Random Oracles in the Real World

Gaëtan Leurent    Thomas Peyrin

Eurocrypt 2018 Rump Session
Practical Cryptography

Crypto/Eurocrypt community is focused on practical cryptography

- Practical Homomorphic MACs for Arithmetic Circuits. [EC13]
- Practical Multilinear Maps over the Integers. [CR13]
- Practical Bootstrapping in Quasilinear Time. [CR13]
- Valiant’s Universal Circuit is Practical. [EC16]
- Practical Functional Encryption for Quadratic Functions with Applications to Predicate Encryption. [CR17]
- Another Step Towards Realizing Random Oracles: Non-Malleable Point Obfuscation [EC18]
Crypto/Eurocrypt community is focused on practical cryptography

- Practical Homomorphic MACs for Arithmetic Circuits. [EC13]
- Practical Multilinear Maps over the Integers. [CR13]
- Practical Bootstrapping in Quasilinear Time. [CR13]
- Valiant’s Universal Circuit is Practical. [EC16]
- Practical Functional Encryption for Quadratic Functions with Applications to Predicate Encryption. [CR17]
- Another Step Towards Realizing Random Oracles: Non-Malleable Point Obfuscation [EC18]
Crypto/Eurocrypt community is focused on practical cryptography

- Practical Homomorphic MACs for Arithmetic Circuits. [EC13]
- Practical Multilinear Maps over the Integers. [CR13]
- Practical Bootstrapping in Quasilinear Time. [CR13]
- Valiant’s Universal Circuit is Practical. [EC16]
- Practical Functional Encryption for Quadratic Functions with Applications to Predicate Encryption. [CR17]
- Another Step Towards Realizing Random Oracles: Non-Malleable Point Obfuscation [EC18]
Practical Cryptography

Crypto/Eurocrypt community is focused on practical cryptography

- Practical Homomorphic MACs for Arithmetic Circuits. [EC13]
- Practical Multilinear Maps over the Integers. [CR13]
- Practical Bootstrapping in Quasilinear Time. [CR13]
- Valiant’s Universal Circuit is Practical. [EC16]
- Practical Functional Encryption for Quadratic Functions with Applications to Predicate Encryption. [CR17]
- Another Step Towards Realizing Random Oracles: Non-Malleable Point Obfuscation [EC18]
Practical Cryptography

Crypto/Eurocrypt community is focused on practical cryptography

- Practical Homomorphic MACs for Arithmetic Circuits. [EC13]
- Practical Multilinear Maps over the Integers. [CR13]
- Practical Bootstrapping in Quasilinear Time. [CR13]
- Valiant’s Universal Circuit is Practical. [EC16]
- Practical Functional Encryption for Quadratic Functions with Applications to Predicate Encryption. [CR17]
- Another Step Towards Realizing Random Oracles: Non-Malleable Point Obfuscation [EC18]
Practical Cryptography

Crypto/Eurocrypt community is focused on practical cryptography

- Practical Homomorphic MACs for Arithmetic Circuits. [EC13]
- Practical Multilinear Maps over the Integers. [CR13]
- Practical Bootstrapping in Quasilinear Time. [CR13]
- Valiant’s Universal Circuit is Practical. [EC16]
- Practical Functional Encryption for Quadratic Functions with Applications to Predicate Encryption. [CR17]
- Another Step Towards Realizing Random Oracles: Non-Malleable Point Obfuscation [EC18]
Practical Cryptography

Crypto/Eurocrypt community is focused on practical cryptography

- Practical Homomorphic MACs for Arithmetic Circuits. [EC13]
- Practical Multilinear Maps over the Integers. [CR13]
- Practical Bootstrapping in Quasilinear Time. [CR13]
- Valiant’s Universal Circuit is Practical. [EC16]
- Practical Functional Encryption for Quadratic Functions with Applications to Predicate Encryption. [CR17]
- Another Step Towards Realizing Random Oracles: Non-Malleable Point Obfuscation [EC18]
**A New Model**

- What if we don’t have access to these powerful constructions?
  - Very restricted model: *cruptography*

**The CRAP model**

- Computation is limited to $O(1)$.
- Hardware leaks in unknown ways.
- Users are stupid.
- Oracles not available.

**A new kind of cryto!**

- Completely theoretical, but interesting questions
  - Single-Party Computation is possible
  - Fully Homomorphic Computation is possible
- Maybe we could have a few papers in the CRAP model in the program?
A New Model

What if we don’t have access to these powerful constructions?
  ▶ Very restricted model: craptography

The CRAP model

- Computation is limited to $O(1)$.
- Hardware leaks in unknown ways.
- Users are stupid.
- Oracles not available.

A new kind of cryto!
  ▶ Completely theoretical, but interesting questions
    ▶ Single-Party Computation is possible
    ▶ Fully Homomorphic Computation is possible
  ▶ Maybe we could have a few papers in the CRAP model in the program?
A New Model

- What if we don’t have access to these powerful constructions?
  - Very restricted model: craptography

The CRAP model

- Computation is limited to $O(1)$.
- Hardware leaks in unknown ways.
- Users are stupid.
- Oracles not available.

- A new kind of cryto!
  - Completely theoretical, but interesting questions
    - Single-Party Computation is possible
    - Fully Homomorphic Computation is possible
  - Maybe we could have a few papers in the CRAP model in the program?
Replacing Random Oracles in the CRAP Model

Hash function

\[ \begin{align*}
IV & \xrightarrow{h} m_0 \xrightarrow{h} m_1 \xrightarrow{h} m_2 \xrightarrow{|M|} g \xrightarrow{H(M)} H(M) \\
\end{align*} \]

- Public function \( \{0, 1\}^* \rightarrow \{0, 1\}^n \)

Collision resistance

Given \( F \), hard to find \( M_1 \neq M_2 \) s.t. \( F(M_1) = F(M_2) \).

- No key: no good security definition
  - Any fixed function has collisions...
Hash functions cryptanalysis

**Collision resistance**

- Find \( M_1 \neq M_2 \) s. t. \( H(M_1) = H(M_2) \)
- Arbitrary common prefix/suffix, random collision blocks
- Breaks integrity verification
- Breaks signatures (in theory)

**Chosen-prefix collision resistance**

- Given \( P_1, P_2 \), find \( M_1 \neq M_2 \) s. t. \( H(P_1 \parallel M_1) = H(P_2 \parallel M_2) \)
- Breaks certificates
  - [Stevens & al, Crypto’09]
- Breaks TLS, IPsec, SSH
  - [Bhargavan & L, NDSS’16]
A concrete example: SHA-1

1993  Designed by NSA
1995  SHA-0 tweaked to SHA-1
1998  SHA-0 collision attack
2005  SHA-1 collision attack in theory
2017  SHA-1 collision attack in practice

SHA-1 in 2018

- Being phased out of web certificates
  - Still possible to buy SHA-1 certificates
  - Still accepted by many email clients
- Still used to authenticated handshake messages
  - 5% of top 1M HTTPS servers prefer SHA-1
- Can we do chosen-prefix collisions?
A concrete example: SHA-1

1993 Designed by NSA
1995 SHA-0 tweaked to SHA-1
1998 SHA-0 collision attack
2005 SHA-1 collision attack in theory
2017 SHA-1 collision attack in practice

SHA-1 in 2018

- Being phased out of web certificates
  - Still possible to buy SHA-1 certificates
  - Still accepted by many email clients
- Still used to authenticated handshake messages
  - 5% of top 1M HTTPS servers prefer SHA-1
- Can we do chosen-prefix collisions?

'Tis but a scratch.
A concrete example: SHA-1

1993  Designed by NSA
1995  SHA-0 tweaked to SHA-1
1998  SHA-0 collision attack
2005  SHA-1 collision attack in theory
2017  SHA-1 collision attack in practice

SHA-1 in 2018

- Being phased out of web certificates
  - Still possible to buy SHA-1 certificates
  - Still accepted by many email clients
- Still used to authenticated handshake messages
  - 5% of top 1M HTTPS servers prefer SHA-1
- Can we do chosen-prefix collisions?

I’ve had worse
A concrete example: SHA-1

1993  Designed by NSA
1995  SHA-0 tweaked to SHA-1
1998  SHA-0 collision attack
2005  SHA-1 collision attack in theory
2017  SHA-1 collision attack in practice

SHA-1 in 2018

- Being phased out of web certificates
  - Still possible to buy SHA-1 certificates
  - Still accepted by many email clients
- Still used to authenticated handshake messages
  - 5% of top 1M HTTPS servers prefer SHA-1
- Can we do chosen-prefix collisions?

Just a flesh wound.
A concrete example: SHA-1

1993  Designed by NSA
1995  SHA-0 tweaked to SHA-1
1998  SHA-0 collision attack
2005  SHA-1 collision attack in theory
2017  SHA-1 collision attack in practice

SHA-1 in 2018

- Being phased out of web certificates
  - Still possible to buy SHA-1 certificates
  - Still accepted by many email clients
- Still used to authenticated handshake messages
  - 5% of top 1M HTTPS servers prefer SHA-1
- Can we do chosen-prefix collisions?

Alright. We’ll call it a draw.
A concrete example: SHA-1

1993  Designed by NSA
1995  SHA-0 tweaked to SHA-1
1998  SHA-0 collision attack
2005  SHA-1 collision attack in theory
2017  SHA-1 collision attack in practice

SHA-1 in 2018

- Being phased out of web certificates
  - Still possible to buy SHA-1 certificates
  - Still accepted by many email clients
- Still used to authenticated handshake messages
  - 5% of top 1M HTTPS servers prefer SHA-1

Alright. We’ll call it a draw.

- Can we do chosen-prefix collisions?
## A concrete example: SHA-1

### 1993
- Designed by NSA

### 1995
- SHA-0 tweaked to SHA-1

### 1998
- SHA-0 collision attack

### 2005
- SHA-1 collision attack in theory

### 2017
- SHA-1 collision attack in practice

### SHA-1 in 2018

- **Being phased out** of web certificates
  - Still possible to buy SHA-1 certificates
  - Still accepted by many email clients
- **Still used** to authenticated handshake messages
  - 5% of top 1M HTTPS servers prefer SHA-1
- Can we do chosen-prefix collisions?
**Chosen-prefix collision attack**

**Differential trails**
- Start from **linear core trail**
- Non-linear part connects to arbitrary input differential
- Relaxing the last rounds $\leadsto$ output difference set $S$

**Birthday phase**

Application to SHA-1
- $|S| = 192$
- **Complexity:** $2^{77.1}$

[Stevens, Eurocrypt’13]
New techniques

1. Larger set of output differences for SHA-1
2. Multi-block technique using a single core trail
3. Dynamic selection of near-collision targets (clustering)

- Complexity: $2^{66.9} - 2^{69.3}$ (depending on assumptions for NL part)
- Almost practical!

(192 → 8768) $|S| \approx 2^{30}$
New techniques

1. Larger set of output differences for SHA-1 (192 → 8768)  
2. Multi-block technique using a single core trail  
3. Dynamic selection of near-collision targets (clustering)

- Complexity: $2^{66.9} - 2^{69.3}$ (depending on assumptions for NL part)
- Almost practical!

Gaëtan Leurent, Thomas Peyrin
Random Oracles in the Real World
Eurocrypt 2018 Rump Session