Tight and Optimal Reductions for Signatures based on Average Trapdoor Preimage Sampleable Functions and Applications to Code-Based Signatures

André Chailloux and Thomas Debris-Alazard

Inria Saclay,
EPI GRACE

Security Reduction

Given a cryptographic scheme and a problem $\mathcal{P}$, prove:

Break the scheme in time $t \implies$ Solve $\mathcal{P}$ in time $C(t) \times t$
(*Security Reduction* to $\mathcal{P}$ with t' lost)

Consequence: No algorithm to solve $\mathcal{P}$ in time $< t$

$\implies$ No algorithm to break the scheme in time $< \frac{t}{C(t)}$

- Tight Security Reduction to $\mathcal{P}$:

  Breaking the scheme in time $t \implies$ Breaking $\mathcal{P}$ in time $\approx t$

Security Reduction

Given a cryptographic scheme and a problem $\mathcal{P}$, prove:

$$\text{Break the scheme in time } t \implies \text{Solve } \mathcal{P} \text{ in time } C(t) \times t$$

(*Security Reduction* to $\mathcal{P}$ with t' lost)

Consequence: No algorithm to solve $\mathcal{P}$ in time $< t$

$$\implies \text{No algorithm to break the scheme in time} < \frac{t}{C(t)}$$

- Tight Security Reduction to $\mathcal{P}$:

  Breaking the scheme in time $t \implies$ Breaking $\mathcal{P}$ in time $\approx t$

Prime example where difficulties occur: the Random Oracle Model (mostly for signatures)

Random Oracle

- The scheme needs a function that behaves like a random function (like FDH signatures),

  $\rightarrow$ Use a hash function $\mathcal{H}$ as SHA-256

- ROM: when proving the security, $\mathcal{H}$ is modelled as a random function,

  $\rightarrow$ $\mathcal{H}$ is accessed only via a black box manner

- Idealized model: allows tighter and simpler proofs.

Quantum Random Oracle

If an adversary has access to a quantum computer,

- For any classical circuit C, there exists a quantum unitary $\mathcal{O}_C$ such that:
  - superposition computation, $\mathcal{O}_C(|x\rangle|0\rangle) = |x\rangle|C(x)\rangle$
  - running time $\mathcal{O}_C \approx$ running time C
- Additional capability of the quantum attacker in the QROM:

  $\rightarrow$ call $\mathcal{O}_{\mathcal{H}}$ and not only $\mathcal{H}$

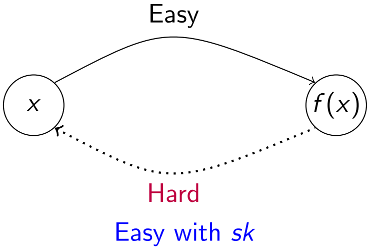
  - Gives additional power: crucial for Grover's algorithm, collision finding...
  - Natural

Full Domain Hash Signatures

- $\mathcal{H}(\cdot)$ hash function,

  $\rightarrow$ $\mathcal{H}$ is modelled with a random function

- f trapdoor one-way function



- To sign m:

  Compute with sk, $\sigma \in f^{-1}(\mathcal{H}(\mathrm{m}))$.

(Q)EUF-CMA

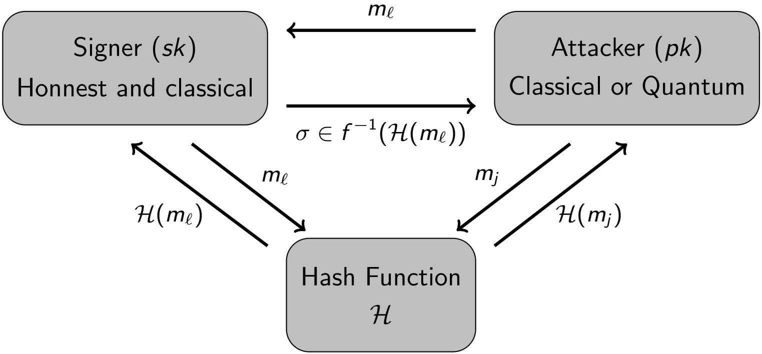
Signer (sk)
Honnest and classical

Attacker (pk)
Classical or Quantum

Hash Function
$\mathcal{H}$

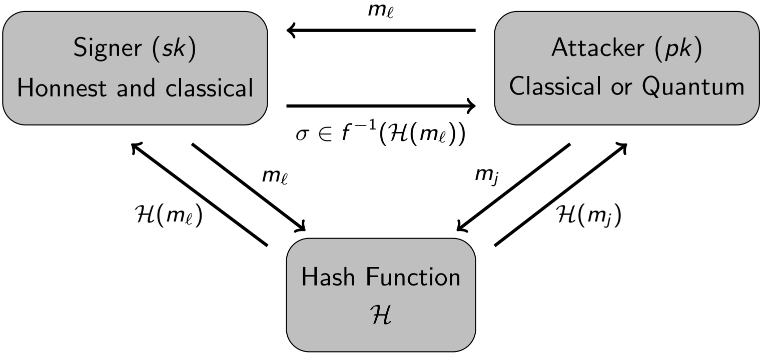
1. The signer honestly generates (sk, pk)

(Q)EUF-CMA



1. The signer honestly generates (sk, pk)
2. Attacker (either quantum or classical) can ask the Signer to sign some messages m_ℓ (classical sign queries)

(Q)EUF-CMA



1. The signer honestly generates (sk, pk)
2. Attacker (either quantum or classical) can ask the Signer to sign some messages m_ℓ (classical sign queries)
3. Attacker goal: produce a signature of a message not signed by the Signer

$\rightarrow$ If quantum can use a $\mathcal{O}_{\mathcal{H}}$ (QROM)

Gentry-Peikert-Vaikuntanathan Approach

- f trapdoor OW-function

$\rightarrow$ Cannot sign with only pk!

But... attacker has access to signatures: leakage on sk?

Add properties to f: preimage sampleable function (TPSF)!

Gentry-Peikert-Vaikuntanathan Approach

- f trapdoor OW-function

$\rightarrow$ Cannot sign with only pk!

But... attacker has access to signatures: leakage on sk?

Add properties to f: preimage sampleable function (TPSF)!

$\mathcal{D}$ be a distribution independent of sk,

1. $\forall y$: $x \overset{sk}{\leftarrow} f^{-1}(y) \overset{close}{\sim} x \leftarrow \mathcal{D}$ conditioning on $f(x) = y$
2. $f(x)$ when $x \leftarrow \mathcal{D} \overset{close}{\sim}$ Uniform

Application to Lattices[GPV08]

- f is OW = ISIS[1]

- With preimage sampleable property

  → Tight security reduction to Collision problem

$$\text{Collision} \approx \mathsf{SIS}^2 \preccurlyeq \text{ Signature } \preccurlyeq \text{One way} = \mathsf{ISIS} \approx \mathsf{SIS}.$$

[1] ISIS: Inhomogeneous Short Integer Solution

[2] SIS: Short Integer Solution problem commonly used in lattice-based cryptography

Application to Lattices[GPV08]

- f is OW = ISIS[1]
- With preimage sampleable property

  → Tight security reduction to Collision problem

$$\text{Collision} \approx \mathsf{SIS}^2 \preccurlyeq \text{ Signature } \preccurlyeq \text{One way} = \mathsf{ISIS} \approx \mathsf{SIS}.$$

Two Questions

1. Tight security reduction: necessary to collision?
2. Preimage sampleable : property hard to meet

   → Relax?

[1] ISIS: Inhomogeneous Short Integer Solution

[2] SIS: Short Integer Solution problem commonly used in lattice-based cryptography

This Work

- Relaxation TPSF $\rightarrow$ Average TPSF
- Tight security reduction to a Claw with Random Function Problem
$$\text{Collision} \preccurlyeq \begin{array}{c}\text{Claw(RF)}\\ \Updownarrow \\ \text{Signature}\end{array} \preccurlyeq \text{One way.}$$
- Extension of these results in the QROM
- Application to Wave a code-based signature
  $\rightarrow$ Crucial in this case: Collision is easy!

Average TPSF

$f : \mathcal{E} \longrightarrow \mathcal{F}$: be a $(\varepsilon_1, \varepsilon_2)$-TPSF for the distribution $\mathcal{D}$

- Δ be the statistical distance

1. Trap. algo: $\forall \mathsf{s}$:

$$\Delta(f^{-1}(\mathsf{s}), \mathsf{e}_\mathsf{s}) = \varepsilon_1 \text{ where } \mathsf{e}_\mathsf{s} \stackrel{\$}{\leftarrow} \mathcal{D} \text{ knowing } f(\mathsf{e}_\mathsf{s}) = \mathsf{s}.$$

2. $\Delta(f(\mathsf{e}), \mathsf{s}^{\mathsf{unif}}) = \varepsilon_2$

$$\text{where } \mathsf{e} \stackrel{\$}{\leftarrow} \mathcal{D} \text{ and } \mathsf{s}^{\mathsf{unif}} \text{ unif distributed over } \mathcal{S}.$$

Average TPSF

$f : \mathcal{E} \longrightarrow \mathcal{F}$: be a $(\varepsilon_1, \varepsilon_2)$-TPSF for the distribution $\mathcal{D}$

- Δ be the statistical distance

1. Trap. algo: $\forall \mathsf{s}$:

$$\Delta(f^{-1}(\mathsf{s}), \mathsf{e_s}) = \varepsilon_1 \text{ where } \mathsf{e_s} \xleftarrow{\$} \mathcal{D} \text{ knowing } f(\mathsf{e_s}) = \mathsf{s}.$$

2. $\Delta(f(\mathsf{e}), \mathsf{s}^{\mathrm{unif}}) = \varepsilon_2$

$$\text{where } \mathsf{e} \xleftarrow{\$} \mathcal{D} \text{ and } \mathsf{s}^{\mathrm{unif}} \text{ unif distributed over } \mathcal{S}.$$

We relax to ε-ATPSF

$$\text{Only: } \Delta(f^{-1}(\mathsf{s}^{\mathrm{unif}}), \mathsf{e}) = \varepsilon$$

Average TPSF

$f : \mathcal{E} \longrightarrow \mathcal{F}$: be a $(\varepsilon_1, \varepsilon_2)$-TPSF for the distribution $\mathcal{D}$

- Δ be the statistical distance

1. Trap. algo: $\forall \mathsf{s}$:

$$\Delta(f^{-1}(\mathsf{s}), \mathsf{e}_\mathsf{s}) = \varepsilon_1 \text{ where } \mathsf{e}_\mathsf{s} \xleftarrow{\$} \mathcal{D} \text{ knowing } f(\mathsf{e}_\mathsf{s}) = \mathsf{s}.$$

2. $\Delta(f(\mathsf{e}), \mathsf{s}^{\mathrm{unif}}) = \varepsilon_2$

$$\text{where } \mathsf{e} \xleftarrow{\$} \mathcal{D} \text{ and } \mathsf{s}^{\mathrm{unif}} \text{ unif distributed over } \mathcal{S}.$$

We relax to ε-ATPSF

Only: $\Delta(f^{-1}(\mathsf{s}^{\mathrm{unif}}), \mathsf{e}) = \varepsilon$

If ε-ATPS then $(\varepsilon_1, \varepsilon_2)$-ATPS with $\begin{cases} \varepsilon_1 \approx \varepsilon^2 \\ \varepsilon_2 = \varepsilon \end{cases}$

(A)TPSF

- TPSF: Falcon a lattice-based signature
- ATPSF: Wave a code-based signature

Claw with Random Function Problem

Problem (Claw with Random Function - Claw(RF))

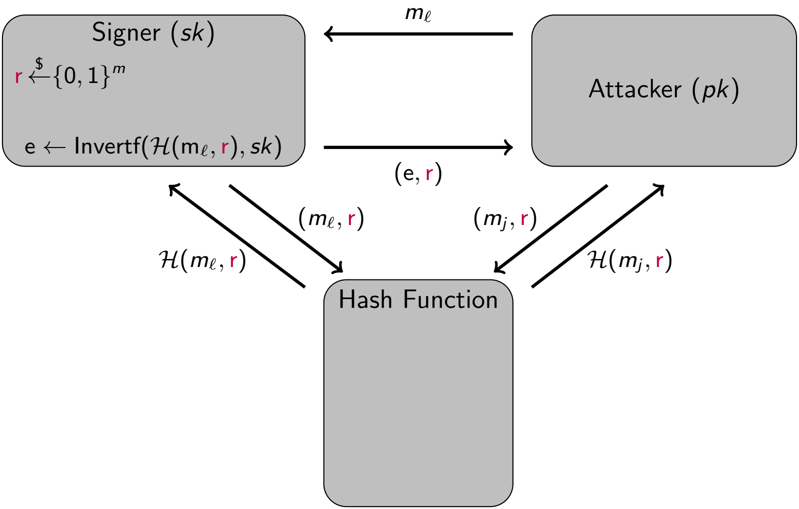
- Instance: *a function f and a random function h to which we only have black box access.*
- Goal: *find x, y such that $f(x) = h(y)$.*

Breaking the problem in time t with q queries to h and f ATPSF,

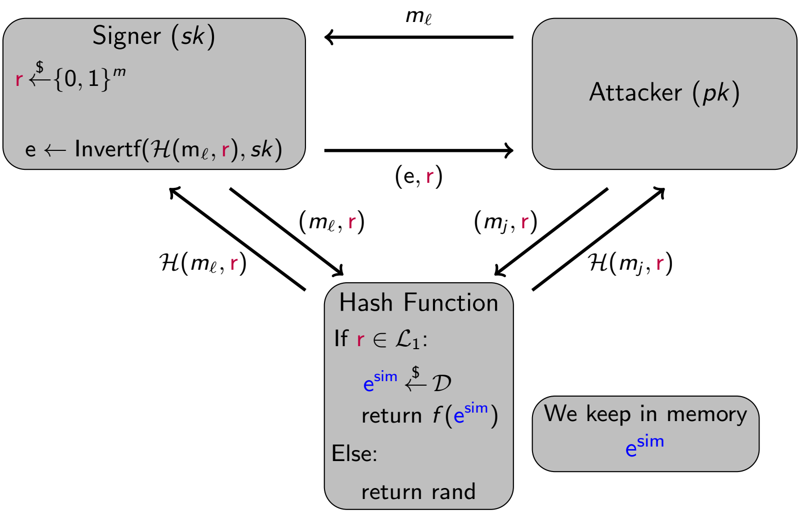
$$\Rightarrow \text{ Invert } f \text{ in time } q \times t$$

One can see Claw(RF) as trying to invert f with "*multiple random targets*"

Sketch of the Proof

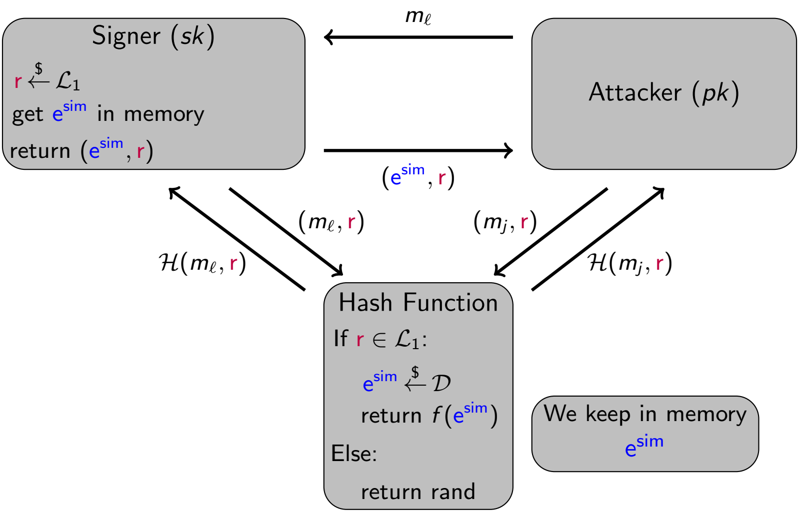


Sketch of the Proof



- We create a random list $\mathcal{L}_1 \subseteq \{0,1\}^m$ of salts r

Sketch of the Proof



- We create a random list $\mathcal{L}_1 \subseteq \{0,1\}^m$ of salts r

Quantum Case[Zhandry 12']

- Distribution $\mathrm{Fun}_{\mathcal{T}}$: $h \leftarrow \mathrm{Fun}_{\mathcal{T}}$ means that for each x, $h(x) \stackrel{\$}{\leftarrow} \mathcal{T}$

Proposition

Let $\mathcal{A}^{\mathrm{ROM}}$ be a quantum query algorithm running in time t and making q queries to the oracle ROM.
Let $\mathcal{T}$ be a probability distribution on $\{0,1\}^m$ such that

$$\Delta(\mathcal{T}, \mathrm{Unif}(\{0,1\}^m)) \leq \varepsilon.$$

We have,

$$\left| \, \mathbb{P}\left(\mathcal{A}^{\mathrm{ROM}} = 1\right) - \mathbb{P}\left(\mathcal{A}^{g} = 1 : g \leftarrow \mathrm{Fun}_{\mathcal{T}}\right) \right| \leq \frac{8\pi}{\sqrt{3}} q^{3/2}\sqrt{\varepsilon}.$$

Conclusion

- Relaxation of GPV's conditions to make signatures with a tight security reduction to Claw(RF)

New Opportunities?

- Application to code-based signatures: Claw(RF) $=$ Decoding One Out of Many (DOOM)

$$\mathrm{DOOM} \approx \mathrm{One\ Way} \text{ for Wave parameters}$$

$$\mathrm{One\ Way} \approx \mathrm{DOOM} = \mathrm{Signature} \preccurlyeq \mathrm{One\ way}.$$

Conclusion

- Relaxation of GPV's conditions to make signatures with a tight security reduction to Claw(RF)

New Opportunities?

- Application to code-based signatures: Claw(RF) = Decoding One Out of Many (DOOM)

$$\mathrm{DOOM} \approx \mathrm{One\ Way}\ \text{for Wave parameters}$$

$$\mathrm{One\ Way} \approx \mathrm{DOOM} = \mathrm{Signature} \preccurlyeq \mathrm{One\ way}.$$

Thank You!