




$$\longrightarrow (m_1^*, t_1^*), (m_2^*, t_2^*), \ldots, (m_{q+1}^*, t_{q+1}^*)$$

Success:
$\mathbf{Mac}_k(m_i^*) = t_i^* \ \forall i = 1, \ldots, q+1$

# The right definition?



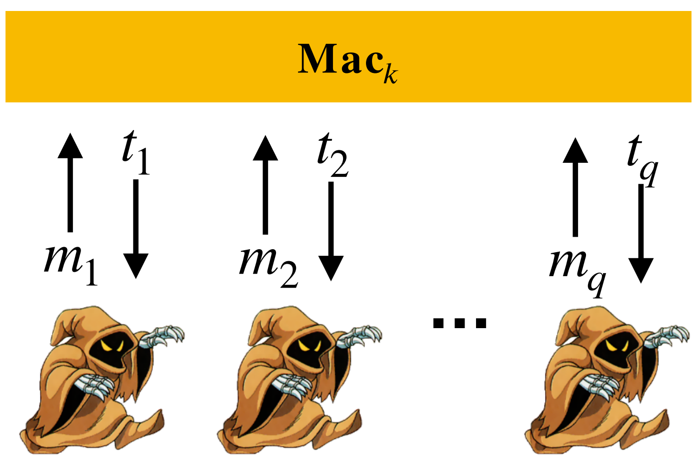

$$\longrightarrow (m_1^*, t_1^*), (m_2^*, t_2^*), \ldots, (m_{q+1}^*, t_{q+1}^*)$$

Success:
$\mathbf{Mac}_k(m_i^*) = t_i^* \ \forall i = 1,\ldots,q+1$

What if…

- an adversary has to fully measure many queries to generate one forgery? (no-cloning)

# The right definition?



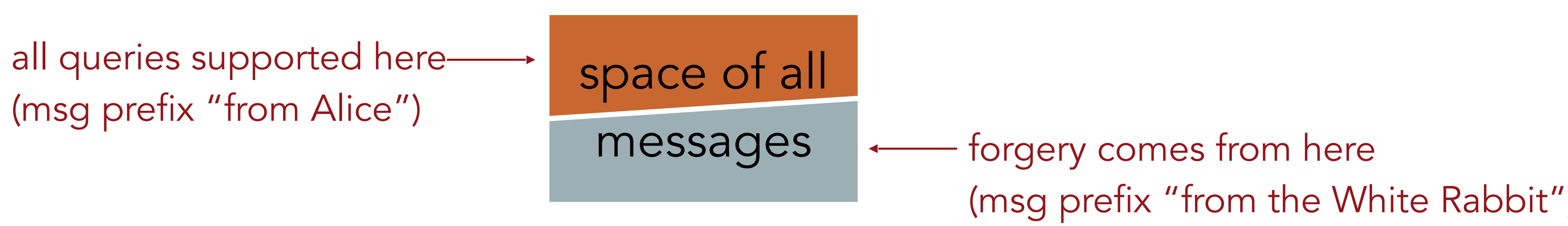

$\rightarrow (m_1^*, t_1^*), (m_2^*, t_2^*), \ldots, (m_{q+1}^*, t_{q+1}^*)$

Success:

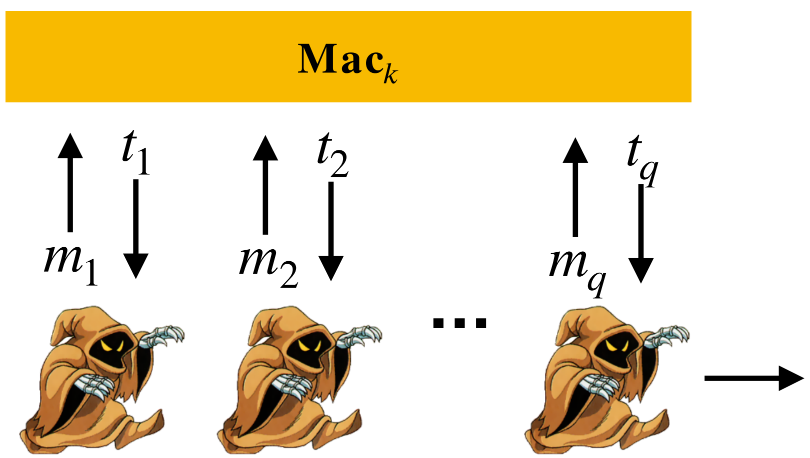
$\mathbf{Mac}_k(m_i^*) = t_i^* \; \forall i = 1,\ldots,q+1$

What if…

- an adversary has to fully measure many queries to generate one forgery? (no-cloning)
- an adversary "queries here, forges there"?



# The right definition?



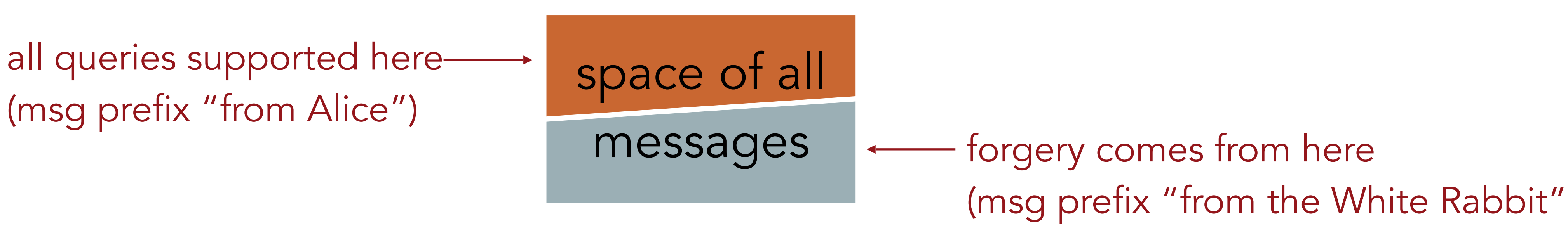

$$\longrightarrow (m_1^*, t_1^*), (m_2^*, t_2^*), \ldots, (m_{q+1}^*, t_{q+1}^*)$$

Success:

$\mathbf{Mac}_k(m_i^*) = t_i^* \ \forall i = 1,\ldots,q+1$

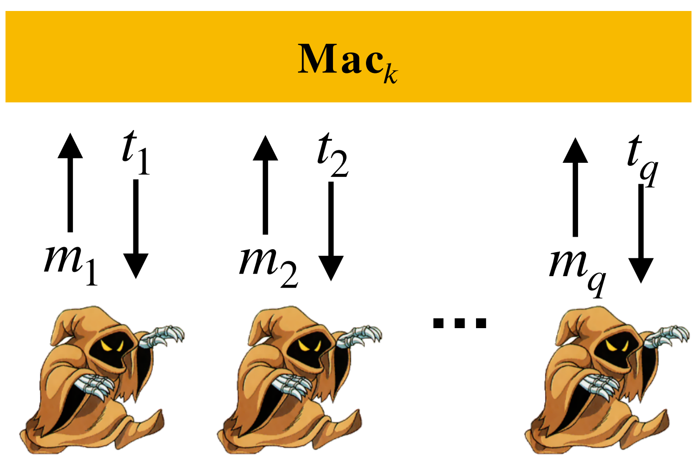
What if…

- an adversary has to fully measure many queries to generate one forgery? (no-cloning)
- an adversary "queries here, forges there"?




In fact, it seems like it should be ***easy*** to find examples like this!

# The right definition?



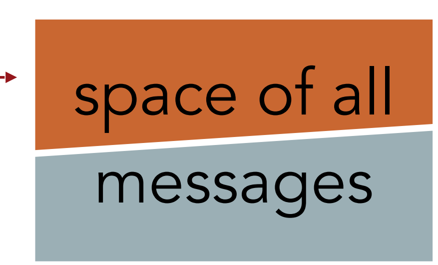

$\longrightarrow (m_1^*, t_1^*), (m_2^*, t_2^*), \ldots, (m_{q+1}^*, t_{q+1}^*)$

Success:
$\mathbf{Mac}_k(m_i^*) = t_i^* \ \forall i = 1,\ldots,q+1$

What if…

- an adversary has to fully measure many queries to generate one forgery? (no-cloning)
- an adversary "queries here, forges there"?

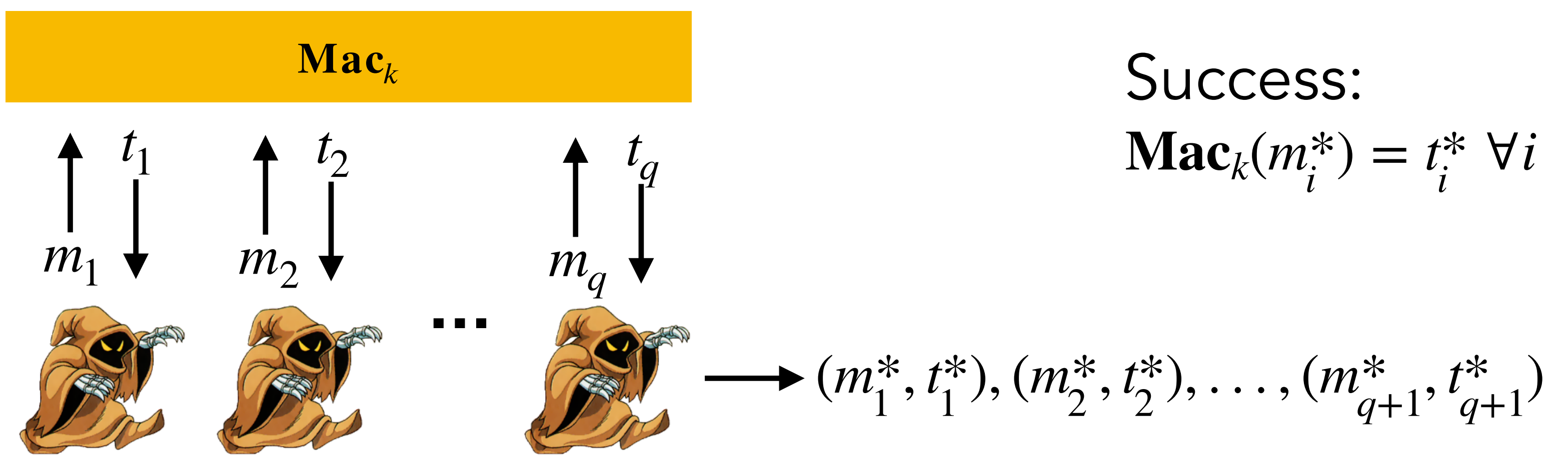
all queries supported here
(msg prefix "from Alice")




forgery comes from here
(msg prefix "from the White Rabbit")

In fact, it ~~seems like it should be~~ is not ***easy*** to find examples like this!

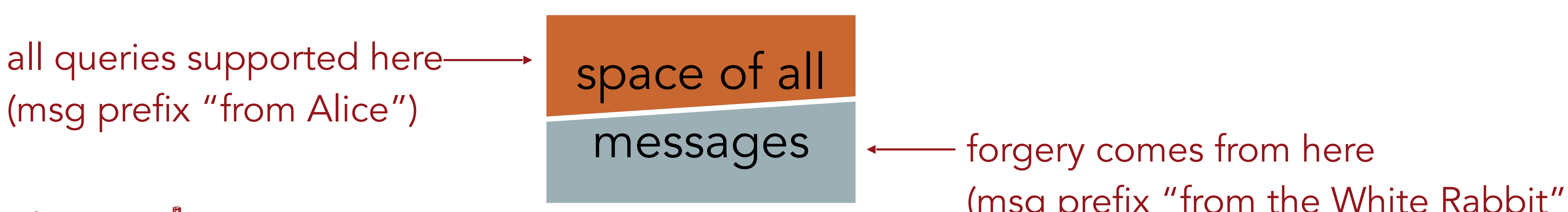
# The right definition?




Success:
$\mathbf{Mac}_k(m_i^*) = t_i^* \ \forall i = 1,\ldots,q+1$

What if…

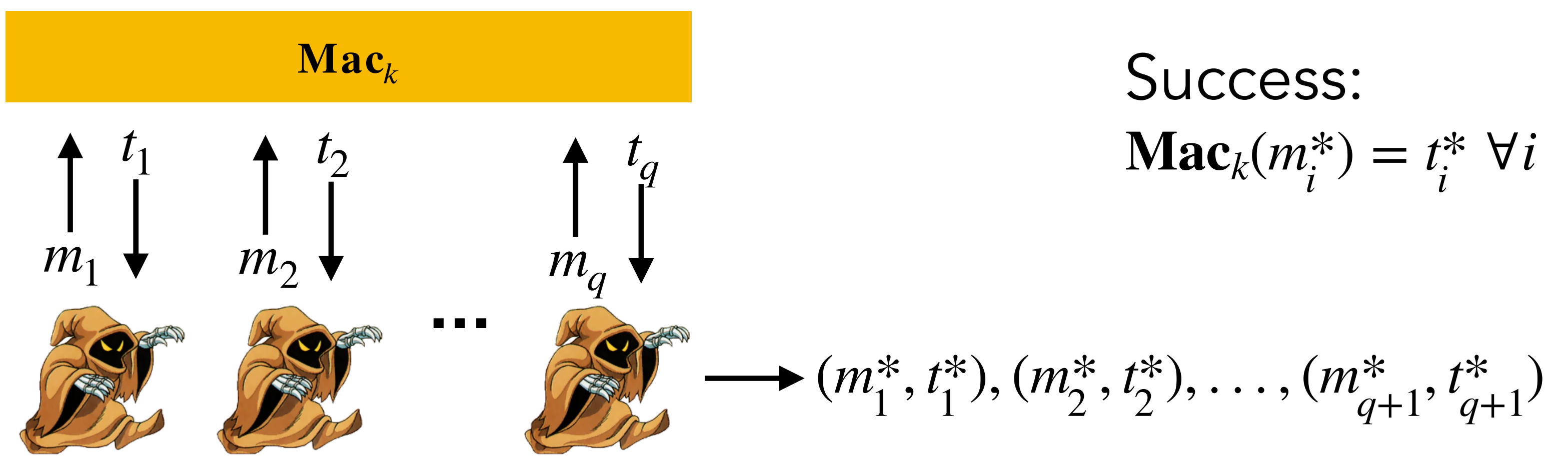
- an adversary has to fully measure many queries to generate one forgery? (no-cloning)
- an adversary "queries here, forges there"?




In fact, it ~~seems like it should be~~ is not ***easy*** to find examples like this!

One obstacle: "property finding" cannot be used.

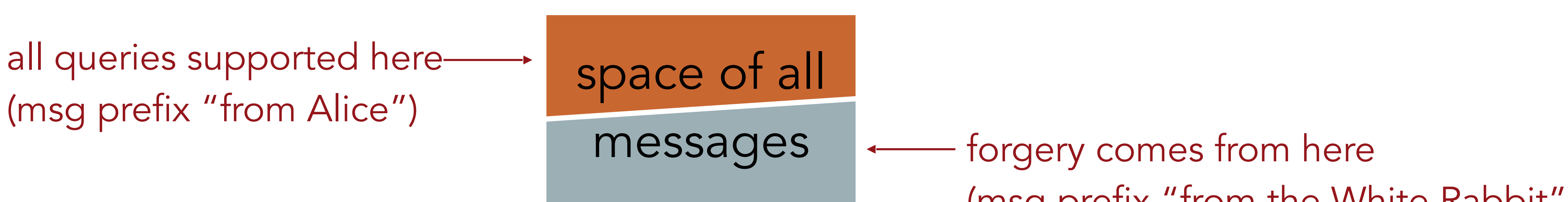
# The right definition?




Success:
$\mathbf{Mac}_k(m_i^*) = t_i^* \ \forall i = 1,\ldots,q+1$

What if…

- an adversary has to fully measure many queries to generate one forgery? (no-cloning)
- an adversary "queries here, forges there"?




In fact, it ~~seems like it should be~~ is not ***easy*** to find examples like this!

One obstacle: "property finding" cannot be used.

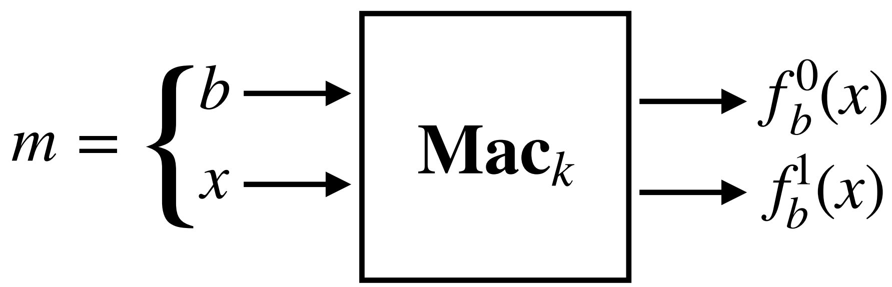
One-time Mac that's BZ secure, GYZ (Garg, Yuen&Zhandry, Crypto '17) insecure, assuming iO (Zhandry, Eurocrypt '19)

# A concrete example

A MAC that unconditionally “breaks” Boneh-Zhandry:

# A concrete example

A MAC that unconditionally "breaks" Boneh-Zhandry:




- $\hat{f}_b^i : \{0,1\}^n \to \{0,1\}^n$ random functions
- $f_0^0(x) = \hat{f}_0^0(x \bmod p)$ for random $p$, $f_0^1 = \hat{f}_0^1$
- $f_1^0 = \begin{cases} 0^n & x = p \\ \hat{f}_1^0(x) & \text{else} \end{cases}, f_1^1 \equiv 0^n$

# A concrete example

A MAC that unconditionally “breaks” Boneh-Zhandry:

Message space

Random periodic function shielded by a random function $b = 0$

Random function punctured at the period $b = 1$

# A concrete example

A MAC that unconditionally "breaks" Boneh-Zhandry:

Message space

- Random periodic function shielded by a random function — $b = 0$
- Random function punctured at the period — $b = 1$

Simple one-query attack:

i) Use period finding to find $p$, "ignoring" $f_0^1$

ii) output $(1p, 0^{2n})$

# A concrete example

A MAC that unconditionally “breaks” Boneh-Zhandry:

Message space

- Random periodic function shielded by a random function — $b = 0$
- Random function punctured at the period — $b = 1$

Simple one-query attack:

i) Use period finding to find $p$, “ignoring” $f_0^1$ $b = 0$

ii) output $(1p, 0^{2n})$ $b = 1$

# A concrete example

A MAC that unconditionally "breaks" Boneh-Zhandry:

Message space

Random periodic function shielded by a random function — $b = 0$

Random function punctured at the period — $b = 1$

Simple one-query attack:

i) Use period finding to find $p$, "ignoring" $f_0^1$

ii) output $(1p, 0^{2n})$

**Theorem (AMRS17).** There is no efficient quantum algorithm which query $\mathbf{Mac}_k$ once but output two distinct input-output pairs of $\mathbf{Mac}_k$.

# A concrete example

A MAC that unconditionally "breaks" Boneh-Zhandry:

Message space

- Random periodic function shielded by a random function — $b = 0$
- Random function punctured at the period — $b = 1$

Simple one-query attack:

i) Use period finding to find $p$, "ignoring" $f_0^1$

Key step: ignorance is necessary

ii) output $(1p, 0^{2n})$

**Theorem (AMRS17).** There is no efficient quantum algorithm which query $\mathbf{Mac}_k$ once but output two distinct input-output pairs of $\mathbf{Mac}_k$.

# New approach: Blind Unforgeability (BU)

**Problem:** how do we define unforgeability vs quantum?

# New approach: Blind Unforgeability (BU)

**Problem:** how do we define unforgeability vs quantum?

**A new approach:** “blind unforgeability.”

**Idea:** to test a forger…

- give it the oracle for the MAC, but “blind” it on some inputs;
- ask the adversary to forge on a blinded spot.

# New approach: Blind Unforgeability (BU)

**Problem:** how do we define unforgeability vs quantum?

**A new approach:** "blind unforgeability."

**Idea:** to test a forger…

- give it the oracle for the MAC, but "blind" it on some inputs;
- ask the adversary to forge on a blinded spot.

More formally: for $\mathbf{Mac}_k$

1. Select $B_\varepsilon \subset \{0,1\}^n$ by putting every $m \in B_\varepsilon$ independently with probability $\varepsilon$;
2. Define "blinded" oracle: $B_\epsilon \mathbf{Mac}_k : m \mapsto \begin{cases} \mathbf{Mac}_k(m) & m \notin B_\epsilon \\ \perp & m \in B_\epsilon \end{cases}$

# New approach: Blind Unforgeability (BU)

**Problem:** how do we define unforgeability vs quantum?

**A new approach:** "blind unforgeability."

**Idea:** to test a forger…

- give it the oracle for the MAC, but "blind" it on some inputs;
- ask the adversary to forge on a blinded spot.

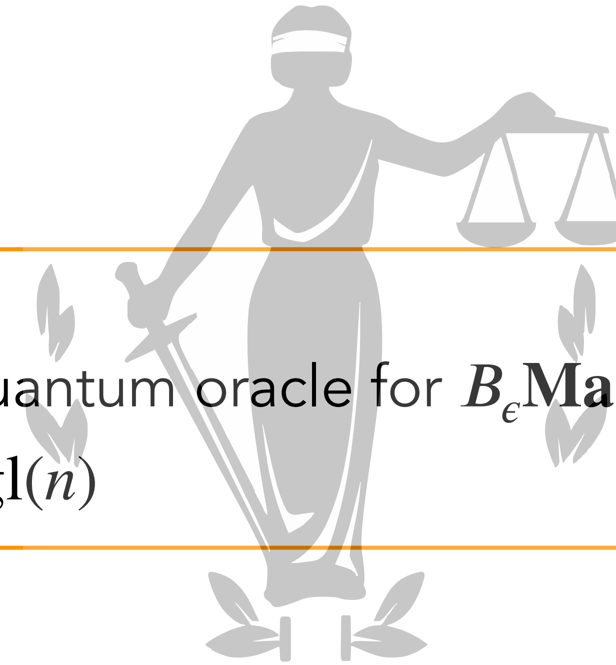
More formally: for $\mathbf{Mac}_k$

1. Select $B_\varepsilon \subset \{0,1\}^n$ by putting every $m \in B_\varepsilon$ independently with probability $\varepsilon$;
2. Define "blinded" oracle: $B_\epsilon \mathbf{Mac}_k : m \mapsto \begin{cases} \mathbf{Mac}_k(m) & m \notin B_\epsilon \\ \perp & m \in B_\epsilon \end{cases}$

Definition (Blind-Unforgeability):
A MAC $\mathbf{Mac}_k$ is blind-unforgeable if for every adversary $\mathscr{A}$ with a quantum oracle for $B_\epsilon \mathbf{Mac}_k$ ,

$$\mathbb{P}\left[(m, \mathbf{Mac}_k(m) \leftarrow \mathscr{A}^{B_\varepsilon \mathbf{Mac}_k} \text{ and } m \in B_\varepsilon\right] = \mathrm{negl}(n)$$

# Blind Unforgeability



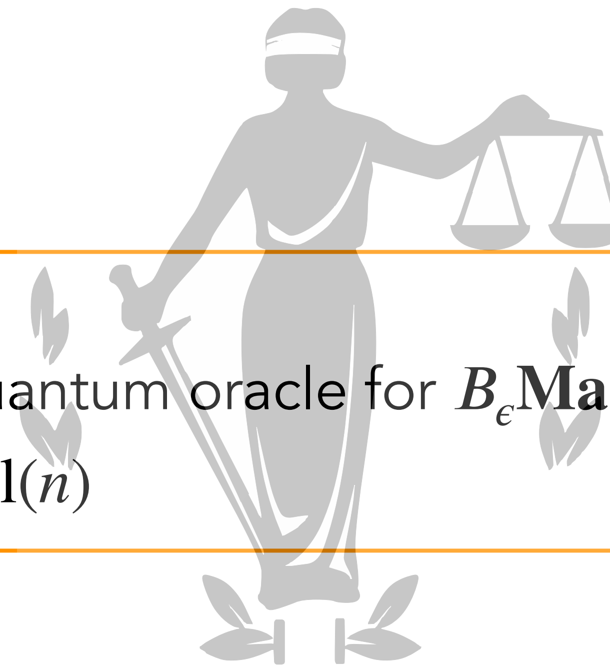
Definition (Blind-Unforgeability):
A MAC $\mathbf{Mac}_k$ is blind-unforgeable if for every adversary $\mathscr{A}$ with a quantum oracle for $B_\epsilon\mathbf{Mac}_k$ ,

$$\mathbb{P}\left[(y, \mathbf{Mac}_k(y) \leftarrow \mathscr{A}^{B_\varepsilon \mathbf{Mac}_k} \text{ and } y \in B_\varepsilon\right] = \mathrm{negl}(n)$$

**Does this work?**

- equivalent to **UF-CMA** in classical setting;

# Blind Unforgeability



Definition (Blind-Unforgeability):

A MAC $\mathbf{Mac}_k$ is blind-unforgeable if for every adversary $\mathscr{A}$ with a quantum oracle for $B_\epsilon \mathbf{Mac}_k$ ,

$$\mathbb{P}\left[(y, \mathbf{Mac}_k(y) \leftarrow \mathscr{A}^{B_\varepsilon \mathbf{Mac}_k} \text{ and } y \in B_\varepsilon\right] = \mathrm{negl}(n)$$

**Does this work?**

- equivalent to **UF-CMA** in classical setting;
- random functions satisfy it;

# Blind Unforgeability

Definition (Blind-Unforgeability):

A MAC $\mathbf{Mac}_k$ is blind-unforgeable if for every adversary $\mathscr{A}$ with a quantum oracle for $B_\epsilon \mathbf{Mac}_k$ ,

$$\mathbb{P}\left[(y, \mathbf{Mac}_k(y)) \leftarrow \mathscr{A}^{B_\varepsilon \mathbf{Mac}_k} \text{ and } y \in B_\varepsilon\right] = \mathrm{negl}(n)$$

**Does this work?**

- equivalent to **UF-CMA** in classical setting;
- random functions satisfy it;
- Implies previous defintion by Boneh and Zhandry;

# Blind Unforgeability

Definition (Blind-Unforgeability):
A MAC $\mathbf{Mac}_k$ is blind-unforgeable if for every adversary $\mathscr{A}$ with a quantum oracle for $B_\epsilon\mathbf{Mac}_k$ ,

$$\mathbb{P}\left[(y, \mathbf{Mac}_k(y) \leftarrow \mathscr{A}^{B_\varepsilon \mathbf{Mac}_k} \text{ and } y \in B_\varepsilon\right] = \text{negl}(n)$$

**Does this work?**

- equivalent to **UF-CMA** in classical setting;
- random functions satisfy it;
- Implies previous defintion by Boneh and Zhandry;
- classifies the examples we have seen thus far correctly.

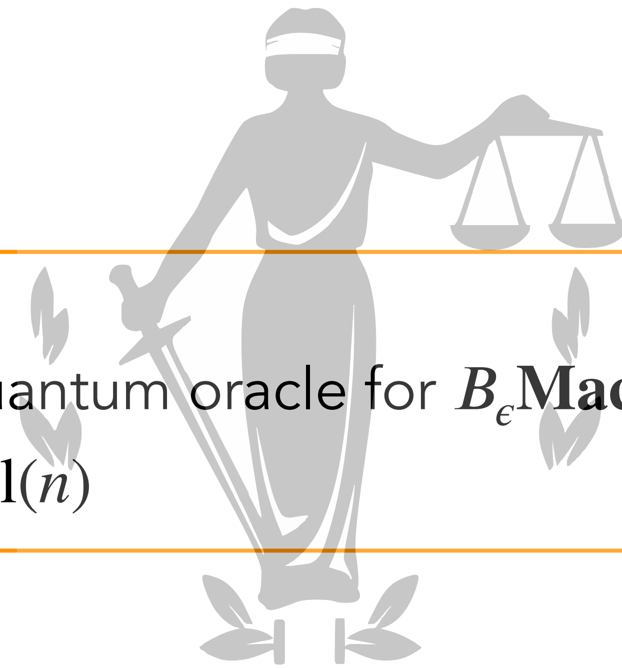
---

1.

1. prepare: $m_1 = \sum_{m \in \{0,1\}^n} |m\rangle |0\rangle$ ;
2. query
3. measure

Output: $(m, B_\varepsilon \mathbf{Mac}_k(m))$ for random $m$.

# Blind Unforgeability



Definition (Blind-Unforgeability):
A MAC $\mathbf{Mac}_k$ is blind-unforgeable if for every adversary $\mathscr{A}$ with a quantum oracle for $B_\epsilon \mathbf{Mac}_k$ ,

$$\mathbb{P}\left[(y, \mathbf{Mac}_k(y) \leftarrow \mathscr{A}^{B_\varepsilon \mathbf{Mac}_k} \text{ and } y \in B_\varepsilon\right] = \mathrm{negl}(n)$$

**Does this work?**

- equivalent to **UF-CMA** in classical setting;
- random functions satisfy it;
- Implies previous defintion by Boneh and Zhandry;
- classifies the examples we have seen thus far correctly.

---

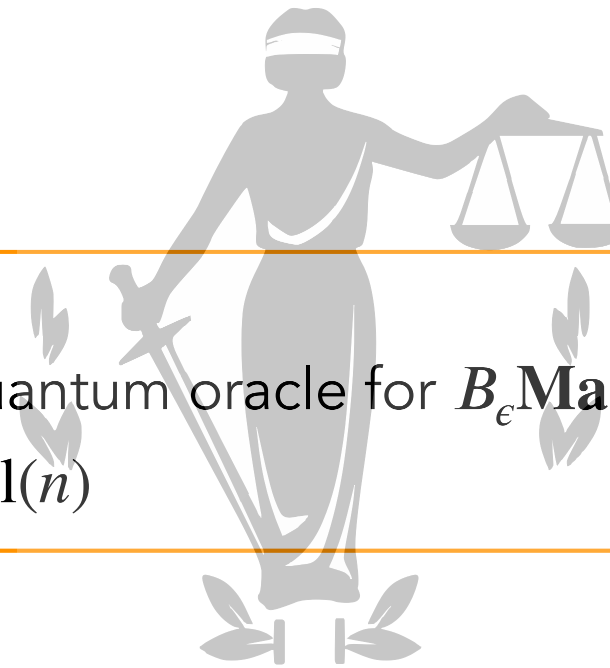
1.

1. prepare: $m_1 = \sum_{m \in \{0,1\}^n} |m\rangle|0\rangle$ ;
2. query
3. measure

Output: $(m, B_\varepsilon \mathbf{Mac}_k(m))$ for random $m$.

Check, e.g., for random functions:

- if oracle is blinded…
- … $\mathbf{Mac}_k(m)$ for blinded $m$ is *independent* of post-query state,
- this adversary fails.



# Blind Unforgeability

Definition (Blind-Unforgeability):
A MAC $\mathbf{Mac}_k$ is blind-unforgeable if for every adversary $\mathscr{A}$ with a quantum oracle for $B_\epsilon \mathbf{Mac}_k$ ,

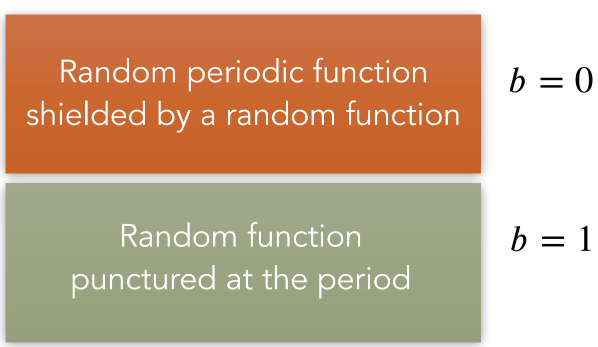
$$\mathbb{P}\left[(y, \mathbf{Mac}_k(y)) \leftarrow \mathscr{A}^{B_\varepsilon \mathbf{Mac}_k} \text{ and } y \in B_\varepsilon\right] = \mathrm{negl}(n)$$

**Does this work?**

- equivalent to **UF-CMA** in classical setting;
- random functions satisfy it;
- Implies previous defintion by Boneh and Zhandry;
- classifies the examples we have seen thus far correctly.

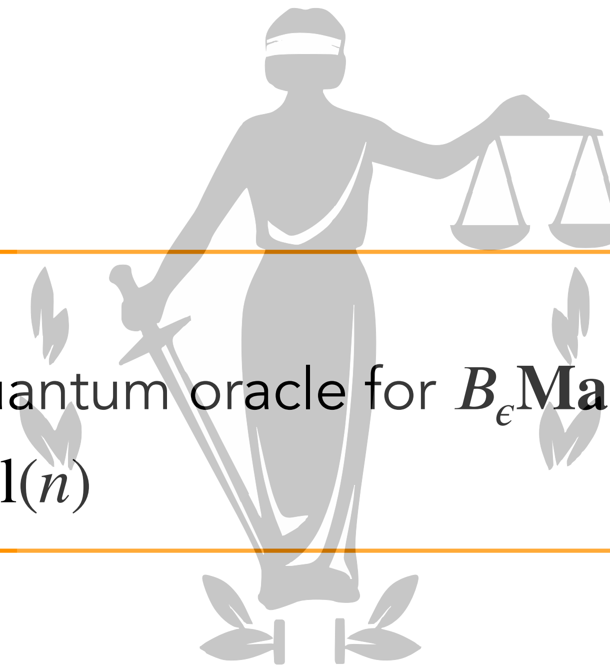
---

2.




One-query attack: Find period in orange part,
forge in olive part.

# Blind Unforgeability



Definition (Blind-Unforgeability):

A MAC $\mathbf{Mac}_k$ is blind-unforgeable if for every adversary $\mathscr{A}$ with a quantum oracle for $B_\epsilon \mathbf{Mac}_k$ ,

$$\mathbb{P}\left[(y, \mathbf{Mac}_k(y)) \leftarrow \mathscr{A}^{B_\varepsilon \mathbf{Mac}_k} \text{ and } y \in B_\varepsilon\right] = \mathrm{negl}(n)$$

**Does this work?**

- equivalent to **UF-CMA** in classical setting;
- random functions satisfy it;
- Implies previous defintion by Boneh and Zhandry;
- classifies the examples we have seen thus far correctly.

---

2.

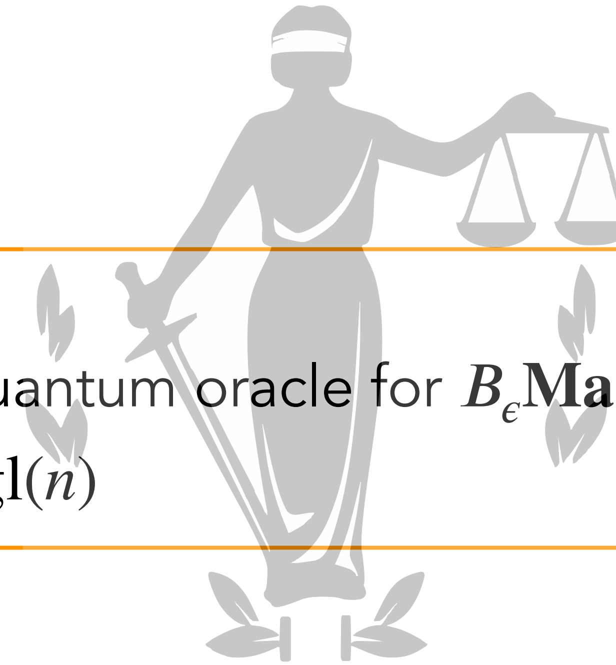
| | |
|---|---|
| Random periodic function shielded by a random function | $b = 0$ |
| Random function punctured at the period | $b = 1$ |

Check, say for $\varepsilon = 0.0001$,

- *oracle is blinded only on few random inputs…*
- *…post-query state won't change too much;*
- $(1p,0)$ is blinded with *independent* probability $\varepsilon$;
- so this adversary succeeds!

One-query attack: Find period in orange part, forge in olive part.

# Blind Unforgeability



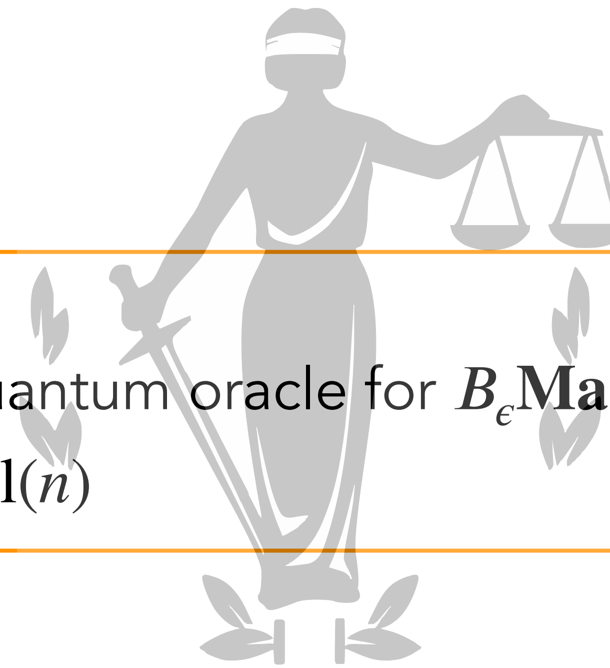
Definition (Blind-Unforgeability):

A MAC $\mathbf{Mac}_k$ is blind-unforgeable if for every adversary $\mathscr{A}$ with a quantum oracle for $B_\epsilon \mathbf{Mac}_k$ ,

$$\mathbb{P}\left[(y, \mathbf{Mac}_k(y) \leftarrow \mathscr{A}^{B_\varepsilon \mathbf{Mac}_k} \text{ and } y \in B_\varepsilon\right] = \mathrm{negl}(n)$$

**Additional results:**

# Blind Unforgeability



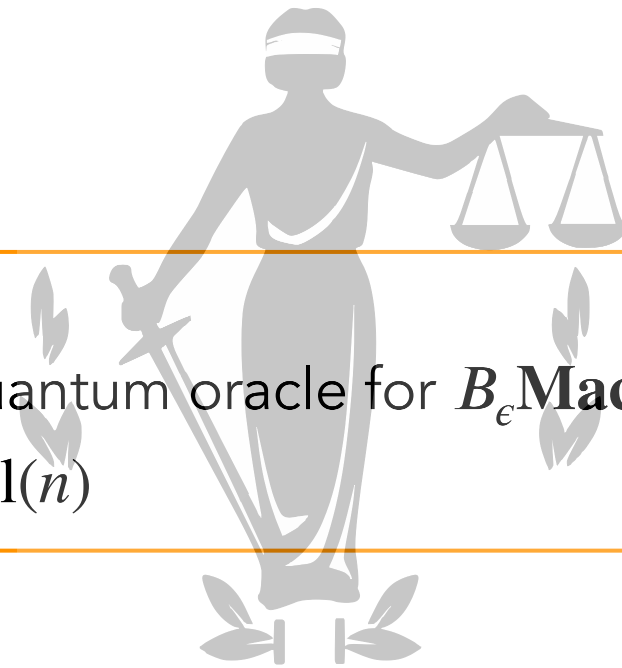
Definition (Blind-Unforgeability):
A MAC $\mathbf{Mac}_k$ is blind-unforgeable if for every adversary $\mathscr{A}$ with a quantum oracle for $B_\epsilon \mathbf{Mac}_k$ ,

$$\mathbb{P}\left[(y, \mathbf{Mac}_k(y) \leftarrow \mathscr{A}^{B_\varepsilon \mathbf{Mac}_k} \text{ and } y \in B_\varepsilon\right] = \mathrm{negl}(n)$$

**Additional results:**

- Bernoulli-preserving hash function: generalizes collision resistance to quantum, strengthens collapsingness

# Blind Unforgeability



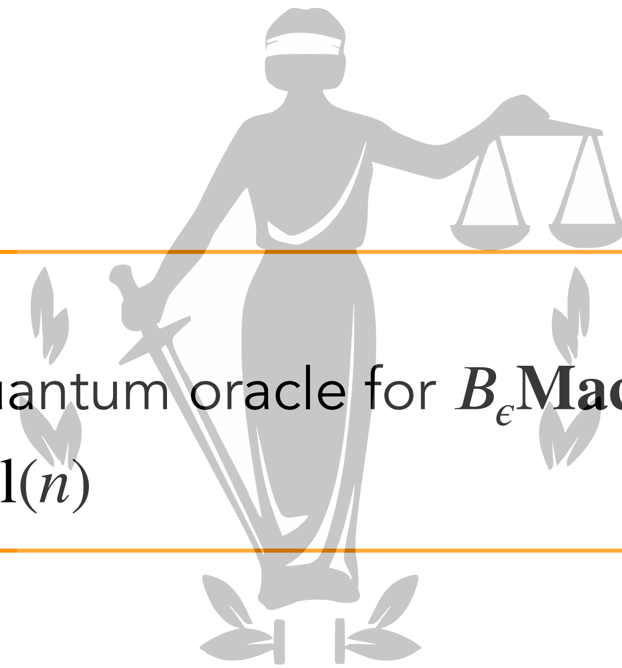
Definition (Blind-Unforgeability):
A MAC $\mathbf{Mac}_k$ is blind-unforgeable if for every adversary $\mathscr{A}$ with a quantum oracle for $B_\epsilon \mathbf{Mac}_k$ ,

$$\mathbb{P}\left[(y, \mathbf{Mac}_k(y)) \leftarrow \mathscr{A}^{B_\varepsilon \mathbf{Mac}_k} \text{ and } y \in B_\varepsilon\right] = \mathrm{negl}(n)$$

**Additional results:**

- Bernoulli-preserving hash function: generalizes collision resistance to quantum, strengthens collapsingness
- Hash-and-MAC is BU-secure when using Bernoulli-preserving hash function

# Blind Unforgeability



Definition (Blind-Unforgeability):

A MAC $\mathbf{Mac}_k$ is blind-unforgeable if for every adversary $\mathscr{A}$ with a quantum oracle for $B_\epsilon \mathbf{Mac}_k$ ,

$$\mathbb{P}\left[(y, \mathbf{Mac}_k(y) \leftarrow \mathscr{A}^{B_\varepsilon \mathbf{Mac}_k} \text{ and } y \in B_\varepsilon\right] = \mathrm{negl}(n)$$

**Additional results:**

- Bernoulli-preserving hash function: generalizes collision resistance to quantum, strengthens collapsingness
- Hash-and-MAC is BU-secure when using Bernoulli-preserving hash function
- A construction of a collapsing hash function based on LWE by Unruh (ASIACRYPT 16) is actually even Bernoulli-preserving

# Blind Unforgeability

Definition (Blind-Unforgeability):

A MAC $\mathbf{Mac}_k$ is blind-unforgeable if for every adversary $\mathscr{A}$ with a quantum oracle for $B_\epsilon\mathbf{Mac}_k$ ,

$$\mathbb{P}\left[(y, \mathbf{Mac}_k(y) \leftarrow \mathscr{A}^{B_\varepsilon \mathbf{Mac}_k} \text{ and } y \in B_\varepsilon\right] = \mathrm{negl}(n)$$

**Additional results:**

- Bernoulli-preserving hash function: generalizes collision resistance to quantum, strengthens collapsingness
- Hash-and-MAC is BU-secure when using Bernoulli-preserving hash function
- A construction of a collapsing hash function based on LWE by Unruh (ASIACRYPT 16) is actually even Bernoulli-preserving
- Lamport signatures are 1-BU in the quantum random oracle model

# Blind Unforgeability

Definition (Blind-Unforgeability):
A MAC $\mathbf{Mac}_k$ is blind-unforgeable if for every adversary $\mathscr{A}$ with a quantum oracle for $B_\epsilon \mathbf{Mac}_k$ ,

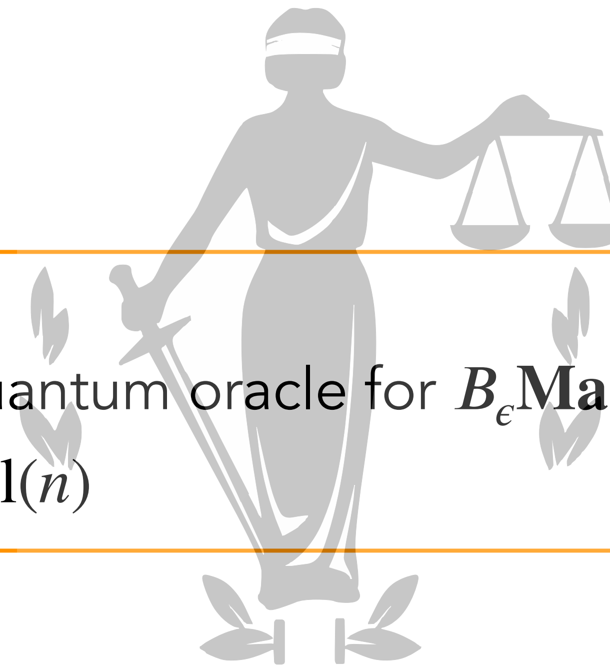
$$\mathbb{P}\left[(y, \mathbf{Mac}_k(y) \leftarrow \mathscr{A}^{B_\varepsilon \mathbf{Mac}_k} \text{ and } y \in B_\varepsilon\right] = \mathrm{negl}(n)$$

**Additional results:**

- Bernoulli-preserving hash function: generalizes collision resistance to quantum, strengthens collapsingness
- Hash-and-MAC is BU-secure when using Bernoulli-preserving hash function
- A construction of a collapsing hash function based on LWE by Unruh (ASIACRYPT 16) is actually even Bernoulli-preserving
- Lamport signatures are 1-BU in the quantum random oracle model

**Tools:**

# Blind Unforgeability



Definition (Blind-Unforgeability):
A MAC $\mathbf{Mac}_k$ is blind-unforgeable if for every adversary $\mathscr{A}$ with a quantum oracle for $B_\epsilon \mathbf{Mac}_k$ ,

$$\mathbb{P}\left[(y, \mathbf{Mac}_k(y)) \leftarrow \mathscr{A}^{B_\varepsilon \mathbf{Mac}_k} \text{ and } y \in B_\varepsilon\right] = \mathrm{negl}(n)$$

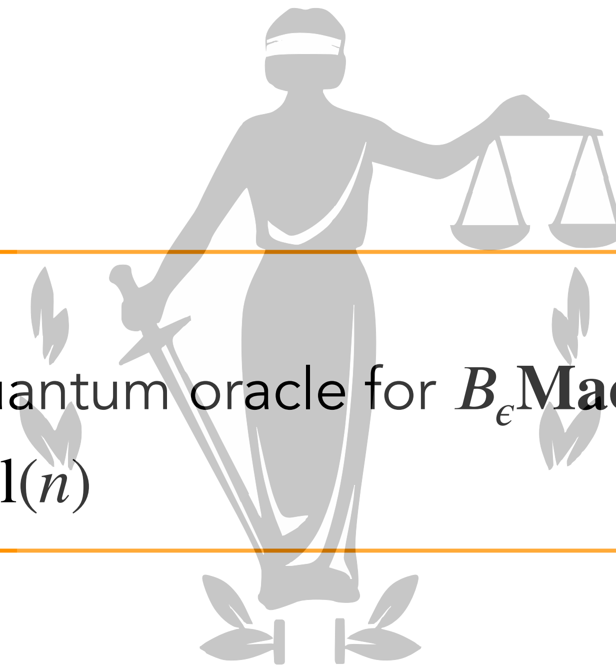
**Additional results:**

- Bernoulli-preserving hash function: generalizes collision resistance to quantum, strengthens collapsingness
- Hash-and-MAC is BU-secure when using Bernoulli-preserving hash function
- A construction of a collapsing hash function based on LWE by Unruh (ASIACRYPT 16) is actually even Bernoulli-preserving
- Lamport signatures are 1-BU in the quantum random oracle model

**Tools:**

- A simulation lemma that relates an adversary's performance in the blinded and unblinded cases

# Blind Unforgeability



Definition (Blind-Unforgeability):

A MAC $\mathbf{Mac}_k$ is blind-unforgeable if for every adversary $\mathscr{A}$ with a quantum oracle for $B_\epsilon \mathbf{Mac}_k$ ,

$$\mathbb{P}\left[(y, \mathbf{Mac}_k(y) \leftarrow \mathscr{A}^{B_\varepsilon \mathbf{Mac}_k} \text{ and } y \in B_\varepsilon\right] = \mathrm{negl}(n)$$

**Additional results:**

- Bernoulli-preserving hash function: generalizes collision resistance to quantum, strengthens collapsingness
- Hash-and-MAC is BU-secure when using Bernoulli-preserving hash function
- A construction of a collapsing hash function based on LWE by Unruh (ASIACRYPT 16) is actually even Bernoulli-preserving
- Lamport signatures are 1-BU in the quantum random oracle model

**Tools:**

- A simulation lemma that relates an adversary's performance in the blinded and unblinded cases
- Zhandry's superposition representation of quantum random oracles

# Summary, open questions

**Summary:**

- We exhibit a MAC that is secure according to a definition by Boneh and Zhandry but allows for an intuitive forgery attack.
- We propose a replacement definition: Blind Unforgeability
- Blind unforgeability has a lot of nice properties and classifies all known examples correctly.

**Open questions:**

- The security game for blind unforgeability is not natural. Can this be fixed?
- Are popular schemes (MACs and DSS) blind-unforgeable? We only have NMAC, HMAC and Lamport in the QROM for now…