Hash functions in post-quantum cryptography

Christian Majenz
CWI
Cryptography is everywhere
Cryptography is everywhere

https://
Cryptography is everywhere
Cryptography is everywhere
Cryptography is everywhere
Cryptography is everywhere
Quantum computers
Quantum computers

- Accelerating effort to build a quantum computer
Quantum computers

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

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

Google, IBM, Intel, Microsoft, Quantum Flagship

We need to prepare cryptography for the arrival of quantum computers!
Quantum computers

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

  Google  IBM  
  intel  Microsoft  

We need to prepare cryptography for the arrival of quantum computers!

- Security against quantum attackers
- Quantum cryptography
Quantum computers

- Accelerating effort to build a quantum computer
- Major investments:
  - Google
  - IBM
  - US National Security Agency
  - US National Institute of Standards and Technology
  - Microsoft
  - QuSpin (China)

We need to prepare cryptography for the arrival of quantum computers!

- This talk: Security against quantum attackers
  (post-quantum cryptography)
Elements of post-quantum crypto
Elements of post-quantum crypto

- Quantum Cryptanalysis
Elements of post-quantum crypto

- Quantum Cryptanalysis
Elements of post-quantum crypto

- Quantum Cryptanalysis

Shor’s algorithm: Complete break
Elements of post-quantum crypto

- Quantum Cryptanalysis

- Shor's algorithm: Complete break
- Grover's algorithm: Might necessitate increased key length
Elements of post-quantum crypto

- Quantum Cryptanalysis: Shor, Grover

- Quantum-secure computational assumptions
  - Lattice problems
  - Decoding random codes
  - Inverting multivariate polynomials
  - Secure hash functions
  - Supersingular isogeny Diffie-Hellman
Elements of post-quantum crypto

- Quantum Cryptanalysis: Shor, Grover

- Quantum-secure computational assumptions
  - Lattice problems
  - Decoding random codes
  - Inverting multivariate polynomials
  - Secure hash functions
  - Supersingular isogeny Diffie-Hellman

- Models: Quantum Random Oracle Model (QROM)
Hash functions
Hash functions

Ubiquitous in cryptography. Example: digital signatures
The (Q)ROM
The (Q)ROM

Reality | Model
The (Q)ROM

Reality

Model
The (Q)ROM

Reality

Model

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

Uniformly random
The (Q)ROM

Reality

Model

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

Uniformly random

All agents have (quantum) oracle access to $H$

$(x, y) \mapsto (x, y \oplus H(x))$
The (Q)ROM

Reality

Model

\[ H : \{0,1\}^* \rightarrow \{0,1\}^n \]

Uniformly random

All agents have (quantum) oracle access to \( H \)

\[ (x, y) \mapsto (x, y \oplus H(x)) \]

- Outrageously optimistic

- SHA-3
### The (Q)ROM

<table>
<thead>
<tr>
<th>Reality</th>
<th>Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outrageously optimistic</td>
<td>$H : {0,1}^* \rightarrow {0,1}^n$</td>
</tr>
<tr>
<td>Seems to work in practice</td>
<td>Uniformly random</td>
</tr>
</tbody>
</table>

All agents have (quantum) oracle access to $H$

$$(x, y) \mapsto (x, y \oplus H(x))$$
The (Q)ROM

<table>
<thead>
<tr>
<th>Reality</th>
<th>Model</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Outrageously optimistic</strong></td>
<td>$H : {0,1}^* \rightarrow {0,1}^n$</td>
</tr>
<tr>
<td><strong>Seems to work in practice</strong></td>
<td>Uniformly random</td>
</tr>
<tr>
<td><strong>Enables very efficient crypto</strong></td>
<td>All agents have (quantum) oracle access to $H$</td>
</tr>
</tbody>
</table>

$(x, y) \mapsto (x, y \oplus H(x))$
QROM challenges
QROM challenges

ROM techniques:
1. Query transcripts
QROM challenges

ROM techniques:
1. Query transcripts
2. Rewinding
QROM challenges

ROM techniques:
1. Query transcripts
2. Rewinding
3. Reprogramming
QROM challenges

ROM techniques:
1. Query transcripts
2. Rewinding
3. Reprogramming

Quantum theory makes things difficult! No-cloning, Measurement disturbance
QROM challenges

ROM techniques:
1. Query transcripts
2. Rewinding
3. Reprogramming

Quantum theory makes things difficult! No-cloning, Measurement disturbance

QROM:
QROM challenges

ROM techniques:
1. Query transcripts
2. Rewinding
3. Reprogramming

Quantum theory makes things difficult! No-cloning, Measurement disturbance

QROM:
1. Query transcripts
QROM challenges

ROM techniques:
1. Query transcripts
2. Rewinding
3. Reprogramming

Quantum theory makes things difficult! No-cloning, Measurement disturbance

QROM:
1. Query transcripts
2. Rewinding 3 specialized rewinding techniques that don’t cover all applications
QROM challenges

ROM techniques:
1. Query transcripts
2. Rewinding
3. Reprogramming

Quantum theory makes things difficult! No-cloning, Measurement disturbance

QROM:
1. Query transcripts
2. Rewinding $\Rightarrow$ 3 specialized rewinding techniques that don’t cover all applications
3. Reprogramming: Sure, if you know how without 1. and 2.
The Fiat Shamir transformation
The Fiat Shamir transformation

Σ-protocol: Interactive proof system

Prover

Verifier

$x$

$a$

$c \in_R \{0,1\}^\ell_c$

$r$

$b$
The Fiat Shamir transformation

\[ \text{Σ-protocol: Interactive proof system} \]

\[ x \rightarrow \text{Prover} \]

\[ a \]

\[ c \in_R \{0,1\}^\ell \]

\[ r \rightarrow \text{Verifier} \]

Fiat Shamir (FS) transformation: \[ c = H(x, a) \]
The Fiat Shamir transformation

Σ-protocol: Interactive proof system

Prover

Verifier

Fiat Shamir (FS) transformation: $c = H(x, a)$
The Fiat Shamir transformation

Σ-protocol: Interactive proof system

Fiat Shamir (FS) transformation: $c = H(x, a)$

non-interactive!!!
The Fiat Shamir transformation

Σ-protocol: Interactive proof system

Fiat Shamir (FS) transformation: $c = H(x, a)$

non-interactive!!! $\implies$ used for efficient digital signatures
ROM security

The FS transformation is secure in the ROM (Pointcheval, Stern 96):
The FS transformation is secure in the ROM (Pointcheval, Stern 96):
ROM security

The FS transformation is secure in the ROM (Pointcheval, Stern 96):

\[ x \rightarrow A \rightarrow S \rightarrow \text{Verifier} \]

\[ a \]

\[ c \in_R \{0,1\}^\ell_c \]

\[ r \]
ROM security

The FS transformation is secure in the ROM (Pointcheval, Stern 96):

\[
\mathcal{S} \subseteq R \{0,1\}^\ell_c
\]

Success probability: \( \epsilon(\mathcal{S}[\mathcal{A}]) \geq \frac{\epsilon(\mathcal{A})}{O(q)} \)
ROM security

The FS transformation is secure in the ROM (Pointcheval, Stern 96):

\[
\mathcal{A} \xrightarrow{c \in_R \{0,1\}^{\ell_c}} \mathcal{S} \xrightarrow{a} \text{Verifier}
\]

Success probability: \( \varepsilon(\mathcal{S}[\mathcal{A}]) \geq \frac{\varepsilon(\mathcal{A})}{O(q)} \)

\# of queries \( \mathcal{A} \) makes to \( H \)
QROM security

The FS transformation is secure in the QROM (Don, Fehr, M, Schaffner ’19):

\[ H \]

\[ \mathcal{A} \]

\[ x \]

\[ p \]
QROM security

The FS transformation is secure in the QROM (Don, Fehr, M, Schaffner ‘19):

\[ a \in \mathcal{R} \{0,1\}^\ell_c \]

\[ c \in \mathcal{R} \{0,1\}^\ell_c \]

\[ r \]
QROM security

The FS transformation is secure in the QROM (Don, Fehr, M, Schaffner ’19):

\[ a \in \mathbb{R} \{0,1\}^{\ell_c} \]

Success probability: \( \varepsilon(\mathcal{S}[\mathcal{A}]) \geq \frac{\varepsilon(\mathcal{A})}{O(q^2)} \)
Technique

\[ x \rightarrow a, r(x, a, H(x, a)) \rightarrow b \]
Suppose $r$ was injective $\implies \mathcal{A}$ essentially needs to classically query $H$ on $(x, a)$.
Suppose $r$ was injective $\Rightarrow$ $A$ essentially needs to classically query $H$ on $(x, a)$. 
Technique

Suppose $r$ was injective $\implies A$ essentially needs to classically query $H$ on $(x, a)$.

**Measure-and-Reprogram:** Pick a random query, measure it and reprogram with $c$ from the $\Sigma$-protocol.
Popular belief about QROM: Grover speed-up is as good as it gets.
Long term goal

Popular belief about QROM: Grover speed-up is as good as it gets.

⟹ Dream: QROM-to-ROM reduction should solve all our problems!
Popular belief about QROM: Grover speed-up is as good as it gets.

Dream: QROM-to-ROM reduction should solve all our problems!

Reality:
Popular belief about QROM: Grover speed-up is as good as it gets.

Dream: QROM-to-ROM reduction should solve all our problems!

Reality: QROM security of FS
Summary

- The (Q)ROM is extremely useful for efficient cryptography
- Quantum theory complicates things, much less coherent picture of QROM security
- Important cases solved, e.g. Fiat Shamir
- General reduction from QROM to ROM would be nice to have!