Probabilistic Hash-and-Sign with Retry in the Quantum Random Oracle Model

Haruhisa Kosuge [1] Keita Xagawa [2]

[1]Japan Ministry of Defense

[2]Technology Innovation Institute

April 16, 2024

Table of Contents

1. Background

2. New Security Proof

3. Applications

4. Summary

Table of Contents

1. Background

2. New Security Proof

3. Applications

4. Summary

Hash-and-sign in NIST PQC

- In 2023, NIST issued additional call for digital signatures for diversity of portfolio.
- Hash-and-sign is adopted in many candidates (14 out of 40).

Hash-and-sign signatures among additional candidates.

Lattice	**Multivariate**	**Code**
HAWK, HuFu, Squirrels	3WISE, HPPC, MAYO, PROV, QR-UOV, SNOVA, TUOV, UOV, VOX	Enhanced pqsigRM, Wave

Hash-and-sign signatures are promissing candidates.

Hash-and-sign

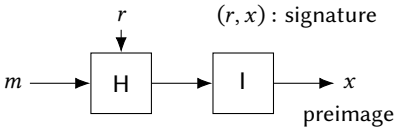
Key generation

$(\mathsf{F}, \mathsf{I}) \leftarrow \mathsf{Gen}(1^\lambda)$

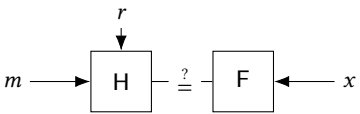
F : hard-to-invert function = verification key

I : trapdoor of F = secret key

Signature generation

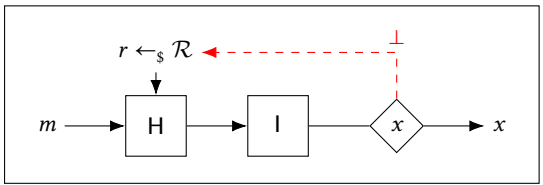


Signature verification



Variations:

- Deterministic hash-and-sign : r is null.
- Probabilistic hash-and-sign : r is random.
- Probabilistic hash-and-sign with retry :

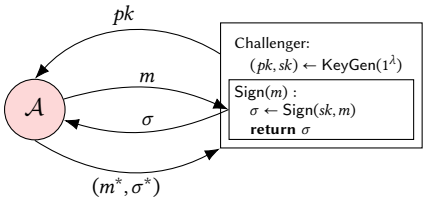


Easier to build signature, harder to prove security.

e.g. surjection is not required.

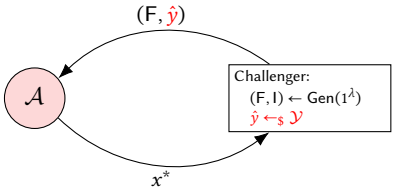
Security Definition

EUF-CMA



$\epsilon_{\mathsf{cma}} = \Pr[\mathsf{Vrfy}(m^*, \sigma^*) = \top \wedge (m^* \text{ was not queried})]$
(EUF-NMA: no signing query)

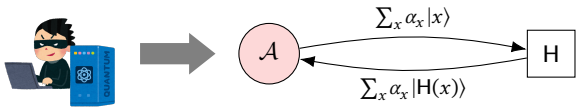
Non-invertibility (INV)



$\epsilon_{\mathsf{inv}} = \Pr[\mathsf{F}(x^*) = \hat{y}]$
(One-wayness: $\hat{y} = \mathsf{F}(x)$ for $x \leftarrow_{\$} \mathcal{X}$)

Provable security requires INV⇒EUF-CMA or CR⇒EUF-CMA.
(CR: Collision Resistance)

(Quantum) Random Oracle Model



Real-world QROM

- INV ⇒ EUF-CMA or CR ⇒ EUF-CMA is proven in (Q)ROM.
- Since QROM models adversary implementing hash function in quantum computer, post-quantum signatures must be provable secure in QROM.

Secure signatures in ROM are not always secure in QROM [YZ22].

[YZ22] Yamanaka, Zhandry (FOCS2022)

Provable Security of Hash-and-sign

Summary on provable security of hash-and-sign

Paradigm	Assumption	Examples	Reduction (ROM)	Reduction (QROM)
deterministic	collision-resistance	Falcon (GPV)	tight [GPV08]	tight [BDH+13]
probabilistic (without retry)	non-invertibility	Wave, MAYO	poly loss [CD20][Beu21]	poly loss [YZ21] (PSF* is required.)
probabilistic with retry	non-invertibility	PROV, QR-UOV	poly loss [SSH11] (Proof is flawed.)	–

*Preimage Sampleable Function: Trapdoor function with some conditions, e.g., F is uniform and surjection.

[GPV08] Gentry, Peikert, Vaikuntanathan (STOC2008)

[BDH+13] Boneh et al. (ASIACRYPT2011)

[YZ21] Yamakawa, Zhandry (EUROCRYPT2021)

[CD20] Chailloux, Debris-Alazard (PKC 2020)

[Beu21] Beullens (SAC2021)

[SSH11] Sakumoto, Shirai, Hiwatari (PQCRYPTO2011)

Table of Contents

1. Background

2. New Security Proof

3. Applications

4. Summary

Overview of New Security Proof

INV⇒EUF-CMA for probabilistic hash-and-sign with retry in QROM

(EUF-NMA ⇒EUF-CMA + INV ⇒EUF-NMA)

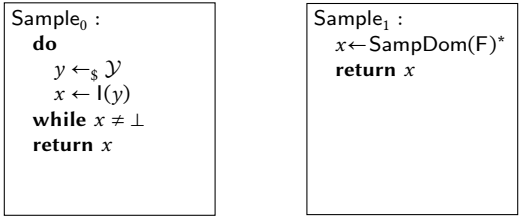
$$\epsilon_{\mathsf{cma}} \leq (2q_{\mathsf{qro}}+1)^2\epsilon_{\mathsf{inv}} + \epsilon_{\mathsf{ps}} + \frac{3}{2}q'_{\mathsf{sign}}\sqrt{\frac{q'_{\mathsf{sign}}+q_{\mathsf{qro}}+1}{2^{|r|}}} + 2(q_{\mathsf{qro}}+2)\sqrt{\frac{q'_{\mathsf{sign}}-q_{\mathsf{sign}}}{2^{|r|}}}$$

q_{qro} : # QRO queries.
q_{sign} : # signing queries.
q'_{sign} : # retries of r.

ϵ_{cma} : advantage for EUF-CMA.
ϵ_{inv} : advantage for non-invertibility.
ϵ_{ps} : explain later.

To make ϵ_{ps} negligible, outputs of trapdoor must be simulatable.

Simulatability of Trapdoor

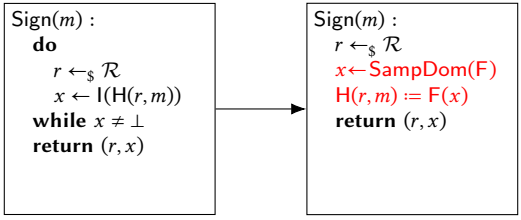


* SampDom : function to simulate preimange-sampling.

- ϵ_{ps} : advantage to distinguish Sample_0 from Sample_1.
- "Negligible ϵ_{ps}" is weakened condition of PSF and computational bound is applicable.

Some trapdoor functions are not PSF but satisfy negligible ϵ_{ps}.

Flaw of Proof in ROM [SSH11]

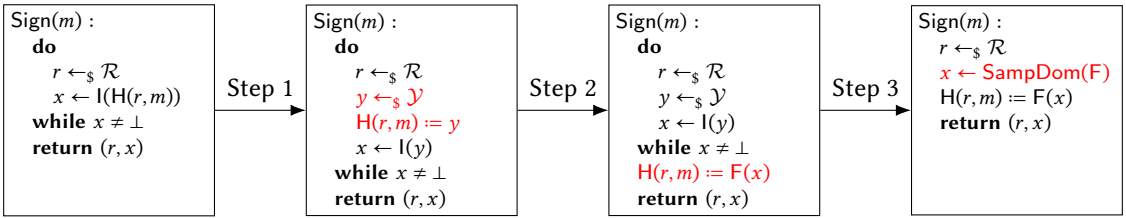


Modification of signing oracle in [SSH11]

- Assuming negligible ϵ_{ps}, signing oracle is simulated by (re)programming $\mathsf{H}(r, m) := \mathsf{F}(x)$.
- Since $\mathsf{F}(x)$ is not uniform, H is no longer random function.

[SSH11] Sakumoto, Shirai, Hiwatari (PQCRYPTO2011)

EUF-NMA ⇒ EUF-CMA in QROM



Modification of signing oracle in our proof

Step 1 : Tight adaptive reprogramming [GHHM21] enables reprogramming H.
Step 2 : Semi-classical O2H [AHU19] cancels reprogramming during retries.
Step 3 : Negligible ϵ_{ps} enables simulation without trapdoor.

[GHHM21] Grilo, Hövelmanns, Hülsing, Majenz (ASIACRYPT2021)
[AHU19] Ambainis, Hamburg, Unruh (CRYPTO2019)

INV ⇒ EUF-NMA in QROM

$\mathcal{A}_{\mathsf{inv}}(\mathsf{F}, \hat{y})$:
  $\mathsf{H} \leftarrow_{\$} \mathcal{Y}^{\mathcal{R}\times\mathcal{M}}$
  $j \leftarrow_{\$} [q_{\mathsf{qro}}]$
  run $\mathcal{A}_{\mathsf{nma}}^{|\mathsf{H}\rangle}(\mathsf{F})$ until j-th query
  measure j-th query as (r', m')
  $\mathsf{H}(r', m') := \hat{y}$
  run $\mathcal{A}_{\mathsf{nma}}^{|\mathsf{H}\rangle}(\mathsf{F})$ until end
  $(m^*, r^*, x^*) \leftarrow \mathcal{A}_{\mathsf{nma}}^{|\mathsf{H}\rangle}(\mathsf{F})$
  return x^*

INV adversary simulating EUF-NMA adversary

Measure-and-reprogram technique [DFM20] results in $\epsilon_{\mathsf{nma}} \leq (2q_{\mathsf{qro}} + 1)^2 \epsilon_{\mathsf{inv}}$.

[DFM20] Don, Fehr, Majenz (CRYPTO2020)

Table of Contents

1. Background

2. New Security Proof

3. Applications

4. Summary

Applications of New Security Proof

Complete 🤗

Updated summary on provable security of hash-and-sign

Paradigm	Assumption	Examples	Reduction (ROM)	Reduction (QROM)
deterministic	collision-resistance	Falcon (GPV)	tight [GPV08]	tight [BDH+13]
probabilistic (without retry)	non-invertibility	Wave, MAYO	poly loss [CD20][Beu21]	poly loss (PSF is not required.)
probabilistic with retry	non-invertibility	PROV, QR-UOV*	poly loss	poly loss

* PROV and QR-UOV adopt our proof.

[GPV08] Gentry, Peikert, Vaikuntanathan (STOC2008)

[BDH+13] Boneh et al. (ASIACRYPT2011)

[CD20] Chailloux, Debris-Alazard (PKC 2020)

[Beu21] Beullens (SAC2021)

Table of Contents

1. Background

2. New Security Proof

3. Applications

4. Summary

Summary

- First security proof for probabilistic hash-and-sign with retry in (Q)ROM.
- Our proof has wide application → Big impact on NIST PQC standardization.
- Our proof is extended to multi-key security (M-EUF-CMA security).