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

Haruhisa Kosuge [1] Keita Xagawa [2]

[1]Japan Ministry of Defense

[2]NTT Social Informatics Laboratories

November 30, 2022

Background

NIST PQC Standardization for Digital Signature

- In new call for signatures, NIST is interested in schemes not based on structured lattices.
  - Multivariate quadratic-based (MQ-based)
  - Code-based
  - Isogeny-based
  - Hash-based/Symmetric-based
- Hash-and-sign is adopted in many past/future candidates.

Post-quantum signatures with NIST security level I and more

	MQ	Code	Isogeny	Hash/Symmetric
Hash-and-sign	UOV, Rainbow, GeMSS, QR-UOV, Mayo	CFS, Wave	–	–
Fiat-shamir	MQDSS	LESS-FM, Durandal	CSI-FISH, SQISign	Picnic
Other	–	–	–	SPHINCS+

Without provable security of hash-and-sign, some candidates are not ready for standardization.

Probabilistic Hash-and-sign with Retry

Key generation

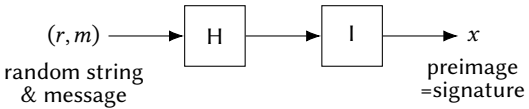
$(\mathsf{F}, \mathsf{I}) \leftarrow \mathrm{Gen}(1^\lambda)$

F : hard-to-invert function=verification key

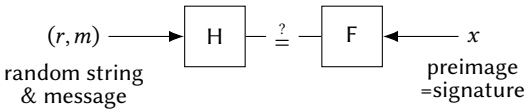
I : trapdoor of F=secret key

$\rightarrow \mathsf{I}(\mathsf{F}(x)) = x$

Signature generation



Signature verification



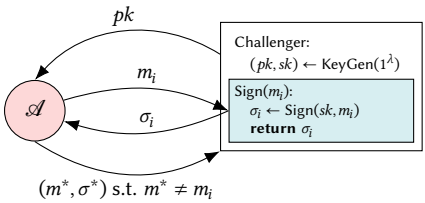
Variations of Hash-and-sign.

- Deterministic : r is null.
- Probabilistic : r is randomly chosen.
- Probabilistic with retry : retries r until obtaining x.
  (F is not surjective.)

Probabilistic hash-and-sign with retry has the largest coverage.

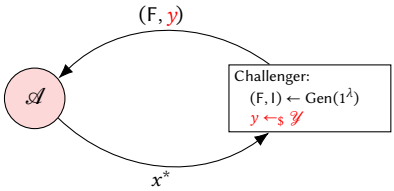
Security Definition

EUF-CMA



$\epsilon_{\mathsf{cma}} = \Pr[\mathsf{Vrfy}(m^*, \sigma^*) = \top]$
(EUF-NMA: no signing query)

Non-invertibility (INV)

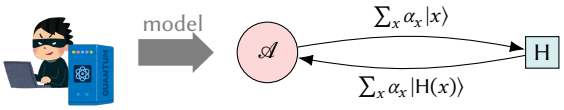


$\epsilon_{\mathsf{inv}} = \Pr[\mathsf{F}(x^*) = y]$
(One-wayness: $y = \mathsf{F}(x)$ for $x \leftarrow_\$ \mathcal{X}$)

INV⇒EUF-CMA (or CR⇒EUF-CMA)
(CR: Collision Resistance)

(Quantum) Random Oracle Model

- INV ⇒ EUF-CMA or CR ⇒ EUF-CMA is proven in (Q)ROM.
- QROM models adversary implementing hash function in quantum computer.



Real-world QROM

→ For PQC, provable security in QROM is necessary.

- Secure signature in ROM is not always secure in QROM [YZ22].

[YZ22] Yamanaka, Zhandry (FOCS2022)

Security of Hash-and-sign in QROM

Secure in ROM ⇒ Secure in QROM? Not yet known 😢

Review on provable security of hash-and-sign signatures

Schemes	Paradigm	Assumtion	Reduction (ROM)	Reduction (QROM)
Falcon, ModFalcon, Mitaka	deterministic	collision-resistance	tight [GPV08]	tight [BDH+13]
Wave	probabilistic	non-invertibility	poly loss [CD20]	–
UOV, Rainbow, GeMSS, QR-UOV, Mayo, CFS	probabilistic with retry	non-invertibility	poly loss [SSH11][Beu21][Dal07]	–

[GPV08] Gentry, Peikert, Vaikuntanathan (STOC2008)

[BDH+13] Boneh, Dagdelen, Fischlin, Lehmann, Schaffner, Zandry (ASIACRYPT2011)

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

[SSH11] Sakumoto, Shirai, Hiwatari (PQCRYPTO2011)

[Beu21] Beullens (SAC2021)

[Dal07] Dallot (WEWoRC 2007)

Existing Proofs for Hash-and-sign

Preimage Sampleable Function (PSF) [GPV08]

- Trapdoor function that x is simulatable without trapdoor in (Q)ROM.
- With domain sampling function SampDom(F), PSF satisfies:
  1. $\mathsf{F}(x)$ is uniform over $\mathcal{Y}$ for $x \leftarrow \mathsf{SampDom}(\mathsf{F})$.
  2. $x \leftarrow \mathsf{I}(y)$ and $x \leftarrow \mathsf{SampDom}(\mathsf{F})$ follow the same dist.
  3. F is surjective.
- PSF is hard to build in MQ-based and code-based crypto.
  →probabilistic hash-and-sign with retry

[GPV08] Gentry, Peikert, Vaikuntanathan (STOC2008)

Existing Proofs of EUF-CMA in QROM

Work	Assumption	PSF?	Bound
[BDH+13]	CR	PSF	$O(\epsilon_{\mathrm{cr}})$
[Zha12]	INV	PSF	$O(q^2\sqrt{\epsilon_{\mathrm{inv}}})$
Ext. of [YZ21]	INV	PSF	$O(q^4\epsilon_{\mathrm{inv}})$
[CD20]	EUF-NMA	non-PSF	$O(\epsilon_{\mathrm{nma}})$

No INV ⇒ EUF-CMA not assuming PSF
→Probabilistic hash-and-sign with retry is not covered.
(hash-and-sign not assuming PSF is not covered)

[BDH+13] Boneh, Dagdelen, Fischlin, Lehmann, Schaffner, Zandry (ASIACRYPT2011)

[Zha12] Zhandry (ePrint Archive, 2012/076)

[YZ21] Yamakawa, Zhandry (EUROCRYPT2021)

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

Q: INV ⇒ EUF-CMA for probabilistic hash-and-sign with retry can be proven in QROM?

Yes! 😉, with poly loss.

New Security Proof

Overview of New Security Proof

EUF-NMA⇒EUF-CMA

$$\epsilon_{\mathsf{cma}} \leq \epsilon_{\mathsf{nma}} + \epsilon_{\mathsf{ps}} + 3q'_{\mathsf{sign}}\sqrt{\frac{q'_{\mathsf{sign}}+q_{\mathsf{qro}}+1}{|\mathscr{R}|}}$$

(tight adaptive reprogramming technique [GHHM21].)

INV⇒EUF-NMA

$$\epsilon_{\mathsf{nma}} \leq (2q_{\mathsf{qro}}+1)^2\epsilon_{\mathsf{inv}}$$

(measure-and-reprogram technique [DFM20])

INV⇒EUF-CMA

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

→tighter than existing proofs [Zha12,YZ21].

q_{qro}: # quantum random oracle queries.

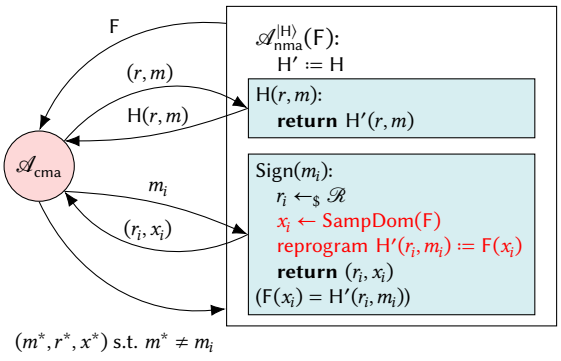
q'_{sign}: # trapdoor computations.

ϵ_{ps}: distinguishing advantage of honestly-generated and simulated preimages.
→ PSF is not necessary.

$\mathscr{R}$: space for r.

[GHHM21] Grilo, Hövelmanns, Hülsing, Majenz (ASIACRYPT2021)
[DFM20] Don, Fehr, Majenz (CRYPTO2020)
[Zha12] Zhandry (ePrint Archive, 2012/076)
[YZ21] Yamanaka, Zhandry (EUROCRYPTO2021)

EUF-NMA ⇒ EUF-CMA

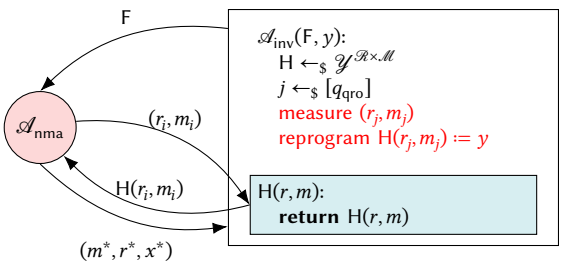


Signature Simulation by Reprogramming

- Tight adaptive reprogramming technique [GHHM21] enables reprogramming of H′.
- Distinguishing advantage ϵ_{ps} of the following should be negligible.
  1. $x \leftarrow \mathsf{I}(y)$ for $y \leftarrow_\$ \mathscr{Y}$ after retries on y.
  2. $x \leftarrow \mathsf{SampDom}(\mathsf{F})$.
- PSF is not necessary.
  → Probabilistic hash-and-sign with retry

[GHHM21] Grilo, Hövelmanns, Hülsing, Majenz (ASIACRYPT2021)

INV ⇒ EUF-NMA



Inversion by Measure and Reprogram

- Measure-and-reprogram technique [DFM20] enables reprogramming $\mathsf{H}(r_j, m_j) := y$ for measured (r_j, m_j).
- $\mathcal{A}_{\text{inv}}$ obtains a preimage of y with $(2q_{\text{qro}} + 1)^2\epsilon_{\text{nma}}$.

[DFM20] Don, Fehr, Majenz (CRYPTO2020)

Applications

Applications of New Security Proof

All Green 🤗

Scheme	Paradigm	Assumption	Primitive	Reduction (ROM)	Reduction (QROM)
Falcon	deterministic	collision-resistance	lattice	tight [GPV08]	tight [BDH+13]
ModFalcon					
Mitaka					
Wave	probabilistic	non-invertibility	code	poly loss [CD20]	poly loss
UOV	probabilistic with retry	non-invertibility	MQ	poly loss [SSH11]	poly loss
Rainbow					poly loss
QR-UOV					poly loss
GeMSS					poly loss
Mayo				poly loss [Beu21]	poly loss
CFS			code	poly loss [Dal07]	poly loss

Same assumptions both in ROM and QROM.

Summary

New Security Proof for Hash-and-sign

Proved INV $\Rightarrow$ EUF-CMA for probabilistic hash-and-sign with retry.

Applications to MQ-based and Code-based Schemes

Proved INV $\Rightarrow$ EUF-CMA for existing MQ-based/code-based signatures.

Extension to Multi-key Security

Proved M-INV $\Rightarrow$ M-EUF-CMA (M stands for Multi).