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] Technology Innovation Institute, keita.xagawa@tii.ae

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 currently 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 assumption 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. Additionally, we extend the proof into the multi-key setting and propose a generic method that provides security reduction without any security loss in the number of keys.
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 since it supports non-repudiation and authentication; if a document is signed, the signer indeed signed it and cannot repudiate the signature. The standard security notion of the digital signature is existential unforgeability against chosen-message attack (EUF-CMA) [30]. Roughly speaking, a signature scheme is said to be EUF-CMA-secure if no efficient adversary can forge a signature even if the adversary can access to a signing oracle, which captures non-repudiation and authentication. Hash-and-sign [4, 5] is a widely adopted paradigm for constructing practical signatures, along with Fiat-Shamir [27], in the ROM [4]. This paper focuses on hash-and-sign.

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 a full-domain hash using a trapdoor permutation (TDP-FDH) such as RSA. TDP-FDH is EUF-CMA-secure in the ROM, assuming the one-wayness (OW) or non-invertibility (INV) of TDP [4].[3] Gentry, Peikert, and Vaikuntanathan proposed FDH and probabilistic FDH (PFDH) signatures with a preimage-sampleable function (PSF) [29], 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 hard to build PSFs in code-based and multivariate-quadratic-based (MQ-based) cryptography; for example, F is not a surjection. In this case, the trapdoor I fails to invert y whose preimage does not exist. For such TDFs, we employ the 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 [18] in code-based cryptography and the Unbalanced Oil and Vinegar (UOV) [37] and Hidden Field Equations (HFE) signatures [46] in MQ-based cryptography use this paradigm.

Hash-and-Sign Signature in 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 [53], and interest has been growing in post-quantum cryptography (PQC). Recently NIST selected PQC candidates of public-key encryption/key-encapsulation mechanism (KEM) and digital signature for standardization [45] and started additional call for PQC digital signatures [44]. In the context of PQC, it is essential for signature schemes to provide EUF-CMA security in the QROM (Quantum Random Oracle Model) [13] since it models real-world quantum adversaries with *offline* access to the hash function. Unfortunately, schemes that are secure in the ROM are not always secure in the QROM, as demonstrated by separation results, including a signature scheme, by Yamakawa and Zhandry [57].

Table 1 summarizes studies on the EUF-CMA security of hash-and-sign signatures in the QROM. Boneh et al. [13] showed a tight reduction from the CR of PSF using the history-free reduction. Zhandry [59] gave a reduction from

[3] An adversary tries to find a preimage of a challenge y that is uniformly chosen in the INV game [32] and that derived by $\mathsf{F}(x)$ for x chosen from some distribution on $\mathcal{X}$ in the OW game [4].

Table 1: Summary of the security proofs for hash-and-sign in the QROM. DHaS, PHaS, and PHaSwR denote 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. q denotes the number of queries to the signing oracle or random oracle.

Name	DHaS	PHaS	PHaSwR	Assumption	Security Bound
[13]	✓	✓	–	CR	$O(\epsilon_{\mathsf{cr}})$
[59]	✓	✓	–	OW/INV	$O(q^2\sqrt{\epsilon_{\mathsf{ow/inv}}})$
ext. of [56]	✓	✓	–	OW/INV	$O(q^4\epsilon_{\mathsf{ow/inv}})$
[16]	–	✓	–	EUF-NMA	$O(\epsilon_{\mathsf{nma}})$
Ours	-	✓	✓	INV	$O(q^2\epsilon_{\mathsf{inv}})$

the OW/INV[4], using a technique called semi-constant distribution.[5] Unfortunately, the semi-constant distribution technique incurs a square-root loss in the success probability. Yamakawa and Zhandry [56] 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 [56], we obtain a reduction from the OW/INV of PSF. Chailloux and Debris-Alazard [16] gave a security proof of the probabilistic hash-and-sign based on non-PSF TDFs. Also, Grilo, Hövelmanns, Hülsing, and Majenz [31] 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.

Based on the summary of previous studies, there are currently *no* security proofs for the probabilistic hash-and-sign with retry in the QROM, which has an impact on the security evaluation of code-based and MQ-based signatures for upcoming additional PQC standardization. Our central question is:

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

Provable Security in 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

[4] For PSFs, a tight reduction from OW to INV and one from INV to OW hold.

[5] Zhandry [59] 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.

[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).

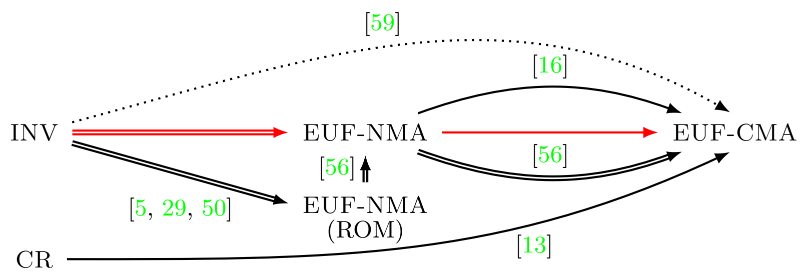

Fig. 1: A diagram illustrating reductions of hash-and-sign in the QROM. Red arrows represent our results, while solid, double, and dashed arrows represent tight reductions, reductions with linear or quadratic loss, and non-tight reductions.

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 [43] of the PQC standardization project. We can ensure resistance against multi-key attacks if there is no security loss in the number of keys. Thus, our additional question is:

Q2. Is there an M-EUF-CMA *security proof for hash-and-sign without any security loss in the number of keys*

The technique of including an entire verification key in the hash computation is known as *key prefixing*, which enables one to separate the domain of the hash function for each verification key. Schnorr signature adopts key prefixing to show a tight reduction in the multi-key setting [41]. Similarly, Duman et al. [25] proposed a technique called *prefix hashing* for the Fujisaki-Okamoto transform of KEM. Prefix hashing is a technique in which the hash function includes only a small unpredictable portion of a verification key, resulting in a smaller increase in execution time compared to key prefixing.

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*). Additionally, the main theorem applies to the probabilistic hash-and-sign *without retry*. Furthermore, 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 the probabilistic hash-and-sign without retry only [59, 16, 56]. Fig. 1 shows a diagram of the reduction. The main theorem comprises two reductions; EUF-NMA $\Rightarrow$ EUF-CMA and INV $\Rightarrow$ EUF-NMA, where X $\Rightarrow$ Y inidicates a reduction from X to Y. The main theorem has a security bound $(2q_{\mathsf{qro}}+1)^2\epsilon_{\mathsf{inv}}$, where q_{qro} is a bound on the number of random oracle queries and ϵ_{inv} is an advantage of the INV game.

Proof Idea: We provide a technical overview of our main theorem: To prove EUF-NMA $\Rightarrow$ EUF-CMA, we first reprogram the quantum random oracle in the signing procedure and, then, simulate the signing oracle. We can employ the tight adaptive reprogramming technique in [31] and reprogram the random oracle in the signing procedure. At first sight, this technique seems directly allow for the simulation of the signing oracle in the absence of a signing key. However, the direct application causes a subtle bias in the distribution of the reprogrammed quantum random oracle in *retries*; thus, we need to cancel the reprogramming performed during retries. Unfortunately, this cancelation also introduces a bias in the distribution of the quantum random oracle. We carefully treat the bias caused by this cancelation using the semi-classical O2H (One-way to Hiding) technique [1]. After this cancelation, we can simulate the signing oracle without the signing key.

For INV $\Rightarrow$ EUF-NMA, we use the measure-and-reprogram technique developed by Don et al. [23]. As far as we know, this usage is new in the context of the probabilistic hash-and-sign. We also note that this usage induces the security loss $(2q_{\mathsf{qro}}+1)^2$.

Applications: Applying the main theorem, we enhance the EUF-CMA security of Wave [20] and give the first proof for the sEUF-CMA security of the modified CFS signature [19] as well as the EUF-CMA security of Rainbow [22], GeMSS [15], MAYO [9], and QR-UOV [28] in the QROM. To the best of our knowledge, the main theorem encompasses all existing post-quantum hash-and-sign signatures such that reductions from the INV are known in the ROM.

NIST has announced an additional call for proposals of the post-quantum signature with short signatures and fast verification [44]. 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 in the QROM.

Security Proof in Multi-Key Setting: We extend the main theorem to the multi-key setting and propose a generic method for establishing a reduction from the security of TDFs in the single-instance setting to the security of the hash-and-sign with prefix hashing in the multi-key setting. The idea behind the generic method is to apply some pairs of randomly generated transformations $\{\mathsf{L}_j, \mathsf{R}_j\}_j$ to a single verification key F' of another TDF that is assumed to be non-invertible, which simulates multiple verification keys by $\{\mathsf{L}_j \circ \mathsf{F}' \circ \mathsf{R}_j\}_j$. Assuming the indistinguishability between $\{\mathsf{L}_j \circ \mathsf{F}' \circ \mathsf{R}_j\}_j$ and real verification keys $\{\mathsf{F}_j\}_j$, we show a reduction of INV $\Rightarrow$ M-EUF-CMA with a security bound $(2q_{\mathsf{qro}}+1)^2\epsilon_{\mathsf{inv}}$ and a tight reduction of CR $\Rightarrow$ M-sEUF-CMA. Since there is no security loss in the number of keys, we can affirmatively answer Q2. Furthermore, we apply the generic method to some hash-and-sign signatures. In these applications, we introduce computational problems that can ensure the indistinguishability between $\{\mathsf{L}_j \circ \mathsf{F} \circ \mathsf{R}_j\}_j$ and $\{\mathsf{F}_j\}_j$.

Organization: Section 2 gives notations, definitions, and so on. Section 3 presents our main theorem and discusses applications. In Section 4, we describe the generic method applied in the multi-key setting. Appendix A gives proof techniques in the QROM. Appendix B reviews the existing security proofs in the (Q)ROM. Appendices C and D show missing proofs for the main theorem and its strong version. Appendix E presents security proofs of hash-and-sign signatures reviewed in Appendix F. Appendix G shows reductions from multi-instance INV and CR (M-INV and M-CR) to M-EUF-CMA and M-sEUF-CMA. Appendices H and I show missing proofs for the theorem in the multi-key setting and its strong version. Appendix J shows applications of the generic method in the multi-key setting.

Concurrent Work: Liu, Jiang, and Zhao [39] 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. [23]. Their security bound 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 hash-and-sign. First, our main theorem applies to the TDP-PFDH and has wider applications in existing signature schemes. Although no post-quantum signatures adopting TDP-FDH/TDP-PFDH have been proposed, numerous post-quantum signatures adopt the probabilistic hash-and-sign with retry. Second, our main theorem has the security bound $(2q_{\mathsf{qro}} + 1)^2 \epsilon_{\mathsf{inv}}$ that is not including q_{sign}.

Two papers [21, 2] recently pointed out a subtle flaw in the security proofs of Fiat-Shamir with Aborts in the QROM [35, 31]. The flaw stems from the bias introduced by the simulation with abort, which we treat in EUF-NMA $\Rightarrow$ EUF-CMA carefully. We note that the games in the corrected proof in [2] are defined in the same spirit as our proof of EUF-NMA $\Rightarrow$ EUF-CMA while the proof techniques and the details are different.

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 $\mathcal{X}$). We denote a set of functions having a domain $\mathcal{X}$ and a range $\mathcal{Y}$ by $\mathcal{Y}^{\mathcal{X}}$.

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

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

$y := \mathcal{A}^{\mathsf{H}}(x)$. 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 $\perp$. A binary operation $a \stackrel{?}{=} b$ outputs $\top$ if $a = b$ and outputs $\perp$ otherwise.

2.2 Digital Signature and Trapdoor Function

Definition 2.1 (Digital Signature). *A digital signature scheme* Sig *consists of three algorithms:*

- $\mathsf{Sig.KeyGen}(1^\lambda)$*: 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* $\perp$ *(rejection).*

Definition 2.2 (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* $\mathrm{Adv}_{\mathsf{Sig}}^{\text{EUF-CMA}}(\mathcal{A}_{\mathsf{cma}}) = \Pr\big[\mathsf{EUF\text{-}CMA}^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\big]$ *and* $\mathrm{Adv}_{\mathsf{Sig}}^{\text{EUF-NMA}}(\mathcal{A}_{\mathsf{nma}}) = \Pr\big[\mathsf{EUF\text{-}NMA}^{\mathcal{A}_{\mathsf{nma}}} \Rightarrow 1\big]$*, respectively. Also, we define an advantage function for an* sEUF-CMA *(strong* EUF-CMA*) game as* $\mathrm{Adv}_{\mathsf{Sig}}^{\text{sEUF-CMA}}(\mathcal{A}_{\mathsf{cma}}) = \Pr\big[\mathsf{sEUF\text{-}CMA}^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\big]$*, 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.*

Definition 2.3 (Trapdoor Function (TDF)). *A 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*.*

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

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

$\mathsf{F}(x)$: *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 2.4 (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* $\mathrm{Adv}_{\mathsf{T}}^{\mathrm{INV}}(\mathcal{B}_{\mathsf{inv}}) = \Pr\left[\mathsf{INV}^{\mathcal{B}_{\mathsf{inv}}} \Rightarrow 1\right]$, $\mathrm{Adv}_{\mathsf{T}}^{\mathrm{OW}}(\mathcal{B}_{\mathsf{ow}}) = \Pr\left[\mathsf{OW}^{\mathcal{B}_{\mathsf{ow}}} \Rightarrow 1\right]$, *and* $\mathrm{Adv}_{\mathsf{T}}^{\mathrm{CR}}(\mathcal{B}_{\mathsf{cr}}) = \Pr\left[\mathsf{CR}^{\mathcal{B}_{\mathsf{cr}}} \Rightarrow 1\right]$, *respectively.*

2.3 Preimage-Sampleable Function

In the ROM, hash-and-sign is EUF-CMA-secure when instantiated with a preimage-sampleable function (PSF) [29]. We first define its weakened version.

Definition 2.5 (Weak Preimage-Sampleable Function (WPSF)). *A WPSF* T *is a TDF that is equipped with an additional function* $\mathsf{SampDom}(\mathsf{F})$, *which takes as input* $\mathsf{F} \in \mathcal{Y}^{\mathcal{X}}$ *and outputs some* $x \in \mathcal{X}$.

We then review PSF:

Definition 2.6 (Preimage-Sampleable Function (PSF) [29]). *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* $y \in \mathcal{Y}$.

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* $\omega(\log(\lambda))$.

In the proof of EUF-CMA security, a TDF may not be a PSF, but it must be a WPSF that satisfies a relaxed version of **Condition 2** that ensures indistinguishability between $x \leftarrow \mathsf{SampDom}(\mathsf{F})$ and $x \leftarrow \mathsf{I}(y)$. To define this relaxed condition, we introduce the following game:

[7] In general, *non-invertibility* of TDFs is called *one-wayness* [29, 50, 16]. We make a distinction between them depending on the way to choose challenges (INV follows [32] and OW follows [4]).

Game: PS_b

$(\mathsf{F}, \mathsf{I}) \leftarrow \mathsf{Gen}(1^\lambda)$
$b^* \leftarrow \mathcal{D}_{\mathsf{ps}}^{\mathsf{Sample}_b}(\mathsf{F})$
return b^*

$\mathsf{Sample}_0()$

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

$\mathsf{Sample}_1()$

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

Fig. 4: PS (Preimage Sampling) game

Game: M-EUF-CMA

1 $\mathcal{Q} := \emptyset$
2 **for** $j \in [q_{\mathsf{key}}]$ **do**
3   $(vk_j, sk_j) \leftarrow \mathsf{Sig.KeyGen}(1^\lambda)$
4 $(j^*, m^*, \sigma^*) \leftarrow \mathcal{A}_{\mathsf{cma^m}}^{\mathsf{Sign}}(\{vk_j\}_{j \in [q_{\mathsf{key}}]})$
5 **if** $(j^*, m^*) \in \mathcal{Q}$ **then**
6   **return** 0
7 **return** $\mathsf{Sig.Verify}(vk_{j^*}, m^*, \sigma^*)$

$\mathsf{Sign}(j, m_i)$

1 $\sigma_i \leftarrow \mathsf{Sig.Sign}(sk_j, m_i)$
2 $\mathcal{Q} := \mathcal{Q} \cup \{(j, m_i)\}$
3 **return** σ_i

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

Definition 2.7 (Preimage Sampling (PS) 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.

2.4 Security Games in Multi-key/Multi-instance Settings

Definition 2.8 (Security of Signature in Multi-key Setting [36]). *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* $\mathrm{Adv}_{\mathsf{Sig}}^{\text{M-EUF-CMA}}(\mathcal{A}_{\mathsf{cma^m}}) = \Pr\left[\mathsf{M\text{-}EUF\text{-}CMA}^{\mathcal{A}_{\mathsf{cma^m}}} \Rightarrow 1\right]$ *and* $\mathrm{Adv}_{\mathsf{Sig}}^{\text{M-sEUF-CMA}}(\mathcal{A}_{\mathsf{cma^m}}) = \Pr\left[\mathsf{M\text{-}sEUF\text{-}CMA}^{\mathcal{A}_{\mathsf{cma^m}}} \Rightarrow 1\right]$, *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 2.9 (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* $\mathrm{Adv}_{\mathsf{T}}^{\text{M-INV}}(\mathcal{B}_{\mathsf{inv^m}}) = \Pr\left[\mathsf{M\text{-}INV}^{\mathcal{B}_{\mathsf{inv^m}}} \Rightarrow 1\right]$, $\mathrm{Adv}_{\mathsf{T}}^{\text{M-CR}}(\mathcal{B}_{\mathsf{cr^m}}) = \Pr\left[\mathsf{M\text{-}CR}^{\mathcal{B}_{\mathsf{cr^m}}} \Rightarrow 1\right]$, *and* $\mathrm{Adv}_{\mathsf{T}}^{\text{M-PS}}(\mathcal{D}_{\mathsf{ps^m}}) = \left|\Pr\left[\mathsf{M\text{-}PS}_0^{\mathcal{D}_{\mathsf{ps^m}}} \Rightarrow 1\right] - \Pr\left[\mathsf{M\text{-}PS}_1^{\mathcal{D}_{\mathsf{ps^m}}} \Rightarrow 1\right]\right|$, *respectively.*

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

2.5 Quantum Random Oracle Model

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 the adversary makes queries to the random oracle (*random oracle queries*) to compute the hash values. In the ROM, the challenger can choose $y \leftarrow_\$ \mathcal{Y}$ and reprogram $\mathsf{H} \coloneqq \mathsf{H}^{(r,m)\mapsto y}$ 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, $\sum_{(r,m)} \alpha_{r,m} |r, m\rangle |y \oplus \mathsf{H}(r, m)\rangle$. Due to the nature of superposition queries in the QROM, traditional proof techniques like lazy sampling used in the ROM cannot be directly applied in the QROM. However, some works enable one to adaptively reprogram H in the security game [55, 33, 23, 31]. Among the works, we use the tight adaptive reprogramming technique [31] and the measure-and-reprogram technique [23]. Also, we use the semi-classical O2H technique [1]. See Appendix A.

2.6 Hash-and-Sign Paradigm

Fig. 7 shows algorithms of the probabilistic hash-and-sign with retry, and $\mathsf{HaS}[\mathsf{T}, \mathsf{H}]$ is 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 empty, $\mathsf{HaS}[\mathsf{T}, \mathsf{H}]$ instantiates the deterministic hash-and-sign. In Appendix B, we present the existing security proofs for hash-and-sign.

3 New Security Proof

The main theorem is as follows:

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

$(\mathsf{F},\mathsf{I}) \leftarrow \mathsf{Gen}(1^\lambda)$
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. 7: Algorithms of the probabilistic hash-and-sign with retry

Theorem 3.1 (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 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 $\mathsf{T}_{\mathsf{wpsf}}$ and a* PS *adversary $\mathcal{D}_{\mathsf{ps}}$ of $\mathsf{T}_{\mathsf{wpsf}}$ issuing q_{sign} sampling queries such that*

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

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 $\mathcal{A}_{\mathsf{cma}}$.

In this section, we provide a proof sketch, while Appendix C contains the complete proof.

Proof Sketch: The main theorem consists of two reductions: EUF-NMA $\Rightarrow$ EUF-CMA and INV $\Rightarrow$ EUF-NMA. To establish EUF-NMA $\Rightarrow$ EUF-CMA, we modify the signing oracle to enable simulation by $\mathsf{SampDom}$ without using the signing key. We employ the tight adaptive reprogramming technique [31] (see Appendix A.1) to modify the signing oracle. This modification involves sampling $r \leftarrow_\$ \mathcal{R}$ and $y \leftarrow_\$ \mathcal{Y}$, and reprogramming H as $\mathsf{H}^{(r,m)\mapsto y}$ every time the signing oracle calls H. If we can reprogram H by $\mathsf{H}^{(r,m)\mapsto \mathsf{F}(x)}$ where $x \leftarrow \mathsf{SampDom}(\mathsf{F})$, (r, x) becomes a valid signature for the reprogrammed H. However, $\mathsf{F}(x)$ is not necessarily a uniform distribution, which introduces bias to the distribution of H after reprogramming. If we can cancel the reprogramming performed during retries, we can simulate the signing oracle with outputting (r, x) and reprogramming $\mathsf{H} := \mathsf{H}^{(r,m)\mapsto \mathsf{F}(x)}$ assuming the hardness of the PS game (see Definition 2.7). Such cancellation is a non-trivial task. Reapplying the tight adaptive reprogramming technique cannot achieve cancellation without introducing the distribution bias. To achieve this goal, we use the semi-classical O2H technique [1] (see Appendix A.3). By puncturing H for reprogrammed points during retries, we prevent the adversary from obtaining the values associated with those points. As a result, the reprogramming during retries can be canceled because it does not affect the adversary's advantage. This cancellation enables the EUF-NMA adversary to simulate the signing oracle, which completes the reduction.

For INV $\Rightarrow$ EUF-NMA, we utilize the measure-and-reprogram technique [23]. The INV adversary $\mathcal{B}_{\mathsf{inv}}$ is given a challenge (F, y) and interacts with $\mathcal{A}_{\mathsf{nma}}$ in the EUF-NMA game. $\mathcal{B}_{\mathsf{inv}}$ measures and reprograms the random function H accessed by $\mathcal{A}_{\mathsf{nma}}$. $\mathcal{B}_{\mathsf{inv}}$ measures one of the random oracle queries made by $\mathcal{A}_{\mathsf{nma}}$. Let (r', m') denote the observed value, and H is reprogrammed as $\mathsf{H}' = \mathsf{H}^{(r',m') \mapsto y}$. Then, $\mathcal{B}_{\mathsf{inv}}$ runs $\mathcal{A}_{\mathsf{nma}}$ again with H' and obtains (m, r, x). Finally, $\mathcal{B}_{\mathsf{inv}}$ outputs x as a preimage of y. From [23, Theorem 2] (see Appendix A.2), we can achieve a reduction with a security loss of $(2q_{\mathsf{qro}} + 1)^2$ in INV $\Rightarrow$ EUF-NMA. $\square$

Remark 3.1. If $\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}}, \mathsf{H}]$ adopts the probabilistic hash-and-sign, then $q'_{\mathsf{sign}} = q_{\mathsf{sign}}$ holds and the last term of Eq. (1) becomes 0.

Remark 3.2. We have a tight reduction in EUF-NMA $\Rightarrow$ EUF-CMA.

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

Compared with the security bound of [16] (see Eq. (4) in Appendix B), the requirement for $\mathsf{T}_{\mathsf{wpsf}}$ is weaker, and there are no square-root terms related to **Condition 2**.

Remark 3.3. If the underlying TDF is PSF (or TDP), $\mathrm{Adv}^{\text{EUF-CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \leq (2q_{\mathsf{qro}}+1)^2\mathrm{Adv}^{\mathrm{INV}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{B}_{\mathsf{inv}}) + \frac{3}{2}q_{\mathsf{sign}}\sqrt{\frac{q_{\mathsf{sign}}+q_{\mathsf{qro}}+1}{|\mathcal{R}|}}$. 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 equivalent from **Condition 2** and $\mathrm{Adv}^{\mathrm{PS}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{D}_{\mathsf{ps}}) = 0$. This bound is tighter than existing ones for $\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}}, \mathsf{H}]$.

Remark 3.4. 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) [31, Theorem 3]. Also, Don et al. gave a generic reduction in the Fiat-Shamir transform of arbitrary ID schemes with a security loss $(2q_{\mathsf{qro}}+1)^2$ [24, Theorem 8]. The above reductions use the same techniques of adaptive reprogramming in the QROM (Lemmas A.1 and A.2) as used in Theorem 3.1. However, the unique aspect of Theorem 3.1 lies in the combination of the semi-classical O2H technique with these two techniques.

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' all at once, requiring statistical indistinguishability between H and H'. On the other hand, our proof reprograms H in each signing query. This approach allows us to bound the advantage gap of games in the reduction using $\mathrm{Adv}^{\mathrm{PS}}_{\mathsf{T}_{\mathsf{wpsf}}}(\mathcal{B}_{\mathsf{ps}})$.

Advantage 2: Tighter proof: Our reduction is tighter than the existing ones [59, 56] as mentioned in Remark 3.3. While we cannot guarantee the optimality of our reduction, we can infer from several observations that a multiplicative loss of $(2q_{\mathsf{qro}}+1)^2$ appears to be unavoidable in the generic (black-box) reduction. First, the reduction incurs the loss $(q_{\mathsf{sign}}+q_{\mathsf{qro}}+1)$ even in the ROM (see Appendix B). Second, the security loss of a generic reduction from ROM to QROM using the lifting theorem [56] 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 3.4.

3.1 Extension to sEUF-CMA Security

If F of the underlying TDF is injective, $\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H}]$ is sEUF-CMA secure (see the proof in Appendix D).

Corollary 3.1 (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 $\mathcal{B}_{\mathsf{inv}}$ of $\mathsf{T}_{\mathsf{wpsf}}$ and a* PS *adversary $\mathcal{D}_{\mathsf{ps}}$ of $\mathsf{T}_{\mathsf{wpsf}}$ issuing q_{sign} sampling queries such that*

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

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 $\mathcal{A}_{\mathsf{cma}}$.

3.2 Applications of New Security Proof

By applying Theorem 3.1, we can establish security proofs for Wave [20], the original/modified UOV signatures [37, 50], the modified HFE signature [50], and MAYO [9]. Additionally, by utilizing Corollary 3.1, we can provide a security proof for the modified CFS signature [19]. If Rainbow [22] and QR-UOV [28] make the same modification as the modified UOV signature, these schemes can be provably secure. Also, GeMSS [15] is provable secure since it follows the modified HFE signature. The security proofs for these schemes, obtained by applying Theorem 3.1 and Corollary 3.1, are provided in Appendix E.

4 Security Proof of Hash-and-Sign with Prefix Hashing in Multi-key Setting

In prefix hashing, the hash function H includes a small unpredictable portion of the verification key. Let $\mathsf{H}\colon \mathcal{U}\times\mathcal{R}\times\mathcal{M} \to \mathcal{Y}$ be a hash function and $\mathsf{HaS}^{\mathsf{ph}}[\mathsf{T},\mathsf{H},\mathsf{E}]$

Game: ST_b	$\mathsf{NewKey}_0()$	$\mathsf{NewKey}_1()$
1 $(\mathsf{F}', \mathsf{I}') \leftarrow \mathsf{Gen}'(1^\lambda)$ 2 $b^* \leftarrow \mathcal{D}_{\mathsf{st}}^{\mathsf{NewKey}_b}()$ 3 **return** b^*	1 $(\mathsf{F}_j, \mathsf{I}_j) \leftarrow \mathsf{Gen}(1^\lambda)$ 2 **return** F_j	1 $\mathsf{L}_j \leftarrow \mathcal{D}_\mathsf{L}$ 2 $\mathsf{R}_j \leftarrow \mathcal{D}_\mathsf{R}$ 3 $\mathsf{F}_j := \mathsf{L}_j \circ \mathsf{F}' \circ \mathsf{R}_j$ 4 **return** F_j

Fig. 8: ST (Sandwich Transformation) game

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 $(\mathsf{F}, \mathsf{I}) \leftarrow \mathsf{Gen}(1^\lambda)$. [8] 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 $x \neq \perp$ holds, 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 $\mathsf{F}(x) \stackrel{?}{=} \mathsf{H}(\mathsf{E}(\mathsf{F}), r, m)$.

In Appendix G, Lemmas G.1 and G.2 establish reductions of M-INV $\Rightarrow$ M-EUF-CMA and M-CR $\Rightarrow$ M-sEUF-CMA without any security loss in the number of keys. However, there are trivial reductions: $\mathrm{Adv}_{\mathsf{T}}^{\text{M-INV}}(\mathcal{B}_{\mathsf{inv^m}}) \leq q_{\mathsf{inst}} \mathrm{Adv}_{\mathsf{T}}^{\text{INV}}(\mathcal{B}_{\mathsf{inv}})$ and $\mathrm{Adv}_{\mathsf{T}}^{\text{M-CR}}(\mathcal{B}_{\mathsf{cr^m}}) \leq q_{\mathsf{inst}} \mathrm{Adv}_{\mathsf{T}}^{\text{CR}}(\mathcal{B}_{\mathsf{cr}})$. If the adversaries can target multiple instances conccurently, equality may hold in these inequalities. To address this issue, we propose a generic method to show reductions from INV or CR by assuming the hardness of the computational problem on keys' distributions.

Let $\{\mathsf{F}_j\}_{j \in [q_{\mathsf{key}}]}$ be verification keys generated by Gen of a TDF T. 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 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 4.1 (ST (Sandwich Transformation) Game). *Let T and T' be TDFs. Using a game given in Fig. 8, we define an advantage function of an adversary $\mathcal{D}_{\mathsf{st}}$ playing the* ST *game against T and T' as* $\mathrm{Adv}_{\mathsf{T},\mathsf{T}'}^{\text{ST}}(\mathcal{D}_{\mathsf{st}}) = \left|\Pr\left[\mathsf{ST}_0^{\mathcal{D}_{\mathsf{st}}} \Rightarrow 1\right] - \Pr\left[\mathsf{ST}_1^{\mathcal{D}_{\mathsf{st}}} \Rightarrow 1\right]\right|$.

We have the following reductions assuming some conditions on L_j and R_j (see the proofs in Appendices H and I).

Lemma 4.1 (INV + ST $\Rightarrow$ M-EUF-CMA). *Let T' be a TDF with $\mathsf{F}'\colon \mathcal{X}' \to \mathcal{Y}$. Suppose that $\mathsf{L}_j\colon \mathcal{Y} \to \mathcal{Y}$ and $\mathsf{R}_j\colon \mathcal{X} \to \mathcal{X}'$ are used to simulate F_j by $\mathsf{L}_j \circ \mathsf{F}' \circ \mathsf{R}_j$ in the* ST *game, where L_j is a bijection.*

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*

[8] 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).

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

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

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 $\mathcal{B}_{\mathsf{inv}}$, $\mathcal{D}_{\mathsf{ps^m}}$, and $\mathcal{D}_{\mathsf{st}}$ are about that of $\mathcal{A}_{\mathsf{cma^m}}$.

Lemma 4.2 (CR + ST $\Rightarrow$ M-sEUF-CMA). *Let T' be a TDF with $\mathsf{F}'\colon \mathcal{X}' \to \mathcal{Y}$. Suppose that $\mathsf{L}_j\colon \mathcal{Y}' \to \mathcal{Y}$ and $\mathsf{R}_j\colon \mathcal{X} \to \mathcal{X}'$ are used to simulate F_j by $\mathsf{L}_j \circ \mathsf{F}' \circ \mathsf{R}_j$ in the* ST *game, where L_j and R_j are injections.*

For any quantum M-sEUF-CMA *adversary $\mathcal{A}_{\mathsf{cma^m}}$ of $\mathsf{HaS^{ph}}[\mathsf{T}_{\mathsf{psf}},\mathsf{H},\mathsf{E}]$ 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 $(\mathsf{T}_{\mathsf{psf}}, \mathsf{T}')$ issuing q_{key} new key queries such that*

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

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 $\mathcal{A}_{\mathsf{cma^m}}$.

In Appendix J, we applly the generic method to some frameworks of hash-and-sign signatures in lattice-based, code-based, and MQ-based cryptography. To bound the ST advantage, we introduce multi-instance variants of established computational problems in code-based and MQ-based cryptography, that is, permutation/linear equivalence [48] and morphism of polynomials [47].

Open problems: There are two open problems for the generic method. First, the computational problems defined in Appendix J used for bounding the ST advantage have not been studied deeply; therefore, future studies are necessary to guarantee the hardness of the problems. Second, we currently fail to use the generic method to show the M-EUF-CMA security under *adaptive corruptions of signing keys*. Solving this issue is the second open problem.

References

1. Ambainis, A., Hamburg, M., Unruh, D.: Quantum security proofs using semi-classical oracles. In: Boldyreva and Micciancio [12], pp. 269–295. https://doi.org/10.1007/978-3-030-26951-7_10 5, 10, 11, 21, 22
2. Barbosa, M., Barthe, G., Doczkal, C., Don, J., Fehr, S., Grégoire, B., Huang, Y.H., Hülsing, A., Lee, Y., Wu, X.: Fixing and mechanizing the security proof of fiat-shamir with aborts and dilithium. Cryptology ePrint Archive, Report 2023/246 (2023), https://eprint.iacr.org/2023/246 6
3. Barenghi, A., Biasse, J.F., Persichetti, E., Santini, P.: On the computational hardness of the code equivalence problem in cryptography. Advances in Mathematics of Communications **17**(1), 23–55 (Feb 2023). https://doi.org/10.3934/amc.2022064, /article/id/62fa202b4cedfd0007b8b288 45
4. 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, 8
5. Bellare, M., Rogaway, P.: The exact security of digital signatures: How to sign with RSA and Rabin. In: Maurer [40], pp. 399–416. https://doi.org/10.1007/3-540-68339-9_34 1, 4, 22
6. Belsley, E.D.: Rates of convergence of Markov chains related to association schemes. Ph.D. thesis (May 1993) 38
7. 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 45
8. Beullens, W.: Improved cryptanalysis of UOV and Rainbow. In: Canteaut, A., Standaert, F.X. (eds.) EUROCRYPT 2021, Part I. LNCS, vol. 12696, pp. 348–373. Springer, Heidelberg (Oct 2021). https://doi.org/10.1007/978-3-030-77870-5_13 39
9. 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 5, 13, 32, 35, 39, 40
10. Beullens, W., Chen, M.S., Hung, S.H., Kannwischer, M.J., Peng, B.Y., Shih, C.J., Yang, B.Y.: Oil and vinegar: Modern parameters and implementations. Cryptology ePrint Archive, Report 2023/059 (2023), https://eprint.iacr.org/2023/059 33, 38
11. 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 21
12. Boldyreva, A., Micciancio, D. (eds.): CRYPTO 2019, Part II, LNCS, vol. 11693. Springer, Heidelberg (Aug 2019) 16, 17
13. 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, 4, 23, 24, 25, 43
14. Bouillaguet, C., Fouque, P.A., Véber, A.: Graph-theoretic algorithms for the "isomorphism of polynomials" problem. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 211–227. Springer, Heidelberg (May 2013). https://doi.org/10.1007/978-3-642-38348-9_13 46

15. 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/post-quantum-cryptography-standardization/round-3-submissions 5, 13, 35
16. 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, 8, 12, 23, 24, 25, 32, 37
17. 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 2022) 24, 25, 32
18. 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, 37
19. 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) 5, 13, 31, 36
20. 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 5, 13, 32, 37
21. Devevey, J., Fallahpour, P., Passelègue, A., Stehlé, D.: A detailed analysis of fiat-shamir with aborts. Cryptology ePrint Archive, Report 2023/245 (2023), https://eprint.iacr.org/2023/245 6
22. 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/post-quantum-cryptography-standardization/round-3-submissions 5, 13, 34
23. 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 5, 6, 10, 12, 20, 21, 25
24. Don, J., Fehr, S., Majenz, C., Schaffner, C.: Security of the Fiat-Shamir transformation in the quantum random-oracle model. In: Boldyreva and Micciancio [12], pp. 356–383. https://doi.org/10.1007/978-3-030-26951-7_13 12
25. 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
26. Faugère, J.C., Perret, L.: Polynomial equivalence problems: Algorithmic and theoretical aspects. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 30–47. Springer, Heidelberg (May / Jun 2006). https://doi.org/10.1007/11761679_3 46
27. 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

28. 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 5, 13, 34
29. 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, 4, 8, 22, 36, 44, 45
30. 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, https://doi.org/10.1137/0217017 1
31. 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, 5, 6, 10, 11, 12, 20
32. 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, 8
33. 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 10
34. Ikematsu, Y., Nakamura, S., Santoso, B., Yasuda, T.: Security analysis on an ElGamal-like multivariate encryption scheme based on isomorphism of polynomials. In: Yu, Y., Yung, M. (eds.) Information Security and Cryptology – Inscrypt 2021. LNCS, vol. 13007, pp. 235–250. Springer, Heidelberg (Oct 2021) 46
35. Kiltz, E., Lyubashevsky, V., Schaffner, C.: A concrete treatment of Fiat-Shamir signatures in the quantum random-oracle model. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018, Part III. LNCS, vol. 10822, pp. 552–586. Springer, Heidelberg (Apr / May 2018). https://doi.org/10.1007/978-3-319-78372-7_18 6
36. 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
37. 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, 13, 32, 33, 37
38. Leon, J.: Computing automorphism groups of error-correcting codes. IEEE Transactions on Information Theory **28**(3), 496–511 (May 1982), https://ieeexplore.ieee.org/document/1056498 45
39. 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, 23, 25
40. Maurer, U.M. (ed.): EUROCRYPT'96, LNCS, vol. 1070. Springer, Heidelberg (May 1996) 16, 19
41. Menezes, A., Smart, N.: Security of signature schemes in a multi-user setting. Designs, Codes and Cryptography **33**(3), 261–274 (Nov 2004), https://link.springer.com/article/10.1023/B:DESI.0000036250.18062.3f 4

42. Morozov, K., Roy, P.S., Steinwandt, R., Xu, R.: On the security of the Courtois-Finiasz-Sendrier signature. Open Mathematics **16**(1), 161–167 (Mar 2018). https://doi.org/doi:10.1515/math-2018-0011, https://doi.org/10.1515/math-2018-0011 31
43. NIST: Submission requirements and evaluation criteria for the post-quantum cryptography standardization process (Jan 2017), https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf 4
44. 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 2, 5
45. NIST: Status report on the third round of the nist post-quantum cryptography standardization process (Sep 2022), https://csrc.nist.gov/publications/detail/nistir/8413/final 2
46. Patarin, J.: Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms. In: Maurer [40], pp. 33–48. https://doi.org/10.1007/3-540-68339-9_4 2, 32
47. 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 15, 46
48. Petrank, E., Roth, R.M.: Is code equivalence easy to decide? IEEE Transactions on Information Theory **43**(5), 1602–1604 (Sep 1997), https://ieeexplore.ieee.org/document/623157 15, 45
49. 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 44
50. 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 4, 8, 13, 24, 32, 34, 35, 37, 38, 39
51. Sendrier, N.: Finding the permutation between equivalent linear codes: The support splitting algorithm. IEEE Transactions on Information Theory **46**(4), 1193–1203 (2000) 45
52. 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 45
53. 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
54. Szepieniec, A., Preneel, B.: Block-anti-circulant unbalanced Oil and Vinegar. In: Paterson, K.G., Stebila, D. (eds.) SAC 2019. LNCS, vol. 11959, pp. 574–588. Springer, Heidelberg (Aug 2019). https://doi.org/10.1007/978-3-030-38471-5_23 46
55. 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 10

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

Fig. 9: AR (Adaptive Reprogramming) game

56. 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, 13, 23, 24
57. Yamakawa, T., Zhandry, M.: Verifiable quantum advantage without structure. In: 63rd FOCS. pp. 69–74. IEEE Computer Society Press (Oct / Nov 2022). https://doi.org/10.1109/FOCS54457.2022.00014 2
58. Zhandry, M.: How to construct quantum random functions. In: 53rd FOCS. pp. 679–687. IEEE Computer Society Press (Oct 2012). https://doi.org/10.1109/FOCS.2012.37 24
59. Zhandry, M.: Secure identity-based encryption in the quantum random oracle model. Cryptology ePrint Archive, Report 2012/076 (2012), https://eprint.iacr.org/2012/076 2, 3, 4, 13, 23, 24, 25

A Proof Techniques in QROM

We introduce three techniques employed in proving Theorem 3.1.

A.1 Tight Adaptive Reprogramming Technique [31]

Fig. 9 shows a game called AR (Adaptive Reprogramming) game, in which the adversary $\mathcal{D}_{\mathsf{ar}}$ attempts 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 A.1 (Tight Adaptive Reprogramming Technique [31, 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*

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

A.2 Measure-and-Reprogram Technique [23]

Fig. 10 shows a two-stage simulator S for $\mathcal{A}$ playing any search-type game in the QROM. The simulator operates as follows: In the first stage, S_1 uniformly

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

Fig. 10: A simulator S for any search-type game adversary $\mathcal{A}$

selects 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 $\mathsf{H}' := \mathsf{H}^{(r',m')\mapsto\theta}$ 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 A.2 (Measure-and-Reprogram Technique [23, 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,*

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

A.3 Semi-classical O2H Technique [1]

We define *punctured oracle* following a notation of [11].

Definition A.1 (Punctured Oracle [11, Definition 1]). *Let $\mathcal{S} \subset \mathcal{R} \times \mathcal{M}$ be a set. Let $\mathsf{f}_{\mathcal{S}} : \mathcal{R} \times \mathcal{M} \to \{0, 1\}$ be a predicate that returns 1 if and only if $(r, m) \in \mathcal{S}$.* 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 $|\mathsf{f}_{\mathcal{S}}(r, m)\rangle$, measures $|\mathsf{f}_{\mathcal{S}}(r, m)\rangle$, runs $\mathsf{H}(r, m)$, and returns the result. Let* FIND *be an event that any of measurements of $|\mathsf{f}_{\mathcal{S}}(r, m)\rangle$ returns 1.*

The answer from the oracle $\mathsf{H} \backslash \mathcal{S}$ depends on the measurement results. Let us consider a query $\sum_{(r,m)} \alpha_{r,m} |r, m\rangle |y\rangle$. $\mathsf{H} \backslash \mathcal{S}$ computes $\sum_{(r,m)} \alpha_{r,m} |r, m\rangle |y\rangle |\mathsf{f}_{\mathcal{S}}(r, m)\rangle$ and measures the third register. If the result is 0, then the query is transformed to $\sum_{(r,m)\notin\mathcal{S}} \alpha_{r,m} |r, m\rangle |y\rangle |0\rangle$ and $\mathsf{H} \backslash \mathcal{S}$ returns $\sum_{(r,m)\notin\mathcal{S}} \alpha_{r,m} |r, m\rangle |y \oplus \mathsf{H}(r, m)\rangle$ to the adversary. If the results is 1 (and thus, FIND $= \top$ holds), $\mathsf{H} \backslash \mathcal{S}$ returns $\sum_{(r,m)\in\mathcal{S}} \alpha_{r,m} |r, m\rangle |y \oplus \mathsf{H}(r, m)\rangle$ to the adversary. Thus, if FIND $= \perp$, then the adversary cannot obtain any information on $\mathsf{H}(r, m)$ for $(r, m) \in \mathcal{S}$. Hence, we have the following:

Lemma A.3 (Indistinguishability of Punctured Oracles [1, Lemma 1]). *Let $\mathsf{H}_0, \mathsf{H}_1 : \mathcal{R} \times \mathcal{M} \to \mathcal{Y}$ 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 $\mathsf{H}_0(r,m) = \mathsf{H}_1(r,m)$ for any $(r,m) \notin \mathcal{S}$.) For any quantum adversary $\mathcal{A}$ and any event* E*,*

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

The following lemma provides a bound on the advantage gap between the original game and a game with a punctured oracle by considering the probability of $\mathrm{FIND} = \top$. Note that we omit unnecessary statements from [1, Theorem 1] and do not consider the parallelization of queries.

Lemma A.4 (Semi-classical O2H Technique [1, Theorem 1]). *Let $\mathsf{H}\colon \mathcal{R} \times \mathcal{M} \to \mathcal{Y}$ 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,*

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

Furthermore, the following provides a bound on $\Pr\left[\mathrm{FIND} = \top : b \leftarrow \mathcal{A}^{|\mathsf{H} \setminus \mathcal{S}\rangle}(z)\right]$.

Lemma A.5 (Search in Semi-classical Oracle [1, Theorem 2 and Corollary 1]). *Let $\mathcal{A}$ be a quantum adversary issuing at most q_{qro} (quantum) random oracle queries to H. 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,*

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

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

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

B Existing Security Proofs

We review the existing security proofs, including our own, and summarize them in Table 2.

Security Proof in the ROM [5, 29]: 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 $x \leftarrow \mathsf{SampDom}(\mathsf{F})$

Table 2: Summary of the existing and our security proofs. In "Conditions of TDF", ✓ indicates this condition of PSF (see Definition 2.6) is necessary, and ✓[1]/✓[2] indicate that **Condition 2** is relaxed as "A bound δ on average of $\delta_{\mathsf{F},\mathsf{I}}$ is negligible" and "$\epsilon_{\mathsf{ps}} = \mathrm{Adv}^{\mathrm{PS}}_{\mathsf{T}_{\mathsf{wpsf}}}(\mathcal{D}_{\mathsf{ps}})$ is negligible". In "Target scheme", $\mathsf{d}/\mathsf{p}/\mathsf{pr}$ stand for the deterministic hash-and-sign, probabilistic hash-and-sign, and probabilistic hash-and-sign with retry.

Security proof	Security Bound	Assumption	Conditions of TDF 1	2	3	4	Target scheme
[13]	$\frac{1}{1-2^{-\omega(\log(\lambda))}}\epsilon_{\mathsf{cr}}$	CR	✓	✓	✓	✓	d/p
[59]	$2\sqrt{\left(q_{\mathsf{sign}} + \frac{8}{3}(q_{\mathsf{sign}} + q_{\mathsf{qro}} + 1)^4\right)\epsilon_{\mathsf{ow/inv}}}$	OW/INV	✓	✓	✓	–	d/p
ext. of [56]	$4q_{\mathsf{sign}}(q_{\mathsf{qro}}+1)(2q_{\mathsf{qro}}+1)^2\epsilon_{\mathsf{ow/inv}}$	OW/INV	✓	✓	✓	–	d/p
[39]	$(2(q_{\mathsf{qro}}+q_{\mathsf{sign}}+1)+1)^2\epsilon_{\mathsf{ow/inv}}$	OW/INV	✓	✓	✓	–	d/p
[16]	$\frac{1}{2}\left(\epsilon_{\mathsf{nma}} + \frac{8\pi}{\sqrt{3}}q_{\mathsf{qro}}^{\frac{3}{2}}\sqrt{\delta} + q_{\mathsf{sign}}\left(\delta + \frac{q_{\mathsf{sign}}}{\lvert\mathcal{R}\rvert}\right)\right)$	EUF-NMA	–	✓[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	–	✓[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	–	✓[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

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**, $\mathcal{B}_{\mathsf{inv}}$ can simulate an honestly generated signature $x_i \leftarrow \mathsf{I}(\mathsf{H}(r_i, m_i))$ by $x_i \leftarrow \mathsf{SampDom}(\mathsf{F})$. 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 $\mathrm{Adv}^{\mathrm{EUF\text{-}CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma^c}}) \le (q_{\mathsf{sign}}+q_{\mathsf{ro}}+1)\mathrm{Adv}^{\mathrm{INV}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{B}_{\mathsf{inv}})$, where $\mathcal{A}_{\mathsf{cma^c}}$ is an adversary who can make only classical queries to H.

Note that $\mathrm{Adv}^{\mathrm{INV}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{B}_{\mathsf{inv}}) = \mathrm{Adv}^{\mathrm{OW}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{B}_{\mathsf{ow}})$ 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 $y = \mathsf{F}(x)$ to the INV adversary, and vice versa.

Security Proof by Semi-constant Distribution [59]: Zhandry showed the reduction from the OW of TDP in the QROM using a technique known as *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 $\mathsf{SampDom}$ [13]. From **Condition 1**, H' is indistinguishable from H.

$\mathcal{B}_{\mathsf{inv}}$ 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 $\frac{8}{3}(q_{\mathsf{sign}} + q_{\mathsf{qro}} + 1)^4\epsilon^2$ [59, 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 [59, Theorem 5.3]

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

Zhandry proposed another technique called *small-range distribution* [58] that also yields a security bound with a square root loss. Chatterjee, Das, and Pandit [17] used this technique to show the EUF-CMA security of the modified UOV signature [50] in the QROM.

Application of Lifting Theorem [56]: 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 [56, Corollary 4.10]. For a hash-and-sign signature $\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}}, \mathsf{H}]$, they showed $\mathrm{Adv}^{\mathrm{EUF\text{-}CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \leq 4q_{\mathsf{sign}}\mathrm{Adv}^{\mathrm{EUF\text{-}NMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{nma}})$ [56, Theorem 4.11]. Extending the results of [56] using the security proof in the ROM, we have a 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 [16]:* 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

[9] The authors of [16] defined a problem called *claw with random function problem*; however, its definition is identical to EUF-NMA game for hash-and-sign.

Appendix E.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 probability $\frac{1}{2}$ and $\mathsf{F}(\mathsf{DetSampDom}(\mathsf{F}, w))$ with probability $\frac{1}{2}$. 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 [16, Theorem 2]

$$\mathrm{Adv}^{\mathrm{EUF\text{-}CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \leq \frac{1}{2}\left(\mathrm{Adv}^{\mathrm{EUF\text{-}NMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{nma}}) + \frac{8\pi}{\sqrt{3}} q_{\mathsf{qro}}^{\frac{3}{2}} \sqrt{\delta} + q_{\mathsf{sign}}\left(\delta + \frac{q_{\mathsf{sign}}}{|\mathcal{R}|}\right)\right). \tag{4}$$

Reduction from Collision-resistance [13]: Boneh et al. [13] 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'). Since $x^* \neq x'$ holds with probability $1 - 2^{-\omega(\log(\lambda))}$ (see **Condition 4**),

$$\mathrm{Adv}^{\mathrm{sEUF\text{-}CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \leq \frac{1}{1 - 2^{-\omega(\log(\lambda))}} \mathrm{Adv}^{\mathrm{CR}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{B}_{\mathsf{cr}}). \tag{5}$$

Concurrent Work [39]: Liu, Jiang, and Zhao [39] showed OW $\Rightarrow$ EUF-CMA for the TDP-FDH and TDP-PFDH in the QROM. Their reduction can be extended to INV $\Rightarrow$ EUF-CMA for the deterministic/probabilistic hash-and-sign based on PSF. As in [17, 13, 59], the random function H is replaced as $\mathsf{H}' = \mathsf{F}(\mathsf{DetSampDom}(\mathsf{F}, \widetilde{\mathsf{H}}(r, m)))$ to answer the signing queries without using the trapdoor. From **Condition 1**, this modification does not incur any security loss. Then, their reduction uses the measure-and-reprogram technique [23, Theorem 2] (see Lemma A.2 in Appendix A) as in our security proof. Since the INV adversary answers signing queries using H', the number of signing queries q_{sign} must be included in the number of queries to H'. As a result, their reduction has a security bound that includes q_{sign} in the multiplicative loss: [10]

$$\mathrm{Adv}^{\mathrm{EUF\text{-}CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \leq (2(q_{\mathsf{qro}} + q_{\mathsf{sign}} + 1) + 1)^2 \mathrm{Adv}^{\mathrm{INV}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{A}_{\mathsf{inv}}). \tag{6}$$

[10] In the latest version of their paper [39], the authors removed q_{sign} from Eq. (6). They claimed that the queries to H' for signing queries are not necessarily considered in [23, Theorem 2]. However, the correctness of their usage of [23, Theorem 2] remains to be fully justified.

C Proof of Theorem 3.1

In the beginning, we show that we can set $q'_{\mathsf{sign}} = \frac{c}{\rho} q_{\mathsf{sign}}$ for some constant $c > 1$, 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. $\mathbb{E}(S) = \rho q'_{\mathsf{sign}} = c q_{\mathsf{sign}}$ holds. From the Chernoff bound, we have $\Pr[S \leq (1-\gamma)\mathbb{E}(S)] \leq e^{-\frac{1}{2}\gamma^2 \mathbb{E}(S)}$. 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. 11 and 12 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 $\Pr\left[\mathsf{G}_0^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] = \mathrm{Adv}^{\text{EUF-CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}}, \mathsf{H}]}(\mathcal{A}_{\mathsf{cma}})$ holds.

Game G_1 (adaptive reprogramming of 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 at most q'_{sign} times.

The AR adversary $\mathcal{D}_{\mathsf{ar}}$ can simulate $\mathsf{G}_0/\mathsf{G}_1$ (the top row of Fig. 12). If $\mathcal{D}_{\mathsf{ar}}$ plays AR_0, $\mathcal{D}_{\mathsf{ar}}$ simulates G_0; otherwise it simulates G_1. From Lemma A.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_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 queried 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.

Game G_3 (puncturing H): Let $\mathcal{S}' = \{(r, m) : r \in \mathcal{S}, m \in \mathcal{M}\}$ 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 FIND $= \top$ (see the definitions of $\mathsf{H}\backslash\mathcal{S}'$ and FIND in Definition A.1). We use Lemma A.4 to bound $\left|\Pr\left[\mathsf{G}_2^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_3^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]\right|$. Suppose that $\Pr\left[\mathsf{G}_2^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] = \Pr\left[1 \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign}, |\mathsf{H}\rangle}(\mathsf{F})\right]$. Since G_3 uses $\mathsf{H}\backslash\mathcal{S}'$ and outputs 0 if FIND $= \top$, we have $\Pr\left[\mathsf{G}_3^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] = \Pr\left[1 \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign}, |\mathsf{H}\backslash\mathcal{S}'\rangle}(\mathsf{F}) \wedge \text{FIND} = \bot\right]$

Game: G_0-G_1

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

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

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

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

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

Game: G_2

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

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

repeat
  $y_i \leftarrow_\$ \mathcal{Y}$
  $x_i \leftarrow \mathsf{I}(y_i)$
  if $x_i = \bot$ **then**
    $ctr := ctr + 1$
    $r_i := \mathcal{S}[ctr]$
  else
    $r_i \leftarrow_\$ \mathcal{R}$
  $\mathsf{H} := \mathsf{H}^{(r_i,m_i)\mapsto y_i}$
until $x_i \neq \bot$
$\mathcal{Q} := \mathcal{Q} \cup \{m_i\}$
return (r_i, x_i)

Game: G_3-G_5

$\mathcal{Q} := \emptyset$
$\mathsf{H} \leftarrow_\$ \mathcal{Y}^{\mathcal{R}\times\mathcal{M}}$
$\mathrm{FIND} := \bot$
$ctr := 0$
$\mathcal{S} := \emptyset$
for $j \in [q'_{\mathsf{sign}} - q_{\mathsf{sign}}]$ **do**
  $r \leftarrow_\$ \mathcal{R}$
  $\mathcal{S} := \mathcal{S} \cup \{r\}$
$\mathcal{S}' := \{(r, m) \colon r \in \mathcal{S}, m \in \mathcal{M}\}$
$(\mathsf{F},\mathsf{I}) \leftarrow \mathsf{Gen}(1^\lambda)$
$(m^*, r^*, x^*) \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign},|\mathsf{H}\backslash\mathcal{S}'\rangle}(\mathsf{F})$
if $m^* \in \mathcal{Q} \vee \mathrm{FIND} = \top$ **then**
  return 0
return $\mathsf{F}(x^*) \stackrel{?}{=} \mathsf{H}(r^*, m^*)$

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

repeat
  $y_i \leftarrow_\$ \mathcal{Y}$
  $x_i \leftarrow \mathsf{I}(y_i)$
  if $x_i = \bot$ **then**
    $ctr := ctr + 1$
    $r_i := \mathcal{S}[ctr]$
  else
    $r_i \leftarrow_\$ \mathcal{R}$
  $\mathsf{H} := \mathsf{H}^{(r_i,m_i)\mapsto y_i}$
until $x_i \neq \bot$
$\mathcal{Q} := \mathcal{Q} \cup \{m_i\}$
return (r_i, x_i)

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

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

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

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

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,

$$\left|\Pr\left[\mathsf{G}_2^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_3^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]\right| \leq \sqrt{(q_{\mathsf{sign}} + q_{\mathsf{qro}} + 2)\Pr\left[\mathrm{FIND} = \top \colon \mathsf{G}_3^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow b\right]}, \quad (7)$$

by Lemma A.4. We will show a bound on Eq. (7) after defining G_4.

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 the punctured oracle $\mathsf{H}\backslash\mathcal{S}'$. By the

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

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

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

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

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

1 $\mathcal{Q} := \emptyset$
2 $\mathsf{H} \leftarrow_\$ \mathcal{Y}^{\mathcal{R} \times \mathcal{M}}$
3 $\mathrm{FIND} := \bot$
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 $\mathcal{S}' := \{(r, m) \colon r \in \mathcal{S}, m \in \mathcal{M}\}$
9 $(m^*, r^*, x^*) \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign}, |\mathsf{H} \setminus \mathcal{S}'\rangle}(\mathsf{F})$
10 **if** $m^* \in \mathcal{Q} \vee \mathrm{FIND} = \top$ **then**
11   **return** 0
12 **return** $\mathsf{F}(x^*) \stackrel{?}{=} \mathsf{H}(r^*, m^*)$

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

1 $r_i \leftarrow_\$ \mathcal{R}$
2 $x_i \leftarrow \mathsf{Sample}_b()$
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)

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

1 $\mathcal{Q} := \emptyset$
2 $\mathsf{H}' := \mathsf{H}$
3 $\mathrm{FIND} := \bot$
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 $\mathcal{S}' := \{(r, m) \colon r \in \mathcal{S}, m \in \mathcal{M}\}$
9 $(m^*, r^*, x^*) \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign}, |\mathsf{H}' \setminus \mathcal{S}'\rangle}(\mathsf{F})$
10 **if** $m^* \in \mathcal{Q} \vee \mathrm{FIND} = \top$ **then**
11   **return** 0
12 **return** $\mathsf{F}(x^*) \stackrel{?}{=} \mathsf{H}'(r^*, m^*)$

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

1 $r_i \leftarrow_\$ \mathcal{R}$
2 $x_i \leftarrow \mathsf{SampDom}(\mathsf{F})$
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. 12: Simulations for EUF-NMA $\Rightarrow$ EUF-CMA

definition of FIND, if $\mathrm{FIND} = \bot$, 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 $\mathrm{FIND} = \bot$, 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

$$\Pr\left[\mathrm{FIND} = \bot : \mathsf{G}_3^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow b\right] = \Pr\left[\mathrm{FIND} = \bot : \mathsf{G}_4^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow b\right] \tag{8}$$

(as Lemma A.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. (8).

Let G'_4 be a game given in Fig. 13 (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

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. 13: A game G'_4 used in the application of Lemma A.5

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, $\Pr\big[\mathsf{G}'^{\mathcal{B}_{\mathsf{cma}}}_4 \Rightarrow 1\big] \leq \Pr[r' \in \mathcal{S}] \leq \frac{q'_{\mathsf{sign}} - q_{\mathsf{sign}}}{|\mathcal{R}|}$ holds. Hence, $\Pr\big[\mathrm{FIND} = \top \colon \mathsf{G}_4^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow b\big] \leq 4(q_{\mathsf{sign}} + q_{\mathsf{qro}} + 1)\frac{q'_{\mathsf{sign}} - q_{\mathsf{sign}}}{|\mathcal{R}|}$ holds from Lemma A.5 and an upper bound on Eq. (7) is $2(q_{\mathsf{sign}} + q_{\mathsf{qro}} + 2)\sqrt{\frac{q'_{\mathsf{sign}} - q_{\mathsf{sign}}}{|\mathcal{R}|}}$.

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. 12. If $\mathcal{D}_{\mathsf{ps}}$ plays PS_0, the procedures of the original and simulated G_4 are identical. If $\mathcal{D}_{\mathsf{ps}}$ plays PS_1, he obviously simulates G_5. Thus, we have $\big|\Pr\big[\mathsf{G}_4^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\big] - \Pr\big[\mathsf{G}_5^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\big]\big| \leq \mathrm{Adv}^{\mathrm{PS}}_{\mathsf{T}_{\mathsf{wpsf}}}(\mathcal{D}_{\mathsf{ps}})$.

We show that the EUF-NMA adversary $\mathcal{A}_{\mathsf{nma}}$ can simulate G_5 as in the bottom row of Fig. 12. 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 $m^* \notin \mathcal{Q}$, $\mathsf{H}'(r^*, m^*) = \mathsf{H}(r^*, m^*)$ holds for (m^*, r^*, x^*) that $\mathcal{A}_{\mathsf{cma}}$ returns. Therefore, $\mathcal{A}_{\mathsf{nma}}$ wins his game if $\mathcal{A}_{\mathsf{cma}}$ wins the EUF-CMA game. 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 $\Pr\big[\mathsf{G}_5^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\big] \leq \mathrm{Adv}^{\mathrm{EUF\text{-}NMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}}, \mathsf{H}]}(\mathcal{A}_{\mathsf{nma}})$ holds. We finally stress that the number of queries $\mathcal{A}_{\mathsf{nma}}$ made to H is q_{qro} rather than $q_{\mathsf{qro}} + q_{\mathsf{sign}}$ since $\mathcal{A}_{\mathsf{nma}}$ never queries to its random oracle in the simulation of the signature.

Summing up, we have Eq. (2) for EUF-NMA $\Rightarrow$ EUF-CMA.

INV $\Rightarrow$ EUF-NMA*:* We use Lemma A.2. Let S be a two-stage algorithm that runs $\mathcal{A}_{\mathsf{nma}}$ in the EUF-NMA game shown in Fig. 14. The INV adversary $\mathcal{B}_{\mathsf{inv}}$ runs 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 $\mathsf{H}' := \mathsf{H}^{(r', m')\mapsto y}$. In the second stage, S_2 runs $\mathcal{A}_{\mathsf{nma}}$ with reprogrammed H' and outputs x' included in an output of $\mathcal{A}_{\mathsf{nma}}^{|\mathsf{H}'\rangle}(\mathsf{F})$.

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

When the predicate is $\mathsf{F}(x) \stackrel{?}{=} \mathsf{H}(r, m)$, we have

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

for any $(\hat{r}, \hat{m}) \in \mathcal{R} \times \mathcal{M}$ from Lemma A.2. By summing up over all $(\hat{r}, \hat{m}) \in \mathcal{R} \times \mathcal{M}$,

$$\begin{aligned} &\Pr\Big[\mathsf{F}(x') = y : (r', m') \leftarrow \mathsf{S}_1^{\mathcal{A}_{\mathsf{nma}}^{\lvert\mathsf{H}\rangle}}(), x' \leftarrow \mathsf{S}_2^{\mathcal{A}_{\mathsf{nma}}^{\lvert\mathsf{H}'\rangle}}(y)\Big] \\ &\qquad \geq \frac{1}{(2q_{\mathsf{qro}}+1)^2} \Pr\Big[\mathsf{F}(x^*) = \mathsf{H}(r^*, m^*) : (m^*, r^*, x^*) \leftarrow \mathcal{A}_{\mathsf{nma}}^{\lvert\mathsf{H}\rangle}(\mathsf{F})\Big]. \end{aligned} \quad (9)$$

Notice that the probability in the RHS of Eq. (9) is the EUF-NMA advantage. Also, $\mathrm{Adv}_{\mathsf{T}_{\mathsf{wpsf}}}^{\mathrm{INV}}(\mathcal{B}_{\mathsf{inv}}) \geq \Pr\Big[\mathsf{F}(x') = y : (r', m') \leftarrow \mathsf{S}_1^{\mathcal{A}_{\mathsf{nma}}^{\lvert\mathsf{H}\rangle}}(), x' \leftarrow \mathsf{S}_2^{\mathcal{A}_{\mathsf{nma}}^{\lvert\mathsf{H}'\rangle}}(y)\Big]$ holds since $\mathcal{B}_{\mathsf{inv}}$ runs S. Hence, we have

$$\mathrm{Adv}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H}]}^{\mathrm{EUF\text{-}NMA}}(\mathcal{A}_{\mathsf{nma}}) \leq (2q_{\mathsf{qro}}+1)^2 \mathrm{Adv}_{\mathsf{T}_{\mathsf{wpsf}}}^{\mathrm{INV}}(\mathcal{B}_{\mathsf{inv}}). \quad (10)$$

From Eqs. (2) and (10), we have Eq. (1). □

D Proof of Corollary 3.1

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 restated as: if $(m^*, r^*) \in \mathcal{Q}'$, where $\mathcal{Q}' = \{(m_i, r_i)\}_{i \in [q_{\mathsf{sign}}]}$. We show that the same bound as Eq. (2) holds for EUF-NMA $\Rightarrow$ sEUF-CMA.

In Corollary 3.1, we can use the same games as defined in Theorem 3.1, and the bound on $\big|\Pr\big[\mathsf{G}_0^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\big] - \Pr\big[\mathsf{G}_5^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\big]\big|$ remains unchanged. In the simulation of G_5 (see the bottom row of Fig. 12), $\mathcal{A}_{\mathsf{cma}}$ 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, $\Pr\big[\mathsf{G}_5^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\big] \leq \mathrm{Adv}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H}]}^{\mathrm{EUF\text{-}NMA}}(\mathcal{A}_{\mathsf{nma}})$ holds, which implies that Eq. (2) holds.

□

E Security Proofs of Hash-and-sign Signatures by Theorem 3.1 and Corollary 3.1

This section shows the applications of Theorem 3.1 and Corollary 3.1 to some code-based and MQ-based hash-and-sign signatures.

E.1 Code-based Cryptography

Application to the Modified CSF Signature: Dallot [19] proposed a modification to the CFS signature, that is, the adaption of the probabilistic hash-and-sign with retry. For the details of the (modified) CFS signature, see Appendix F.2.

Let us assume that (n, k)-Goppa code over $\mathbb{F}_q$ can decode up to t errors. Let $\mathsf{T_{cfs}} = (\mathsf{Gen_{cfs}}, \mathsf{F_{cfs}}, \mathsf{I_{cfs}})$ be the underlying TDF of the modified CFS signature and $\mathcal{X}_{n,\leq t} = \{x \in \mathbb{F}_q^n : 0 < \mathsf{hw}(x) \leq t\}$ be a domain of $\mathsf{F_{cfs}}$, where $\mathsf{hw}(x)$ denotes a Hamming weight of x. $\mathsf{F_{cfs}} = UH_0P$ ($\mathsf{F_{cfs}} : \mathcal{X}_{n,\leq t} \to \mathbb{F}_q^{n-k}$) consists of a parity-check matrix of an (n, k)-binary Goppa code $H_0 \in \mathbb{F}_q^{(n-k)\times n}$, an invertible matrix $U \in \mathbb{F}_q^{(n-k)\times(n-k)}$, and a permutation matrix $P \in \mathbb{F}_q^{n\times n}$. 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 $\mathsf{I_{cfs}}(y)$ outputs $\perp$ for $y \notin \mathcal{Y}_{dec}$. Therefore, $\mathsf{F_{cfs}} : \mathcal{X}_{n,\leq t} \to \mathbb{F}_q^{n-k}$ is an injection. Using the fact, Morozov et al. gave INV $\Rightarrow$ sEUF-CMA in the ROM [42, Theorem 3.1]. We show that the modified CFS signature is sEUF-CMA-secure in the QROM, assuming that $\mathsf{T_{cfs}}$ is non-invertible.

Proposition E.1 (INV $\Rightarrow$ sEUF-CMA (Modified CFS Signature)). *For any quantum* sEUF-CMA *adversary $\mathcal{A}_{\mathsf{cma}}$ of $\mathsf{HaS}[\mathsf{T_{cfs}}, \mathsf{H}]$ 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 exists an* INV *adversary $\mathcal{B}_{\mathsf{inv}}$ of $\mathsf{T_{cfs}}$ such that*

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

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 $\mathsf{SampDom}(\mathsf{F_{cfs}})$ as $x \leftarrow_{\$} \mathcal{X}_{n,\leq t}$, $\mathsf{T_{cfs}}$ becomes WPSF. Since $\mathsf{F_{cfs}}$ is an injection, we can apply Corollary 3.1 to the modified CFS signature. In the PS game, we show that $\mathsf{SampDom}(\mathsf{F_{cfs}})$ 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 $\mathcal{Y}_{dec}$, $x \leftarrow \mathsf{I_{cfs}}(y)$ 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 $\mathsf{I_{cfs}}(y_i) \neq \perp$ holds; therefore y_i is uniformly chosen from $\mathcal{Y}_{dec}$. Hence, the distribution of x_i output by Sample_0 is equivalent to that of $x_i \leftarrow \mathsf{SampDom}(\mathsf{F_{cfs}})$ and, thus, $\mathrm{Adv}^{\mathrm{PS}}_{\mathsf{T_{cfs}}}(\mathcal{D}_{\mathsf{ps}}) = 0$ holds. $\square$

Application to Wave: Wave is a practical and unbroken hash-and-sign signature [20]. See Appendix F.3 for the details.

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)* [16, 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 E.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 an* INV *adversary $\mathcal{B}_{\mathsf{inv}}$ of $\mathsf{T}_{\mathsf{wave}}$ such that*

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

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 [16] that is a special case of WPSF, we can apply Theorem 3.1 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. (1) is 0). From the first condition of ATPSF, there is a bound δ on the expectation of $\delta_{\mathsf{F},\mathsf{I}}$; therefore, $\mathrm{Adv}^{\mathrm{PS}}_{\mathsf{T}_{\mathsf{wave}}}(\mathcal{D}_{\mathsf{ps}}) \leq q_{\mathsf{sign}}\delta$ holds from the union bound. □

Compared with the existing reduction using Eq. (4) [16], 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 $\mathsf{T}_{\mathsf{wave}}$ [16, Proposition 8].

E.2 Multivariate-quadratic-based Cryptography

Many schemes based on the UOV [37] and HFE [46] 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 [50]. [11] We prove that the original/modified UOV signatures and the modified HFE signature are EUF-CMA-secure in the QROM if their TDFs are non-invertible. Also, we prove the EUF-CMA security of MAYO [9].

[11] Chatterjee et al. [17] pointed out that the security proof of [50] is flawed slightly, that is, ignorance of the bias of the programmed random oracle introduced by the simulation of the signature. They resolved the issue by making the failure probability negligible, which employs exponential q. We note that the security proof of [50] can easily be corrected using the ROM version of our technique that is used in Theorem 3.1.

$\mathsf{HaS}[\mathsf{T}_{\mathsf{uov}}, \mathsf{H}].\mathsf{Sign}(\mathsf{I}_{\mathsf{uov}}, m)$	$\mathsf{I}_{\mathsf{uov}}(y)$
$r \leftarrow_\$ \mathcal{R}$	**repeat**
$x \leftarrow \mathsf{I}_{\mathsf{uov}}(\mathsf{H}(r, m))$	$\quad z^v \leftarrow_\$ \mathbb{F}_q^v$
return (r, x)	**until** $\{z^o : \mathsf{P}(z^v, z^o) = y\} \neq \emptyset$
	$z^o \leftarrow_\$ \{z^o : \mathsf{P}(z^v, z^o) = y\}$
	$x := \mathsf{S}^{-1}(z^v \| z^o)$
	return x

Fig. 15: Signature generation algorithm of the original UOV signature

Application to the Original UOV Signature: We briefly review the Original UOV scheme. For the details, see Appendix F.4.

Let $\mathsf{T}_{\mathsf{uov}} = (\mathsf{Gen}_{\mathsf{uov}}, \mathsf{F}_{\mathsf{uov}}, \mathsf{I}_{\mathsf{uov}})$ be a TDF used in the original 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 map $\mathsf{P} : \mathbb{F}_q^n \to \mathbb{F}_q^o$. 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 $n = v + o$. By design of P, $\mathsf{P}(z^v, \cdot)$ becomes a set of linear functions on oil variables z^o by fixing z^v. $\mathsf{I}_{\mathsf{uov}}$ chooses $z^v \leftarrow_\$ \mathbb{F}_q^v$ and obtains z^o after retrying z^v until $\{z^o \colon \mathsf{P}(z^v, z^o) = \mathsf{H}(r, m)\} \neq \emptyset$ holds or $\mathsf{P}(z^v, z^o)$ is full-rank. [12] See Fig. 15 for the signing algorithm and $\mathsf{I}_{\mathsf{uov}}$.

We show the EUF-CMA security of the original UOV signature in the QROM if it adopts the probabilistic hash-and-sign.

Proposition E.3 (INV ⇒ EUF-CMA (Original 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* $\mathsf{T}_{\mathsf{uov}}$ *and a* PS *adversary* $\mathcal{D}_{\mathsf{ps}}$ *of* $\mathsf{T}_{\mathsf{uov}}$ *issuing* q_{sign} *sampling queries such that*

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

where the running times of $\mathcal{B}_{\mathsf{inv}}$ *and* $\mathcal{D}_{\mathsf{ps}}$ *are 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; therefore, we can apply Theorem 3.1. Note that $\mathsf{HaS}[\mathsf{T}_{\mathsf{uov}}, \mathsf{H}].\mathsf{Sign}$ generates signatures without retry to take r. Thus, $q'_{\mathsf{sign}} = q_{\mathsf{sign}}$ holds as in Proposition E.2. □

If the PS advantage $\mathrm{Adv}^{\mathrm{PS}}_{\mathsf{T}_{\mathsf{uov}}}(\mathcal{D}_{\mathsf{ps}})$ is negligible, the original UOV signature is provable secure. However, we must consider the *computational* indistinguishability of $x \leftarrow \mathsf{I}_{\mathsf{uov}}(y)$ for $y \leftarrow_\$ \mathbb{F}_q^o$ $(b = 0)$ and $x \leftarrow_\$ \mathbb{F}_q^n$ $(b = 1)$ in the PS game since x output by $\mathsf{HaS}[\mathsf{T}_{\mathsf{uov}}, \mathsf{H}].\mathsf{Sign}$ is not uniform. Note that we can apply Proposition E.3 to a signature scheme recently proposed by Beullens et al. [10] since it follows the original UOV signature.

[12] The original UOV [37] does not use r, but we here employ r.

$\underline{\mathsf{HaS}[\mathsf{T}_{\mathsf{muov}}, \mathsf{H}].\mathsf{Sign}(\mathsf{I}_{\mathsf{muov}}, m)}$
$z^v \leftarrow \mathsf{I}^1_{\mathsf{muov}}()$
repeat
  $r \leftarrow_\$ \mathcal{R}$
  $x \leftarrow \mathsf{I}^2_{\mathsf{muov}}(z^v, \mathsf{H}(r, m))$
until $x \neq \perp$
return (r, x)

$\underline{\mathsf{I}^1_{\mathsf{muov}}()}$
$z^v \leftarrow_\$ \mathbb{F}_q^v$
return z^v

$\underline{\mathsf{I}^2_{\mathsf{muov}}(z^v, y)}$
if $\{z^o : \mathsf{P}(z^v, z^o) = y\} = \emptyset$ **then**
  return $\perp$
$z^o \leftarrow_\$ \{z^o : \mathsf{P}(z^v, z^o) = y\}$
$x := \mathsf{S}^{-1}(z^v \| z^o)$
return x

Fig. 16: Signature generation algorithm of the modified UOV signature

Application to the Modified UOV Signature: Sakumoto et al. [50] proposed the modified UOV signature to solve the problem of the original one, that is, the non-uniformity of signatures. For the details, see Appendix F.4.

Let $\mathsf{T}_{\mathsf{muov}} = (\mathsf{Gen}_{\mathsf{muov}}, \mathsf{F}_{\mathsf{muov}}, \mathsf{I}_{\mathsf{muov}})$ be a TDF used in the modified UOV signature ($\mathsf{Gen}_{\mathsf{muov}} = \mathsf{Gen}_{\mathsf{uov}}$ and $\mathsf{F}_{\mathsf{muov}} = \mathsf{F}_{\mathsf{uov}}$) and Fig. 16 depicts $\mathsf{HaS}[\mathsf{T}_{\mathsf{muov}}, \mathsf{H}].\mathsf{Sign}$ and $\mathsf{I}_{\mathsf{muov}}$. The modified UOV signature retries r instead of z^v and $\mathsf{I}_{\mathsf{muov}}$ is divided into two functions; $\mathsf{I}^1_{\mathsf{muov}}$ and $\mathsf{I}^2_{\mathsf{muov}}$. $\mathsf{I}^1_{\mathsf{muov}}$ chooses $z^v \leftarrow_\$ \mathbb{F}_q^v$ and $\mathsf{I}^2_{\mathsf{muov}}$ finds z^o after retrying r until $\{z^o \colon \mathsf{P}(z^v, z^o) = \mathsf{H}(r, m)\} \neq \emptyset$ holds. Considering the difference in the signing procedure, we show the EUF-CMA security of the modified UOV signature in the QROM.

Proposition E.4 (INV $\Rightarrow$ EUF-CMA (Modified UOV Signature)). *For any quantum* EUF-CMA *adversary* $\mathcal{A}_{\mathsf{cma}}$ *of* $\mathsf{HaS}[\mathsf{T}_{\mathsf{muov}}, \mathsf{H}]$ *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* $\mathsf{T}_{\mathsf{muov}}$ *such that*

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

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 $\mathsf{SampDom}(\mathsf{F}_{\mathsf{muov}})$ as $x \leftarrow_\$ \mathbb{F}_q^n$, $\mathsf{T}_{\mathsf{muov}}$ 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 $z^v \leftarrow \mathsf{I}^1_{\mathsf{muov}}()$ in the beginning and replacing $x_i \leftarrow \mathsf{I}(y_i)$ with $x_i \leftarrow \mathsf{I}^2_{\mathsf{muov}}(z^v, y_i)$. 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 3.1. Hence, we can apply Theorem 3.1 to the modified UOV signature. In Sample_0 of the PS game, $x_i \leftarrow \mathsf{I}^2_{\mathsf{muov}}(z^v, y)$ for $z^v \leftarrow \mathsf{I}^1_{\mathsf{muov}}()$ after retrying y follows $\mathsf{U}(\mathbb{F}_q^n)$ form [50, Theorem 1] (we show the proof sketch in Appendix F.4); therefore, $x_i \leftarrow \mathsf{SampDom}(\mathsf{F}_{\mathsf{muov}})$ in Sample_1 is indistinguishable form x_i output by Sample_0. Hence, $\mathrm{Adv}^{\mathrm{PS}}_{\mathsf{T}_{\mathsf{muov}}}(\mathcal{D}_{\mathsf{ps}}) = 0$ holds. $\square$

We can apply Proposition E.4 to Rainbow [22] and QR-UOV [28] if these schemes make the same modification as the modified UOV signature.

Application to the Modified HFE Signature: The modified HFE signature proposed by Sakumoto et al. [50] is designed to be EUF-CMA secure in the ROM. For the details, see Appendix F.5.

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

Proposition E.5 (INV $\Rightarrow$ EUF-CMA (Modified HFE Signature)). *For any quantum* EUF-CMA *adversary $\mathcal{A}_{\mathsf{cma}}$ of $\mathsf{HaS}[\mathsf{T}_{\mathsf{mhfe}}, \mathsf{H}]$ 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 $\mathsf{T}_{\mathsf{mhfe}}$ such that*

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

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 $\mathsf{F}_{\mathsf{mhfe}}$ has a domain $\mathbb{F}_q^n$, we can define $\mathsf{SampDom}(\mathsf{F}_{\mathsf{mhfe}})$ as $x \leftarrow_{\$} \mathbb{F}_q^n$. Then, $\mathsf{T}_{\mathsf{mhfe}}$ becomes WPSF and we can apply Theorem 3.1 to the modified HFE scheme. The authors of [50] showed that $x \leftarrow \mathsf{I}_{\mathsf{mhfe}}(y)$ after retrying y is uniformly distributed over $\mathbb{F}_q^n$ (we show the proof sketch in Appendix F.5). Therefore, in the PS game, $x_i \leftarrow \mathsf{SampDom}(\mathsf{F}_{\mathsf{mhfe}})$ in Sample_1 is indistinguishable from x_i output by Sample_0, and thus, $\mathrm{Adv}^{\text{PS}}_{\mathsf{T}_{\mathsf{mhfe}}}(\mathcal{D}_{\mathsf{ps}}) = 0$ holds. □

We can apply Proposition E.5 to GeMSS [15] since GeMSS takes the same modification as the modified HFE signature.

Application to MAYO: MAYO, proposed by Beullens [9], is a signature scheme that adopts the probabilistic hash-and-sign and its TDF is based on UOV. For the details, see Appendix F.6.

Let $\mathsf{T}_{\mathsf{mayo}} = (\mathsf{Gen}_{\mathsf{mayo}}, \mathsf{F}_{\mathsf{mayo}}, \mathsf{I}_{\mathsf{mayo}})$ be a TDF used in MAYO. $\mathsf{I}_{\mathsf{mayo}}$ finds a preimage $x = x^v + x^o$ of y for a multivariate quadratic map $\mathsf{P}^* : \mathbb{F}_q^{kn} \to \mathbb{F}_q^m$. Once x^v is uniformly chosen from $(\mathbb{F}_q^{n-o} \times \{0^o\})^k \subset \mathbb{F}_q^{kn}$, where 0^o denotes a vector of o 0s, $\mathsf{P}^*(x^v + x^o) = y$ becomes a linear system of equations for x^o. $\mathsf{I}_{\mathsf{mayo}}$ outputs a preimage after retrying x^v until $\mathsf{P}^*(x^v + x^o)$ has full rank. MAYO is EUF-CMA-secure in the ROM [9, Theorem 6] assuming that it follows *no leakage* parameter sets [9, Table 1]. For the parameter sets, x is uniformly distributed over $\mathbb{F}_q^{kn}$ if $\mathsf{I}_{\mathsf{mayo}}$ outputs x without retaking x^v. Let τ be a bound on the probability that $\mathsf{P}^*(x^v + x^o)$ does not have full rank for a random x^v. The no-leakage parameter sets satisfy $\tau \leq 2^{-65}$. We show the EUF-CMA security of MAYO following the no leakage parameter sets in the QROM. [13]

[13] For the other parameter sets, Proposition E.3 applies to MAYO.

Proposition E.6 (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*

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

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

Proof. We apply Theorem 3.1 with defining an intermediate game G'_1. G'_1 is the same as G_1 except that G'_1 aborts and outputs 0 whenever $\mathsf{I}_{\mathsf{mayo}}$ retakes x^v. 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. 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 since $x \leftarrow \mathsf{I}_{\mathsf{mayo}}(y)$ follows $\mathsf{U}(\mathbb{F}_q^{kn})$ if $\mathsf{I}_{\mathsf{mayo}}$ never retakes x^v. Therefore, the view of the adversary is identical in the simulated one with the case that G'_1 does not abort, and thus $\Pr\left[\mathsf{G}_1'^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] \leq \Pr\left[\mathsf{G}_5^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]$ holds. Since the EUF-NMA adversary can simulate G_5, $\Pr\left[\mathsf{G}_5^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] \leq \mathrm{Adv}^{\text{EUF-NMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{mayo}},\mathsf{H}]}(\mathcal{A}_{\mathsf{nma}})$ holds, which yields the claimed bound. □

F Review of Hash-and-sign Signatures

F.1 GPV Framework [29]

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 $x \in \{x \in \mathbb{Z}^m : \|x\| \leq s\sqrt{m}\}$, 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 a collision-resistant PSF (see Definition 2.6) whose security is based on the hardness of the short integer solution (SIS) problem [29, Theorem 4.9].

F.2 Modified CFS Signature [19]

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. We assume that (n,k)-Goppa code over $\mathbb{F}_q$ can decode up to t errors. $\mathcal{X}_{n,\leq t} = \{x \in \mathbb{F}_q^n : 0 < \mathsf{hw}(x) \leq t\}$ 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, an invertible matrix $U \in \mathbb{F}_q^{(n-k)\times(n-k)}$, and a 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)-Goppa code over $\mathbb{F}_q$ can decode up to t errors, which is our assumption, there is a one-to-one correspondence between $\mathcal{X}_{n,\leq t}$ and $\mathcal{Y}_{dec} = \{y \in \mathbb{F}_q^{n-k} : y(U^{-1})^T \text{ is decodable}\}$ (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 $\frac{|\mathcal{Y}_{dec}|}{|\mathbb{F}_q^{n-k}|} = \frac{|\mathcal{X}_{n,\leq t}|}{|\mathbb{F}_q^{n-k}|}$. As shown in [18], $\frac{|\mathcal{X}_{n,\leq t}|}{|\mathbb{F}_q^{n-k}|} \approx \frac{1}{t!}$ holds.

We show that a preimage x output by $\mathsf{HaS}[\mathsf{T}_{\mathsf{cfs}}, \mathsf{H}].\mathsf{Sign}$ follows $\mathsf{U}(\mathcal{X}_{n,\leq t})$. First, $x \leftarrow \mathsf{I}_{\mathsf{cfs}}(y)$ for $y \leftarrow_{\$} \mathcal{Y}_{dec}$ follows $\mathsf{U}(\mathcal{X}_{n,\leq t})$ from the one-to-one correspondance between $\mathcal{X}_{n,\leq t}$ 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 $\mathsf{U}(\mathcal{X}_{n,\leq t})$.

F.3 Wave [20]

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 [16, Definition 2] and we can take a statistical bound on the distinguishing advantage of honestly generated signatures and simulated ones.

F.4 Original/Modified UOV Signature [37, 50]

Let $\mathsf{T}_{\mathsf{uov}} = (\mathsf{Gen}_{\mathsf{uov}}, \mathsf{F}_{\mathsf{uov}}, \mathsf{I}_{\mathsf{uov}})$ (resp., $\mathsf{T}_{\mathsf{muov}} = (\mathsf{Gen}_{\mathsf{muov}}, \mathsf{F}_{\mathsf{muov}}, \mathsf{I}_{\mathsf{muov}})$) be a TDF used in the original (resp., modified) UOV signatures. Note that $\mathsf{Gen}_{\mathsf{uov}} = \mathsf{Gen}_{\mathsf{muov}}$ and $\mathsf{F}_{\mathsf{uov}} = \mathsf{F}_{\mathsf{muov}}$. $\mathsf{Gen}_{\mathsf{uov}}$ generates an invertible affine map $\mathsf{S} \colon \mathbb{F}_q^n \to \mathbb{F}_q^n$ and a multivariate quadratic map $\mathsf{P} : \mathbb{F}_q^n \to \mathbb{F}_q^o$ defined as $\mathsf{P} = (p_1, p_2, \ldots, p_o)$, where

$$p_k(z^v, z^o) = \sum_{i\in[v+o]} \sum_{j\in[v]} \alpha_{i,j}^k z_i z_j,$$

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 $n = v + o$. On input $y \in \mathbb{F}_q^o$, $\mathsf{I}_{\mathsf{uov}}$ chooses $z^v \leftarrow_{\$} \mathbb{F}_q^v$ and outputs $x = \mathsf{S}^{-1}(z^v \| z^o)$ by solving a linear equation system $\mathsf{P}(z^v, \cdot) = y$. There is possibly no solution. In the original UOV signature, $\mathsf{I}_{\mathsf{uov}}$ retries z^v until $\{z^o : \mathsf{P}(z^v, z^o) = y\} \neq \emptyset$ holds or $\mathsf{P}(z^v, \cdot)$ has full rank [10] (see Fig. 15).

Since $x \leftarrow \mathsf{I}_{\mathsf{uov}}(y)$ for $y \leftarrow_\$ \mathbb{F}_q^o$ is not uniformly distributed, it is hard to simulate a signature without using the trapdoor; therefore, the computational indistinguishability of $x \leftarrow \mathsf{I}_{\mathsf{uov}}(y)$ for $y \leftarrow_\$ \mathbb{F}_q^o$ and $x \leftarrow_\$ \mathbb{F}_q^n$, that is, the PS advantage, appears in the security bound (see Proposition E.3).

Modified UOV signature: To solve the above problem, Sakumoto et al. [50] proposed the modified UOV signature. Instead of retaking z^v, the modified UOV signature retakes the randomness r for the hash function. The signing procedure of the modified UOV signature (see Fig. 16) is different from the others. $\mathsf{HaS}[\mathsf{T}_{\mathsf{muov}}, \mathsf{H}]$ using $\mathsf{I}^1_{\mathsf{muov}}$ and $\mathsf{I}^2_{\mathsf{muov}}$ generates a signature as follows: $\mathsf{I}^1_{\mathsf{muov}}$ chooses vinegar variables z^v uniformly at random. Fixing z^v, P becomes a set of linear functions on oil variables z^o. $\mathsf{I}^2_{\mathsf{muov}}$ finds a preimage of $\mathsf{P} \circ \mathsf{S}$ by solving a linear equation system and taking the inverse of S. If there is no solution, $\mathsf{I}^2_{\mathsf{muov}}$ outputs $\perp$ and $\mathsf{HaS}[\mathsf{T}_{\mathsf{muov}}, \mathsf{H}]$ retakes r and executes $\mathsf{I}^2_{\mathsf{muov}}$ again without retaking z^v.

Sakumoto et al. showed that preimages generated by $\mathsf{HaS}[\mathsf{T}_{\mathsf{muov}}, \mathsf{H}].\mathsf{Sign}$ are uniformly distributed over $\mathbb{F}_q^n$. For completeness, we give the proof sketch.

In the beginning, z^v is uniformly chosen, that is, 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 $\mathsf{U}(\mathbb{F}_q^n)$.

In Proposition E.4, we cannot take q'_{sign} as in the other schemes since the probability that $\mathsf{I}_{\mathsf{muov}}(z^v, y)$ outputs $\perp$ varies depending on z^v. We set $q'_{\mathsf{sign}} = q_{\mathsf{retry}} q_{\mathsf{sign}}$, where q_{retry} is a bound on the number of queries to H in each signing query. Let X_i be a random variable for the number of queries to H in i-th queries and $X = \sum_{i=1}^{q_{\mathsf{sign}}} X_i$. We have

$$\Pr[X_i > q_{\mathsf{retry}}] = \sum_{j=1}^{o} p_j (1 - q^{j-o})^{q_{\mathsf{retry}}},$$

where p_j is a probability that $\mathsf{P}(z^v, \cdot)$ has rank j for $z^v \leftarrow_\$ \mathbb{F}_q^v$. It is known that a random $o \times o$ matrix over $\mathbb{F}_q$ has rank $o - a$ for $a \in \{0, 1, \ldots, o\}$ with a probability [6]:

$$\frac{1}{q^{a^2}} \cdot \frac{\prod_{k=1}^{o}(1 - q^{-k}) \prod_{k=a+1}^{o}(1 - q^{-k})}{\prod_{k=1}^{o-a}(1 - q^{-k}) \prod_{k=1}^{a}(1 - q^{-k})}. \tag{11}$$

When we assume that $\mathsf{P}(z^v, \cdot)$ becomes a random $o \times o$ matrix for any z^v, p_j follows Eq. (11). Since $X > q'_{\mathsf{sign}}$ implies $\exists i, X_i > q_{\mathsf{retry}}$, $\Pr[X > q'_{\mathsf{sign}}] \leq q_{\mathsf{sign}} \Pr[X_i > q_{\mathsf{retry}}]$ holds. To determine an appropriate value for $q'_{\mathsf{sign}} = q_{\mathsf{retry}} q_{\mathsf{sign}}$ in the security bound, we need to take q_{retry} such that $q_{\mathsf{sign}} \Pr[X_i > q_{\mathsf{retry}}]$ is negligible for the security parameter.

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

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

Fig. 17: Trapdoor of the modified HFE signature

F.5 Modified HFE Signature [50]

Let $\mathsf{T}_{\mathsf{mhfe}} = (\mathsf{Gen}_{\mathsf{mhfe}}, \mathsf{F}_{\mathsf{mhfe}}, \mathsf{I}_{\mathsf{mhfe}})$ be a TDF used in the modified HFE signature and $\phi\colon K \to \mathbb{F}_q^n$ be a standard linear isomorphism $\phi(a_0+a_1x+\cdots+a_{n-1}x^{n-1}) = (a_0, a_1, \ldots, a_{n-1})$, where $K = \mathbb{F}_q[x]/g(x)$ for an irreducible polynomial $g(x)$ of degree n. $\mathsf{Gen}_{\mathsf{mhfe}}$ 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 $\mathsf{F}_{\mathsf{mhfe}}$ and $(\mathsf{P}, \mathsf{S}, \mathsf{S}')$ as $\mathsf{I}_{\mathsf{mhfe}}$. On input $y \in \mathbb{F}_q^{n-m}$, $\mathsf{I}_{\mathsf{mhfe}}$ computes a preimage $x \in \mathbb{F}_q^n$ as in Fig. 17.

As in the modified UOV signature, the authors of [50] showed that preimages generated by $\mathsf{HaS}[\mathsf{T}_{\mathsf{mhfe}}, \mathsf{H}].\mathsf{Sign}$ are uniformly distributed over $\mathbb{F}_q^n$. We give the proof sketch.

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

F.6 MAYO [9]

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 map $\mathsf{P}\colon \mathbb{F}_q^n \to \mathbb{F}_q^m$ with a subspace $\mathcal{O} \subset \mathbb{F}_q^n$ of dimension o called *oil space* such that $\mathsf{P}(x) = 0$ for any $x \in \mathcal{O}$, and outputs P as $\mathsf{F}_{\mathsf{mayo}}$ and a basis of $\mathcal{O}$ as $\mathsf{I}_{\mathsf{mayo}}$. [14] 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

[14] The notation of UOV in MAYO follows [8] which is a generalization of the traditional description of Appendix F.4.

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

$\mathsf{P}^*(x_1, \dots, x_k) \coloneqq \sum_{i\in[k]} E_{i,i}\mathsf{P}(x_i) + \sum_{(i,j)\in\mathcal{I}} E_{i,j}\mathsf{P}'(x_i, x_j)$
repeat
  $x^v \leftarrow_\$ (\mathbb{F}_q^{n-m} \times 0^m)^k$
until $\mathsf{P}^*(x^v + x^o)$ *has full rank*
$x^o \leftarrow \{x^o : \mathsf{P}^*(x^v + x^o) = y\}$
$x = x^v + x^o$
return x

Fig. 18: Trapdoor of MAYO

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 $\mathsf{P}'(x, y) = (p'_1(x, y), \dots, p'_m(x, y))$.

Let $\mathcal{I} = \{(i, j) \in [k] \times [k] : i \le j\}$ and $\{E_{ij}\}_{(i,j)\in\mathcal{I}}$ be a set of invertible matrices such that $E = \{E_{i,j}\}$ is nonsingular. We set $\{E_{ij}\}_{(i,j)\in\mathcal{I}}$ as a system parameter. On input $x = (x_1, \dots, x_k) \in \mathbb{F}_q^{kn}$, $\mathsf{F}_{\mathsf{mayo}}$ 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, $\mathsf{P}^* : \mathbb{F}_q^{kn} \to \mathbb{F}_q^m$ 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 $x^* = (x_1^*, \dots, x_k^*)$ satisfying $\sum_{i\in[k]} E_{i,i}\mathsf{P}(x_i^*) + \sum_{(i,j)\in\mathcal{I}} E_{i,j}\mathsf{P}'(x_i^*, x_j^*)$ [9, Definition 4]. On input $y \in \mathbb{F}_q^m$, $\mathsf{I}_{\mathsf{mayo}}$ computes x as in Fig. 18. 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 $(\mathbb{F}_q^{n-o} \times \{0^o\})^k \subset \mathbb{F}_q^{kn}$, where 0^o denotes a vector of o 0s. Fixing x^v, $\mathsf{P}^*(x^v + x^o) = y$ becomes a linear system of equations for x^o. If $\mathsf{P}^*(x^v + x^o)$ has full rank, $\mathsf{I}_{\mathsf{mayo}}$ outputs $x^v + x^o$ by solving $\mathsf{P}^*(x^v + x^o) = y$. Otherwise, $\mathsf{I}_{\mathsf{mayo}}$ retakes x^v. The probability that $\mathsf{P}^*(x^v + x^o)$ does not have full rank is bounded by $\tau = \frac{q^{k-n+o} + q^{m-ko}}{q-1}$ [9, Lemma 2]. For *no leakage* parameter sets [9, Table 1], $\tau \le 2^{-65}$ holds.

A preimage $x \leftarrow \mathsf{I}_{\mathsf{mayo}}(y)$ is uniform over $\mathbb{F}_q^{kn}$ if $\mathsf{I}_{\mathsf{mayo}}$ does not retake x^v in the signature generation [9, Lemma 7]. Since this property is necessary for applying Theorem 3.1, we show the proof sketch.

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

G Reductions of M-INV⇒M-EUF-CMA and M-CR⇒M-sEUF-CMA

First, we have the following as an extension of Theorem 3.1.

Lemma G.1 (M-INV ⇒ M-EUF-CMA). *For any quantum* M-EUF-CMA *adversary* $\mathcal{A}_{\mathsf{cma^m}}$ *of* $\mathsf{HaS^{ph}}[\mathsf{T_{wpsf}}, \mathsf{H}, \mathsf{E}]$ *with* q_{key} *keys and issuing at most* q_{sign} *classical queries to the signing oracle and* q_{qro} *(quantum) random oracle queries*

Game: M-EUF-NMA

for $j \in [q_{\mathsf{key}}]$ **do**

$\quad (vk_j, sk_j) \leftarrow \mathsf{Sig.KeyGen}(1^\lambda)$

$(j^*, m^*, \sigma^*) \leftarrow \mathcal{A}_{\mathsf{nma^m}}(\{vk_j\}_{j \in [q_{\mathsf{key}}]})$

return $\mathsf{Sig.Verify}(vk_{j^*}, m^*, \sigma^*)$

Fig. 19: M-EUF-NMA (Multi-key EUF-NMA) game

to $\mathsf{H} \leftarrow_\$ \mathcal{Y}^{\mathcal{U}\times\mathcal{R}\times\mathcal{M}}$*, there exist an* M-INV $\mathcal{B}_{\mathsf{inv^m}}$ *of* $\mathsf{T_{wpsf}}$ *with* q_{inst} *instances and an* M-PS *adversary* $\mathcal{D}_{\mathsf{ps^m}}$ *of* $\mathsf{T_{wpsf}}$ *with* q_{key} *instances and issuing* q_{sign} *sampling queries such that*

$$\mathrm{Adv}^{\text{M-EUF-CMA}}_{\mathsf{HaS^{ph}}[\mathsf{T_{wpsf}},\mathsf{H},\mathsf{E}]}(\mathcal{A}_{\mathsf{cma^m}}) \leq (2q_{\mathsf{qro}}+1)^2 \mathrm{Adv}^{\text{M-INV}}_{\mathsf{T_{wpsf}}}(\mathcal{B}_{\mathsf{inv^m}}) + \mathrm{Adv}^{\text{M-PS}}_{\mathsf{T_{wpsf}}}(\mathcal{D}_{\mathsf{ps^m}})$$
$$+ \frac{3}{2} q'_{\mathsf{sign}} \sqrt{\frac{q'_{\mathsf{sign}} + q_{\mathsf{qro}} + 1}{|\mathcal{R}|}} + 2(q_{\mathsf{sign}} + q_{\mathsf{qro}} + 2)\sqrt{\frac{q'_{\mathsf{sign}} - q_{\mathsf{sign}}}{|\mathcal{R}|}} + \frac{q^2_{\mathsf{key}}}{|\mathcal{U}|}, \quad (12)$$

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* $\mathcal{B}_{\mathsf{inv^m}}$ *and* $\mathcal{D}_{\mathsf{ps^m}}$ *are about that of* $\mathcal{A}_{\mathsf{cma^m}}$*.*

Proof. We prove two reductions; M-EUF-NMA ⇒ M-EUF-CMA and M-INV ⇒ 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. 19 as $\mathrm{Adv}^{\text{M-EUF-NMA}}_{\mathsf{Sig}}(\mathcal{A}_{\mathsf{nma^m}}) = \Pr[\mathsf{M\text{-}EUF\text{-}NMA}^{\mathcal{A}_{\mathsf{nma^m}}} \Rightarrow 1]$. 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 ⇒ M-EUF-CMA*:*

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

Game G_1 (adaptive reprogramming and puncturing of H): In the same manner as G_4 of Theorem 3.1, 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 $= \top$. Also, the signing oracle reprograms $\mathsf{H} := \mathsf{H}^{(\mathsf{E}(\mathsf{F}_j), r_i, m_i) \mapsto y_i}$ after repeating $r_i \leftarrow \mathcal{R}$ and $y_i \leftarrow_\$ \mathcal{Y}$ until $\mathsf{I}_j(y_i)$ does not output $\perp$.

By analyzing the number of queries to H, the number of times H is reprogrammed, and the number of punctured points of H, we can derive the bounds on the advantage gaps of $\mathsf{G}_0/\mathsf{G}_1$, $\mathsf{G}_1/\mathsf{G}_2$, and $\mathsf{G}_3/\mathsf{G}_4$ in Theorem 3.1. Since these numbers are the same in both the single-key and multi-key settings, we can apply the same bound as $\mathsf{G}_0/\mathsf{G}_4$ in Theorem 3.1. Thus, we have

$$\left|\Pr\left[\mathsf{G}_0^{\mathcal{A}_{\mathsf{cma}^\mathsf{m}}}\Rightarrow 1\right]-\Pr\left[\mathsf{G}_1^{\mathcal{A}_{\mathsf{cma}^\mathsf{m}}}\Rightarrow 1\right]\right| \leq \frac{3}{2}q'_{\mathsf{sign}}\sqrt{\frac{q'_{\mathsf{sign}}+q_{\mathsf{qro}}+1}{|\mathcal{R}|}} + 2(q_{\mathsf{sign}}+q_{\mathsf{qro}}+2)\sqrt{\frac{q'_{\mathsf{sign}}-q_{\mathsf{sign}}}{|\mathcal{R}|}}.$$

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 $\mathsf{SampDom}$, $\Pr\left[\mathsf{G}_2^{\mathcal{A}_{\mathsf{cma}^\mathsf{m}}}\Rightarrow 1\right] \leq \mathrm{Adv}^{\text{M-EUF-NMA}}_{\mathsf{HaS}^{\mathsf{ph}}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H},\mathsf{E}]}(\mathcal{A}_{\mathsf{nma}^\mathsf{m}})$ 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 A.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 of S 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 A.2, we have

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

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. (12) by combining the two reductions. □

Next, we show a reduction M-CR ⇒ M-sEUF-CMA extending the single-key version of [13, Theorem 2].

Lemma G.2 (M-CR ⇒ M-EUF-CMA). *For any quantum* M-sEUF-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-CR $\mathcal{B}_{\mathsf{cr}^{\mathsf{m}}}$ *of* $\mathsf{T}_{\mathsf{wpsf}}$ *with* q_{inst} *instances such that*

$$\mathrm{Adv}^{\text{M-sEUF-CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \leq \frac{1}{1-2^{-\omega(\log(\lambda))}} \mathrm{Adv}^{\text{M-CR}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{B}_{\mathsf{cr}^{\mathsf{m}}}) + \frac{q_{\mathsf{key}}^2}{|\mathcal{U}|}, \tag{13}$$

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* $\mathcal{B}_{\mathsf{cr}^{\mathsf{m}}}$ *and* $\mathcal{D}_{\mathsf{st}}$ *are about that of* $\mathcal{A}_{\mathsf{cma}^{\mathsf{m}}}$*.*

Proof. We define a sequence of games as follows:

- Game G_0 (M-sEUF-CMA game): This is the original M-sEUF-CMA game and $\Pr\left[\mathsf{G}_0^{\mathcal{A}_{\mathsf{cma}^{\mathsf{m}}}} \Rightarrow 1\right] = \mathrm{Adv}^{\text{M-sEUF-CMA}}_{\mathsf{HaS}^{\mathsf{ph}}[\mathsf{T}_{\mathsf{psf}},\mathsf{H},\mathsf{E}]}(\mathcal{A}_{\mathsf{cma}^{\mathsf{m}}})$ 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 $\left|\Pr\left[\mathsf{G}_0^{\mathcal{A}_{\mathsf{nma}^{\mathsf{m}}}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_1^{\mathcal{A}_{\mathsf{nma}^{\mathsf{m}}}} \Rightarrow 1\right]\right| \leq \frac{q_{\mathsf{key}}^2}{|\mathcal{U}|}$.
- 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' follow the same distribution, $\Pr\left[\mathsf{G}_1^{\mathcal{A}_{\mathsf{nma}^{\mathsf{m}}}} \Rightarrow 1\right] = \Pr\left[\mathsf{G}_2^{\mathcal{A}_{\mathsf{nma}^{\mathsf{m}}}} \Rightarrow 1\right]$ holds.

The M-CR adversary $\mathcal{B}_{\mathsf{cr}^{\mathsf{m}}}$ can simulate G_2. As in Lemma G.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 $\mathcal{B}_{\mathsf{cr}^{\mathsf{m}}}$ can simulate the signing oracle. When responding to the i-th signing query m_i for the j-th verification key F_j, $\mathcal{B}_{\mathsf{cr}^{\mathsf{m}}}$ 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 the game by submitting (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 $1 - 2^{-\omega(\log(\lambda))}$, and we thus have Eq. (13). □

H Proof of Lemma 4.1

We extend the proof of Lemma G.1 (Appendix G) by defininh a new game G_5. In G_5, the verification keys $\{\mathsf{F}_j\}_{j\in[q_{\mathsf{key}}]}$ 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 the verification keys as the results of querying $\mathsf{NewKey}b$. If $\mathcal{D}_{\mathsf{st}}$ plays ST_0, G_4 is simulated; otherwise, G_5 is simulated. Consequently, we have $\left|\Pr\left[\mathsf{G}_4^{\mathcal{A}_{\mathsf{nma^m}}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_5^{\mathcal{A}_{\mathsf{nma^m}}} \Rightarrow 1\right]\right| \leq \mathrm{Adv}^{\mathrm{ST}}_{\mathsf{T}_{\mathsf{wpsf}},\mathsf{T}'}(\mathcal{D}_{\mathsf{st}})$.

To use Lemma A.2, we assume that $\mathcal{B}_{\mathsf{inv}}$ runs a two-stage algorithm S in G_5 with input θ (see Fig. 10). As in Lemma G.1, $\mathcal{B}_{\mathsf{inv}}$ has knowledge of the target key for the observed random oracle query. When the observed value is targeted at j'-th verification key, $\mathcal{B}_{\mathsf{inv}}$ sets $\theta := \mathsf{L}_{j'}(y)$ as the input to S. Since $\mathsf{L}_{j'}$ is bijective, $\mathsf{L}_{j'}(y)$ for $y \leftarrow_{\$} \mathcal{Y}$ is uniformly distributed. 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, $\mathsf{F}(\mathsf{R}_{j^*}(x^*)) = y$ holds. Therefore, $\mathcal{B}_{\mathsf{inv}}$ can win the INV game by submitting $\mathsf{R}_{j^*}(x^*)$, and we have $\Pr\left[\mathsf{G}_5^{\mathcal{A}_{\mathsf{nma^m}}} \Rightarrow 1\right] \leq (2q_{\mathsf{qro}}+1)^2 \mathrm{Adv}^{\mathrm{INV}}_{\mathsf{T}'}(\mathcal{B}_{\mathsf{inv}})$ from Lemma A.2, which proves this lemma. □

I Proof of Lemma 4.2

To prove a reduction of CR ⇒ M-CR, we define a sequence of games as follows:

Game G_0 (M-CR game): This is the original M-CR game and $\Pr\left[\mathsf{G}_0^{\mathcal{B}_{\mathsf{cr^m}}} \Rightarrow 1\right] = \mathrm{Adv}^{\text{M-CR}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{B}_{\mathsf{cr^m}})$ holds.

Game G_1 (replacing verification keys): We replace F_j with $\mathsf{L}_j \circ \mathsf{F}' \circ \mathsf{R}_j$. Since the ST adversary can simulate $\mathsf{G}_0/\mathsf{G}_1$, we have $\left|\Pr\left[\mathsf{G}_0^{\mathcal{B}_{\mathsf{cr^m}}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_1^{\mathcal{B}_{\mathsf{cr^m}}} \Rightarrow 1\right]\right| \leq \mathrm{Adv}^{\mathrm{ST}}_{\mathsf{T}_{\mathsf{psf}},\mathsf{T}'}(\mathcal{D}_{\mathsf{st}})$.

The CR adversary $\mathcal{B}_{\mathsf{cr}}$ simulates G_1 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 $\mathcal{B}_{\mathsf{cr^m}}$. When $\mathcal{B}_{\mathsf{cr^m}}$ submits (j^*, x_1^*, x_2^*), $\mathcal{B}_{\mathsf{cr}}$ 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 and $x_1^* \neq x_2^*$ implies $\mathsf{R}_{j^*}(x_1^*) \neq \mathsf{R}_{j^*}(x_2^*)$. Therefore, $\mathcal{B}_{\mathsf{cr}}$ can win the CR game and can perfectly simulate G_4. Therefore, we have

$$\mathrm{Adv}^{\text{M-CR}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{B}_{\mathsf{cr^m}}) \leq \mathrm{Adv}^{\mathrm{CR}}_{\mathsf{T}'}(\mathcal{B}_{\mathsf{cr}}) + \mathrm{Adv}^{\mathrm{ST}}_{\mathsf{T}_{\mathsf{psf}},\mathsf{T}'}(\mathcal{D}_{\mathsf{st}}). \tag{14}$$

Combining Eq. (14) with Eq. (13) of Lemma G.2 (Appendix G), we obtain the security bound of Lemma 4.2. □

J Applications of Generic Method in Multi-key Setting

In this section, we explore the applications of the generic method presented in Lemma 4.2 for lattice-based cryptography and Lemma 4.1 for code-based and MQ-based cryptography. Rather than focusing on specific schemes such as FALCON [49], our paper applies the generic method to frameworks of the schemes, such as the GPV framework [29]. We leave the applicability to the specific schemes for future works.

Lattice-based Cryptography: We apply the generic method to the GPV framework (see Appendix F.1) [29]. For Lemma 4.2, 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 is bounded by an advantage of the following problem.

Definition J.1 (Multi-instance Signed Permutation Equivalence). *Given matrices $\{G_j\}_{j\in[q_{\mathsf{inst}}]}$ ($G_j \in \mathbb{F}_q^{n\times m}$), do there exist a matrix $G \in \mathbb{F}_q^{n\times m}$, $n \times n$ 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 [48]. The code equivalence is defined as: Given a pair of 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*)[52].

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 [48]. Also, there are some algorithms for the permutation equivalence and linear equivalence. In the general case, Leon's algorithm solves the problems by enumerating all the codewords with Hamming weight w for some w [38], and Beullens [7] recently improved this algorithm. The complexity of this approach grows exponentially with w, and we cannot solve the problems with low w [3]. There is a special case where we can easily solve the permutation equivalence with the Support Splitting Algorithm (SSA) proposed by Sendrier [51]. The SSA runs in $O(m^3 + m^2 q^h \ln(m))$, where h is a dimension of the hull space of a code, that is, the intersection between the code and its dual code [3]. Therefore, the SSA can efficiently solve the permutation equivalence if the dimension of the hull space is low. Note that the SSA does not apply to the case with an empty hull.

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 F.2 and F.3). For Lemma 4.1, 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 is bounded by an advantage of the following problem.

Definition J.2 (Multi-instance Linear Equivalence). *Given matrices $\{G_j\}_{j\in[q_{\mathsf{inst}}]}$ ($G_j \in \mathbb{F}_q^{n\times m}$), do there exist a matrix $G \in \mathbb{F}_q^{n\times m}$, $n \times n$ invert-*

ible 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 mentioned in the previous paragraph, some algorithms exist for the (single-instance) linear equivalence.

Multivariate-quadratic-based Cryptography: We assume a TDF of the original/-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 a multivariate quadratic map ($n' \geq n$). For Lemma 4.1, 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 is bounded by an advantage of the following game.

Definition J.3 (Multi-instance Decision Morphism of Polynomials). *Given multivariate quadratic maps* $\{\mathsf{F}_j\}_{j\in[q_{\mathsf{inst}}]}$*, do there exist a multivariate quadratic map* F *and 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, that is, given a pair of multivariate quadratic maps $(\mathsf{F}, \mathsf{F}')$, do there exist affine maps L and R such that $\mathsf{F}' = \mathsf{L} \circ \mathsf{F} \circ \mathsf{R}$?, is proven NP-complete [47]. 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 [47]. For signature schemes with some structures in their verification key, only invertible R may preserve the structures, e.g., only block-anti-circulant matrices can maintain a structure of BAC-UOV [54]; therefore, we need to use invertible R as in the decision isomorphism of polynomials for such signature schemes.

A search version of the isomorphism of polynomials has been well-studied. Bouillaguet, Fouque, and Véber [14] studied and surveyed the algorithms for the isomorphism of polynomials. Their algorithms run in $O(q^n) \cdot \mathsf{poly}(n, q)$, $O(q^{2n/3}) \cdot \mathsf{poly}(n, q)$, or $O(q^{n/2}) \cdot \mathsf{poly}(n, q)$ assuming that $n = m$. The Gröbner-based algorithm proposed by Faugère and Perret [26] can efficiently solve random instances of an *inhomogeneous* version of the problem. We also note that if L and R are very structured, then the problems become easier (see, e.g., [34]).