Quantum-secure message authentication via blind-unforgeability

Gorjan Alagic, Christian Majenz, Alexander Russell and Fang Song

Eurocrypt 2020, in Cyberspace
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

Alice

$m$  $k$

Bob

$k$
Message authentication

Alice

Bob

\( m \quad k \)

\[ \text{Mac} \]

\[ t \]
Message authentication

...the Internet is a scary place...
Message authentication

... the Internet is a scary place...
Security: UF-CMA

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

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

\[ m^* \neq m_i \text{ for all } i = 1, \ldots, q \]

\[ \text{Success:} \]

1) \( m^* \neq m_i \) for all \( i = 1, \ldots, q \)
2) \( \text{Mac}_k(m^*) = t^* \)
Quantum Access Security

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

$$ |m\rangle |t\rangle \mapsto |m\rangle |t \oplus \text{Mac}_k(m)\rangle $$
Quantum Access Security

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

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

Why?
Quantum Access Security

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

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

Why?

- As-strong-as-possible security
Quantum Access Security

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

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

Why?

- As-strong-as-possible security
- Post-quantum Composability
Quantum Access Security

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

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

Why?

- As-strong-as-possible security
- Post-quantum Composability
- Physics?
Quantum Access Security

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

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

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 $\text{Mac}_k$:

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

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 $\sum_{m \in \{0,1\}^n} |m\rangle|\text{Mac}_k(m)\rangle$

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

iii) Output $(m, \text{Mac}_k(m))$
Quantum Access Security

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

\[ |m\rangle |t\rangle \mapsto |m\rangle |t \oplus \text{Mac}_k(m)\rangle \]

Why?

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

Let’s try \textbf{UF}--“QCMA”

Example:

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

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

iii) Output \((m, \text{Mac}_k(m))\)

\textbf{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 $\sum_{m \in \{0,1\}^n} |m\rangle |\text{Mac}_k(m)\rangle$

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

iii) Output $(m, \text{Mac}_k(m))$
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 $\sum_{m \in \{0,1\}^n} |m\rangle |\text{Mac}_k(m)\rangle$

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

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

We should be worried about:

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

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

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

ii) output $(p_k,0)$
Quantum problems

\[ \text{Success:} \]

\begin{align*}
&i) \ m^* \neq m_i \text{ for all } i = 1,\ldots,q \\
&ii) \ \text{Mac}_k(m^*) = t^*
\end{align*}
Quantum problems

Success:

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

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

- 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 and Zhandry (Eurocrypt 2013) propose:

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

Success:
$\text{Mac}_k(m^*_i) = t^*_i \ \forall i = 1, \ldots, q + 1$
Boneh Zhandry unforgeability

Boneh and Zhandry (Eurocrypt 2013) propose:

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

\[
\text{Success: } \quad \text{Mac}_k(m_i^*) = t_i^* \quad \forall i = 1,\ldots,q + 1
\]

Has some nice properties:

- Equivalent to \textbf{UF-CMA} for classical oracle
- A random oracle is BZ-unforgeable (BZ ’13)
The right definition?

Success:
\[ \text{Mac}_k(m^*_i) = t^*_i \ \forall i = 1, \ldots, q+1 \]
The right definition?

Success:
\[ \text{Mac}_k(m_i^*) = t_i^* \quad \forall i = 1, ..., q+1 \]

What if…

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

Success:
\[ \text{Mac}_k(m_i^*) = t_i^* \quad \forall i = 1, \ldots, q+1 \]

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”)

space of all messages

forgery comes from here
(msg prefix “from the White Rabbit”)

\[ (m_1^*, t_1^*), (m_2^*, t_2^*), \ldots, (m_{q+1}^*, t_{q+1}^*) \]
The right definition?

Success:
$$\text{Mac}_k(m^*_i) = t^*_i \forall i = 1, \ldots, q+1$$

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?

Success:
\[ \text{Mac}_k(m_i^*) = t_i^* \quad \forall i = 1,...,q+1 \]

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")

space of all
messages

is not

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

In fact, it seems like it should be easy to find examples like this!
The right definition?

Success: \( \text{Mac}_k(m^*_i) = t^*_i \ \forall i = 1,\ldots,q+1 \)

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!

One obstacle: “property finding” cannot be used.
The right definition?

\[ \text{Mac}_k (m_i^*) = t_i^* \quad \forall i = 1, \ldots, q+1 \]

Success:

What if…

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

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)

In fact, it seems like it should be easy to find examples like this!
A concrete example

A MAC that unconditionally “breaks” Boneh-Zhandry:
A concrete example

A MAC that unconditionally “breaks” Boneh-Zhandry:

\[
m = \begin{cases} 
    b & \rightarrow \text{Mac}_k \\
    x & \rightarrow f^0_b(x) \\
    & \rightarrow f^1_b(x)
\end{cases}
\]

- \( \hat{f}^i_b : \{0,1\}^n \rightarrow \{0,1\}^n \) random functions
- \( f^0_b(x) = \hat{f}^0_0(x \mod p) \) for random \( p \), \( f^0_b = \hat{f}^0_0 \)
- \( f^0 = \begin{cases} 
    0^n & x = p \\
    \hat{f}^0_1(x) & \text{else}
\end{cases}, f^1_1 \equiv 0^n \)
A MAC that unconditionally “breaks” Boneh-Zhandry:

Message space

\[
\begin{align*}
\{ & \text{Random periodic function shielded by a random function} & b = 0 \\
& \text{Random function punctured at the period} & b = 1
\end{align*}
\]
A concrete example

A MAC that unconditionally “breaks” Boneh-Zhandry:

Simple one-query attack:

i) Use period finding to find \( p \), “ignoring” \( f_0^1 \)

ii) output \((1p,0^{2^n})\)
A MAC that unconditionally "breaks" Boneh-Zhandry:

A concrete example

Simple one-query attack:

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

ii) output $(1p,0^{2n})$
A MAC that unconditionally “breaks” Boneh-Zhandry:

A concrete example

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

A concrete example

A MAC that unconditionally “breaks” Boneh-Zhandry:

Simple one-query attack:

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

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

Key step: ignorance is necessary

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

A MAC that unconditionally “breaks” Boneh-Zhandry:

Simple one-query attack:

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

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

Key step: ignorance is necessary
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 $\text{Mac}_k$

1. Select $B_\varepsilon \subset \{0,1\}^n$ by putting every $m \in B_\varepsilon$ independently with probability $\varepsilon$;

2. Define "blinded" oracle: $B_\varepsilon \text{Mac}_k : m \mapsto \begin{cases} \text{Mac}_k(m) & m \notin B_\varepsilon \\ \bot & m \in B_\varepsilon \end{cases}$
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 $\text{Mac}_k$

1. Select $B_\varepsilon \subset \{0,1\}^n$ by putting every $m \in B_\varepsilon$ independently with probability $\varepsilon$;

2. Define “blinded” oracle: $B_\varepsilon \text{Mac}_k : m \mapsto \begin{cases} \text{Mac}_k(m) & m \notin B_\varepsilon \\ \bot & m \in B_\varepsilon \end{cases}$

**Definition (Blind-Unforgeability):**

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

$$\Pr [(m, \text{Mac}_k(m) \leftarrow A^{B_\varepsilon \text{Mac}_k} \text{ and } m \in B_\varepsilon ) = \text{negl}(n)]$$
Blind Unforgeability

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

$$\Pr[(y, \text{Mac}_k(y) \leftarrow \mathcal{A}^{B_\epsilon \text{Mac}_k} \text{ and } y \in B_\epsilon] = \text{negl}(n)$$

Does this work?
- equivalent to UF-CMA in classical setting;
Blind Unforgeability

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

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

Does this work?
- equivalent to UF-CMA in classical setting;
- random functions satisfy it;
Blind Unforgeability

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

$$\Pr[(y, \text{Mac}_k(y) \leftarrow \mathcal{A}^{B_\epsilon \text{Mac}_k} \text{ and } y \in B_\epsilon] = \text{negl}(n)$$

Does this work?
- equivalent to \textbf{UF-CMA} in classical setting;
- random functions satisfy it;
- Implies previous definition by Boneh and Zhandry;
Blind Unforgeability

Definition (Blind-Unforgeability): A MAC $\text{Mac}_k$ is blind-unforgeable if for every adversary $\mathcal{A}$ with a quantum oracle for $B_{\varepsilon}\text{Mac}_k$, 
$$
\mathbb{P} \left[ (y, \text{Mac}_k(y) \leftarrow \mathcal{A}^{B_{\varepsilon}\text{Mac}_k} \text{ and } y \in B_{\varepsilon} ) \right] = \text{negl}(n)
$$

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

1. prepare: $m_1 = \sum_{m \in \{0,1\}^n} |m\rangle |0\rangle$;
2. query
3. measure
Output: $(m, B_{\varepsilon}\text{Mac}_k(m))$ for random $m$. 
Blind Unforgeability

Definition (Blind-Unforgeability):
A MAC $\text{Mac}_k$ is blind-unforgeable if for every adversary $\mathcal{A}$ with a quantum oracle for $B^e\text{Mac}_k$, 
\[ \mathbb{P}\left[(y, \text{Mac}_k(y) \leftarrow \mathcal{A}^{B^e\text{Mac}_k} \text{ and } y \in B_e]\right) = \text{negl}(n) \]

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

1. prepare: $m_1 = \sum_{m \in \{0,1\}^n} |m\rangle |0\rangle$ ;
2. query
3. measure
Output: $(m, B^e_{\text{Mac}_k}(m))$ for random $m$.

Check, e.g., for random functions:
- if oracle is blinded…
- … $\text{Mac}_k(m)$ for blinded $m$ is independent of post-query state,
- this adversary fails.
Blind Unforgeability

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

$$\Pr \left[ (y, \text{Mac}_k(y) \leftarrow A^{B_\epsilon \text{Mac}_k} \text{ and } y \in B_\epsilon \right] = \text{negl}(n)$$

Does this work?

- equivalent to UF-CMA in classical setting;
- random functions satisfy it;
- Implies previous definition 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 $\text{Mac}_k$ is blind-unforgeable if for every adversary $\mathcal{A}$ with a quantum oracle for $B_\varepsilon \text{Mac}_k$,
\[
\mathbb{P} \left[ (y, \text{Mac}_k(y) \leftarrow \mathcal{A}^{B_\varepsilon \text{Mac}_k} \text{ and } y \in B_\varepsilon \right] = \text{negl}(n)
\]

Does this work?
- equivalent to $\text{UF-CMA}$ in classical setting;
- random functions satisfy it;
- Implies previous definition 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.
Definition (Blind-Unforgeability):
A MAC $\text{Mac}_k$ is blind-unforgeable if for every adversary $\mathcal{A}$ with a quantum oracle for $B_{\varepsilon}\text{Mac}_k$,

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

Additional results:
Definition (Blind-Unforgeability):
A MAC $\text{Mac}_k$ is blind-unforgeable if for every adversary $\mathcal{A}$ with a quantum oracle for $B_{\varepsilon} \text{Mac}_k$,

$$\Pr \left[ (y, \text{Mac}_k(y) \leftarrow B_{\varepsilon} \text{Mac}_k \text{ and } y \in B_{\varepsilon}) = \text{negl}(n) \right]$$

Additional results:
- Bernoulli-preserving hash function: generalizes collision resistance to quantum, strengthens collapsingness
Blind Unforgeability

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

$$\Pr[(y, \text{Mac}_k(y) \leftarrow \mathcal{A}^{B_\varepsilon \text{Mac}_k} \text{ and } y \in B_\varepsilon] = \text{negl}(n)$$

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

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

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
Definition (Blind-Unforgeability):
A MAC $\text{Mac}_k$ is blind-unforgeable if for every adversary $\mathcal{A}$ with a quantum oracle for $\mathcal{B}_\epsilon \text{Mac}_k$,
$$\mathbb{P} \left[ (y, \text{Mac}_k(y) \leftarrow \mathcal{A}^{B_\epsilon \text{Mac}_k} \text{ and } y \in B_\epsilon \right] = \text{negl}(n)$$

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 $\text{Mac}_k$ is blind-unforgeable if for every adversary $\mathcal{A}$ with a quantum oracle for $B_{\epsilon} \text{Mac}_k$, $\Pr[(y, \text{Mac}_k(y) \leftarrow \mathcal{A}^{B_{\epsilon}\text{Mac}_k} \text{ and } y \in B_{\epsilon}) = \text{negl}(n)]$

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

$$\Pr[(y, \text{Mac}_k(y) \leftarrow \mathcal{A}^{B_{\epsilon}\text{Mac}_k} \text{ and } y \in B_{\epsilon})] = \text{negl}(n)$$

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

$$\Pr \left[ (y, \text{Mac}_k(y) \leftarrow \mathcal{A}^{B_{\epsilon}\text{Mac}_k} \text{ and } y \in \mathcal{B}_{\epsilon} \right) = \text{negl}(n) \right]$$

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:

- 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...