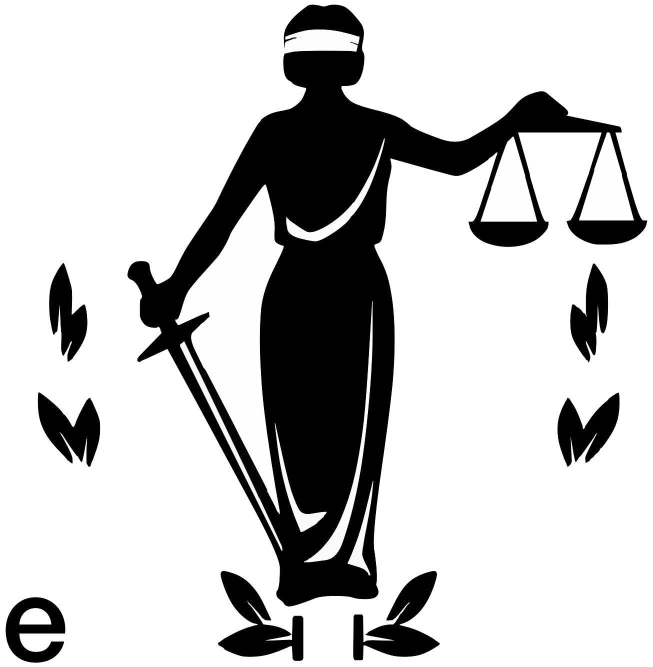


Quantum secure message authentication via blind-unforgeability

Christian Majenz

Joint work with Gorjan Alagic, Alexander Russell and Fang Song

QCrypt 2018, Shanghai, China

QuSoft Research Center for Quantum Software

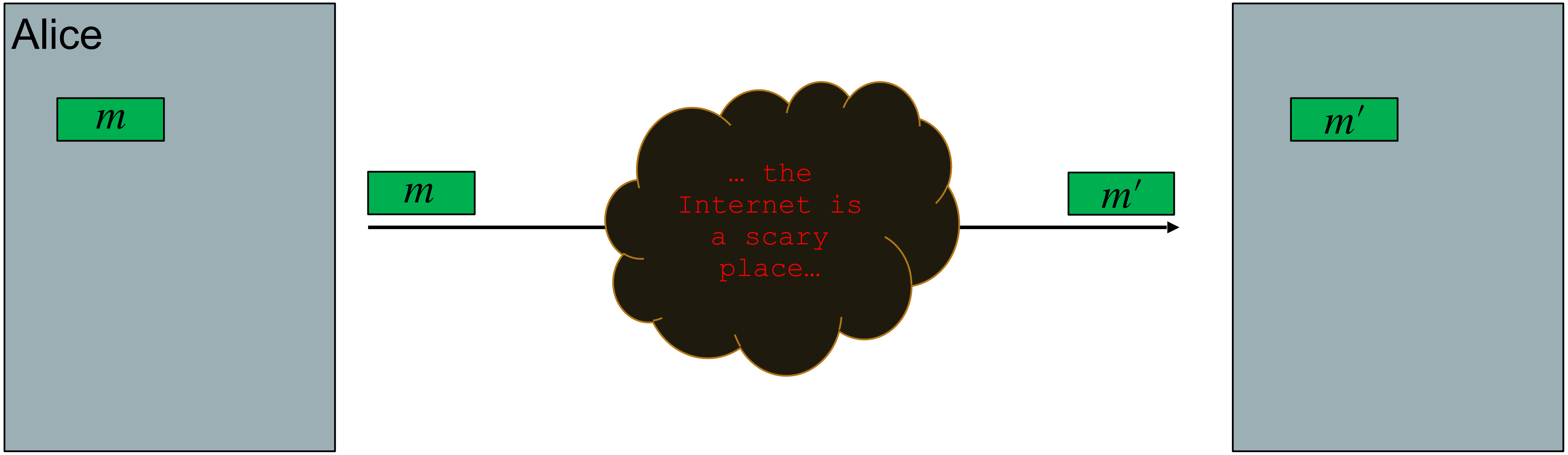
UCONN

Portland State University

Joint Center for Quantum Information and Computer Science

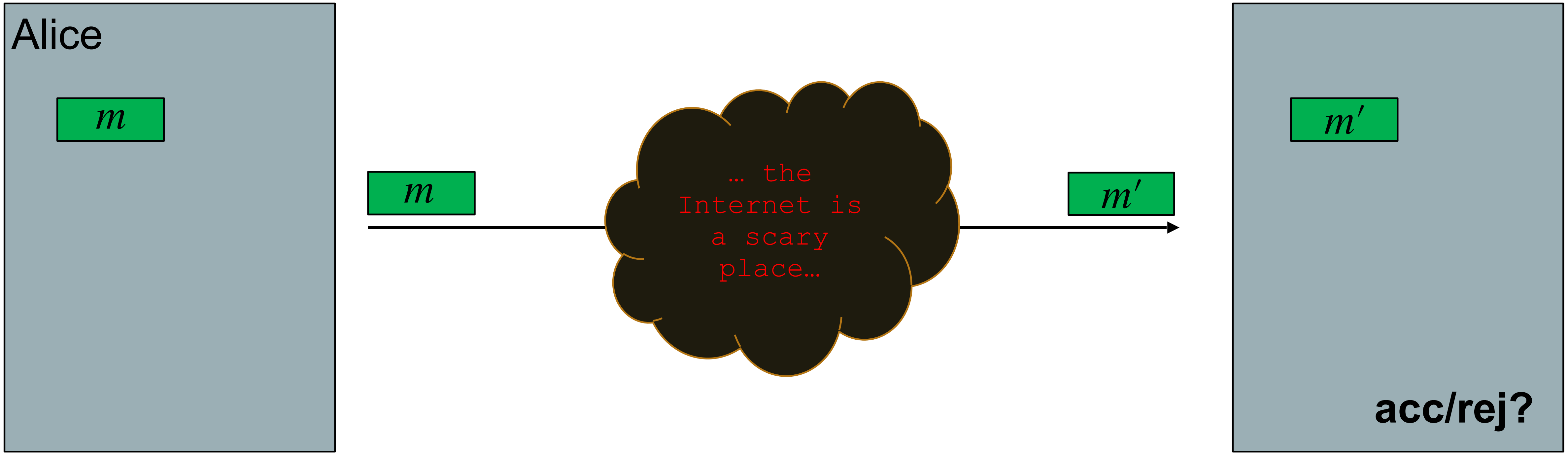
Message authentication

Message authentication



Message authentication

Problem: how can Bob check if a message came from Alice and is unchanged?



Message authentication

Problem: how can Bob check if a message came from Alice and is unchanged?

Solution: message authentication code (MAC) (some efficient function **Mac**)

Message authentication

Problem: how can Bob check if a message came from Alice and is unchanged?

Solution: message authentication code (MAC) (some efficient function **Mac**)

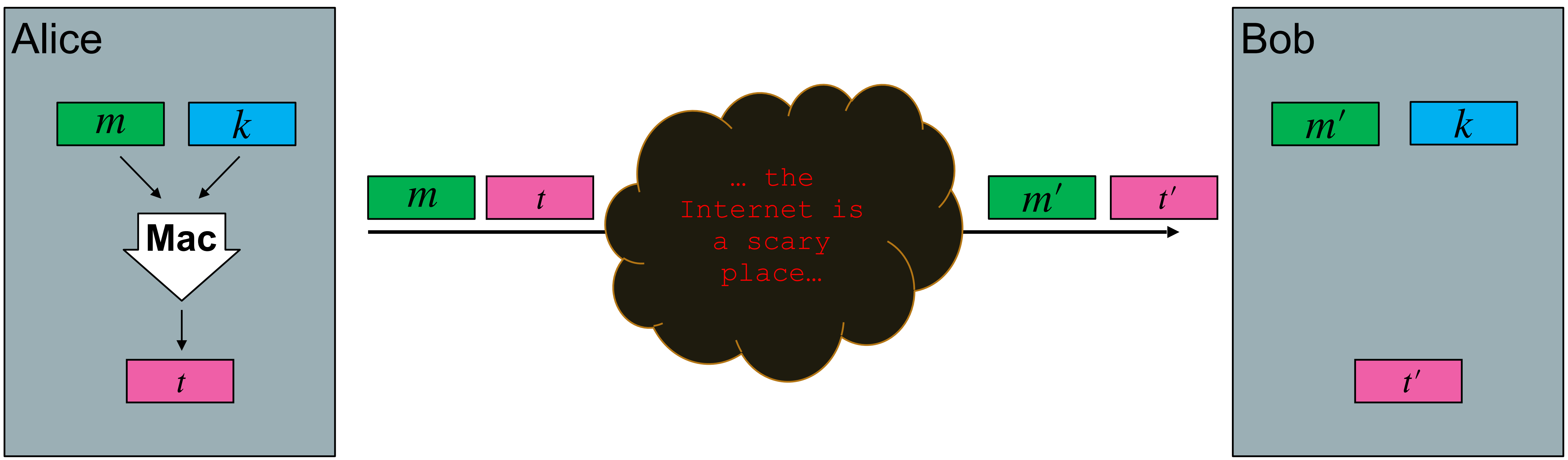
Message authentication

Problem: how can Bob check if a message came from Alice and is unchanged?

Solution: message authentication code (MAC) (some efficient function **Mac**)

Message authentication

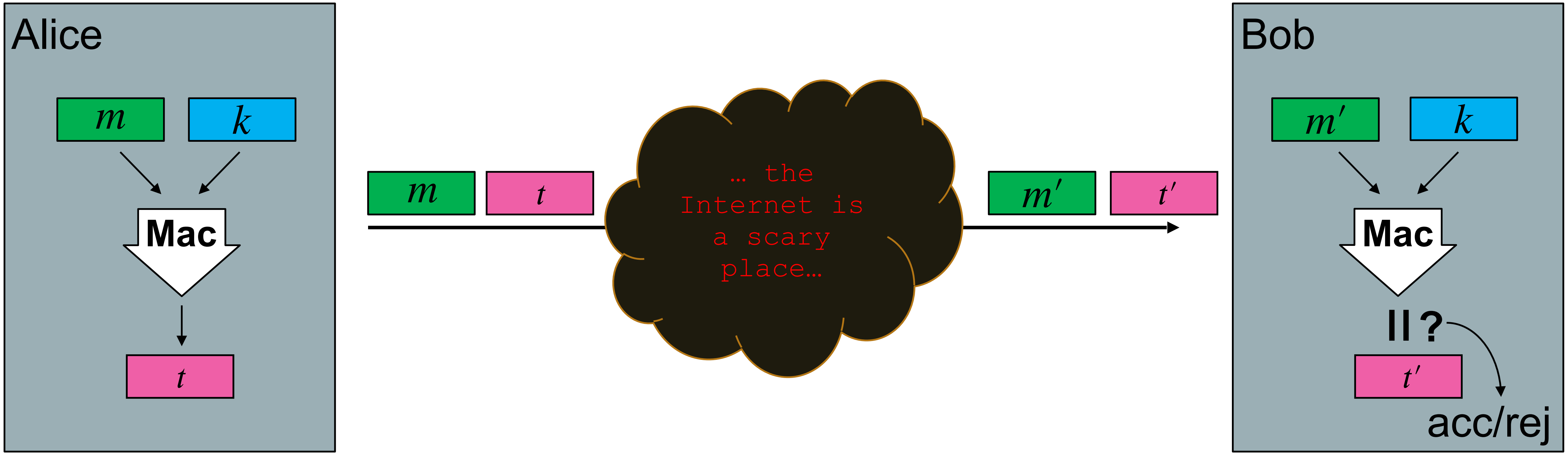
Problem: how can Bob check if a message came from Alice and is unchanged?
Solution: message authentication code (MAC) (some efficient function **Mac**)



Message authentication

Problem: how can Bob check if a message came from Alice and is unchanged?

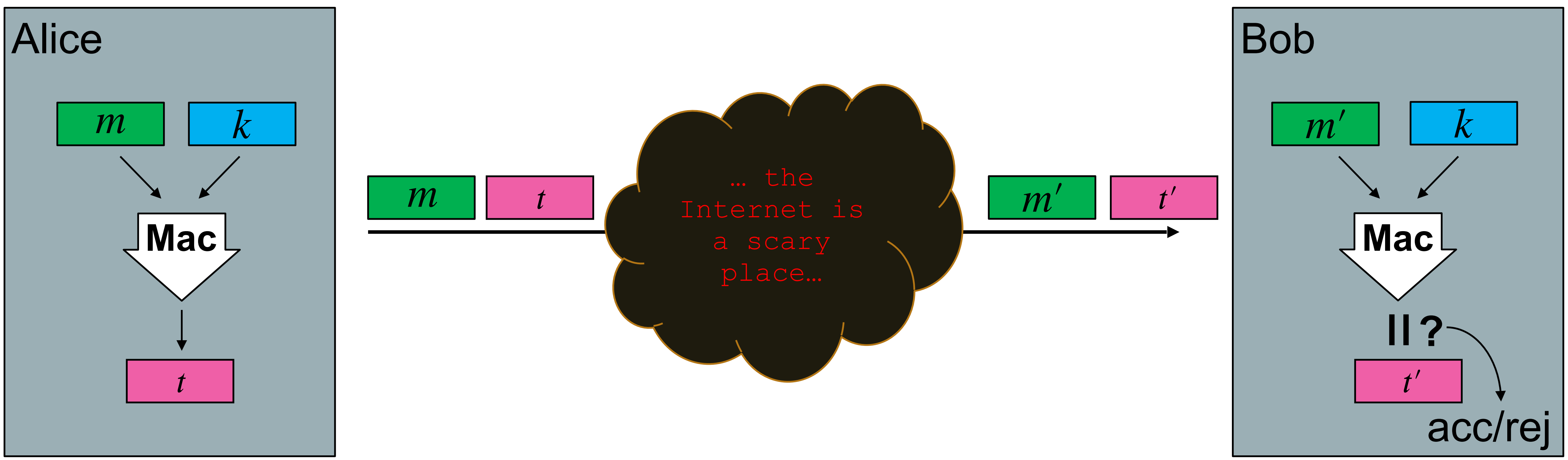
Solution: message authentication code (MAC) (some efficient function **Mac**)



Message authentication

Problem: how can Bob check if a message came from Alice and is unchanged?

Solution: message authentication code (MAC) (some efficient function **Mac**)



Note: Bob is only checking *consistency with the function .*

Message authentication

What properties should a MAC satisfy to be secure?

Message authentication

What properties should a MAC satisfy to be secure?

What are we worried about? Forgeries!

Message authentication

What properties should a MAC satisfy to be secure?

What are we worried about? Forgeries!

- plain forgery:

$\longrightarrow (m,\ \mathbf{Mac}_k(m))$

Message authentication

What properties should a MAC satisfy to be secure?

What are we worried about? Forgeries!

- plain forgery:

 $\longrightarrow (m,\ \mathbf{Mac}_k(m))$

- "malleability" attacks:

$(m,\ \mathbf{Mac}_k(m)) \longrightarrow$  $\longrightarrow (m',\ \mathbf{Mac}_k(m'))$

Message authentication

What properties should a MAC satisfy to be secure?

What are we worried about? Forgeries!

- plain forgery:

 $\longrightarrow (m,\ \mathbf{Mac}_k(m))$

- "malleability" attacks:

$(m,\ \mathbf{Mac}_k(m)) \longrightarrow$  $\longrightarrow (m',\ \mathbf{Mac}_k(m'))$

- using an oracle to produce a fresh forgery (most general attack):

$\mathbf{Mac}_k$

 $\longrightarrow$ (fresh)

Message authentication

What properties should a MAC satisfy to be secure?

What are we worried about? Forgeries!

- plain forgery:

$\longrightarrow (m,\ \mathbf{Mac}_k(m))$

- “malleability” attacks:

$(m,\ \mathbf{Mac}_k(m)) \longrightarrow$

$\longrightarrow (m',\ \mathbf{Mac}_k(m'))$

- using an oracle to produce a fresh forgery (most general attack):

$\boxed{\mathbf{Mac}_k}$

$\longrightarrow$ (fresh)

Key property: ***unpredictability*** of $\mathbf{Mac}_k$.

Classical security: Unforgeability

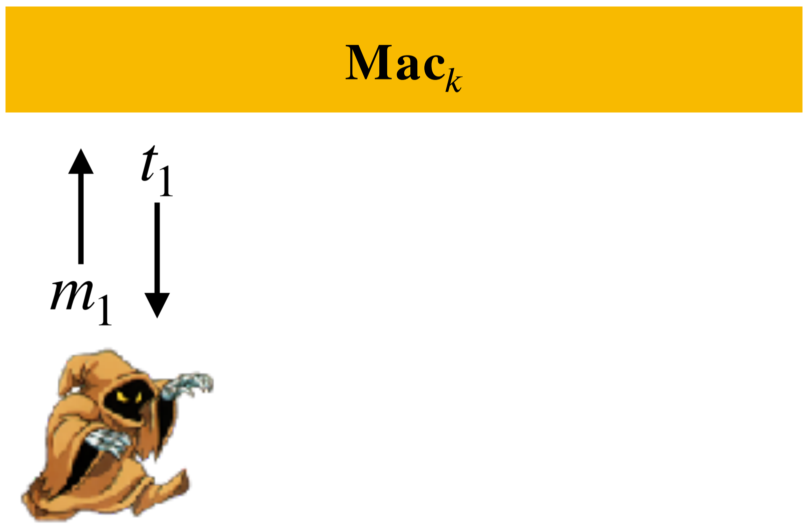
A message authentication code is secure, if no successful forger exists:

Classical security: Unforgeability

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

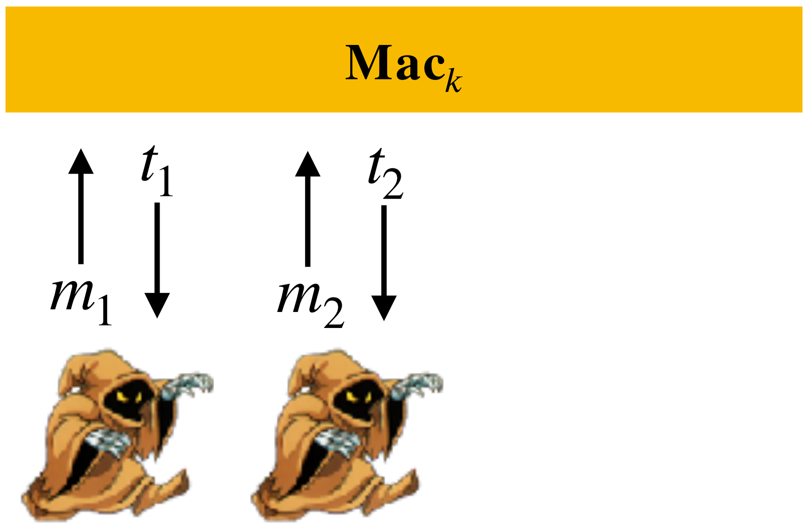
Classical security: Unforgeability

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



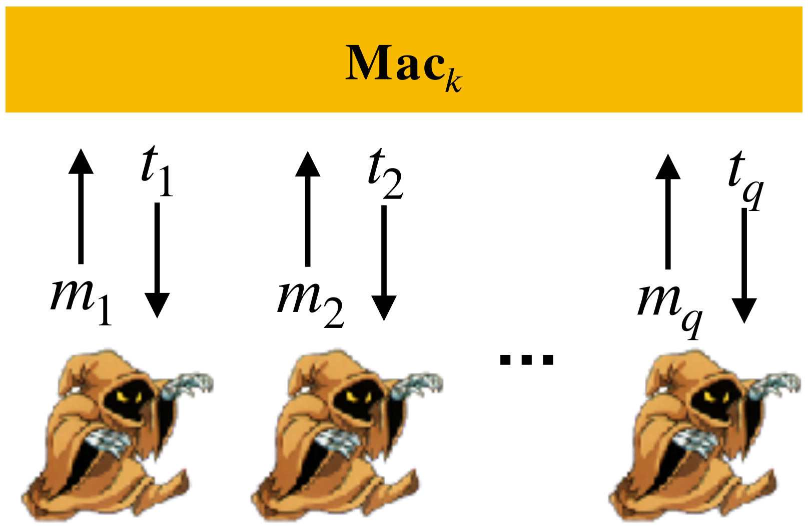
Classical security: Unforgeability

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



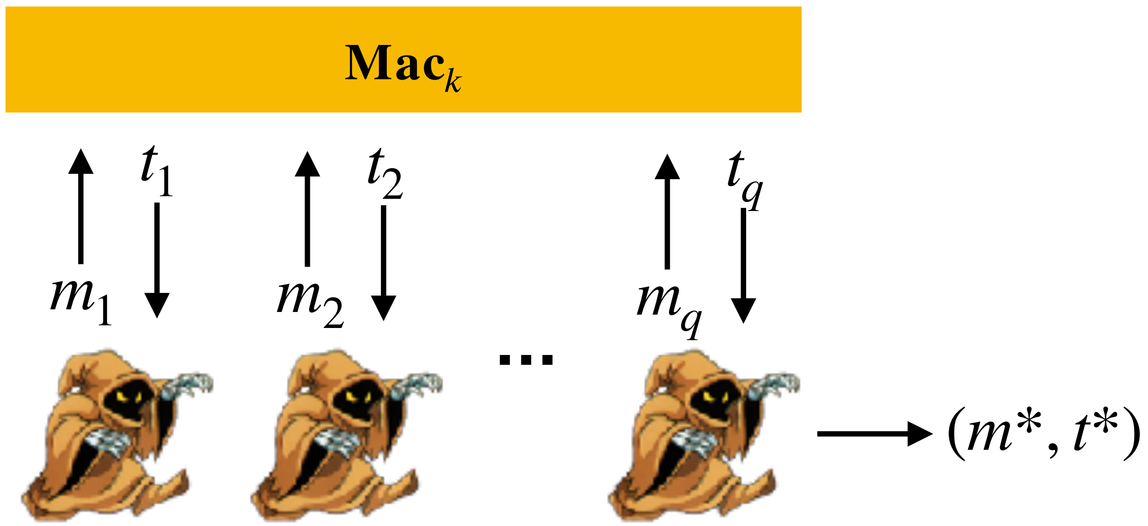
Classical security: Unforgeability

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



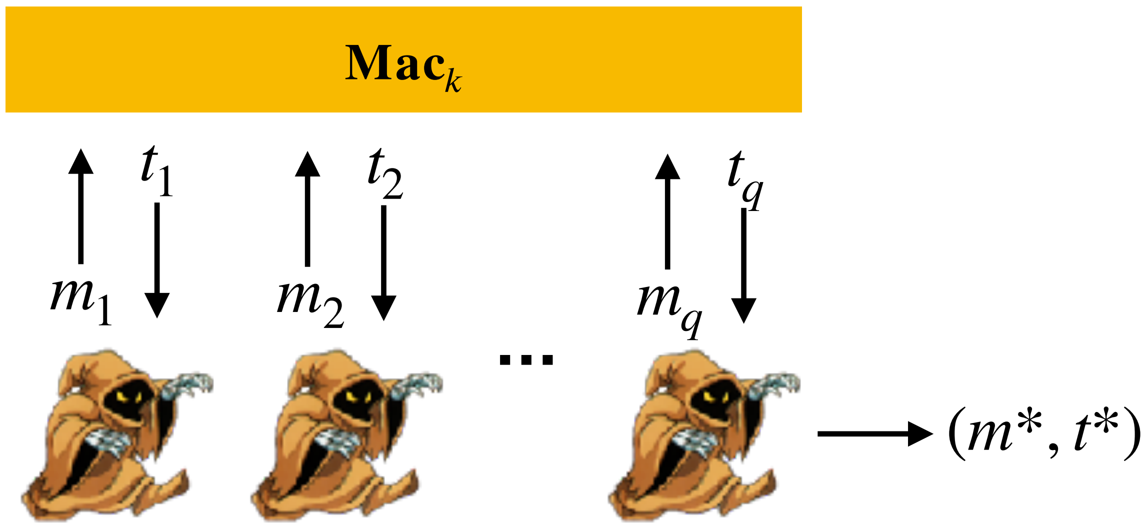
Classical security: Unforgeability

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



Classical security: Unforgeability

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



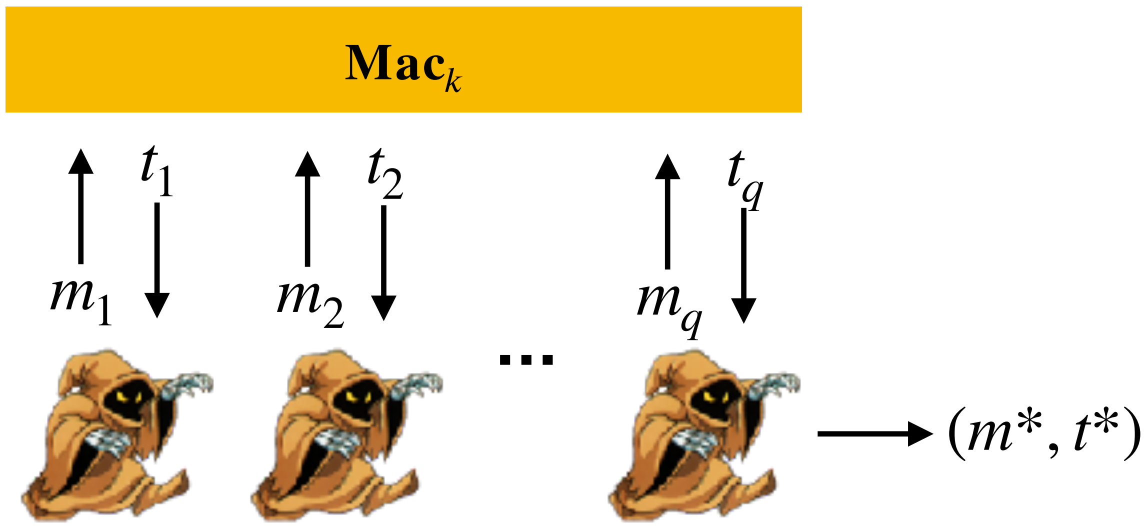
Success:

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

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

Classical security: Unforgeability

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



Success:

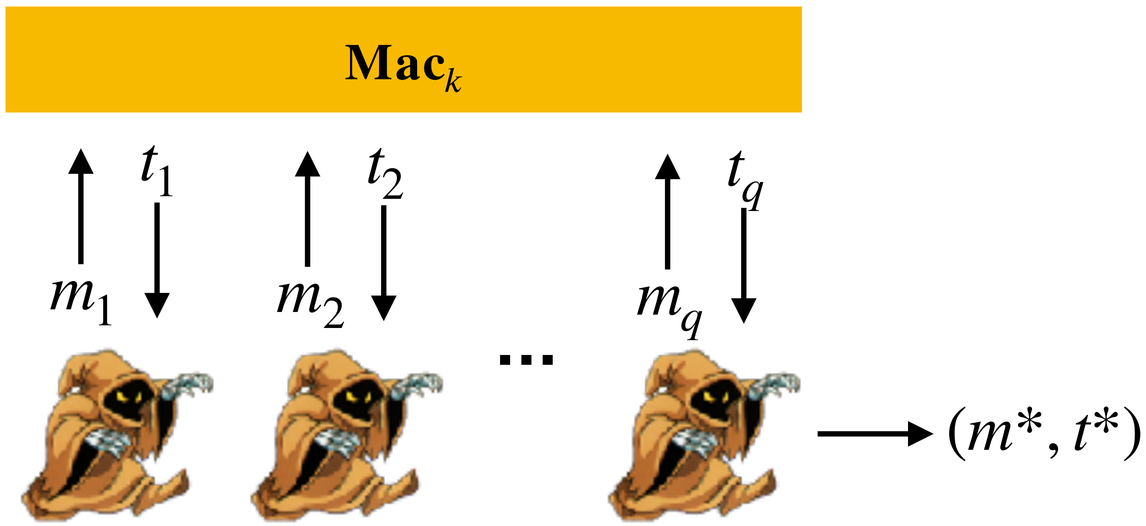
$i)$ $m^* \neq m_i$ for all $i = 1,\ldots,q$

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

“Existential unforgeability under chosen message attacks”, **EUF-CMA**

Classical security: Unforgeability

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



Success:

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

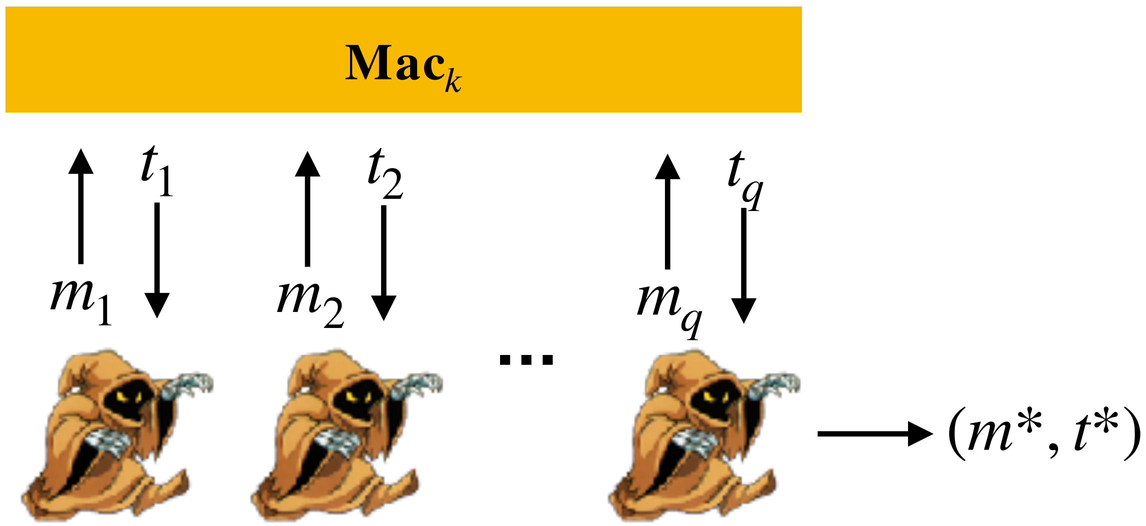
$ii)\ \mathbf{Mac}_k(m^*) = t^*$

"Existential unforgeability under chosen message attacks", **EUF-CMA**

What if the adversary has quantum oracle access to $\mathbf{Mac}_k$?

Classical security: Unforgeability

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



Success:

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

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

“Existential unforgeability under chosen message attacks”, **EUF-CMA**

What if the adversary has quantum oracle access to $\mathbf{Mac}_k$?

Example:

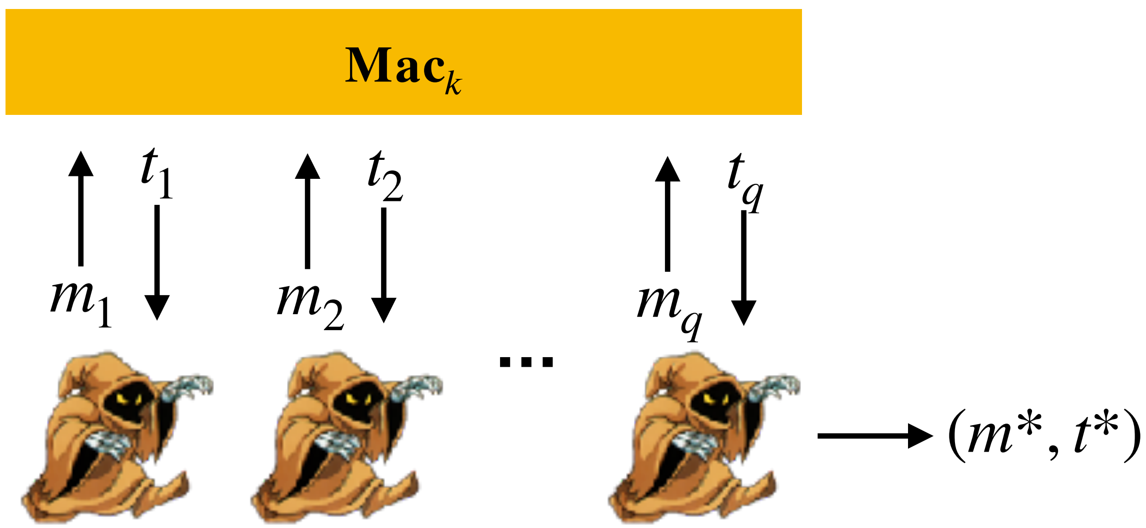
i) Query $m_1 = \sum_{m\in\{0,1\}^n} |m\rangle|0\rangle$ to obtain $\sum_{m\in\{0,1\}^n} |m\rangle|\mathrm{Mac}_k(m)\rangle$

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

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

Classical security: Unforgeability

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



Success:

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

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

"Existential unforgeability under chosen message attacks", **EUF-CMA**

What if the adversary has quantum oracle access to $\mathbf{Mac}_k$?

Example:

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

EUF-CMA doesn't make sense anymore…

Quantum

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

What is a good predictor?

Quantum

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

What is a good predictor?

Not a good predictor:

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

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

What is a good predictor?

Not a good predictor:

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

A good predictor:

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 to find p_k

ii) output $(p_k, 0)$

Boneh Zhandry unforgeability

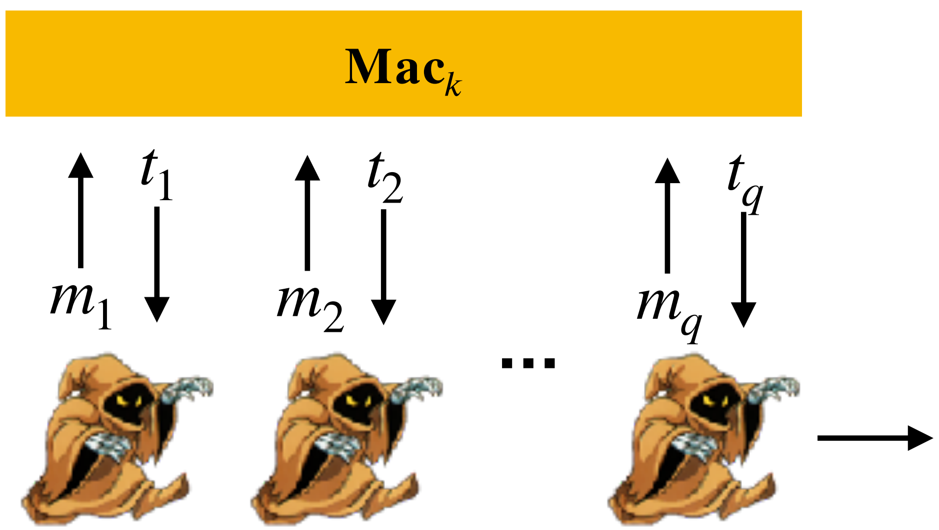
A proposal: (Boneh and Zhandry, EUROCRYPT 2013):

Ask $q+1$ forgeries for q queries!

Boneh Zhandry unforgeability

A proposal: (Boneh and Zhandry, EUROCRYPT 2013):

Ask $q + 1$ forgeries for q queries!



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

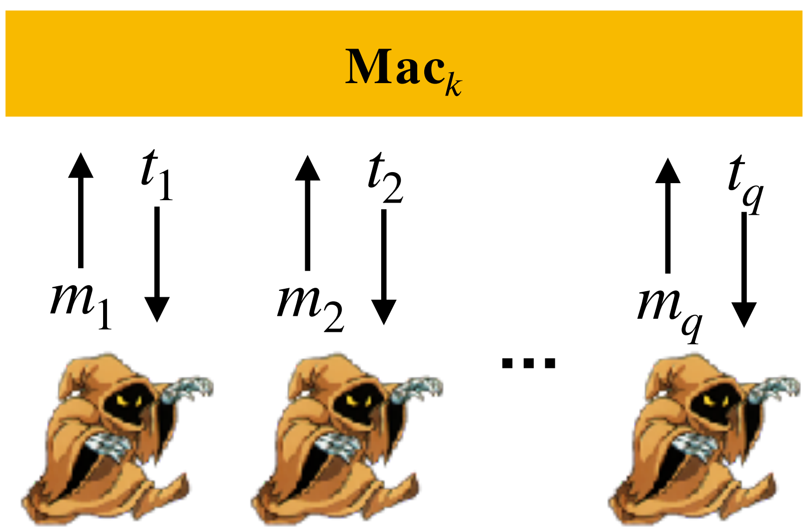
Success:

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

Boneh Zhandry unforgeability

A proposal: (Boneh and Zhandry, EUROCRYPT 2013):

Ask $q + 1$ forgeries for q queries!



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

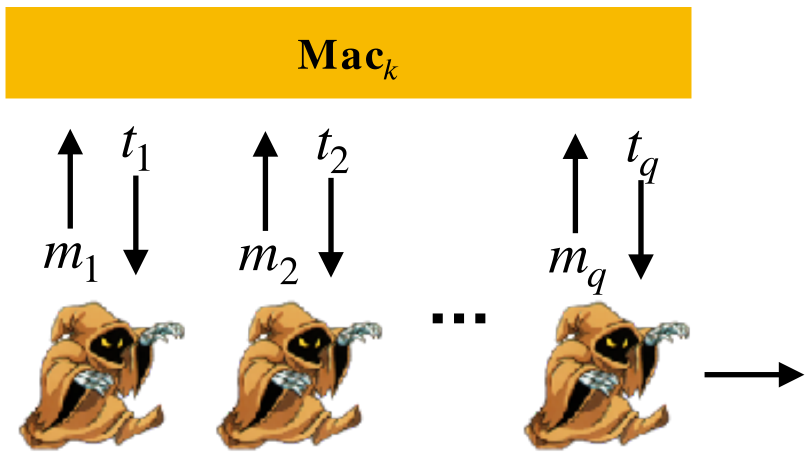
Success:

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

Has some nice properties:

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

The right definition?

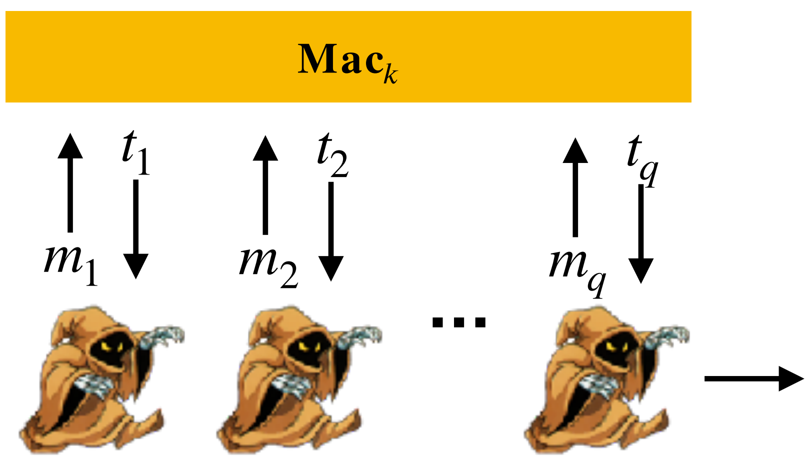


$(m_1^*, t_1^*), (m_2^*, t_2^*), \ldots, (m_{q+1}^*, t_{q+1}^*)$

Success:

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

The right definition?



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

Success:

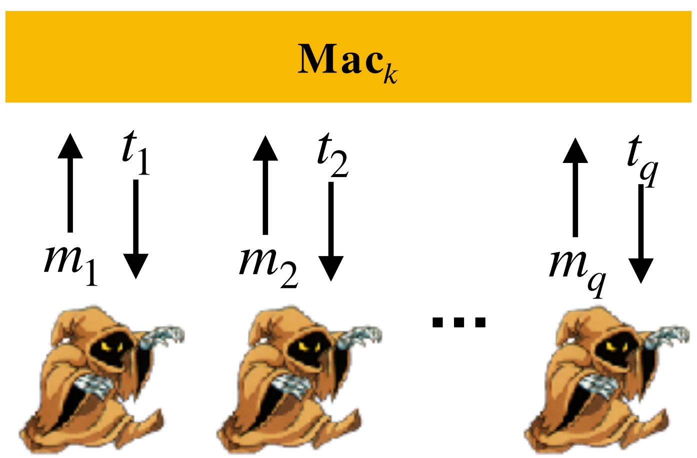
$\mathbf{Mac}_k(m_i^*) = t_i^* \ \forall i = 1,\ldots,q+1$

Is this really right? What does your quantum intuition tell you?

What if…

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

The right definition?



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

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

Is this really right? What does your quantum intuition tell you?

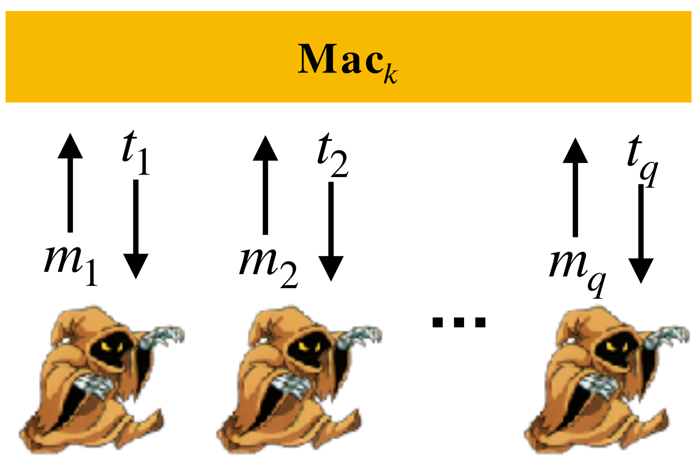
What if…

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

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

forgery comes from here
(msg prefix "from Gilles")

The right definition?



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

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

Is this really right? What does your quantum intuition tell you?

What if…

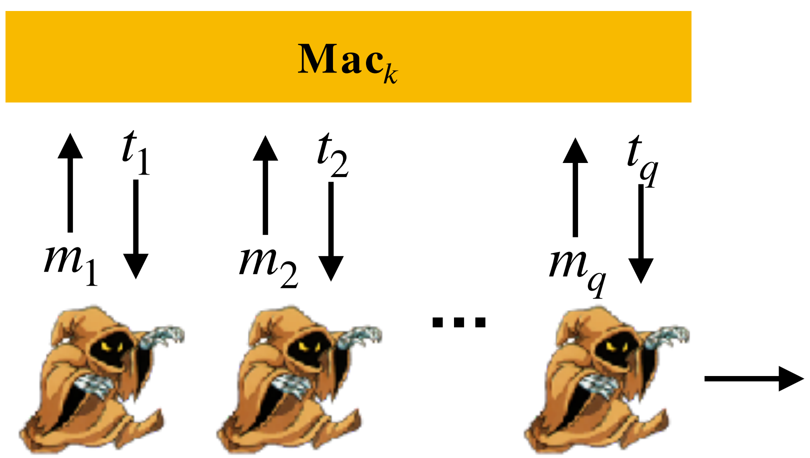
- adversary has to fully measure many queries to generate one forgery? (no-cloning)
- adversary “queries here, forges there”?

all queries supported here
(msg prefix “from Charlie”)

forgery comes from here
(msg prefix “from Gilles”)

In fact, it seems like it should be ***easy*** to find examples like this! It’s not, though.

The right definition?



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

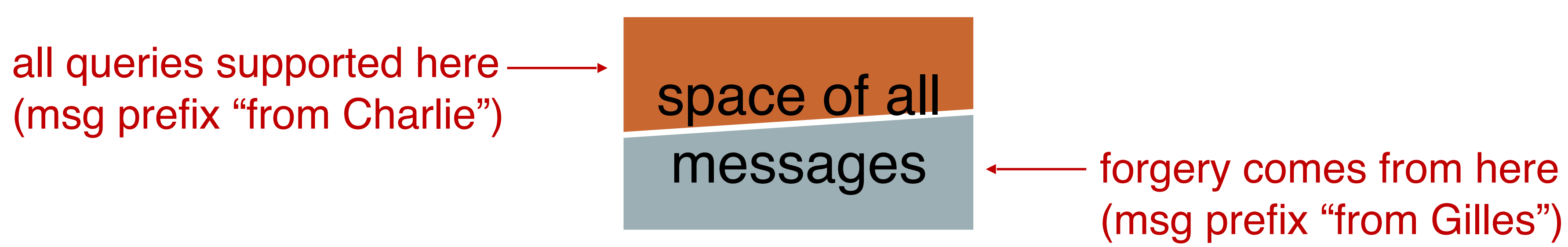
Success:

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

Is this really right? What does your quantum intuition tell you?

What if…

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



In fact, it seems like it should be ***easy*** to find examples like this! It's not, though.

Is our intuition right? One obstacle: "property finding" cannot be used.

Not the right definition!

A concrete MAC that “breaks” Boneh-Zhandry:

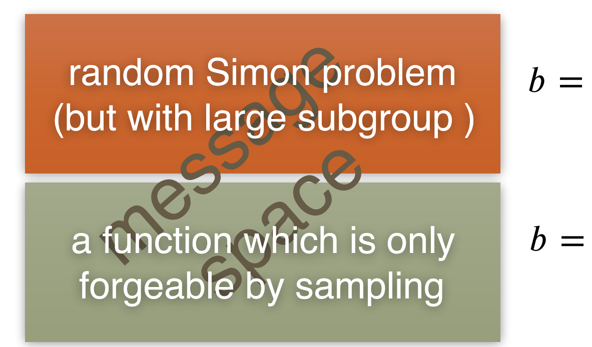
Idea: build a function where forging requires sampling from a large space of symmetries.

Not the right definition!

A concrete MAC that “breaks” Boneh-Zhandry:

Idea: build a function where forging requires sampling from a large space of symmetries.

- Let f_0, f_1 be random functions; let A be a large random subgroup of $\mathbb{Z}_2^n$;
- Define $f_0^A(x) = \bigoplus_{a \in A} f_0(x \oplus a)$
- Define $f_1^A(x) = f_1(x)$ unless $x \in A^\perp$, and $f_1^A(x) = 0^n$ for $x \in A^\perp$.
- MAC: $\mathbf{Mac}_k(bx) = f_b^A(x)$ with $k = (f_0, f_1, A)$.

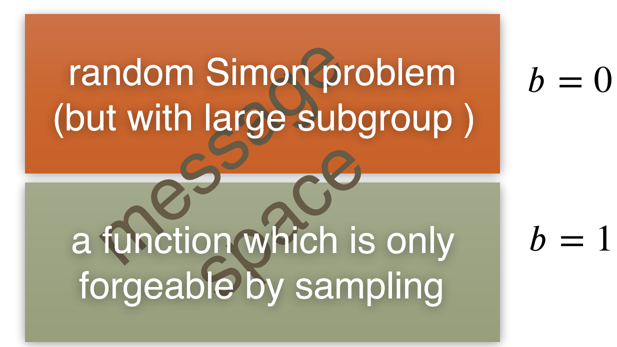


Not the right definition!

A concrete MAC that “breaks” Boneh-Zhandry:

Idea: build a function where forging requires sampling from a large space of symmetries.

- Let f_0, f_1 be random functions; let A be a large random subgroup of $\mathbb{Z}_2^n$;
- Define $f_0^A(x) = \bigoplus_{a \in A} f_0(x \oplus a)$
- Define $f_1^A(x) = f_1(x)$ unless $x \in A^\perp$, and $f_1^A(x) = 0^n$ for $x \in A^\perp$.
- MAC: $\mathbf{Mac}_k(bx) = f_b^A(x)$ with $k = (f_0, f_1, A)$.



Simple one-query attack:

i) use Fourier sampling to get random $x \in A^\perp$

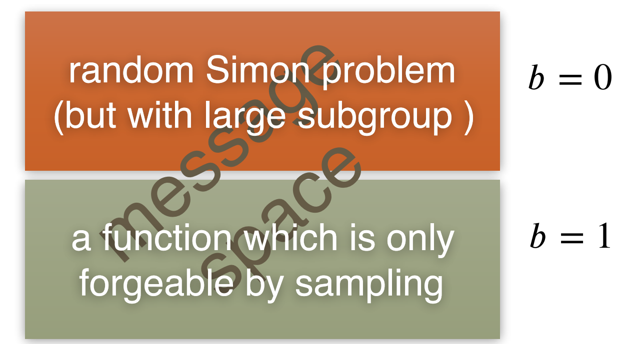
ii) output $(0x, 0^n)$

Not the right definition!

A concrete MAC that "breaks" Boneh-Zhandry:

Idea: build a function where forging requires sampling from a large space of symmetries.

- Let f_0, f_1 be random functions; let A be a large random subgroup of $\mathbb{Z}_2^n$;
- Define $f_0^A(x) = \bigoplus_{a \in A} f_0(x \oplus a)$
- Define $f_1^A(x) = f_1(x)$ unless $x \in A^\perp$, and $f_1^A(x) = 0^n$ for $x \in A^\perp$.
- MAC: $\mathbf{Mac}_k(bx) = f_b^A(x)$ with $k = (f_0, f_1, A)$.



Simple one-query attack:

i) use Fourier sampling to get random $x \in A^\perp$

ii) output $(0x, 0^n)$

Theorem (AMRS17). There are no efficient quantum algorithms 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 unpredictability vs quantum?

New approach: Blind Unforgeability (BU)

Problem: how do we define unpredictability vs quantum?

A new approach: "blind unforgeability." **(AMRS17)**

Idea: to check if a predictor is good…

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

New approach: Blind Unforgeability (BU)

Problem: how do we define unpredictability vs quantum?

A new approach: "blind unforgeability." **(AMRS17)**

Idea: to check if a predictor is good…

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

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

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

New approach: Blind Unforgeability (BU)

Problem: how do we define unpredictability vs quantum?

A new approach: "blind unforgeability." **(AMRS17)**

Idea: to check if a predictor is good…

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

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

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

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

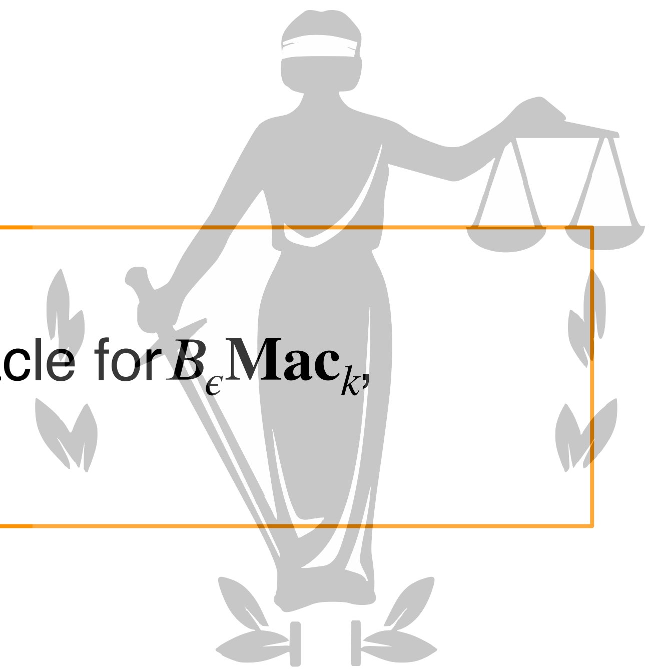
$$\mathbb{P}\left[(y, \mathbf{Mac}_k(y)) \leftarrow \mathscr{A}^{B_\epsilon\mathbf{Mac}_k} \text{ and } y \in B_\varepsilon\right] = \mathrm{negl}(n)$$

Blind Unforgeability

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

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

Blind Unforgeability



Definition (Blind-Unforgeability):
A MAC $\mathbf{Mac}_k$ is unpredictable 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 **EUF-CMA** in classical setting;

Blind Unforgeability

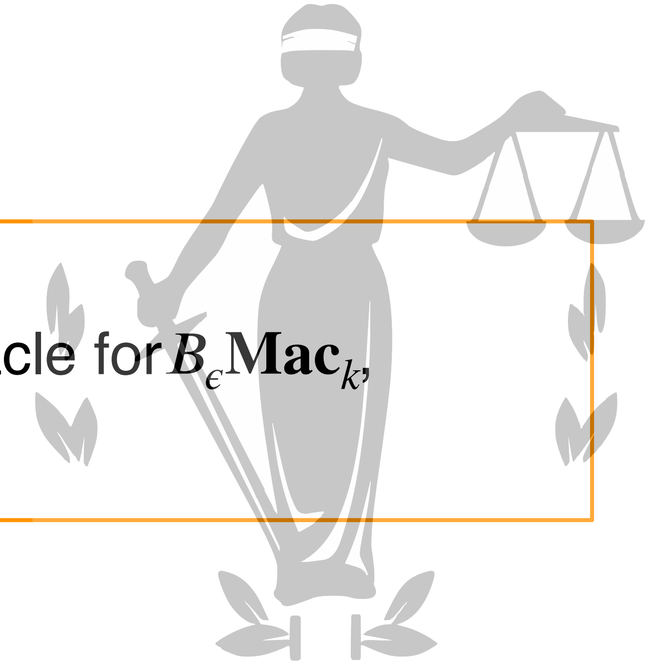
Definition (Blind-Unforgeability):
A MAC $\mathbf{Mac}_k$ is unpredictable if for every adversary $\mathscr{A}$ with a quantum oracle for $B_\epsilon \mathbf{Mac}_k$,

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

Does this work?

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

Blind Unforgeability



Definition (Blind-Unforgeability):
A MAC $\mathbf{Mac}_k$ is unpredictable 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?

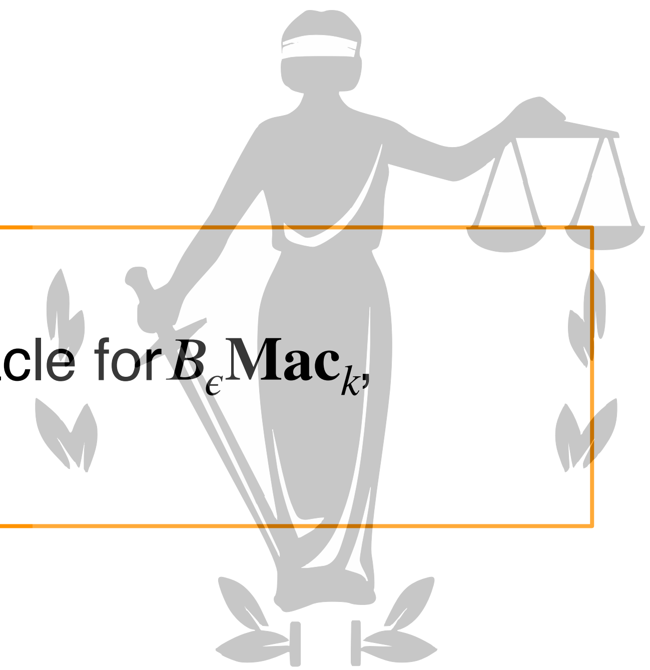
- equivalent to **EUF-CMA** in classical setting;
- random functions satisfy it;
- classifies the examples we have seen thus far correctly.

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 unpredictable 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 **EUF-CMA** in classical setting;
- random functions satisfy it;
- 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 unpredictable 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 **EUF-CMA** in classical setting;
- random functions satisfy it;
- classifies the examples we have seen thus far correctly.

2.

random Simon problem
(but with large subgroup) f_0^A

a function which is only
forgeable by sampling f_1^A

Blind Unforgeability

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

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

Does this work?

- equivalent to **EUF-CMA** in classical setting;
- random functions satisfy it;
- classifies the examples we have seen thus far correctly.

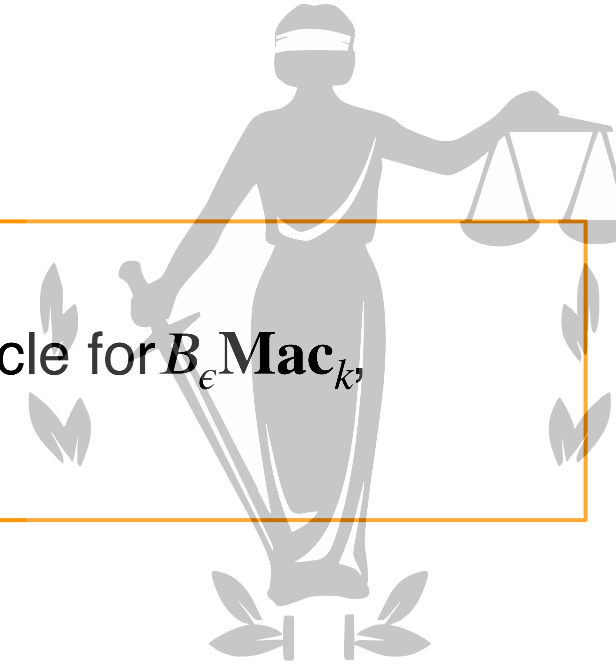
2.

random Simon problem (but with large subgroup) f_0^A

a function which is only forgeable by sampling f_1^A

One-query attack: Fourier sample orange part, forge in olive part.

Blind Unforgeability



Definition (Blind-Unforgeability):
A MAC $\mathbf{Mac}_k$ is unpredictable 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 **EUF-CMA** in classical setting;
- random functions satisfy it;
- classifies the examples we have seen thus far correctly.

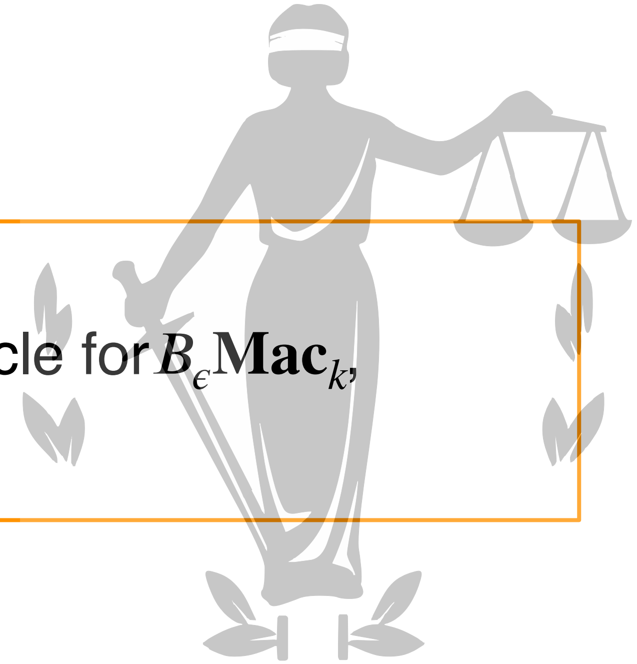
2.

random Simon problem (but with large subgroup)	f_0^A
a function which is only forgeable by sampling	f_1^A

Check, say for $\varepsilon = 0.0001$,

One-query attack: Fourier sample orange part,
forge in olive part.

Blind Unforgeability



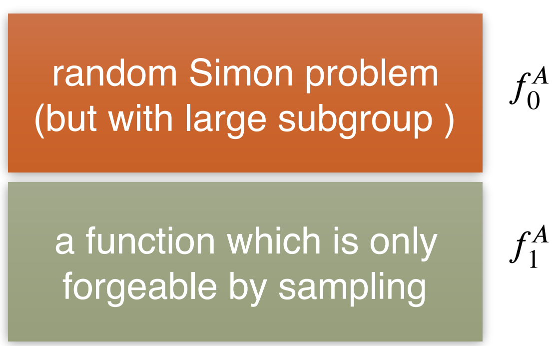
Definition (Blind-Unforgeability):
A MAC $\mathbf{Mac}_k$ is unpredictable if for every adversary $\mathscr{A}$ with a quantum oracle for $B_\epsilon \mathbf{Mac}_k$,

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

Does this work?

- equivalent to **EUF-CMA** in classical setting;
- random functions satisfy it;
- classifies the examples we have seen thus far correctly.

2.

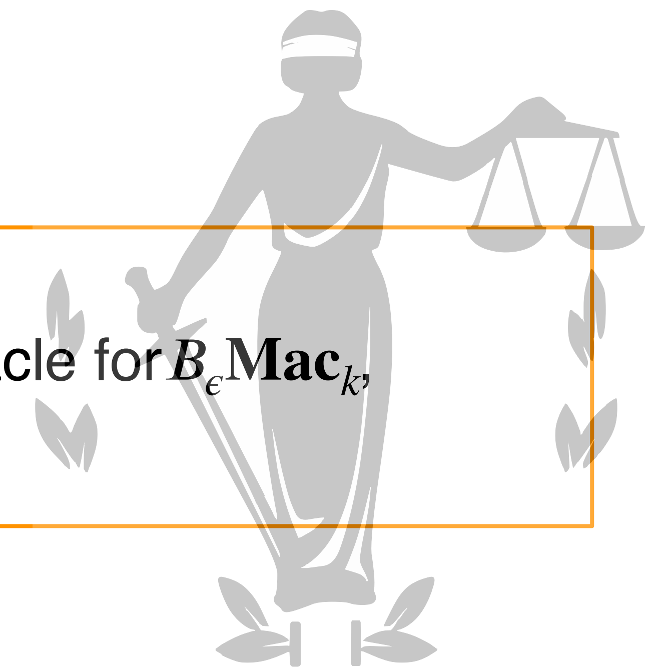


Check, say for $\varepsilon = 0.0001$,

- *oracle is blinded only on few random inputs…*

One-query attack: Fourier sample orange part, forge in olive part.

Blind Unforgeability



Definition (Blind-Unforgeability):
A MAC $\mathbf{Mac}_k$ is unpredictable 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 **EUF-CMA** in classical setting;
- random functions satisfy it;
- classifies the examples we have seen thus far correctly.

2.

random Simon problem (but with large subgroup) f_0^A

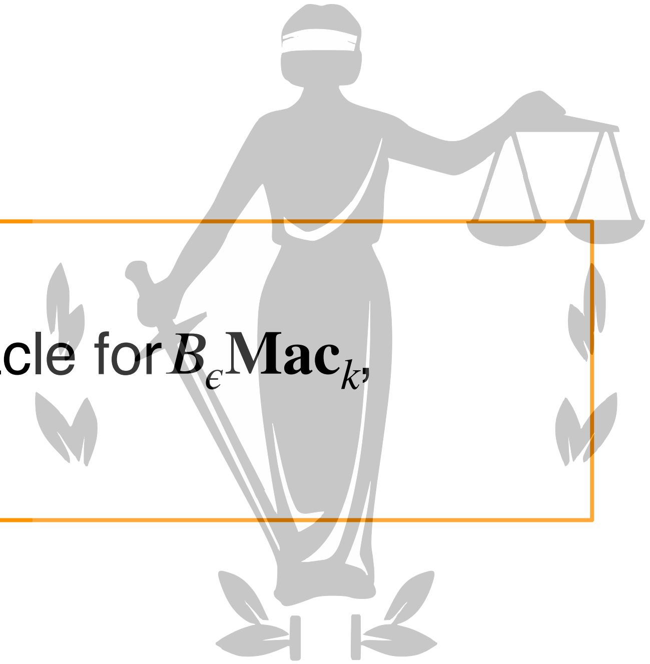
a function which is only forgeable by sampling f_1^A

Check, say for $\varepsilon = 0.0001$,

- *oracle is blinded only on few random inputs…*
- *…post-query state won't change too much;*

One-query attack: Fourier sample orange part, forge in olive part.

Blind Unforgeability



Definition (Blind-Unforgeability):
A MAC $\mathbf{Mac}_k$ is unpredictable 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 **EUF-CMA** in classical setting;
- random functions satisfy it;
- classifies the examples we have seen thus far correctly.

2.

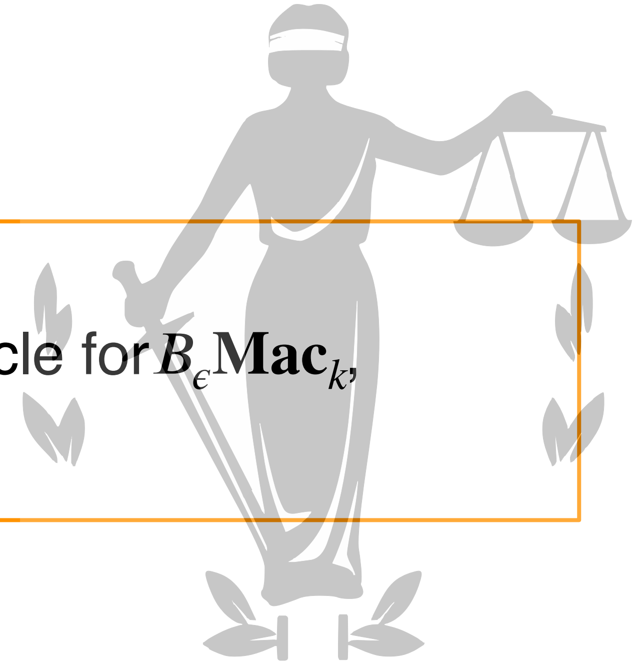
random Simon problem (but with large subgroup)	f_0^A
a function which is only forgeable by sampling	f_1^A

Check, say for $\varepsilon = 0.0001$,

- *oracle is blinded only on few random inputs…*
- *…post-query state won't change too much;*
- The Fourier sample is blinded with *independent* probability ε;

One-query attack: Fourier sample orange part, forge in olive part.

Blind Unforgeability



Definition (Blind-Unforgeability):
A MAC $\mathbf{Mac}_k$ is unpredictable 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 **EUF-CMA** in classical setting;
- random functions satisfy it;
- classifies the examples we have seen thus far correctly.

2.

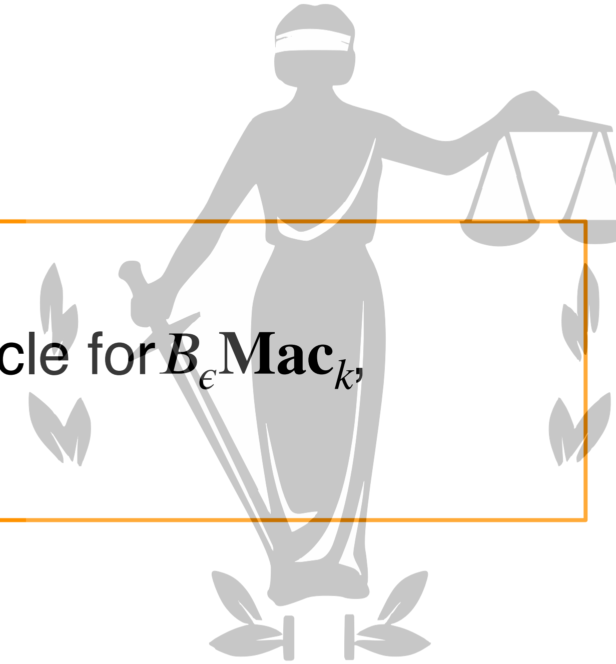
random Simon problem (but with large subgroup)	f_0^A
a function which is only forgeable by sampling	f_1^A

Check, say for $\varepsilon = 0.0001$,

- *oracle is blinded only on few random inputs…*
- *…post-query state won't change too much;*
- The Fourier sample is blinded with *independent* probability ε;
- so this adversary succeeds!

One-query attack: Fourier sample orange part, forge in olive part.

Blind Unforgeability



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

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

Additional results:

Blind Unforgeability

Definition (Blind-Unforgeability):
A MAC $\mathbf{Mac}_k$ is unpredictable 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 unpredictable 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

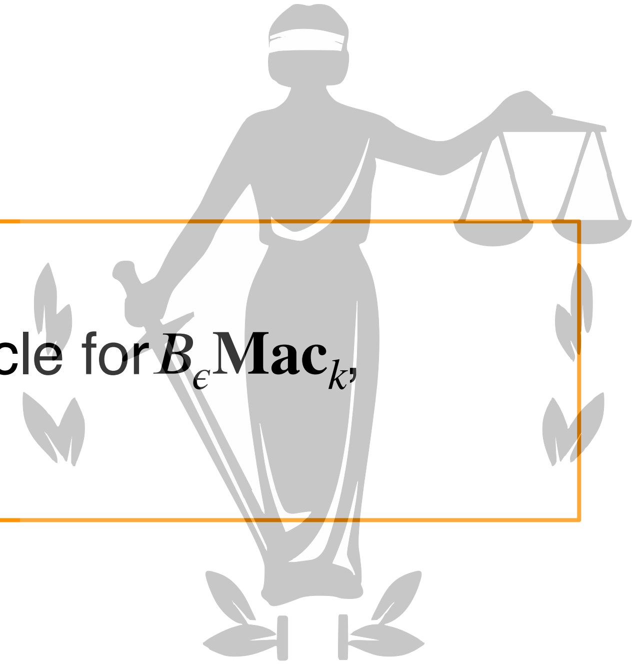
Definition (Blind-Unforgeability):
A MAC $\mathbf{Mac}_k$ is unpredictable if for every adversary $\mathscr{A}$ with a quantum oracle for $B_\epsilon \mathbf{Mac}_k$,

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

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



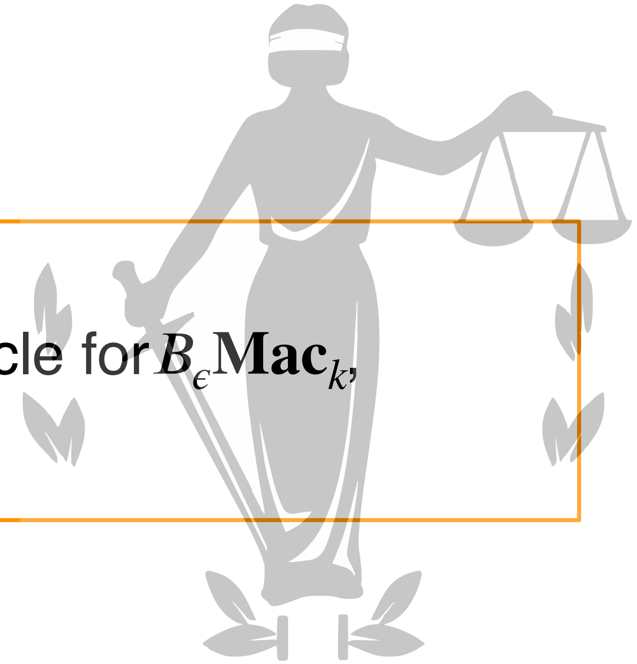
Definition (Blind-Unforgeability):
A MAC $\mathbf{Mac}_k$ is unpredictable if for every adversary $\mathscr{A}$ with a quantum oracle for $B_\epsilon \mathbf{Mac}_k$,

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

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 unpredictable if for every adversary $\mathscr{A}$ with a quantum oracle for $B_\epsilon \mathbf{Mac}_k$,

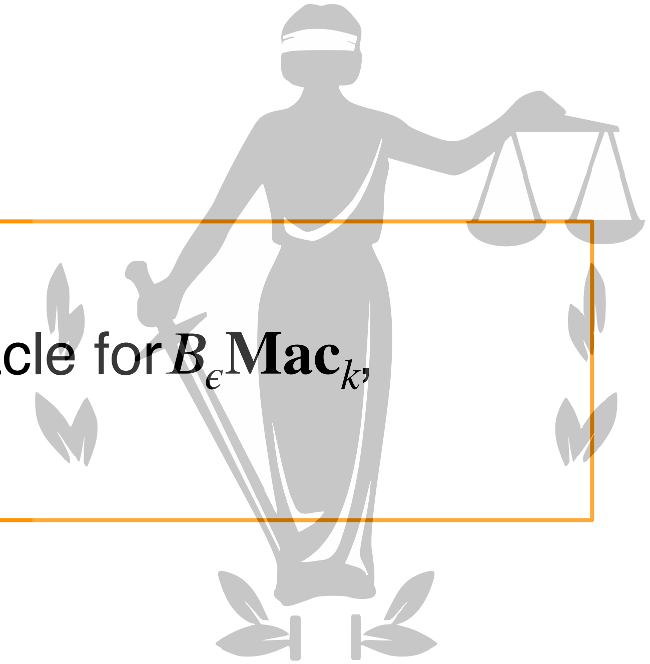
$$\mathbb{P}\left[(y, \mathbf{Mac}_k(y) \leftarrow \mathscr{A}^{B_\varepsilon \mathbf{Mac}_k} \text{ and } y \in B_\varepsilon\right] = \mathrm{negl}(n)$$

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 unpredictable if for every adversary $\mathscr{A}$ with a quantum oracle for $B_\epsilon \mathbf{Mac}_k$,

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

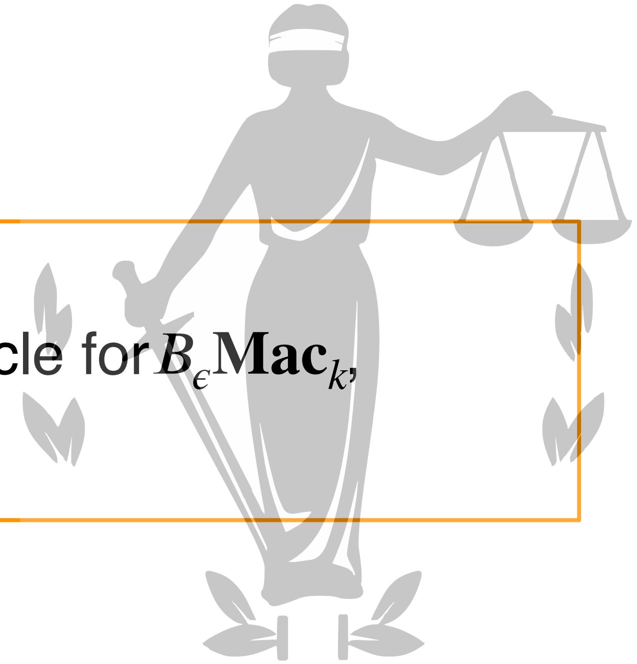
Additional results:

- 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 unpredictable 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
- Boneh and Zhandry's rank method

Blind Unforgeability

Definition (Blind-Unforgeability):
A MAC $\mathbf{Mac}_k$ is unpredictable 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
- Boneh and Zhandry's rank method
- Zhandry's superposition representation of quantum random oracles

Outlook

What's next?

- did we solve the problem?
- is blind-unforgeability the "right" notion of unforgeability against quantum adversaries?
- maybe: it does the right thing on all the examples we could think of;
- maybe not: it seems hard to prove that it implies **BZ** (does that matter?); we can come up with lots of seemingly inequivalent variants of **BU.**

In general: we need to develop and refine new techniques for quantum query complexity to suit "crypto needs", e.g. to analyze

1. algorithms which only succeed on a small space of inputs;
2. algorithms which succeed with vanishing (but non-negligible) probability;
3. non-asymptotics: problems with an "easy/impossible" thresholds of one (or few) queries.