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., Sakamoto 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.


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) [31]. 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 [5, 6]
is a widely adopted paradigm for constructing practical signatures, along with Fiat-Shamir [28], in the ROM [5]. This paper focuses on hash-and-sign.

A hash-and-sign signature scheme is realized by a hard-to-invert function $F : \mathcal{X} \rightarrow \mathcal{Y}$, its trapdoor $I : \mathcal{Y} \rightarrow \mathcal{X}$, and a hash function $H : \{0,1\}^* \rightarrow \mathcal{Y}$ modeled as a random oracle. To sign on a message $m$, a signer first computes $y = H(r, m)$, where $r$ is a random string, computes $x = I(y)$, and outputs $\sigma = (r, x)$ as a signature. A verifier verifies the signature $\sigma$ with the verification key $F$ by checking if $H(r, m) = F(x)$ 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 [5].$^3$ Gentry, Peikert, and Vaikuntanathan proposed FDH and probabilistic FDH (PFDH) signatures with a preimage-sampleable function (PSF) [30], 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 $y = H(r, m)$. The Courtois-Finiasz-Sendrier (CFS) signature [19] in code-based cryptography and the Unbalanced Oil and Vinegar (UOV) [38] and Hidden Field Equations (HFE) signatures [48] 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 [55]. Consequently, there has been a growing interest in post-quantum cryptography (PQC). Recently NIST selected PQC candidates of public-key encryption/key-encapsulation mechanism (KEM) and digital signature for standardization [47]. Furthermore, NIST initiated an additional call for PQC digital signatures [46]. In the context of PQC, it is essential for signature schemes to provide EUF-CMA security in the QROM (Quantum Random Oracle Model) [14] since it models real-world quantum adversaries having 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 [59].

**Table 1** summarizes studies on the EUF-CMA security of hash-and-sign signatures in the QROM. Boneh et al. [14] showed a tight reduction from the CR of PSF using the history-free reduction. Zhandry [61] gave a reduction from

---

$^3$ An adversary tries to find a preimage of a challenge $y$ that is uniformly chosen in the INV game [33] and that derived by $F(x)$ for $x$ chosen from some distribution on $\mathcal{X}$ in the OW game [5].
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. $\epsilon$ 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.

<table>
<thead>
<tr>
<th>Name</th>
<th>DHaS</th>
<th>PHaS</th>
<th>PHaSwR</th>
<th>Assumption</th>
<th>Security Bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>[14]</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>CR</td>
<td>$O(\epsilon_{\text{cr}})$</td>
</tr>
<tr>
<td>ext. of [58]</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>OW/INV</td>
<td>$O(q^2\sqrt{\epsilon_{\text{ow/inv}}})$</td>
</tr>
<tr>
<td>[17]</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>EUF-NMA</td>
<td>$O(\epsilon_{\text{nma}})$</td>
</tr>
<tr>
<td>Ours</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>INV</td>
<td>$O(q^2\epsilon_{\text{inv}})$</td>
</tr>
</tbody>
</table>

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\(^6\) 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\(^5\) [58], we obtain a reduction from the OW/INV of PSF. Chailloux and Debris-Alazard\(^6\) gave a security proof of the probabilistic hash-and-sign based on non-PSF TDFs. Also, Grilo, Hövelmanns, Hülsing, and Majenz\(^6\) gave a reduction from the EUF-RMA security of a signature scheme for fixed-length messages, where RMA stands for Random-Message Attack. 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. 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 PSF, tight reductions exist both from OW to INV and from INV to OW.

\(^5\) Zhandry\(^6\) 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 $m' = H(r, m)$, and signs on $m'$ by using a signing algorithm of the signature scheme for fixed-length messages, and outputs $(r, \sigma)$. 

---

3
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 [45] 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 as part of the input for the hash function 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 [43]. 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 $\text{sEUF-CMA}$-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 [61, 17, 58]. Fig. 1 shows a diagram of the reduction. The main theorem comprises two reductions; EUF-NMA $\Rightarrow$ EUF-CMA
and INV ⇒ EUF-NMA, where X ⇒ Y indicates a reduction from X to Y. The main theorem has a security bound $(2q_{qro} + 1)^2 \epsilon_{inv}$, where $q_{qro}$ is a bound on the number of random oracle queries and $\epsilon_{inv}$ is an advantage of the INV game.

**Proof Idea:** We provide a technical overview of the main theorem: To prove EUF-NMA ⇒ EUF-CMA, we first reprogram the random function to simulate the signing oracle. We employ the tight adaptive reprogramming technique [32]. Given a message $m$, the signing oracle repeatedly reprograms $H$ such that $H(r, m) = y$ holds for randomly chosen $(r, y) \in \mathcal{R} \times \mathcal{Y}$, and this reprogramming continues until the trapdoor $I$ can provide a preimage $x \in X$ of $y$ ($F(x) = y$). In this context, we assume that the following two values are indistinguishable:

- $x$ obtained after retrying $y$ until $y$ becomes invertible by the trapdoor $I$.
- $x$ obtained by a simulator that does not use $I$.

If the reprogramming during retries can be canceled, the signing oracle can be simulated by outputting $(r, x)$ and reprogramming $H$ such that $H(r, m) = F(x)$ holds. Unfortunately, a cancelation using the tight adaptive reprogramming technique introduces a bias in the distribution of the random function. We carefully cancel the reprogramming during retries using the semi-classical One-way to Hiding lemma [1]. After this cancelation, the EUF-NMA adversary can simulate the signing oracle in the absence of the signing key $I$.

As for INV ⇒ EUF-NMA, we use the measure-and-reprogram technique developed by Don et al. [23], incurring a security loss of $(2q_{qro} + 1)^2$. As far as we know, this usage is new in the context of the probabilistic hash-and-sign.

**Applications:** Applying the main theorem, we enhance the EUF-CMA security of Wave [2] and give the first proof for the sEUF-CMA security of the modified CFS signature [20] as well as the EUF-CMA security of Rainbow [22], GeMSS [16], MAYO [10], QR-UOV [29], and PROV [26] in the QROM. To the best of our knowledge, the main theorem encompasses all existing hash-and-sign signatures such that reductions from the INV are known in the ROM.

NIST has recently announced additional candidates for post-quantum signatures. NIST has the intention of standardizing schemes that are not based on structured lattices [46]. The main theorem has wide application in code-based and MQ-based cryptography, promising candidate for this call. The additional candidates include Wave, MAYO, QR-UOV, and PROV. Notably, QR-UOV and PROV have utilized the main theorem in their specifications [29, 26].

**Security Proof in Multi-Key Setting:** We introduce 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 core idea behind this generic method is to apply pairs of randomly generated transformations $\{L_j, R_j\}_j$ to a single verification key $F'$. Here, $F'$ belongs to another TDF, assumed to be non-invertible. This process effectively simulates multiple verification keys through $\{L_j \circ F' \circ R_j\}_j$. Assuming the indistinguishability between $\{L_j \circ F' \circ R_j\}_j$ and real verification keys $\{F_j\}_j$, we show a reduction.
of INV ⇒ M-EUF-CMA with a security bound \((2q_{qro} + 1)^2\epsilon_{inv}\) and a tight reduction of CR ⇒ 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 computationally ensure the indistinguishability between \(\{L_j \circ F \circ R_j\}_j\) and \(\{F_j\}_j\).

Concurrent Work: Liu, Jiang, and Zhao [40] 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 \((2(q_{qro} + q_{sign} + 1) + 1)^2\epsilon_{inv}\), 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, the 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, the main theorem has the security bound \((2q_{qro} + 1)^2\epsilon_{inv}\), which does not include \(q_{sign}\).

Two papers [21, 3] recently pointed out a subtle flaw in the security proofs of Fiat-Shamir with aborts [41] in the QROM [36, 32]. The flaw stems from the bias introduced by the simulation with abort, which we treat in EUF-NMA ⇒ EUF-CMA carefully. We note that the games in the corrected proof in [3] are defined in the same spirit as our proof of EUF-NMA ⇒ EUF-CMA while the proof techniques and the details are different. Leveraging its structural resemblance to the probabilistic hash-and-sign with retry, we present an alternative security proof for the Fiat-Shamir with aborts by employing the same techniques used in the main theorem of this paper.

Organization: Section 2 gives notations, definitions, and so on. Section 3 reviews the existing security proofs in the (Q)ROM. Section 4 presents the main theorem and discusses applications. In Section 5, we describe the generic method applied in the multi-key setting. Appendix A demonstrates a flaw in the security proof of concurrent work. Appendix B presents security proofs of hash-and-sign signatures reviewed in Appendix C. Appendices D and E show missing proofs for the theorem in the multi-key setting. Appendix F shows applications of the generic method in the multi-key setting. Appendix G provides a security proof for the Fiat-Shamir with aborts, employing the same techniques as the main theorem.

2 Preliminaries

2.1 Notations and Terminology

For \(n \in \mathbb{N}\), we let \([n] := \{1, \ldots, n\}\). We write any symbol for sets in calligraphic font. For a finite set \(\mathcal{X}\), \(|\mathcal{X}|\) is the cardinality of \(\mathcal{X}\) and \(U(\mathcal{X})\) is the uniform distribution over \(\mathcal{X}\). By \(x \leftarrow \mathcal{X}\) and \(x \leftarrow D_\mathcal{X}\), we denote the sampling of an element from \(U(\mathcal{X})\) and \(D_\mathcal{X}\) (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 $A$ be an adversary. We denote by $y \leftarrow F^H(x)$ and $y \leftarrow A^H(x)$ (resp., $y \leftarrow F^H(x)$ and $y \leftarrow A^H(x)$) probabilistic computations of $F$ and $A$ on input $x$ with a classical (resp., quantum) oracle access to a function $H$. If $F$ and $A$ are deterministic, we write $y := F^H(x)$ and $y := A^H(x)$. For a random function $H$, we denote by $H^{x \mapsto y}$ a function such that $H^{x \mapsto y}(x) = H(x)$ for $x \neq x^*$ and $H^{x \mapsto y}(x^*) = y^*$. The notation $G^A \Rightarrow y$ denotes an event in which a game $G$ played by $A$ returns $y$.

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

### 2.2 Digital Signature and Trapdoor Function

**Definition 2.1 (Digital Signature).** A digital signature scheme $\text{Sig}$ consists of three algorithms:

1. $\text{Sig.KeyGen}(1^\lambda)$: This algorithm takes the security parameter $1^\lambda$ as input and outputs a verification key $vk$ and a signing key $sk$.
2. $\text{Sig.Sign}(sk, m)$: This algorithm takes a signing key $sk$ and a message $m$ as input and outputs a signature $\sigma$.
3. $\text{Sig.Verify}(vk, m, \sigma)$: This algorithm takes a verification key $vk$, a message $m$, and a signature $\sigma$ as input, and outputs $\top$ (acceptance) or $\bot$ (rejection).

**Definition 2.2 (Security of Signature).** Let $\text{Sig}$ 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 $\text{Sig}$ as $\text{Adv}_{\text{Sig}}^{\text{EUF-CMA}}(A_{\text{nma}}) = \Pr[\text{EUF-CMA}_{\text{A_{nma}}} \Rightarrow 1]$ and $\text{Adv}_{\text{Sig}}^{\text{EUF-NMA}}(A_{\text{nma}}) = \Pr[\text{EUF-NMA}_{\text{A_{nma}}} \Rightarrow 1]$, respectively. Also, we define an advantage function for an sEUF-CMA (strong EUF-CMA) game as $\text{Adv}_{\text{Sig}}^{\text{sEUF-CMA}}(A_{\text{nma}}) = \Pr[\text{sEUF-CMA}_{\text{A_{nma}}} \Rightarrow 1]$, where the sEUF-CMA game is identical to the EUF-CMA game except that Line 4 is changed as “if $(m^*, \sigma^*) \in Q'$ then” and $Q'$ keeps messages and signatures in the signing oracle. We say $\text{Sig}$ 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.
Game: INV
1 \((F, I) \leftarrow \text{Gen}(1^\lambda)\)
2 \(y \leftarrow \mathcal{Y}\)
3 \(x^* \leftarrow B_{\text{inv}}(F, y)\)
4 return \(F(x^*) = y\)

Game: OW
1 \((F, I) \leftarrow \text{Gen}(1^\lambda)\)
2 \(x \leftarrow \mathcal{D}_X\)
3 \(y := F(x)\)
4 \(x^* \leftarrow B_{\text{ow}}(F, y)\)
5 return \(F(x^*) = y\)

Game: CR
1 \((F, I) \leftarrow \text{Gen}(1^\lambda)\)
2 \((x^*_1, x^*_2) \leftarrow B_{\text{cr}}(F)\)
3 return \(F(x^*_1) = F(x^*_2)\)

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

Definition 2.3 (Trapdoor Function (TDF)). A TDF \(T\) consists of three algorithms:
- \(\text{Gen}(1^\lambda)\): This algorithm takes the security parameter \(1^\lambda\) as input and outputs a function \(F\) with a trapdoor \(I\) of \(F\).
- \(F(x)\): This algorithm takes \(x \in \mathcal{X}\) and deterministically outputs \(F(x) \in \mathcal{Y}\).
- \(I(y)\): This algorithm takes \(y \in \mathcal{Y}\) and outputs \(x \in \mathcal{X}\), s.t., \(F(x) = y\), or outputs \(\perp\).

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), OW (One-Wayness), and CR (Collision-Resistance) games against \(T\) as \(\text{Adv}^{\text{INV}}_T(B_{\text{inv}}) = \Pr[\text{INV}_{B_{\text{inv}}} \Rightarrow 1]\), \(\text{Adv}^{\text{OW}}_T(B_{\text{ow}}) = \Pr[\text{OW}_{B_{\text{ow}}} \Rightarrow 1]\), and \(\text{Adv}^{\text{CR}}_T(B_{\text{cr}}) = \Pr[\text{CR}_{B_{\text{cr}}} \Rightarrow 1]\), respectively.

2.3 Preimage-Sampleable Function

In the ROM, hash-and-sign is EUF-CMA-secure when instantiated with a preimage-sampleable function (PSF) [30]. 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 \(\text{SampDom}(F)\), which takes as input \(F \in \mathcal{Y}^\lambda\) and outputs some \(x \in \mathcal{X}\).

We then review PSF:

Definition 2.6 (Preimage-Sampleable Function (PSF) [30]). A WPSF \(T\) is said to be a PSF if it satisfies three conditions for any \((F, I) \leftarrow \text{Gen}(1^\lambda)\):

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

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

\(^7\) In general, non-invertibility of TDFs is called one-wayness [30, 52, 17]. We make a distinction between them depending on the way to choose challenges (INV follows [33] and OW follows [5]).
\begin{itemize}
\item Game: PS
\begin{itemize}
\item \(1 (F, 1) \leftarrow \text{Gen}(1^\lambda)\)
\item \(2 b^* \leftarrow T_{\text{Sample}}(F)\)
\item a return \(b^*\)
\end{itemize}
\item Sample\(_0()\)
\begin{itemize}
\item \(1 \text{ repeat}\)
\item \(2 y_i \leftarrow \mathcal{Y}\)
\item \(3 x_i \leftarrow I(y_i)\)
\item \(4 \text{ until } x_i \neq \perp\)
\item \(5 \text{ return } x_i\)
\end{itemize}
\item Sample\(_1()\)
\end{itemize}

Fig. 4: PS (Preimage Sampling) game

**Condition 4:** For any \(y \in \mathcal{Y}\), the conditional min-entropy of \(x \leftarrow \text{SampDom}(F)\) given \(F(x) = y\) 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 \(x \leftarrow \text{SampDom}(F)\) and \(x \leftarrow I(y)\). To define this relaxed condition, we introduce the following 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:

\[
\text{Adv}_{PS}^T(D_{ps}) = \left| \Pr[M_{PS0} \Rightarrow 1] - \Pr[M_{PS1} \Rightarrow 1] \right|
\]

The condition that \(\text{Adv}_{PS}^T(D_{ps})\) 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 [37]).** Let \(\text{Sig}\) 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 \(\text{Sig}\) as:

\[
\text{Adv}_{Sig}^{\text{M-EUF-CMA}}(A_{cma}) = \Pr[M_{\text{EUF-CMA}} \Rightarrow 1] \quad \text{and} \quad \text{Adv}_{Sig}^{\text{M-sEUF-CMA}}(A_{cma}) = \Pr[M_{\text{sEUF-CMA}} \Rightarrow 1],
\]

where the M-EUF-CMA game is identical to the M-EUF-CMA game except that Line 5 is changed as “if \((j^*, m^*, \sigma^*) \in Q'\) then” and \(Q'\) keeps key IDs, messages, and signatures in the signing oracle. We say \(\text{Sig}\) 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:

\[
\text{Adv}_{T}^{\text{M-INV}}(B_{inv}) = \Pr[M_{\text{INV}} \Rightarrow 1], \quad \text{Adv}_{T}^{\text{M-CR}}(B_{cr}) = \Pr[M_{\text{CR}} \Rightarrow 1], \quad \text{and} \quad \text{Adv}_{T}^{\text{M-PS}}(D_{ps}) = \left| \Pr[M_{\text{PS0}} \Rightarrow 1] - \Pr[M_{\text{PS1}} \Rightarrow 1] \right|,
\]

respectively.
We introduce three techniques employed in proving Theorem 4.1.

2.6 Proof Techniques in QROM

we use the semi-classical O2H technique [1].

gramming technique [32] and the measure-and-reprogram technique [23].

Among the works, we use the tight adaptive repro-

H QROM. However, some works enable one to adaptively reprogram

different values, e.g.,

compute the hash values. In the ROM, the challenger can choose

random oracle queries

The challenger computes H and gives a superposition of the results to the adversary, \( \sum_{(r,m)} \alpha_{r,m} |r, m\rangle |y\). 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 [57, 34, 23, 32]. Among the works, we use the tight adaptive reprogramming technique [32] and the measure-and-reprogram technique [23]. Also, we use the semi-classical O2H technique [1].

2.6 Proof Techniques in QROM

We introduce three techniques employed in proving Theorem 4.1.
Tight Adaptive Reprogramming Technique [32]: Fig. 7 shows a game called AR (Adaptive Reprogramming) game, in which the adversary \( D_{ar} \) attempts to distinguish \( H_0 \) (no reprogramming) from \( H_1 \) (reprogrammed by \( \text{Repro} \)). For \( i \)-th reprogramming query, the challenger reprograms \( H_1 \) for \( r_i \leftarrow D_R \) and \( y_i \leftarrow Y \), and gives \( r_i \) to \( D_{ar} \). Let \( \epsilon \) be a bound on the maximum probability of \( r \leftarrow D_R \), that is, \( \max_{r \in R} \Pr[r = \hat{r} : r \leftarrow D_R] \leq \epsilon \). A distinguishing advantage of the AR game is defined by
\[
\text{Adv}_{AR}^{H}(D_{ar}) = \left| \Pr[AR_0^{H} \Rightarrow 1] - \Pr[AR_1^{H} \Rightarrow 1] \right|.
\]

Lemma 2.1 (Tight Adaptive Reprogramming Technique [32, Proposition 2]). For any quantum AR adversary \( D_{ar} \) issuing at most \( q_{\text{rep}} \) classical reprogramming queries and \( q_{\text{qro}} \) (quantum) random oracle queries to \( H_b \), the distinguishing advantage of the AR game is bounded by
\[
\text{Adv}_{AR}^{H}(D_{ar}) \leq \frac{3}{2} q_{\text{rep}} \sqrt{q_{\text{qro}} \epsilon}.
\]
Especially, if \( D_R \) is the uniform distribution \( U(R) \), then \( \epsilon \) is equal to \( \frac{1}{|R|} \).

Measure-and-Reprogram Technique [23]: Let \( A \) be a quantum adversary playing a search-type game making \( q_{\text{qro}} \) quantum queries to \( H \leftarrow Y^{R \times M} \). A two-stage algorithm \( S \) comprises \( S_1 \) and \( S_2 \), and it operates with black-box access to \( A \) as follows:

1. Choose \((i, b) \leftarrow \$ ((q_{\text{qro}}) \times \{0, 1\}) \cup \{(q_{\text{qro}} + 1, 0)\} \).
2. Run \( A \) with \( H \) until \( i \)-th query.
3. Measure \( i \)-th query and output \((r, m)\) as the output of \( S_1 \).
4. Given a random \( \theta \), reprogram \( H' = H^{\langle r, m \rangle \rightarrow \theta} \).
5. If \( i = q_{\text{qro}} + 1 \), then go to Step 8.
6. Answer \( i \)-th query with \( H \) (if \( b = 0 \)) or \( H' \) (if \( b = 1 \)).
7. Run \( A \) with \( H' \) until the end.
8. Output \( A \)'s output \( z \) (possibly quantum) as the output of \( S_2 \).

Then, the following lemma holds for \( S \) and \( A \):

Lemma 2.2 (Measure-and-Reprogram Technique [23, Theorem 2]). For any quantum adversary \( A \) issuing at most \( q_{\text{qro}} \) (quantum) random oracle queries to \( H \leftarrow Y^{R \times M} \), there exists a two-stage algorithm \( S \) given uniformly
chosen \( \theta \) such that for any \( (\hat{r}, \hat{m}) \in \mathcal{R} \times \mathcal{M} \) and any predicate \( \mathcal{V} \),

\[
\Pr\left[(r, m) = (\hat{r}, \hat{m}) \land \mathcal{V}(r, m, \theta, z) : (r, m) \leftarrow \mathcal{S}_1^d(), \ z \leftarrow \mathcal{S}_2^d(\theta)\right] \geq \frac{1}{(2q_{\text{ro}} + 1)^2} \Pr\left[(r, m) = (\hat{r}, \hat{m}) \land \mathcal{V}(r, m, \mathcal{H}(r, m), z) : (r, m, z) \leftarrow \mathcal{A}^{(\mathcal{H})()}\right].
\]

Semi-classical O2H Technique [1]: We define punctured oracle following a notation of [12].

**Definition 2.10 (Punctured Oracle [12, Definition 1]).** Let \( \mathcal{S} \subset \mathcal{R} \times \mathcal{M} \) be a set. Let \( f_\mathcal{S}: \mathcal{R} \times \mathcal{M} \to \{0, 1\} \) be a predicate that returns 1 if and only if \( (r, m) \in \mathcal{S} \). Punctured oracle \( \mathcal{H} \setminus \mathcal{S} (H \text{ punctured by } \mathcal{S}) \) of \( H \in \mathcal{Y}^{\mathcal{R} \times \mathcal{M}} \) runs as follows: on input \((r, m), \) computes whether \((r, m) \in \mathcal{S} \) in an auxiliary qubit \( |f_\mathcal{S}(r, m)\rangle \), measures \( |f_\mathcal{S}(r, m)\rangle \), runs \( H(r, m) \), and returns the result. Let FIND be an event that any of measurements of \(|f_\mathcal{S}(r, m)\rangle\) returns 1.

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

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

\[
\Pr[\mathcal{E} \land \text{FIND} = \bot : b \leftarrow \mathcal{A}^{(H_0 \setminus \mathcal{S})}(z)] = \Pr[\mathcal{E} \land \text{FIND} = \bot : b \leftarrow \mathcal{A}^{(H_1 \setminus \mathcal{S})}(z)].
\]

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 FIND = \( \top \). Note that we omit unnecessary statements from [1, Theorem 1] and do not consider the parallelization of queries.

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

\[
\left| \Pr[1 \leftarrow \mathcal{A}^{(H)}(z)] - \Pr[1 \leftarrow \mathcal{A}^{(H \setminus \mathcal{S})}(z) \land \text{FIND} = \bot] \right| \leq \sqrt{(q_{\text{ro}} + 1) \Pr[\text{FIND} = \top : b \leftarrow \mathcal{A}^{(H \setminus \mathcal{S})}(z)]},
\]
Furthermore, the following provides a bound on \( \Pr[FIND = \top]: b \leftarrow A^{[H \setminus S]}(z) \).

**Lemma 2.5 (Search in Semi-classical Oracle [1, Theorem 2 and Corollary 1])**. Let \( A \) be a quantum adversary issuing at most \( q_{\text{qro}} \) (quantum) random oracle queries to \( H \). Let \( B^{[H]}(z) \) be an algorithm that runs as follows: Picks \( i \leftarrow [q_{\text{qro}}] \), runs \( A^{[H]}(z) \) until just before \( i \)-th query, measures a query input register in the computational basis, and outputs the measurement outcome as \((r, m)\). Then,

\[
\Pr[FIND = \top] \leq 4q_{\text{qro}} \Pr[(r, m) \in S: (r, m) \leftarrow B^{[H]}(z)].
\]

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

\[
\Pr[FIND = \top] \leq 4q_{\text{qro}}\epsilon.
\]

### 2.7 Hash-and-Sign Paradigm

Fig. 8 shows algorithms of the probabilistic hash-and-sign with retry, and \( \text{HaS}[T, H] \) is a signature scheme using a TDF \( T \) and a hash function \( H \). If \( \text{HaS}[T, H].\text{Sign} \) outputs a signature without retry, \( \text{HaS}[T, H] \) instantiates the probabilistic hash-and-sign. If \( r \) is empty, \( \text{HaS}[T, H] \) instantiates the deterministic hash-and-sign.

### 3 Existing Security Proofs

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

**Security Proof in the ROM [6, 30]**: Let \( T_{\text{psf}} \) be a PSF. A reduction from the \( \text{INV} \) of \( T_{\text{psf}} \) to the \( \text{EUF-CMA} \) security of \( \text{HaS}[T_{\text{psf}}, H] \) in the ROM is given by lazy sampling and programming. The \( \text{INV} \) adversary \( B_{\text{inv}} \), given a challenge \((F, y)\), simulates the \( \text{EUF-CMA} \) game played by an adversary \( A_{\text{cma}} \) as follows: For a random oracle query \((r, m)\), \( B_{\text{inv}} \) returns \( F(x) \) for \( x \leftarrow \text{SampDom}(F) \) and stores \((r, m, x)\) in a database \( D \). If \((r, m, x) \in D \) with some \( x \), then \( B_{\text{inv}} \) gives \( F(x) \) to \( A_{\text{cma}} \). For a signing query \( m \), \( B_{\text{inv}} \) chooses \((r, x)\) by \( r \leftarrow R \) and
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 ✓/$1\sqrt{\epsilon}$ indicate that Condition 2 is necessary, and ✓/$\epsilon$ indicate that Condition 1 is necessary. Also from Conditions 2, |R| is negligible. In “Target scheme”, d/p/pr stand for the deterministic hash-and-sign, probabilistic hash-and-sign, and probabilistic hash-and-sign with retry.

<table>
<thead>
<tr>
<th>Security proof</th>
<th>Security Bound</th>
<th>Conditions</th>
<th>Target scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>[14]</td>
<td>$\frac{1}{2^{n+1}}\epsilon_{cr}^2$</td>
<td>CR ✓ ✓ ✓ ✓</td>
<td>d/p</td>
</tr>
<tr>
<td>[61]</td>
<td>$2\sqrt{(\frac{\epsilon_{ps} + 3}{\sqrt{\epsilon_{inv}}})}$</td>
<td>OW/INV ✓ ✓ ✓ ✓</td>
<td>d/p</td>
</tr>
<tr>
<td>ext. of [58]</td>
<td>$4q_{qro}^2(q_{qro} + 1)^2\epsilon_{ow/inv}$</td>
<td>OW/INV ✓ ✓ ✓ ✓</td>
<td>d/p</td>
</tr>
<tr>
<td>[40]</td>
<td>$(2(q_{qro} + \epsilon_{ps} + 1)^2\epsilon_{ow/inv}$</td>
<td>OW/INV ✓ ✓ ✓ ✓</td>
<td>d/p</td>
</tr>
<tr>
<td>[17]</td>
<td>$\frac{1}{2}(\epsilon_{nma} + \frac{2}{\sqrt{\epsilon_{ow}}})\sqrt{\delta} + \frac{\epsilon_{ps} + 1}{\epsilon_{inv}}\sqrt{\frac{q_{qro}^2 + q_{qro} + 1}{</td>
<td>R</td>
<td>}}$</td>
</tr>
<tr>
<td>our</td>
<td>$(2(q_{qro} + 1)^2\epsilon_{inv} + \epsilon_{ps} + \frac{3}{2}\epsilon_{ps} + 2\sqrt{\frac{q_{qro}^2 + q_{qro} + 1}{</td>
<td>R</td>
<td>}})$</td>
</tr>
<tr>
<td>our</td>
<td>$\epsilon_{nma} + \frac{2}{\sqrt{\epsilon_{ow}}}\sqrt{\frac{q_{qro}^2 + q_{qro} + 1}{</td>
<td>R</td>
<td>}} + 2(q_{qro} + 2)$</td>
</tr>
<tr>
<td>our</td>
<td>$(2q_{qro} + 1)^2\epsilon_{ow/inv} + \frac{\epsilon_{ps} + 1}{\epsilon_{inv}}\sqrt{\frac{q_{qro}^2 + q_{qro} + 1}{</td>
<td>R</td>
<td>}}$</td>
</tr>
</tbody>
</table>

$x \leftarrow SampDom(F)$. If $(r, m, y) \notin D$, $B_{inv}$ returns $(r, x)$ and stores $(r, m, x)$ in $D$; otherwise $B_{inv}$ returns stored $(r, x)$.

From Condition 1 of PSF ($F(x)$ is uniform), $B_{inv}$ can use $F(x)$ as an output of the random function. Also from Conditions 2 and 3, $B_{inv}$ can simulate an honestly generated signature $x_i \leftarrow I(H(r_i, m_i))$ by $x_i \leftarrow SampDom(F)$. To win the INV game, $B_{inv}$ gives his query $y$ to $A_{psf}$ in one of the $(q_{qro} + 1)$ queries to $H$. If $A_{psf}$ outputs a valid signature $(m^*, r^*, x^*)$, $H(r^*, m^*) = y$ holds and $B_{inv}$ can win the INV game with probability $\frac{1}{q_{qro}^2 + q_{qro} + 1}$. Hence, we have $Adv_{H_{psf}}(A_{psf}) \leq (q_{qro} + 1)Adv_{INV}^{T_{ref}}(B_{inv})$, where $A_{psf}$ is an adversary who can make only classical queries to $H$.

Note that $Adv_{INV}^{T_{ref}}(B_{inv}) = Adv_{T_{psf}}^{INV}(B_{inv})$ holds ($D_X$ is defined as $SampDom$ ($F$) in the OW game (see Fig. 3)) since the OW adversary can simulate the INV game by giving a uniform $y = F(x)$ to the INV adversary, and vice versa.

Security Proof by Semi-constant Distribution [61]: 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. $B_{inv}$
simulates the EUF-CMA game by generating signatures without the trapdoor as the above security proof in the ROM. Instead of adaptively programming $H$, $B_{inv}$ replaces $H$ as $H' = F(DetSampDom(F, H(r, m)))$, where $H \leftarrow R^W \times \mathcal{M}$ is a random function to output randomness $w$ and $DetSampDom$ is a deterministic function of $SampDom$ [14]. From **Condition 1**, $H'$ is indistinguishable from $H$.

$B_{inv}$ programs $H'$ that outputs $y$ with probability $\epsilon$ (semi-constant distribution). In the signing oracle, if $H'(r_i, m_i)$ outputs $y$, $B_{inv}$ aborts this game. A bound on the statistical distance between the random function and the programmed one with the semi-constant distribution is $\frac{1}{2}(q_{sign} + q_{qro} + 1)^4 \epsilon^2$ [61, Corollary 4.3]. When $A_{cma}$ wins the EUF-CMA game, $B_{inv}$ can win the INV game with probability $(1 - \epsilon)^{q_{qro}} \approx \epsilon - q_{sign} \epsilon^2$. Minimizing the bound $\frac{1}{\epsilon} \text{Adv}^{\text{INV}}_{T_{psf}} + (q_{sign} + \frac{8}{3}(q_{sign} + q_{qro} + 1)^4) \epsilon$ gives [61, Theorem 5.3]

$$\text{adv}^{\text{EUF-CMA}}_{\text{HaS}[T_{psf}, H]}(A_{cma}) \leq 2 \left( q_{sign} + \frac{8}{3}(q_{sign} + q_{qro} + 1)^4 \right) \text{Adv}^{\text{INV}}_{T_{psf}}(B_{inv}).$$

Zhanda proposed another technique called **small-range distribution** [60] that also yields a security bound with a square root loss. Chatterjee, Das, and Pandit [18] used this technique to show the EUF-CMA security of the modified UOV signature [52] in the QROM.

**Application of Lifting Theorem [58]**: Yamakawa and Zhanda gave the lifting theorem for search-type games. As an application of the lifting theorem, they showed $\text{Adv}^{\text{EUF-NMA}}_{\text{HaS}[T_{psf}, H]}(A_{nma}) \leq (2q_{qro} + 1)^2 \text{Adv}^{\text{EUF-NMA}}_{\text{HaS}[T_{psf}, H]}(A_{nma^x})$, where $A_{nma^x}$ is an EUF-NMA adversary making classical queries to $H$ [58, Corollary 4.10]. For a hash-and-sign signature $\text{HaS}[T_{psf}, H]$, they showed $\text{Adv}^{\text{EUF-NMA}}_{\text{HaS}[T_{psf}, H]}(A_{cma}) \leq 4q_{sign} \text{Adv}^{\text{EUF-NMA}}_{\text{HaS}[T_{psf}, H]}(A_{nma})$ [58, Theorem 4.11]. Extending the results of [58] using the security proof in the ROM, we have a bound:

$$\text{Adv}^{\text{EUF-CMA}}_{\text{HaS}[T_{psf}, H]}(A_{cma}) \leq 4q_{sign}(q_{qro} + 1)(2q_{qro} + 1)^2 \text{Adv}^{\text{INV}}_{T_{psf}}(B_{inv}).$$

**Reduction from EUF-NMA for WPSF [17]**: 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. The authors assumed a WPSF with **Condition 3** and a weaker version of **Condition 2**, that is, there is a bound $\delta$ on the average of statistical distance $\delta_{F, I} = \Delta(SampDom(F), I(U(\mathcal{Y})))$ over all $(F, I) \leftarrow \text{Gen}(1^\lambda)$ (see details in **Appendix B.1**). Let $T_{wpf}$ be a WPSF. The EUF-NMA adversary $A_{nma}$ replaces the random function $H$ by $H'$, which outputs $H(r, m)$ with probability $\frac{1}{2}$ and

---

8 The authors of [17] defined a problem called claw with random function problem; however, its definition is identical to EUF-NMA game for hash-and-sign.
\[ F(\text{DetSampDom}(F, w)) \text{ with probability } \frac{1}{2}. \] A bound on the advantage of distinguishing \( H \) from \( H' \) is \( \frac{8\pi}{\sqrt{3}} q_{\text{ro}} \sqrt{3} q_{\text{sign}} \). The authors gave [17, Theorem 2] \( 1 \) bound on the advantage of distinguishing \( H \) from \( H' \) is \( \frac{8\pi}{\sqrt{3}} q_{\text{ro}} \sqrt{3} q_{\text{sign}} \).

Reduction from Collision-resistance [14]: Boneh et al. [14] gave a reduction from the CR of \( T_{psf} \) to the sEUF-CMA security of \( \text{HaS}[T_{psf}, H] \). Let us assume that the CR adversary \( B_{cr} \) given \( F \) simulates the sEUF-CMA game for \( A_{cma} \). For a random function \( H \leftarrow Y R \times M \), \( B_{cr} \) replaces the random function \( H' \) with \( H' \) \( (r, s) = F(\text{DetSampDom}(F, H(r, s))) \), where \( H \) and \( H' \) are indistinguishable from Condition 1. Also, the CR adversary simulates the signing oracle using Conditions 2 and 3. If \( A_{cma} \) wins by \( (r^*, s^*, x^*) \), then \( F(x^*) = H'(r^*, s^*) = F(x') \) holds for \( x' = \text{DetSampDom}(F, H(r^*, s^*)) \). When \( x^* \neq x' \), \( B_{cr} \) can obtain a collision pair \( (x^*, x') \). Since \( x^* \neq x' \) holds with probability \( 1 - 2^{-\omega(\log(\lambda))} \) (see Condition 4),

\[
\text{Adv}^\text{EUF-CMA}_{\text{HaS}[T_{psf}, H]}(A_{cma}) \leq \frac{1}{1 - 2^{-\omega(\log(\lambda))}} \text{Adv}^\text{CR}_{T_{psf}}(B_{cr}).
\]

Concurrent Work [40]: Liu, Jiang, and Zhao [40] 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 [18, 14, 61], the random function \( H \) is replaced as \( H' = F(\text{DetSampDom}(F, H(m))) \) to answer the signing queries without using the trapdoor. From Condition 1, this modification does not incur any security loss. Then, their reduction for TDP-FDH uses the measure-and-reprogram technique [23, Theorem 2] (see Lemma 2.2 in Section 2.6) as in our security proof. Their reduction has a security bound that includes \( q_{\text{sign}} \) in the multiplicative loss:

\[
\text{Adv}^\text{EUF-CMA}_{\text{HaS}[T_{psf}, H]}(A_{cma}) \leq (2(q_{\text{ro}} + q_{\text{sign}} + 1))^2 \text{Adv}^\text{INV}_{T_{psf}}(A_{inv}).
\]

4 New Security Proof

The main theorem is as follows:

Theorem 4.1 (INV \( \Rightarrow \) EUF-CMA (Main Theorem)). For any quantum EUF-CMA adversary \( A_{cma} \) of \( \text{HaS}[T_{psf}, H] \) issuing at most \( q_{\text{sign}} \) classical queries to the signing oracle and \( q_{\text{ro}} \) (quantum) random oracle queries to \( H \leftarrow Y R \times M \),
there exist an INV adversary \( B_{inv} \) of \( T_{wpsf} \) and a PS adversary \( D_{ps} \) of \( T_{wpsf} \) issuing \( q_{\text{sign}} \) sampling queries such that

\[
\begin{align*}
\text{Adv}_{HaS[T_{wpsf}, H]}^{\text{EUF-CMA}}(A_{cma}) & \leq (2q_{\text{qro}} + 1)^2 \text{Adv}_{T_{wpsf}}^{\text{INV}}(B_{inv}) + \text{Adv}_{T_{wpsf}}^{\text{PS}}(D_{ps}) \\
& + \frac{3}{2} q_{\text{sign}}' \sqrt{\frac{q_{\text{sign}} + q_{\text{qro}} + 1}{|R|}} + 2(q_{\text{qro}} + 2) \sqrt{\frac{q_{\text{sign}} - q_{\text{sign}}}{|R|}},
\end{align*}
\]

where \( q_{\text{sign}}' \) is a bound on the total number of queries to \( H \) in all the signing queries, and the running times of \( B_{inv} \) and \( D_{ps} \) are about that of \( A_{cma} \).

Here, we provide a proof sketch, while Section 4.1 contains the complete proof.

**Proof Sketch:** The main theorem comprises two reductions: EUF-NMA \( \Rightarrow \) EUF-CMA and INV \( \Rightarrow \) EUF-NMA. To establish EUF-NMA \( \Rightarrow \) EUF-CMA, we introduce modifications to the signing oracle, enabling simulation by SampDom. We employ the tight adaptive reprogramming technique [32] (see Section 2.6) to modify the signing oracle. This modification involves sampling \( r \leftarrow \mathcal{S} \mathcal{R} \) and \( y \leftarrow \mathcal{S} \mathcal{Y} \), and reprogramming \( H \) as \( H^{(r, m) \rightarrow y} \) every time the signing oracle calls \( H \). A straightforward way to simulate the signing oracle by \( \text{SampDom} \) is to sample \( x \leftarrow \text{SampDom}(F) \) instead of \( x \leftarrow I(y) \) and reprogram \( H \) as \( H^{(r, m) \rightarrow F(x)} \).

However, \( x \leftarrow \text{SampDom}(F) \) cannot simulate \( x \leftarrow I(y) \) when it outputs \( x = \perp \) during retries. The hardness of the PS game (see Definition 2.7) only ensures that \( x \leftarrow \text{SampDom}(F) \) can simulate \( x \leftarrow I(y) \) that is obtained after some retries until \( x \neq \perp \) holds. Fortunately, if we can cancel the reprogramming done during retries, we can simulate the signing oracle by selecting \( r \leftarrow \mathcal{S} \mathcal{R} \) and \( x \leftarrow \text{SampDom}(F) \), and then reprogramming \( H \) as \( H^{(r, m) \rightarrow F(x)} \). To achieve this, we use the semi-classical O2H technique [1] (see Section 2.6). 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, completing the reduction.

For INV \( \Rightarrow \) EUF-NMA, we utilize the measure-and-reprogram technique [23]. The INV adversary \( B_{inv} \) is given a challenge \( (F, y) \) and interacts with \( A_{nma} \) in the EUF-NMA game. \( B_{inv} \) measures and reprograms the random function \( H \) accessed by \( A_{nma} \). \( B_{inv} \) measures one of the random oracle queries made by \( A_{nma} \). Let \( (r, m) \) denote the observed value, and \( H \) is reprogrammed as \( H' = H^{(r, m) \rightarrow y} \). Then, \( B_{inv} \) runs \( A_{nma} \) again with \( H' \) and obtains \((m, r, x)\). Finally, \( B_{inv} \) outputs \( x \) as a preimage of \( y \). From [23, Theorem 2] (see Section 2.6), we can achieve a reduction with a security loss of \((2q_{\text{qro}} + 1)^2\) in INV \( \Rightarrow \) EUF-NMA.

Theorem 4.1 has the following two advantages:

**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 the random
function $H$ with $H'$ all at once, requiring statistical indistinguishability between $H$ and $H'$. On the other hand, our proof adaptively reprograms $H$ in each signing query. This approach enables us to provide the security proof under a weaker assumption compared to the one required by PSF.

**Advantage 2: Tighter proof:** Our reduction is tighter than the existing ones [61, 58]. While we cannot guarantee the optimality of our reduction, we can infer from several observations that a multiplicative loss of $(2q_{qro} + 1)^2$ appears to be unavoidable in the generic (black-box) reduction. The reduction incurs a loss of the number of queries to the random function, even in the ROM (see Section 3). Second, the security loss of a generic reduction from ROM to QROM using the lifting theorem [58] is at least $(2q_{qro} + 1)^2$. Third, in the Fiat-Shamir paradigm, a generic reduction from arbitrary ID schemes incurs the same security loss (see Remark 4.4).

We give some remarks on Theorem 4.1.

**Remark 4.1.** If $HaS[T_{psf}, H]$ adopts the probabilistic hash-and-sign, then $q'_{sign} = q_{sign}$ holds and the last term of Eq. (4) becomes 0.

**Remark 4.2.** We have a tight reduction in $EUF-NMA \Rightarrow EUF-CMA$ with the following bound:

$$\text{Adv}^{EUF-CMA}_{HaS[T_{psf}, H]}(A_{cma}) \leq \text{Adv}^{EUF-NMA}_{HaS[T_{psf}, H]}(A_{nma}) + \text{Adv}^{PS}_{T_{psf}}(D_{ps}) + \frac{3}{2} q'_{sign} \sqrt{q_{sign} + q_{qro} + 1 - \frac{1}{|R|}} + 2(q_{qro} + 2) \sqrt{q_{sign} - q_{sign}}.$$  \hspace{1cm} (5)

Comparing this bound with the one presented in [17] (refer to Eq. (1) in Section 3), we observe that our requirement for $T_{psf}$ is weaker, and there are no square-root terms associated with Condition 2.

**Remark 4.3.** When the underlying TDF is PSF (or TDP), we have:

$$\text{Adv}^{EUF-CMA}_{HaS[T_{psf}, H]}(A_{cma}) \leq (2q_{qro} + 1)^2 \text{Adv}^{INV}_{T_{psf}}(B_{inv}) + \frac{3}{2} q_{sign} \sqrt{q_{sign} + q_{qro} + 1 - \frac{1}{|R|}}.$$  

As $HaS[T_{psf}, H.]Sign$ produces a signature without retry (Condition 3), $q'_{sign} = q_{sign}$ holds. In the PS game, the outputs of $I$ and $\text{SampDom}(F)$ are equivalent due to Condition 2, resulting in $\text{Adv}^{PS}_{T_{psf}}(D_{ps}) = 0$. This bound is tighter than existing ones for $HaS[T_{psf}, H]$ (see Table 2).

**Remark 4.4.** Grilo et al. showed a tight reduction of $EUF-NMA \Rightarrow EUF-CMA$ in the Fiat-Shamir (without aborts) paradigm, assuming that the underlying ID scheme is honest verifier zero-knowledge (HVZK) [32, Theorem 3]. Also, Don et al. gave a generic reduction in the Fiat-Shamir transform of arbitrary ID schemes with a security loss $(2q_{qro} + 1)^2$ [24, Theorem 8]. The above reductions use the tight adaptive reprogramming technique and the measure-and-reprogram technique, respectively.
4.1 Proof of Theorem 4.1

In the beginning, we show that we can set \( q_{\text{sign}}' = \frac{c}{\rho} q_{\text{sign}} \) for some constant \( c > 1 \), where \( \rho = \Pr[x \neq \bot; y \leftarrow \mathcal{Y}, x \leftarrow I(y)] \). In \( q_{\text{sign}}' \) trials, at least \( q_{\text{sign}} \) signatures are generated if the number of successful trials (where \( I(H(r, m)) \) outputs a preimage) is \( q_{\text{sign}} \) or more. Let \( S \) be a random variable for the number of successful trials. \( E(S) = \rho q_{\text{sign}} = c q_{\text{sign}} \) holds. From the Chernoff bound, we have \( \Pr[S \leq (1 - \gamma)E(S)] \leq e^{-\frac{1}{2} \gamma^2 E(S)} \). Substituting \( \gamma = \frac{\frac{E(S) - q_{\text{sign}} + 1}{E(S)}}{c} \), the LHS becomes \( \Pr[S \leq q_{\text{sign}} - 1] \) and is a probability that we cannot generate \( q_{\text{sign}} \) signatures with \( q_{\text{sign}}' \) trials. Since we set \( q_{\text{sign}}' = \frac{c}{\rho} q_{\text{sign}} \), the exponent of the RHS becomes \( \frac{(-c \gamma q_{\text{sign}}' + 1)^2}{2 c q_{\text{sign}}'} \geq -\frac{c}{2c} q_{\text{sign}} \) and the bound on \( \Pr[S \leq q_{\text{sign}} - 1] \) becomes negligible for \( q_{\text{sign}} = \omega(\log(\lambda)) \).

EUF-NMA \( \Rightarrow \) EUF-CMA: Figs. 9 and 10 show the games and simulations described below. Without loss of generality, we assume that \( \mathcal{A}_{\text{cma}} \) makes a query \((s^*, m^*)\) (the final output) to \( H \). Then, the total number of queries to \( H \) is \( q_{\text{cma}} + 1 \).

GAME \( G_0 \) (EUF-CMA game): This is the original EUF-CMA game and \( \Pr[G_0^{A_{\text{cma}} \Rightarrow 1}] = \text{Adv}^\text{EUF-CMA}_{H}(A_{\text{cma}}) \) holds.

GAME \( G_1 \) (adaptive reprogramming of \( H \)): The signing oracle \( \text{Sign}^H \) uniformly chooses \((r_i, y_i)\) and reprograms \( H := H(r_i, m_i) \rightarrow y_i \) until \( I(y_i) \) does not output \( \bot \) (see Lines 2 to 5 in \( \text{Sign}^H \) for \( G_1 \)). Considering the number of retries, \( H \) is reprogrammed for at most \( q_{\text{sign}}' \) times.

The AR adversary \( D_{\text{ar}} \) can simulate \( G_0/G_1 \) (the top row of Fig. 10). If \( D_{\text{ar}} \) plays \( A_{\text{cma}} \) for \( G_0 \); otherwise it simulates \( G_1 \). From Lemma 2.1, we have \( |\Pr[G_0^{A_{\text{cma}} \Rightarrow 1}] - \Pr[G_1^{A_{\text{cma}} \Rightarrow 1}]| \leq \text{Adv}^\text{AR}_{H}(D_{\text{ar}}) \leq \frac{3}{2} q_{\text{sign}}' \sqrt{\frac{q_{\text{cma}} + q_{\text{sign}} + 1}{|\kappa|}} \).

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

Hence, \( \Pr[G_1^{A_{\text{cma}} \Rightarrow 1}] = \Pr[G_2^{A_{\text{cma}} \Rightarrow 1}] \) holds.

GAME \( G_3 \) (puncturing \( H \)): Let \( S' = \{(r, m) : r \in S, m \in M\} \) be a set induced by \( S \). Instead of \( H \), \( \mathcal{A}_{\text{cma}} \) makes queries to \( H \backslash S' \) (\( H \) punctured by \( S' \)). Also, \( G_3 \) outputs 0 if \( \text{FIND} = \top \) (see the definitions of \( H \backslash S' \) and \( \text{FIND} \) in Definition 2.10). We use Lemma 2.4 to bound \( |\Pr[G_2^{A_{\text{cma}} \Rightarrow 1}] - \Pr[G_3^{A_{\text{cma}} \Rightarrow 1}]| \). Suppose that \( \Pr[G_2^{A_{\text{cma}} \Rightarrow 1}] = \Pr[1 \leftarrow \mathcal{A}_{\text{cma}}^{\text{Sign}_{\mathcal{H}}^H}(F)] \). Since \( G_3 \) uses \( H \backslash S' \) and outputs 0 if \( \text{FIND} = \top \), we have \( \Pr[G_3^{A_{\text{cma}} \Rightarrow 1}] = \Pr[1 \leftarrow \mathcal{A}_{\text{cma}}^{\text{Sign}_{\mathcal{H}}^H}(S') \land \text{FIND} = \bot] \).
and \( \Pr[\text{FIND} = \top : G_3^{A_{\text{cma}}} \Rightarrow b] = \Pr[\text{FIND} = \top : b \leftarrow A_{\text{cma}}^{\text{Sign}_{\mathcal{H}\setminus S'}}(F)] \). Then,

\[
\left| \Pr[G_2^{A_{\text{cma}}} \Rightarrow 1] - \Pr[G_3^{A_{\text{cma}}} \Rightarrow 1] \right| \leq \sqrt{(q_{\text{qro}} + 2) \Pr[\text{FIND} = \top : G_3^{A_{\text{cma}}} \Rightarrow b]},
\]

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

GAME \( G_4 \) (reprogramming only for successful trials): The signing oracle reprograms \( H := H'(r_i, m_i) \rightarrow y_i \), only for \( r_i \leftarrow \mathcal{R}, y_i \leftarrow \mathcal{Y}, \) and \( x_i \leftarrow l(y_i) \) satisfying \( x_i \neq \perp \). Notice that \( A_{\text{cma}} \) makes queries to the punctured oracle \( H\setminus S' \). By the
Fig. 10: Simulations for EUF-NMA $\Rightarrow$ EUF-CMA

definition of FIND, if FIND $= \perp$, that is, the measurements of $[f_G(r, m)]$ are
0 for all queries, then $\mathcal{A}_{cma}$'s queries never contain any $(r, m) \in S'$ and $\mathcal{A}_{cma}$
cannot obtain $H(r, m)$ for $(r, m) \in S'$. Hence, if FIND $= \perp$, then $\mathcal{A}_{cma}$
cannot distinguish whether $H$ is reprogrammed at $(r, m) \in S'$ in $G_3$ or not in $G_4$ and
we have

$$\Pr[FIND = \perp : G_3^{A_{cma}} \Rightarrow b] = \Pr[FIND = \perp : G_4^{A_{cma}} \Rightarrow b]$$

(as Lemma 2.3). Especially, if $G_3$ or $G_4$ outputs 1, then FIND should be $\perp$ (Line 12 of
$G_3$-$G_4$). Thus, we also have $\Pr[G_3^{A_{cma}} \Rightarrow 1] = \Pr[G_4^{A_{cma}} \Rightarrow 1]$. Moreover,
$\Pr[FIND = \top : G_3^{A_{cma}} \Rightarrow b] = \Pr[FIND = \top : G_4^{A_{cma}} \Rightarrow b]$ holds from
Eq. (7).

Let $G'_4$ be a game given in Fig. 11 (identical to $G_4$ except that $B_{cma}$
outputs $(r', m')$ and $H$ is not punctured). Choosing $j \leftarrow [q_{qro} + 1]$, $B_{cma}$ runs
INV ⇒ EUF-NMA: We use Lemma 2.2. Let S be a two-stage algorithm that consists of S₁ and S₂ and runs Aₐₙₚ in the EUF-NMA game as follows:

1. Choose \((i, b) \leftarrow S\) with \(\{(\text{qro}) \times \{0, 1\}\} \cup \{(\text{qro} + 1, 0)\}\).
2. Run Aₐₙₚ with H until \(i\)-th query.
3. Measure \(i\)-th query and output \((r, m)\) as the output of S₁.
4. Given a random \(\theta\), reprogram \(H' = H^{(r, m) \rightarrow \theta}\).
5. If \(i = \text{qro} + 1\), then go to Step 8.

\[\text{Sign}^b(m_i) \text{ for } G_4\]

\[
\begin{array}{l}
\text{repeat} \\
2 \quad y_i \leftarrow 1 \smallsetminus \mathcal{Y} \\
3 \quad x_i \leftarrow l(y_i) \\
4 \quad \text{until } x_i \neq \perp \\
5 \quad r_i \leftarrow \mathcal{R} \\
6 \quad H := H^{(r, m_i) \rightarrow y_i} \\
7 \quad Q := Q \cup \{m_i\} \\
8 \quad \text{return } (r_i, x_i)
\end{array}
\]

Fig. 11: A game \(G_4\) used in the application of Lemma 2.5.

\(A_{\text{cma}}\) playing \(G_4\). Just before \(A_{\text{cma}}\) makes \(j\)-th query to \(H\), \(B_{\text{cma}}\) measures a query input register of \(A_{\text{cma}}\) and outputs the measurement outcome as \((r', m')\). Since the oracles of \(G_4\) reveal no information on \(S\), \(B_{\text{cma}}\) has no information on \(S\); therefore, \(\Pr[G_4^{B_{\text{cma}}} = 1] \leq \Pr[r' \in S] \leq \frac{q_{\text{qro}} - q_{\text{sign}}}{|\mathcal{R}|}\) holds. Hence, \(\Pr[\text{FIND} = \perp : A_{\text{cma}}^{G_4^{B_{\text{cma}}}} \Rightarrow b] \leq 4(q_{\text{qro}} + 1)\sqrt{\frac{q_{\text{qro}} - q_{\text{sign}}}{|\mathcal{R}|}}\) holds from Lemma 2.5 and an upper bound on Eq. (6) is \(2(q_{\text{qro}} + 2)\sqrt{\frac{q_{\text{qro}} - q_{\text{sign}}}{|\mathcal{R}|}}\).

GAME \(G_5\) (simulating the signing oracle by \(\text{SampDom}\)): The signing oracle generates signatures by \(r_i \leftarrow \mathcal{R}\) and \(x_i \leftarrow \text{SampDom}(F)\). The PS adversary \(D_{\text{ps}}\) can simulate \(G_4/G_5\) as in the second row of Fig. 10. If \(D_{\text{ps}}\) plays \(\text{PS}_0\), the procedures of the original and simulated \(G_4\) are identical. If \(D_{\text{ps}}\) plays \(\text{PS}_1\), he simulates \(G_5\). Thus, we have \(|\Pr[G_4^{A_{\text{cma}}} = 1] - \Pr[G_5^{A_{\text{cma}}} = 1]| \leq \text{Adv}_{\text{PS}}^{\text{ps}}(D_{\text{ps}})\).

We show that the EUF-NMA adversary \(A_{\text{dma}}\) can simulate \(G_5\) as in the bottom row of Fig. 10. In the simulation, \(A_{\text{cma}}\) makes queries to \(H \setminus S'\), where \(H'\) outputs whatever \(H\) outputs except for \(\{(r_i, m_i)\}_{i \in [\text{qro}]}\). Since \(m^* \not\in Q\) holds if \(A_{\text{cma}}\) wins, \(H'(r^*, m^*) = H(r^*, m^*)\) holds for \((m^*, r^*, x^*)\) that \(A_{\text{cma}}\) returns. Therefore, \(A_{\text{dma}}\) wins his game if \(A_{\text{cma}}\) wins the EUF-CMA game. Hence, \(A_{\text{dma}}\) can perfectly simulate \(G_5\) with the same number of queries and almost the same running time as \(A_{\text{cma}}\), and \(\Pr[G_5^{A_{\text{cma}}} = 1] \leq \text{Adv}_{\text{EUF-NMA}}^{\text{PS}}(A_{\text{cma}})\) holds. We finally stress that the number of queries \(A_{\text{cma}}\) made to \(H\) is \(q_{\text{qro}}\) rather than \(q_{\text{qro}} + q_{\text{sign}}\) since \(A_{\text{dma}}\) never queries to its random oracle in the simulation of the signature.

Summing up, we have Eq. (5) for EUF-NMA ⇒ EUF-CMA.
6. Answer \(i\)-th query with \(H\) (if \(b = 0\)) or \(H'\) (if \(b = 1\)).
7. Run \(A_{\text{nma}}\) with \(H'\) until the end.
8. Output \(A_{\text{nma}}\)’s output \((m^*, r^*, x^*)\) as the output of \(S_2\).

The INV adversary \(B_{\text{inv}}\) runs \(S\). Since \(y\) is uniform in the INV game, \(B_{\text{inv}}\) can set the input for \(S_2\) as \(\theta := y\). When the predicate is \(F(x) \overset{?}{=} H(r, m)\), we have

\[
Pr\left[ (r, m) = (\hat{r}, \hat{m}) \land F(x) = y : (r, m) \leftarrow S_{\text{nma}}^A(), (m, r, x) \leftarrow S_{\text{nma}}^A(y) \right] \\
\geq \frac{1}{(2q_{\text{qro}} + 1)^2} Pr\left[ (r, m) = (\hat{r}, \hat{m}) \land F(x) = H(r, m) : (m, r, x) \leftarrow A_{\text{nma}}^H(F) \right],
\]

for any \((\hat{r}, \hat{m}) \in \mathcal{R} \times \mathcal{M}\) from Lemma 2.2. By summing over all \((\hat{r}, \hat{m}) \in \mathcal{R} \times \mathcal{M}\),

\[
Pr\left[ F(x) = y : (r, m) \leftarrow S_{\text{nma}}^A(), (m, r, x) \leftarrow S_{\text{nma}}^A(y) \right] \\
\geq \frac{1}{(2q_{\text{qro}} + 1)^2} Pr\left[ F(x) = H(r, m) : (m, r, x) \leftarrow A_{\text{nma}}^H(F) \right].
\]

Notice that the probability in the RHS of Eq. (8) is the EUF-NMA advantage.

Also, \(\text{Adv}^{\text{INV}}_{T_{\text{wpsf}}} (B_{\text{inv}}) \geq Pr\left[ F(x) = y : (r, m) \leftarrow S_{\text{nma}}^A(), (m, r, x) \leftarrow S_{\text{nma}}^A(y) \right]\) holds since \(B_{\text{inv}}\) runs \(S\). Hence, we have

\[
\text{Adv}^{\text{EUF-NMA}}_{H_\mathcal{S}[T_{\text{wpsf}}, H]} (A_{\text{nma}}) \leq (2q_{\text{qro}} + 1)^2 \text{Adv}^{\text{INV}}_{T_{\text{wpsf}}} (B_{\text{inv}}).
\]  

(9)

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

4.2 Extension to sEUF-CMA Security

If \(F\) of the underlying TDF is injective, \(H_\mathcal{S}[T_{\text{wpsf}}, H]\) is sEUF-CMA secure.

**Corollary 4.1 (INV \(\Rightarrow\) sEUF-CMA).** Suppose that \(F\) of \(T_{\text{wpsf}}\) is an injection. For any quantum sEUF-CMA adversary \(A_{\text{cma}}\) of \(H_\mathcal{S}[T_{\text{wpsf}}, H]\) issuing at most \(q_{\text{sign}}\) classical queries to the signing oracle and \(q_{\text{qro}}\) (quantum) random oracle queries to \(H \leftarrow_{\xi} \mathcal{R} \times \mathcal{M}\), there exist an INV adversary \(B_{\text{inv}}\) of \(T_{\text{wpsf}}\) and a PS adversary \(D_{\text{ps}}\) of \(T_{\text{wpsf}}\) issuing \(q_{\text{sign}}\) sampling queries such that

\[
\text{Adv}^{\text{sEUF-CMA}}_{H_\mathcal{S}[T_{\text{wpsf}}, H]} (A_{\text{cma}}) \leq (2q_{\text{qro}} + 1)^2 \text{Adv}^{\text{INV}}_{T_{\text{wpsf}}} (B_{\text{inv}}) + \text{Adv}^{\text{PS}}_{T_{\text{wpsf}}} (D_{\text{ps}})
\]

\[
+ \frac{3}{2} q_{\text{sign}} \sqrt{\frac{q_{\text{sign}} + q_{\text{qro}} + 1}{|\mathcal{R}|}} + 2(q_{\text{qro}} + 1) \sqrt{\frac{q_{\text{sign}} - q_{\text{sign}}}{|\mathcal{R}|}},
\]

(10)

where \(q_{\text{sign}}\) is a bound on the total number of queries to \(H\) in all the signing queries, and the running times of \(B_{\text{inv}}\) and \(D_{\text{ps}}\) are about that of \(A_{\text{cma}}\).

**Proof.** The sEUF-CMA game outputs 0 if \((m^*, r^*, x^*) \in \mathcal{Q}'\). Due to the injection of \(F\), if \((m^*, r^*) = (m_i, r_i)\), it implies \(x^* = x_i\). Therefore, we can rephrase the condition for outputting 0 as follows: the game outputs 0 if \((m^*, r^*) \in \mathcal{Q}',\)
where $Q' = \{(m_i, r_i)\}_{i\in[q_{\text{psf}}]}$. With this reinterpretation, we demonstrate that the same bound as Eq. (5) holds for \text{EUF-NMA} \Rightarrow \text{sEUF-CMA}.

In Corollary 4.1, we can use the same games as defined in Theorem 4.1, and the bound on $|\Pr[G_0^{\text{acma}} \Rightarrow 1] - \Pr[G_5^{\text{acma}} \Rightarrow 1]|$ remains unchanged. In the simulation of $G_5$ (see the bottom row of Fig. 10), $A_{\text{acma}}$ uses $H'_\S'$ reprogrammed on $\{(r_i, m_i)\}_{i\in[q_{\text{psf}}]}$ instead of the original $H$. By $(m^*, r^*) \notin Q'$, $H'(r^*, m^*) = H(r^*, m^*)$ holds and $A_{\text{acma}}$ can win his game if $F(x^*) = H'(r^*, m^*)$. Therefore, $\Pr[G_5^{\text{acma}} \Rightarrow 1] \leq \text{Adv}_\text{EUF-NMA}[T_{\text{psf}}, H](A_{\text{acma}})$ holds, which implies that Eq. (5) holds.

4.3 Applications of New Security Proof

By applying Theorem 4.1, we can establish security proofs for Wave [2], the original/modified UOV signatures [38, 52], the modified HFE signature [52], and MAYO [10]. Additionally, by utilizing Corollary 4.1, we can provide a security proof for the modified CFS signature [20]. QR-UOV [29] and PROV [26] are provable secure since they follow the modified UOV signature. If Rainbow [22] makes the same modification as the modified UOV signature, the scheme can be provably secure. Also, GeMSS [16] is provably secure since it follows the modified HFE signature. The security proofs for these schemes, obtained by applying Theorem 4.1 and Corollary 4.1, are provided in Appendix B.

4.4 Extension to Security Proof of Fiat-Shamir with Aborts

The Fiat-Shamir with aborts paradigm [41] shares a similar structure with the probabilistic hash-and-sign with retry. Concurrent works by Devevey et al. [21] and Barbosa et al. [3] independently demonstrate reductions from \text{EUF-NMA} to \text{EUF-CMA} for the Fiat-Shamir with aborts. Devevey et al. rely on the strong HVZK assumption [21, Definition 6], which allows for statistical simulation of protocol outputs, even in cases of failure. Their proof utilizes the tight adaptive reprogramming technique to alter the game such that the \text{EUF-NMA} adversary can simulate. In contrast, Barbosa et al. rely on a weaker HVZK assumption called accepting HVZK [3, Definition 1]. The accepting HVZK assumes that protocol outputs can be statistically simulated conditioned on that the protocol does not fail. This definition closely resembles the existence of a statistical bound on the PS advantage (see Definition 2.7).

Given the structural similarity to the probabilistic hash-and-sign with retry, it is natural to explore the possibility of establishing a security proof for the Fiat-Shamir with aborts using the same techniques as presented in Theorem 4.1. In Appendix G, we present an alternative tight reduction of \text{EUF-NMA} \Rightarrow \text{EUF-CMA} for the Fiat-Shamir with aborts. The security bound, assuming the accepting HVZK, is almost identical to that of Barbosa et al. [3, Theorem 2].
5 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 $H: \mathcal{U} \times \mathcal{R} \times \mathcal{M} \rightarrow \mathcal{Y}$ be a hash function and $HaS^p[T, H, E] \in \text{sign schemes}$ be a signature scheme adopting the probabilistic hash-and-sign with retry and prefix hashing, where $E: \mathcal{Y}^X \rightarrow \mathcal{U}$ is a deterministic function to extract a small unpredictable part of $F$ into a key ID $u \in \mathcal{U}$. We assume that $E(F)$ is uniform over $\mathcal{U}$ for $(F, 1)^\lambda$.\footnote{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).} For a message $m$, $HaS^p[T, H, E].\text{Sign}$ repeats $r \leftarrow \mathcal{R}$ and $x \leftarrow 1(H(E(F), r, m))$ until $x \neq \perp$ holds, and outputs $(r, x)$. For a verification key $F$, a message $m$, and a signature $(r, x)$, $HaS^p[T, H, E].\text{Vrfy}$ verifies by $F(x) = H(E(F), r, m)$.

We show that $\text{M-INN} \Rightarrow \text{M-EUF-CMA}$ and $\text{M-CR} \Rightarrow \text{M-sEUF-CMA}$ hold without any security loss in the number of keys (see Lemma D.1 in Appendix D and Lemma E.1 in Appendix E). We note that there exist trivial reductions: $\text{Adv}^{\text{M-INN}}(\mathcal{B}_{\text{inv}^\lambda}) \leq q_{\text{inst}} \text{Adv}^{\text{INV}}(\mathcal{B}_{\text{inv}^\lambda})$ and $\text{Adv}^{\text{M-CR}}(\mathcal{B}_{\text{cr}^\lambda}) \leq q_{\text{inst}} \text{Adv}^{\text{CR}}(\mathcal{B}_{\text{cr}^\lambda})$, and equality may hold in these inequalities if adversaries can target multiple instances concurrently. 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 $\{F_j\}_{j \in [\lambda]}$ be verification keys generated by $\text{Gen}$ of a TDF $T$. Given a verification key $F': \mathcal{X}' \rightarrow \mathcal{Y}'$ generated by $\text{Gen}'$ of another TDF $T'$, we simulate $\{F_j\}_{j \in [\lambda]}$ by $\{L_j \circ F' \circ R_j\}_{j \in [\lambda]}$, where $L_j: \mathcal{Y}' \rightarrow \mathcal{Y}$ and $R_j: \mathcal{X} \rightarrow \mathcal{X}'$. Let $D_L$ and $D_R$ 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 $\{F_j\}_{j \in [\lambda]}$ and $\{L_j \circ F' \circ R_j\}_{j \in [\lambda]}$.

**Definition 5.1 (ST (Sandwich Transformation) Game).** Let $T$ and $T'$ be TDFs. Using a game given in Fig. 12, we define an advantage function of an adversary $D_a$ playing the ST game against $T$ and $T'$ as $\text{Adv}^{\text{ST}}_{T,T'}(D_a) = |\Pr[\text{ST}_T \Rightarrow 1] - \Pr[\text{ST}_{T'} \Rightarrow 1]|$.

We have the following reductions assuming some conditions on $L_j$ and $R_j$ (see the proofs in Appendices D and E).

<table>
<thead>
<tr>
<th>Game: ST</th>
<th>NewKey$_0$</th>
<th>NewKey$_1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 $(F', l') \leftarrow \text{Gen'}(1^\lambda)$</td>
<td>1 $(F_j, l_j) \leftarrow \text{Gen}(1^\lambda)$</td>
<td>1 $L_j \leftarrow D_h$</td>
</tr>
<tr>
<td>2 $b^* \leftarrow D_a^{\text{NewKey}_0}$</td>
<td>2 $R_j \leftarrow D_R$</td>
<td>2 $R_j \leftarrow D_R$</td>
</tr>
<tr>
<td>a return $b^*$</td>
<td>3 $F_j := L_j \circ F' \circ R_j$</td>
<td>3 $F_j := L_j \circ F' \circ R_j$</td>
</tr>
<tr>
<td></td>
<td>4 return $F_j$</td>
<td>4 return $F_j$</td>
</tr>
</tbody>
</table>

Fig. 12: ST (Sandwich Transformation) game
Lemma 5.1 (INV + ST $\Rightarrow$ M-EUF-CMA). Let $T'$ be a TDF with $F': \chi' \rightarrow \mathcal{Y}$. Suppose that $L_j: \mathcal{Y} \rightarrow \mathcal{Y}$ and $R_j: \mathcal{X} \rightarrow \chi'$ are used to simulate $F_j$ by $L_j \circ F' \circ R_j$ in the ST game, where $L_j$ is a bijection.

For any quantum M-EUF-CMA adversary $A_{cma}^m$ of $HaS^p|T_{wpsf},H,E|$ with $q_{key}$ keys and issuing at most $q_{sign}$ classical queries to the signing oracle and $q_{qro}$ (quantum) random oracle queries to $H \leftarrow \mathcal{Y}^{M \times \mathcal{R} \times \mathcal{M}}$, there exist an INV adversary $B_{inv}$ of $T'$ with $q_{inst}$ instances, an M-PS adversary $D_{ps}^m$ of $T_{wpsf}$ with $q_{key}$ instances and issuing $q_{sign}$ sampling queries, and an ST adversary $D_{st}$ of $(T_{wpsf}, T')$ issuing $q_{key}$ new key queries such that

$$Adv_{HaS^p|T_{wpsf},H,E}^{M-EUF-CMA}(A_{cma}^m) \leq (2q_{qro} + 1)^2 Adv_T^{INV}(B_{inv}) + Adv_{T_{wpsf}}^{M-PS}(D_{ps}^m)$$

$$+ Adv_{T_{wpsf},T'}^{ST}(D_{st}) + \frac{3}{2}q_{sign} q_{qro} + q_{sign} + 1 \frac{q_{sign} + q_{qro} + 1}{|R|}$$

$$+ 2(q_{qro} + 2) \sqrt{\frac{q_{sign} - q_{sign}}{|R|} + \frac{q_{key}}{|U|}}, \quad (11)$$

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

Lemma 5.2 (CR + ST $\Rightarrow$ M-sEUF-CMA). Let $T$ be a TDF with $F': \chi' \rightarrow \mathcal{Y}$. Suppose that $L_j: \mathcal{Y} \rightarrow \mathcal{Y}$ and $R_j: \mathcal{X} \rightarrow \chi'$ are used to simulate $F_j$ by $L_j \circ F \circ R_j$ in the ST game, where $L_j$ and $R_j$ are injections.

For any quantum M-sEUF-CMA adversary $A_{cma}^m$ of $HaS^p|T_{psf},H,E|$ with $q_{key}$ keys and issuing at most $q_{sign}$ classical queries to the signing oracle and $q_{qro}$ (quantum) random oracle queries to $H \leftarrow \mathcal{Y}^{M \times \mathcal{R} \times \mathcal{M}}$, there exist a CR adversary $B_{cr}$ of $T_{psf}$ with $q_{inst}$ instances and an ST adversary $D_{st}$ of $(T_{psf}, T')$ issuing $q_{key}$ new key queries such that

$$Adv_{HaS^p|T_{psf},H,E}^{M-sEUF-CMA}(A_{cma}^m) \leq \frac{1}{1 - 2^{-\omega(\log(\lambda))}} \left( Adv_T^{CR}(B_{cr}) + Adv_T^{ST}(D_{st}) \right) + \frac{q_{key}}{|U|}$$

where $\mathbb{E}_{F,1}(q_{inst}) \leq q_{key} \left( \frac{|U| - |q_{key} + 1|}{|U| - |q_{key} + 1|} \right)$ holds and the running times of $B_{cr}$ and $D_{st}$ are about that of $A_{cma}^m$.

In Appendix F, we apply 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 [50] and morphism of polynomials [49].

Open problems: There are two open problems for the generic method. First, the computational problems defined in Appendix F 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


47. 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


A Issue with Security Proof of [40]

We have identified a security flaw in the proof of $\text{OW} \Rightarrow \text{EUF-CMA}$ presented in Theorem 2 of the latest version of [40]. $T_{\text{tdp}}$ is a trapdoor permutation with $(F, 1)$, and $\text{HaS}[T_{\text{tdp}}, H]$ is a TDP-FDH signature scheme, where $F: \mathcal{X} \rightarrow \mathcal{Y}$ and $H: \mathcal{M} \rightarrow \mathcal{Y}$. In the security proof, the random function $H$ is replaced by $H = F(H(m))$, where $H \leftarrow \mathcal{X}^{\mathcal{M}}$, and the signing oracle returns $H(m)$. The security proof relies on the measure-and-reprogram technique and involves a two-stage algorithm $S$ composed of $S_1$ and $S_2$, which interacts with $\mathcal{A}_{\text{cma}}$ in the modified EUF-CMA game. The algorithm $S$ behaves as follows:

1. Choose $(i, b) \leftarrow \mathcal{S}([q] \times \{0, 1\}) \cup \{(q + 1, 0)\}.$
2. Run $\mathcal{A}_{\text{cma}}$ with $H$ until $i$-th query.
3. Measure $i$-th query and output $m$ as the output of $S_1$.
4. Given a random $\theta$, reprogram $H' = H^m \rightarrow \theta$.
5. If $i = q_{\text{qro}} + 1$, then go to Step 8.
6. Answer $i$-th query with $H$ (if $b = 0$) or $\hat{H}'$ (if $b = 1$).
7. Run $\mathcal{A}_{\text{cma}}$ with $H'$ until the end.
8. Output $\mathcal{A}_{\text{cma}}$’s output $(m^*, x^*)$ as the output of $S_2$. 

31
The authors argue that the following inequality holds from Lemma 2.2.

\[
\Pr\left[x = \theta : m \leftarrow S_1^{\text{cma}}(), (m, x) \leftarrow S_2^{\text{cma}}(\theta)\right] \\
\geq \frac{1}{(2q + 1)^2} \Pr\left[x = \theta : (m, x) \leftarrow A_H^{\text{cma}}(F)\right].
\]

(12)

In the original version, \(i\) is chosen from all the queries to \(\tilde{H}\) \((q = q_{\text{ro}} + q_{\text{sign}})\), while in the latest version, it is chosen only from queries to \(\tilde{H}\) outside the signing oracle \((q = q_{\text{ro}})\). The latter implies that query inputs for \(\tilde{H}\) are not measured and \(H\) is not reprogrammed in the signing oracle.

In the proof of [32, Theorem 2], the measure-and-reprogram technique relies on the assumption that when applying \(\mathbb{I} - |m\rangle\langle m|\) (where \(\mathbb{I}\) is the identity operator) onto the query input register at the \(i\)-th query, the quantum states in the following two cases are identical:

- Answers the \(i\)-th query by \(\tilde{H}\) and responds to subsequent queries by \(\tilde{H}'\).
- Answers the \(i\)-th query by \(\tilde{H}'\) and responds to subsequent queries by \(\tilde{H}'\).

If \(i\) indicates the index of queries to \(\tilde{H}\) outside the signing oracle, either \(\tilde{H}\) (in the first case) or \(\tilde{H}'\) (in the second case) is queried in the signing oracle between the \(i\)-th and \((i+1)\)-th queries. Due to this difference in the signing oracle’s behavior, the quantum states are not necessarily identical. The authors claim that queries to \(\tilde{H}\) within the signing oracle can be disregarded based on the observation that when \(A^{\text{cma}}\) does not output 0, it implies that \(m\) has not been queried for the signing oracle. However, they need to clearly demonstrate how this fact affects the above assumption and Eq. (12).

B Security Proofs of Hash-and-sign Signatures by Theorem 4.1 and Corollary 4.1

This section shows the applications of Theorem 4.1 and Corollary 4.1 to some code-based and MQ-based hash-and-sign signatures.

B.1 Code-based Cryptography

**Application to the Modified CSF Signature:** Dallot [20] 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 C.2.

Let us assume that \((n, k)\)-Goppa code over \(\mathbb{F}_q\) can decode up to \(t\) errors. Let \(T_{\text{cfs}} = (\text{Gen}_{\text{cfs}}, F_{\text{cfs}}, l_{\text{cfs}})\) be the underlying TDF of the modified CFS signature and \(\mathcal{X}_{n, \leq t} = \{x \in \mathbb{F}_q^n : 0 < \text{hw}(x) \leq t\}\) be a domain of \(F_{\text{cfs}},\) where \(\text{hw}(x)\) denotes a Hamming weight of \(x. \) \(F_{\text{cfs}} = U H_0 P (F_{\text{cfs}} : \mathcal{X}_{n, \leq t} \rightarrow \mathbb{F}_q^{n-k})\) 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 \(P \in \mathbb{F}_q^{n \times n}.\) One-to-one
Proposition B.1 (INV $\Rightarrow$ sEUF-CMA (Modified CFS Signature)). For any quantum sEUF-CMA adversary $A_{cma}$ of HaS[T_{cfs}, H] issuing at most $q_{sign}$ classical queries to the signing oracle and $q_{qro}$ (quantum) random oracle queries to $H \leftarrow \{Y_R \times M\}$, there exists an INV adversary $B_{inv}$ of $T_{cfs}$ such that

$$Adv_{HaS[T_{cfs}, H]}^{sEUF-CMA}(A_{cma}) \leq (2q_{qro} + 1)^2 Adv_{T_{cfs}}^{INV}(B_{inv}) + \frac{3}{2} q_{sign} \sqrt{\frac{q_{sign} + q_{qro} + 1}{|R|}} + 2(q_{qro} + 2) \sqrt{\frac{q_{sign} - q_{sign}}{|R|}},$$

where $q_{sign}$ is a bound on the total number of queries to $H$ in all the signing queries and the running time of $B_{inv}$ is about that of $A_{cma}$.

Proof. When we define SampDom(F_{cfs}) as $x \leftarrow X_{n, \leq t}$, $T_{cfs}$ becomes WPSF. Since $F_{cfs}$ is an injection, we can apply Corollary 4.1 to the modified CFS signature. In the PS game, we show that SampDom(F_{cfs}) in Sample_1 can perfectly simulate $x_i$ output by Sample_0. From the one-to-one correspondence between $X_{n, \leq t}$ and $Y_{dec}$, $x \leftarrow I_{cfs}(y)$ for $y \leftarrow Y_{dec}$ follows $U(X_{n, \leq t})$. Also, Sample_0 outputs $x_i$ after retrying $y_i \leftarrow U_{q,n}^k$ until $I_{cfs}(y_i) \neq \bot$ holds; therefore, $y_i$ is uniformly chosen from $Y_{dec}$. Hence, the distribution of $x_i$ output by Sample_0 is equivalent to that of $x_i \leftarrow SampDom(F_{cfs})$ and, thus, Adv_{T_{cfs}}^{PS}(D_{ps}) = 0 holds. \qed

Application to Wave: Wave is a practical and unbroken hash-and-sign signature [2]. See Appendix C.3 for the details.

Wave adopts the probabilistic hash-and-sign (without retry) and Wave’s TDF $T_{wave} = (Gen_{wave}, F_{wave}, I_{wave})$ satisfies conditions of average trapdoor PSF (ATPSF) [17, Definition 2] that is a special case of WPSF satisfying:

1. There is a bound $\delta$ on the average of $\delta_F, I \leftarrow Gen(1^k)$, that is, $E_{F,I}(\delta_F, I) \leq \delta$, where $\delta_F, I = \Delta(SampDom(F), I(U(Y)))$ is a statistical distance between SampDom(F) and I(y) for $y \leftarrow U(Y)$ (relaxed Condition 2).
2. I(y) outputs $x$ satisfying $F(x) = y$ for any $y \in Y$ (Condition 3).

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

Proposition B.2 (INV $\Rightarrow$ EUF-CMA (Wave)). For any quantum EUF-CMA adversary $A_{cma}$ of HaS[T_{wave}, H] issuing at most $q_{sign}$ classical queries to the signing oracle and $q_{qro}$ (quantum) random oracle queries to $H \leftarrow \{Y_R \times M\}$, there exists an INV adversary $B_{inv}$ of $T_{wave}$ such that

$$Adv_{HaS[T_{wave}, H]}^{EUF-CMA}(A_{cma}) \leq (2q_{qro} + 1)^2 Adv_{T_{wave}}^{INV}(B_{inv}) + q_{sign} \delta \frac{3}{2} q_{sign} \sqrt{\frac{q_{sign} + q_{qro} + 1}{|R|}.}$$
where the running time of $B_{\text{inv}}$ is about that of $A_{\text{cma}}$.

Proof. Since $T_{\text{wave}}$ is ATPSF \cite{17} that is a special case of WPSF, we can apply Theorem 4.1 to Wave. Since $\text{HaS}[T_{\text{wave}}, H]. \text{Sign}$ generates signatures without retry, $q'_{\text{sign}} = q_{\text{sign}}$ holds (the last term of Eq. (4) is 0). From the first condition of ATPSF, there is a bound $\delta$ on the expectation of $\delta_{F, i}$; therefore, $\text{Adv}^{\text{PS}}_{T_{\text{wave}}}(D_{\text{ps}}) \leq q_{\text{sign}} \delta$ holds from the union bound. \hfill \qed

Compared with the existing reduction using Eq. (1) \cite{17}, the factor of $\delta$ 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 $T_{\text{wave}}$ \cite{17, Proposition 8}.

B.2 Multivariate-quadratic-based Cryptography

Many schemes based on the UOV \cite{38} and HFE \cite{48} 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 \cite{52}.\footnote{Chatterjee et al. \cite{18} pointed out that the security proof of \cite{52} 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 \cite{52} can easily be corrected using the ROM version of our technique that is used in Theorem 4.1.} 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 \cite{10}.

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

Let $T_{\text{uov}} = (\text{Gen}_{\text{uov}}, F_{\text{uov}}, I_{\text{uov}})$ be a TDF used in the original UOV signature. $F_{\text{uov}} = P \circ S (F_{\text{uov}} : \mathbb{F}_q^n \to \mathbb{F}_q^n)$ consists of an invertible affine map $S : \mathbb{F}_q^n \to \mathbb{F}_q^n$ and a multivariate quadratic map $P : \mathbb{F}_q^n \to \mathbb{F}_q^n$. Variables in $P$ are called vinegar variables $z^v \in \mathbb{F}_q^n$ and oil variables $z^o \in \mathbb{F}_q^n$, where $n = v + o$. By design of $P$, $P(z^v, \cdot)$ becomes a set of linear functions on oil variables $z^o$ by fixing $z^v$. $I_{\text{uov}}$ chooses $z^v \leftarrow \mathbb{F}_q^n$ and obtains $z^o$ after retrying $z^v$ until $\{z^o : P(z^v, z^o) = H(r, m)\} \neq \emptyset$ holds (or $P(z^v, z^o)$ is full-rank).\footnote{The original UOV \cite{38} does not use $r$, but we here employ $r$.} See Fig. 13 for the signing algorithm and $I_{\text{uov}}$.

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

Proposition B.3 (INV $\Rightarrow$ EUF-CMA (Original UOV Signature)). For any quantum EUF-CMA adversary $A_{\text{cma}}$ of $\text{HaS}[T_{\text{uov}}, H]$ issuing at most $q_{\text{sign}}$ classical queries to the signing oracle and $q_{\text{oro}}$ (quantum) random oracle queries
to \( H \leftarrow \mathbb{Z}^{R \times M} \), there exist an INV adversary \( B_{inv} \) of \( T_{uov} \) and a PS adversary \( D_{ps} \) of \( T_{uov} \) issuing \( q_{sign} \) sampling queries such that

\[
\text{Adv}^{\text{EUF-CMA}}_{\text{HaS}[T_{uov}, H], \text{Sign}(l_{uov}, m)} \leq (2q_{qro} + 1)^2 \text{Adv}^{\text{INV}}_{T_{uov}}(B_{inv}) + \text{Adv}^{\text{PS}}_{T_{uov}}(D_{ps}) + \frac{3}{2} q_{sign} \frac{q_{sign} + q_{qro} + 1}{|R|},
\]

where the running times of \( B_{inv} \) and \( D_{ps} \) are about that of \( A_{cma} \).

**Proof.** Defining \( \text{SampDom}(F_{uov}) \) as \( x \leftarrow \mathbb{F}_q^n \), \( T_{uov} \) becomes WPSF; therefore, we can apply Theorem 4.1. Note that \( \text{HaS}[T_{uov}, H], \text{Sign} \) generates signatures without retry to take \( r \). Thus, \( q_{sign}' = q_{sign} \) holds as in Proposition B.2.

If the PS advantage \( \text{Adv}^{\text{PS}}_{T_{uov}}(D_{ps}) \) is negligible, the original UOV signature is provably secure. However, we must consider the computational indistinguishability of \( x \leftarrow l_{uov}(y) \) for \( y \leftarrow \mathbb{F}_q^2 \) and \( x \leftarrow \mathbb{F}_q^n \) in the PS game since \( x \) output by \( \text{HaS}[T_{uov}, H], \text{Sign} \) is not uniform. Note that we can apply Proposition B.3 to the UOV signature scheme recently submitted to the NIST PQC standardization [11] since it follows the original UOV signature.

**Application to the Modified UOV Signature:** Sakumoto et al. [52] 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 C.4.

Let \( T_{muov} = (\text{Gen}_{muov}, F_{muov}, l_{muov}) \) be a TDF used in the modified UOV signature (\( \text{Gen}_{muov} = \text{Gen}_{uov} \) and \( F_{muov} = F_{uov} \)) and Fig. 14 depicts \( \text{HaS}[T_{muov}, H], \text{Sign} \) and \( l_{muov} \). The modified UOV signature retries \( r \) instead of \( z'' \) and \( l_{muov} \) is divided into two functions; \( l_{muov}^1 \) and \( l_{muov}^2 \). \( l_{muov}^1 \) chooses \( z'' \leftarrow \mathbb{F}_q^2 \) and \( l_{muov}^2 \) finds \( z'' \) after retrying \( r \) until \( \{z'' : P(z'', z'') = H(r, m)\} \neq \emptyset \) holds. Considering the difference in the signing procedure, we show the EUF-CMA security of the modified UOV signature in the QROM.

**Proposition B.4 (INV \( \Rightarrow \) EUF-CMA (Modified UOV Signature)).** For any quantum EUF-CMA adversary \( A_{cma} \) of \( \text{HaS}[T_{muov}, H] \) issuing at most \( q_{sign} \) classical queries to the signing oracle and \( q_{qro} \) (quantum) random oracle queries
to $H \leftarrow \mathcal{S}^{\mathcal{R} \times \mathcal{M}}$, there exists an INV adversary $B_{\text{inv}}$ of $T_{\text{muov}}$ such that

$$
\text{Adv}^{\text{EUF-CMA}}_{\text{HaS}[T_{\text{muov}},H].\text{Sign}(I_{\text{muov}},m)}(A_{\text{cma}}) \leq (2q_{\text{qro}} + 1)^2 \text{Adv}^{\text{INV}}_{T_{\text{muov}}}(B_{\text{inv}}) + \frac{3}{2}q_{\text{sign}}^2 \sqrt{\frac{q_{\text{sign}} + q_{\text{qro}} + 1}{|\mathcal{R}|}} + 2(q_{\text{qro}} + 2) \sqrt{\frac{q_{\text{sign}} - q_{\text{sign}}}{|\mathcal{R}|}},
$$

where $q_{\text{sign}}$ is a bound on the total number of queries to $H$ in all the signing queries and the running time of $B_{\text{inv}}$ is about that of $A_{\text{cma}}$.

**Proof.** Defining $\text{SampDom}(F_{\text{muov}})$ as $x \leftarrow \mathcal{S}^{\mathcal{F}^n_q}$, $T_{\text{muov}}$ becomes WPSF. Considering the signing procedure of the modified UOV signature, we modify the signing oracles of $G_0-G_4$ and $\text{Sample}_0$ of the PS game by adding $z^o \leftarrow l^o_{\text{muov}}()$ in the beginning and replacing $x_i \leftarrow l(y_i)$ with $x_i \leftarrow l^2_{\text{muov}}(z^o, y_i)$. Then, $D_{\text{ps}}$ playing the modified PS game can simulate $G_4$ ($b = 0$) and $G_5$ ($b = 1$) in the proof of Theorem 4.1. Hence, we can apply Theorem 4.1 to the modified UOV signature. In $\text{Sample}_0$ of the PS game, $x_i \leftarrow l^2_{\text{muov}}(z^o, y)$ for $z^o \leftarrow l^1_{\text{muov}}()$ after retrying $y$ follows $U(\mathcal{F}^n_q)$ form [52, Theorem 1] (we show the proof sketch in Appendix C.4); therefore, $x_i \leftarrow \text{SampDom}(F_{\text{muov}})$ in $\text{Sample}_1$ is indistinguishable form $x_i$ output by $\text{Sample}_0$. Hence, $\text{Adv}^{\text{PS}}_{T_{\text{muov}}}(D_{\text{ps}}) = 0$ holds. $\square$

We can apply Proposition B.4 to Rainbow [22], QR-UOV [29], and PROV [26] 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. [52] is designed to be EUF-CMA secure in the ROM. For the details, see Appendix C.5.

Let $T_{\text{mhfe}} = (\text{Gen}_{\text{mhfe}}, F_{\text{mhfe}}, l_{\text{mhfe}})$ be a TDF used in the modified HFE scheme. We show that the modified HFE signature is EUF-CMA secure.

**Proposition B.5 (INV $\Rightarrow$ EUF-CMA (Modified HFE Signature)).** For any quantum EUF-CMA adversary $A_{\text{cma}}$ of $\text{HaS}[T_{\text{mhfe}},H]$ issuing at most $q_{\text{sign}}$ classical queries to the signing oracle and $q_{\text{qro}}$ (quantum) random oracle queries
to $H \leftarrow \mathcal{Y}^{R \times M}$, there exists an INV adversary $B_{\text{inv}}$ of $T_{\text{mhfe}}$ such that

$$Adv_{\text{HaS}[T_{\text{mhfe}}, H]}^{\text{EUF-CMA}}(A_{\text{cma}}) \leq (2q_{\text{qro}} + 1)^2 Adv_{T_{\text{mhfe}}}(B_{\text{inv}}) + \frac{3}{2} q_{\text{sign}} \sqrt{\frac{q_{\text{sign}} + q_{\text{qro}} + 1}{|\mathcal{R}|}}$$

$$+ 2(q_{\text{qro}} + 2) \sqrt{\frac{q_{\text{sign}} - q_{\text{sign}}}{|\mathcal{R}|}},$$

where $q_{\text{sign}}$ is a bound on the total number of queries to $H$ in all the signing queries and the running time of $B_{\text{inv}}$ is about that of $A_{\text{cma}}$.

Proof. Since $F_{\text{mhfe}}$ has a domain $F_q^n$, we can define $\text{SampDom}(F_{\text{mhfe}})$ as $x \leftarrow F_q^n$. Then, $T_{\text{mhfe}}$ becomes WPSF and we can apply Theorem 4.1 to the modified HFE scheme. The authors of [52] showed that $x \leftarrow l_{\text{mhfe}}(y)$ after retrying $y$ is uniformly distributed over $F_q^n$ (we show the proof sketch in Appendix C.5). Therefore, in the PS game, $x_i \leftarrow \text{SampDom}(F_{\text{mhfe}})$ in Sample$_i$ is indistinguishable from $x_i$ output by Sample$_0$, and thus, $Adv_{T_{\text{mhfe}}}(D_{\text{ps}}) = 0$ holds. \hfill \Box

We can apply Proposition B.5 to GeMSS [16] since GeMSS takes the same modification as the modified HFE signature.

Application to MAYO: MAYO, proposed by Beullens [10], is a signature scheme that adopts the probabilistic hash-and-sign and its TDF is based on UOV. For the details, see Appendix C.6.

Let $T_{\text{mayo}} = (\text{Gen}_{\text{mayo}}, \text{F}_{\text{mayo}}, l_{\text{mayo}})$ be a TDF used in MAYO. $l_{\text{mayo}}$ finds a preimage $x = x^o + x^v$ of $y$ for a multivariate quadratic map $P^* : F_q^{kn} \rightarrow F_q^n$. Once $x^v$ is uniformly chosen from $(F_q^{n-o} \times \{0\}^k) \subset F_q^n$, where $\{0\}$ denotes a vector of 0s, $P^*(x^v + x^o) = y$ becomes a linear system of equations for $x^o$. $l_{\text{mayo}}$ outputs a preimage after retrying $x^v$ until $P^*(x^v + x^o)$ has full rank. MAYO is EUF-CMA-secure in the ROM [10, Theorem 6] assuming that it follows no leakage parameter sets [10, Table 1]. For the parameter sets, $x$ is uniformly distributed over $F_q^n$ if $l_{\text{mayo}}$ outputs $x$ without retaking $x^v$. Let $\tau$ be a bound on the probability that $P^*(x^v + x^o)$ 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. \hfill 13

Proposition B.6 (INV$\Rightarrow$EUF-CMA (MAYO)). For any quantum EUF-CMA adversary $A_{\text{cma}}$ of $\text{HaS}[T_{\text{mayo}}, H]$ issuing at most $q_{\text{sign}}$ classical queries to the signing oracle and $q_{\text{qro}}$ (quantum) random oracle queries to $H \leftarrow \mathcal{Y}^{R \times M}$, there exists an INV adversary $B_{\text{inv}}$ of $T_{\text{mayo}}$ such that

$$Adv_{\text{HaS}[T_{\text{mayo}}, H]}^{\text{EUF-CMA}}(A_{\text{cma}}) \leq \frac{(2q_{\text{qro}} + 1)^2}{1 - q_{\text{sign}} \tau} Adv_{T_{\text{mayo}}}(B_{\text{inv}}) + \frac{3}{2} q_{\text{sign}} \sqrt{\frac{q_{\text{sign}} + q_{\text{qro}} + 1}{|\mathcal{R}|}},$$

where the running time of $B_{\text{inv}}$ is about that of $A_{\text{cma}}$.

For the other parameter sets, Proposition B.3 applies to MAYO.
Proof. We apply Theorem 4.1 with defining an intermediate game \( G'_1 \). \( G'_1 \) is the same as \( G_1 \) except that \( G'_1 \) aborts and outputs 0 whenever \( I_{\text{mayo}} \) retakes \( x^v \). The probability that \( G'_1 \) does not abort while \( q_{\text{sign}} \) signing queries is at least \( 1 - q_{\text{sign}} \). Therefore, \( \Pr[G'_1^{A_{\text{ms}}} \Rightarrow 1] \leq \frac{1}{1 - q_{\text{sign}}} \Pr[G'_1^{A_{\text{ms}}} \Rightarrow 1] \) holds. We define \( \text{SampDom}(F_{\text{mayo}}) \) 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 \( x \leftarrow I_{\text{mayo}}(y) \) follows \( U(\mathbb{F}_q^{kn}) \) if \( I_{\text{mayo}} \) 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 \( \Pr[G'_1^{A_{\text{ms}}} \Rightarrow 1] \leq \Pr[G_5^{A_{\text{ms}}} \Rightarrow 1] \) holds. Since the EUF-NMA adversary can simulate \( G_5 \), \( \Pr[G_5^{A_{\text{ms}}} \Rightarrow 1] \leq \text{Adv}_{\text{HaS}[T_{\text{mayo}}, H]}^{\text{EUF-NMA}}(A_{\text{ms}}) \) holds, which yields the claimed bound.

\( \square \)

C Review of Hash-and-sign Signatures

C.1 GPV Framework [30]

Let \( T_{\text{gpv}} = (\text{Gen}_{\text{gpv}}, F_{\text{gpv}}, I_{\text{gpv}}) \) be a TDF used in the GPV framework. \( \text{Gen}_{\text{gpv}} \) outputs a full-rank matrix \( A \in \mathbb{F}_q^{m \times n} \) generating a \( q \)-ary lattice \( \Lambda \) as \( F_{\text{gpv}} \) and a matrix \( B \) generating \( A_q^\perp \) that is orthogonal to \( \Lambda \) modulo \( q \) as \( I_{\text{gpv}} \). The function \( F_{\text{gpv}} \) 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 \( I_{\text{gpv}} \) outputs a short vector \( x \) for \( y \in \mathbb{F}_q^n \) using \( B \). \( T_{\text{gpv}} \) is a collision-resistant PSF (see Definition 2.6) whose security is based on the hardness of the short integer solution (SIS) problem [30, Theorem 4.9].

C.2 Modified CFS Signature [20]

Let \( T_{\text{cfs}} = (\text{Gen}_{\text{cfs}}, F_{\text{cfs}}, I_{\text{cfs}}) \) 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. \( X_{n, \leq t} = \{ x \in \mathbb{F}_q^n : 0 < \text{hw}(x) \leq t \} \) denotes a set of vectors \( x \in \mathbb{F}_q^n \) whose Hamming weight, denoted by \( \text{hw}(x) \), is \( t \). \( \text{Gen}_{\text{cfs}} \) 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 \( F_{\text{cfs}} \) and \( (U, H_0, P) \) as \( I_{\text{cfs}} \). On input \( x \in X_{n, \leq t} \), the function \( F_{\text{cfs}} \) computes a syndrome \( y := xH^T \in \mathbb{F}_q^{n-k} \). On input \( y \in \mathbb{F}_q^{n-k} \), the trapdoor \( I_{\text{cfs}} \) 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 \( X_{n, \leq t} \) and \( Y_{\text{dec}} = \{ y \in \mathbb{F}_q^{n-k} : y(U^{-1})^T \text{ is decodable} \} \) (decodable syndromes). Therefore, \( F_{\text{cfs}} \) is injective and \( I_{\text{cfs}}(y) \) outputs a preimage for \( y \leftarrow \mathbb{F}_q^{n-k} \) with probability \( \frac{|Y_{\text{dec}}|}{|\mathbb{F}_q^{n-k}|} = \frac{|X_{n, \leq t}|}{|\mathbb{F}_q^{n-k}|} \). As shown in [19], \( |X_{n, \leq t}| \approx \frac{1}{t} \) holds.

We show that a preimage \( x \) output by \( \text{HaS}[T_{\text{cfs}}, H] \cdot \text{Sign} \) follows \( U(X_{n, \leq t}) \). First, \( x \leftarrow I_{\text{cfs}}(y) \) for \( y \leftarrow \mathbb{F}_q^{n-k} \) with \( Y_{\text{dec}} \) follows \( U(X_{n, \leq t}) \) from the one-to-one correspondence between \( X_{n, \leq t} \) and \( Y_{\text{dec}} \). Next, \( \text{HaS}[T_{\text{cfs}}, H] \cdot \text{Sign} \) outputs \( x \) after retrying.
y \leftarrow \mathbb{F}_q^{n-k} \text{ until } l_{\text{ctf}}(y) \neq \perp \text{ holds; therefore } y \text{ follows } U(\mathcal{Y}_{\text{dec}}). \text{ Hence, } x \text{ output by HaS}[T_{\text{ctf}}, H]_{\text{Sign}} \text{ follows } U(\mathcal{X}_{n,\leq t}).

C.3 Wave [2]

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

$T_{\text{wave}}$ satisfies the conditions of ATPSF [17, Definition 2] and we can take a statistical bound on the distinguishing advantage of honestly generated signatures and simulated ones.

C.4 Original/Modified UOV Signature [38, 52]

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

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

and outputs $P \circ S$ as $F_{\text{uov}}$ and $(P, S)$ as $l_{\text{uov}}$. 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 $y \in \mathbb{F}_q^n$, $l_{\text{uov}}$ chooses $z^v \leftarrow \mathbb{F}_q^v$ and outputs $x = S^{-1}(z^v \parallel z^o)$ by solving a linear equation system $P(z^v, \cdot) = y$. There is possibly no solution. In the original UOV signature, $l_{\text{uov}}$ retries $z^v$ until $\{z^v : P(z^v, z^o) = y\} \neq \emptyset$ holds or $P(z^v, \cdot)$ has full rank [11] (see Fig. 13).

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

**Modified UOV signature:** To solve the above problem, Sakamoto et al. [52] proposed the modified UOV signature. Instead of retaking $z^o$, the modified UOV signature retakes the randomness $r$ for the hash function. The signing procedure of the modified UOV signature (see Fig. 14) is different from the others. HaS$[T_{\text{muov}}, H]$ using $l_{\text{muov}}^1$ and $l_{\text{muov}}^2$ generates a signature as follows: $l_{\text{muov}}^1$ chooses vinegar variables $z^v$ uniformly at random. Fixing $z^v$, $P$ becomes a set of linear
functions on oil variables \( z^o \). \( \lambda_{\muov}^2 \) finds a preimage of \( P \circ S \) by solving a linear equation system and taking the inverse of \( S \). If there is no solution, \( \lambda_{\muov}^2 \) outputs \( \perp \) and \( \text{HaS}[T_{\muov}, H] \) retakes \( r \) and executes \( \lambda_{\muov}^2 \) again without retaking \( z^v \).

Sakamoto et al. showed that preimages generated by \( \text{HaS}[T_{\muov}, H], \text{Sign} \) are uniformly distributed over \( \mathbb{F}_q^o \). For completeness, we give the proof sketch.

In the beginning, \( z^v \) is uniformly chosen, that is, \( z^v \) follows \( \mathbb{U}(\mathbb{F}_q^o) \). By fixing \( z^v \), \( P(z^v, \cdot) \) 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 \( i \), \( P(z^v, \cdot) \) 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 \( \{ z^o : P(z^v, z^o) = H(r, m) \} \neq \emptyset \). 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 \( \mathbb{U}(\mathbb{F}_q^o) \) and thus \( x = S^{-1}(z^v \parallel z^o) \) follows \( \mathbb{U}(\mathbb{F}_q^o) \).

In Proposition B.4, we cannot take \( q_{\text{sign}} \) as in the other schemes since the probability that \( l_{\muov}(z^v, y) \) outputs \( \perp \) varies depending on \( z^v \). We set \( q_{\text{sign}} = q_{\text{retry}} q_{\text{sign}} \), where \( q_{\text{retry}} \) 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 \( X = \sum_{i=1}^{q_{\text{sign}}} X_i \). We have

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

where \( p_j \) is a probability that \( P(z^v, \cdot) \) has rank \( j \) for \( z^v \) \( \overset{\circ}{\leftarrow} \mathbb{F}_q^o \). 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 [7]:

\[
\frac{1}{q^{o^2}} \prod_{k=1}^{o}(1 - q^{-k}) \prod_{k=a+1}^{o}(1 - q^{-k}) \prod_{k=1}^{a}(1 - q^{-k}).
\]

(13)

When we assume that \( P(z^v, \cdot) \) becomes a random \( o \times o \) matrix for any \( z^v \), \( p_j \) follows Eq. (13). Since \( X > q_{\text{sign}} \) implies \( \exists x, X_i > q_{\text{retry}} \), \( \Pr[X > q_{\text{sign}}] \leq q_{\text{sign}} \Pr[X_i > q_{\text{retry}}] \) holds. To determine an appropriate value for \( q_{\text{sign}} = q_{\text{retry}} q_{\text{sign}} \) in the security bound, we need to take \( q_{\text{retry}} \) such that \( q_{\text{sign}} \Pr[X_i > q_{\text{retry}}] \) is negligible for the security parameter.

C.5 Modified HFE Signature [52]

Let \( T_{\muhfe} = (\text{Gen}_{\muhfe}, F_{\muhfe}, l_{\muhfe}) \) be a TDF used in the modified HFE signature and \( \phi : K \rightarrow \mathbb{F}_q^n \) be a standard linear isomorphism \( \phi(a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}) = (a_0, a_1, \ldots, a_{n-1}) \), where \( K = \mathbb{F}_q[x]/g(x) \) for an irreducible polynomial \( g(x) \) of degree \( n \). \( \text{Gen}_{\muhfe} \) generates invertible affine maps \((S, S')\) over \( \mathbb{F}_q^n \) and a central map \( P : K \rightarrow K \) defined as

\[
P(X) = \sum_{(i, j) \in |n| \times |n|} \alpha_{i,j} X^{q^{i-1} + q^{j-1}} + \sum_{i \in |n|} \beta_{i} X^{q^{i-1}},
\]

s.t. \( q^{i-1} + q^{j-1} < d \)

s.t. \( q^{i-1} < d \)

40
The notation of UOV in MAYO follows [9] which is a generalization of the traditional

tured to be non-invertible. Therefore, the

parameter. On input matrices such that

which is bilinear. We define the polar form of multivariate quadratic map

such that

mayo

ty description of Appendix C.4.

On input $y \in \mathbb{F}_q^{n-m}$, $l_{\text{mhfe}}$ computes a preimage $x \in \mathbb{F}_q^n$ as in Fig. 15.

As in the modified UOV signature, the authors of [52] showed that preimages generated by $\text{HaS}[T_{\text{mhfe}}, H].\text{Sign}$ 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 $\frac{|\{z': P(z') = z\}|}{N}$, $l_{\text{mhfe}}$ chooses $z'$ out of $\{|z': P(z') = z\}$ elements, where $N$ is set as $d$ in general. Therefore, for any $x \in \mathbb{F}_q^n$, $\text{HaS}[T_{\text{mhfe}}, H].\text{Sign}$ outputs $x$ with probability

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

Hence, preimages output by $\text{HaS}[T_{\text{mhfe}}, H].\text{Sign}$ are uniformly distributed over $\mathbb{F}_q^n$. Also, $l_{\text{mhfe}}$ does not output $\bot$ with probability $\sum_{x \in \mathbb{F}_q^n} \frac{1}{q^n N} = \frac{1}{N}$.

C.6 MAYO [10]

Let $T_{\text{mayo}} = (\text{Gen}_{\text{mayo}}, F_{\text{mayo}}, l_{\text{mayo}})$ be a TDF used in MAYO. $\text{Gen}_{\text{mayo}}$ generates a multivariate quadratic map $P: \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ with a subspace $O \subset \mathbb{F}_q^n$ of dimension $o$ called oil space such that $P(x) = 0$ for any $x \in O$, and outputs $P$ as $F_{\text{mayo}}$ and a basis of $O$ as $l_{\text{mayo}}$.\footnote{The notation of UOV in MAYO follows [9] which is a generalization of the traditional description of Appendix C.4.} Let $P(x) = (p_1(x), \ldots, p_m(x))$, where $p_i(x): \mathbb{F}_q^n \rightarrow \mathbb{F}_q$ is a multivariate quadratic polynomial. The polar form of $p(x)$ is defined as

$p'(x, y) := p(x + y) - p(x) - p(y),$

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

Let $\mathcal{I} = \{(i, j) \in [k] \times [k] : i < j\}$ and $\{E_{ij}\}_{(i, j) \in \mathcal{I}}$ be a set of invertible matrices such that $E = \{E_{ij}\}$ is nonsingular. We set $\{E_{ij}\}_{(i, j) \in \mathcal{I}}$ as a system parameter. On input $x = (x_1, \ldots, x_k) \in \mathbb{F}_q^n$, $F_{\text{mayo}}$ computes $y = P^*(x) = \sum_{i \in [k]} E_{i, 0} P(x_i) + \sum_{(i, j) \in \mathcal{I}} E_{ij} P'(x_i, x_j)$. In MAYO, $P^*: \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$ is conjectured to be non-invertible. Therefore, the INV game of $T_{\text{mayo}}$ is defined as:
given \((P, \{E_{ij}\}_{(i,j) \in I})\), find \(x^* = (x_1^*, \ldots, x_k^*)\) satisfying \(\sum_{i \in [k]} E_{ii} P(x_i^*) + \sum_{(i,j) \in I} E_{ij} P(x_i^*, x_j^*)\) \cite{10, Definition 4}. On input \(y \in \mathbb{F}_q^m\), \(l_{\text{mayo}}\) computes \(x\) as in Fig. 16. Let \(x, x^0\) and \(x^o\) be vectors over \(\mathbb{F}_q^{kn}\). \(l_{\text{mayo}}\) 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 \(x^v\), \(P^*(x^v + x^o) = y\) becomes a linear system of equations for \(x^o\). If \(P^*(x^v + x^o)\) has full rank, \(l_{\text{mayo}}\) outputs \(x^v + x^o\) by solving \(P^*(x^v + x^o) = y\). Otherwise, \(l_{\text{mayo}}\) retakes \(x^v\). The probability that \(P^*(x^v + x^o)\) does not have full rank is bounded by \(\tau = \frac{q^{k-o} + q^{m-k-o}}{q - 1}\) \cite{10, Lemma 2}. For no leakage parameter sets \cite{10, Table 1}, \(\tau \leq 2^{-65}\) holds.

A preimage \(x \leftarrow l_{\text{mayo}}(y)\) is uniform over \(\mathbb{F}_q^{kn}\) if \(l_{\text{mayo}}\) does not take \(x^v\) in the signature generation \cite{10, Lemma 7}. Since this property is necessary for applying Theorem 4.1, we show the proof sketch.

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

\section{Proof of Lemma 5.1}
First, we extend Theorem 4.1 to prove the following lemma:

\textbf{Lemma D.1 (M-INV \Rightarrow M-EUF-CMA).} For any quantum M-EUF-CMA adversary \(A_{\text{cmam}}\) of \(\text{HaS}^p_{\text{psf}, H, E}\) with \(q_{\text{key}}\) keys and issuing at most \(q_{\text{sign}}\) classical queries to the signing oracle and \(q_{\text{qro}}\) (quantum) random oracle queries to \(H \leftarrow_{\text{qs}} \mathcal{X} \times \mathcal{R} \times \mathcal{M}\), there exist an M-INV \(B_{\text{invm}}\) of \(T_{\text{psf}}\) with \(q_{\text{inst}}\) instances and an M-PS adversary \(D_{\text{psm}}\) of \(T_{\text{psf}}\) with \(q_{\text{key}}\) instances and issuing \(q_{\text{sign}}\) sampling queries such that

\[
\text{Adv}_{\text{HaS}^p_{\text{psf}, T_{\text{psf}}, H, E}}(A_{\text{cmam}}) \leq (2q_{\text{qro}} + 1)^2 \text{Adv}_{T_{\text{psf}}}^\text{M-INV}(B_{\text{invm}}) + \text{Adv}_{T_{\text{psf}}}^\text{M-PS}(D_{\text{psm}}) + 3q_{\text{sign}} \sqrt{\frac{q_{\text{sign}} + q_{\text{qro}} + 1}{|R|}} + 2(q_{\text{qro}} + 2) \sqrt{\frac{q_{\text{sign}} - q_{\text{sign}}^2}{|R|}} + q_{\text{key}} \frac{|U|}{|U'|},
\]

(14)

where \(q_{\text{sign}}\) is a bound on the total number of queries to \(H\) in all the signing queries, \(\mathbb{E}_F(1|\text{inst}) \leq q_{\text{key}} \left(\frac{|U'|}{|U'| - q_{\text{sign}} + 1}\right)\) holds, and the running times of \(B_{\text{invm}}\) and \(D_{\text{psm}}\) are about that of \(A_{\text{cmam}}\).
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. 17 as $\text{Adv}_{\text{M-EUF-NMA}}(A_{\text{nma}}) = \Pr_{\text{M-EUF-NMA}}[A_{\text{nma}} \Rightarrow 1]$. Without loss of generality, we assume that adversaries make random oracle queries while fixing key ID $u$ to be one of the $q_{\text{key}}$ verification keys.

**M-EUF-NMA ⇒ M-EUF-CMA:**

**GAME $G_0$ (M-EUF-CMA game):** This is the original M-EUF-CMA game and $\Pr[G_0^{\text{cma}} \Rightarrow 1] = \text{Adv}_{\text{M-EUF-CMA}}^{\text{M-EUF-CMA}}(T_{\text{cmp}}, H, E)(A_{\text{cma}})$ holds.

**GAME $G_1$ (adaptive reprogramming and puncturing of H):** In the same manner as $G_4$ of Theorem 4.1, the challenger chooses $r \leftarrow R$ for $q_{\text{sign}}' - q_{\text{sign}}$ times and keeps them in a sequence $S$, punctures $H$ by $S' = \{u \in U, r \in S, m \in M\}$, and outputs 0 if FIND = $\top$. Also, the signing oracle reprograms $H := H(E(r), r, m_j) \rightarrow y_i$ after repeating $r_i \leftarrow R$ and $y_i \leftarrow Y$ until $l_j(y_i)$ does not output $\bot$. 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 $G_0/G_1, G_1/G_2, and G_3/G_4 in Theorem 4.1. Since these numbers are the same in both the single-key and multi-key settings, we can apply the same bound as $G_0/G_4 in Theorem 4.1. Thus, we have

$$\left| \Pr[G_0^{\text{cma}} \Rightarrow 1] - \Pr[G_1^{\text{cma}} \Rightarrow 1] \right| \leq \frac{3}{2} q_{\text{sign}}' \sqrt{\frac{q_{\text{sign}}' + q_{\text{qro}} + 1}{|R|}} + 2(q_{\text{qro}} + 2) \sqrt{\frac{q_{\text{sign}}' - q_{\text{sign}}}{|R|}}.$$  

**GAME $G_2$ (simulating the signing oracle by $\text{SampDom}$):** The signing oracle reprograms $H := H(E(r_j), r_j, m_j) \rightarrow F_j(x_i)$ for $r_i \leftarrow R$ and $x_i \leftarrow \text{SampDom}(F_j)$, and outputs $(r_i, x_i)$. Since the M-PS adversary can simulate $G_1/G_2$, we have

$$\left| \Pr[G_1^{\text{cma}} \Rightarrow 1] - \Pr[G_2^{\text{cma}} \Rightarrow 1] \right| \leq \text{Adv}_{\text{M-PS}}^{\text{M-PS}}(D_{\text{ps}}).$$

Since the M-EUF-NMA adversary $A_{\text{nma}}$ can simulate $G_2 by \text{SampDom}$, $\Pr[G_2^{\text{cma}} \Rightarrow 1] \leq \text{Adv}_{\text{M-EUF-NMA}}^{\text{M-EUF-NMA}}(T_{\text{cmp}}, H, E)(A_{\text{nma}})$ holds. As above, we have

$$\text{Adv}_{\text{M-EUF-CMA}}^{\text{M-EUF-CMA}}(T_{\text{cmp}}, H, E)(A_{\text{cma}}) \leq \text{Adv}_{\text{M-EUF-NMA}}^{\text{M-EUF-NMA}}(T_{\text{cmp}}, H, E)(A_{\text{nma}}) + \text{Adv}_{\text{M-PS}}^{\text{M-PS}}(D_{\text{ps}}) \leq \frac{3}{2} q_{\text{sign}}' \sqrt{\frac{q_{\text{sign}}' + q_{\text{qro}} + 1}{|R|}} + 2(q_{\text{qro}} + 2) \sqrt{\frac{q_{\text{sign}}' - q_{\text{sign}}}{|R|}}.$$  

Fig. 17: M-EUF-NMA (Multi-key EUF-NMA) game
We obtain Eq. (14) by combining the two reductions.

\[ \sum_{i=1}^{n_{\text{inst}}} \frac{|U| - i}{|U| - \theta + 1} \leq q_{\text{key}} \left( \frac{|U|}{|U| - q_{\text{key}} + 1} \right). \]

A two-stage algorithm \( S \) composed of \( S_1 \) and \( S_2 \) operates as follows:

1. Choose \((i, b) \leftarrow S((q_{\text{qro}}) \times \{0, 1\}) \cup \{(q_{\text{qro}} + 1, 0)\}.\)
2. Run \( A_{\text{nma}} \) with \( H \) until \( i \)-th query.
3. Measure \( i \)-th query and output \((u, r, m)\) as the output of \( S_1 \).
4. Given a random \( \theta \), reprogram \( H' = H^{(u, r, m)} \)
5. If \( i = q_{\text{qro}} + 1 \), then go to Step 8.
6. Answer \( i \)-th query with \( H \) (if \( b = 0 \)) or \( H' \) (if \( b = 1 \)).
7. Run \( A_{\text{nma}} \) with \( H' \) until the end.
8. Output \( A_{\text{nma}} \)'s output \((j^*, m^*, r^*, x^*)\) as the output of \( S_2 \).

Since there is no collision on key IDs, \( B_{\text{nma}} \) can understand the target key of the observed random oracle query. If \( u = E(F_j), B_{\text{nma}} \) sets \( \theta = y_j \), reprograms \( H \) as \( H' := H^{(u, r, m)} \)

By summing over all \( j \in [q_{\text{qro}}] \), we have \( \text{Adv}_{\text{M-INV}}(B_{\text{nma}}) \geq \frac{1}{(2q_{\text{qro}} + 1)^2} \text{Pr}[G_{\text{INV}} \Rightarrow 1]. \)

Then, we extend the proof of \( \text{M-INV} \Rightarrow \text{M-EUF-NMA} \) in Lemma D.1 by introducing a new game, \( G_5 \). In \( G_5 \), the verification keys \( \{F_j\}_{j \in [q_{\text{qro}}]} \) are replaced with \( \{L_j \circ F' \circ R_j\} \), where \( F' : X' \rightarrow Y \) is generated by \( \text{Gen}' \). The ST adversary \( D_{\text{ST}} \) can simulate \( G_4 \) and \( G_5 \) by setting the verification keys based on the outcomes of

\[ \text{Pr}[G_{\text{nma}}^\text{INV} \Rightarrow 1] \]
Proof. We define a sequence of games as follows:

\[ \text{GAME } G_6 \] (M-CR game): This is the original M-CR game and \( \Pr[G_6^{\text{cr}} \Rightarrow 1] = \text{Adv}^{\text{M-CR}}_{\text{M-CR}}(\mathcal{A}_{\text{cr}}) \) holds. 

\[ \text{GAME } G_1 \] (abort with collision on key IDs): When a collision of the key IDs is detected, \( G_1 \) aborts and outputs 0. We have \( \Pr[G_1^{\text{cr}} \Rightarrow 1] \leq \frac{q_{\text{sym}}^2}{|\mathcal{U}|} \).

\[ \text{GAME } G_2 \] (replacing \( H \) with \( H' \)): This game replaces \( H \) with \( H' \) satisfying

\[ H' = \text{DetSampDom} \left( F_j, \tilde{H}(E(F_j), r, m) \right), \]

where \( \text{DetSampDom} \) is a deterministic function of \( \text{SampDom} \) and \( \tilde{H} : \mathcal{U} \times \mathcal{R} \times \mathcal{M} \rightarrow \mathcal{W} \) is another random function to output randomness for \( \text{DetSampDom} \). From Condition 1 of PSF, \( F_j(x) \) is uniform for \( x \leftarrow \text{SampDom}(F_j) \). Since \( H \) and \( H' \) follow the same distribution, \( \Pr[G_1^{\text{cr}} \Rightarrow 1] = \Pr[G_2^{\text{cr}} \Rightarrow 1] \) holds.

By combining Eq. (15) and Eq. (16), we arrive at Eq. (11).
The M-CR adversary $B_{cr^m}$ can simulate $G_2$. As in Lemma D.1, the expected number of instances is at most $q_{key} \left( \frac{\lambda}{|\mathcal{D}| - q_{m} + 1} \right)$ over all $(F, 1) \leftarrow \text{Gen}(1^{\lambda})$. From **Conditions 2** and 3, the M-CR adversary $B_{cr^m}$ can simulate the signing oracle. When responding to the $i$-th signing query $m_i$ for the $j$-th verification key $F_j$, $B_{cr^m}$ returns $(r_i, x_i)$, where $r_i \leftarrow \mathcal{R}$ and $x_i := \text{DetSampDom} \left( F_j, \text{H}(F_j, r_i, m_i) \right)$. If the M-sEUF-CMA adversary $A_{cr^m}$ wins the game by submitting $(j^*, m^*, r^*, x^*)$, $F_j, (x^*) = F_j, (x')$ holds, where $x' = \text{DetSampDom}(F_j, \text{H}(E(F_j), r^*, m^*))$. From **Condition 4**, $x^* \neq x'$ holds with probability $1 - 2^{-\omega(\log(\lambda))}$, and we thus have Eq. (17).

Then, we show a reduction of $CR \Rightarrow M$-CR. We define a sequence of games as follows:

**GAME $G_0$ (M-CR game):** This is the original M-CR game and $\Pr[G_0^{B_{cr^m}} \Rightarrow 1] = \text{Adv}^\text{M-CR}_{\text{cr}}(B_{cr^m})$ holds.

**GAME $G_1$ (replacing verification keys):** We replace $F_j$ with $L_j \circ F' \circ R_j$. Since the ST adversary can simulate $G_0/G_1$, we have $|\Pr[G_0^{B_{cr^m}} \Rightarrow 1] - \Pr[G_1^{B_{cr^m}} \Rightarrow 1]| \leq \text{Adv}^\text{ST}_{\text{cr}}(D_{st})$.

The CR adversary $B_{cr}$ simulates $G_1$ as follows: Given $F'$, $B_{cr}$ gives $\{L_j \circ F' \circ R_j\}_{j \in [q_m]}$ to $B_{cr^m}$. When $B_{cr^m}$ submits $(j^*, x_1^*, x_2^*), B_{cr}$ outputs $(R_{j^*}(x_1^*), R_{j^*}(x_2^*))$. Suppose that $L_j \circ F(R_j, (x_i)) = L_j \circ F(R_j, (x'_i))$ holds. Since $L_j$ is injective, $F(R_j, (x_1^*)) = F(R_j, (x_2^*))$ holds and $x_1^* \neq x_2^*$ implies $R_{j^*}(x_1^*) \neq R_{j^*}(x_2^*)$. Therefore, $B_{cr}$ can win the CR game and can perfectly simulate $G_4$. Therefore, we have

$$\text{Adv}^\text{M-CR}_{\text{cr}}(B_{cr^m}) \leq \text{Adv}^\text{CR}_{\text{cr}}(B_{cr}) + \text{Adv}^\text{ST}_{\text{cr}}(D_{st}).$$  \hfill (18)

Combining Eq. (18) with Eq. (17), we obtain the security bound of Lemma 5.2.

**F Applications of Generic Method in Multi-key Setting**

In this section, we explore the applications of the generic method presented in **Lemma 5.2** for lattice-based cryptography and **Lemma 5.1** for code-based cryptography. Rather than focusing on specific schemes such as FALCON [51], our paper applies the generic method to frameworks of the schemes, such as the GPV framework [30]. 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 C.1**) [30]. For **Lemma 5.2**, we design simulation of verification keys by $\{L_j \circ A R_j\}_{j \in [q_m]}$ 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 $\pm 1$. Then, the ST advantage is bounded by an advantage of the following problem.
Definition F.1 (Multi-instance Signed Permutation Equivalence).
Given matrices \( \{G_j\}_{j \in [q_{\text{inst}}]} \) (\( G_j \in \mathbb{F}_q^{n \times m} \)), do there exist a matrix \( G \in \mathbb{F}_q^{n \times m} \), \( n \times n \) invertible matrices \( \{L_j\}_{j \in [q_{\text{inst}}]} \) over \( \mathbb{F}_q \), and \( m \times m \) signed permutation matrices \( \{R_j\}_{j \in [q_{\text{inst}}]} \) over \( \mathbb{F}_q \) such that \( G_j = L_jGR_j \)?

This problem is a variant of the well-studied problem called code equivalence in code-based cryptography [50]. 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)[54].

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 [50]. 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 \( w \) [39], and Beullens [8] recently improved this algorithm. The complexity of this approach grows exponentially with \( w \), and we cannot solve the problems with low \( w \) [4]. There is a special case where we can easily solve the permutation equivalence with the Support Splitting Algorithm (SSA) proposed by Sendrier [53]. The SSA runs in \( O(m^3 + m^2q^h \ln(m)) \), where \( h \) is a dimension of the hull space of a code, that is, the intersection between the code and its dual code [4]. 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 C.2 and C.3). For Lemma 5.1, we simulate verification keys by \( \{L_jHR_j\}_{j \in [q_{\text{inst}}]} \), 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 F.2 (Multi-instance Linear Equivalence).** Given matrices \( \{G_j\}_{j \in [q_{\text{inst}}]} \) (\( G_j \in \mathbb{F}_q^{n \times m} \)), do there exist a matrix \( G \in \mathbb{F}_q^{n \times m} \), \( n \times n \) invertible matrices \( \{L_j\}_{j \in [q_{\text{inst}}]} \) over \( \mathbb{F}_q \), and \( m \times m \) generalized permutation matrices \( \{R_j\}_{j \in [q_{\text{inst}}]} \) over \( \mathbb{F}_q \) such that \( G_j = L_jGR_j \)?

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 \( F: \mathbb{F}_q^m \rightarrow \mathbb{F}_q^m \) and
\( F_j : \mathbb{F}_q^{n'} \rightarrow \mathbb{F}_q^m \) be a multivariate quadratic map \((n' \geq n)\). For Lemma 5.1, we simulate verification keys by \( \{ L_j \circ F \circ R_j \}_{j \in [q\text{key}]} \), 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 F.3 (Multi-instance Decision Morphism of Polynomials).**

Given multivariate quadratic maps \( \{ F_j \}_{j \in [q\text{inst}]} \), do there exist a multivariate quadratic map \( F \) and affine maps \( \{ L_j \}_{j \in [q\text{inst}]} \) and \( \{ R_j \}_{j \in [q\text{inst}]} \) over \( \mathbb{F}_q \) such that \( F_j = L_j \circ F \circ R_j ? \)

The (single-instance) decision morphism of polynomials, that is, given a pair of multivariate quadratic maps \((F,F')\), do there exist affine maps \( L \) and \( R \) such that \( F' = L \circ F \circ R \), is proven NP-complete [49]. If \( L \) and \( R \) are invertible affine maps, this problem is called decision isomorphism of polynomials that is in the complexity class \( \text{coAM} \) and not conjectured to be NP-hard [49]. 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 [56]; 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 [15] studied and surveyed the algorithms for the isomorphism of polynomials. Their algorithms run in \( O(q^{n'}) \cdot \text{poly}(n,q) \), \( O(q^{2n'/3}) \cdot \text{poly}(n,q) \), or \( O(q^{n/2}) \cdot \text{poly}(n,q) \) assuming that \( n = m \). The Gröbner-based algorithm proposed by Faugère and Perret [27] 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., [35]).

### G Security Proof of Fiat-Shamir with Aborts

We consider a signature scheme adopting the Fiat-Shamir with aborts paradigm. We define a 3-round public-coin identification scheme with aborts.

**Definition G.1 (3-round Public-coin Identification Scheme with Aborts).**

A 3-round public-coin identification scheme with aborts, denoted as \( \text{ID} \), consists of four algorithms:

- \( \text{Gen}(1^\lambda) \): This algorithm takes the security parameter \( 1^\lambda \) as input and outputs a public key \( pk \) and a secret key \( sk \).
- \( \text{P}_1(sk) \): This algorithm takes a secret key \( sk \) as input and outputs a commitment \( w \in \mathcal{W} \) and a state \( st \).
- \( \text{P}_2(sk, w, c, st) \): This algorithm takes a secret key \( sk \), a commitment \( w \in \mathcal{W} \), a randomly chosen challenge \( c \leftarrow \mathcal{C} \), and a state \( st \) as input and outputs a response \( z \in \mathcal{Z} \) or outputs \( \bot \).
- \( \text{V}(pk, w, c, z) \): This algorithm takes a public key \( pk \), a commitment \( w \in \mathcal{W} \), a challenge \( c \in \mathcal{C} \), and a response \( z \in \mathcal{Z} \) (a transcript) as inputs and outputs \( \top \) (acceptance) or \( \bot \) (rejection).
Let $\text{Sim}$ denote a simulator for $\text{ID}$, which takes a public key $pk$ as its input and yields a transcript in the form of $(w, c, z)$ as its output. To establish the indistinguishability between a transcript generated honestly and one generated through simulation, we introduce an accepting HVZK game.

**Definition G.2 (Accepting HVZK ($A$-HVZK) Game).** Let $\text{ID}$ be a 3-round public-coin identification scheme with aborts. Using a game defined in Fig. 18, we define an advantage function of an adversary playing the $A$-HVZK game against $\text{ID}$ as $\text{Adv}_{\text{ID}}^{A\text{-HVZK}}(D_{\text{zk}}) = \text{Pr}[A\text{-HVZK}^D_{\text{zk}} \Rightarrow 1] - \text{Pr}[A\text{-HVZK}^0_{\text{zk}} \Rightarrow 1]$.

We can construct a signature scheme, denoted as $\text{FSwA}[\text{ID}, H]$, from $\text{ID}$ as depicted in Fig. 19. The security reduction for this scheme can be provided using the same techniques as presented in Theorem 4.1.

**Theorem G.1 (EUF-NMA $\Rightarrow$ EUF-CMA).** For any quantum EUF-CMA adversary $A_{\text{cma}}$ of $\text{FSwA}[\text{ID}, H]$ issuing at most $q_{\text{sign}}$ classical queries to the signing oracle and $q_{\text{qro}}$ (quantum) random oracle queries to $H \leftarrow \mathcal{S}(W \times M)$, there exist an EUF-NMA adversary $A_{\text{nma}}$ of $\text{FSwA}[\text{ID}, H]$ issuing $q_{\text{qro}}$ (quantum) random oracle queries to $H$ and an $A$-HVZK adversary $D_{\text{zk}}$ of $\text{ID}$ issuing $q_{\text{sign}}$ sampling queries such that

$$\text{Adv}_{\text{FSwA}[\text{ID}, H]}^{\text{EUF-CMA}}(A_{\text{cma}}) \leq \text{Adv}_{\text{FSwA}[\text{ID}, H]}^{\text{EUF-NMA}}(A_{\text{nma}}) + \text{Adv}_{\text{ID}}^{A\text{-HVZK}}(D_{\text{zk}})$$

$$+ \frac{3}{2} q_{\text{sign}} \sqrt{(q_{\text{sign}} + q_{\text{qro}} + 1) \epsilon + 4(q_{\text{qro}} + 2) \sqrt{q_{\text{sign}} - q_{\text{sign}}}} \epsilon,$$

where $q_{\text{sign}}$ is a bound on the total number of queries to $H$ in all the signing queries, $\max_{z \in W} \text{Pr}[w = \tilde{w} : (w, st) \leftarrow P_1(sk)] \leq \epsilon$ holds except with negligible probability, and the running times of $A_{\text{nma}}$ and $D_{\text{zk}}$ are about that of $A_{\text{cma}}$. 49
**Proof.** As in Theorem 4.1, we can set $q'_{\text{sign}} = \frac{c}{\rho} q_{\text{sign}}$ for some constant $c > 1$, where $\rho = \Pr[z \neq \perp : (w, st) \leftarrow P_1(sk), c \leftarrow G, z \leftarrow P_2(sk, w, c, st)]$. To show Eq. (19), we use a sequence of games defined in Fig. 20.

![Table](https://example.com/table.png)

Fig. 20: Games for EUF-NMA \rightarrow EUF-CMA for Fiat-Shamir with aborts.
GAME $G_0$ (EUF-CMA game): This is the original EUF-CMA game and $Pr[G_0^{\text{cma}} \Rightarrow 1] = Adv_{EUF-CMA}^{\text{cma}}(\mathcal{A}_{\text{cma}})$ holds.

GAME $G_1$ (adaptive reprogramming of $H$): The signing oracle $\text{Sign}^H$ adaptively reprograms $H$. This reprogramming occurs as $H := H^{(w, m) \rightarrow c_i}$, where $(w_i, s_i) \leftarrow P_1(sk)$ and $c_i \leftarrow \mathcal{C}$, and this process repeats until $P_2(s_k, w_i, c_i, s_t)$ no longer outputs $\perp$. The AR adversary $D_{\text{ar}}$ can simulate the games $G_0$ and $G_1$. When $D_{\text{ar}}$ plays $AR_0$, it simulates $G_0$; otherwise, it simulates $G_1$. According to Lemma 2.1, the difference between $Pr[G_0^{\text{cma}} \Rightarrow 1]$ and $Pr[G_1^{\text{cma}} \Rightarrow 1]$ can be bounded as follows:

$$|Pr[G_0^{\text{cma}} \Rightarrow 1] - Pr[G_1^{\text{cma}} \Rightarrow 1]| \leq Adv_{EUF-CMA}^{AR}(D_{\text{ar}}) \leq \frac{3}{2} q_{\text{sign}} \sqrt{(q_{\text{sign}} + q_{\text{qro}} + 1)\epsilon}.$$

GAME $G_2$ (pre-generating transcripts): At the start, the challenger pre-generates $q_{\text{sign}}$ accepting transcripts for ID along with non-accepting ones. An accepting transcript is denoted as $(w_i, c_i, z_i)$, and non-accepting transcripts are stored in $\mathcal{S}_{i}$. During the $i$-th query, the signing oracle reprograms $H$ as $H^{(w, m) \rightarrow c}$ for $(w, c, z) \in \mathcal{S}_{i}$ as well as for $(w, c, z) = (w_i, c_i, z_i)$. This pre-generation of transcripts is feasible since they are chosen independently of adaptively queried messages $m_i$ from $\mathcal{A}_{\text{cma}}$ in $G_1$, ensuring that $Pr[G_1^{\text{cma}} \Rightarrow 1] = Pr[G_2^{\text{cma}} \Rightarrow 1]$.

GAME $G_3$ (puncturing $H$): Let $\mathcal{S} = \{w: (w, *, *) \in \bigcup_i S_i \}$ and $\mathcal{S}' = \{(w, m): w \in S, m \in M\}$. We define a punctured oracle $H \setminus \mathcal{S}'$ and an event $\text{FIND}$. In $G_3$, instead of querying $H$, $\mathcal{A}_{\text{cma}}$ makes queries to $H \setminus \mathcal{S}'$ and $G_3$ outputs 0 if $\text{FIND} = \perp$. To apply Lemma 2.4, we use the notation of Lemma 2.4. Assume that $Pr[G_2^{\text{cma}} \Rightarrow 1] = Pr[1 \leftarrow \mathcal{A}_{\text{cma}}^{\text{Sign}_{H}(F)}]$. Since $G_3$ differs from $G_2$ in two aspects: the use of $H \setminus \mathcal{S}'$ and the output of 0 when $\text{FIND} = \perp$, $Pr[G_2^{\text{cma}} \Rightarrow 1] = Pr[1 \leftarrow \mathcal{A}_{\text{cma}}^{\text{Sign}_{H}(F)} \wedge \text{FIND} = \perp]$ and $Pr[\text{FIND} = \perp: G_3^{\text{cma}} \Rightarrow b] = Pr[\text{FIND} = \perp: b \leftarrow \mathcal{A}_{\text{cma}}^{\text{Sign}_{H}(F)}]$ hold. Applying Lemma 2.4,

$$|Pr[G_2^{\text{cma}} \Rightarrow 1] - Pr[G_3^{\text{cma}} \Rightarrow 1]| \leq \sqrt{(q_{\text{qro}} + 2)Pr[\text{FIND} = \perp: G_3^{\text{cma}} \Rightarrow b]}.$$

We will show a bound on Eq. (20) after defining $G_4$.

GAME $G_4$ (reprogramming only for successful trials): The signing oracle reprograms $H := H^{(w, m) \rightarrow c_i}$ only for accepting transcripts. It’s important to note that $\mathcal{A}_{\text{cma}}$ makes queries to the punctured oracle $H \setminus \mathcal{S}'$. If $\text{FIND} = \perp$, then $\mathcal{A}_{\text{cma}}$’s queries never contain any $(w, m) \in \mathcal{S}'$, and as a result, $\mathcal{A}_{\text{cma}}$ cannot obtain $H(w, m)$ for $(w, m) \in \mathcal{S}'$. Therefore, if $\text{FIND} = \perp$, $\mathcal{A}_{\text{cma}}$ cannot distinguish whether $H$ is reprogrammed at $(w, m) \in \mathcal{S}'$ in $G_3$ or not in $G_4$. From Lemma 2.3, we have

$$Pr[\text{FIND} = \perp: G_3^{\text{cma}} \Rightarrow b] = Pr[\text{FIND} = \perp: G_4^{\text{cma}} \Rightarrow b].$$

Especially, if $G_3$ or $G_4$ outputs 1, then $\text{FIND}$ must be $\perp$. Therefore, we conclude that $Pr[G_3^{\text{cma}} \Rightarrow 1] = Pr[G_4^{\text{cma}} \Rightarrow 1]$. Also, $Pr[\text{FIND} = \perp: G_3^{\text{cma}} \Rightarrow b] = Pr[\text{FIND} = \perp: G_4^{\text{cma}} \Rightarrow b]$ holds from Eq. (21).
We show a bound on Eq. (20). Let $G_4$ be a modified $G_4$ played by $B_{cma}$. $B_{cma}$ outputs $(w', m')$ and wins the game if $(w', m') \in S'$. Choosing $j \leftarrow [q_{qro} + 1]$, $B_{cma}$ runs $A_{cma}$ playing $G_4$. Just before $A_{cma}$ makes $j$-th query to $H$, $B_{cma}$ measures a query input register of $A_{cma}$ and outputs the measurement outcome as $(w', m')$. The oracles of $G_4'$ reveal no information on $S$ and $S'$. If we assume that $\max_{\hat{w} \in W} Pr[w = \hat{w}: (w, st) \leftarrow P_1(sk)] \leq \epsilon$ holds, then $Pr[G_4'_{B_{cma}} = 1] \leq Pr[w' \in S] \leq (q_{\text{sign}} - q_{\text{sign}})\epsilon$ holds. From Lemma 2.5, we have

$$Pr[FIND = T: G_4^{A_{cma}} = b] \leq 4(q_{qro} + 1)(q_{\text{sign}} - q_{\text{sign}})\epsilon.$$}

Hence, an upper bound on Eq. (20) is $2(q_{qro} + 2)\sqrt{(q_{\text{sign}} - q_{\text{sign}})\epsilon}$.

GAME $G_5$ (Canceling the punctuation on $H$): The challenger no longer punctures $H$, and we remove the unused $S_i$, $S$, and $S'$ from the game. By applying Lemma 2.4, we obtain the same bound as Eq. (20):

$$|Pr[G_5^{A_{cma}} = 1] - Pr[G_5^{A_{cma}} = 1]| \leq 2(q_{qro} + 2)\sqrt{(q_{\text{sign}} - q_{\text{sign}})\epsilon}.$$}

GAME $G_6$ (simulating the signing oracle by $\text{Sim}$): The challenger generates $(w_i, c_i, z_i) \leftarrow \text{Sim}(pk)$ for $i \in [q_{\text{sign}}]$. The $A$-HVZK adversary $D_{zk}$ can simulate $G_5$ and $G_6$. If $D_{zk}$ plays $A$-HVZK$_0$, the procedures of the original and simulated $G_5$ are identical. If $D_{zk}$ plays $A$-HVZK$_1$, he obviously simulates $G_6$. Therefore, we have:

$$|Pr[G_5^{A_{cma}} = 1] - Pr[G_6^{A_{cma}} = 1]| \leq \text{Adv}_{\text{A-HVZK}}^{A-HVZK}(D_{zk}).$$}

Since $G_6$ can be simulated without using $sk$, the EUF-NMA adversary $A_{nma}$ can simulate $G_6$. Summing up, we have Eq. (19) for EUF-NMA $\Rightarrow$ EUF-CMA. ⊓⊔

Notice that Theorem G.1 does not yield a worse bound than [3, Theorem 2], except for a factor of 2 in the last term of Eq. (19).