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]

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]

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: craptography

The CRAP model

- Computation is limited to $\mathcal{O}(1)$.
- 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 $\mathcal{O}(1)$.
- 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

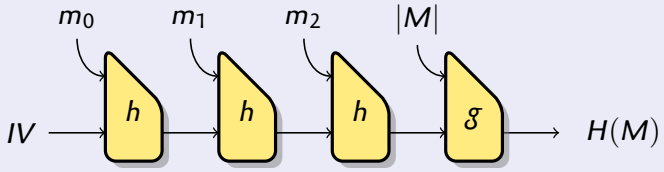
- What if we don't have access to these powerful constructions?
  - Very restricted model: craptography

The CRAP model

- Computation is limited to $\mathcal{O}(1)$.
- 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?

Hash function



- Public function $\{0,1\}^* \to \{0,1\}^n$

Collision resistance

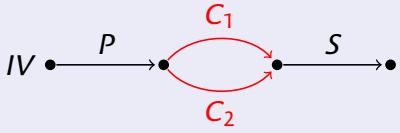
Given F, hard to find $M_1 \neq M_2$ s.t. $F(M_1) = F(M_2)$.

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

Hash functions cryptanalysis

Collision resistance

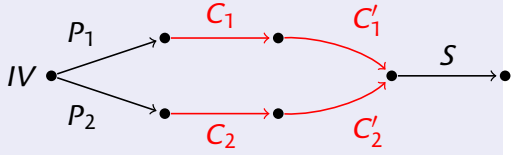
- Find $M_1 \neq M_2$ s. t. $H(M_1) = H(M_2)$



- 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

'Tis but a scratch.

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

I've had worse

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

Just a flesh wound.

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

Alright.
We'll call it a draw.

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

Alright.
We'll call it a draw.

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

Alright.
We'll call it a draw.

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

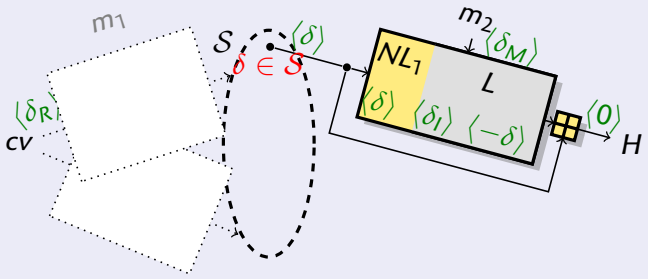
- Can we do chosen-prefix collisions?

Chosen-prefix collision attack

Differential trails

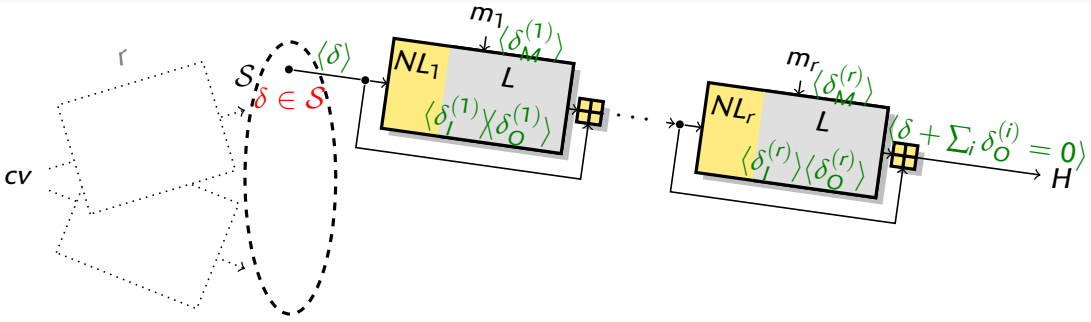
- Start from linear core trail
- Non-linear part connects to arbitrary input differential
- Relaxing the last rounds $\rightsquigarrow$ output difference set $\mathcal{S}$

Birthday phase



- Application to SHA-1 [Stevens, Eurocrypt'13]
  - $|\mathcal{S}| = 192$
  - Complexity: $2^{77.1}$

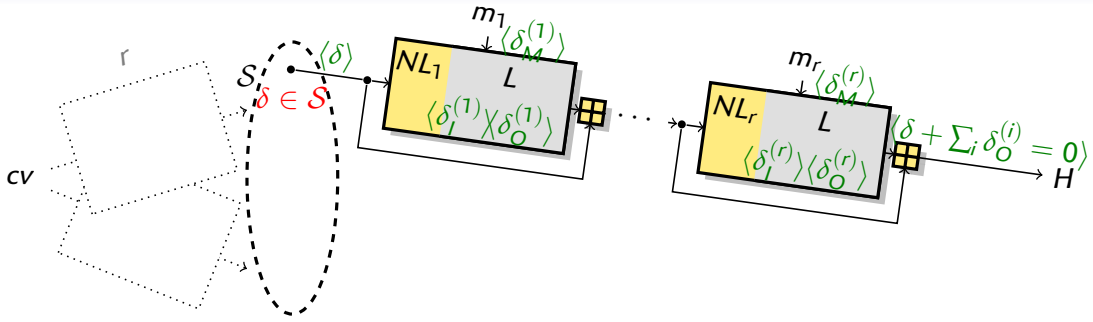
New techniques



1. Larger set of output differences for SHA-1 $(192 \rightarrow 8768)$
2. Multi-block technique using a single core trail $|\mathcal{S} \approx 2^{30}|$
3. Dynamic selection of near-collision targets (clustering)

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

New techniques



1. Larger set of output differences for SHA-1 $(192 \rightarrow 8768)$
2. Multi-block technique using a single core trail $|\mathcal{S} \approx 2^{30}|$
3. Dynamic selection of near-collision targets (clustering)

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