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

Haruhisa Kosuge[1] and Keita Xagawa[2]

[1] Japan Ministry of Defense, harucrypto@gmail.com
[2] NTT Social Informatics Laboratories, keita.xagawa@ntt.com

Abstract. A hash-and-sign signature based on a preimage-sampleable function (PSF) (Gentry et al. [STOC 2008]) is secure in the Quantum Random Oracle Model (QROM) if the PSF is collision-resistant (Boneh et al. [ASIACRYPT 2011]) or one-way (Zhandry [CRYPTO 2012]). However, trapdoor functions (TDFs) in code-based and multivariate-quadratic-based (MQ-based) signatures are not PSFs; for example, underlying TDFs of the Courtois-Finiasz-Sendrier (CFS), Unbalanced Oil and Vinegar (UOV), and Hidden Field Equations (HFE) signatures are not surjections. Thus, such signature schemes adopt *probabilistic hash-and-sign with retry*. This paradigm is secure in the (classical) Random Oracle Model (ROM), assuming that the underlying TDF is non-invertible; that is, it is hard to find a preimage of a given random value in the range (e.g., Sakumoto et al. [PQCRYPTO 2011] for the modified UOV/HFE signatures). Unfortunately, there is no known security proof for the probabilistic hash-and-sign with retry *in the QROM*.

We give the first security proof for the probabilistic hash-and-sign with retry in the QROM, assuming that the underlying *non-PSF* TDF is non-invertible. Our reduction from the non-invertibility is tighter than the existing ones that apply only to signature schemes based on PSFs. We apply the security proof to code-based and MQ-based signatures. Moreover, we extend the proof into the multi-key setting by using prefix hashing (Duman et al. [ACM CCS 2021]).

keywords: Post-quantum cryptography, digital signature, hash-and-sign, quantum random oracle model (QROM), preimage sampleable function.

1 Introduction

Hash-and-Sign Signature in the Random Oracle Model (ROM): A digital signature is an essential and versatile primitive in cryptography since it supports non-repudiation and authentication; if a document is signed, the signer indeed signed it and cannot repudiate the signature. The existential unforgeability against chosen-message attack, the EUF-CMA security, is the standard security notion of the digital signature [23]. Roughly speaking, a signature scheme is said to be EUF-CMA-secure if no efficient adversary can forge a signature even if it can use a signing oracle, which captures non-repudiation and authentication. The hash-and-sign paradigm [2, 3] is one of the most widely adopted paradigms to construct practical signatures along with the Fiat-Shamir paradigm [20] in the ROM [2]. This paper focuses on the hash-and-sign paradigm.

A hash-and-sign signature scheme is realized by a hard-to-invert function $\mathsf{F}\colon \mathcal{X} \to \mathcal{Y}$, its trapdoor $\mathsf{I}\colon \mathcal{Y} \to \mathcal{X}$, and a hash function $\mathsf{H}\colon \{0,1\}^* \to \mathcal{Y}$ modeled as a random oracle. To sign on a message m, a signer first computes $y = \mathsf{H}(r, m)$, where r is a random string, computes $x = \mathsf{I}(y)$, and outputs $\sigma = (r, x)$ as a signature. A verifier verifies the signature σ with the verification key F by checking if $\mathsf{H}(r, m) = \mathsf{F}(x)$ or not. We refer to this construction as *probabilistic hash-and-sign*; if r is an empty string, then *deterministic hash-and-sign*.

A prime example is TDP-FDH, a full-domain hash (FDH) using a trapdoor permutation (TDP) such as RSA. TDP-FDH is EUF-CMA-secure in the ROM, assuming the one-wayness (OW) or non-invertibility (INV) of TDP [2]. [3] Since TDPs are generally hard to build, Gentry, Peikert, and Vaikuntanathan proposed a (probabilistic) FDH signature with a preimage-sampleable function (PSF) [22], which is a trapdoor function (TDF) with additional conditions, e.g., surjection. Gentry et al. showed a tight reduction from the collision-resistance (CR) property of PSF to the *strong* EUF-CMA (sEUF-CMA) security of PSF-FDH (and PSF-PFDH), and they constructed a collision-resistant PSF from lattices.

Unfortunately, it is even hard to build PSFs in code-based and multivariate-quadratic-based (MQ-based) cryptography; for example, F is not surjection. In this case, the trapdoor I would output $\perp$ on input y whose preimage does not exist. For such TDFs, we use probabilistic hash-and-sign *with retry*, where a signer takes randomness r until r allows inversion of $y = \mathsf{H}(r, m)$. The Courtois-Finiasz-Sendrier (CFS) signature [13] in code-based cryptography and the Unbalanced Oil and Vinegar (UOV) [29] and Hidden Field Equations (HFE) signatures [38] in MQ-based cryptography use this paradigm. Dallot [14] and Morozov, Roy, Steinwandt, and Xu [34] showed the security of the modified CFS signature in the ROM. Sakumoto, Shirai, and Hiwatari [43] also showed the security of the modified HFE and UOV signatures in the ROM.

Hash-and-Sign Signature in the Quantum Random Oracle Model (QROM): Large-scale quantum computers will be able to break widely deployed public-key cryptography such as RSA and ECDSA because of Shor's algorithm [46], and interest has been growing in post-quantum cryptography (PQC). NIST has initiated a PQC standardization project for public-key encryption/key-encapsulation mechanism (KEM) and digital signature. Many post-quantum hash-and-sign signature schemes have been proposed in lattice-based, code-based, and MQ-based cryptography [15, 16, 10, 7, 21, 41]. Post-quantum signatures should be EUF-CMA-secure in *the quantum random oracle model (QROM)* [9] since the QROM models real-world quantum adversaries with *offline* access to the hash function. In the QROM, the adversary can query the random oracle in a superposition of many different values, say a superposition of all inputs in a query.

[3] An adversary tries to find a preimage of a challenge y that is uniformly chosen in the INV game [25] and that derived by $\mathsf{F}(x)$ for x chosen from some distribution on $\mathcal{X}$ in the OW game [2].

Table 1: Summary of the security proofs for the hash-and-sign in the QROM. DHaS/PHaS/PHaSwR stand for deterministic hash-and-sign, probabilistic hash-and-sign, and probabilistic hash-and-sign with retry. ϵ denotes the adversary's advantage in the game of the underlying assumption and $\epsilon_{\mathsf{ow/inv}} \in \{\epsilon_{\mathsf{ow}}, \epsilon_{\mathsf{inv}}\}$. q denotes the number of queries to the signing oracle or the random oracle. Table 2 shows the complete table.

Name	DHaS	PHaS	PHaSwR	Assumption	Security Bound
[9]	✓	✓	–	CR	$O(\epsilon_{\mathsf{cr}})$
[50]	✓	✓	–	OW/INV	$O(q^2\epsilon_{\mathsf{ow/inv}}^{1/2})$
ext. of [49]	✓	✓	–	OW/INV	$O(q^4\epsilon_{\mathsf{ow/inv}})$
[11]	–	✓	–	EUF-NMA	$O(\epsilon_{\mathsf{nma}})$
Ours	-	✓	✓	INV	$O(q^2\epsilon_{\mathsf{inv}})$

Thus, we could not directly use the proof techniques for the ROM, such as lazy sampling in the QROM. Moreover, schemes that are secure in the ROM are not always secure in the QROM, and Yamakawa and Zhandry gave separation results, including a signature scheme [48]. The history-free reduction, which avoids adaptive reprogramming, has been generally adopted [9, 27, 42]. Recently, some breakthrough results have shown that adaptive reprogramming is feasible in some cases [47, 26, 17, 24].

Summarizing the previous studies, we find that there are *no* security proofs for signature schemes using the probabilistic hash-and-sign with retry in the QROM, which impacts the security evaluation of code-based and MQ-based signatures. Thus, it is natural to ask the following question:

Q1. Is there an EUF-CMA *security proof for the probabilistic hash-and-sign with retry? How tight is the security proof?*

Table 1 summarizes studies on the EUF-CMA security of the hash-and-sign in the QROM. Boneh et al. [9] showed a tight reduction from the CR of PSF using the history-free reduction. Zhandry [50] gave a reduction from the OW/INV [4], using a technique called semi-constant distribution. [5] Unfortunately, the semi-constant distribution incurs a square-root loss in the success probability. Yamakawa and Zhandry [49] gave the lifting theorem that shows that any search-type game is hard in the QROM if the game is hard in the ROM. They used the lifting theorem to show that an EUF-NMA-secure signature in the ROM is EUF-NMA-secure in the QROM, where NMA stands for No-Message Attack. By extending the results of [49], we obtain a reduction from the OW/INV of PSF. Chailloux and Debris-Alazard [11] gave a security proof of the probabilistic hash-and-sign based on non-PSF TDFs. However, their reduction does not apply

[4] If a TDF is PSF, a tight reduction from OW to INV holds.

[5] Zhandry [50] proved the EUF-CMA security of TDP-FDH in the QROM, assuming that the underlying TDP is one-way. The security proof applies to the case for the OW/INV of PSF.

to the probabilistic hash-and-sign with retry. Also, Grilo, Hövelmanns, Hülsing, and Majenz [24] gave a reduction from the EUF-RMA security of a signature scheme for fixed-length messages, where RMA stands for Random-Message Attack. [6] However, there is no known reduction to the EUF-RMA security of the underlying signature from the OW/INV of TDF.

Provable Security in the Multi-key Setting: The EUF-CMA security is sometimes insufficient to ensure the security of the digital signature in the real world since exploiting one of many users may be sufficient for a real-world adversary to intrude into a system. We must consider the EUF-CMA security *in the multi-key setting*, the M-EUF-CMA security in short. The adversary, given multiple verification keys, tries to forge a valid signature for one of the verification keys. If the adversary can gain an advantage by targeting multiple keys (*multi-key attack*), the M-EUF-CMA security degrades with the number of keys or users. NIST mentioned resistance to multi-key attacks as a "desirable property" in their call for proposals [36] in their PQC standardization project.

The inclusion of an entire verification key in the hash computation enables one to separate the domain of the hash function for each verification key. This technique is called *key prefixing*, and Schnorr signature adopts it for showing a tight reduction in the multi-key setting [33]. Similarly, Duman et al. [19] proposed a technique called *prefix hashing* for the Fujisaki-Okamoto transform of KEM. In prefix hashing, the hash function includes only a small unpredictable part of a public key. This modification causes less increase in the execution time than in the case of including the entire key. Since this technique only changes the method of hashing, the hash-and-sign can adopt it. Thus, one might also ask the following question:

Q2. Is there an M-EUF-CMA *security proof for the hash-and-sign as tight as the* EUF-CMA *security proof?*

1.1 Contributions

Security Proof of Probabilistic Hash-and-Sign with Retry in the QROM: We affirmatively answer Q1 by giving the *first* reduction from the INV of the underlying TDF to the EUF-CMA security of the probabilistic hash-and-sign with retry in the QROM (*main theorem*). Also, we show that a signature scheme is sEUF-CMA-secure if the underlying TDF is an injection.

Our reduction is tighter than the existing ones from the INV that apply to probabilistic hash-and-sign without retry only [50, 11, 49]. Fig. 1 shows a diagram of the existing and our reductions. The main theorem comprises two reductions; INV $\Rightarrow$ EUF-NMA and EUF-NMA $\Rightarrow$ EUF-CMA, where X $\Rightarrow$ Y inidicates a reduction from X to Y. Our reduction of INV $\Rightarrow$ EUF-NMA is tighter than the one using the lifting theorem [49], and our reduction of EUF-NMA $\Rightarrow$

[6] A signer chooses r, computes $m' = \mathsf{H}(r, m)$, and signs on m' by using a signing algorithm of the signature scheme for fixed-length messages, and outputs (r, σ).

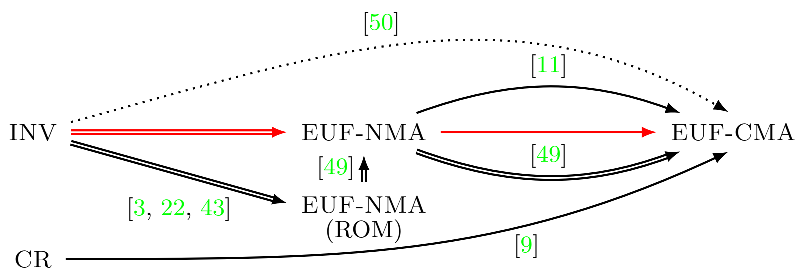

Fig. 1: A diagram for reductions of the hash-and-sign in the QROM. Red arrows indicate our reductions. Solid, double, and dashed arrows indicate tight reductions, reductions with linear or quadratic loss, and non-tight reductions.

EUF-CMA is tight. In the main theorem, a bound on the EUF-CMA advantage is $(2q_{\mathsf{qro}}+1)^2\epsilon_{\mathsf{inv}}$, where q_{qro} is a bound on the number of random oracle queries and ϵ_{inv} is the INV advantage of the underlying TDF.

Applications: We apply the main theorem to the existing code-based and MQ-based hash-and-sign signatures. We improve the EUF-CMA security of Wave [15] and give the first proof for the sEUF-CMA security of the modified CFS signature [14] and the EUF-CMA security of some MQ-based signatures, including Rainbow [16], GeMSS [10], MAYO [7], and QR-UOV [21] in the QROM. To the best of our knowledge, the main theorem covers all post-quantum hash-and-sign signature schemes with provable securities in the ROM.

NIST has announced a new call for proposals of the post-quantum signature with short signatures and fast verification [37]. NIST has the intention of standardizing schemes that are not based on structured lattices. Since the main theorem has wide application in code-based and MQ-based cryptography, promising candidates for this call, our work can and very likely will be used to ensure the security of new candidates.

Multi-Key Extension: We affirmatively answer Q2 by showing a reduction from the multi-instance INV (M-INV) of TDF to the M-EUF-CMA security of the hash-and-sign with prefix hashing by extending the main theorem. The M-EUF-CMA advantage has a bound $(2q_{\mathsf{qro}}+1)^2\epsilon_{\mathsf{inv^m}}$, where $\epsilon_{\mathsf{inv^m}}$ is the M-INV advantage. Also, we show a tight reduction from the multi-instance CR (M-CR). Note that the above reductions incur security losses in the number of keys without prefix hashing. The reduction from the M-INV or M-CR does not assure resistance to multi-key attacks in general. However, if there is a reduction from the INV or CR without the security loss in the number of keys, we can ensure resistance to multi-key attacks. This paper proposes a generic method for such *single-key to multi-key reduction*.

Organization: Section 2 gives notations, definitions, and so on. Section 3 reviews the existing security proofs in the (Q)ROM. Section 4 introduces our main theorem. Section 5 applies the main theorem to code-based and MQ-based signatures. Section 6 shows the multi-key extension of the main theorem. Section 7 explains the generic method for single-key to multi-key reduction. In appendix, Appendix A reviews the TDFs of signature schemes. Appendix B shows missing proofs. Appendix C applies the generic method for single-key to multi-key reduction to lattice-based, code-based, and MQ-based signatures.

Concurrent Work: There are two concurrent and independent works for the probable security of the hash-and-sign. Liu, Jiang, and Zhao [31] show the EUF-CMA security of the TDP-FDH and TDP-PFDH in the QROM by using the measure-and-reprogram technique by Don et al. [17]. Their bound on the EUF-CMA advantage is $(2(q_{\mathsf{qro}}+q_{\mathsf{sign}}+1)+1)^2\epsilon_{\mathsf{inv}}$, where q_{sign} is a bound on the number of signing queries. They also give an analysis for (H)IBE in the QROM. Our work has two advantages over their work on the provable security of the hash-and-sign. First, our main theorem applies to the TDP-PFDH and has wider applications in existing signature schemes. Note that no known post-quantum signatures adopting TDP-FDH/TDP-PFDH have been proposed. Second, our main theorem has the bound $(2q_{\mathsf{qro}}+1)^2\epsilon_{\mathsf{inv}}$ that is not including q_{sign}.

Chatterjee, Das, and Pandit [12] show the EUF-CMA security of the modified UOV signature [43] in the QROM. Since their security proof requires a superpolynomial-size finite field, it cannot guarantee the security of UOV-based schemes with practical parameter sets (polynomial-size finite fields).

2 Preliminaries

2.1 Notations and Terminology

For $n \in \mathbb{N}$, we let $[n] \coloneqq \{1, \ldots, n\}$. We write any symbol for sets in calligraphic font. For a finite set $\mathcal{X}$, $|\mathcal{X}|$ is the cardinality of $\mathcal{X}$ and $\mathsf{U}(\mathcal{X})$ is the uniform distribution over $\mathcal{X}$. By $x \leftarrow_\$ \mathcal{X}$ and $x \leftarrow \mathcal{D}_\mathcal{X}$, we denote the sampling of an element from $\mathsf{U}(\mathcal{X})$ and $\mathcal{D}_\mathcal{X}$ (distribution on $\mathcal{X}$). For a domain $\mathcal{X}$ and a range $\mathcal{Y}$, by $\mathcal{Y}^\mathcal{X}$ we denote a set of functions $\mathsf{F}\colon \mathcal{X} \to \mathcal{Y}$.

We write any symbol for functions in sans-serif font and adversaries in calligraphic font. Let F be a function and $\mathcal{A}$ be an adversary. We denote by $y \leftarrow \mathsf{F}^{\mathsf{H}}(x)$ and $y \leftarrow \mathcal{A}^{\mathsf{H}}(x)$ (resp., $y \leftarrow \mathsf{F}^{|\mathsf{H}\rangle}(x)$ and $y \leftarrow \mathcal{A}^{|\mathsf{H}\rangle}(x)$) probabilistic computations of F and $\mathcal{A}$ on input x with a classical (resp., quantum) oracle access to a function H. If F and $\mathcal{A}$ are deterministic, we write $y \coloneqq \mathsf{F}^{\mathsf{H}}(x)$ and $y \coloneqq \mathcal{A}^{\mathsf{H}}(x)$. For a random function H, we denote by $\mathsf{H}^{x^*\mapsto y^*}$ a function such that $\mathsf{H}^{x^*\mapsto y^*}(x) = \mathsf{H}(x)$ for $x \neq x^*$ and $\mathsf{H}^{x^*\mapsto y^*}(x^*) = y^*$. The notation $\mathsf{G}^\mathcal{A} \Rightarrow y$ denotes an event in which a game G played by $\mathcal{A}$ returns y.

We denote 1 if the Boolean statement is true $\top$ and 0 if the statement is false $\bot$. A binary operation $a \stackrel{?}{=} b$ outputs $\top$ if $a = b$ and outputs $\bot$ otherwise.

2.2 Digital Signature

A digital signature scheme Sig consists of three algorithms:

GAME: EUF-CMA	$\mathsf{Sign}(m_i)$	GAME: EUF-NMA
1 $\mathcal{Q} := \emptyset$ 2 $(vk, sk) \leftarrow \mathsf{Sig.KeyGen}(1^\lambda)$ 3 $(m^*, \sigma^*) \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign}}(vk)$ 4 **if** $m^* \in \mathcal{Q}$ **then** 5 **return** 0 6 **return** $\mathsf{Sig.Verify}(vk, m^*, \sigma^*)$	1 $\sigma_i \leftarrow \mathsf{Sig.Sign}(sk, m_i)$ 2 $\mathcal{Q} := \mathcal{Q} \cup \{m_i\}$ 3 **return** σ_i	1 $(vk, sk) \leftarrow \mathsf{Sig.KeyGen}(1^\lambda)$ 2 $(m^*, \sigma^*) \leftarrow \mathcal{A}_{\mathsf{nma}}(vk)$ 3 **return** $\mathsf{Sig.Verify}(vk, m^*, \sigma^*)$

Fig. 2: EUF-CMA and EUF-NMA games

$\mathsf{Sig.KeyGen}(1^\lambda)$: This algorithm takes the security parameter 1^λ as input and outputs a verification key vk and a signing key sk.

$\mathsf{Sig.Sign}(sk, m)$: This algorithm takes a signing key sk and a message m as input and outputs a signature σ.

$\mathsf{Sig.Vrfy}(vk, m, \sigma)$: This algorithm takes a verification key vk, a message m, and a signature σ as input, and outputs $\top$ (acceptance) or $\bot$ (rejection).

Definition 2.1 (Security of Signature). *Let* Sig *be a signature scheme. Using games given in Fig. 2, we define advantage functions of adversaries playing* EUF-CMA *(Existential UnForgeability against Chosen-Message Attack) and* EUF-NMA *(No-Message Attack) games against* Sig *as* $\mathrm{Adv}_{\mathsf{Sig}}^{\text{EUF-CMA}}(\mathcal{A}_{\mathsf{cma}}) = \Pr\left[\mathsf{EUF\text{-}CMA}^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]$ *and* $\mathrm{Adv}_{\mathsf{Sig}}^{\text{EUF-NMA}}(\mathcal{A}_{\mathsf{nma}}) = \Pr\left[\mathsf{EUF\text{-}NMA}^{\mathcal{A}_{\mathsf{nma}}} \Rightarrow 1\right]$*, respectively. Also, we define an advantage function for an* sEUF-CMA *(strong* EUF-CMA*) game as* $\mathrm{Adv}_{\mathsf{Sig}}^{\text{sEUF-CMA}}(\mathcal{A}_{\mathsf{cma}}) = \Pr\left[\mathsf{sEUF\text{-}CMA}^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]$*, where the* sEUF-CMA *game is identical to the* EUF-CMA *game except that Line 4 is changed as "* **if** $(m^*, \sigma^*) \in \mathcal{Q}'$ **then** *" and* $\mathcal{Q}'$ *keeps messages and signatures in the signing oracle. We say* Sig *is* EUF-CMA*-secure,* sEUF-CMA*-secure, or* EUF-NMA*-secure if its corresponding advantage is negligible for any efficient adversary in the security parameter.*

2.3 Trapdoor Function

A trapdoor function (TDF) T consists of three algorithms:

$\mathsf{Gen}(1^\lambda)$: This algorithm takes the security parameter 1^λ as input and outputs a function F with a trapdoor I of F.

$\mathsf{F}(x)$: This algorithm takes $x \in \mathcal{X}$ and deterministically outputs $\mathsf{F}(x) \in \mathcal{Y}$.

$\mathsf{I}(y)$: This algorithm takes $y \in \mathcal{Y}$ and outputs $x \in \mathcal{X}$, s.t., $\mathsf{F}(x) = y$, or outputs $\bot$.

Definition 2.2 (Security of TDF). *Let* T *be a TDF. Using games given in Fig. 3, we define advantage functions of adversaries playing the* INV *(non-INVertibility)* [7]*,* OW *(One-Wayness), and* CR *(Collision-Resistance) games against* T *as* $\mathrm{Adv}_{\mathsf{T}}^{\text{INV}}(\mathcal{B}_{\mathsf{inv}}) = \Pr\left[\mathsf{INV}^{\mathcal{B}_{\mathsf{inv}}} \Rightarrow 1\right]$, $\mathrm{Adv}_{\mathsf{T}}^{\text{OW}}(\mathcal{B}_{\mathsf{ow}}) = \Pr\left[\mathsf{OW}^{\mathcal{B}_{\mathsf{ow}}} \Rightarrow 1\right]$*, and* $\mathrm{Adv}_{\mathsf{T}}^{\text{CR}}(\mathcal{B}_{\mathsf{cr}}) = \Pr\left[\mathsf{CR}^{\mathcal{B}_{\mathsf{cr}}} \Rightarrow 1\right]$*, respectively.*

[7] In general, *non-invertibility* of TDFs is called *one-wayness* [22, 43, 11]. We make a distinction between them depending on the way to choose challenges (INV follows [25] and OW follows [2]).

$\underline{\textsc{Game}: \mathsf{INV}}$	$\underline{\textsc{Game}: \mathsf{OW}}$	$\underline{\textsc{Game}: \mathsf{CR}}$
$(\mathsf{F},\mathsf{I}) \leftarrow \mathsf{Gen}(1^\lambda)$	$(\mathsf{F},\mathsf{I}) \leftarrow \mathsf{Gen}(1^\lambda)$	$(\mathsf{F},\mathsf{I}) \leftarrow \mathsf{Gen}(1^\lambda)$
$y \leftarrow_\$ \mathcal{Y}$	$x \leftarrow \mathcal{D}_\mathcal{X}$	$(x_1^*, x_2^*) \leftarrow \mathcal{B}_{\mathsf{cr}}(\mathsf{F})$
$x^* \leftarrow \mathcal{B}_{\mathsf{inv}}(\mathsf{F}, y)$	$y := \mathsf{F}(x)$	**return** $\mathsf{F}(x_1^*) \stackrel{?}{=} \mathsf{F}(x_2^*)$
return $\mathsf{F}(x^*) \stackrel{?}{=} y$	$x^* \leftarrow \mathcal{B}_{\mathsf{ow}}(\mathsf{F}, y)$	
	return $\mathsf{F}(x^*) \stackrel{?}{=} y$	

Fig. 3: INV (non-INVertibility), OW (One-Wayness), and CR (Collision-Resistance) games

2.4 Preimage-Sampleable Function

In the ROM, the hash-and-sign is EUF-CMA-secure when instantiated with a preimage-sampleable function (PSF) [22]. We first define its weakened version.

Definition 2.3 (Weak Preimage-Sampleable Function (WPSF)). *A TDF* T *is said to be a WPSF if it consists of the following four algorithms:*

- $\mathsf{Gen}(1^\lambda)$*: This algorithm takes the security parameter* 1^λ *as input and outputs a function* F *with a trapdoor* I.
- $\mathsf{F}(x)$*: This algorithm takes* $x \in \mathcal{X}$ *and deterministically outputs* $\mathsf{F}(x) \in \mathcal{Y}$.
- $\mathsf{I}(y)$*: This algorithm takes* $y \in \mathcal{Y}$ *and outputs* $x \in \mathcal{X}$ *satisfying* $\mathsf{F}(x) = y$ *or outputs* $\perp$.
- $\mathsf{SampDom}(\mathsf{F})$*: This algorithm takes* $\mathsf{F} \in \mathcal{Y}^\mathcal{X}$ *and outputs* $x \in \mathcal{X}$.

We then review PSF [22]:

Definition 2.4 (Preimage-Sampleable Function (PSF) [22]). *A WPSF* T *is said to be a PSF if it satisfies three conditions for any* $(\mathsf{F},\mathsf{I}) \leftarrow \mathsf{Gen}(1^\lambda)$*:*

- ***Condition 1****:* $\mathsf{F}(x)$ *is uniform over* $\mathcal{Y}$ *for* $x \leftarrow \mathsf{SampDom}(\mathsf{F})$.
- ***Condition 2****:* $x \leftarrow \mathsf{I}(y)$ *follows a distribution of* $x \leftarrow \mathsf{SampDom}(\mathsf{F})$ *given* $\mathsf{F}(x) = y$.
- ***Condition 3****:* $\mathsf{I}(y)$ *outputs* x *satisfying* $\mathsf{F}(x) = y$ *for any* $y \in \mathcal{Y}$. [8]

If T *is collision-resistant PSF, it satisfies the above conditions plus the following:*

- ***Condition 4****: For any* $y \in \mathcal{Y}$*, the conditional min-entropy of* $x \leftarrow \mathsf{SampDom}(\mathsf{F})$ *given* $\mathsf{F}(x) = y$ *is at least* $\omega(\log n)$.

We define a condition for indistinguishability of $x \leftarrow \mathsf{SampDom}(\mathsf{F})$ and $x \leftarrow \mathsf{I}(y)$ in a different manner from **Condition 2**.

Definition 2.5 (PS (Preimage Sampling) Game). *Let* T *be a WPSF. Using a game defined in Fig. 4, we define an advantage function of an adversary playing the* PS *game against* T *as* $\mathrm{Adv}_\mathsf{T}^{\mathrm{PS}}(\mathcal{D}_{\mathsf{ps}}) = \left|\Pr\left[\mathsf{PS}_0^{\mathcal{D}_{\mathsf{ps}}} \Rightarrow 1\right] - \Pr\left[\mathsf{PS}_1^{\mathcal{D}_{\mathsf{ps}}} \Rightarrow 1\right]\right|$.

The condition that $\mathrm{Adv}_\mathsf{T}^{\mathrm{PS}}(\mathcal{D}_{\mathsf{ps}})$ is negligible is a relaxation of **Condition 2** in which we can use computational indistinguishability.

[8] The original definition of PSF [22] does not explicitly assume **Condition 3** but implicitly assumes it by **Condition 2**. **Condition 3** is necessary for a signature generation without retry.

```
Game: PS_b
(F, I) ← Gen(1^λ)
b* ← D_ps^{Sample_b}(F)
return b*

Sample_0()
repeat
    y_i ←$ 𝒴
    x_i ← I(y_i)
until x_i ≠ ⊥
return x_i

Sample_1()
x_i ← SampDom(F)
return x_i
```

Fig. 4: PS (Preimage Sampling) game

```
Game: M-EUF-CMA
1 𝒬 := ∅
2 for j ∈ [q_key] do
3     (vk_j, sk_j) ← Sig.KeyGen(1^λ)
4 (j*, m*, σ*) ← A_{cma^m}^{Sign}({vk_j}_{j∈[q_key]})
5 if (j*, m*) ∈ 𝒬 then
6     return 0
7 return Sig.Verify(vk_{j*}, m*, σ*)

Sign(j, m_i)
1 σ_i ← Sig.Sign(sk_j, m_i)
2 𝒬 := 𝒬 ∪ {(j, m_i)}
3 return σ_i
```

Fig. 5: M-EUF-CMA (Multi-key EUF-CMA) game

2.5 Security Games in the Multi-key/Multi-instance Settings

We define multi-key/multi-instance versions of the security notions.

Definition 2.6 (Security of Signature in the Multi-key Setting [28]). *Let* Sig *be a signature scheme. Using a game given in Fig. 5, we define advantage functions of adversaries playing the* M-EUF-CMA *and* M-sEUF-CMA *(Multi-key* EUF-CMA/sEUF-CMA*) games against* Sig *as* $\mathrm{Adv}_{\mathsf{Sig}}^{\text{M-EUF-CMA}}(\mathcal{A}_{\mathsf{cma^m}}) = \Pr\left[\text{M-EUF-CMA}^{\mathcal{A}_{\mathsf{cma^m}}} \Rightarrow 1\right]$ *and* $\mathrm{Adv}_{\mathsf{Sig}}^{\text{M-sEUF-CMA}}(\mathcal{A}_{\mathsf{cma^m}}) = \Pr\left[\text{M-sEUF-CMA}^{\mathcal{A}_{\mathsf{cma^m}}} \Rightarrow 1\right]$, *where the* M-sEUF-CMA *game is identical to the* M-EUF-CMA *game except that Line 5 is changed as "* **if** $(j^*, m^*, \sigma^*) \in \mathcal{Q}'$ **then***" and* $\mathcal{Q}'$ *keeps key IDs, messages, and signatures in the signing oracle. We say* Sig *is* M-EUF-CMA*-secure or* M-sEUF-CMA*-secure if its corresponding advantage is negligible for any efficient adversary in the security parameter.*

Definition 2.7 (INV, CR, and PS in Multi-instance Setting). *Let* T *be a TDF or a WPSF. Using games given in Fig. 6, we define advantage functions of adversaries playing the* M-INV *(Multi-instance* INV*),* M-CR *(Multi-instance* CR*), and* M-PS *(Multi-instance* PS*) against* T *as* $\mathrm{Adv}_{\mathsf{T}}^{\text{M-INV}}(\mathcal{B}_{\mathsf{inv^m}}) = \Pr\left[\text{M-INV}^{\mathcal{B}_{\mathsf{inv^m}}} \Rightarrow 1\right]$, $\mathrm{Adv}_{\mathsf{T}}^{\text{M-CR}}(\mathcal{B}_{\mathsf{cr^m}}) = \Pr\left[\text{M-CR}^{\mathcal{B}_{\mathsf{cr^m}}} \Rightarrow 1\right]$, *and* $\mathrm{Adv}_{\mathsf{T}}^{\text{M-PS}}(\mathcal{D}_{\mathsf{ps^m}}) = \left|\Pr\left[\text{M-PS}_0^{\mathcal{D}_{\mathsf{ps^m}}} \Rightarrow 1\right] - \Pr\left[\text{M-PS}_1^{\mathcal{D}_{\mathsf{ps^m}}} \Rightarrow 1\right]\right|$, *respectively.*

2.6 Quantum Random Oracle Model and Proof Techniques

In the ROM, a hash function $\mathsf{H}\colon \mathcal{R} \times \mathcal{M} \to \mathcal{Y}$ is modeled as a random function $\mathsf{H} \leftarrow_\$ \mathcal{Y}^{\mathcal{R}\times\mathcal{M}}$. The random function is under the control of the challenger, and

Game: M-INV

for $j \in [q_{\mathsf{inst}}]$ **do**
  $(\mathsf{F}_j, \mathsf{I}_j) \leftarrow_\$ \mathsf{Gen}(1^\lambda)$
  $y_j \leftarrow_\$ \mathcal{Y}$
$(j^*, x^*) \leftarrow \mathcal{B}_{\mathsf{inv^m}}(\{(\mathsf{F}_j, y_j)\}_{j\in[q_{\mathsf{inst}}]})$
return $\mathsf{F}_{j^*}(x^*) \stackrel{?}{=} y_{j^*}$

Game: M-CR

for $j \in [q_{\mathsf{inst}}]$ **do**
  $(\mathsf{F}_j, \mathsf{I}_j) \leftarrow_\$ \mathsf{Gen}(1^\lambda)$;
$(j^*, x_1^*, x_2^*) \leftarrow \mathcal{B}_{\mathsf{cr^m}}(\{\mathsf{F}_j\}_{j\in[q_{\mathsf{inst}}]})$
return $\mathsf{F}_{j^*}(x_1^*) \stackrel{?}{=} \mathsf{F}_{j^*}(x_2^*)$

Game: M-PS$_b$

for $j \in [q_{\mathsf{inst}}]$ **do**
  $(\mathsf{F}_j, \mathsf{I}_j) \leftarrow_\$ \mathsf{Gen}(1^\lambda)$
$b^* \leftarrow \mathcal{D}_{\mathsf{ps^m}}^{\mathsf{Sample}_b}(\{\mathsf{F}_j\}_{j\in[q_{\mathsf{inst}}]})$
return b^*

$\mathsf{Sample}_0(j)$

repeat
  $y_i, \leftarrow_\$ \mathcal{Y}$
  $x_i \leftarrow \mathsf{I}_j(y_i)$
until $x_i \neq \perp$
return x_i

$\mathsf{Sample}_1(j)$

$x_i \leftarrow \mathsf{SampDom}(\mathsf{F}_j)$
return x_i

Fig. 6: M-INV, M-CR, and M-PS (Multi-instance INV, CR, and PS) games

the adversary makes queries to the random oracle (*random oracle queries*) to compute the hash values. In the ROM, the challenger chooses $y \leftarrow_\$ \mathcal{Y}$ and programs H as $\mathsf{H}(r, m) := y$ for queried (r, m) on-the-fly instead of choosing $\mathsf{H} \leftarrow_\$ \mathcal{Y}^{\mathcal{R}\times\mathcal{M}}$ at the beginning (lazy sampling technique).

In the QROM, the adversary makes queries to H in a superposition of many different values, e.g., $\sum_{(r,m)} \alpha_{r,m} |r, m\rangle |y\rangle$. The challenger computes H and gives a superposition of the results to the adversary, $\sum_{(r,m)} \alpha_{r,m} |r, m\rangle |y \oplus \mathsf{H}(r, m)\rangle$. Some works enable one to adaptively reprogram H in the security game [47, 26, 17, 24]. Among the works, we will use the tight adaptive reprogramming technique [24] and the measure-and-reprogram technique [17]. Also, we use the semi-classical O2H (One-way to Hiding) technique [1].

Tight Adaptive Reprogramming Technique [24]: Fig. 7 shows a game called AR (Adaptive Reprogramming) game, in which the adversary $\mathcal{D}_{\mathsf{ar}}$ tries to distinguish H_0 (no reprogramming) from H_1 (reprogrammed by Repro). For i-th reprogramming query, the challenger reprograms H_1 for uniformly chosen (r_i, y_i), and gives r_i to $\mathcal{D}_{\mathsf{ar}}$. A distinguishing advantage of the AR game is defined by $\mathrm{Adv}_{\mathsf{H}}^{\mathrm{AR}}(\mathcal{D}_{\mathsf{ar}}) = \left|\Pr\left[\mathsf{AR}_0^{\mathcal{D}_{\mathsf{ar}}} \Rightarrow 1\right] - \Pr\left[\mathsf{AR}_1^{\mathcal{D}_{\mathsf{ar}}} \Rightarrow 1\right]\right|$.

Lemma 2.1 (Tight Adaptive Reprogramming Technique [24, Proposition 1]). *For any quantum* AR *adversary $\mathcal{D}_{\mathsf{ar}}$ issuing at most q_{rep} classical reprogramming queries and q_{qro} (quantum) random oracle queries to H_b, the distinguishing advantage of the* AR *game is bounded by*

$$\mathrm{Adv}_{\mathsf{H}}^{\mathrm{AR}}(\mathcal{D}_{\mathsf{ar}}) \leq \frac{3}{2} q_{\mathsf{rep}} \sqrt{\frac{q_{\mathsf{qro}}}{|\mathcal{R}|}}.$$

Measure-and-Reprogram Technique [17]: Fig. 8 shows a two-stage simulator S for $\mathcal{A}$ playing any search-type game in the QROM. In the first stage, S_1 uniformly chooses one of the $\mathcal{A}$'s queries to a random function H and outputs the observed value (r', m') of the chosen query. Then, H is reprogrammed as $\mathsf{H}' := \mathsf{H}^{(r',m')\mapsto\theta}$

Game: AR_b	$\mathsf{Repro}(m_i)$
1 $\mathsf{H}_0 \leftarrow_\$ \mathcal{Y}^{\mathcal{R}\times\mathcal{M}}$	1 $(r_i, y_i) \leftarrow_\$ \mathcal{R} \times \mathcal{Y}$
2 $\mathsf{H}_1 := \mathsf{H}_0$	2 $\mathsf{H}_1 := \mathsf{H}_1^{(r_i,m_i)\mapsto y_i}$
3 $b^* \leftarrow \mathcal{D}_{\mathsf{ar}}^{\lvert\mathsf{H}_b\rangle,\mathsf{Repro}}()$	3 **return** r_i
4 **return** b^*	

Fig. 7: AR (Adaptive Reprogramming) game

Adversary: $\mathcal{A}^{\lvert\mathsf{H}\rangle}()$	Simulator: $\mathsf{S}(\theta)$ for $\mathcal{A}^{\lvert\mathsf{H}\rangle}()$
1 $(r, m, z) \leftarrow \mathcal{A}^{\lvert\mathsf{H}\rangle}()$	1 $\mathsf{H} \leftarrow_\$ \mathcal{Y}^{\mathcal{R}\times\mathcal{M}}$
2 **return** (r, m, z)	2 $(r', m') \leftarrow \mathsf{S}_1^{\mathcal{A}^{\lvert\mathsf{H}\rangle}}()$
	3 $\mathsf{H}' := \mathsf{H}^{(r',m')\mapsto\theta}$
	4 $z \leftarrow \mathsf{S}_2^{\mathcal{A}^{\lvert\mathsf{H}'\rangle}}(\theta)$
	5 **return** (r', m', z)

Fig. 8: A simulator S for any search-type game adversary $\mathcal{A}$

for a random θ. In the second stage, S_2 runs $\mathcal{A}$ using H'. Finally, S_2 outputs whatever $\mathcal{A}$ outputs, which is denoted by z and maybe quantum.

Lemma 2.2 (Measure-and-Reprogram Technique [17, Theorem 2]). *For any quantum adversary $\mathcal{A}$ issuing at most q_{qro} (quantum) random oracle queries to $\mathsf{H} \leftarrow_\$ \mathcal{Y}^{\mathcal{R}\times\mathcal{M}}$, there exists a two-stage quantum simulator S given uniformly chosen θ such that for any $(\hat{r}, \hat{m}) \in \mathcal{R} \times \mathcal{M}$ and any predicate V,*

$$\begin{aligned}&\Pr\left[(r', m') = (\hat{r}, \hat{m}) \wedge \mathsf{V}(r', m', \theta, z) : (r', m') \leftarrow \mathsf{S}_1^{\mathcal{A}^{\lvert\mathsf{H}\rangle}}(),\ z \leftarrow \mathsf{S}_2^{\mathcal{A}^{\lvert\mathsf{H}'\rangle}}(\theta)\right] \\ &\geq \frac{1}{(2q_{\mathsf{qro}}+1)^2} \Pr\left[(r, m) = (\hat{r}, \hat{m}) \wedge \mathsf{V}(r, m, \mathsf{H}(r, m), z) : (r, m, z) \leftarrow \mathcal{A}^{\lvert\mathsf{H}\rangle}()\right].\end{aligned}$$

Semi-classical O2H Technique [1]: We define *punctured oracle* following a notation of [5].

Definition 2.8 (Punctured Oracle [5, Definition 1]). *For a set $\mathcal{S} \subset \mathcal{R}\times\mathcal{M}$ and its predicate $\mathsf{f}_\mathcal{S}$,* punctured oracle *$\mathsf{H}\backslash\mathcal{S}$ (H punctured by $\mathcal{S}$) of $\mathsf{H} \in \mathcal{Y}^{\mathcal{R}\times\mathcal{M}}$ runs as follows: on input (r, m), computes whether $(r, m) \in \mathcal{S}$ in an auxilliary qubit $\lvert\mathsf{f}_\mathcal{S}(r, m)\rangle$, measures $\lvert\mathsf{f}_\mathcal{S}(r, m)\rangle$, runs $\mathsf{H}(r, m)$, and returns the result. Let* FIND *be an event that any of measurements of $\lvert\mathsf{f}_\mathcal{S}(r, m)\rangle$ returns 1.*

Querying $\sum_{(r,m)} \alpha_{r,m} \lvert r, m\rangle \lvert y\rangle$ to H, we obtain $\sum_{(r,m)} \alpha_{r,m} \lvert r, m\rangle \lvert y \oplus \mathsf{H}(r, m)\rangle$. However, if we query $\mathsf{H}\backslash\mathcal{S}$, the answer depends on the results of the measurement. Let us consider the same query $\sum_{(r,m)} \alpha_{r,m} \lvert r, m\rangle \lvert y\rangle$ to $\mathsf{H}\backslash\mathcal{S}$. The oracle computes $\sum_{(r,m)} \alpha_{r,m} \lvert r, m\rangle \lvert y\rangle \lvert\mathsf{f}_\mathcal{S}(r, m)\rangle$ and measures the third register. If the result is 0, then the query becomes $\sum_{(r,m):(r,m)\notin\mathcal{S}} \alpha_{r,m} \lvert r, m\rangle \lvert y\rangle \lvert 0\rangle$ and we obtain $\sum_{(r,m):(r,m)\notin\mathcal{S}} \alpha_{r,m} \lvert r, m\rangle \lvert y \oplus \mathsf{H}(r, m)\rangle$, where we ignore scaling of the amplitudes $\alpha_{r,m}$. Otherwise, that is, if the results is 1 (and thus, FIND $= \top$), then the query becomes $\sum_{(r,m):(r,m)\in\mathcal{S}} \alpha_{r,m} |r,m\rangle |y\rangle |1\rangle$ and we obtain $\sum_{(r,m):(r,m)\in\mathcal{S}} \alpha_{r,m} |r,m\rangle |y \oplus \mathsf{H}(r,m)\rangle$. Thus, if FIND $= \perp$, then we cannot obtain any information on $\mathsf{H}(r,m)$ for $(r,m) \in \mathcal{S}$. Hence, we have the following:

Lemma 2.3 (Indistinguishability of Punctured Oracles [1, Lemma 1]). *Let $\mathsf{H}_0, \mathsf{H}_1 \colon \mathcal{X} \to \mathcal{Y}$ and $\mathcal{S} \subset \mathcal{R} \times \mathcal{M}$, and z be a bitstring. ($\mathcal{S}$, H_0, H_1, and z are taken from arbitrary joint distribution satisfying $\mathsf{H}_0(x) = \mathsf{H}_1(x)$ for any $(r,m) \notin \mathcal{S}$.) For any quantum adversary $\mathcal{A}$ and any event* E*,*

$$\Pr\left[\mathrm{E} \wedge \mathrm{FIND} = \perp \colon b \leftarrow \mathcal{A}^{|\mathsf{H}_0 \setminus \mathcal{S}\rangle}(z)\right] = \Pr\left[\mathrm{E} \wedge \mathrm{FIND} = \perp \colon b \leftarrow \mathcal{A}^{|\mathsf{H}_1 \setminus \mathcal{S}\rangle}(z)\right].$$

The following lemma shows that a probability that FIND $= \top$ occurs can bound the advantage gap between an original game and a game with the punctured oracle. Note that we omit unnecessary statements for the main theorem from [1, Theorem 1] and do not consider the parallelization of queries.

Lemma 2.4 (Semi-classical O2H Technique [1, Theorem 1]). *Let $\mathsf{H} \colon \mathcal{X} \to \mathcal{Y}$ and $\mathcal{S} \subset \mathcal{R} \times \mathcal{M}$, and z be a bitstring. ($\mathcal{S}$, H, and z are taken from arbitrary joint distribution.) For any quantum adversary $\mathcal{A}$ issuing at most q_{qro} (quantum) random oracle queries to H,*

$$\left|\Pr\left[1 \leftarrow \mathcal{A}^{|\mathsf{H}\rangle}(z)\right] - \Pr\left[1 \leftarrow \mathcal{A}^{|\mathsf{H} \setminus \mathcal{S}\rangle}(z) \wedge \mathrm{FIND} = \perp\right]\right| \\ \leq \sqrt{(q_{\mathsf{qro}} + 1) \Pr\left[\mathrm{FIND} = \top \colon b \leftarrow \mathcal{A}^{|\mathsf{H} \setminus \mathcal{S}\rangle}(z)\right]}.$$

Also, we can take a bound on $\Pr\left[\mathrm{FIND} = \top \colon b \leftarrow \mathcal{A}^{|\mathsf{H} \setminus \mathcal{S}\rangle}(z)\right]$.

Lemma 2.5 (Search in Semi-classical Oracle [1, Theorem 2 and Corollary 1]). *Let $\mathcal{B}^{|\mathsf{H}\rangle}(z)$ be an algorithm that runs as follows: Picks $i \leftarrow_{\$} [q_{\mathsf{qro}}]$, runs $\mathcal{A}^{|\mathsf{H}\rangle}(z)$ until just before i-th query, measures a query input register in the computational basis, and outputs the measurement outcome as (r', m'). Then,*

$$\Pr\left[\mathrm{FIND} = \top \colon b \leftarrow \mathcal{A}^{|\mathsf{H} \setminus \mathcal{S}\rangle}(z)\right] \leq 4 q_{\mathsf{qro}} \Pr\left[(r', m') \in \mathcal{S} \colon (r', m') \leftarrow \mathcal{B}^{|\mathsf{H}\rangle}(z)\right].$$

In particular, if for each $(r', m') \in \mathcal{S}$, $\Pr[(r', m') \in \mathcal{S}] \leq \epsilon$ (conditioned on z, on other oracles $\mathcal{A}$ has access to, and on other outputs of H), then

$$\Pr\left[\mathrm{FIND} = \top \colon b \leftarrow \mathcal{A}^{|\mathsf{H} \setminus \mathcal{S}\rangle}(z)\right] \leq 4 q_{\mathsf{qro}} \epsilon.$$

3 Hash-and-Sign Paradigm and Existing Security Proofs

3.1 Hash-and-Sign Paradigm

Fig. 9 shows algorithms of the probabilistic hash-and-sign with retry, and $\mathsf{HaS}[\mathsf{T}, \mathsf{H}]$ denotes a signature scheme using a TDF T and a hash function H. If $\mathsf{HaS}[\mathsf{T}, \mathsf{H}].\mathsf{Sign}$ outputs a signature without retry, $\mathsf{HaS}[\mathsf{T}, \mathsf{H}]$ instantiates the probabilistic hash-and-sign. If r is an empty string, $\mathsf{HaS}[\mathsf{T}, \mathsf{H}]$ instantiates the deterministic hash-and-sign.

$\underline{\mathsf{HaS}[\mathsf{T},\mathsf{H}].\mathsf{KeyGen}(1^\lambda)}$	$\underline{\mathsf{HaS}[\mathsf{T},\mathsf{H}].\mathsf{Sign}(\mathsf{I},m)}$	$\underline{\mathsf{HaS}[\mathsf{T},\mathsf{H}].\mathsf{Vrfy}(\mathsf{F},m,(r,x))}$

$(\mathsf{F},\mathsf{I}) \leftarrow \mathsf{Gen}(1^\lambda)$
return (F,I)
	repeat
	  $r \leftarrow_\$ \mathcal{R}$
	  $x \leftarrow \mathsf{I}(\mathsf{H}(r,m))$
	until $x \neq \bot$
	return (r,x)
		return $\mathsf{F}(x) \stackrel{?}{=} \mathsf{H}(r,m)$

Fig. 9: Algorithms of the probabilistic hash-and-sign with retry

3.2 Existing Security Proofs

We review existing security proofs. Table 2 summarizes the existing security proofs (and ours).

Security Proof in the ROM [3, 22]: Let $\mathsf{T}_{\mathsf{psf}}$ be a PSF. A reduction from the INV of $\mathsf{T}_{\mathsf{psf}}$ to the EUF-CMA security of $\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}},\mathsf{H}]$ in the ROM is given by lazy sampling and programming. The INV adversary $\mathcal{B}_{\mathsf{inv}}$, given a challenge (F,y), simulates the EUF-CMA game played by an adversary $\mathcal{A}_{\mathsf{cma}}$ as follows: For a random oracle query (r,m), $\mathcal{B}_{\mathsf{inv}}$ returns $\mathsf{F}(x)$ for $x \leftarrow \mathsf{SampDom}(\mathsf{F})$ and stores (r,m,x) in a database $\mathcal{D}$. If $(r,m,x) \in \mathcal{D}$ with some x, then $\mathcal{B}_{\mathsf{inv}}$ gives $\mathsf{F}(x)$ to $\mathcal{A}_{\mathsf{cma}}$. For a signing query m, $\mathcal{B}_{\mathsf{inv}}$ chooses (r,x) by $r \leftarrow_\$ \mathcal{R}$ and $x \leftarrow \mathsf{SampDom}(\mathsf{F})$. If $(r,m,*) \notin \mathcal{D}$, $\mathcal{B}_{\mathsf{inv}}$ returns (r,x) and stores (r,m,x) in $\mathcal{D}$; otherwise $\mathcal{B}_{\mathsf{inv}}$ returns stored (r,x).

From **Condition 1** of PSF ($\mathsf{F}(x)$ is uniform), $\mathcal{B}_{\mathsf{inv}}$ can use $\mathsf{F}(x)$ as an output of the random function. Also from **Conditions 2** and **3**, honestly generated signatures $x_i \leftarrow \mathsf{I}(\mathsf{H}(r_i,m_i))$ and simulated signatures $x_i \leftarrow \mathsf{SampDom}(\mathsf{F})$ are statistically indistinguishable. To win the INV game, $\mathcal{B}_{\mathsf{inv}}$ gives his query y to $\mathcal{A}_{\mathsf{cma}}$ in one of $(q_{\mathsf{sign}} + q_{\mathsf{ro}} + 1)$ queries to H. If $\mathcal{A}_{\mathsf{cma}}$ outputs a valid signature (m^*,r^*,x^*), $\mathsf{H}(r^*,m^*) = y$ holds and $\mathcal{B}_{\mathsf{inv}}$ can win the INV game with probability $\frac{1}{q_{\mathsf{sign}}+q_{\mathsf{ro}}+1}$. Hence, we have

$$\mathrm{Adv}^{\text{EUF-CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}^c}) \leq (q_{\mathsf{sign}} + q_{\mathsf{ro}} + 1)\mathrm{Adv}^{\text{INV}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{B}_{\mathsf{inv}}),$$

where $\mathcal{A}_{\mathsf{cma}^c}$ is an adversary who can make only classical queries to H.

Note that a tight reduction of $\mathrm{Adv}^{\text{INV}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{B}_{\mathsf{inv}}) \leq \mathrm{Adv}^{\text{OW}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{B}_{\mathsf{ow}})$ holds ($\mathcal{D}_{\mathcal{X}}$ is defined as $\mathsf{SampDom}(\mathsf{F})$ in the OW game (see Fig. 3)) since the OW adversary can simulate the INV game by giving a uniform $\mathsf{F}(x)$ to the INV adversary.

Security Proof by Semi-constant Distribution [50]: Zhandry showed the reduction from the OW of TDP in the QROM using a technique called *semi-constant distribution*. This technique leads to a reduction from the INV of PSF. $\mathcal{B}_{\mathsf{inv}}$ simulates the EUF-CMA game by generating signatures without the trapdoor as the above security proof in the ROM. Instead of adaptively programming H, $\mathcal{B}_{\mathsf{inv}}$ replaces H as $\mathsf{H}' = \mathsf{F}(\mathsf{DetSampDom}(\mathsf{F},\widetilde{\mathsf{H}}(r,m)))$, where $\widetilde{\mathsf{H}} \leftarrow_\$ \mathcal{W}^{\mathcal{R}\times\mathcal{M}}$ is a random function to output randomness w and $\mathsf{DetSampDom}$ is a deterministic function of $\mathsf{SampDom}$ [9]. From **Condition 1**, H' is indistinguishable from H.

Table 2: Summary of the existing and our security proofs. ϵ denotes the adversary's advantage in the game of the underlying assumption and $\epsilon_{\mathsf{ow/inv}} \in \{\epsilon_{\mathsf{ow}}, \epsilon_{\mathsf{inv}}\}$. In "Conditions of PSF", ✓ indicates this condition is necessary, and $\checkmark^1/\checkmark^2$ indicates that **Condition 2** is relaxed as "A bound δ on average of $\delta_{\mathsf{F,I}}$ is negligible" and "$\epsilon_{\mathsf{ps}} = \mathrm{Adv}^{\mathrm{PS}}_{\mathsf{T}_{\mathsf{wpsf}}}(\mathcal{D}_{\mathsf{ps}})$ is negligible". In "Target scheme", d/p/pr indicate that the security proof is applied to deterministic hash-and-sign, probabilistic hash-and-sign, and probabilistic hash-and-sign with retry.

Security proof	Security Bound	Assumption	Conditions of PSF 1	2	3	4	Target scheme
[9]	$\frac{1}{1-2^{-\omega(\log n)}}\epsilon_{\mathsf{cr}}$	CR	✓	✓	✓	✓	d/p
[50]	$2\sqrt{\left(q_{\mathsf{sign}} + \frac{8}{3}(q_{\mathsf{sign}} + q_{\mathsf{qro}} + 1)^4\right)\epsilon_{\mathsf{ow/inv}}}$	OW/INV	✓	✓	✓	–	d/p
ext. of [49]	$4q_{\mathsf{sign}}(q_{\mathsf{qro}}+1)(2q_{\mathsf{qro}}+1)^2\epsilon_{\mathsf{ow/inv}}$	OW/INV	✓	✓	✓	–	d/p
[11]	$\frac{1}{2}\left(\epsilon_{\mathsf{nma}} + \frac{8\pi}{\sqrt{3}}q_{\mathsf{qro}}^{\frac{3}{2}}\sqrt{\delta} + q_{\mathsf{sign}}\left(\delta + \frac{q_{\mathsf{sign}}}{\lvert\mathcal{R}\rvert}\right)\right)$	EUF-NMA	–	$\checkmark^1$	✓	–	p
ours	$(2q_{\mathsf{qro}}+1)^2\epsilon_{\mathsf{inv}} + \epsilon_{\mathsf{ps}} + \frac{3}{2}q'_{\mathsf{sign}}\sqrt{\frac{q'_{\mathsf{sign}}+q_{\mathsf{qro}}+1}{\lvert\mathcal{R}\rvert}}$ $+2(q_{\mathsf{sign}}+q_{\mathsf{qro}}+2)\sqrt{\frac{q'_{\mathsf{sign}}-q_{\mathsf{sign}}}{\lvert\mathcal{R}\rvert}}$	INV	–	$\checkmark^2$	–	–	p/pr
ours	$\epsilon_{\mathsf{nma}} + \epsilon_{\mathsf{ps}} + \frac{3}{2}q'_{\mathsf{sign}}\sqrt{\frac{q'_{\mathsf{sign}}+q_{\mathsf{qro}}+1}{\lvert\mathcal{R}\rvert}}$ $+2(q_{\mathsf{sign}}+q_{\mathsf{qro}}+2)\sqrt{\frac{q'_{\mathsf{sign}}-q_{\mathsf{sign}}}{\lvert\mathcal{R}\rvert}}$	EUF-NMA	–	$\checkmark^2$	–	–	p/pr
ours	$(2q_{\mathsf{qro}}+1)^2\epsilon_{\mathsf{ow/inv}} + \frac{3}{2}q_{\mathsf{sign}}\sqrt{\frac{q_{\mathsf{sign}}+q_{\mathsf{qro}}+1}{\lvert\mathcal{R}\rvert}}$	OW/INV	✓	✓	✓	–	p

To find a preimage of his challenge y, $\mathcal{B}_{\mathsf{inv}}$ programs H' that outputs y with probability ϵ (semi-constant distribution). In the signing oracle, if $\mathsf{H}'(r_i, m_i)$ outputs y, $\mathcal{B}_{\mathsf{inv}}$ aborts this game. A bound on the statistical distance between the random function and the programmed one with the semi-constant distribution is $\frac{8}{3}(q_{\mathsf{sign}} + q_{\mathsf{qro}} + 1)^4\epsilon^2$ [50, Corollary 4.3]. When $\mathcal{A}_{\mathsf{cma}}$ wins the EUF-CMA game, $\mathcal{B}_{\mathsf{inv}}$ can win the INV game with probability $(1-\epsilon)^{q_{\mathsf{sign}}}\epsilon \approx \epsilon - q_{\mathsf{sign}}\epsilon^2$. Minimizing the bound $\frac{1}{\epsilon}\mathrm{Adv}^{\mathrm{INV}}_{\mathsf{T}_{\mathsf{psf}}} + \left(q_{\mathsf{sign}} + \frac{8}{3}(q_{\mathsf{sign}} + q_{\mathsf{qro}} + 1)^4\right)\epsilon$ gives [50, Theorem 5.3]:

$$\mathrm{Adv}^{\mathrm{EUF\text{-}CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \leq 2\sqrt{\left(q_{\mathsf{sign}} + \frac{8}{3}\left(q_{\mathsf{sign}} + q_{\mathsf{qro}} + 1\right)^4\right)\mathrm{Adv}^{\mathrm{INV}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{B}_{\mathsf{inv}})} \quad (1)$$

Application of Lifting Theorem [49]: Yamakawa and Zhandry gave the lifting theorem for search-type games. As an application of the lifting theorem, they showed $\mathrm{Adv}^{\mathrm{EUF\text{-}NMA}}_{\mathsf{Sig}}(\mathcal{A}_{\mathsf{nma}}) \leq (2q_{\mathsf{qro}}+1)^2\mathrm{Adv}^{\mathrm{EUF\text{-}NMA}}_{\mathsf{Sig}}(\mathcal{A}_{\mathsf{nma^c}})$, where $\mathcal{A}_{\mathsf{nma^c}}$ is an EUF-NMA adversary making classical queries to H [49, Corollary 4.10].

For a hash-and-sign signature $\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}}, \mathsf{H}]$, they showed $\mathrm{Adv}^{\mathrm{EUF\text{-}CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \leq 4q_{\mathsf{sign}}\mathrm{Adv}^{\mathrm{EUF\text{-}NMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{nma}})$ [49, Theorem 4.11]. Extending the results of [49] using the security proof in the ROM, we have the following bound:

$$\mathrm{Adv}^{\mathrm{EUF\text{-}CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \leq 4q_{\mathsf{sign}}(q_{\mathsf{qro}}+1)(2q_{\mathsf{qro}}+1)^2\mathrm{Adv}^{\mathrm{INV}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{B}_{\mathsf{inv}})$$

Reduction from EUF-NMA *for WPSF [11]:* The security proofs mentioned above hold only if the underlying TDF is PSF. Unfortunately, some TDFs cannot satisfy some conditions. To relax the conditions on TDFs, Chailloux and Debris-Alazard gave EUF-NMA $\Rightarrow$ EUF-CMA for the probabilistic hash-and-sign. [9] The authors assumed a WPSF with **Condition 3** and a weaker version of **Condition 2**, that is, there is a bound δ on the average of statistical distance $\delta_{\mathsf{F},\mathsf{I}} = \Delta(\mathsf{SampDom}(\mathsf{F}), \mathsf{I}(\mathsf{U}(\mathcal{Y})))$ over all $(\mathsf{F}, \mathsf{I}) \leftarrow \mathsf{Gen}(1^\lambda)$ (see details in Section 5.1). Let $\mathsf{T}_{\mathsf{wpsf}}$ be a WPSF. The EUF-NMA adversary $\mathcal{A}_{\mathsf{nma}}$ replaces the random function H by H', which outputs $\mathsf{H}(r,m)$ with $\frac{1}{2}$ and $\mathsf{F}(\mathsf{DetSampDom}(\mathsf{F}, w))$ with $\frac{1}{2}$. A bound on the advantage of distinguishing H from H' is $\frac{8\pi}{\sqrt{3}}q_{\mathsf{qro}}^{3/2}\sqrt{\delta}$. The authors gave the following reduction [11, Theorem 2]:

$$\mathrm{Adv}^{\mathrm{EUF\text{-}CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \leq \frac{1}{2}\left(\mathrm{Adv}^{\mathrm{EUF\text{-}NMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{nma}}) + \frac{8\pi}{\sqrt{3}}q_{\mathsf{qro}}^{\frac{3}{2}}\sqrt{\delta} + q_{\mathsf{sign}}\left(\delta + \frac{q_{\mathsf{sign}}}{|\mathcal{R}|}\right)\right) \tag{2}$$

Reduction from Collision-resistance [9]: The authors of [9] gave a reduction from the CR of $\mathsf{T}_{\mathsf{psf}}$ to the sEUF-CMA security of $\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}}, \mathsf{H}]$. Let us assume that the CR adversary $\mathcal{B}_{\mathsf{cr}}$ given F simulates the sEUF-CMA game for $\mathcal{A}_{\mathsf{cma}}$. For a random function $\widetilde{\mathsf{H}} \leftarrow_\$ \mathcal{W}^{\mathcal{R}\times\mathcal{M}}$, $\mathcal{B}_{\mathsf{cr}}$ replaces the random function H as $\mathsf{H}'(r,m) = \mathsf{F}(\mathsf{DetSampDom}(\mathsf{F}, \widetilde{\mathsf{H}}(r,m)))$, where H and H' are indistinguishable from **Condition 1**. Also, the CR adversary simulates the signing oracle using **Conditions 2** and **3**. If $\mathcal{A}_{\mathsf{cma}}$ wins by (m^*, r^*, x^*), then $\mathsf{F}(x^*) = \mathsf{H}'(r^*, m^*) = \mathsf{F}(x')$ holds for $x' = \mathsf{DetSampDom}(\mathsf{F}, \widetilde{\mathsf{H}}(r^*, m^*))$. When $x^* \neq x'$, $\mathcal{B}_{\mathsf{cr}}$ can obtain a collision pair (x^*, x'). From **Condition 4**, $x^* \neq x'$ holds with probability $1 - 2^{-\omega(\log n)}$, and the following inequality holds [9, Theorem 2]:

$$\mathrm{Adv}^{\mathrm{sEUF\text{-}CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \leq \frac{1}{1-2^{-\omega(\log n)}}\mathrm{Adv}^{\mathrm{CR}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{B}_{\mathsf{cr}}) \tag{3}$$

4 New Security Proof

The main theorem is as follows:

Theorem 4.1 (INV $\Rightarrow$ EUF-CMA (Main Theorem)). *For any quantum* EUF-CMA *adversary* $\mathcal{A}_{\mathsf{cma}}$ *of* $\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}}, \mathsf{H}]$ *issuing at most* q_{sign} *classical queries*

[9] The authors of [11] defined a problem called *claw with random function problem*; however, the definition of this problem is identical to that of the EUF-NMA game for the hash-and-sign.

to the signing oracle and q_{qro} (quantum) random oracle queries to $\mathsf{H} \leftarrow_\$ \mathcal{Y}^{\mathcal{R}\times\mathcal{M}}$, there exist an INV *adversary $\mathcal{B}_{\mathsf{inv}}$ and a* PS *adversary $\mathcal{D}_{\mathsf{ps}}$ of $\mathsf{T}_{\mathsf{wpsf}}$ issuing q_{sign} sampling queries such that*

$$\begin{aligned}\mathrm{Adv}^{\text{EUF-CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) &\leq (2q_{\mathsf{qro}}+1)^2\mathrm{Adv}^{\mathrm{INV}}_{\mathsf{T}_{\mathsf{wpsf}}}(\mathcal{B}_{\mathsf{inv}}) + \mathrm{Adv}^{\mathrm{PS}}_{\mathsf{T}_{\mathsf{wpsf}}}(\mathcal{D}_{\mathsf{ps}}) \\ &+ \frac{3}{2}q'_{\mathsf{sign}}\sqrt{\frac{q'_{\mathsf{sign}}+q_{\mathsf{qro}}+1}{|\mathcal{R}|}} + 2(q_{\mathsf{sign}}+q_{\mathsf{qro}}+2)\sqrt{\frac{q'_{\mathsf{sign}}-q_{\mathsf{sign}}}{|\mathcal{R}|}},\end{aligned} \tag{4}$$

where q'_{sign} is a bound on the total number of queries to H in all the signing queries, and the running times of $\mathcal{B}_{\mathsf{inv}}$ and $\mathcal{D}_{\mathsf{ps}}$ are about that of $\mathcal{A}_{\mathsf{cma}}$.

We give some remarks beforehand and show the proof in Section 4.1.

Remark 4.1. If $\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H}].\mathsf{Sign}$ outputs a signature without retry ($\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H}]$ adopts the probabilistic hash-and-sign), then $q'_{\mathsf{sign}} = q_{\mathsf{sign}}$ holds and the last term of Eq. (4) becomes 0.

Remark 4.2. We have the following tight reduction in EUF-NMA $\Rightarrow$ EUF-CMA.

$$\begin{aligned}\mathrm{Adv}^{\text{EUF-CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) &\leq \mathrm{Adv}^{\text{EUF-NMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{nma}}) + \mathrm{Adv}^{\mathrm{PS}}_{\mathsf{T}_{\mathsf{wpsf}}}(\mathcal{D}_{\mathsf{ps}}) \\ &+ \frac{3}{2}q'_{\mathsf{sign}}\sqrt{\frac{q'_{\mathsf{sign}}+q_{\mathsf{qro}}+1}{|\mathcal{R}|}} + 2(q_{\mathsf{sign}}+q_{\mathsf{qro}}+2)\sqrt{\frac{q'_{\mathsf{sign}}-q_{\mathsf{sign}}}{|\mathcal{R}|}}\end{aligned} \tag{5}$$

Compared with the similar bound of Eq. (2) [11], the requirement for the TDF is weaker, and there are no square-root terms related to **Condition 2**.

Remark 4.3. If the underlying TDF is PSF (or TDP), we have

$$\begin{aligned}\mathrm{Adv}^{\text{EUF-CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) &\leq (2q_{\mathsf{qro}}+1)^2\mathrm{Adv}^{\mathrm{INV}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{B}_{\mathsf{inv}}) + \frac{3}{2}q_{\mathsf{sign}}\sqrt{\frac{q_{\mathsf{sign}}+q_{\mathsf{qro}}+1}{|\mathcal{R}|}}, \\ &\leq (2q_{\mathsf{qro}}+1)^2\mathrm{Adv}^{\mathrm{OW}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{B}_{\mathsf{ow}}) + \frac{3}{2}q_{\mathsf{sign}}\sqrt{\frac{q_{\mathsf{sign}}+q_{\mathsf{qro}}+1}{|\mathcal{R}|}}.\end{aligned}$$

Since $\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}},\mathsf{H}].\mathsf{Sign}$ outputs a signature without retry (**Condition 3**), $q'_{\mathsf{sign}} = q_{\mathsf{sign}}$ holds. In the PS game, outputs of I and $\mathsf{SampDom}(\mathsf{F})$ are statistically indistinguishable from **Condition 2**; therefore, $\mathrm{Adv}^{\mathrm{PS}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{D}_{\mathsf{ps}}) = 0$ holds. The above bounds are tighter than existing ones for $\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}},\mathsf{H}]$ (see Table 2).

Remark 4.4. Grilo et al. showed a tight reduction of EUF-NMA $\Rightarrow$ EUF-CMA in the Fiat-Shamir paradigm, assuming that the underlying ID scheme is honest verifier zero-knowledge (HVZK) [24, Theorem 3]. Also, Don et al. gave a generic reduction in the Fiat-Shamir transform of arbitrary ID schemes with a security loss $(2q_{\mathsf{qro}}+1)^2$ [18, Theorem 8]. The above reductions use the same techniques of adaptive reprogramming in the QROM (Lemmas 2.1 and 2.2) and their combination has the same security loss as Theorem 4.1.

There are two advantages compared with the existing security proofs.

Advantage 1: Wide applications: Our reduction gives security proofs for code-based and MQ-based hash-and-sign signatures. Relaxation of **Condition 2** is necessary for such applications. The existing security proofs replace H with H' at all once, which requires statistical indistinguishability of H and H'. On the other hand, our proof reprograms H in each signing query, and $\mathrm{Adv}^{\mathrm{PS}}_{\mathsf{T}_{\mathsf{wpsf}}}(\mathcal{B}_{\mathsf{ps}})$ can bound the advantage gap of games in EUF-NMA $\Rightarrow$ EUF-CMA.

Advantage 2: Tighter proof: Our reduction is tighter than the existing ones [50, 49] as mentioned in Remarks 4.2 and 4.3. The optimality of our reduction is not guaranteed; however, the multiplicative loss $(2q_{\mathsf{qro}}+1)^2$ seems unavoidable in the generic (black-box) reduction when we infer from three facts. First, the reduction incurs the loss $(q_{\mathsf{sign}}+q_{\mathsf{qro}}+1)$ even in the ROM (see Section 3.2). Second, the security loss of a generic reduction from ROM to QROM using the lifting theorem [49] is at least $(2q_{\mathsf{qro}}+1)^2$. Third, in the Fiat-Shamir paradigm, a generic reduction from arbitrary ID schemes incurs the same security loss as mentioned in Remark 4.4.

4.1 Proof of Theorem 4.1

Before showing INV $\Rightarrow$ EUF-CMA, we show that we can set $q'_{\mathsf{sign}} = \frac{c}{\rho} q_{\mathsf{sign}}$ for some integer $c > 1$, where $\rho = \Pr[x \neq \bot : y \leftarrow_{\$} \mathcal{Y}, x \leftarrow \mathsf{I}(y)]$. In q'_{sign} trials (queries to H), the number of successful trials ($\mathsf{I}(\mathsf{H}(r,m))$ outputs a preimage) must be at least q_{sign} to generate q_{sign} signatures. Let S be a random variable for the number of successful trials and $\mathbb{E}(S) = \rho q'_{\mathsf{sign}} = c q_{\mathsf{sign}}$ holds. From the Chernoff bound,

$$\Pr[S \leq (1-\gamma)\mathbb{E}(S)] \leq e^{-\frac{1}{2}\gamma^2 \mathbb{E}(S)}.$$

Substituting $\gamma = \frac{\mathbb{E}(S) - q_{\mathsf{sign}} + 1}{\mathbb{E}(S)}$, the LHS becomes $\Pr[S \leq q_{\mathsf{sign}} - 1]$ that is a probability that we cannot generate q_{sign} signatures with q'_{sign} trials. When we set $q'_{\mathsf{sign}} = \frac{c}{\rho} q_{\mathsf{sign}}$, the exponent of the RHS becomes $-\frac{((c-1)q_{\mathsf{sign}}+1)^2}{2c q_{\mathsf{sign}}} \geq -\frac{c-1}{2c} q_{\mathsf{sign}}$ and the bound on $\Pr[S \leq q_{\mathsf{sign}} - 1]$ becomes negligible for $q_{\mathsf{sign}} = \omega(\log(\lambda))$.

EUF-NMA $\Rightarrow$ EUF-CMA**:** Figs. 10 and 11 show the games and simulations described below. Without loss of generality, we assume that $\mathcal{A}_{\mathsf{cma}}$ makes queries $\{(r_i, m_i)\}_{i \in [q_{\mathsf{sign}}]}$ and (r^*, m^*) to H, where m_i is i-th query for $\mathsf{Sign}^{\mathsf{H}}$ and r_i is output by $\mathsf{Sign}^{\mathsf{H}}$. Then, the total number of queries to H is $q_{\mathsf{sign}} + q_{\mathsf{qro}} + 1$.

Game G_0 (EUF-CMA game): This is the original EUF-CMA game and $\Pr\left[\mathsf{G}_0^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] = \mathrm{Adv}^{\mathrm{EUF\text{-}CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}})$ holds.

Game G_1 (adaptive reprogramming on H): The signing oracle $\mathsf{Sign}^{\mathsf{H}}$ uniformly chooses (r_i, y_i) and reprograms $\mathsf{H} \coloneqq \mathsf{H}^{(r_i,m_i)\mapsto y_i}$ until $\mathsf{I}(y_i)$ does not output $\bot$ (see Lines 2 to 5 in $\mathsf{Sign}^{\mathsf{H}}$ for G_1). Considering the number of retries, H is reprogrammed for q'_{sign} times.

The AR adversary $\mathcal{D}_{\mathsf{ar}}$ can simulate $\mathsf{G}_0/\mathsf{G}_1$ (the top row of Fig. 11). If $\mathcal{D}_{\mathsf{ar}}$ plays AR_0, $\mathcal{D}_{\mathsf{ar}}$ simulates G_0; otherwise it simulates G_1. From Lemma 2.1, we have $\left|\Pr\left[\mathsf{G}_0^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_1^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]\right| \leq \mathrm{Adv}^{\mathrm{AR}}_{\mathsf{H}}(\mathcal{D}_{\mathsf{ar}}) \leq \frac{3}{2} q'_{\mathsf{sign}} \sqrt{\frac{q'_{\mathsf{sign}} + q_{\mathsf{qro}} + 1}{|\mathcal{R}|}}$.

Game: G_0-G_1

1 $\mathcal{Q} := \emptyset$
2 $\mathsf{H} \leftarrow_\$ \mathcal{Y}^{\mathcal{R}\times\mathcal{M}}$
3 $(\mathsf{F}, \mathsf{I}) \leftarrow \mathsf{Gen}(1^\lambda)$
4 $(m^*, r^*, x^*) \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign}, |\mathsf{H}\rangle}(\mathsf{F})$
5 **if** $m^* \in \mathcal{Q}$ **then**
6   **return** 0
7 **return** $\mathsf{F}(x^*) \stackrel{?}{=} \mathsf{H}(r^*, m^*)$

$\mathsf{Sign}^{\mathsf{H}}(m_i)$ for G_0

1 **repeat**
2     $r_i \leftarrow_\$ \mathcal{R}$
3     $x_i \leftarrow \mathsf{I}(\mathsf{H}(r_i, m_i))$
4 **until** $x_i \neq \bot$
5 $\mathcal{Q} := \mathcal{Q} \cup \{m_i\}$
6 **return** (r_i, x_i)

$\mathsf{Sign}^{\mathsf{H}}(m_i)$ for G_1

1 **repeat**
2     $y_i \leftarrow_\$ \mathcal{Y}$
3     $x_i \leftarrow \mathsf{I}(y_i)$
4     $r_i \leftarrow_\$ \mathcal{R}$
5     $\mathsf{H} := \mathsf{H}^{(r_i, m_i)\mapsto y_i}$
6 **until** $x_i \neq \bot$
7 $\mathcal{Q} := \mathcal{Q} \cup \{m_i\}$
8 **return** (r_i, x_i)

Game: G_2

1 $\mathcal{Q} := \emptyset$
2 $\mathsf{H} \leftarrow_\$ \mathcal{Y}^{\mathcal{R}\times\mathcal{M}}$
3 $ctr := 0$
4 $\mathcal{S} := \emptyset$
5 **for** $j \in [q'_{\mathsf{sign}} - q_{\mathsf{sign}}]$ **do**
6     $r \leftarrow_\$ \mathcal{R}$
7     $\mathcal{S} := \mathcal{S} \cup \{r\}$
8 $(\mathsf{F}, \mathsf{I}) \leftarrow \mathsf{Gen}(1^\lambda)$
9 $(m^*, r^*, x^*) \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign}, |\mathsf{H}\rangle}(\mathsf{F})$
10 **if** $m^* \in \mathcal{Q}$ **then**
11   **return** 0
12 **return** $\mathsf{F}(x^*) \stackrel{?}{=} \mathsf{H}(r^*, m^*)$

$\mathsf{Sign}^{\mathsf{H}}(m_i)$ for G_2

1 **repeat**
2     $y_i \leftarrow_\$ \mathcal{Y}$
3     $x_i \leftarrow \mathsf{I}(y_i)$
4   **if** $x_i = \bot$ **then**
5         $ctr := ctr + 1$
6         $r_i := \mathcal{S}[ctr]$
7   **else**
8         $r_i \leftarrow_\$ \mathcal{R}$
9     $\mathsf{H} := \mathsf{H}^{(r_i, m_i)\mapsto y_i}$
10 **until** $x_i \neq \bot$
11 $\mathcal{Q} := \mathcal{Q} \cup \{m_i\}$
12 **return** (r_i, x_i)

Game: G_3-G_5

1 $\mathcal{Q} := \emptyset$
2 $\mathsf{H} \leftarrow_\$ \mathcal{Y}^{\mathcal{R}\times\mathcal{M}}$
3 $\mathrm{FIND} := \bot$
4 $ctr := 0$
5 $\mathcal{S} := \emptyset$
6 **for** $j \in [q'_{\mathsf{sign}} - q_{\mathsf{sign}}]$ **do**
7     $r \leftarrow_\$ \mathcal{R}$
8     $\mathcal{S} := \mathcal{S} \cup \{r\}$
9 $\mathcal{S}' := \{(r, m) : r \in \mathcal{S}, m \in \mathcal{M}\}$
10 $(\mathsf{F}, \mathsf{I}) \leftarrow \mathsf{Gen}(1^\lambda)$
11 $(m^*, r^*, x^*) \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign}, |\mathsf{H}\setminus\mathcal{S}'\rangle}(\mathsf{F})$
12 **if** $m^* \in \mathcal{Q} \vee \mathrm{FIND} = \top$ **then**
13   **return** 0
14 **return** $\mathsf{F}(x^*) \stackrel{?}{=} \mathsf{H}(r^*, m^*)$

$\mathsf{Sign}^{\mathsf{H}}(m_i)$ for G_3

1 **repeat**
2     $y_i \leftarrow_\$ \mathcal{Y}$
3     $x_i \leftarrow \mathsf{I}(y_i)$
4   **if** $x_i = \bot$ **then**
5         $ctr := ctr + 1$
6         $r_i := \mathcal{S}[ctr]$
7   **else**
8         $r_i \leftarrow_\$ \mathcal{R}$
9     $\mathsf{H} := \mathsf{H}^{(r_i, m_i)\mapsto y_i}$
10 **until** $x_i \neq \bot$
11 $\mathcal{Q} := \mathcal{Q} \cup \{m_i\}$
12 **return** (r_i, x_i)

$\mathsf{Sign}^{\mathsf{H}}(m_i)$ for G_4

1 **repeat**
2     $y_i \leftarrow_\$ \mathcal{Y}$
3     $x_i \leftarrow \mathsf{I}(y_i)$
4 **until** $x_i \neq \bot$
5 $r_i \leftarrow_\$ \mathcal{R}$
6 $\mathsf{H} := \mathsf{H}^{(r_i, m_i)\mapsto y_i}$
7 $\mathcal{Q} := \mathcal{Q} \cup \{m_i\}$
8 **return** (r_i, x_i)

$\mathsf{Sign}^{\mathsf{H}}(m_i)$ for G_5

1 $x_i \leftarrow \mathsf{SampDom}(\mathsf{F})$
2 $r_i \leftarrow \mathcal{R}$
3 $\mathsf{H} := \mathsf{H}^{(r_i, m_i)\mapsto \mathsf{F}(x_i)}$
4 $\mathcal{Q} := \mathcal{Q} \cup \{m_i\}$
5 **return** (r_i, x_i)

Fig. 10: Games for EUF-NMA $\Rightarrow$ EUF-CMA

Game G_2 (pre-choosing r for unsuccessful trials): In the beginning, the challenger chooses $r \leftarrow_\$ \mathcal{R}$ for $q'_{\mathsf{sign}} - q_{\mathsf{sign}}$ times and keeps them in a sequence $\mathcal{S}$ (elements of $\mathcal{S}$ are ordered and may be duplicated.). In the signing oracle, $r_i = \mathcal{S}[ctr]$ is used for reprogramming if $\mathsf{I}(y_i)$ outputs $\bot$ for $y_i \leftarrow_\$ \mathcal{Y}$ (see Lines 6 and 9 of $\mathsf{Sign}^{\mathsf{H}}$ for G_2), where $\mathcal{S}[j]$ is j-th element of $\mathcal{S}$ and ctr is a counter that increments just before using $\mathcal{S}[ctr]$. In G_1, the challenger can choose r_i in the beginning since r_i is chosen independently of m_i chosen by $\mathcal{A}_{\mathsf{cma}}$. Also, r_i is always uniformly chosen whatever $\mathsf{I}(y_i)$ outputs. Therefore, the challenger can use r_i chosen in the beginning only when $\mathsf{I}(y)$ outputs $\bot$. Hence, $\Pr\left[\mathsf{G}_1^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] = \Pr\left[\mathsf{G}_2^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]$ holds.

$\mathcal{D}_{\mathsf{ar}}^{|\mathsf{H}_b\rangle}()$ simulates $\mathsf{G}_0/\mathsf{G}_1$

$\mathcal{Q} := \emptyset$
$(\mathsf{F}, \mathsf{I}) \leftarrow \mathsf{Gen}(1^\lambda)$
$(m^*, r^*, x^*) \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign}, |\mathsf{H}_b\rangle}(\mathsf{F})$
if $m^* \in \mathcal{Q}$ **then**
  return 0
return $\mathsf{F}(x^*) \stackrel{?}{=} \mathsf{H}_b(r^*, m^*)$

$\mathsf{Sign}^{\mathsf{H}_b, \mathsf{Repro}}(m_i)$

repeat
  $r_i \leftarrow \mathsf{Repro}(m_i)$
  $x_i \leftarrow \mathsf{I}(\mathsf{H}_b(r_i, m_i))$
until $x_i \neq \perp$
$\mathcal{Q} := \mathcal{Q} \cup \{m_i\}$
return (r_i, x_i)

$\mathcal{D}_{\mathsf{ps}}^{\mathsf{Sample}_b}(\mathsf{F})$ simulates $\mathsf{G}_4/\mathsf{G}_5$

$\mathcal{Q} := \emptyset$
$\mathsf{H} \leftarrow_\$ \mathcal{Y}^{\mathcal{R} \times \mathcal{M}}$
$\mathrm{FIND} := \perp$
$\mathcal{S} := \emptyset$
for $j \in [q'_{\mathsf{sign}} - q_{\mathsf{sign}}]$ **do**
  $r \leftarrow_\$ \mathcal{R}$
  $\mathcal{S} := \mathcal{S} \cup \{r\}$
$\mathcal{S}' := \{(r, m) \colon r \in \mathcal{S}, m \in \mathcal{M}\}$
$(m^*, r^*, x^*) \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign}, |\mathsf{H} \backslash \mathcal{S}'\rangle}(\mathsf{F})$
if $m^* \in \mathcal{Q} \vee \mathrm{FIND} = \top$ **then**
  return 0
return $\mathsf{F}(x^*) \stackrel{?}{=} \mathsf{H}(r^*, m^*)$

$\mathsf{Sign}^{\mathsf{H}, \mathsf{Sample}_b}(m_i)$

$r_i \leftarrow_\$ \mathcal{R}$
$x_i \leftarrow \mathsf{Sample}_b()$
$\mathsf{H} := \mathsf{H}^{(r_i, m_i) \mapsto \mathsf{F}(x_i)}$
$\mathcal{Q} := \mathcal{Q} \cup \{m_i\}$
return (r_i, x_i)

$\mathcal{A}_{\mathsf{nma}}^{|\mathsf{H}\rangle}(\mathsf{F})$ simulates G_5

$\mathcal{Q} := \emptyset$
$\mathsf{H}' := \mathsf{H}$
$\mathrm{FIND} := \perp$
$\mathcal{S} := \emptyset$
for $j \in [q'_{\mathsf{sign}} - q_{\mathsf{sign}}]$ **do**
  $r \leftarrow_\$ \mathcal{R}$
  $\mathcal{S} := \mathcal{S} \cup \{r\}$
$\mathcal{S}' := \{(r, m) \colon r \in \mathcal{S}, m \in \mathcal{M}\}$
$(m^*, r^*, x^*) \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign}, |\mathsf{H}' \backslash \mathcal{S}'\rangle}(\mathsf{F})$
if $m^* \in \mathcal{Q} \vee \mathrm{FIND} = \top$ **then**
  return 0
return $\mathsf{F}(x^*) \stackrel{?}{=} \mathsf{H}'(r^*, m^*)$

$\mathsf{Sign}^{\mathsf{H}'}(m_i)$

$r_i \leftarrow_\$ \mathcal{R}$
$x_i \leftarrow \mathsf{SampDom}(\mathsf{F})$
$\mathsf{H}' := \mathsf{H}'^{(r_i, m_i) \mapsto \mathsf{F}(x_i)}$
$\mathcal{Q} := \mathcal{Q} \cup \{m_i\}$
return (r_i, x_i)

Fig. 11: Simulations for EUF-NMA $\Rightarrow$ EUF-CMA

Game G_3 (puncturing H): Let $\mathcal{S}' = \{(r, m) \colon r \in \mathcal{S}, m \in \mathcal{M}\}$ be a set induced by $\mathcal{S}$. Instead of H, $\mathcal{A}_{\mathsf{cma}}$ makes queries to $\mathsf{H} \backslash \mathcal{S}'$ (H punctured by $\mathcal{S}'$). Also, G_3 outputs 0 if $\mathrm{FIND} = \top$ (see the definitions of $\mathsf{H} \backslash \mathcal{S}'$ and FIND in Definition 2.8). We use Lemma 2.4 to bound $\left|\Pr\left[\mathsf{G}_2^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_3^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]\right|$. We have $\Pr\left[\mathsf{G}_2^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] = \Pr\left[1 \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign}, |\mathsf{H}\rangle}(\mathsf{F})\right]$. Since G_3 uses $\mathsf{H} \backslash \mathcal{S}'$ and outputs 0 if $\mathrm{FIND} = \top$, we also have $\Pr\left[\mathsf{G}_3^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] = \Pr\left[1 \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign}, |\mathsf{H} \backslash \mathcal{S}'\rangle}(\mathsf{F}) \wedge \mathrm{FIND} = \perp\right]$ and $\Pr\left[\mathrm{FIND} = \top \colon \mathsf{G}_3^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow b\right] = \Pr\left[\mathrm{FIND} = \top \colon b \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign}, |\mathsf{H} \backslash \mathcal{S}'\rangle}(\mathsf{F})\right]$. Then,

$$\left|\Pr\left[\mathsf{G}_2^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_3^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]\right| \leq \sqrt{(q_{\mathsf{sign}} + q_{\mathsf{qro}} + 2) \Pr\left[\mathrm{FIND} = \top \colon \mathsf{G}_3^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow b\right]}, \quad (6)$$

by Lemma 2.4. We will show a bound on Eq. (6) after defining G_4.

Game: G_4'

$\mathcal{Q} := \emptyset$
$\mathsf{H} \leftarrow_{\$} \mathcal{Y}^{\mathcal{R}\times\mathcal{M}}$
$\mathcal{S} := \emptyset$
for $j \in [q'_{\mathsf{sign}}]$ **do**
  $r \leftarrow_{\$} \mathcal{R}$
  $\mathcal{S} := \mathcal{S} \cup \{r\}$
$\mathcal{S}' = \{(r,m) \colon r \in \mathcal{S}, m \in \mathcal{M}\}$
$(\mathsf{F},\mathsf{I}) \leftarrow \mathsf{Gen}(1^\lambda)$
$(r',m') \leftarrow \mathcal{B}_{\mathsf{cma}}^{\mathsf{Sign},|\mathsf{H}\rangle}(\mathsf{F})$
return $(r',m') \overset{?}{\in} \mathcal{S}'$

$\mathsf{Sign}^{\mathsf{H}}(m_i)$ for G_4'

repeat
  $y_i \leftarrow_{\$} \mathcal{Y}$
  $x_i \leftarrow \mathsf{I}(y_i)$
until $x_i \neq \bot$
$r_i \leftarrow_{\$} \mathcal{R}$
$\mathsf{H} := \mathsf{H}^{(r_i,m_i)\mapsto y_i}$
$\mathcal{Q} := \mathcal{Q} \cup \{m_i\}$
return (r_i, x_i)

Fig. 12: A game G_4' used in the application of Lemma 2.5

Game G_4 (reprogramming only for successful trials): The signing oracle reprograms $\mathsf{H} := \mathsf{H}^{(r_i,m_i)\mapsto y_i}$ only for $r_i \leftarrow \mathcal{R}$, $y_i \leftarrow_{\$} \mathcal{Y}$, and $x_i \leftarrow \mathsf{I}(y_i)$ satisfying $x_i \neq \bot$. Notice that $\mathcal{A}_{\mathsf{cma}}$ makes queries to $\mathsf{H}\backslash\mathcal{S}'$. By the definition of FIND, if FIND $= \bot$, that is, the measurements of $|\mathsf{f}_{\mathcal{S}'}(r,m)\rangle$ are 0 for all queries, then $\mathcal{A}_{\mathsf{cma}}$'s queries never contain any $(r,m) \in \mathcal{S}'$ and $\mathcal{A}_{\mathsf{cma}}$ cannot obtain $\mathsf{H}(r,m)$ for $(r,m) \in \mathcal{S}'$. Hence, if FIND $= \bot$, then $\mathcal{A}_{\mathsf{cma}}$ cannot distinguish whether H is reprogrammed at $(r,m) \in \mathcal{S}'$ in G_3 or not in G_4 and we have

$$\Pr\left[\mathrm{FIND} = \bot : \mathsf{G}_3^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow b\right] = \Pr\left[\mathrm{FIND} = \bot : \mathsf{G}_4^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow b\right] \tag{7}$$

(as Lemma 2.3). Especially, if $\mathsf{G}_3/\mathsf{G}_4$ outputs 1, then FIND should be $\bot$ (Line 12 of G_3-G_5). Thus, we also have $\Pr\left[\mathsf{G}_3^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] = \Pr\left[\mathsf{G}_4^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]$. Moreover, $\Pr\left[\mathrm{FIND} = \top \colon \mathsf{G}_3^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow b\right] = \Pr\left[\mathrm{FIND} = \top \colon \mathsf{G}_4^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow b\right]$ holds from Eq. (7).

Let G_4' be a game given in Fig. 12 (identical to G_4 except that $\mathcal{B}_{\mathsf{cma}}$ outputs (r',m') and H is not punctured). Choosing $j \leftarrow_{\$} [q_{\mathsf{sign}} + q_{\mathsf{qro}} + 1]$, $\mathcal{B}_{\mathsf{cma}}$ runs $\mathcal{A}_{\mathsf{cma}}$ playing G_4. Just before $\mathcal{A}_{\mathsf{cma}}$ makes j-th query to H, $\mathcal{B}_{\mathsf{cma}}$ measures a query input register of $\mathcal{A}_{\mathsf{cma}}$ and outputs the measurement outcome as (r',m'). Since the oracles of G_4' reveal no information on $\mathcal{S}$, $\mathcal{B}_{\mathsf{cma}}$ has no information on $\mathcal{S}$; therefore, $\Pr\left[\mathsf{G}_4'^{\mathcal{B}_{\mathsf{cma}}} \Rightarrow 1\right] \leq \Pr\left[r' \in \mathcal{S}\right] \leq \frac{q'_{\mathsf{sign}} - q_{\mathsf{sign}}}{|\mathcal{R}|}$ holds. Hence, $\Pr\left[\mathrm{FIND} = \top \colon \mathsf{G}_4^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow b\right] \leq 4(q_{\mathsf{sign}} + q_{\mathsf{qro}} + 1)\frac{q'_{\mathsf{sign}} - q_{\mathsf{sign}}}{|\mathcal{R}|}$ holds from Lemma 2.5 and we have a bound $2(q_{\mathsf{sign}} + q_{\mathsf{qro}} + 2)\sqrt{\frac{q'_{\mathsf{sign}} - q_{\mathsf{sign}}}{|\mathcal{R}|}}$ on Eq. (6).

Game G_5 (simulating the signing oracle by $\mathsf{SampDom}$): The signing oracle generates signatures by $r_i \leftarrow_{\$} \mathcal{R}$ and $x_i \leftarrow \mathsf{SampDom}(\mathsf{F})$. The PS adversary $\mathcal{D}_{\mathsf{ps}}$ can simulate G_4 and G_5 as in the second row of Fig. 11. If $\mathcal{D}_{\mathsf{ps}}$ plays PS_0, the procedures of the original and simulated G_4 are the same since $\mathsf{H} := \mathsf{H}^{(r_i,m_i)\mapsto \mathsf{F}(x_i)}$ in the simulated G_4 is identical to $\mathsf{H} := \mathsf{H}^{(r_i,m_i)\mapsto y_i}$ in the original G_4 (see Line 6 in $\mathsf{Sign}^{\mathsf{H}}$ for G_4). If $\mathcal{D}_{\mathsf{ps}}$ plays PS_1, he obviously simulates G_5. Thus, we have $\left|\Pr\left[\mathsf{G}_4^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_5^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]\right| \leq \mathrm{Adv}^{\mathrm{PS}}_{\mathsf{T}_{\mathsf{wpsf}}}(\mathcal{D}_{\mathsf{ps}})$.

We show that the EUF-NMA adversary $\mathcal{A}_{\mathsf{nma}}$ can simulate G_5 as in the bottom row of Fig. 11. In the simulation, $\mathcal{A}_{\mathsf{cma}}$ makes queries to $\mathsf{H}'\backslash\mathcal{S}'$, where H' outputs whatever H outputs except on $\{(r_i,m_i)\}_{i\in[q_{\mathsf{sign}}]}$. From $m^* \notin \mathcal{Q}$,

Adversary: $\mathcal{A}_{\mathsf{nma}}^{\lvert\mathsf{H}\rangle}(\mathsf{F})$	Simulator: $\mathsf{S}(\theta)$ for $\mathcal{A}_{\mathsf{nma}}^{\lvert\mathsf{H}\rangle}(\mathsf{F})$
$(m^*, r^*, x^*) \leftarrow \mathcal{A}_{\mathsf{nma}}^{\lvert\mathsf{H}\rangle}(\mathsf{F})$	$\mathsf{H} \leftarrow_{\$} \mathcal{Y}^{\mathcal{X}}$
return (m^*, r^*, x^*)	$(r', m') \leftarrow \mathsf{S}_1^{\mathcal{A}_{\mathsf{nma}}^{\lvert\mathsf{H}\rangle}}()$
	$\mathsf{H}' := \mathsf{H}^{(r',m')\mapsto\theta}$
	$x' \leftarrow \mathsf{S}_2^{\mathcal{A}_{\mathsf{nma}}^{\lvert\mathsf{H}'\rangle}}(\theta)$
	return (m', r', x')

Fig. 13: A two-stage simulator S for the EUF-NMA adversary $\mathcal{A}_{\mathsf{nma}}$

$\mathcal{A}_{\mathsf{nma}}$ wins his game if $\mathcal{A}_{\mathsf{cma}}$ wins the EUF-CMA game ($\mathsf{F}(x^*) = \mathsf{H}'(r^*, m^*)$ holds) since $\mathsf{H}'(r^*, m^*) = \mathsf{H}(r^*, m^*)$ holds. Hence, $\mathcal{A}_{\mathsf{nma}}$ can perfectly simulate G_5 with the same number of queries and almost the same running time as $\mathcal{A}_{\mathsf{cma}}$, and $\Pr\left[\mathsf{G}_5^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] \leq \mathrm{Adv}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H}]}^{\text{EUF-NMA}}(\mathcal{A}_{\mathsf{nma}})$ holds.

Summing up, we have Eq. (5).

INV $\Rightarrow$ EUF-NMA**:** We use Lemma 2.2. Let S be a two-stage algorithm that runs $\mathcal{A}_{\mathsf{nma}}$ in the EUF-NMA game shown in Fig. 13. The INV adversary $\mathcal{B}_{\mathsf{inv}}$ runs $\mathcal{A}_{\mathsf{nma}}$ indirectly by S. Since y is uniformly chosen in the INV game, $\mathcal{B}_{\mathsf{inv}}$ can set the input for S as $\theta := y$. In the first stage, S_1 observes one of the quantum queries to H made by $\mathcal{A}_{\mathsf{nma}}$ at random to obtain (r', m'). Then, H is reprogrammed as $\mathsf{H}' := \mathsf{H}^{(r',m')\mapsto\theta}$. In the second stage, S_2 runs $\mathcal{A}_{\mathsf{nma}}$ with reprogrammed H' and outputs x' included in an output of $\mathcal{A}_{\mathsf{nma}}^{\lvert\mathsf{H}'\rangle}(\mathsf{F})$.

When the predicate is $\mathsf{F}(x) \stackrel{?}{=} \mathsf{H}(r, m)$, we have the following inequality for any $(\hat{r}, \hat{m}) \in \mathcal{R} \times \mathcal{M}$ from Lemma 2.2:

$$\Pr\left[(r', m') = (\hat{r}, \hat{m}) \wedge \mathsf{F}(x') = y : (r', m') \leftarrow \mathsf{S}_1^{\mathcal{A}_{\mathsf{nma}}^{\lvert\mathsf{H}\rangle}}(), x' \leftarrow \mathsf{S}_2^{\mathcal{A}_{\mathsf{nma}}^{\lvert\mathsf{H}'\rangle}}(y)\right]$$
$$\geq \frac{1}{(2q_{\mathsf{qro}}+1)^2} \Pr\left[(r^*, m^*) = (\hat{r}, \hat{m}) \wedge \mathsf{F}(x^*) = \mathsf{H}(r^*, m^*) : (m^*, r^*, x^*) \leftarrow \mathcal{A}_{\mathsf{nma}}^{\lvert\mathsf{H}\rangle}(\mathsf{F})\right].$$

By summing up over all $(\hat{r}, \hat{m}) \in \mathcal{R} \times \mathcal{M}$,

$$\Pr\left[\mathsf{F}(x') = y : (r', m') \leftarrow \mathsf{S}_1^{\mathcal{A}_{\mathsf{nma}}^{\lvert\mathsf{H}\rangle}}(), x' \leftarrow \mathsf{S}_2^{\mathcal{A}_{\mathsf{nma}}^{\lvert\mathsf{H}'\rangle}}(y)\right]$$
$$\geq \frac{1}{(2q_{\mathsf{qro}}+1)^2} \Pr\left[\mathsf{F}(x^*) = \mathsf{H}(r^*, m^*) : (m^*, r^*, x^*) \leftarrow \mathcal{A}_{\mathsf{nma}}^{\lvert\mathsf{H}\rangle}(\mathsf{F})\right]. \quad (8)$$

Notice that the probability in the RHS of Eq. (8) is the EUF-NMA advantage. Also, $\mathrm{Adv}_{\mathsf{T}_{\mathsf{wpsf}}}^{\text{INV}}(\mathcal{B}_{\mathsf{inv}}) \geq \Pr\left[\mathsf{F}(x') = y : (r', m') \leftarrow \mathsf{S}_1^{\mathcal{A}_{\mathsf{nma}}^{\lvert\mathsf{H}\rangle}}(), x' \leftarrow \mathsf{S}_2^{\mathcal{A}_{\mathsf{nma}}^{\lvert\mathsf{H}'\rangle}}(y)\right]$ holds. Hence, we have

$$\mathrm{Adv}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H}]}^{\text{EUF-NMA}}(\mathcal{A}_{\mathsf{nma}}) \leq (2q_{\mathsf{qro}}+1)^2 \mathrm{Adv}_{\mathsf{T}_{\mathsf{wpsf}}}^{\text{INV}}(\mathcal{B}_{\mathsf{inv}}). \quad (9)$$

From Eqs. (5) and (9), we have Eq. (4). $\square$

4.2 Extension to sEUF-CMA Security

If F is injective, $\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}}, \mathsf{H}]$ is sEUF-CMA-secure.

Corollary 4.1 (INV $\Rightarrow$ sEUF-CMA). *Suppose that F of $\mathsf{T}_{\mathsf{wpsf}}$ is an injection. For any quantum* sEUF-CMA *adversary $\mathcal{A}_{\mathsf{cma}}$ of $\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}}, \mathsf{H}]$ issuing at most q_{sign} classical queries to the signing oracle and q_{qro} (quantum) random oracle queries to $\mathsf{H} \leftarrow_{\$} \mathcal{Y}^{\mathcal{R}\times\mathcal{M}}$, there exist an* INV *adversary $\mathcal{B}_{\mathsf{inv}}$ and a* PS *adversary $\mathcal{D}_{\mathsf{ps}}$ of $\mathsf{T}_{\mathsf{wpsf}}$ issuing q_{sign} sampling queries such that*

$$\begin{aligned}\mathrm{Adv}^{\text{sEUF-CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) &\le (2q_{\mathsf{qro}}+1)^2\mathrm{Adv}^{\mathrm{INV}}_{\mathsf{T}_{\mathsf{wpsf}}}(\mathcal{B}_{\mathsf{inv}}) + \mathrm{Adv}^{\mathrm{PS}}_{\mathsf{T}_{\mathsf{wpsf}}}(\mathcal{D}_{\mathsf{ps}})\\ &\quad + \frac{3}{2}q'_{\mathsf{sign}}\sqrt{\frac{q'_{\mathsf{sign}}+q_{\mathsf{qro}}+1}{|\mathcal{R}|}} + 2(q_{\mathsf{sign}}+q_{\mathsf{qro}}+2)\sqrt{\frac{q'_{\mathsf{sign}}-q_{\mathsf{sign}}}{|\mathcal{R}|}},\end{aligned}$$

where q'_{sign} is a bound on the total number of queries to H in all the signing queries, and the running times of $\mathcal{B}_{\mathsf{inv}}$ and $\mathcal{D}_{\mathsf{ps}}$ are about that of $\mathcal{A}_{\mathsf{cma}}$.

Proof. The sEUF-CMA game outputs 0 if $(m^*, r^*, x^*) \in \mathcal{Q}'$. Since F is injective, $(m^*, r^*) = (m_i, r_i)$ implies $x^* = x_i$. Therefore, the condition to output 0 is re-stated as: if $(m^*, r^*) \in \mathcal{Q}'$, where $\mathcal{Q}' = \{(m_i, r_i)\}_{i\in[q_{\mathsf{sign}}]}$. We show that EUF-NMA $\Rightarrow$ sEUF-CMA with the same bound as Eq. (5) holds.

In the games of Theorem 4.1, the same bound on $\left|\Pr\left[\mathsf{G}_0^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_5^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]\right|$ holds. In the simulation of G_5 (see the bottom row of Fig. 11), $\mathcal{A}_{\mathsf{cma}}$ uses $\mathsf{H}'\backslash\mathcal{S}'$ reprogrammed on $\{(r_i, m_i)\}_{i\in[q_{\mathsf{sign}}]}$ instead of the original H. By $(m^*, r^*) \notin \mathcal{Q}'$, $\mathsf{H}'(r^*, m^*) = \mathsf{H}(r^*, m^*)$ holds and $\mathcal{A}_{\mathsf{nma}}$ can win his game if $\mathsf{F}(x^*) = \mathsf{H}'(r^*, m^*)$. Therefore, $\Pr\left[\mathsf{G}_5^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] \le \mathrm{Adv}^{\text{EUF-NMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{nma}})$ holds, and thus, EUF-NMA $\Rightarrow$ sEUF-CMA holds with the same bound as Eq. (5). $\square$

5 Applications of New Security Proof

This section shows the applications of Theorem 4.1 (the main theorem) to some code-based and MQ-based hash-and-sign signatures. We briefly review the underlying TDFs of the signatures in Appendix A. Note that in lattice-based cryptography, all the practical and provable secure hash-and-sign signatures use collision-resistant PSFs given by the GPV framework [22]. Since the tight reduction in the QROM already exists for the GPV framework [9], it is unnecessary to apply Theorem 4.1.

5.1 Code-based Cryptography

Application to the Modified CSF Signature: Dallot [14] proposed a modification to the CFS signature, that is, adaption of the probabilistic hash-and-sign with retry. Let $\mathsf{T}_{\mathsf{cfs}} = (\mathsf{Gen}_{\mathsf{cfs}}, \mathsf{F}_{\mathsf{cfs}}, \mathsf{I}_{\mathsf{cfs}})$ be the underlying TDF of the modified CFS signature and $\mathcal{X}_{n,\le t} = \{x \in \mathbb{F}_q^n : 0 < \mathsf{hw}(x) \le t\}$ be a domain of $\mathsf{F}_{\mathsf{cfs}}$, where $\mathsf{hw}(x)$ denotes a Hamming weight of x. $\mathsf{F}_{\mathsf{cfs}} = UH_0P$ ($\mathsf{F}_{\mathsf{cfs}} : \mathcal{X}_{n,\le t} \to \mathbb{F}_q^{n-k}$) consists of an invertible matrix $H \in \mathbb{F}_q^{(n-k)\times(n-k)}$, a permutation matrix $P \in \mathbb{F}_q^{n\times n}$, and a parity-check matrix of an (n,k)-binary Goppa code. Since the (n,k)-binary Goppa code can decode up to t errors, there is a one-to-one correspondence between $\mathcal{X}_{n,\leq t}$ and $\mathcal{Y}_{dec} = \{y \in \mathbb{F}_q^{n-k} : y(U^{-1})^T \text{ is decodable}\}$, and $\mathsf{I}_{\mathsf{cfs}}(y)$ outputs $\perp$ for $y \notin \mathcal{Y}_{dec}$. Therefore, $\mathsf{F}_{\mathsf{cfs}} : \mathcal{X}_{n,\leq t} \to \mathbb{F}_q^{n-k}$ is an injection. Using the fact, Morozov et al. gave INV $\Rightarrow$ sEUF-CMA in the ROM [34, Theorem 3.1].

We show that the modified CFS signature is sEUF-CMA-secure in the QROM, assuming that $\mathsf{T}_{\mathsf{cfs}}$ is non-invertible.

Proposition 5.1 (INV $\Rightarrow$ sEUF-CMA (Modified CFS Signature)). *For any quantum* sEUF-CMA *adversary $\mathcal{A}_{\mathsf{cma}}$ of $\mathsf{HaS}[\mathsf{T}_{\mathsf{cfs}}, \mathsf{H}]$ issuing at most q_{sign} classical queries to the signing oracle and q_{qro} (quantum) random oracle queries to $\mathsf{H} \leftarrow_{\$} \mathcal{Y}^{\mathcal{R}\times\mathcal{M}}$, there exist an* INV *adversary $\mathcal{B}_{\mathsf{inv}}$ of $\mathsf{T}_{\mathsf{cfs}}$ such that*

$$\mathrm{Adv}^{\mathrm{sEUF\text{-}CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{cfs}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \leq (2q_{\mathsf{qro}}+1)^2 \mathrm{Adv}^{\mathrm{INV}}_{\mathsf{T}_{\mathsf{cfs}}}(\mathcal{B}_{\mathsf{inv}}) + \frac{3}{2} q'_{\mathsf{sign}} \sqrt{\frac{q'_{\mathsf{sign}} + q_{\mathsf{qro}} + 1}{|\mathcal{R}|}}$$
$$+ 2(q_{\mathsf{sign}} + q_{\mathsf{qro}} + 2)\sqrt{\frac{q'_{\mathsf{sign}} - q_{\mathsf{sign}}}{|\mathcal{R}|}},$$

where q'_{sign} is a bound on the total number of queries to H in all the signing queries and the running time of $\mathcal{B}_{\mathsf{inv}}$ is about that of $\mathcal{A}_{\mathsf{cma}}$.

Proof. When we define $\mathsf{SampDom}(\mathsf{F}_{\mathsf{cfs}})$ as $x \leftarrow_{\$} \mathcal{X}_{n,\leq t}$, $\mathsf{T}_{\mathsf{cfs}}$ becomes WPSF. Since $\mathsf{F}_{\mathsf{cfs}}$ is an injection, we can apply Corollary 4.1 to the modified CFS signature. In the PS game, we show that $\mathsf{SampDom}(\mathsf{F}_{\mathsf{cfs}})$ in Sample_1 can perfectly simulate x_i output by Sample_0. From the one-to-one correspondance between $\mathcal{X}_{n,\leq t}$ and $\mathcal{Y}_{dec}$, $x \leftarrow \mathsf{I}_{\mathsf{cfs}}(y)$ for $y \leftarrow_{\$} \mathcal{Y}_{dec}$ follows $\mathsf{U}(\mathcal{X}_{n,\leq t})$. Also, Sample_0 outputs x_i after retrying $y_i \leftarrow_{\$} \mathbb{F}_q^{n-k}$ until $\mathsf{I}_{\mathsf{cfs}}(y_i) \neq \perp$ holds; therefore y_i is uniformly chosen from $\mathcal{Y}_{dec}$. Hence, x_i output by Sample_0 is statistically indistinguishable from $x_i \leftarrow \mathsf{SampDom}(\mathsf{F}_{\mathsf{cfs}})$ and thus $\mathrm{Adv}^{\mathrm{PS}}_{\mathsf{T}_{\mathsf{cfs}}}(\mathcal{D}_{\mathsf{ps}}) = 0$ holds. $\square$

Application to Wave: Wave is a practical and unbroken hash-and-sign signature [15]. Wave adopts the probabilistic hash-and-sign (without retry) and Wave's TDF $\mathsf{T}_{\mathsf{wave}} = (\mathsf{Gen}_{\mathsf{wave}}, \mathsf{F}_{\mathsf{wave}}, \mathsf{I}_{\mathsf{wave}})$ satisfies conditions of *average trapdoor PSF (ATPSF)* [11, Definition 2] that is a special case of WPSF satisfying:

1. There is a bound δ on the average of $\delta_{\mathsf{F},\mathsf{I}}$ over all $(\mathsf{F},\mathsf{I}) \leftarrow \mathsf{Gen}(1^\lambda)$, that is, $\mathbb{E}_{\mathsf{F},\mathsf{I}}(\delta_{\mathsf{F},\mathsf{I}}) \leq \delta$, where $\delta_{\mathsf{F},\mathsf{I}} = \Delta(\mathsf{SampDom}(\mathsf{F}), \mathsf{I}(\mathsf{U}(\mathcal{Y})))$ is a statistical distance between $\mathsf{SampDom}(\mathsf{F})$ and $\mathsf{I}(y)$ for $y \leftarrow_{\$} \mathcal{Y}$ (**relaxed Condition 2**).
2. $\mathsf{I}(y)$ outputs x satisfying $\mathsf{F}(x) = y$ for any $y \in \mathcal{Y}$ (**Condition 3**).

We show that Wave is EUF-CMA-secure using the above conditions.

Proposition 5.2 (INV $\Rightarrow$ EUF-CMA (Wave)). *For any quantum* EUF-CMA *adversary $\mathcal{A}_{\mathsf{cma}}$ of $\mathsf{HaS}[\mathsf{T}_{\mathsf{wave}}, \mathsf{H}]$ issuing at most q_{sign} classical queries to the signing oracle and q_{qro} (quantum) random oracle queries to $\mathsf{H} \leftarrow_{\$} \mathcal{Y}^{\mathcal{R}\times\mathcal{M}}$, there exists*

$\underline{\mathsf{HaS}[\mathsf{T}_{\mathsf{uov}}, \mathsf{H}].\mathsf{Sign}(\mathsf{I}_{\mathsf{uov}}, m)}$

$z^v \leftarrow \mathsf{I}^1_{\mathsf{uov}}()$
repeat
  $r \leftarrow_\$ \mathcal{R}$
  $x \leftarrow \mathsf{I}^2_{\mathsf{uov}}(z^v, \mathsf{H}(r, m))$
until $x \neq \bot$
return (r, x)

$\underline{\mathsf{I}^1_{\mathsf{uov}}()}$

$z^v \leftarrow_\$ \mathbb{F}_q^v$
return z^v

$\underline{\mathsf{I}^2_{\mathsf{uov}}(z^v, y)}$

if $\{z^o : \mathsf{P}(z^v, z^o) = y\} = \emptyset$ **then**
  return $\bot$
$z^o \leftarrow_\$ \{z^o : \mathsf{P}(z^v, z^o) = y\}$
$x := \mathsf{S}^{-1}(z^v, z^o)$
return x

Fig. 14: Signature generation algorithm of the modified UOV signature

an INV *adversary* $\mathcal{B}_{\mathsf{inv}}$ *of* $\mathsf{T}_{\mathsf{wave}}$ *such that*

$$\mathrm{Adv}^{\text{EUF-CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{wave}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \leq (2q_{\mathsf{qro}} + 1)^2 \mathrm{Adv}^{\text{INV}}_{\mathsf{T}_{\mathsf{wave}}}(\mathcal{B}_{\mathsf{inv}}) + q_{\mathsf{sign}}\delta + \frac{3}{2} q_{\mathsf{sign}} \sqrt{\frac{q_{\mathsf{sign}} + q_{\mathsf{qro}} + 1}{|\mathcal{R}|}},$$

where the running time of $\mathcal{B}_{\mathsf{inv}}$ *is about that of* $\mathcal{A}_{\mathsf{cma}}$*.*

Proof. Since $\mathsf{T}_{\mathsf{wave}}$ is ATPSF [11] that is a special case of WPSF, we can apply Theorem 4.1 to Wave. Since $\mathsf{HaS}[\mathsf{T}_{\mathsf{wave}}, \mathsf{H}].\mathsf{Sign}$ generates signatures without retry, $q'_{\mathsf{sign}} = q_{\mathsf{sign}}$ holds (the last term of Eq. (4) is 0). From the first condition of ATPSF, there is a bound δ on the expectation of $\delta_{\mathsf{F},\mathsf{I}}$; therefore, $\mathrm{Adv}^{\text{PS}}_{\mathsf{T}_{\mathsf{wave}}}(\mathcal{D}_{\mathsf{ps}}) \leq q_{\mathsf{sign}}\delta$ holds from the union bound. □

Compared with the existing reduction using Eq. (2) [11], the factor of δ is not a square root in our reduction. Also, its security can be proved on the basis of hardness assumption of the syndrome decoding since there is a tight reduction from the syndrome decoding to the INV of $\mathsf{T}_{\mathsf{wave}}$ [11, Proposition 8].

5.2 Multivariate-quadratic-based Cryptography

Many schemes based on the UOV [29] and HFE [38] signatures have been proposed. Sakumoto et al. proposed modifications of the schemes adopting the probabilistic hash-and-sign with retry, and the modified schemes are EUF-CMA-secure in the ROM [43]. We prove that the modified UOV/HFE signatures are EUF-CMA-secure in the QROM if their TDFs are non-invertible. By the proof, we can show the EUF-CMA security of concrete signature schemes based on these two schemes, including Rainbow [16], QR-UOV [21], and GeMSS [10]. Also, we prove the EUF-CMA security of MAYO [7].

Application to the Modified UOV Signature: Let $\mathsf{T}_{\mathsf{uov}} = (\mathsf{Gen}_{\mathsf{uov}}, \mathsf{F}_{\mathsf{uov}}, \mathsf{I}_{\mathsf{uov}})$ be a TDF used in the modified UOV signature. $\mathsf{F}_{\mathsf{uov}} = \mathsf{P} \circ \mathsf{S}$ ($\mathsf{F}_{\mathsf{uov}} \colon \mathbb{F}_q^n \to \mathbb{F}_q^o$) consists of an invertible affine map $\mathsf{S} \colon \mathbb{F}_q^n \to \mathbb{F}_q^n$ and a multivariate quadratic polynomial $\mathsf{P} : \mathbb{F}_q^n \to \mathbb{F}_q^o$. Variables in P are called vinegar variables $z^v \in \mathbb{F}_q^v$ and oil variables $z^o \in \mathbb{F}_q^o$, where $n = v + o$. $\mathsf{P}(z^v, \cdot)$ becomes a set of linear functions on oil variables z^o by fixing z^v. Fig. 14 shows a signature generation algorithm.

Once z^v is randomly chosen by $\mathsf{I}^1_{\mathsf{uov}}$, $\mathsf{I}^2_{\mathsf{uov}}$ can easily find a preimage of $\mathsf{P} \circ \mathsf{S}$ by solving the linear equation system and taking the inverse of S.

Considering the difference in the signing procedure, we show the EUF-CMA security of the modified UOV signature in the QROM.

Proposition 5.3 (INV $\Rightarrow$ EUF-CMA (Modified UOV Signature)). *For any quantum* EUF-CMA *adversary $\mathcal{A}_{\mathsf{cma}}$ of $\mathsf{HaS}[\mathsf{T}_{\mathsf{uov}}, \mathsf{H}]$ issuing at most q_{sign} classical queries to the signing oracle and q_{qro} (quantum) random oracle queries to $\mathsf{H} \leftarrow_{\$} \mathcal{Y}^{\mathcal{R} \times \mathcal{M}}$, there exist an* INV *adversary $\mathcal{B}_{\mathsf{inv}}$ of $\mathsf{T}_{\mathsf{uov}}$ such that*

$$\mathrm{Adv}^{\mathrm{EUF\text{-}CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{uov}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \leq (2q_{\mathsf{qro}} + 1)^2 \mathrm{Adv}^{\mathrm{INV}}_{\mathsf{T}_{\mathsf{uov}}}(\mathcal{B}_{\mathsf{inv}}) + \frac{3}{2} q'_{\mathsf{sign}} \sqrt{\frac{q'_{\mathsf{sign}} + q_{\mathsf{qro}} + 1}{|\mathcal{R}|}} + 2(q_{\mathsf{sign}} + q_{\mathsf{qro}} + 2)\sqrt{\frac{q'_{\mathsf{sign}} - q_{\mathsf{sign}}}{|\mathcal{R}|}},$$

where q'_{sign} is a bound on the total number of queries to H in all the signing queries and the running time of $\mathcal{B}_{\mathsf{inv}}$ is about that of $\mathcal{A}_{\mathsf{cma}}$.

Proof. Defining $\mathsf{SampDom}(\mathsf{F}_{\mathsf{uov}})$ as $x \leftarrow_{\$} \mathbb{F}_q^n$, $\mathsf{T}_{\mathsf{uov}}$ becomes WPSF. Considering the signing procedure of the modified UOV signature, we modify the signing oracles of G_0-G_4 and Sample_0 of the PS game by adding $z^v \leftarrow \mathsf{I}^1_{\mathsf{uov}}()$ in the beginning and replacing $x_i \leftarrow \mathsf{I}(y_i)$ with $x_i \leftarrow \mathsf{I}^2_{\mathsf{uov}}(z^v, y_i)$. Then, $\mathcal{D}_{\mathsf{ps}}$ playing the modified PS game can simulate G_4 $(b = 0)$ and G_5 $(b = 1)$ in the proof of Theorem 4.1. Hence, we can apply Theorem 4.1 to the modified UOV scheme. In Sample_0 of the PS game, $x_i \leftarrow \mathsf{I}^2_{\mathsf{uov}}(z^v, y)$ after retrying y for $z^v \leftarrow \mathsf{I}^1_{\mathsf{uov}}()$ follows $\mathsf{U}(\mathbb{F}_q^n)$ form [43, Theorem 1] (we show the proof sketch in Appendix A.4); therefore, $\mathsf{SampDom}(\mathsf{F}_{\mathsf{uov}})$ in Sample_1 can simulate x_i output by Sample_0. Hence, $\mathrm{Adv}^{\mathrm{PS}}_{\mathsf{T}_{\mathsf{uov}}}(\mathcal{D}_{\mathsf{ps}}) = 0$ holds. □

We can apply Proposition 5.3 to Rainbow [16] and QR-UOV [21] if these schemes make the same modification as the modified UOV signature.

Application to the Modified HFE Signature: Let $\mathsf{T}_{\mathsf{hfe}} = (\mathsf{Gen}_{\mathsf{hfe}}, \mathsf{F}_{\mathsf{hfe}}, \mathsf{I}_{\mathsf{hfe}})$ be a TDF used in the modified HFE scheme. We show that the modified HFE signature is EUF-CMA secure.

Proposition 5.4 (INV $\Rightarrow$ EUF-CMA (Modified HFE Signature)). *For any quantum* EUF-CMA *adversary $\mathcal{A}_{\mathsf{cma}}$ of $\mathsf{HaS}[\mathsf{T}_{\mathsf{hfe}}, \mathsf{H}]$ issuing at most q_{sign} classical queries to the signing oracle and q_{qro} (quantum) random oracle queries to $\mathsf{H} \leftarrow_{\$} \mathcal{Y}^{\mathcal{R} \times \mathcal{M}}$, tthere exist an* INV *adversary $\mathcal{B}_{\mathsf{inv}}$ of $\mathsf{T}_{\mathsf{hfe}}$ such that*

$$\mathrm{Adv}^{\mathrm{EUF\text{-}CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{hfe}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \leq (2q_{\mathsf{qro}} + 1)^2 \mathrm{Adv}^{\mathrm{INV}}_{\mathsf{T}_{\mathsf{hfe}}}(\mathcal{B}_{\mathsf{inv}}) + \frac{3}{2} q'_{\mathsf{sign}} \sqrt{\frac{q'_{\mathsf{sign}} + q_{\mathsf{qro}} + 1}{|\mathcal{R}|}} + 2(q_{\mathsf{sign}} + q_{\mathsf{qro}} + 2)\sqrt{\frac{q'_{\mathsf{sign}} - q_{\mathsf{sign}}}{|\mathcal{R}|}},$$

where q'_{sign} *is a bound on the total number of queries to* H *in all the signing queries and the running time of* $\mathcal{B}_{\mathsf{inv}}$ *is about that of* $\mathcal{A}_{\mathsf{cma}}$*.*

Proof. Since $\mathsf{F}_{\mathsf{hfe}}$ has a domain $\mathbb{F}_q^n$, we can define $\mathsf{SampDom}(\mathsf{F}_{\mathsf{hfe}})$ as $x \leftarrow_{\$} \mathbb{F}_q^n$. Then, $\mathsf{T}_{\mathsf{hfe}}$ becomes WPSF and we can apply Theorem 4.1 to the modified HFE scheme. The authors of [43] showed that $x \leftarrow \mathsf{I}_{\mathsf{hfe}}(y)$ after retrying y is uniformly distributed over $\mathbb{F}_q^n$ (we show the proof sketch in Appendix A.5). Therefore, in the PS game, $\mathsf{SampDom}(\mathsf{F}_{\mathsf{hfe}})$ in Sample_1 can simulate x_i output by Sample_0, and thus, $\mathrm{Adv}^{\mathrm{PS}}_{\mathsf{T}_{\mathsf{hfe}}}(\mathcal{D}_{\mathsf{ps}}) = 0$ holds. □

We can apply Proposition 5.4 to GeMSS [10] since GeMSS takes the same modification as the modified HFE signature.

Application to MAYO: MAYO is a signature scheme adopting the probabilistic hash-and-sign with retry and its TDF is based on UOV [7]. Let $\mathsf{T}_{\mathsf{mayo}} = (\mathsf{Gen}_{\mathsf{mayo}}, \mathsf{F}_{\mathsf{mayo}}, \mathsf{I}_{\mathsf{mayo}})$ be a TDF used in MAYO. MAYO has an interesting property related to **Condition 2**. If $\mathsf{I}_{\mathsf{mayo}}$ never outputs $\perp$ (no retry), its output x is uniformly distributed over $\mathbb{F}_q^{kn}$ that is a domain of $\mathsf{F}_{\mathsf{mayo}}$. Let τ be a bound on the probability that $\mathsf{I}_{\mathsf{mayo}}$ outputs $\perp$. MAYO offers *no leakage* parameter sets that satisfy $\tau \leq 2^{-65}$.

Proposition 5.5 (INV⇒EUF-CMA (MAYO)). *For any quantum* EUF-CMA *adversary* $\mathcal{A}_{\mathsf{cma}}$ *of* $\mathsf{HaS}[\mathsf{T}_{\mathsf{mayo}}, \mathsf{H}]$ *issuing at most* q_{sign} *classical queries to the signing oracle and* q_{qro} *(quantum) random oracle queries to* $\mathsf{H} \leftarrow_{\$} \mathcal{Y}^{\mathcal{R}\times\mathcal{M}}$*, there exists an* INV *adversary* $\mathcal{B}_{\mathsf{inv}}$ *of* $\mathsf{T}_{\mathsf{mayo}}$ *such that*

$$\mathrm{Adv}^{\mathrm{EUF\text{-}CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{mayo}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \leq \frac{(2q_{\mathsf{qro}}+1)^2}{1-q_{\mathsf{sign}}\tau}\mathrm{Adv}^{\mathrm{INV}}_{\mathsf{T}_{\mathsf{mayo}}}(\mathcal{B}_{\mathsf{inv}}) + \frac{3}{2}q'_{\mathsf{sign}}\sqrt{\frac{q'_{\mathsf{sign}}+q_{\mathsf{qro}}+1}{|\mathcal{R}|}},$$

where q'_{sign} *is a bound on the total number of queries to* H *in all the signing queries and the running time of* $\mathcal{B}_{\mathsf{inv}}$ *is about that of* $\mathcal{A}_{\mathsf{cma}}$*.*

Proof. We only use the property of MAYO proven in proof of [7, Lemma 7], that is, $x \leftarrow \mathsf{I}_{\mathsf{mayo}}(y)$ follows $\mathsf{U}(\mathbb{F}_q^{kn})$ if $\mathsf{I}_{\mathsf{mayo}}$ never outputs $\perp$ (we show the proof sketch in Appendix A.6). We apply Theorem 4.1 with defining an intermediate game G'_1. G'_1 is the same as G_1 except that G'_1 aborts and outputs 0 whenever $\mathsf{I}_{\mathsf{mayo}}$ outputs $\perp$. The probability that G'_1 does not abort while q_{sign} signing queries is at least $1 - q_{\mathsf{sign}}\tau$. Therefore, $\Pr\left[\mathsf{G}_1^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] \leq \frac{1}{1-q_{\mathsf{sign}}\tau}\Pr\left[\mathsf{G}_1'^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]$ holds. Also, we consider G_5 without puncturing on H. When we define $\mathsf{SampDom}(\mathsf{F}_{\mathsf{mayo}})$ as $x \leftarrow_{\$} \mathbb{F}_q^{kn}$, the adversary of G_5 perfectly simulates the signing oracle in the case that G'_1 does not abort by using his oracle, and the view of the adversary is identical in the simulated one with the case that G'_1 does not abort. Hence, $\Pr\left[\mathsf{G}_1'^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] \leq \Pr\left[\mathsf{G}_5^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]$ holds. Since the EUF-NMA adversary can simulate G_5, $\Pr\left[\mathsf{G}_5^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] \leq \frac{1}{1-q_{\mathsf{sign}}\tau}\mathrm{Adv}^{\mathrm{EUF\text{-}NMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{mayo}},\mathsf{H}]}(\mathcal{A}_{\mathsf{nma}})$ holds, which yields the claimed bound. □

6 Provable Security of Hash-and-Sign with Prefix Hashing in Multi-key Setting

We show that the probabilistic hash-and-sign with retry is M-EUF-CMA-secure when *prefix hashing* [19] is adopted. In prefix hashing, the hash function H includes a small unpredictable part of the verification key. Let $\mathsf{H}\colon \mathcal{U}\times\mathcal{R}\times\mathcal{M}\to\mathcal{Y}$ be a hash function and $\mathsf{HaS}^{\mathsf{ph}}[\mathsf{T},\mathsf{H},\mathsf{E}]$ be a signature scheme adopting the probabilistic hash-and-sign with retry and prefix hashing, where $\mathsf{E}\colon \mathcal{Y}^{\mathcal{X}}\to\mathcal{U}$ is a deterministic function to extract a small unpredictable part of F into a key ID $u\in\mathcal{U}$. We assume that $\mathsf{E}(\mathsf{F})$ is uniform over $\mathcal{U}$ for $(\mathsf{F},\mathsf{I})\leftarrow\mathsf{Gen}(1^\lambda)$. [10] For a message m, $\mathsf{HaS}^{\mathsf{ph}}[\mathsf{T},\mathsf{H},\mathsf{E}].\mathsf{Sign}$ repeats $r\leftarrow\mathcal{R}$ and $x\leftarrow\mathsf{I}(\mathsf{H}(\mathsf{E}(\mathsf{F}),r,m))$ until $x\neq\bot$, and outputs (r,x). For a verification key F, a message m, and a signature (r,x), $\mathsf{HaS}^{\mathsf{ph}}[\mathsf{T},\mathsf{H},\mathsf{E}].\mathsf{Vrfy}$ verifies by $\mathsf{F}(x)\stackrel{?}{=}\mathsf{H}(\mathsf{E}(\mathsf{F}),r,m)$.

We have the following as an extension of Theorem 4.1 (we show the proof in Appendix B.1).

Theorem 6.1 (M-INV $\Rightarrow$ M-EUF-CMA). *For any quantum* M-EUF-CMA *adversary $\mathcal{A}_{\mathsf{cma}^{\mathsf{m}}}$ of $\mathsf{HaS}^{\mathsf{ph}}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H},\mathsf{E}]$ with q_{key} keys and issuing at most q_{sign} classical queries to the signing oracle and q_{qro} (quantum) random oracle queries to $\mathsf{H}\leftarrow_{\$}\mathcal{Y}^{\mathcal{U}\times\mathcal{R}\times\mathcal{M}}$, there exist an* M-INV *$\mathcal{B}_{\mathsf{inv}^{\mathsf{m}}}$ of $\mathsf{T}_{\mathsf{wpsf}}$ with q_{inst} instances and an* M-PS *adversary $\mathcal{D}_{\mathsf{ps}^{\mathsf{m}}}$ of $\mathsf{T}_{\mathsf{wpsf}}$ with q_{key} instances and issuing q_{sign} sampling queries such that*

$$\begin{aligned}\mathrm{Adv}^{\text{M-EUF-CMA}}_{\mathsf{HaS}^{\mathsf{ph}}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H},\mathsf{E}]}(\mathcal{A}_{\mathsf{cma}^{\mathsf{m}}}) \le (2q_{\mathsf{qro}}+1)^2\mathrm{Adv}^{\text{M-INV}}_{\mathsf{T}_{\mathsf{wpsf}}}(\mathcal{B}_{\mathsf{inv}^{\mathsf{m}}}) + \mathrm{Adv}^{\text{M-PS}}_{\mathsf{T}_{\mathsf{wpsf}}}(\mathcal{D}_{\mathsf{ps}^{\mathsf{m}}})\\ + \frac{3}{2}q'_{\mathsf{sign}}\sqrt{\frac{q'_{\mathsf{sign}}+q_{\mathsf{qro}}+1}{|\mathcal{R}|}} + 2(q_{\mathsf{sign}}+q_{\mathsf{qro}}+2)\sqrt{\frac{q'_{\mathsf{sign}}-q_{\mathsf{sign}}}{|\mathcal{R}|}}\\ + \frac{q_{\mathsf{key}}^2}{|\mathcal{U}|},\end{aligned} \tag{10}$$

where q'_{sign} is a bound on the total number of queries to H in all the signing queries, $\mathbb{E}_{\mathsf{F},\mathsf{I}}(q_{\mathsf{inst}})\le q_{\mathsf{key}}\left(\frac{|\mathcal{U}|}{|\mathcal{U}|-q_{\mathsf{key}}+1}\right)$ holds, and the running times of $\mathcal{B}_{\mathsf{inv}^{\mathsf{m}}}$ and $\mathcal{D}_{\mathsf{ps}^{\mathsf{m}}}$ are about that of $\mathcal{A}_{\mathsf{cma}^{\mathsf{m}}}$.

Also, we have the following (see the proof of Lemma 7.2 in Appendix B.3).

$$\mathrm{Adv}^{\text{M-sEUF-CMA}}_{\mathsf{HaS}^{\mathsf{ph}}[\mathsf{T}_{\mathsf{psf}},\mathsf{H},\mathsf{E}]}(\mathcal{A}_{\mathsf{cma}^{\mathsf{m}}}) \le \frac{1}{1-2^{-\omega(\log n)}}\mathrm{Adv}^{\text{M-CR}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{B}_{\mathsf{cr}^{\mathsf{m}}}) + \frac{q_{\mathsf{key}}^2}{|\mathcal{U}|}$$

7 Generic Method for Single-key to Multi-key Reduction.

There are trivial reductions with bounds; $\mathrm{Adv}^{\text{M-INV}}_{\mathsf{T}}(\mathcal{B}_{\mathsf{inv}^{\mathsf{m}}})\le q_{\mathsf{inst}}\mathrm{Adv}^{\text{INV}}_{\mathsf{T}}(\mathcal{B}_{\mathsf{inv}})$ and $\mathrm{Adv}^{\text{M-CR}}_{\mathsf{T}}(\mathcal{B}_{\mathsf{cr}^{\mathsf{m}}})\le q_{\mathsf{inst}}\mathrm{Adv}^{\text{CR}}_{\mathsf{T}}(\mathcal{B}_{\mathsf{cr}})$. If the adversaries can target multiple

[10] If unpredictable parts do not exist or are computationally expensive to include in H, a fixed nonce can be used instead (the nonce is put in the verification key).

Game: ST_b	$\mathsf{NewKey}_0()$	$\mathsf{NewKey}_1()$
$(\mathsf{F}, \mathsf{I}) \leftarrow \mathsf{Gen}'(1^\lambda)$	$(\mathsf{F}_j, \mathsf{I}_j) \leftarrow \mathsf{Gen}(1^\lambda)$	$\mathsf{L}_j \leftarrow \mathcal{D}_\mathsf{L}$
$b^* \leftarrow \mathcal{D}_{\mathsf{st}}^{\mathsf{NewKey}_b}(\mathsf{F})$	**return** F_j	$\mathsf{R}_j \leftarrow \mathcal{D}_\mathsf{R}$
return b^*		$\mathsf{F}_j := \mathsf{L}_j \circ \mathsf{F} \circ \mathsf{R}_j$
		return F_j

Fig. 15: ST (Sandwich Transformation) game

instances simultaneously, equality may hold in these inequalities. If we do not assume any security property on the underlying TDF, we cannot deny the feasibility of such attacks. To solve this problem, we propose a generic method for the single-key to multi-key reductions, that is, INV $\Rightarrow$ M-EUF-CMA and CR $\Rightarrow$ M-EUF-CMA.

Let $\{\mathsf{F}_j\}_{j\in[q_{\mathsf{key}}]}$ be verification keys generated by Gen of a TDF T in the M-EUF-CMA game. Given a verification key $\mathsf{F}\colon \mathcal{X}' \to \mathcal{Y}'$ generated by Gen' of another TDF T', we simulate $\{\mathsf{F}_j\}_{j\in[q_{\mathsf{key}}]}$ by $\{\mathsf{L}_j \circ \mathsf{F} \circ \mathsf{R}_j\}_{j\in[q_{\mathsf{key}}]}$, where $\mathsf{L}_j\colon \mathcal{Y}' \to \mathcal{Y}$ and $\mathsf{R}_j\colon \mathcal{X} \to \mathcal{X}'$. Let $\mathcal{D}_\mathsf{L}$ and $\mathcal{D}_\mathsf{R}$ be some distributions of L_j and R_j. We note that the domains and the ranges of F and F_j's may differ.

We define a new game to give a bound on the distinguishing advantage of $\{\mathsf{F}_j\}_{j\in[q_{\mathsf{key}}]}$ and $\{\mathsf{L}_j \circ \mathsf{F} \circ \mathsf{R}_j\}_{j\in[q_{\mathsf{key}}]}$.

Definition 7.1 (ST (Sandwich Transformation) Game). *Let* T *and* T' *be TDFs. Using a game given in Fig. 15, we define an advantage function of an adversary playing the* ST *game against* T *and* T' *as* $\mathrm{Adv}^{\mathrm{ST}}_{\mathsf{T},\mathsf{T}'}(\mathcal{D}_{\mathsf{st}}) = \left|\Pr\left[\mathsf{ST}_0^{\mathcal{D}_{\mathsf{st}}} \Rightarrow 1\right] - \Pr\left[\mathsf{ST}_1^{\mathcal{D}_{\mathsf{st}}} \Rightarrow 1\right]\right|$.

Note that we use a term, *valid* preimage, in this section. A *valid* preimage is a preimage that satisfies some conditions, e.g., *shortness* in lattice-based and code-based cryptography.

We have the following single-key to multi-key reductions assuming some conditions on L_j and R_j (see the proofs in Appendices B.2 and B.3).

Lemma 7.1 (INV $\Rightarrow$ M-EUF-CMA). *Suppose that* L_j *and* R_j *in the* ST *game satisfy:*

1. $\mathsf{L}_j\colon \mathcal{Y} \to \mathcal{Y}$ *is a bijection.*
2. *For any valid preimage* x *of* F_j, $\mathsf{R}_j(x)$ *is a valid preimage of* F ($\mathsf{R}_j\colon \mathcal{X} \to \mathcal{X}'$).

For any quantum M-EUF-CMA *adversary* $\mathcal{A}_{\mathsf{cma^m}}$ *of* $\mathsf{HaS}^{\mathsf{ph}}[\mathsf{T}_{\mathsf{wpsf}}, \mathsf{H}, \mathsf{E}]$ *with* q_{key} *keys and issuing at most* q_{sign} *classical queries to the signing oracle and* q_{qro} *(quantum) random oracle queries to* $\mathsf{H} \leftarrow_\$ \mathcal{Y}^{\mathcal{U}\times\mathcal{R}\times\mathcal{M}}$, *there exist an* INV *adversary* $\mathcal{B}_{\mathsf{inv}}$ *of* $\mathsf{T}'_{\mathsf{wpsf}}$ *with* q_{inst} *instances, an* M-PS *adversary* $\mathcal{D}_{\mathsf{ps^m}}$ *of* $\mathsf{T}_{\mathsf{wpsf}}$ *with* q_{key} *instances and issuing* q_{sign} *sampling queries, and an* ST *adversary* $\mathcal{D}_{\mathsf{st}}$ *of*

$(\mathsf{T}_{\mathsf{wpsf}}, \mathsf{T}'_{\mathsf{wpsf}})$ *issuing* q_{key} *new key queries such that*

$$\begin{aligned}\mathrm{Adv}^{\text{M-EUF-CMA}}_{\mathsf{HaS}^{\mathsf{ph}}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H},\mathsf{E}]}(\mathcal{A}_{\mathsf{cma}^{\mathsf{m}}}) \leq (2q_{\mathsf{qro}}+1)^2 \mathrm{Adv}^{\mathrm{INV}}_{\mathsf{T}'_{\mathsf{wpsf}}}(\mathcal{B}_{\mathsf{inv}}) + \mathrm{Adv}^{\text{M-PS}}_{\mathsf{T}_{\mathsf{wpsf}}}(\mathcal{D}_{\mathsf{ps}^{\mathsf{m}}}) \\ + \mathrm{Adv}^{\mathrm{ST}}_{\mathsf{T}_{\mathsf{wpsf}},\mathsf{T}'_{\mathsf{wpsf}}}(\mathcal{D}_{\mathsf{st}}) + \frac{3}{2} q'_{\mathsf{sign}} \sqrt{\frac{q'_{\mathsf{sign}} + q_{\mathsf{qro}} + 1}{|\mathcal{R}|}} \\ + 2(q_{\mathsf{sign}} + q_{\mathsf{qro}} + 2)\sqrt{\frac{q'_{\mathsf{sign}} - q_{\mathsf{sign}}}{|\mathcal{R}|}} + \frac{q^2_{\mathsf{key}}}{|\mathcal{U}|},\end{aligned}$$

where q'_{sign} *is a bound on the total number of queries to* H *in all the signing queries,* $\mathbb{E}_{\mathsf{F},\mathsf{I}}(q_{\mathsf{inst}}) \leq q_{\mathsf{key}} \left(\frac{|\mathcal{U}|}{|\mathcal{U}|-q_{\mathsf{key}}+1}\right)$ *holds, and the running times of* $\mathcal{B}_{\mathsf{inv}}$*,* $\mathcal{D}_{\mathsf{ps}^{\mathsf{m}}}$*, and* $\mathcal{D}_{\mathsf{st}}$ *are about that of* $\mathcal{A}_{\mathsf{cma}^{\mathsf{m}}}$*.*

Lemma 7.2 (CR ⇒ M-sEUF-CMA). *Suppose that* L_j *and* R_j *in the* ST *game satisfy:*

1. $\mathsf{R}_j : \mathcal{X} \to \mathcal{X}'$ *and* $\mathsf{L}_j : \mathcal{Y}' \to \mathcal{Y}$ *are injections.*
2. *For any valid preimage* x *of* F_j*,* $\mathsf{R}_j(x)$ *is a valid preimage of* F*.*

For any quantum M-sEUF-CMA *adversary* $\mathcal{A}_{\mathsf{cma}^{\mathsf{m}}}$ *of* $\mathsf{HaS}^{\mathsf{ph}}[\mathsf{T}_{\mathsf{psf}}, \mathsf{H}, \mathsf{E}]$ *with* q_{key} *keys and issuing at most* q_{sign} *classical queries to the signing oracle and* q_{qro} *(quantum) random oracle queries to* $\mathsf{H} \leftarrow_{\$} \mathcal{Y}^{\mathcal{U}\times\mathcal{R}\times\mathcal{M}}$*, there exist a* CR *adversary* $\mathcal{B}_{\mathsf{cr}}$ *of* $\mathsf{T}_{\mathsf{psf}}$ *with* q_{inst} *instances and an* ST *adversary* $\mathcal{D}_{\mathsf{st}}$ *of* $(\mathsf{T}_{\mathsf{psf}}, \mathsf{T}'_{\mathsf{psf}})$ *issuing* q_{key} *new key queries such that*

$$\mathrm{Adv}^{\text{M-sEUF-CMA}}_{\mathsf{HaS}^{\mathsf{ph}}[\mathsf{T}_{\mathsf{psf}},\mathsf{H},\mathsf{E}]}(\mathcal{A}_{\mathsf{cma}^{\mathsf{m}}}) \leq \frac{1}{1-2^{-\omega(\log n)}} \left(\mathrm{Adv}^{\mathrm{CR}}_{\mathsf{T}'_{\mathsf{psf}}}(\mathcal{B}_{\mathsf{cr}}) + \mathrm{Adv}^{\mathrm{ST}}_{\mathsf{T}_{\mathsf{psf}},\mathsf{T}'_{\mathsf{psf}}}(\mathcal{D}_{\mathsf{st}})\right) + \frac{q^2_{\mathsf{key}}}{|\mathcal{U}|},$$

where $\mathbb{E}_{\mathsf{F},\mathsf{I}}(q_{\mathsf{inst}}) \leq q_{\mathsf{key}} \left(\frac{|\mathcal{U}|}{|\mathcal{U}|-q_{\mathsf{key}}+1}\right)$ *holds and the running times of* $\mathcal{B}_{\mathsf{cr}}$ *and* $\mathcal{D}_{\mathsf{st}}$ *are about that of* $\mathcal{A}_{\mathsf{cma}^{\mathsf{m}}}$*.*

In Appendix C, we show use cases of the generic method in lattice-based, code-based, and MQ-based hash-and-sign signatures. We find that the ST advantage is bounded by some computational problems such as multi-instance versions of permutation equivalence [40] and morphism of polynomials [39].

There are two open problems for the generic method. First, the hardness of computational problems used for bounding the ST advantage has not been well studied; therefore, future studies are necessary for the underlying computational problems. Second, we cannot use the generic method to show the M-EUF-CMA security under *adaptive corruptions of secret keys.*

References

1. Ambainis, A., Hamburg, M., Unruh, D.: Quantum security proofs using semi-classical oracles. In: Boldyreva and Micciancio [6], pp. 269–295. https://doi.org/10.1007/978-3-030-26951-7_10 10, 11, 12

2. Bellare, M., Rogaway, P.: Random oracles are practical: A paradigm for designing efficient protocols. In: Denning, D.E., Pyle, R., Ganesan, R., Sandhu, R.S., Ashby, V. (eds.) ACM CCS 93. pp. 62–73. ACM Press (Nov 1993). https://doi.org/10.1145/168588.168596 1, 2, 7
3. Bellare, M., Rogaway, P.: The exact security of digital signatures: How to sign with RSA and Rabin. In: Maurer [32], pp. 399–416. https://doi.org/10.1007/3-540-68339-9_34 1, 5, 13
4. Beullens, W.: Not enough LESS: An improved algorithm for solving code equivalence problems over $\mathbb{F}_q$. Cryptology ePrint Archive, Report 2020/801 (2020), https://eprint.iacr.org/2020/801 41
5. Bindel, N., Hamburg, M., Hövelmanns, K., Hülsing, A., Persichetti, E.: Tighter proofs of CCA security in the quantum random oracle model. In: Hofheinz, D., Rosen, A. (eds.) TCC 2019, Part II. LNCS, vol. 11892, pp. 61–90. Springer, Heidelberg (Dec 2019). https://doi.org/10.1007/978-3-030-36033-7_3 11
6. Boldyreva, A., Micciancio, D. (eds.): CRYPTO 2019, Part II, LNCS, vol. 11693. Springer, Heidelberg (Aug 2019) 29
7. Beullens, W.: MAYO: Practical post-quantum signatures from oil-and-vinegar maps. Cryptology ePrint Archive, Report 2021/1144 (2021), https://eprint.iacr.org/2021/1144 2022-09-30 ver. 2, 5, 24, 26, 36, 37
8. Beullens, W.: Breaking Rainbow takes a weekend on a laptop. Cryptology ePrint Archive, Report 2022/214 (2022), https://eprint.iacr.org/2022/214
9. Boneh, D., Dagdelen, Ö., Fischlin, M., Lehmann, A., Schaffner, C., Zhandry, M.: Random oracles in a quantum world. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 41–69. Springer, Heidelberg (Dec 2011). https://doi.org/10.1007/978-3-642-25385-0_3 2, 3, 5, 13, 14, 15, 22, 39
10. Casanova, A., Faugère, J.C., Macario-Rat, G., Patarin, J., Perret, L., Ryckeghem, J.: GeMSS. Tech. rep., National Institute of Standards and Technology (2020), available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions 2, 5, 24, 26
11. Chailloux, A., Debris-Alazard, T.: Tight and optimal reductions for signatures based on average trapdoor preimage sampleable functions and applications to code-based signatures. In: Kiayias, A., Kohlweiss, M., Wallden, P., Zikas, V. (eds.) PKC 2020, Part II. LNCS, vol. 12111, pp. 453–479. Springer, Heidelberg (May 2020). https://doi.org/10.1007/978-3-030-45388-6_16 3, 4, 5, 7, 14, 15, 16, 23, 24, 34
12. Chatterjee, S., Das, M.P.L., Pandit, T.: Revisiting the Security of Salted UOV Signature. In: Isobe, T., Sarkar, S. (eds) Progress in Cryptology – INDOCRYPT 2022. LNCS, vol. 13774, pp. 697–719. Springer, Heidelberg (Jan 2023). https://doi.org/10.1007/978-3-031-22912-1_31 6
13. Courtois, N., Finiasz, M., Sendrier, N.: How to achieve a McEliece-based digital signature scheme. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 157–174. Springer, Heidelberg (Dec 2001). https://doi.org/10.1007/3-540-45682-1_10 2, 34
14. Dallot, L.: Towards a concrete security proof of Courtois, Finiasz and Sendrier signature scheme. In: WEWoRC 2007. LNCS, vol. 4945, pp. 65–77. Springer, Heidelberg (Jul 2007) 2, 5, 22, 33
15. Debris-Alazard, T., Sendrier, N., Tillich, J.P.: Wave: A new family of trapdoor one-way preimage sampleable functions based on codes. In: Galbraith, S.D., Moriai, S. (eds.) ASIACRYPT 2019, Part I. LNCS, vol. 11921, pp. 21–51. Springer, Heidelberg (Dec 2019). https://doi.org/10.1007/978-3-030-34578-5_2 2, 5, 23, 34

16. Ding, J., Chen, M.S., Petzoldt, A., Schmidt, D., Yang, B.Y., Kannwischer, M., Patarin, J.: Rainbow. Tech. rep., National Institute of Standards and Technology (2020), available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions 2, 5, 24, 25
17. Don, J., Fehr, S., Majenz, C.: The measure-and-reprogram technique 2.0: Multi-round fiat-shamir and more. In: Micciancio, D., Ristenpart, T. (eds.) CRYPTO 2020, Part III. LNCS, vol. 12172, pp. 602–631. Springer, Heidelberg (Aug 2020). https://doi.org/10.1007/978-3-030-56877-1_21 3, 6, 10, 11
18. Don, J., Fehr, S., Majenz, C., Schaffner, C.: Security of the Fiat-Shamir transformation in the quantum random-oracle model. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019, Part II. LNCS, vol. 11693, pp. 356–383. Springer, Heidelberg (Aug 2019). https://doi.org/10.1007/978-3-030-26951-7_13 16
19. Duman, J., Hövelmanns, K., Kiltz, E., Lyubashevsky, V., Seiler, G.: Faster lattice-based KEMs via a generic fujisaki-okamoto transform using prefix hashing. In: Vigna, G., Shi, E. (eds.) ACM CCS 2021. pp. 2722–2737. ACM Press (Nov 2021). https://doi.org/10.1145/3460120.3484819 4, 27
20. Fiat, A., Shamir, A.: How to prove yourself: Practical solutions to identification and signature problems. In: Odlyzko, A.M. (ed.) CRYPTO'86. LNCS, vol. 263, pp. 186–194. Springer, Heidelberg (Aug 1987). https://doi.org/10.1007/3-540-47721-7_12 2
21. Furue, H., Ikematsu, Y., Kiyomura, Y., Takagi, T.: A new variant of unbalanced Oil and Vinegar using quotient ring: QR-UOV. In: Tibouchi, M., Wang, H. (eds.) ASIACRYPT 2021, Part IV. LNCS, vol. 13093, pp. 187–217. Springer, Heidelberg (Dec 2021). https://doi.org/10.1007/978-3-030-92068-5_7 2, 5, 24, 25
22. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Ladner, R.E., Dwork, C. (eds.) 40th ACM STOC. pp. 197–206. ACM Press (May 2008). https://doi.org/10.1145/1374376.1374407 2, 5, 7, 8, 13, 22, 33, 40
23. Goldwasser, S., Micali, S., Rivest, R.L.: A digital signature scheme secure against adaptive chosen-message attacks. SIAM J. Comput. **17**(2), 281–308 (1988). https://doi.org/10.1137/0217017 1
24. Grilo, A.B., Hövelmanns, K., Hülsing, A., Majenz, C.: Tight adaptive reprogramming in the QROM. In: Tibouchi, M., Wang, H. (eds.) ASIACRYPT 2021, Part I. LNCS, vol. 13090, pp. 637–667. Springer, Heidelberg (Dec 2021). https://doi.org/10.1007/978-3-030-92062-3_22 3, 4, 10, 16
25. Hosoyamada, A., Yasuda, K.: Building quantum-one-way functions from block ciphers: Davies-Meyer and Merkle-Damgård constructions. In: Peyrin, T., Galbraith, S. (eds.) ASIACRYPT 2018, Part I. LNCS, vol. 11272, pp. 275–304. Springer, Heidelberg (Dec 2018). https://doi.org/10.1007/978-3-030-03326-2_10 2, 7
26. Hülsing, A., Rijneveld, J., Song, F.: Mitigating multi-target attacks in hash-based signatures. In: Cheng, C.M., Chung, K.M., Persiano, G., Yang, B.Y. (eds.) PKC 2016, Part I. LNCS, vol. 9614, pp. 387–416. Springer, Heidelberg (Mar 2016). https://doi.org/10.1007/978-3-662-49384-7_15 3, 10
27. Kiltz, E., Lyubashevsky, V., Schaffner, C.: A concrete treatment of Fiat-Shamir signatures in the quantum random-oracle model. In: Nielsen and Rijmen [35], pp. 552–586. https://doi.org/10.1007/978-3-319-78372-7_18 3
28. Kiltz, E., Masny, D., Pan, J.: Optimal security proofs for signatures from identification schemes. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016, Part II. LNCS, vol. 9815, pp. 33–61. Springer, Heidelberg (Aug 2016). https://doi.org/10.1007/978-3-662-53008-5_2 9

29. Kipnis, A., Patarin, J., Goubin, L.: Unbalanced Oil and Vinegar signature schemes. In: Stern, J. (ed.) EUROCRYPT'99. LNCS, vol. 1592, pp. 206–222. Springer, Heidelberg (May 1999). https://doi.org/10.1007/3-540-48910-X_15 2, 24, 34
30. Leon, J.: Computing automorphism groups of error-correcting codes. IEEE Transactions on Information Theory **28**(3), 496–511 (1982) 41
31. Liu, Y., Jiang, H., Zhao, Y.: Tighter Post-quantum Proof for Plain FDH, PFDH and GPV-IBE. Cryptology ePrint Archive, Report 2022/1441 (2022), https://eprint.iacr.org/2022/1441 6
32. Maurer, U.M. (ed.): EUROCRYPT'96, LNCS, vol. 1070. Springer, Heidelberg (May 1996) 30, 32
33. Menezes, A., Smart, N.: Security of signature schemes in a multi-user setting. Designs, Codes and Cryptography **33**(3), 261–274 (2004) 4
34. Morozov, K., Roy, P.S., Steinwandt, R., Xu, R.: On the security of the Courtois-Finiasz-Sendrier signature. Open Mathematics **16**(1), 161–167 (2018). https://doi.org/doi:10.1515/math-2018-0011, https://doi.org/10.1515/math-2018-0011 2, 23
35. Nielsen, J.B., Rijmen, V. (eds.): EUROCRYPT 2018, Part III, LNCS, vol. 10822. Springer, Heidelberg (Apr / May 2018) 31, 32
36. NIST: Submission requirements and evaluation criteria for the post-quantum cryptography standardization process (January 2017), https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf 4
37. NIST: Call for additional digital signature schemes for the post-quantum cryptography standardization process (Sep 2022), https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022.pdf 5
38. Patarin, J.: Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms. In: Maurer [32], pp. 33–48. https://doi.org/10.1007/3-540-68339-9_4 2, 24
39. Patarin, J., Goubin, L., Courtois, N.: Improved algorithms for isomorphisms of polynomials. In: Nyberg, K. (ed.) EUROCRYPT'98. LNCS, vol. 1403, pp. 184–200. Springer, Heidelberg (May / Jun 1998). https://doi.org/10.1007/BFb0054126 29, 42
40. Petrank, E., Roth, R.M.: Is code equivalence easy to decide? IEEE Transactions on Information Theory **43**(5), 1602–1604 (1997) 29, 41
41. Prest, T., Fouque, P.A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Ricosset, T., Seiler, G., Whyte, W., Zhang, Z.: FALCON. Tech. rep., National Institute of Standards and Technology (2022), available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022 2, 40
42. Saito, T., Xagawa, K., Yamakawa, T.: Tightly-secure key-encapsulation mechanism in the quantum random oracle model. In: Nielsen and Rijmen [35], pp. 520–551. https://doi.org/10.1007/978-3-319-78372-7_17 3
43. Sakumoto, K., Shirai, T., Hiwatari, H.: On provable security of UOV and HFE signature schemes against chosen-message attack. In: Yang, B.Y. (ed.) Post-Quantum Cryptography - 4th International Workshop, PQCrypto 2011. pp. 68–82. Springer, Heidelberg (Nov / Dec 2011). https://doi.org/10.1007/978-3-642-25405-5_5 2, 5, 6, 7, 24, 25, 26, 34, 35
44. Sendrier, N.: Finding the permutation between equivalent linear codes: The support splitting algorithm. IEEE Transactions on Information Theory **46**(4), 1193–1203 (2000) 41

45. Sendrier, N., Simos, D.E.: The hardness of code equivalence over and its application to code-based cryptography. In: Gaborit, P. (ed.) Post-Quantum Cryptography - 5th International Workshop, PQCrypto 2013. pp. 203–216. Springer, Heidelberg (Jun 2013). https://doi.org/10.1007/978-3-642-38616-9_14 41
46. Shor, P.W.: Algorithms for quantum computation: Discrete logarithms and factoring. In: 35th FOCS. pp. 124–134. IEEE Computer Society Press (Nov 1994). https://doi.org/10.1109/SFCS.1994.365700 2
47. Unruh, D.: Quantum position verification in the random oracle model. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014, Part II. LNCS, vol. 8617, pp. 1–18. Springer, Heidelberg (Aug 2014). https://doi.org/10.1007/978-3-662-44381-1_1 3, 10
48. Yamakawa, T., Zhandry, M.: Verifiable quantum advantage without structure. In: FOCS 2022 (2022), https://eprint.iacr.org/2022/434. To appear in FOCS 2022 3
49. Yamakawa, T., Zhandry, M.: Classical vs quantum random oracles. In: Canteaut, A., Standaert, F.X. (eds.) EUROCRYPT 2021, Part II. LNCS, vol. 12697, pp. 568–597. Springer, Heidelberg (Oct 2021). https://doi.org/10.1007/978-3-030-77886-6_20 3, 4, 5, 14, 15, 17
50. Zhandry, M.: Secure identity-based encryption in the quantum random oracle model. Cryptology ePrint Archive, Paper 2012/076 (2012), https://eprint.iacr.org/2012/076 3, 4, 5, 13, 14, 17

A Review of Trapdoor Functions in Hash-and-sign Signatures

A.1 GPV Framework [22]

Let $\mathsf{T}_{\mathsf{gpv}} = (\mathsf{Gen}_{\mathsf{gpv}}, \mathsf{F}_{\mathsf{gpv}}, \mathsf{I}_{\mathsf{gpv}})$ be a TDF used in the GPV framework. $\mathsf{Gen}_{\mathsf{gpv}}$ outputs a full-rank matrix $A \in \mathbb{Z}_q^{n\times m}$ generating a q-ary lattice Λ as $\mathsf{F}_{\mathsf{gpv}}$ and a matrix B generating $\Lambda_q^{\perp}$ that is orthogonal to Λ modulo q as $\mathsf{I}_{\mathsf{gpv}}$. The function $\mathsf{F}_{\mathsf{gpv}}$ computes $y = xA^T$ for a short vector $x \in \{x \in \mathbb{Z}^m \colon \|x\| \leq s\sqrt{m}\}$, where s is a Gaussian parameter. The trapdoor $\mathsf{I}_{\mathsf{gpv}}$ outputs a short vector x for $y \in \mathbb{F}_q^n$ using B. $\mathsf{T}_{\mathsf{gpv}}$ is collision-resistant PSF (see Definition 2.4) whose security is based on the hardness of the short integer solution (SIS) problem [22, Theorem 4.9].

A.2 Modified CFS Signature [14]

Let $\mathsf{T}_{\mathsf{cfs}} = (\mathsf{Gen}_{\mathsf{cfs}}, \mathsf{F}_{\mathsf{cfs}}, \mathsf{I}_{\mathsf{cfs}})$ be a TDF used in the modified CFS signature. $\mathcal{X}_{n,\leq t} = \{x \in \mathbb{F}_q^n : 0 < \mathsf{hw}(x) \leq t\}$ denotes a set of vectors $x \in \mathbb{F}_q^n$ whose Hamming weight, denoted by $\mathsf{hw}(x)$, is at most t. $\mathsf{Gen}_{\mathsf{cfs}}$ generates a parity-check matrix $H_0 \in \mathbb{F}_q^{(n-k)\times n}$ of an (n, k)-binary Goppa code, a random invertible matrix $U \in \mathbb{F}_q^{(n-k)\times(n-k)}$, and a random permutation matrix $P \in \mathbb{F}_q^{n\times n}$, and outputs $H = UH_0P \in \mathbb{F}_q^{(n-k)\times n}$ as $\mathsf{F}_{\mathsf{cfs}}$ and (U, H_0, P) as $\mathsf{I}_{\mathsf{cfs}}$. On input $x \in \mathcal{X}_{n,\leq t}$, the function $\mathsf{F}_{\mathsf{cfs}}$ computes a syndrome $y \coloneqq xH^T \in \mathbb{F}_q^{n-k}$. On input $y \in \mathbb{F}_q^{n-k}$, the trapdoor $\mathsf{I}_{\mathsf{cfs}}$ composed of (U, H_0, P) computes an error vector as follows: It decodes $y(U^{-1})^T$ using H_0 to obtain x', and outputs an error vector

$x = x'(P^{-1})^T$; if $y(U^{-1})^T$ is not decodable, it outputs $\perp$. Since the (n, k)-binary Goppa code can decode up to t errors, there is a one-to-one correspondence between $\mathcal{X}_{n,\le t}$ and $\mathcal{Y}_{dec} = \{y \in \mathbb{F}_q^{n-k} : y(U^{-1})^T \text{ is decodable}\}$ (decodable syndromes). Therefore, $\mathsf{F}_{\mathsf{cfs}}$ is injective and $\mathsf{I}_{\mathsf{cfs}}(y)$ outputs a preimage for $y \leftarrow_\$ \mathbb{F}_q^{n-k}$ with probability $\frac{|\mathcal{Y}_{dec}|}{|\mathbb{F}_q^{n-k}|} = \frac{|\mathcal{X}_{n,\le t}|}{|\mathbb{F}_q^{n-k}|}$. As shown in [13], $\frac{|\mathcal{X}_{n,\le t}|}{|\mathbb{F}_q^{n-k}|} \approx \frac{1}{t!}$ holds.

We show that a preimage x output by $\mathsf{HaS}[\mathsf{T}_{\mathsf{cfs}}, \mathsf{H}].\mathsf{Sign}$ follows $\mathsf{U}(\mathcal{X}_{n,\le t})$. First, $x \leftarrow \mathsf{I}_{\mathsf{cfs}}(y)$ for $y \leftarrow_\$ \mathcal{Y}_{dec}$ follows $\mathsf{U}(\mathcal{X}_{n,\le t})$ from the one-to-one correspondance between $\mathcal{X}_{n,\le t}$ and $\mathcal{Y}_{dec}$. Next, $\mathsf{HaS}[\mathsf{T}_{\mathsf{cfs}}, \mathsf{H}].\mathsf{Sign}$ outputs x after retrying $y \leftarrow_\$ \mathbb{F}_q^{n-k}$ until $\mathsf{I}_{\mathsf{cfs}}(y) \neq \perp$ holds; therefore y follows $\mathsf{U}(\mathcal{Y}_{dec})$. Hence, x output by $\mathsf{HaS}[\mathsf{T}_{\mathsf{cfs}}, \mathsf{H}].\mathsf{Sign}$ follows $\mathsf{U}(\mathcal{X}_{n,\le t})$.

A.3 Wave [15]

Let $\mathsf{T}_{\mathsf{wave}} = (\mathsf{Gen}_{\mathsf{wave}}, \mathsf{F}_{\mathsf{wave}}, \mathsf{I}_{\mathsf{wave}})$ be a TDF used in Wave and $H \in \mathbb{F}_q^{(n-k)\times n}$ be a parity-check matrix for an (n, k)-code over $\mathbb{F}_q$. $\mathcal{X}_{n,t} = \{x \in \mathbb{F}_q^n : \mathsf{hw}(x) = t\}$ denotes a set of vectors $x \in \mathbb{F}_q^n$ whose Hamming weight is exactly t, where t is chosen such that $\mathsf{F}_{\mathsf{wave}} \colon \mathcal{X}_{n,t} \to \mathbb{F}_q^{n-k}$ is a surjection. $\mathsf{Gen}_{\mathsf{wave}}$ outputs a parity-check matrix $H \in \mathbb{F}_q^{(n-k)\times n}$ for an (n, k)-code over $\mathbb{F}_q$ as $\mathsf{F}_{\mathsf{wave}}$ and parity-check matrices of generalized $(U, U+V)$-codes as $\mathsf{I}_{\mathsf{wave}}$. On input $x \in \mathcal{X}_{n,t}$, the function $\mathsf{F}_{\mathsf{wave}}$ computes a syndrome $y \coloneqq xH^T \in \mathbb{F}_q^{n-k}$. On input $y \in \mathbb{F}_q^{n-k}$, the trapdoor $\mathsf{I}_{\mathsf{wave}}$ outputs an element of $\mathcal{X}_{n,t}$. Since a description of $\mathsf{I}_{\mathsf{wave}}$ is out of the scope of this paper, we omit the description.

$\mathsf{T}_{\mathsf{wave}}$ satisfies the conditions of ATPSF [11, Definition 2] and we can take a statistical bound on the distinguishing advantage of honestly generated signatures and simulated ones.

A.4 Modified UOV Signature [43]

Let $\mathsf{T}_{\mathsf{uov}} = (\mathsf{Gen}_{\mathsf{uov}}, \mathsf{F}_{\mathsf{uov}}, \mathsf{I}_{\mathsf{uov}})$ be a TDF used in the modified UOV signatures. $\mathsf{Gen}_{\mathsf{uov}}$ generates an invertible affine map $\mathsf{S} \colon \mathbb{F}_q^n \to \mathbb{F}_q^n$ and a multivariate quadratic polynomial $\mathsf{P} : \mathbb{F}_q^n \to \mathbb{F}_q^o$ defined as $\mathsf{P} = (\mathsf{P}^1, \mathsf{P}^2, \ldots, \mathsf{P}^o)$, where

$$\mathsf{P}^k(z^v, z^o) = \sum_{i\in[v+o]} \sum_{j\in[v]} \alpha^k_{i,j} z_i z_j,$$

and outputs $\mathsf{P} \circ \mathsf{S}$ as $\mathsf{F}_{\mathsf{uov}}$ and (P, S) as $\mathsf{I}_{\mathsf{uov}}$. Variables in P are called vinegar variables $z^v = (z_1, z_2, \ldots, z_v) \in \mathbb{F}_q^v$ and oil variables $z^o = (z_{v+1}, z_{v+2}, \ldots, z_{v+o}) \in \mathbb{F}_q^o$, where $n = v + o$. The signing procedure of the modified UOV signature (see Fig. 14) is different from the others. $\mathsf{HaS}[\mathsf{T}_{\mathsf{uov}}, \mathsf{H}]$ using $\mathsf{I}^1_{\mathsf{uov}}$ and $\mathsf{I}^2_{\mathsf{uov}}$ generates a signature as follows: $\mathsf{I}^1_{\mathsf{uov}}$ chooses vinegar variables z^v uniformly at random. Fixing z^v, P becomes a set of linear functions on oil variables z^o. $\mathsf{I}^2_{\mathsf{uov}}$ finds a preimage of $\mathsf{P} \circ \mathsf{S}$ by solving a linear equation system and taking the inverse of S. There is possibly no solution. In the original UOV signature [29], the signing algorithm retakes the vinegar variables z^v. The modified UOV signature fixes vinegar variables z^v in $\mathsf{I}^1_{\mathsf{uov}}$ and retakes r in $\mathsf{I}^2_{\mathsf{uov}}$.

$\mathsf{I}_{\mathsf{hfe}}(y)$

$y' \leftarrow_\$ \mathbb{F}_q^m$
$z := \phi^{-1}(\mathsf{S}'^{-1}(y \| y'))$
$i \leftarrow_\$ [N]$
if $1 \le i \le \big|\{z' : \mathsf{P}(z') = z\}\big|$ **then**
  return $\perp$
$z' \leftarrow_\$ \{z' : \mathsf{P}(z') = z\}$
$x := \mathsf{S}^{-1}(\phi(z'))$
return x

Fig. 16: Trapdoor of the modified HFE signature

The authors of [43] showed that a probability that $\mathsf{I}_{\mathsf{uov}}$ does not output $\perp$ is

$$\sum_{i=1}^{o} p_i q^{i-o}, \text{ where } p_i = \frac{\left(\prod_{j=o-i+1}^{o}(1-q^{-j})\right)^2}{\prod_{j=1}^{i}(1-q^{-j})},$$

when we assume that $\mathsf{P}(z^v, \cdot)$ becomes a random $o \times o$ matrix for any z^v.

The authors of [43] also showed that preimages generated by $\mathsf{HaS}[\mathsf{T}_{\mathsf{uov}}, \mathsf{H}].\mathsf{Sign}$ are uniformly distributed over $\mathbb{F}_q^n$. For completeness, we give the proof sketch.

In the beginning, z^v is uniformly chosen (z^v follows $\mathsf{U}(\mathbb{F}_q^v)$). By fixing z^v, $\mathsf{P}(z^v, \cdot)$ becomes a set of linear functions containing $o \times o$ matrix whose rank is determined by choice of z^v if solutions exist. When the rank is i, $\mathsf{P}(z^v, \cdot)$ becomes a q^{o-i}-to-1 mapping for each element in the range $\mathbb{F}_q^o$. There are only q^i possible outputs of H satisfying $\{z^o : \mathsf{P}(z^v, z^o) = \mathsf{H}(r, m)\} \neq \emptyset$. When H is a random function, one of the q^i outputs is uniformly chosen after some retries. Once the output is fixed, one of q^{o-i} solutions is uniformly chosen. In this way, z^o follows $\mathsf{U}(\mathbb{F}_q^o)$ and thus $x = \mathsf{S}^{-1}(z^v, z^o)$ follows $\mathsf{U}(\mathbb{F}_q^n)$.

A.5 Modified HFE Signature [43]

Let $\mathsf{T}_{\mathsf{hfe}} = (\mathsf{Gen}_{\mathsf{hfe}}, \mathsf{F}_{\mathsf{hfe}}, \mathsf{I}_{\mathsf{hfe}})$ be a TDF used in the modified HFE signature and $\phi\colon K \to \mathbb{F}_q^n$ be a standard linear isomorphism $\phi(a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}) = (a_0, a_1, \ldots, a_{n-1})$, where $K = \mathbb{F}_q[x]/\mathsf{g}(x)$ for an irreducible polynomial $\mathsf{g}(x)$ of degree n. $\mathsf{Gen}_{\mathsf{hfe}}$ generates invertible affine maps $(\mathsf{S}, \mathsf{S}')$ over $\mathbb{F}_q^n$ and a central map $\mathsf{P}\colon K \to K$ defined as

$$\mathsf{P}(X) = \sum_{\substack{(i,j)\in[n]\times[n] \\ \text{s.t. } q^{i-1}+q^{j-1}<d}} \alpha_{i,j} X^{q^{i-1}+q^{j-1}} + \sum_{\substack{i\in[n] \\ \text{s.t. } q^{i-1}<d}} \beta_i X^{q^{i-1}},$$

where $\alpha_{i,j}, \beta_i \in K$, and outputs $\mathsf{S}' \circ \phi \circ \mathsf{P} \circ \phi^{-1} \circ \mathsf{S}$ as $\mathsf{F}_{\mathsf{hfe}}$ and $(\mathsf{P}, \mathsf{S}, \mathsf{S}')$ as $\mathsf{I}_{\mathsf{hfe}}$. On input $y \in \mathbb{F}_q^{n-m}$, $\mathsf{I}_{\mathsf{hfe}}$ computes a preimage $x \in \mathbb{F}_q^n$ as in Fig. 16.

As in the modified UOV signature, the authors of [43] showed that preimages generated by $\mathsf{HaS}[\mathsf{T}_{\mathsf{hfe}}, \mathsf{H}].\mathsf{Sign}$ are uniformly distributed over $\mathbb{F}_q^n$. We give the proof sketch too.

$\underline{\mathsf{I}_{\mathsf{mayo}}(y)}$

```
1 P*(x_1, ..., x_k) := Σ_{i∈[k]} E_{i,i} P(x_i) + Σ_{(i,j)∈I} E_{i,j} P'(x_i, x_j)
2 x^v ←$ (F_q^{n−m} × 0^m)^k
3 if P*(x^v + x^o) does not have full rank then
4     return ⊥
5 x^o ←$ {x^o : P*(x^v + x^o) = y}
6 x = x^v + x^o
7 return x
```

Fig. 17: Trapdoor of MAYO

When H is a random function, each $z \in \mathbb{F}_q^n$ is chosen with probability $\frac{1}{q^n}$. With probability $\frac{|\{z':\mathsf{P}(z')=z\}|}{N}$, $\mathsf{I}_{\mathsf{hfe}}$ chooses z' out of $|\{z' : \mathsf{P}(z') = z\}|$ elements, where N is set as d in general. Therefore, for any $x \in \mathbb{F}_q^n$, $\mathsf{HaS}[\mathsf{T}_{\mathsf{hfe}}, \mathsf{H}].\mathsf{Sign}$ outputs x with probability

$$\frac{1}{q^n} \cdot \frac{|\{z' : \mathsf{P}(z') = z\}|}{N} \cdot \frac{1}{|\{z' : \mathsf{P}(z') = z\}|} = \frac{1}{q^n N}.$$

Hence, preimages output by $\mathsf{HaS}[\mathsf{T}_{\mathsf{hfe}}, \mathsf{H}].\mathsf{Sign}$ are uniformly distributed over $\mathbb{F}_q^n$. Also, $\mathsf{I}_{\mathsf{hfe}}$ does not output $\perp$ with probability $\sum_{x\in\mathbb{F}_q^n} \frac{1}{q^n N} = \frac{1}{N}$.

A.6 MAYO [7]

Let $\mathsf{T}_{\mathsf{mayo}} = (\mathsf{Gen}_{\mathsf{mayo}}, \mathsf{F}_{\mathsf{mayo}}, \mathsf{I}_{\mathsf{mayo}})$ be a TDF used in MAYO. $\mathsf{Gen}_{\mathsf{mayo}}$ generates a multivariate quadratic polynomial $\mathsf{P}\colon \mathbb{F}_q^n \to \mathbb{F}_q^m$ with a subspace $\mathcal{O} \subset \mathbb{F}_q^n$ called *oil space* such that $\mathsf{P}(x) = 0$ for $x \in \mathcal{O}$, and outputs P as $\mathsf{F}_{\mathsf{mayo}}$ and a basis of $\mathcal{O}$ as $\mathsf{I}_{\mathsf{mayo}}$. [11] Let $\mathsf{P}(x) = (p_1(x), \ldots, p_m(x))$, where $p_i(x)\colon \mathbb{F}_q^n \to \mathbb{F}_q$ is a multivariate quadratic polynomial. The polar form of $p(x)$ is defined as

$$p'(x, y) \coloneqq p(x + y) - p(x) - p(y),$$

which is bilinear. We define the polar form of multivariate quadratic map $\mathsf{P}(x)$ to be $\mathsf{P}'(x, y) = (p'_1(x, y), \ldots, p'_m(x, y))$.

Let $\mathcal{I} = \{(i, j) \in [k] \times [k]\colon i \le j\}$ and $\{E_{ij}\}_{(i,j)\in\mathcal{I}}$ be a set of invertible matrices such that $E = \{E_{i,j}\}$ is nonsingular. On input $x = (x_1, \ldots, x_k) \in \mathbb{F}_q^{kn}$ and $\{E_{i,j}\}_{(i,j)\in\mathcal{I}}$, $\mathsf{F}_{\mathsf{mayo}}$ computes $y = \mathsf{P}^*(x) = \sum_{i\in[k]} E_{i,i}\mathsf{P}(x_i) + \sum_{(i,j)\in\mathcal{I}} E_{i,j}\mathsf{P}'(x_i, x_j)$. In MAYO, $\mathsf{P}^*\colon \mathbb{F}_q^{kn} \to \mathbb{F}_q^m$ is conjectured to be non-invertible. Therefore, the INV game of $\mathsf{T}_{\mathsf{mayo}}$ is defined as: given $(\mathsf{P}, \{E_{ij}\}_{(i,j)\in\mathcal{I}}, y)$, find $x^* = (x_1^*, \ldots, x_k^*)$ satisfying $\sum_{i\in[k]} E_{i,i}\mathsf{P}(x_i^*) + \sum_{(i,j)\in\mathcal{I}} E_{i,j}\mathsf{P}'(x_i^*, x_j^*)$ [7, Definition 4]. On input $y \in \mathbb{F}_q^m$, $\mathsf{I}_{\mathsf{mayo}}$ computes x as in Fig. 17. Let x, x^o and x^v be vectors over $\mathbb{F}_q^{kn}$. $\mathsf{I}_{\mathsf{mayo}}$ finds a preimage $x = x^v + x^o$ of y for P^*. In the beginning, x^v is uniformly chosen from $(\mathbb{F}_q^{n-m} \times 0^m)^k \subset \mathbb{F}_q^{kn}$, where 0^m denotes a vector of m 0s. Fixing x^v, $\mathsf{P}^*(x^v + x^o) = y$ becomes a linear system of equations for x^o. $\mathsf{I}_{\mathsf{mayo}}$ outputs

[11] For the convenience of MAYO's description, the notation of UOV follows [7] which is slightly different from Appendix A.4.

<u>GAME: M-EUF-NMA</u>
for $j \in [q_{\mathsf{key}}]$ do
$(vk_j, sk_j) \leftarrow \mathsf{Sig.KeyGen}(1^\lambda)$
$(j^*, m^*, \sigma^*) \leftarrow \mathcal{A}_{\mathsf{nma^m}}(\{vk_j\}_{j\in[q_{\mathsf{key}}]})$
return $\mathsf{Sig.Verify}(vk_{j^*}, m^*, \sigma^*)$

Fig. 18: M-EUF-NMA (Multi-key EUF-NMA) game

$x^v + x^o$ by solving $\mathsf{P}^*(x^v + x^o) = y$ if $\mathsf{P}^*(x^v + x^o)$ has full rank and outputs $\perp$ otherwise. The probability that $\mathsf{I}_{\mathsf{mayo}}$ outputs $\perp$, that is, $\mathsf{P}^*(x^v + x^o)$ does not have full rank, is bounded by $\tau = \frac{q^{k-n+o}+q^{m-ko}}{q-1}$ [7, Lemma 2].

Bullens showed that a preimage $x \leftarrow \mathsf{I}_{\mathsf{mayo}}(y)$ is uniform over $\mathbb{F}_q^{kn}$ if $\mathsf{I}_{\mathsf{mayo}}$ has never output $\perp$ in the signature generation [7, Lemma 7]. Since this property is necessary for applying Theorem 4.1, we show the proof sketch.

First, x^v is uniformly chosen from $(\mathbb{F}_q^{n-m} \times 0^m)^k$. Next, x^o is uniformly chosen from $\mathcal{O}^k$ since $\mathsf{P}^*(x^v + x^o)$ has full rank when $\mathsf{I}_{\mathsf{mayo}}$ does not output $\perp$. Hence, the output $x = (x^v + x^o)$ follows $\mathsf{U}(\mathbb{F}_q^{kn})$ since $(\mathbb{F}_q^{n-m} \times 0^m) + \mathcal{O} = \mathbb{F}_q^n$.

B Missing Proofs

B.1 Proof of Theorem 6.1

We prove two reductions; M-EUF-NMA $\Rightarrow$ M-EUF-CMA and M-INV $\Rightarrow$ M-EUF-CMA, where M-EUF-NMA stands for *multi-key* EUF-NMA. We define an advantage function of the M-EUF-NMA game given in Fig. 18 as $\mathrm{Adv}_{\mathsf{Sig}}^{\text{M-EUF-NMA}}(\mathcal{A}_{\mathsf{nma^m}}) = \Pr\left[\mathsf{M\text{-}EUF\text{-}NMA}^{\mathcal{A}_{\mathsf{nma^m}}} \Rightarrow 1\right]$. Without loss of generality, we assume that adversaries make random oracle queries by fixing key ID u as one of the q_{key} verification keys.

M-EUF-NMA $\Rightarrow$ M-EUF-CMA*:*

GAME G_0 (M-EUF-CMA game): This is the original M-EUF-CMA game and $\Pr\left[\mathsf{G}_0^{\mathcal{A}_{\mathsf{cma^m}}} \Rightarrow 1\right] = \mathrm{Adv}_{\mathsf{HaS^{ph}}[\mathsf{T_{wpsf}},\mathsf{H},\mathsf{E}]}^{\text{M-EUF-CMA}}(\mathcal{A}_{\mathsf{cma^m}})$ holds.

GAME G_1 (reprogramming H): We make modifications in the same manner as G_1-G_4 of Theorem 4.1. The challenger chooses $r \leftarrow_\$ \mathcal{R}$ for $q'_{\mathsf{sign}} - q_{\mathsf{sign}}$ times and keeps them in a sequence $\mathcal{S}$, punctures H by $\mathcal{S}' = \{u \in \mathcal{U}, r \in \mathcal{S}, m \in \mathcal{M}\}$, and outputs 0 if FIND $= \top$. In answering i-th signing query for j-th verification key, the signing oracle reprograms $\mathsf{H} := \mathsf{H}^{(\mathsf{E}(\mathsf{F}_j), r_i, m_i) \mapsto y_i}$ for $r_i \leftarrow \mathcal{R}$ and $y_i \leftarrow_\$ \mathcal{Y}$ after some retries until $\mathsf{I}_j(y_i)$ does not output $\perp$.

By considering the differences in the single-key/multi-key settings, we show that the same bound as $\mathsf{G}_0/\mathsf{G}_4$ of Theorem 4.1 holds in $\mathsf{G}_0/\mathsf{G}_1$ of Theorem 6.1. Note that we can derive the bound on advantage gaps of G_0-G_4 in Theorem 4.1 by considering queries to H, reprogramming on H, and puncturing on H. The difference in H, that is, domain of H is $\mathcal{R}\times\mathcal{M}$ or $\mathcal{U}\times\mathcal{R}\times\mathcal{M}$, does not affect the bound since we can regard the message space of H as $\mathcal{U} \times \mathcal{M}$.

Also, the difference in the signing oracle, that is, usage of I or $\{\mathsf{I}_j\}_{j\in[q_{\mathsf{key}}]}$, does not affect the bound. Hence, the same bound as $\mathsf{G}_0/\mathsf{G}_4$ of Theorem 4.1 holds, that is, $\left|\Pr\left[\mathsf{G}_0^{\mathcal{A}_{\mathsf{cma}^{\mathsf{m}}}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_1^{\mathcal{A}_{\mathsf{cma}^{\mathsf{m}}}} \Rightarrow 1\right]\right| \leq \frac{3}{2}q'_{\mathsf{sign}}\sqrt{\frac{q'_{\mathsf{sign}}+q_{\mathsf{qro}}+1}{|\mathcal{R}|}} + 2(q_{\mathsf{sign}} + q_{\mathsf{qro}} + 2)\sqrt{\frac{q'_{\mathsf{sign}}-q_{\mathsf{sign}}}{|\mathcal{R}|}}$.

Game G_2 (simulating the signing oracle by $\mathsf{SampDom}$): The signing oracle reprograms $\mathsf{H} := \mathsf{H}^{(\mathsf{E}(\mathsf{F}_j), r_i, m_i)\mapsto \mathsf{F}_j(x_i)}$ for $r_i \leftarrow \mathcal{R}$ and $x_i \leftarrow \mathsf{SampDom}(\mathsf{F}_j)$, and outputs (r_i, x_i). Since the M-PS adversary can simulate $\mathsf{G}_1/\mathsf{G}_2$, we have $\left|\Pr\left[\mathsf{G}_1^{\mathcal{A}_{\mathsf{cma}^{\mathsf{m}}}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_2^{\mathcal{A}_{\mathsf{cma}^{\mathsf{m}}}} \Rightarrow 1\right]\right| \leq \mathrm{Adv}^{\text{M-PS}}_{\mathsf{T}_{\mathsf{wpsf}}}(\mathcal{D}_{\mathsf{ps}^{\mathsf{m}}})$.

Since the M-EUF-NMA adversary $\mathcal{A}_{\mathsf{nma}^{\mathsf{m}}}$ can simulate G_2 by using $\mathsf{SampDom}$, $\Pr\left[\mathsf{G}_2^{\mathcal{A}_{\mathsf{cma}^{\mathsf{m}}}} \Rightarrow 1\right] \leq \mathrm{Adv}^{\text{M-EUF-NMA}}_{\mathsf{HaS}^{\mathsf{ph}}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H},\mathsf{E}]}(\mathcal{A}_{\mathsf{nma}^{\mathsf{m}}})$ holds.

M-INV $\Rightarrow$ M-EUF-NMA*:*

Game G_3 (M-EUF-NMA game): This is the original M-EUF-NMA game and $\Pr\left[\mathsf{G}_3^{\mathcal{A}_{\mathsf{nma}^{\mathsf{m}}}} \Rightarrow 1\right] = \mathrm{Adv}^{\text{M-EUF-NMA}}_{\mathsf{HaS}^{\mathsf{ph}}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H},\mathsf{E}]}(\mathcal{A}_{\mathsf{nma}^{\mathsf{m}}})$ holds.

Game G_4 (abort with the collision on key IDs): When a collision on the key IDs is detected, G_4 aborts and outputs 0. From the collision probability of uniformly chosen key IDs, $\left|\Pr\left[\mathsf{G}_3^{\mathcal{A}_{\mathsf{nma}^{\mathsf{m}}}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_4^{\mathcal{A}_{\mathsf{nma}^{\mathsf{m}}}} \Rightarrow 1\right]\right| \leq \frac{q_{\mathsf{key}}^2}{|\mathcal{U}|}$.

We use Lemma 2.2 to show a reduction from the M-INV of $\mathsf{T}_{\mathsf{wpsf}}$. The M-INV adversary $\mathcal{B}_{\mathsf{inv}^{\mathsf{m}}}$ given $\{(\mathsf{F}_j, y_j)\}_{j\in[q_{\mathsf{inst}}]}$ runs a two-stage algorithm S for $\mathcal{A}_{\mathsf{nma}^{\mathsf{m}}}$ playing G_4 and chooses the input θ for the algorithm from $\{y_j\}_{j\in[q_{\mathsf{inst}}]}$. To simulate G_4 without collision on key IDs, $\mathcal{B}_{\mathsf{inv}^{\mathsf{m}}}$ needs to prepare q_{key} verification keys with different key IDs. The expected number of instances $\mathbb{E}(q_{\mathsf{inst}})$ needed for obtaining q_{key} different key IDs is

$$\sum_{i=1}^{q_{\mathsf{key}}} \frac{|\mathcal{U}|}{|\mathcal{U}| - i + 1} \leq q_{\mathsf{key}}\left(\frac{|\mathcal{U}|}{|\mathcal{U}| - q_{\mathsf{key}} + 1}\right).$$

In the first stage, S_1 observes one of the quantum queries to H at random to obtain (u', r', m'). Since there is no collision on key IDs, $\mathcal{B}_{\mathsf{inv}^{\mathsf{m}}}$ can understand the target key of the observed random oracle query. If $u' = \mathsf{E}(\mathsf{F}_{j'})$, H is reprogrammed as $\mathsf{H}' := \mathsf{H}^{(u',r',m')\mapsto y_{j'}}$. In the second stage, S_2 runs $\mathcal{A}_{\mathsf{nma}^{\mathsf{m}}}$ with reprogrammed H' and outputs x' included in an output of $\mathcal{A}_{\mathsf{nma}^{\mathsf{m}}}^{|\mathsf{H}'\rangle}(\{\mathsf{F}_j\}_{j\in[q_{\mathsf{key}}]})$. From Lemma 2.2, we have the following bound:

$$\begin{aligned}
&\Pr\left[\mathsf{F}_{j'}(x') = y_{j'} : (j', m', r') \leftarrow \mathsf{S}_1^{\mathcal{A}_{\mathsf{nma}^{\mathsf{m}}}^{|\mathsf{H}\rangle}}(), x' \leftarrow \mathsf{S}_2^{\mathcal{A}_{\mathsf{nma}^{\mathsf{m}}}^{|\mathsf{H}'\rangle}}(y_{j'})\right] \\
\geq& \frac{1}{(2q_{\mathsf{qro}}+1)^2} \Pr\left[\mathsf{F}_{j^*}(x^*) = \mathsf{H}(\mathsf{E}(\mathsf{F}_{j^*}), r^*, m^*) : (j^*, m^*, r^*, x^*) \leftarrow \mathcal{A}_{\mathsf{nma}^{\mathsf{m}}}^{|\mathsf{H}\rangle}(\{\mathsf{F}_j\}_{j\in[q_{\mathsf{key}}]})\right] \\
=& \frac{1}{(2q_{\mathsf{qro}}+1)^2} \Pr\left[\mathsf{G}_4^{\mathcal{A}_{\mathsf{nma}^{\mathsf{m}}}} \Rightarrow 1\right]
\end{aligned}$$

Therefore, we have $\Pr\left[\mathsf{G}_4^{\mathcal{A}_{\mathsf{nma}^{\mathsf{m}}}} \Rightarrow 1\right] \leq (2q_{\mathsf{qro}}+1)^2 \mathrm{Adv}^{\text{M-INV}}_{\mathsf{T}_{\mathsf{wpsf}}}(\mathcal{B}_{\mathsf{inv}^{\mathsf{m}}})$.

We obtain Eq. (10) by combining the two reductions. □

B.2 Proof of Lemma 7.1

We extend the proof of Theorem 6.1 (Appendix B.1). We define G_5 in which verification keys $\{\mathsf{F}_j\}_{j\in[q_{\mathsf{key}}]}$ in G_4 are replaced with $\{\mathsf{L}_j \circ \mathsf{F} \circ \mathsf{R}_j\}$ for given $\mathsf{F}\colon \mathcal{X}' \to \mathcal{Y}$ generated by Gen'. The ST adversary $\mathcal{D}_{\mathsf{st}}$ can simulate $\mathsf{G}_4/\mathsf{G}_5$ by setting his challenges as verification keys. If $\mathcal{D}_{\mathsf{st}}$ plays ST_0, G_4 is simulated; otherwise, G_5 is simulated. Therefore, $\left|\Pr\left[\mathsf{G}_4^{\mathcal{A}_{\mathsf{nma^m}}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_5^{\mathcal{A}_{\mathsf{nma^m}}} \Rightarrow 1\right]\right| \leq \mathrm{Adv}^{\mathrm{ST}}_{\mathsf{T}_{\mathsf{wpsf}},\mathsf{T}'_{\mathsf{wpsf}}}(\mathcal{D}_{\mathsf{st}})$ holds.

To use Lemma 2.2, we assume that $\mathcal{B}_{\mathsf{inv}}$ runs a two-stage algorithm S in G_5 with input θ (see Fig. 8). As in Theorem 6.1, $\mathcal{B}_{\mathsf{inv}}$ can understand the target key of the observed random oracle query. When the observed value is targeted to j'-th verification key, $\mathcal{B}_{\mathsf{inv}}$ sets $\theta \coloneqq \mathsf{L}_{j'}(y)$ as the input to S. Since $\mathsf{L}_{j'}$ is bijective (first condition of Lemma 7.1), $\mathsf{L}_{j'}(y)$ for $y \leftarrow_{\$} \mathcal{Y}$ is statistically indistinguishable from random $y' \leftarrow_{\$} \mathcal{Y}$. When $\mathcal{B}_{\mathsf{inv^m}}$ submits x^* for F_{j^*} ($j^* = j'$), $\mathcal{B}_{\mathsf{inv}}$ outputs $\mathsf{R}_{j^*}(x^*)$. Suppose that $\mathsf{L}_{j^*}(\mathsf{F}(\mathsf{R}_{j^*}(x^*))) = \mathsf{L}_{j^*}(y)$ holds. Since L_{j^*} is a bijection, $\mathsf{F}(\mathsf{R}_{j^*}(x^*)) = y$. From the second condition of Lemma 7.1, $\mathsf{R}_{j^*}(x^*)$ is valid. Therefore, $\mathcal{B}_{\mathsf{inv}}$ can win the INV game by submitting $\mathsf{R}_{j^*}(x^*)$, and we have $\Pr\left[\mathsf{G}_5^{\mathcal{A}_{\mathsf{nma^m}}} \Rightarrow 1\right] \leq (2q_{\mathsf{qro}}+1)^2 \mathrm{Adv}^{\mathrm{INV}}_{\mathsf{T}'_{\mathsf{wpsf}}}(\mathcal{B}_{\mathsf{inv}})$ from Lemma 2.2, which proves this lemma.

□

B.3 Proof of Lemma 7.2

First, we show a reduction M-CR ⇒ M-sEUF-CMA extending the single-key version of [9, Theorem 2].

- Game G_0 (M-sEUF-CMA game): This is the original M-sEUF-CMA game and $\Pr\left[\mathsf{G}_0^{\mathcal{A}_{\mathsf{cma^m}}} \Rightarrow 1\right] = \mathrm{Adv}^{\text{M-sEUF-CMA}}_{\mathsf{HaS^{ph}}[\mathsf{T}_{\mathsf{psf}},\mathsf{H},\mathsf{E}]}(\mathcal{A}_{\mathsf{cma^m}})$ holds.
- Game G_1 (abort with collision on key IDs): When a collision of the key IDs is detected, G_1 aborts and outputs 0. We have $\left|\Pr\left[\mathsf{G}_0^{\mathcal{A}_{\mathsf{nma^m}}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_1^{\mathcal{A}_{\mathsf{nma^m}}} \Rightarrow 1\right]\right| \leq \frac{q_{\mathsf{key}}^2}{|\mathcal{U}|}$.
- Game G_2 (replacing H with H'): This game replaces H with H' satisfying

  $$\mathsf{H}'\left(\mathsf{E}\left(\mathsf{F}_j\right), r, m\right) = \mathsf{F}_j\left(\mathsf{DetSampDom}\left(\mathsf{F}_j, \widetilde{\mathsf{H}}\left(\mathsf{E}\left(\mathsf{F}_j\right), r, m\right)\right)\right),$$

  where $\mathsf{DetSampDom}$ is a deterministic function of $\mathsf{SampDom}$ and $\widetilde{\mathsf{H}}\colon \mathcal{U}\times\mathcal{R}\times\mathcal{M} \to \mathcal{W}$ is another random function to output randomness for $\mathsf{DetSampDom}$. From **Condition 1** of PSF, $\mathsf{F}_j(x)$ is uniform for $x \leftarrow \mathsf{SampDom}(\mathsf{F}_j)$. Since H and H' are statistically indistinguishable, $\Pr\left[\mathsf{G}_1^{\mathcal{A}_{\mathsf{nma^m}}} \Rightarrow 1\right] = \Pr\left[\mathsf{G}_2^{\mathcal{A}_{\mathsf{nma^m}}} \Rightarrow 1\right]$ holds.

The M-CR adversary $\mathcal{B}_{\mathsf{cr^m}}$ can simulate G_2. As in Theorem 6.1, the expected number of instances is at most $q_{\mathsf{key}}\left(\frac{|\mathcal{U}|}{|\mathcal{U}|-q_{\mathsf{key}}+1}\right)$ over all $(\mathsf{F},\mathsf{I}) \leftarrow \mathsf{Gen}(1^\lambda)$. From **Conditions 2** and **3**, the M-CR adversary $\mathcal{B}_{\mathsf{cr^m}}$ can simulate the signing oracle. In answering the i-th signing query m_i for the j-th verification key F_j, he returns

(r_i, x_i), where $r_i \leftarrow_\$ \mathcal{R}$ and $x_i \coloneqq \mathsf{DetSampDom}\left(\mathsf{F}_j, \widetilde{\mathsf{H}}\left(\mathsf{E}\left(\mathsf{F}_j\right), r_i, m_i\right)\right)$. If the M-sEUF-CMA adversary $\mathcal{A}_{\mathsf{cma}^\mathsf{m}}$ wins by (j^*, m^*, r^*, x^*), $\mathsf{F}_{j^*}(x^*) = \mathsf{F}_{j^*}(x')$ holds, where $x' = \mathsf{DetSampDom}(\mathsf{F}_{j^*}, \widetilde{\mathsf{H}}(\mathsf{E}(\mathsf{F}_{j^*}), r^*, m^*)))$. From **Condition 4**, $x^* \neq x'$ holds with probability $1 - 2^{-\omega(\log n)}$, and we have

$$\mathrm{Adv}^{\text{M-sEUF-CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \leq \frac{1}{1 - 2^{-\omega(\log n)}} \mathrm{Adv}^{\text{M-CR}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{B}_{\mathsf{cr}^\mathsf{m}}) + \frac{q_{\mathsf{key}}^2}{|\mathcal{U}|}.$$

Next, we show CR $\Rightarrow$ M-CR.

Game G_3 (M-CR game): This is the original M-CR game and $\Pr\left[\mathsf{G}_3^{\mathcal{B}_{\mathsf{cr}^\mathsf{m}}} \Rightarrow 1\right] = \mathrm{Adv}^{\text{M-CR}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{B}_{\mathsf{cr}^\mathsf{m}})$ holds.

Game G_4 (replacing verification keys): We replace F_j with $\mathsf{L}_j \circ \mathsf{F} \circ \mathsf{R}_j$. Since the ST adversary can simulate $\mathsf{G}_3/\mathsf{G}_4$, we have $\left|\Pr\left[\mathsf{G}_3^{\mathcal{B}_{\mathsf{cr}^\mathsf{m}}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_4^{\mathcal{B}_{\mathsf{cr}^\mathsf{m}}} \Rightarrow 1\right]\right| \leq \mathrm{Adv}^{\text{ST}}_{\mathsf{T}_{\mathsf{psf}},\mathsf{T}'_{\mathsf{psf}}}(\mathcal{D}_{\mathsf{st}})$.

The CR adversary $\mathcal{B}_{\mathsf{cr}}$ simulates G_4 as follows: Given F, $\mathcal{B}_{\mathsf{cr}}$ gives $\{\mathsf{L}_j \circ \mathsf{F} \circ \mathsf{R}_j\}_{j\in[q_{\mathsf{key}}]}$ to $\mathcal{B}_{\mathsf{cr}^\mathsf{m}}$. When $\mathcal{B}_{\mathsf{cr}^\mathsf{m}}$ submits (x_1^*, x_2^*) for F_{j^*}, $\mathcal{B}_{\mathsf{cr}}$ outputs $(\mathsf{R}_{j^*}(x_1^*), \mathsf{R}_{j^*}(x_2^*))$. Suppose that $\mathsf{L}_{j^*}(\mathsf{F}(\mathsf{R}_{j^*}(x_1^*))) = \mathsf{L}_{j^*}(\mathsf{F}(\mathsf{R}_{j^*}(x_2^*)))$ holds. Since L_j is injective, $\mathsf{F}(\mathsf{R}_{j^*}(x_1^*)) = \mathsf{F}(\mathsf{R}_{j^*}(x_2^*))$ holds. From the second condition of Lemma 7.2, $\mathsf{R}_{j^*}(x_1^*)$ and $\mathsf{R}_{j^*}(x_2^*)$ are valid. Moreover, we have $\mathsf{R}_{j^*}(x_1^*) \neq \mathsf{R}_{j^*}(x_2^*)$ if $x_1^* \neq x_2^*$ since R_j is also injective. Therefore, $\mathcal{B}_{\mathsf{cr}}$ can win the CR game, and he can perfectly simulate G_4. Therefore, we have

$$\mathrm{Adv}^{\text{M-CR}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{B}_{\mathsf{cr}^\mathsf{m}}) \leq \mathrm{Adv}^{\text{CR}}_{\mathsf{T}'_{\mathsf{psf}}}(\mathcal{B}_{\mathsf{cr}}) + \mathrm{Adv}^{\text{ST}}_{\mathsf{T}_{\mathsf{psf}},\mathsf{T}'_{\mathsf{psf}}}(\mathcal{D}_{\mathsf{st}}).$$

Combination of the reductions M-CR $\Rightarrow$ M-EUF-CMA and CR $\Rightarrow$ M-CR yields Lemma 7.2. □

C Use Cases of Generic Method

We show use cases of Lemma 7.2 in lattice-based cryptography and Lemma 7.1 in code-based and MQ-based cryptography. In this paper, we apply the generic method to frameworks of the schemes (e.g., GPV framework [22]) instead of specific schemes (e.g., FALCON [41]). We will study the applicability to the specific schemes in future works.

Lattice-based Cryptography: We apply the generic method to the GPV framework (see Appendix A.1) [22]. For Lemma 7.2, we design simulation of verification keys by $\{L_j A R_j\}_{j\in[q_{\mathsf{key}}]}$ where L_j is an $n \times n$ invertible matrix over $\mathbb{F}_q$ and R_j is an $m \times m$ signed permutation matrix. Note that we require the orthogonality of R_j for $\|x\| = \|x R_j^T\|$ and any integer orthogonal matrices are signed permutation matrices whose non-zero entries are ± 1. Then, the ST advantage $\mathrm{Adv}^{\text{ST}}_{\mathsf{T},\mathsf{T}'}(\mathcal{D}_{\mathsf{st}})$ is bounded by an advantage of the following problem.

Definition C.1 (Multi-instance Signed Permutation Equivalence (M-SPE)). *Given matrices $G \in \mathbb{F}_q^{n\times m}$ and $\{G_j\}_{j\in[q_{\mathsf{inst}}]}$ ($G_j \in \mathbb{F}_q^{n\times m}$), do there exist $n \times n$ invertible matrices $\{L_j\}_{j\in[q_{\mathsf{inst}}]}$ over $\mathbb{F}_q$ and $m \times m$ signed permutation matrices $\{R_j\}_{j\in[q_{\mathsf{inst}}]}$ over $\mathbb{F}_q$ such that $G_j = L_j G R_j$?*

This problem is a variant of the well-studied problem called *code equivalence* in code-based cryptography [40]. The code equivalence is defined as: Given a pair of generator matrices (G, G'), do there exist an invertible matrix L and an isometric matrix R such that $G' = LGR$? There are variations of this problem in terms of R. When R is a permutation matrix (resp., generalized permutation matrix), this problem is called *permutation equivalence* (resp., *linear equivalence*)[45].

In lattice-based cryptography, there is a closely related problem called *lattice isomorphism*, that is, given a pair of lattice bases (B, B'), do there exist a unimodular matrix L and an orthogonal matrix R such that $B' = LBR$? The conditions on L and R are required to keep the geometry of lattices; however, it is not necessary for our purpose.

Any variants of the code equivalence listed above are in the complexity class coAM and not conjectured to be NP-hard [40]. Also, there are some algorithms for the code equivalence [30, 44, 4]. It is necessary to confirm that existing algorithms cannot efficiently solve the target instance of M-SPE.

Code-based Cryptography: We apply the generic method to a TDF using a parity-check matrix $H \in \mathbb{F}_q^{n\times m}$ as in the modified CFS signature and Wave (see Appendices A.2 and A.3). For Lemma 7.1, we simulate verification keys by $\{L_j H R_j\}_{j\in[q_{\mathsf{key}}]}$, where L_j is an $m \times m$ invertible matrix over $\mathbb{F}_q$ and R_j is an $n \times n$ generalized permutation matrix over $\mathbb{F}_q$. Note that generalized permutation matrices preserve the Hamming weights of vectors. Then, the ST advantage $\mathrm{Adv}^{\mathrm{ST}}_{\mathsf{T},\mathsf{T}'}(\mathcal{D}_{\mathsf{st}})$ is bounded by an advantage of the following problem.

Definition C.2 (Multi-instance Linear Equivalence (M-LE)). *Given generator matrices $G \in \mathbb{F}_q^{n\times m}$ and $\{G_j\}_{j\in[q_{\mathsf{inst}}]}$ ($G_j \in \mathbb{F}_q^{n\times m}$), do there exist $n \times n$ invertible matrices $\{L_j\}_{j\in[q_{\mathsf{inst}}]}$ over $\mathbb{F}_q$ and $m \times m$ generalized permutation matrices $\{R_j\}_{j\in[q_{\mathsf{inst}}]}$ over $\mathbb{F}_q$ such that $G_j = L_j G R_j$?*

As with the M-SPE (Definition C.1), it is necessary to confirm that existing algorithms cannot efficiently solve the target instance of M-LE.

Multivariate-quadratic-based Cryptography: We assume a TDF of the modified UOV signature or the modified HFE signature. Let $\mathsf{F}\colon \mathbb{F}_q^{n'} \to \mathbb{F}_q^m$ and $\mathsf{F}_j\colon \mathbb{F}_q^n \to \mathbb{F}_q^m$ be functions composed of multivariate quadratic polynomials ($n' \geq n$). For Lemma 7.1, we simulate verification keys by $\{\mathsf{L}_j \circ \mathsf{F} \circ \mathsf{R}_j\}_{j\in[q_{\mathsf{key}}]}$, where L_j is an invertible affine map over $\mathbb{F}_q$ and R_j is an affine map over $\mathbb{F}_q$. Then, the ST advantage $\mathrm{Adv}^{\mathrm{ST}}_{\mathsf{T},\mathsf{T}'}(\mathcal{D}_{\mathsf{st}})$ is bounded by an advantage of the following game.

Definition C.3 (Multi-instance Decision Morphism of Polynomials (M-DMP)). *Given functions composed of quadratic polynomials F and $\{\mathsf{F}_j\}_{j\in[q_{\mathsf{inst}}]}$, do there exist affine maps $\{\mathsf{L}_j\}_{j\in[q_{\mathsf{inst}}]}$ and $\{\mathsf{R}_j\}_{j\in[q_{\mathsf{inst}}]}$ over $\mathbb{F}_q$ such that $\mathsf{F}_j = \mathsf{L}_j \circ \mathsf{F} \circ \mathsf{R}_j$?*

The (single-instance) decision morphism of polynomials is proven NP-complete if a general case that both L and R are arbitrary affine maps [39]. If L and R are invertible affine maps, this problem is called *decision isomorphism of polynomials* that is in the complexity class coAM and not conjectured to be NP-hard [39]. Therefore, we recommend using non-invertible affine maps; however, further study of the M-DMP is needed since it has not yet been well studied.