Revisiting the Security of Fiat-Shamir Signature Schemes under Superposition Attacks

Quan Yuan[1], Chao Sun[2], and Tsuyoshi Takagi[1]

[1] The University of Tokyo, Tokyo, Japan
[2] Southeast University, Nanjing, China

Abstract. The Fiat-Shamir transformation is a widely employed technique in constructing signature schemes, known as Fiat-Shamir signature schemes (FS-SIG), derived from secure identification (ID) schemes. However, the existing security proof only takes into account *classical* signing queries and does not consider *superposition attacks*, where the signing oracle is quantum-accessible to the adversaries. Alagic et al. proposed a security model called *blind unforgeability* (BUF, Eurocrypt'20), regarded as a preferable notion under superposition attacks.

In this paper, we conduct a thorough security analysis of FS-SIGs in the BUF model. First, we propose a special property for ID schemes called quantum special honest-verifier zero-knowledge (qsHVZK), which is stronger than classical HVZK. We prove that qsHVZK is a sufficient property for BUF (with implicit rejection) of the resulting FS-SIG in the quantum random oracle model (QROM). Next, we give an efficient construction of (a weaker variant) of qsHVZK ID scheme based on the quantum hardness of LWE problems.

To avoid enhancing the requirement of HVZK, we then progress to the deterministic FS-SIG (DFS) for more efficient constructions. We show that if the pseudorandom function is quantum-access-secure (QPRF), then we can prove the BUF security of the resulting DFS only with the requirement of the standard (multi-)HVZK in the QROM. A similar result can be extended to the hedged version of FS-SIG.

Keywords: Fiat-Shamir transform, digital signatures, identification schemes, superposition attacks, quantum random oracle

1 Introduction

1.1 Background

The Fiat-Shamir transformation [25] serves as a fundamental tool for converting interactive protocols into their non-interactive ones. Specifically, given a three-round identification scheme (ID scheme), we can apply this transformation to construct a signature scheme known as the Fiat-Shamir signature scheme

(FS-SIG). This transformation incorporates a hash function H, resulting in the scheme denoted as $\mathsf{FS}[\mathsf{ID}, \mathsf{H}]$. More precisely, if the underlying ID scheme is secure and honest-verifier zero-knowledge (HVZK) and if we model H as a quantum random oracle (QRO [9]), then $\mathsf{FS}[\mathsf{ID}, \mathsf{H}]$ is existentially unforgeable under chosen message attacks (EUF-CMA) [22, 30, 36, 37].

Two types of security models are used in the post-quantum security analysis: Q1 and Q2 [34] . In both settings, the adversary can execute (offline) quantum computations. The difference is that in Q1 security, the online communications of the adversary should be classical rather than quantum. Regarding the signature schemes, the adversary can only send *classical* messages to the signing oracle before forging a signature. The EUF-CMA is of this type. The adversary succeeds if it forges a signature for a *fresh* message that has never been queried to the signing oracle. By contrast, in Q2 security, the adversary can send messages in quantum states $\sum_{m,t} \alpha_{m,t} |m, t\rangle$ to the signing oracle and obtain quantum signatures in response $\sum_{m,t} \alpha_{m,t} |m, t \oplus \mathsf{Sig}(sk, m; r)\rangle$. Such an attack, called *superposition attack*, could occur in many scenarios [19]. There is a large amount of research in Q2 models on various cryptographic primitives, such as pseudorandom functions [48], MACs [1], encryption schemes [11, 14] and signature schemes [11, 15].

In the Q2 setting, defining a *fresh* forgery is not as natural as in Q1. We cannot record the list of signing queries. The adversary can, for instance, send a superposition of *all* the messages $m \in \mathcal{M}$ to the signing oracle with a single quantum query. Boneh and Zhandry [11] propose the first notion in the Q2 model for a signature scheme, called EUF-qCMA, where the adversary is required to eventually output $(q + 1)$ forgeries after q signing queries. However, this "plus-one-type" notion is then considered insufficient in practice [1, 28]. For instance, the adversary may send signing queries starting with 0 (in superpositions), and then gain the ability to forge a signature for a message starting with 1. It successfully forged a fresh signature, but unfortunately cannot be ruled out from EUF-qCMA.

We usually care more about the *freshness* than the number of forgeries. Recently, Alagic et al. [1] propose a preferable notion called *blind unforgeability* (BUF). Informally speaking, the signing oracle holds an ϵ-subset of the message space, say the blind region B_ϵ. The signing oracle only signs the messages $m \notin B_\epsilon$ in superposition, and the adversary is eventually required to return a forgery for some $m^* \in B_\epsilon$. It ensures that the forgery is not contained in any signing queries and is thus fresh. In many cases, an automated signing machine is programmed to (or not to) only sign certain types of messages. The BUF security guarantees that any adversary cannot forge a signature for any message that is impossible to be signed by the signing oracle even if it is quantum-accessible.

As one of the most general and practical constructions of signature schemes, FS-SIG requires comprehensive cryptanalysis under various attacks, not limited to CMAs in the Q1 models. As far as we know, there is neither a concrete superposition attack nor security proof for FS-SIG in the Q2 type. It is tempting to ask the following question:

1.2 Our Contributions

As a preparation work, we give fine-grained security notions on BUF, which are natural extension from previous work. Previously, a quantum signing oracle maps $|m,t\rangle$ to $|m,t\oplus \mathsf{Sig}(sk,m;r)\rangle$. In [14], Carstens et al. propose a weaker version called *embedding oracle* for encryption schemes, where the input register only includes the quantum state of plaintexts and the response register is always initialized by the all-zero state. We extend it to the signature scheme. That is, an *embedding* blind signing oracle maps $|m\rangle\,|0\rangle_t$ to $|m,\mathsf{Sig}(sk,m;r)\rangle$ for $m\notin B_\epsilon$ and to $|m,\perp\rangle$ otherwise. We call the new notion under the embedding signing oracle as *weak blind unforgeability* (wBUF). The embedding oracle frequently appears in many quantum cases. For instance, even if the signing machine is open for quantum queries, the initial state for computation may still be prepared by itself and out of the control of adversaries.

In addition, we give a variant of BUF with *implicit rejection* (say $\mathrm{BUF}^{\not\perp}$), which is frequently used in key encapsulations and encryptions. For the message m in the blind region, the blind signing oracle returns a random string $\mathsf{F}(m;r)$ instead of $\perp$. It is equivalent to the original version when the signing oracle is classical, but it is non-trivial for quantum settings.

Next, we try to prove BUF for FS-SIGs. Recall that to prove the EUF-CMA for FS-SIG, the ID scheme is supposed to be post-quantum sound and *honest-verifier zero-knowledge* (HVZK) [30, 36, 37]. However, an HVZK ID scheme is not enough for BUF: it only ensures that a *classical* honest-verifier transcript is zero-knowledge, but a quantum signature may contain a quantum state of exponentially-many transcripts, which may leak information. We later give an example of HVZK ID scheme whose security can be completely broken from quantum transcripts[3].

Thus, we need to enhance the requirement of HVZK. To fill the gap, we propose stronger variants of HVZK, called *(weak) quantum special honest-verifier zero-knowledge* (wqsHVZK/qsHVZK), which remains zero-knowledge given *quantum* transcripts of the ID scheme. We show that they are sufficient for proving (weak) BUF with implicit rejection of FS-SIG in the QROM.

Result 1 *(Informal.) If an identification scheme ID is post-quantum secure and (weak) qsHVZK, then the resulting Fiat-Shamir signature $\mathsf{FS}[\mathsf{ID},\mathsf{H}]$ is (weak) BUF in the QROM.*

Next, a natural question is how to construct an ID scheme with stronger properties. We construct a weak qsHVZK ID scheme based on *noisy trapdoor claw-free function families* (NTCFs), which can be based on the quantum hardness of learning with errors (LWE) problem. Interestingly, NTCFs are mainly used in constructing protocols proving quantum computing capabilities (say,

[3] But it is an open question whether it implies an attack on the resulting FS-SIG.

proof of quantumness) in previous work. To the best of our knowledge, it is the first application related to identification and zero-knowledge.

Result 2 *(Informal.) If LWE problem is hard in the post-quantum settings, then there exists a post-quantum secure and* $\mathsf{wqsHVZK}$ *identification scheme.*

Unfortunately, the construction is less efficient and we do not know how to construct a (strong) qsHVZK ID scheme. Thus, we try to seek another solution to achieve (strong) BUF. Note that if the signature algorithm is deterministic, then BUF and wBUF are equivalent. Inspired by this, we then turn to *deterministic Fiat-Shamir signature scheme* (DFS).

Similar to the original one, it is also necessary to enhance the requirements. The difference is, we now only need to enhance the property of the pseudorandom function (PRF) instead of the ID scheme, which is much easier to implement.

Result 3 *(Informal.) If an identification scheme* ID *is post-quantum secure and* HVZK*,* H *is a random oracle, and* PRF *is a quantum-access pseudorandom function, then* $\mathsf{DFS}[\mathsf{ID}, \mathsf{H}, \mathsf{PRF}]$ *is (weak)* $BUF/BUF^{\not\perp}$ *in the QROM.*

Finally, we move to another variant called *hedged* Fiat-Shamir signature scheme (HFS [4]), where the randomness is computed with an additional nonce. Similarly, we prove the BUF security of HFS with standard HVZK. Furthermore, we extend the security model to the case where the adversary can control both the message and the nonce as in [4] but under superposition attacks, and also give the security proof.

Result 4 *(Informal.) If an identification scheme* ID *is post-quantum secure and* HVZK*, and* H *and* G *are secure hash functions, then* $\mathsf{HFS}[\mathsf{ID}, \mathsf{H}, \mathsf{G}]$ *is (weak)* $BUF/BUF^{\not\perp}$ *in the QROM, even in the case that the nonce is also under control in the quantum signing queries.*

Our contributions are concluded in Figure 1.

1.3 Technical Overview

How to prove the security for FS-SIG? Let us first review how to prove EUF-CMA of FS-SIG from HVZK. First, it reduces the EUF-NMA (no message attacks) from the soundness of the underlying ID scheme [22,37]. Next, it reduces EUF-CMA to the EUF-NMA by simulating the signing oracle with the simulator Sim of HVZK. Roughly, to answer a query m, the reduction generates a simulated transcript $(\tilde{a}, \tilde{c}, \tilde{z})$ and reprograms $\mathsf{H}(pk, \tilde{a}, m) := \tilde{c}$. Due to the high entropy of $\tilde{a}$, it is infeasible for a quantum polynomial-time (QPT) adversary to detect the reprogramming [30].

Then, it is not hard to see that the second step does not work when the signing oracle is quantum-accessible: the reduction now needs to generate a superposition of transcripts $(\tilde{a}, \tilde{c}_m, \tilde{z}_m)$ with a common $\tilde{a}$. Here are the problems. First, the reduction *cannot* simulate transcripts with a common $\tilde{a}$ and distinct c_m's due

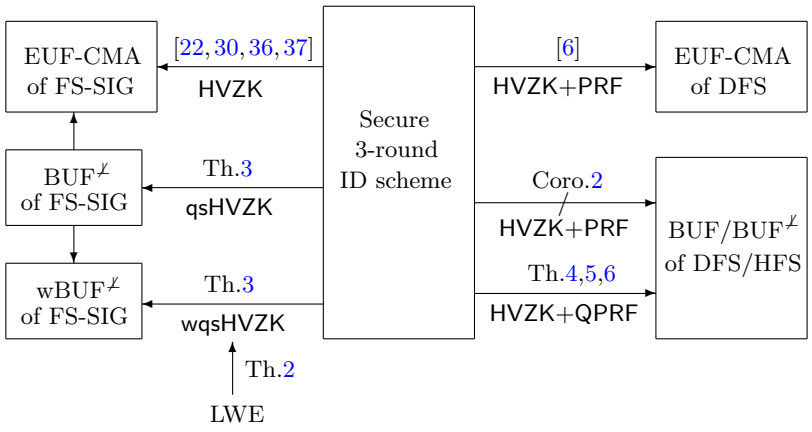

Fig. 1. Sufficient properties for provable security of (variants of) FS-SIG.

to the special soundness. Second, the reduction cannot reprogram $\mathsf{H}(pk, \tilde{a}, m)$ as before, since the reduction cannot learn m: a measurement will cause collapse on the quantum query, and the adversary can immediately detect it with high probability.

To fill the gaps, we define a new and stronger variant of HVZK, called *quantum special honest-verifier zero-knowledge* (qsHVZK), which is essentially a quantum version of multi-special-HVZK [30] defined in a game-based manner described as follows: Let $\mathsf{Trans}(sk, \cdot)$ be an oracle that takes as input c and returns an honest transcript (a, c, z) conditioned on challenge c. There exists an efficient simulator $\mathsf{Sim}(pk, \cdot)$ that also takes as input c and returns a transcript $(\tilde{a}, c, \tilde{z})$. The adversary has the negligible advantage of distinguishing oracle $\mathsf{Sim}(sk, \cdot)$ from $\mathsf{Trans}(pk, \cdot)$ after sending multiple (but polynomially-many) queries.

Then, we extend the above definition to the quantum-accessible settings. We show a direct (and weak) version at first. Given a quantum challenge $|\phi\rangle = \sum_c \alpha_c |c\rangle$, the honest oracle Trans returns $|\phi'\rangle = \sum_c \alpha_c |a, c, z_{a,c}\rangle$, where $(a, St) \leftarrow \mathsf{Com}(sk)$ and $z_{a,c} = \mathsf{Resp}(sk, c, St; r)$ for random r. On the other hand, the simulator Sim must be a quantum algorithm, returning a simulated state $\left|\widetilde{\phi'}\right\rangle$. We require that oracles Trans and Sim cannot be distinguished with polynomially-many quantum queries. Without loss of generality, we always assume that Sim measures a-register at the end.

Next, we can simulate the *embedding* signing oracle of $\mathsf{FS}[\mathsf{ID}, \mathsf{H}]$ in the QROM equipped with Sim. Informally, given a query $\sum_m \alpha_m |m\rangle$, pick a random oracle U mapping the message to the challenge space ChSet. (Note that a new U is picked in each signing query.) Then, perform U on m and get $\sum_m \alpha_m |c_m, m\rangle$, where $c_m = \mathsf{U}(m)$. Then, run $\mathsf{Sim}(pk, \cdot)$ on the c-register, we get a quantum state indistinguishable with $\sum_m \alpha_m |a, c_m, z_{a,c_m}, m\rangle$. Next, uncompute c_m with another query to U and discard c-register, we have $\sum_m \alpha_m |a, z_{a,c_m}, m\rangle$, which is quite close to a quantum state of signatures, and a-register is a pure state and can be measured as $\tilde{a}$.

To make the simulated signatures valid, we reprogram $\mathsf{H}(pk, \tilde{a}, m) = c_m := \mathsf{U}(m)$ for *all* $m \in \mathcal{M}$. In other words, $\mathsf{H}(a, m)$ is syntactically reprogrammed by $\mathsf{U}(m)$ after checking whether $a = \tilde{a}$ holds. Then, we use a generalized version of reprogramming lemma [30] to show that the reprogramming operation cannot be detected even if an exponential number of records are reprogrammed.

However, we only simulated the embedding oracle. For a general one, we need to map $|m, t_1, t_2\rangle$ to $|m, t_1 \oplus a, t_2 \oplus z_{a,c_m}\rangle$. If we simply perform an xor operation to the response state, we then have $\sum_{m,t_1,t_2} \alpha_m |m, t_1 \oplus a, t_2 \oplus z_{a,c_m}, z_{a,c_m}\rangle$. Here is the problem: since the third and fourth register are entangled, we cannot discard the fourth register as "the garbage". We cannot uncompute it either: Sim is obviously a probabilistic algorithm and we cannot compute z_{a,c_m} twice with the same a.

Thus, we turn back to the definition of new (and stronger) HVZK. Now, we redefine Trans as follows: Given $|\phi\rangle = \sum_{c,z} \alpha_{c,z} |c, z\rangle$, it returns $|\phi'\rangle = \sum_{c,z} \alpha_{c,z} |a, c, z \oplus z_{a,c}\rangle$. Denote the previous version by $\mathsf{emTrans}$ instead. It is a natural extension to the non-embedding one. If it still can be simulated by Sim, we can use the above approach to simulate the non-embedding oracle without additional xor operations.

Finally, the adversary should return a forgery $(m^*, (a^*, z^*))$ after the queries. We desire that $\mathsf{H}(pk, a^*, m^*)$ has not been reprogrammed above. (Otherwise, it is not a valid forgery for the original $\mathsf{FS}[\mathsf{ID}, \mathsf{H}]$.) Thus, we carefully reprogram $\mathsf{H}(pk, \tilde{a}, m)$ only for $m \notin B_\epsilon$ and finish the reduction from BUF to EUF-NMA. Then, since EUF-NMA can be reduced to the security of the underlying ID scheme in previous work, we complete the proof.

How to construct a wqsHVZK ID scheme? We then try to construct a $\mathsf{wqsHVZK}$ ID scheme from known primitives. We introduce the trapdoor claw-free function family (TCF) as a building block. Roughly, a (non-noisy) trapdoor claw-free function implies $f_b : \{0,1\}^\lambda \mapsto \{0,1\}^\lambda$ for $b \in \{0,1\}$ and a trapdoor function f_b^{-1} such that: (1) $f_0(\cdot)$ and $f_1(\cdot)$ are bijective; (2) it is hard to find a claw (x_0, x_1) such that $f_0(x_0) = f_1(x_1)$, and (3) one can inverse $f_0(\cdot)$ and $f_1(\cdot)$ using the trapdoor f_b^{-1}.

Then, a TCF implies a $\mathsf{wqsHVZK}$ ID scheme. We give a simple example with 1-bit challenge (and thus 1-bit soundness) and it can be simply extended to a full version by picking multiple commitments. The public key and the secret key are f and f^{-1}, respectively. The commitment contains a random $y \xleftarrow{\$} \{0,1\}^\lambda$. Given the challenge c, the response is $x = f_c^{-1}(y)$. The verification algorithm returns 1 iff $f_c(x) = y$. Previous work [37] shows that the soundness of an ID scheme can be proven from two properties: 2-soundness and strict soundness [45]. The 2-soundness can be reduced to the claw-free property: two responses for a same y and different c immediately implies a claw. The strict soundness is implied from the fact that $f_b(\cdot)$ is injective.

We next prove the (perfect) $\mathsf{wqsHVZK}$ property. Given a quantum challenge $|\phi\rangle = \alpha |0\rangle + \beta |1\rangle$, we are supposed to output a uniformly random y and $|\phi'\rangle = \alpha |0, x_0\rangle + \beta |1, x_1\rangle$ such that $f_0(x_0) = f_1(x_1) = y$. Let λ be the length of x.

We can make it by generating a uniform state of $|x\rangle$, say $|\phi_x\rangle = \sum_x 2^{-\lambda/2}|x\rangle$, computing f on $|\phi\rangle \otimes |\phi_x\rangle$, and finally measuring the value. The state before measurement can be written as

$$\begin{aligned}&\sum_x \frac{\alpha}{2^{\lambda/2}}|0, x, f_0(x)\rangle + \frac{\beta}{2^{\lambda/2}}|1, x, f_1(x)\rangle \\ =&\sum_y \frac{\alpha}{2^{\lambda/2}}\left|0, f_0^{-1}(y), y\right\rangle + \frac{\beta}{2^{\lambda/2}}\left|1, f_1^{-1}(y), y\right\rangle.\end{aligned}$$

After the measurement on y-register, the result is $y^* \in \{0,1\}^\lambda$ with probability $2^{-\lambda}(\alpha^2+\beta^2) = 2^{-\lambda}$ and the final state is thus $\alpha\left|0, f_0^{-1}(y^*), y^*\right\rangle + \beta\left|1, f_1^{-1}(y^*), y^*\right\rangle$, which are the same as the honest response.

As far as we know, only a relaxation of TCF, say *noisy* TCF [12,13], can be constructed based on post-quantum assumptions, such as the quantum hardness of learning with error (LWE) problem [41]. In the formal version, we replace the TCF with a noisy TCF, and the above properties still hold.

How to prove BUF for the deterministic FS-SIG? We then turn to the deterministic FS-SIG, where the randomness is replaced by $\mathsf{PRF}(k, m)$ with a pseudorandom function PRF. In the sense of EUF-CMA, the security of $\mathsf{FS}[\mathsf{ID}, \mathsf{H}]$ immediately implies that of the deterministic one ($\mathsf{DFS}[\mathsf{ID}, \mathsf{H}, \mathsf{PRF}]$, or simply DFS) assuming that PRF is post-quantum secure [8]. However, the cases are different in the sense of BUF. A quantum signature of DFS includes a *mixed* state of the commitment a, while that of FS-SIG includes a *pure* commitment. It is, interestingly, simpler to simulate the signing oracle in a reduction.

Again, we need to enhance the requirement for proving BUF compared to EUF-CMA: a post-quantum secure PRF is not enough, since PRF runs with quantum states in signing queries but post-quantum security only ensure the indistinguishability with *classical* queries. A superposition attack on PRF may immediately breaks the resulting DFS (see Proposition 2). A natural solution is to instead use a quantum-access-secure one, say QPRF [48].

Then, the resulting $\mathsf{DFS}[\mathsf{ID}, \mathsf{H}, \mathsf{PRF}]$ can be proven BUF, where ID is only required to be standard multi-HVZK. The proof sketch is *history-free* following the ideas of [11,36]. Let U' be a random oracle. To simulate the (non-embedding) signing oracle, the reduction computes $(a_m, c_m, z_m) = \mathsf{Sim}(pk; \mathsf{U}'(m))$ on m-register and XORs (a_m, c_m) to the response register. Then, reprogram $\mathsf{H}(pk, a, m)$ as follows: compute $(a_m, c_m, z_m) = \mathsf{Sim}(pk; \mathsf{U}'(m))$ and return c_m if $a = a_m$.

There is still a problem. Multi-HVZK only guarantees the indistinguishability when *polynomial* number of transcripts are given, while a superposition of $(a_m, c_m, z_m) = \mathsf{Sim}(pk; \mathsf{U}'(m))$ may contain an *exponential* number of them. To solve this, we use the small-range distribution lemma [48] and replace U' with a random oracle mapping to a polynomial-size space, and the adversary cannot tell the different. Finally, if we only reprogram H condition that $m \notin B_\epsilon$, a forgery from $\mathcal{A}$ then implies a forgery of $\mathsf{FS}[\mathsf{ID}, \mathsf{H}]$.

Extension to hedged Fiat-Shamir signatures. The hedged Fiat-Shamir signature (HFS, [4]) is a variant of DFS. The randomness of the signing algorithm is replaced with $\mathsf{G}(sk, m, n)$, where G is modeled as a QRO, sk is the secret key and n is a nonce. If $\mathsf{FS}[\mathsf{ID}, \mathsf{H}]$ is EUF-CMA, then the hedged version $\mathsf{HFS}[\mathsf{ID}, \mathsf{H}, \mathsf{G}]$ is secure even if the nonce n is also controlled by the adversary [4, 30].

Thus, two security models should be considered for HFS: the adversary can send quantum message queries or message-and-nonce queries. Note that the previous approaches in CMA model [4, 30] cannot be directly extended to our case: they need to check whether a message-nonce pair is queried twice, which is trivial in the quantum-access setting. We again use the history-free approach to fill the gap. As a price, the security bound in the second model is looser than the first one.

1.4 Related Work

Fiat-Shamir Signature schemes. The security of Fiat-Shamir signatures can be proven in two steps. First, EUF-NMA can be reduced to the special soundness in the ROM [7] by the forking lemma [40]. Next, EUF-CMA can be reduced to EUF-NMA when the underlying ID scheme is HVZK. The first step fails in the quantum setting due to the hardness of quantum rewinding [3]. A series of work is done to analyze the security of Fiat-Shamir transformation [21–23, 30, 36, 37] in the QROM.

Superposition Attacks. Superposition attacks are first considered for pseudorandom functions [18, 48], and then extended to MACs [1, 10, 28, 31, 44], block ciphers [27], one-way functions [32], public-key encryption schemes [11, 17] and signatures [1, 11, 16]. As for signature schemes, Lamport's scheme [1], Winternitz scheme [39] and GPV signatures based on the QSIS assumption [16] are proven secure in the BUF model. Lamport's scheme, Merkle's scheme, deterministic GPV [11] and variant of SPHINCS+ [47] are proven secure in the EUF model.

Very recently, Xagawa [46] proves the security of DFS under superposition attacks in concurrent work with a similar approach. His proof focuses on memory-tight reductions, and thus requires the ID scheme to be lossy and statistical HVZK, while our proof only requires computational multi-HVZK.

De-randomized and Hedged Signatures. De-randomization of a signature scheme can avoid the risk of randomness failures [6, 8], but arise the vulnerability under fault attacks. A hedged construction is general to avoid such attacks. The security notion of the hedged Fiat-Shamir signatures is formally defined in [4] in ROM, and extended to QROM in [30].

2 Security Notions under Superposition Attacks

Blind Unforgeability [1] is a preferable security notion for signature schemes under superposition attacks [16, 39]. Let $\epsilon_\lambda \in (0, 1)$. Define a probabilistic algorithm

$\mathsf{Blind}(\mathcal{M}_\lambda, \epsilon_\lambda)$ that outputs a subset of $\mathcal{M}_\lambda$, say B_ϵ, such that each $m \in \mathcal{M}_\lambda$ is placed in B_ϵ independently with probability ϵ_λ. Then, define the quantum-accessible *blind signing oracle* as follows. Let $\mathcal{R}_\lambda$ be the randomness space of SigO. In each query, it randomly picks $r \leftarrow \mathcal{R}_\lambda$ [4], and maps

$$\mathsf{BSigO} : |m, t\rangle \mapsto |m, t \oplus B_\epsilon\mathsf{Sig}(sk, m; r)\rangle ,$$

where

$$B_\epsilon\mathsf{Sig}(sk, m; r) := \begin{cases} \bot & \text{if } m \in B_\epsilon \\ \mathsf{Sig}(sk, m; r) & \text{if } m \notin B_\epsilon \end{cases}.$$

Additionally, we define an embedding version called $\mathsf{emBSigO}$ that maps

$$\mathsf{emBSigO} : |m\rangle |0\rangle_t \to |m, B_\epsilon\mathsf{Sig}(sk, m; r)\rangle .$$

Then, we define BUF with implicit rejection. Here, the signing oracle (privately) picks a random oracle F mapping to the signature space and lets

$$B_\epsilon\mathsf{Sig}^{\not\perp}(sk, m; r) := \begin{cases} \mathsf{F}(m, r) & \text{if } m \in B_\epsilon \\ \mathsf{Sig}(sk, m; r) & \text{if } m \notin B_\epsilon \end{cases}.$$

$\mathsf{BSigO}^{\not\perp}$ and $\mathsf{emBSigO}^{\not\perp}$ are similarly defined by replacing $B_\epsilon\mathsf{Sig}$ with $B_\epsilon\mathsf{Sig}^{\not\perp}$.

Definition 1. *Let $\Gamma = (\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$ be a signature scheme and $\epsilon_\lambda > 0$. Let $* \in \{\mathsf{EUF\text{-}NMA}, \mathsf{EUF\text{-}CMA}, \epsilon_\lambda\text{-}\mathsf{BUF}\}$. For an adversary $\mathcal{A}$, let $Adv^*_\Gamma(\lambda, \mathcal{A}) := \Pr[\mathsf{Exp}^*_\Gamma(\lambda, \mathcal{A})]$, defined in Figure 2. We say Γ is $*$ if for any QPT adversary $\mathcal{A}$, there exists a negligible function negl such that $Adv^*_\Gamma(\lambda, \mathcal{A}) \leq \mathsf{negl}(\lambda)$.*

In particular, if for any QPT adversary $\mathcal{A}$, there exists a negligible function negl such that $Adv^{\epsilon_\lambda\text{-}\mathsf{BUF}}_\Gamma(\lambda, \mathcal{A}) \leq \mathsf{negl}(\lambda)$ holds for any ϵ_λ, we omit ϵ_λ and simply say that Γ is BUF[5]*.*

Additionally, we say it is weak BUF (wBUF)/BUF$^{\not\perp}$/wBUF$^{\not\perp}$ on the same condition except that BSigO is replaced with $\mathsf{emBSigO}$/$\mathsf{BSigO}^{\not\perp}$/$\mathsf{emBSigO}^{\not\perp}$.

Remark 1. When $\mathcal{M}_\lambda$ is exponentially large, it is inefficient to pick B_ϵ from $\mathcal{M}_\lambda$ and store it. To solve this, we can simulate this step by using a random function $\mathsf{F}' : \mathcal{M}_\lambda \mapsto [2^\lambda]$ and define $m \in B_\epsilon \Leftrightarrow \mathsf{F}'(m)/2^\lambda \leq \epsilon_\lambda$. F' can be instantiated by a pseudorandom function or a random oracle.

[4] The reason why the randomness is chosen globally for all messages in superposition in a quantum signing oracle has been discussed in [11], Section 3.

[5] If $\epsilon_\lambda \geq 1$ or negligibly close to 0 or 1, then all QPT adversary can only succeed in ϵ_λ-BUF experiment with negligible probability regardless of whether the scheme is secure. Even so, we do not place such restrictions on ϵ_λ, as such "trivial experiments" does not contradict our security notion.

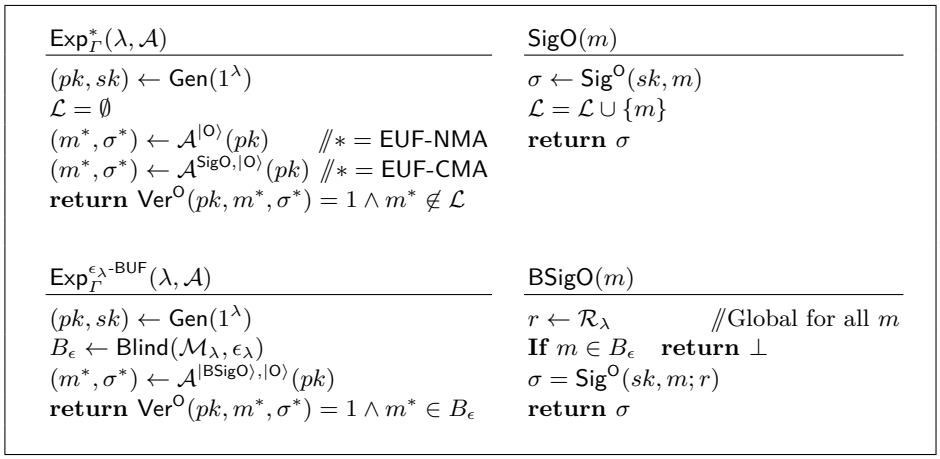

Fig. 2. Security experiment of a signature scheme $\Gamma = (\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$.

In the following, we omit the security parameter λ if it is clearly known.

With a *deterministic* signing algorithm, BUF and wBUF are equivalent since BSigO can be simulated by a query to emBigO, an xor operation, and another query to emBigO for uncomputation.

Corollary 1. *A deterministic signature scheme is ϵ-BUF if and only if it is ϵ-wBUF.*

3 Blind Unforgeability of Fiat-Shamir Signature Schemes

In this section, we analyze the sufficient properties for proving the blind unforgeability of Fiat-Shamir signature schemes.

3.1 Quantum Special Honest-Verifier Zero Knowledge

As a preparation work, we propose a stronger variant of HVZK for identification (ID) schemes. (See details in Appendix A.3 about the definitions and standard properties of ID schemes.)

Let $\mathsf{ID} = (\mathsf{IGen}, \mathsf{Com}, \mathsf{Resp}, \mathsf{IVer})$ be an ID scheme. We define the quantum-accessible transcript oracle $\mathsf{Trans}(sk, \cdot)$ as follows: Take as input a quantum state of challenge and response $\sum_{c,z} \alpha_{c,z} |c, z\rangle$. It runs $(a, St) \leftarrow \mathsf{Com}(sk)$ and returns $|a\rangle \otimes \sum_{c,z} \alpha_{c,z} |c, z \oplus \mathsf{Resp}(sk, c, St; r)\rangle$ [6], which can be instantiated by a quantum circuit running ID. We say ID is *quantum* special honest-verifier zero-knowledge if there exists a quantum simulator $\mathsf{Sim}(pk, \cdot)$, whose behavior is indistinguishable with $\mathsf{Trans}(sk)$.

[6] The query state may be entangled with some local states from the sender. In this case, we assume that the local states are also sent to the oracle and returned unchanged, and omit the local states for simplicity.

Remark 2. Here, the input state does not explicitly include a-register. It is natural to consider a more general version, say Trans', that maps $\sum_{a,c,z} \alpha_{a,c,z} |a,c,z\rangle$ to $\sum_{a,c,z} \alpha_{a,c,z} |a \oplus a', c, z \oplus z'_c\rangle$, where (a', c, z'_c) are transcripts in superposition. Indeed, Trans immediately implies Trans': Treat a-register as a part of the local state and send $\sum_{a,c,z} \alpha_{a,c,z} |a,c,z\rangle$ to Trans. Obtain $|a'\rangle \otimes \sum_{a,c,z} \alpha_{a,c,z} |a,c,z \oplus z'_c\rangle$ with unchanged a-register. Then, xor a'-register to a-register and measure and discard a'-register. Also, Trans' implies Trans by adding $|0\rangle_a$ to the input.

In addition, we define embedding transcript oracle, say $\mathsf{emTrans}$, which is the same as Trans except that the z-register of the input is always all-zero state. In other words, it maps $\sum_c \alpha_c |c\rangle |0\rangle_z$ to $|a\rangle \otimes \sum_c \alpha_c |c, \mathsf{Resp}(sk, c, St; r)\rangle$.

Definition 2. *(Computationally/Statistically Quantum Special Honest Verifier Zero-Knowledge (qsHVZK)). We say that ID is q-time computationally/statistically-qsHVZK if there exists a QPT algorithm Sim such that for $(pk, sk) \leftarrow \mathsf{IGen}(1^\lambda)$ and all QPT/unbounded adversary $\mathcal{A}$, there exists a negligible function ε such that*

$$Adv^{q\text{-}\mathsf{qsHVZK}}_{\mathsf{ID},\mathsf{Sim}}(\mathcal{A}) := \left|\Pr[\mathcal{A}^{\mathsf{Trans}(sk,\cdot)}(pk)] - \Pr[\mathcal{A}^{\mathsf{Sim}(pk,\cdot)}(pk)]\right| \leq \varepsilon(\lambda),$$

where q denotes the maximum number of quantum queries from $\mathcal{A}$. [7] *In addition, we say it is q-time computationally/statistically weak qsHVZK on the same condition except that Trans is replaced with emTrans.*

Next, we show that qsHVZK is strictly stronger than the classical HVZK by constructing a counterexample as follows.

Construction 1 *Let $\mathsf{ID} = (\mathsf{IGen}, \mathsf{Com}, \mathsf{Resp}, \mathsf{IVer})$ be a secure identification scheme with challenge space ChSet of size $N = 2^l$ for some integer l. Let G be a quantum random oracle mapping to the randomness of IGen and $\mathsf{GenPrime}(n)$ be the algorithm that randomly picks a prime in $[n/2, n)$. Let PRF be a pseudorandom function mapping ChSet to $\{0,1\}^\lambda$. Construct ID' as follows:*

- *$\mathsf{IGen}(1^\lambda)$: $p \leftarrow \mathsf{GenPrime}(\sqrt{N})$, $s = \mathsf{G}(p)$, $k \xleftarrow{\$} \{0,1\}^\kappa$, $(pk, sk) \leftarrow \mathsf{IGen}(1^\lambda; s)$. Let $sk' = (sk, k, p)$. Return (pk, sk').*
- *$\mathsf{Com}'(sk')$: Parse $sk' = (sk, k, p)$. Return $\mathsf{Com}(sk)$.*
- *$\mathsf{Resp}'(sk', c, St)$: Parse $sk' = (sk, k, p)$. $d = \mathsf{PRF}(k, c \bmod p)$. $z \leftarrow \mathsf{Resp}(sk, c, St)$. Return $z' := (z, d)$.*
- *$\mathsf{IVer}'(pk, a, c, z')$: Parse $z' = (z, d)$. Return $\mathsf{IVer}(pk, a, c, z)$.*

Theorem 1. *If ID is computationally multi-HVZK, then ID' is secure and computationally multi-HVZK, but not qsHVZK.*

The proof sketch is similar to the counterexample in [11]. We only show the sketch here and delay the formal proof in Appendix C.1. Compared with

[7] Note that the challenge may contain some $c \notin \mathsf{ChSet}$, since $|\mathsf{ChSet}|$ may not be a power of 2 in some cases.

ID, the transcripts of ID' additionally include a pseudorandom value d with a secret period p, the trapdoor of the keys. Suppose G is a *classical* random oracle, and L_G is the list of queries from the adversary. We consider the following two cases: (1) If $p \notin L_G$, then $(pk, sk) \leftarrow \mathsf{IGen}(1^\lambda; \mathsf{G}(p))$ is perfectly indistinguishable with $(pk, sk) \leftarrow \mathsf{IGen}(1^\lambda)$. A simulator can generate simulated transcripts as before with an additional d. (2) If $p \in L_G$, the simulation will be problematic. However, it happens with negligible probability, since the only information about p in the adversary's view (before sending p to G) is that p is the secret period of the pseudorandom function, and only polynomially-many input-output pairs of the function are given from the transcripts. Assuming PRF is perfect, then p is information-theoretically hidden and thus infeasible to be included in L_G. By Lemma 5, the proof can be extended to a quantum random oracle G.

On the other hand, if Trans is quantum-accessible, we can then construct an oracle that only computes $d(c) := \mathsf{PRF}(k, c \mod p)$ in a quantum manner. By period-finding algorithm, we can retrieve p and then the secret key. Thus, Trans is never zero-knowledge and cannot be simulated due to the soundness.

3.2 A secure wqsHVZK identification scheme from noisy trapdoor claw-free function families

In this section, we show an example of a wqsHVZK identification scheme (with overwhelming completeness) assuming the existence of noisy trapdoor claw-free function families (NTCFs, see Appendix A.5), which can be implied from the quantum hardness of (Ring-)LWE [12, 13].

Construction 2 *Let $\mathcal{F}$ be a NTCF. $ID = (IGen, Com, Resp, IVer)$ is constructed as follows:*

- $IGen(1^\lambda)$*:* $(k, t_k) \leftarrow FuncGen(1^\lambda)$*.* $pk := k$*.* $sk := t_k$*. Return* (pk, sk)*.*
- $Com(sk)$*: For* $i \in [\lambda]$*,* $x_i^{(0)} \xleftarrow{\$} \mathcal{X}$*. Pick* $y_i \leftarrow f_{k,0}(x_i^{(0)})$ *using* sk*. Return* $((y_1, ..., y_\lambda), (y_1, ..., y_\lambda))$*.*
- $Resp(sk, c, St)$*: Parse* $c = (c_1, ..., c_\lambda) \in \{0,1\}^\lambda$ *and* $St = (y_1, ..., y_\lambda)$*. For* $i \in [\lambda]$*,* $x_i = Inv(sk, c_i, y_i)$*. Return* $x = (x_1, ..., x_\lambda)$*.*
- $IVer(pk, a, c, z)$*: Parse* $a = (y_1, ..., y_\lambda)$*,* $c = (c_1, ..., c_\lambda)$ *and* $z = (x_1, ..., x_\lambda)$*. Return* 1 *iff* $Chk(k, c_i, x_i, y_i) = 1$ *for each* $i \in [\lambda]$*.*

Theorem 2. *ID in Construction 2 has overwhelming completeness, post-quantum soundness and statistical weak qsHVZK.*

We delay the proof in Appendix C.2.

3.3 Fiat-Shamir Signature Schemes

Construction 3 *Let $ID = (IGen, Com, Resp, IVer)$ be an identification scheme and H be a hash function mapping to $ChSet$, the challenge space of ID. The Fiat-Shamir signature $FS[ID, H]$ is constructed as follows.*

– $\mathsf{FS.Gen}(1^\lambda) : (pk, sk) \leftarrow \mathsf{IGen}(1^\lambda)$. $sk' := (pk, sk)$. *Return* (pk, sk').
– $\mathsf{FS.Sig}(sk', m)$: *Parse* $sk' = (pk, sk)$. $(a, St) \leftarrow \mathsf{Com}(sk)$. $c := \mathsf{H}(pk, a, m)$. $z \leftarrow \mathsf{Resp}(sk, c, St)$. *Return* (a, z).
– $\mathsf{FS.Ver}(pk, m, (a, z))$. *Return* $\mathsf{IVer}(pk, a, \mathsf{H}(pk, a, m), z)$.

If ID has perfect/overwhelming completeness, then the resulting $\mathsf{FS}[\mathsf{ID}, \mathsf{H}]$ is perfect/overwhelming correct. Then, the following lemmas imply that post-quantum security and HVZK of an identification scheme are sufficient for proving the EUF-CMA security of the resulting Fiat-Shamir signature schemes.

Lemma 1. *[22,37] If ID is post-quantum sound and H is modeled as a quantum random oracle, then $\mathsf{FS}[\mathsf{ID}, \mathsf{H}]$ is EUF-NMA.*

Next, we show that (weak) qsHVZK is sufficient for proving the (weak) $\mathrm{BUF}^{\not\perp}$ of FS-SIG. Since EUF-NMA security of FS-SIG has been proven in Lemma 1. The remaining work is reducing $\mathrm{BUF}^{\not\perp}$ to EUF-NMA with qsHVZK.

Theorem 3. *If ID is post-quantum sound, computationally qsHVZK, and has γ-bit min-entropy, and H is modeled as a quantum random oracle, then $\mathsf{FS}[\mathsf{ID}, \mathsf{H}]$ is BUF with q_s signing queries. Formally, let $\epsilon \in (0, 1)$. Assume there exists a quantum algorithm $\mathcal{A}$ that breaks ϵ-BUF security of $\mathsf{FS}[\mathsf{ID}, \mathsf{H}]$ with q_s quantum signing queries and q_h quantum hash queries. Then, there exists (1) a quantum adversary $\mathcal{B}$ breaking EUF-NMA of $\mathsf{FS}[\mathsf{ID}, \mathsf{H}]$ with q_h queries to H, $(q_s + 2q_h)$ queries to its own quantum random oracle, and (2) a quantum adversary $\mathcal{C}$ breaking q_s-qsHVZK with regard to the qsHVZK-simulator Sim such that*

$$Adv^{\epsilon\text{-}\mathsf{BUF}^{\not\perp}}_{\mathsf{FS}[\mathsf{ID},\mathsf{H}]}(\mathcal{A}) \leq Adv^{\mathsf{EUF\text{-}NMA}}_{\mathsf{FS}[\mathsf{ID},\mathsf{H}]}(\mathcal{B}) + Adv^{q_s\text{-}\mathsf{qsHVZK}}_{\mathsf{ID},\mathsf{Sim}}(\mathcal{C}) + q_s^2 \cdot 2^{-\gamma+1} + \frac{3}{2} q_s \sqrt{q_h 2^{-\gamma}},$$

where $Time(\mathcal{B}) \approx Time(\mathcal{A}) + \Theta(q_s)$ and $Time(\mathcal{C}) \approx Time(\mathcal{A})$.

In addition, the above statement also holds if $\mathrm{BUF}^{\not\perp}$ and qsHVZK are replaced with $\mathrm{wBUF}^{\not\perp}$ and wqsHVZK, respectively.

We delay the proof in Appendix C.3.

4 Blind Unforgeability of Deterministic Fiat-Shamir Signature Schemes

In this section, we analyze the BUF security of the deterministic Fiat-Shamir signature schemes. Here, we only focus on BUF instead of wBUF/$\mathrm{BUF}^{\not\perp}$/$\mathrm{wBUF}^{\not\perp}$, since the proof can be simply extended to other versions.

4.1 Deterministic Fiat-Shamir Signatures

Construction 4 *Let ID be an identification scheme and PRF be a pseudorandom function mapping to the randomness space of ID with key space $\{0, 1\}^\kappa$. The deterministic Fiat-Shamir signature scheme $\mathsf{DFS}[\mathsf{ID}, \mathsf{H}, \mathsf{PRF}]$ is constructed as follows:*

– $\mathsf{DFS.Gen}(1^\lambda)$: $k \xleftarrow{\$} \{0,1\}^\kappa$. $(pk, sk) \leftarrow \mathsf{IGen}(1^\lambda)$. $sk' := (pk, sk, k)$. *Return* (pk, sk').
– $\mathsf{DFS.Sig}(sk', m)$: *Parse* $sk' = (pk, sk, k)$. $(a, St) := \mathsf{Com}(sk; \mathsf{PRF}(k, 0||m))$. $c := \mathsf{H}(pk, a, m)$. $z := \mathsf{Resp}(sk, c, St; \mathsf{PRF}(k, 1||m))$. *Return* (a, z)
– $\mathsf{DFS.Ver}(pk, m, (a, z))$. *Return* $\mathsf{IVer}(pk, a, \mathsf{H}(pk, a, m), z)$.

Lemma 2. *([6]) If* $\mathsf{FS}[\mathsf{ID}, \mathsf{H}]$ *is EUF-CMA and* PRF *is a pseudorandom function, then* $\mathsf{DFS}[\mathsf{ID}, \mathsf{H}, \mathsf{PRF}]$ *is also EUF-CMA.*

We give a separating example of DFS showing that the requirements for EUF-CMA is not sufficient for BUF. Here, the PRF is classical-query-secure but not QPRF. The resulting DFS is immediately EUF-CMA from Lemma 2, but not BUF.

Corollary 2. *Assume pseudorandom functions exist. Then, there exists a pseudorandom function* PRF' *such that for any* k*-special-sound* ID*,* $\mathsf{DFS}[\mathsf{ID}, \mathsf{H}, \mathsf{PRF}']$ *is not BUF in the QROM.*

Proof. The proof is similar to Theorem 1, so we only show the sketch. We first consider the signing oracle without a blind region. Let PRF be a post-quantum pseudorandom function. Define $\mathsf{PRF}'((k, p), m) := \mathsf{PRF}(k, m \mod p)$ for some large prime p. Then, PRF' is pseudorandom with secret period p. Fix the keys and denote $(a_m, St_m) := \mathsf{Com}(sk; \mathsf{PRF}'(k, m))$ and $f(m) := a_m$. Then $f(m)$ can be calculated by querying m to the signing oracle. Note that f also has period p, which can be retrieved by the period-finding algorithm in Lemma 8.

Then, for $i \in [k]$ and some $m_0 \in \mathcal{M}$, query $m_i := m_0 + ip$ with pure state to the signing oracle, and obtains (a_{m_i}, z_{m_i}), where a_{m_i} are equal to some a for each i. Since H is modeled as a random oracle, $c_{m_i} := \mathsf{H}(pk, a, ip)$ are distinct with overwhelming probability for each i. The adversary can run the extractor of special soundness to extract the secret key of ID, and then be able to forge signatures for any messages. From Lemma 9, the attack can be extended to the case when the signing oracle is partially blind for some polynomial ϵ, and thus break BUF.

It is natural to enhance the requirement of PRF to QPRF to avoid the above attack. Next, we show that QPRF is sufficient for provable security.

4.2 Provable Security

Theorem 4. *Let* ID *be a post-quantum sound identification scheme that is multi-*HVZK *with distinguisher's advantage at most* $\varepsilon_{\mathsf{HVZK}}$ *with power* τ*, and* PRF *be a quantum-accessible pseudorandom function. Assume there exists an adversary* $\mathcal{A}$ *that can break the BUF security of* $\mathsf{DFS}[\mathsf{ID}, \mathsf{H}, \mathsf{PRF}]$ *with* q_s *queries to the signing oracle and* q_h *queries to* H*. Then, there exist (1) a quantum adversary* $\mathcal{B}$ *breaking EUF-NMA of* $\mathsf{FS}[\mathsf{ID}, \mathsf{H}']$ *with* $(q_h + 1)$ *queries to the quantum oracle* H' *and* $(2q_s + 3q_h)$ *queries to its own quantum random oracle, (3) a quantum*

distinguisher $\mathcal{D}$ breaking Ind-qPRF of PRF with $2q_s$ quantum queries and (4) a negligible function $\varepsilon_{\mathsf{HVZK}}$ such that for any ϵ,

$$Adv^{\epsilon\text{-}\mathsf{BUF}}_{\mathsf{DFS}[\mathsf{ID},\mathsf{H},\mathsf{PRF}]}(\mathcal{A}) \leq 2\sqrt{Adv^{\mathsf{EUF\text{-}NMA}}_{\mathsf{FS}[\mathsf{ID},\mathsf{H}']}(\mathcal{B})} + 54\left(q^{3\tau}\varepsilon_{\mathsf{HVZK}}\right)^{\frac{1}{\tau+2}} + 2Adv^{\mathsf{Ind\text{-}qPRF}}_{\mathsf{PRF}}(\mathcal{D}), \tag{1}$$

where $Time(\mathcal{B}) \approx Time(\mathcal{A}) + \Theta(q)$, $Time(\mathcal{D}) \approx Time(\mathcal{A})$ and $q = q_s + q_h$.

We delay the proof in Appendix C.4.

5 Blind Unforgeability of Hedged Fiat-Shamir Signature Schemes

In this section, we analyze the security for hedged Fiat-Shamir signature schemes, where the signing algorithm additionally takes a random nonce n as the input.

5.1 Hedged Fiat-Shamir Signature Schemes and New Security Notions

Construction 5 *Let ID be an identification scheme, H and G be random oracles mapping to the challenge and the randomness space of ID respectively. The hedged Fiat-Shamir signature scheme $\mathsf{HFS}[\mathsf{ID},\mathsf{H},\mathsf{G}]$ is constructed as follows:*

- $\mathsf{HFS.Gen}(1^\lambda) : (pk, sk) \leftarrow \mathsf{IGen}(1^\lambda)$. $sk' := (pk, sk)$. *Return* (pk, sk').
- $\mathsf{HFS.Sig}(sk', m, n)$: *Parse* $sk' = (pk, sk)$. $(a, St) := \mathsf{Com}(sk; \mathsf{G}(sk, 0||m, n))$. $c := \mathsf{H}(pk, a, m)$. $z := \mathsf{Resp}(sk, c, St; \mathsf{G}(sk, 1||m, n))$. *Return* (a, z).
- $\mathsf{HFS.Ver}(pk, m, (a, z))$. *Return* $\mathsf{IVer}(pk, a, \mathsf{H}(pk, a, m), z)$.

Next, we give fine-grained security notions for HFS against superposition attacks. Aranha et al [4] consider a stronger adversary than CMA that can also control the nonce in the (classical) signing queries. We extend this model to the superposition attack case, where the message and the nonce are both quantum-accessible. To separate the two cases, we call the previous BUF security BUF-qCMA, where only the message can be controlled. For the case that the nonce is also controlled (in a quantum-accessible manner), we call it BUF-qCNMA.

Definition 3. *Let $\mathsf{HFS}[\mathsf{ID},\mathsf{H},\mathsf{G}]$ be depicted in Construction 5 and experiments be depicted in Figure 3. Define $Adv^{\epsilon\text{-}\mathsf{BUF\text{-}qCMA}}_{\mathsf{HFS}[\mathsf{ID},\mathsf{H},\mathsf{G}]}(\mathcal{A})$ and $Adv^{\epsilon\text{-}\mathsf{BUF\text{-}qCNMA}}_{\mathsf{HFS}[\mathsf{ID},\mathsf{H},\mathsf{G}]}(\mathcal{A})$ as in Definition 1. We say $\mathsf{HFS}[\mathsf{ID},\mathsf{H},\mathsf{G}]$ is blind unforgeable under quantum chosen message attacks (BUF-qCMA) or blind unforgeable under quantum chosen nonce and message attacks (BUF-qCNMA) if for any polynomial adversary $\mathcal{A}$ and any ϵ, there exists a negligible function negl such that $Adv^{\epsilon\text{-}\mathsf{BUF\text{-}qCMA}}_{\mathsf{HFS}[\mathsf{ID},\mathsf{H},\mathsf{G}]}(\mathcal{A})$ or $Adv^{\epsilon\text{-}\mathsf{BUF\text{-}qCNMA}}_{\mathsf{HFS}[\mathsf{ID},\mathsf{H},\mathsf{G}]}(\mathcal{A})$ is upper-bounded by $\mathsf{negl}(\lambda)$.*

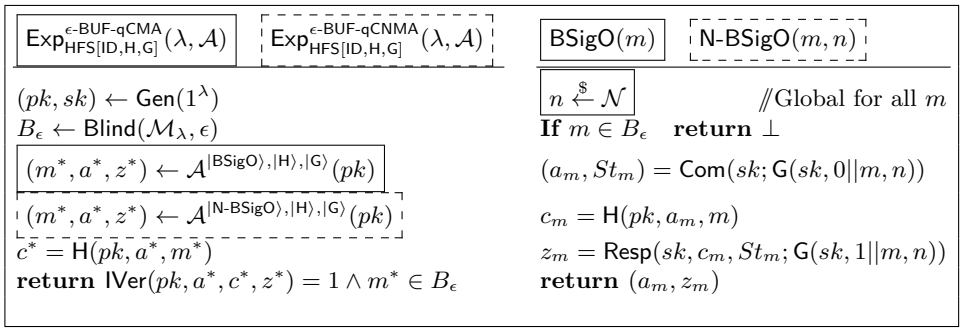

Fig. 3. Blind Unforgeablity Experiment of $\mathsf{HFS}[\mathsf{ID},\mathsf{H},\mathsf{G}]$.

5.2 Provable Security

Theorem 5. *Let ID be a secure identification scheme that is multi-HVZK with advantage power τ, and has γ-bit min-entropy. Let $\epsilon\in(0,1)$. Assume there exists an adversary $\mathcal{A}$ that can break BUF-qCMA security of $\mathsf{HFS}[\mathsf{ID},\mathsf{H},\mathsf{G}]$ with q_s queries to the signing oracle, q_h queries to H, and q_G queries to G. Then, there exist (1) a quantum adversary $\mathcal{B}$ breaking EUF-NMA of $\mathsf{FS}[\mathsf{ID},\mathsf{H}']$ with (q_h+1) queries to the quantum oracle H' and $O(q_sq_h)$ queries to its own quantum random oracle and (2) a negligible function $\varepsilon_{\mathsf{HVZK}}$ such that*

$$Adv^{\epsilon\text{-BUF-qCMA}}_{\mathsf{HFS[ID,H,G]}}(\mathcal{A})\le\min\left\{8(q_s+1)^2\epsilon,\left(\frac{2q_G}{\sqrt{\epsilon}}+1\right)\left(2\sqrt{Adv^{\mathsf{EUF\text{-}NMA}}_{\mathsf{FS[ID,H']}}(\mathcal{B})}+\mathsf{negl}\right)^{1/2}\right\},\tag{2}$$

where $\mathsf{negl}=\frac{q_s^2}{2^\kappa}+\frac{11q_sq^{3/2}}{2^{\gamma/2}}+54\left(q^{3\tau}\varepsilon_{\mathsf{HVZK}}\right)^{\frac{1}{\tau+2}}$, $Time(\mathcal{B})\approx Time(\mathcal{A})+\Theta(q_sq_h)$ *and* $q=2q_s+q_h$.

Remark 3. If we replace $\mathsf{G}(sk,\cdot)$ with $\mathsf{G}(k,\cdot)$ in the hedged construction, where $k\xleftarrow{\$}\{0,1\}^{\kappa'}$ be an additional part of the secret key (which is essentially the construction in [6]). From Lemma 2.2 in [42], the left-hand side of Equation (2) can be bounded by $2\sqrt{\mathrm{Adv}^{\mathsf{EUF\text{-}NMA}}_{\mathsf{FS[ID,H']}}(\mathcal{B})}+2q_s\cdot2^{-\kappa'/2}+\mathsf{negl}$ (independent to q_G), a tighter bound.

Theorem 6. *Let ID be a secure identification scheme that is multi-HVZK with advantage power τ, and has γ-bit min-entropy. Let $\epsilon\in(0,1)$. Assume there exists an adversary $\mathcal{A}$ that can break BUF-qCNMA security of $\mathsf{HFS}[\mathsf{ID},\mathsf{H},\mathsf{G}]$ with probability $p_{\mathcal{A}}$ and with q_s queries to the signing oracle, q_h queries to H, and q_G queries to G. Then, there exist (1) a quantum adversary $\mathcal{B}$ breaking EUF-NMA of $\mathsf{FS}[\mathsf{ID},\mathsf{H}']$ with (q_h+1) queries to the quantum oracle H' and $O(q^4)$ queries to its own quantum random oracle and (2) a negligible function $\varepsilon_{\mathsf{HVZK}}$ such that*

$$Adv^{\epsilon\text{-BUF-qCNMA}}_{\mathsf{HFS[ID,H,G]}}(\mathcal{A})\le\min\left\{8(q_s+1)^2\epsilon,\left(\frac{2q_G}{\sqrt{\epsilon}}+1\right)\left(2\sqrt{Adv^{\mathsf{EUF\text{-}NMA}}_{\mathsf{FS[ID,H']}}(\mathcal{B})}+\mathsf{negl}\right)^{1/2}\right\},\tag{3}$$

where $\mathsf{negl} = \frac{34q^{9/4}}{2^{\gamma/4}} + 54\left(q^{6\tau}\varepsilon_{\mathsf{HVZK}}\right)^{\frac{1}{2\tau+2}}$, $Time(\mathcal{B}) \approx Time(\mathcal{A}) + \Theta(q^4/p_{\mathcal{A}})$ *and* $q = 2q_s + q_h$.

The proof sketch is similar to that of Theorem 4. We delay the proof in Appendix C.5 and C.6.

6 Conclusion and Open Questions

In this paper, we give comprehensive cryptanalysis on BUF security of (common variants of) FS-SIG. There are still open questions and we believe they are interesting enough for further research.

- **Fiat-Shamir with Aborts.** Fiat-Shamir with aborts (FSwBA) [38] is a variant of Fiat-Shamir transformation from ID schemes with polynomial completeness. Recent work [5,20] fixes a flaw in the security proof of FSwBA in [36]. Note that the proof of Theorem 4,5,6 for DFS/HFS in this paper use a similar approach as in [36], the similar problem also appears in FSwBA. It is an open question whether our results can be extended to FSwBA.
- **Practical Superposition Attacks.** Although we explain the hardness of proving BUF for FS-SIGs from the standard requirements, it is still an open question whether superposition attacks can be more powerful than classical CMAs for practical schemes, such as lattice-based FS-SIGs.
- **Construction of qsHVZK.** We only attempt to construct a weak qsHVZK scheme and it is not as efficient as the practical ones. It is an open question that whether we can construct a more practical ID scheme with (weak) qsHVZK. It is also interesting to observe whether practical lattice-based ID schemes can be proven qsHVZK.

7 Acknowldegement

We would like to thank Keita Xagawa for valuable discussion and anonymous reviewers of ACISP 2024 for comments. Quan Yuan and Tsuyoshi Takagi are supported by JST CREST Grant Number JPMJCR2113, Japan.

References

1. G. Alagic, C. Majenz, A. Russell, and F. Song. Quantum-access-secure message authentication via blind-unforgeability. In A. Canteaut and Y. Ishai, editors, *EUROCRYPT 2020, Part III*, volume 12107 of *LNCS*, pages 788–817. Springer, Heidelberg, May 2020.
2. A. Ambainis, M. Hamburg, and D. Unruh. Quantum security proofs using semi-classical oracles. In A. Boldyreva and D. Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 269–295. Springer, Heidelberg, Aug. 2019.
3. A. Ambainis, A. Rosmanis, and D. Unruh. Quantum attacks on classical proof systems: The hardness of quantum rewinding. In *55th FOCS*, pages 474–483. IEEE Computer Society Press, Oct. 2014.

4. D. F. Aranha, C. Orlandi, A. Takahashi, and G. Zaverucha. Security of hedged Fiat-Shamir signatures under fault attacks. In A. Canteaut and Y. Ishai, editors, *EUROCRYPT 2020, Part I*, volume 12105 of *LNCS*, pages 644–674. Springer, Heidelberg, May 2020.
5. M. Barbosa, G. Barthe, C. Doczkal, J. Don, S. Fehr, B. Grégoire, Y.-H. Huang, A. Hülsing, Y. Lee, and X. Wu. Fixing and mechanizing the security proof of fiat-shamir with aborts and dilithium. In *Advances in Cryptology - CRYPTO 2023*, pages 358–389. Springer, 2023.
6. M. Bellare, B. Poettering, and D. Stebila. From identification to signatures, tightly: A framework and generic transforms. In J. H. Cheon and T. Takagi, editors, *ASIACRYPT 2016, Part II*, volume 10032 of *LNCS*, pages 435–464. Springer, Heidelberg, Dec. 2016.
7. M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In D. E. Denning, R. Pyle, R. Ganesan, R. S. Sandhu, and V. Ashby, editors, *ACM CCS 93*, pages 62–73. ACM Press, Nov. 1993.
8. M. Bellare and B. Tackmann. Nonce-based cryptography: Retaining security when randomness fails. In M. Fischlin and J.-S. Coron, editors, *EUROCRYPT 2016, Part I*, volume 9665 of *LNCS*, pages 729–757. Springer, Heidelberg, May 2016.
9. D. Boneh, Ö. Dagdelen, M. Fischlin, A. Lehmann, C. Schaffner, and M. Zhandry. Random oracles in a quantum world. In D. H. Lee and X. Wang, editors, *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 41–69. Springer, Heidelberg, Dec. 2011.
10. D. Boneh and M. Zhandry. Quantum-secure message authentication codes. In T. Johansson and P. Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 592–608. Springer, Heidelberg, May 2013.
11. D. Boneh and M. Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. In R. Canetti and J. A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 361–379. Springer, Heidelberg, Aug. 2013.
12. Z. Brakerski, P. Christiano, U. Mahadev, U. Vazirani, and T. Vidick. A cryptographic test of quantumness and certifiable randomness from a single quantum device. *Journal of the ACM (JACM)*, 68(5):1–47, 2021.
13. Z. Brakerski, V. Koppula, U. Vazirani, and T. Vidick. Simpler proofs of quantumness. In *15th Conference on the Theory of Quantum Computation, Communication and Cryptography*, 2020.
14. T. V. Carstens, E. Ebrahimi, G. N. Tabia, and D. Unruh. Relationships between quantum IND-CPA notions. In K. Nissim and B. Waters, editors, *TCC 2021, Part I*, volume 13042 of *LNCS*, pages 240–272. Springer, Heidelberg, Nov. 2021.
15. R. Chatterjee, K.-M. Chung, X. Liang, and G. Malavolta. A note on the post-quantum security of (ring) signatures. In *Public-Key Cryptography - PKC 2022*, pages 407–436. Springer, 2022.
16. R. Chatterjee, K.-M. Chung, X. Liang, and G. Malavolta. A note on the post-quantum security of (ring) signatures. In G. Hanaoka, J. Shikata, and Y. Watanabe, editors, *PKC 2022, Part II*, volume 13178 of *LNCS*, pages 407–436. Springer, Heidelberg, Mar. 2022.
17. C. Chevalier, E. Ebrahimi, and Q.-H. Vu. On security notions for encryption in a quantum world. In *Progress in Cryptology - INDOCRYPT 2022*, pages 592–613. Springer, 2023.
18. J. Czajkowski, A. Hülsing, and C. Schaffner. Quantum indistinguishability of random sponges. In A. Boldyreva and D. Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 296–325. Springer, Heidelberg, Aug. 2019.

19. I. Damgård, J. Funder, J. B. Nielsen, and L. Salvail. Superposition attacks on cryptographic protocols. In C. Padró, editor, *ICITS 13*, volume 8317 of *LNCS*, pages 142–161. Springer, Heidelberg, 2014.
20. J. Devevey, P. Fallahpour, A. Passelègue, and D. Stehlé. A detailed analysis of Fiat-Shamir with aborts. In *Advances in Cryptology - CRYPTO 2023*, pages 327–357. Springer, 2023.
21. J. Don, S. Fehr, and C. Majenz. The measure-and-reprogram technique 2.0: Multi-round fiat-shamir and more. In D. Micciancio and T. Ristenpart, editors, *CRYPTO 2020, Part III*, volume 12172 of *LNCS*, pages 602–631. Springer, Heidelberg, Aug. 2020.
22. J. Don, S. Fehr, C. Majenz, and C. Schaffner. Security of the Fiat-Shamir transformation in the quantum random-oracle model. In A. Boldyreva and D. Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 356–383. Springer, Heidelberg, Aug. 2019.
23. J. Don, S. Fehr, C. Majenz, and C. Schaffner. Online-extractability in the quantum random-oracle model. In O. Dunkelman and S. Dziembowski, editors, *EUROCRYPT 2022, Part III*, volume 13277 of *LNCS*, pages 677–706. Springer, Heidelberg, May / June 2022.
24. S. Faust, M. Kohlweiss, G. A. Marson, and D. Venturi. On the non-malleability of the Fiat-Shamir transform. In S. D. Galbraith and M. Nandi, editors, *INDOCRYPT 2012*, volume 7668 of *LNCS*, pages 60–79. Springer, Heidelberg, Dec. 2012.
25. A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In A. M. Odlyzko, editor, *CRYPTO'86*, volume 263 of *LNCS*, pages 186–194. Springer, Heidelberg, Aug. 1987.
26. M. Fischlin. Communication-efficient non-interactive proofs of knowledge with online extractors. In V. Shoup, editor, *CRYPTO 2005*, volume 3621 of *LNCS*, pages 152–168. Springer, Heidelberg, Aug. 2005.
27. T. Gagliardoni, A. Hülsing, and C. Schaffner. Semantic security and indistinguishability in the quantum world. In M. Robshaw and J. Katz, editors, *CRYPTO 2016, Part III*, volume 9816 of *LNCS*, pages 60–89. Springer, Heidelberg, Aug. 2016.
28. S. Garg, H. Yuen, and M. Zhandry. New security notions and feasibility results for authentication of quantum data. In J. Katz and H. Shacham, editors, *CRYPTO 2017, Part II*, volume 10402 of *LNCS*, pages 342–371. Springer, Heidelberg, Aug. 2017.
29. I. Giacomelli, J. Madsen, and C. Orlandi. ZKBoo: Faster zero-knowledge for Boolean circuits. In T. Holz and S. Savage, editors, *USENIX Security 2016*, pages 1069–1083. USENIX Association, Aug. 2016.
30. A. B. Grilo, K. Hövelmanns, A. Hülsing, and C. Majenz. Tight adaptive reprogramming in the QROM. In M. Tibouchi and H. Wang, editors, *ASIACRYPT 2021, Part I*, volume 13090 of *LNCS*, pages 637–667. Springer, Heidelberg, Dec. 2021.
31. A. Hosoyamada and T. Iwata. 4-round Luby-Rackoff construction is a qPRP. In S. D. Galbraith and S. Moriai, editors, *ASIACRYPT 2019, Part I*, volume 11921 of *LNCS*, pages 145–174. Springer, Heidelberg, Dec. 2019.
32. A. Hosoyamada and K. Yasuda. Building quantum-one-way functions from block ciphers: Davies-Meyer and Merkle-Damgård constructions. In T. Peyrin and S. Galbraith, editors, *ASIACRYPT 2018, Part I*, volume 11272 of *LNCS*, pages 275–304. Springer, Heidelberg, Dec. 2018.
33. A. Hülsing, J. Rijneveld, and F. Song. Mitigating multi-target attacks in hash-based signatures. In C.-M. Cheng, K.-M. Chung, G. Persiano, and B.-Y. Yang,

editors, *PKC 2016, Part I*, volume 9614 of *LNCS*, pages 387–416. Springer, Heidelberg, Mar. 2016.
34. M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia. Quantum differential and linear cryptanalysis. *IACR Trans. Symm. Cryptol.*, 2016(1):71–94, 2016. https://tosc.iacr.org/index.php/ToSC/article/view/536.
35. J. Katz, V. Kolesnikov, and X. Wang. Improved non-interactive zero knowledge with applications to post-quantum signatures. In D. Lie, M. Mannan, M. Backes, and X. Wang, editors, *ACM CCS 2018*, pages 525–537. ACM Press, Oct. 2018.
36. E. Kiltz, V. Lyubashevsky, and C. Schaffner. A concrete treatment of Fiat-Shamir signatures in the quantum random-oracle model. In J. B. Nielsen and V. Rijmen, editors, *EUROCRYPT 2018, Part III*, volume 10822 of *LNCS*, pages 552–586. Springer, Heidelberg, Apr. / May 2018.
37. Q. Liu and M. Zhandry. Revisiting post-quantum Fiat-Shamir. In A. Boldyreva and D. Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 326–355. Springer, Heidelberg, Aug. 2019.
38. V. Lyubashevsky. Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures. In M. Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 598–616. Springer, Heidelberg, Dec. 2009.
39. C. Majenz, C. M. Manfouo, and M. Ozols. Quantum-Access Security of the Winternitz One-Time Signature Scheme. In *2nd Conference on Information-Theoretic Cryptography (ITC 2021)*, volume 199, pages 21:1–21:22. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021.
40. D. Pointcheval and J. Stern. Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, 13(3):361–396, June 2000.
41. O. Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6):1–40, 2009.
42. T. Saito, K. Xagawa, and T. Yamakawa. Tightly-secure key-encapsulation mechanism in the quantum random oracle model. In J. B. Nielsen and V. Rijmen, editors, *EUROCRYPT 2018, Part III*, volume 10822 of *LNCS*, pages 520–551. Springer, Heidelberg, Apr. / May 2018.
43. P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *35th FOCS*, pages 124–134. IEEE Computer Society Press, Nov. 1994.
44. F. Song and A. Yun. Quantum security of NMAC and related constructions - PRF domain extension against quantum attacks. In J. Katz and H. Shacham, editors, *CRYPTO 2017, Part II*, volume 10402 of *LNCS*, pages 283–309. Springer, Heidelberg, Aug. 2017.
45. D. Unruh. Quantum proofs of knowledge. In D. Pointcheval and T. Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 135–152. Springer, Heidelberg, Apr. 2012.
46. K. Xagawa. Signatures with memory-tight security in the quantum random oracle model. *Cryptology ePrint Archive*, 2023.
47. Q. Yuan, M. Tibouchi, and M. Abe. Quantum-access security of hash-based signature schemes. In *Australasian Conference on Information Security and Privacy*, pages 343–380. Springer, 2023.
48. M. Zhandry. How to construct quantum random functions. In *53rd FOCS*, pages 679–687. IEEE Computer Society Press, Oct. 2012.

A Preliminaries

A.1 Notations

For integer $n \geq 1$, $[n]$ denotes the set $\{1, ..., n\}$. For a set S, $|S|$ denotes the cardinality of S, and $x \xleftarrow{\$} S$ means that x is uniformly picked from S. We say $f : \mathbb{N} \mapsto \mathbb{R}$ is a negligible function if for every constant C, there exists $N_C \in \mathbb{N}$ such that $f(n) < n^{-C}$ holds for any $n > N_C$. Let D_1, D_2 be two distributions. Define the statistical distance between D_1 and D_2 as $\Delta(D_1, D_2) = \frac{1}{2} \max_x \left| \Pr[x \leftarrow D_1] - \Pr[x \leftarrow D_2] \right|$.

Let O_f be the oracle computing (classical) function $f : \{0,1\}^m \mapsto \{0,1\}^n$, we say O_f is quantum-accessible, say $|\mathsf{O}_f\rangle$, if O_f behaves as an unitary operator $\mathbf{U}_f$ that maps a $(m+n)$-qubit $\sum_{m,t} \alpha_{m,t} |m, t\rangle$ to $\sum_{m,t} \alpha_{m,t} |m, t \oplus f(m)\rangle$. In particular, if $\mathsf{H} : X \mapsto Y$ is a function modeled as a random oracle, then $|\mathsf{H}\rangle$ is the corresponding quantum random oracle that maps $|x, y\rangle$ to $|x, y \oplus \mathsf{H}(x)\rangle$. In particular, we assume that any quantum register (adaptively) has a base denoted by the error symbol $\perp$.

Let M be a *classical* polynomial-time algorithm with input space X, randomness space R, and output space Y. We write $y = \mathsf{M}(x; r)$ indicating that y is the output of M with input $x \in X$ and randomness $r \in R$. We say O_M is the oracle running M: (1) takes as input x; (2) picks $r \xleftarrow{\$} R$ and (3) returns $\mathsf{M}(x; r)$. The quantum-accessible O_M, say $|\mathsf{O}_\mathsf{M}\rangle$, runs as follows: (1) picks $r \xleftarrow{\$} R$, (2) takes as input $|\phi\rangle = \sum_{x,t} \alpha_{x,t} |x, t\rangle$ and (3) returns $|\phi'\rangle = \sum_{x,t} \alpha_{x,t} |x, t \oplus \mathsf{M}(x; r)\rangle$. Let M be an algorithm that outputs a bit, we simply write $\Pr[\mathsf{M} \Rightarrow 1]$ as $\Pr[\mathsf{M}]$.

For a density function f on domain X, the support of f is denoted by $\mathsf{SUPP}(f) := \{x : f(x) > 0\}$. For two density functions f_1 and f_2 with the same domain X, the Hellinger distance between f_1 and f_2 is denoted by $H^2(f_1, f_2) = 1 - \sum_{x \in X} \sqrt{f_1(x) f_2(x)}$.

A.2 Pseudorandom Functions

Definition 4. *([48]) Let $\mathsf{PRF} : \mathcal{K} \times \{0,1\}^n \mapsto \{0,1\}^\lambda$, where $\mathcal{K}$ is the key space. Let $\mathcal{F} : \{\mathsf{F} : \{0,1\}^n \mapsto \{0,1\}^\lambda\}$ be the function family mapping $\{0,1\}^n$ to $\{0,1\}^\lambda$. Let $\mathcal{A}$ be a quantum polynomial-time (QPT) adversary. Define*

$$Adv^{\mathsf{Ind\text{-}PRF}}_{\mathsf{PRF}}(\mathcal{A}) := \left| \Pr\left[\mathcal{A}^{\mathsf{PRF}(k,\cdot)}(1^\lambda) | k \xleftarrow{\$} \mathcal{K}\right] - \Pr\left[\mathcal{A}^{\mathsf{F}(\cdot)}(1^\lambda) | \mathsf{F} \xleftarrow{\$} \mathcal{F}\right] \right|,$$

and

$$Adv^{\mathsf{Ind\text{-}qPRF}}_{\mathsf{PRF}}(\mathcal{A}) := \left| \Pr\left[\mathcal{A}^{|\mathsf{PRF}(k,\cdot)\rangle}(1^\lambda) | k \xleftarrow{\$} \mathcal{K}\right] - \Pr\left[\mathcal{A}^{|\mathsf{F}(\cdot)\rangle}(1^\lambda) | \mathsf{F} \xleftarrow{\$} \mathcal{F}\right] \right|.$$

We say PRF is a pseudorandom function (PRF) if for all QPT adversary $\mathcal{A}$, there exists a negligible function negl such that $Adv^{\mathsf{Ind\text{-}PRF}}_{\mathsf{PRF}}(\mathcal{A}) \leq \mathsf{negl}(\lambda)$. Additionally, if $Adv^{\mathsf{Ind\text{-}qPRF}}_{\mathsf{PRF}}(\mathcal{A}) \leq \mathsf{negl}(\lambda)$, we also say PRF is an indistinguishable quantum pseudorandom function (Ind-qPRF), or in short QPRF.

A.3 Identification Schemes

Definition 5. *An identification scheme* ID *consists of four algorithms* IGen, Com, Resp, *and* IVer:

- $\mathsf{IGen}(1^\lambda)$ *takes as input the security parameter and outputs a key pair* (pk, sk). *We assume that* pk *defines a (samplable) challenge space* ChSet.
- $\mathsf{Com}(sk)$ *takes as input a secret key* sk *and output a commitment* a *and a state* St.
- $\mathsf{Resp}(sk, c, St)$ *takes as input a secret key* sk, *challenge* c *and a state* St. *It outputs a response* z.
- $\mathsf{IVer}(pk, a, c, z)$ *takes as input a public key* pk, *a commitment* a, *a challenge* c *and a response* z. *It outputs a bit* $b \in \{0, 1\}$.

The corresponding canonical identification protocol between a prover P *and a verifier* V *runs as follows.* $(pk, sk) \leftarrow \mathsf{IGen}(1^\lambda)$. P *and* V *respectively holds* sk *and* pk. *First,* P *runs* $(a, St) \leftarrow \mathsf{Com}(sk)$ *and sends* a *to* V. *Then,* V *randomly picks* $c \xleftarrow{\$} \mathsf{ChSet}$ *and sends* c *to* P. P *runs* $z \leftarrow \mathsf{Resp}(sk, c, St)$ *and sends* z *to* V. *Finally,* V *runs* $b = \mathsf{IVer}(pk, a, c, z)$ *and returns* b. *We say* (a, c, z) *in the communication between* P *and* V *is a transcript of* ID, *and say it is a valid transcript for* pk *if* $\mathsf{IVer}(pk, a, c, z) = 1$.

In this paper, we always require a secure ID be (perfectly) complete and post-quantum sound:

- Completeness: For $(pk, sk) \leftarrow \mathsf{IGen}(1^\lambda)$, $(a, St) \leftarrow \mathsf{Com}(sk)$, and $z \leftarrow \mathsf{Resp}(sk, c, St)$. If $c \in \mathsf{ChSet}$, it holds that $\mathsf{IVer}(pk, a, c, z) = 1$. Otherwise, $z = \perp$ and $\mathsf{IVer}(pk, a, c, z) = 0$. We say it has overwhelming completeness if $\mathsf{IVer}(pk, a, c, z) = 0$ holds with negligible probability for some c, where the probability is taken over the randomness of IGen, Com and Resp.
- Post-quantum soundness: Denote $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ as follows. $(pk, sk) \leftarrow \mathsf{IGen}(1^\lambda)$. $(a, |\phi\rangle) \leftarrow \mathcal{A}_1(pk)$. $c \xleftarrow{\$} \mathsf{ChSet}$. $z \leftarrow \mathcal{A}_2(c, |\phi\rangle)$. Then, $\Pr[\mathsf{IVer}(pk, a, c, z) = 1]$ is negligible for any QPT algorithm $\mathcal{A}$, where the probability is taken over the choice of c and the randomness of IGen and $\mathcal{A}$. [8]

In addition, $(pk, sk) \leftarrow \mathsf{IGen}(1^\lambda)$ should be hard relation, which means the computational hardness of computing sk from pk.

Definition 6. *We say* ID *has* γ *bits of min-entropy if*

$$\Pr_{(pk,sk)\leftarrow \mathsf{Gen}}\left[\max_a p_{a,sk} \leq 2^{-\gamma}\right] \geq 1 - 2^{-\gamma},$$

where $p_{a,sk} := \Pr\left[a = a' | (a', St) \leftarrow \mathsf{Com}(sk)\right]$.

Definition 7. *(Multi-HVZK.) For an identification scheme* ID, *we say an algorithm* Sim *is a simulator of* ID *that takes as input* pk *and outputs a transcript*

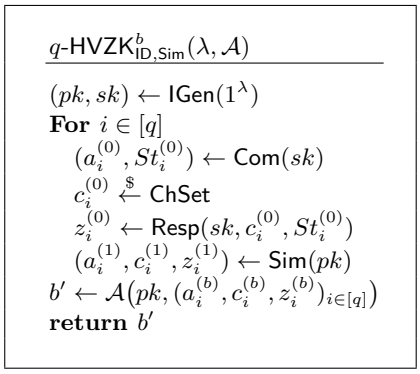

Fig. 4. Multiple HVZK Experiment.

(a,c,z). *For some integer* $q\geq 1$*, denote* q*-HVZK experiment of* ID *as in Figure 4.*

Let τ *be some constant. We say* ID *is computationally/statistically multiple honest-verifier zero-knowledge (multi-HVZK) with advantage power* τ *if there exists a polynomial-time algorithm* Sim *such that for any QPT/unbounded adversary* $\mathcal{A}$*, there exists a negligible function* ε *such that for any* q

$$Adv^{q\text{-}HVZK}_{ID,Sim}(\mathcal{A}) := \left|\Pr[q\text{-}HVZK^0_{ID,Sim}(\lambda,\mathcal{A})]-\Pr[q\text{-}HVZK^1_{ID,Sim}(\lambda,\mathcal{A})]\right|\leq q^\tau\varepsilon(\lambda), \tag{4}$$

where ε *is independent to* q*.*

Remark 4. The motivation for introducing τ is to clearly describe the relation between the advantage and the number of transcripts. In practice, the multi-HVZK property is usually proven by showing that the left-hand side of Equation (4) is upper-bounded by some $\mu(q,\xi,\lambda)$, where ξ is the running time of the adversary. Our definition essentially requires $\mu(q,\xi,\lambda)\leq q^\tau\varepsilon(\xi,\lambda)$ where ε is negligible in λ and independent to q.

If ID is statistically HVZK with advantage ε, then it is immediately statistically multi-HVZK with advantage ε and $\tau=1$. As for the computational setting, HVZK does not directly imply multi-HVZK [4]. Fortunately, many well-known computationally HVZK ID scheme is also computationally multi-HVZK in our definition. For example, the ID scheme used in KKW protocol and Picnic2 [35] is proven computationally multi-HVZK with $\tau=1$ [4].

A (classical) transcript oracle $\mathsf{Trans}(sk,\cdot)$ is defined as follows: Take as input a challenge c. It runs $(a,St)\leftarrow\mathsf{Com}(sk)$, $z\leftarrow\mathsf{Resp}(sk,St,c)$ and returns (a,z).

Definition 8. *(Special HVZK.) We say* ID *is computationally/statistically special honest-verifier zero-knowledge if there exists an efficient algorithm* Sim *such that* $\mathsf{Sim}(pk,\cdot)$ *and* $\mathsf{Trans}(sk,\cdot)$ *is computationally/statistically indistinguishable.*

[8] In some literature, the soundness is defined with adversaries that additionally have polynomially-many transcripts. In this paper, we use the version without transcripts since the gap can be filled by multi-HVZK property.

Definition 9. *(2-Soundness [37].) We say* ID *is post-quantum 2-soundness if for any quantum adversary* $\mathcal{A}$*, there exists a negligible function* negl *such that*

$$\Pr\left[\mathsf{IVer}(pk,a,c,z)=\mathsf{IVer}(pk,a,c',z')=1\wedge c\neq c'\right]<\mathsf{negl}(\lambda), \tag{5}$$

where the probability is taken over the randomness of $(pk,sk)\leftarrow\mathsf{IGen}(1^\lambda)$ *and* $(a,c,z,c',z')\leftarrow\mathcal{A}(pk)$*.*

Definition 10. *(Strict Soundness [45].* [9]*) We say* ID *is strictly sound if* $z=z'$ *holds for any* $\mathsf{IVer}(pk,a,c,z)=\mathsf{IVer}(pk,a,c,z')=1$*, where* $(pk,sk)\leftarrow\mathsf{IGen}(1^\lambda)$ *and* $c\in\mathsf{ChSet}$*.*

Definition 11. *(Special Soundness. [29]) For some constant* k*, We say* ID *is* k*-special-sound if there exists a QPT algorithm* Ext *such that: For* $(pk,sk)\leftarrow\mathsf{IGen}(1^\lambda)$*, let* (a,c_i,z_i) *be valid transcripts for* pk *such that* $c_i\neq c_j$ *for* $i\neq j$*. Taking as input* pk*,* a *and* $(c_i,z_i)_{i\in[k]}$*,* Ext *extracts the secret key* sk *with non-negligible probability.*

Lemma 3. *([37]*[10]*) Suppose* $\mathsf{ChSet}=\{0,1\}^\lambda$ *where* λ *is the security parameter. If* ID *has (1) overwhelming completeness, (2) post-quantum 2-soundness, and (3) strict soundness, then it is post-quantum sound.*

A.4 Signature Schemes

Definition 12. *An (oracle-aided) digital signature scheme* Γ *consists of three algorithms* Gen*,* Sig*,* Ver *with an oracle* O*:*

- $\mathsf{Gen}(1^\lambda)$ *takes as input the security parameter and returns a public key* pk *and a secret key* sk*. We assume that* pk *decides a message space* $\mathcal{M}_\lambda$*.*
- $\mathsf{Sig}^{\mathsf{O}}(sk,m)$ *takes as input a secret key* sk *and a message* $m\in\mathcal{M}_\lambda$*. It returns a signature* σ*.*
- $\mathsf{Ver}^{\mathsf{O}}(pk,m,\sigma)$ *takes as input the public key* pk*, a message* $m\in\mathcal{M}_\lambda$ *and a signature* σ*, and returns a bit* $b\in\{0,1\}$*.*

In this paper, we require that signature schemes should be overwhelming correct, which means that for all $m\in\mathcal{M}_\lambda$*,* $\mathsf{Ver}^{\mathsf{O}}(pk,m,\sigma)=1$ *holds with all but negligible probability, where* $(pk,sk)\leftarrow\mathsf{Gen}(1^\lambda)$ *and* $\sigma\leftarrow\mathsf{Sig}^{\mathsf{O}}(sk,m)$*.*

[9] Also known as (perfect) unique response in [24, 26].

[10] There are some differences with the original version in [37]: First, the original version requires *weak collapsingness* instead of strict soundness, which is a weaker property. Second, the original additional requires computational HVZK, since the post-quantum soundness in [37] considers transcripts but ours does not.

A.5 Noisy Trapdoor Claw-free Function Families

Let $\mathcal{X}$ and $\mathcal{Y}$ be two finite sets. A noisy trapdoor claw-free function maps $x \in \mathcal{X}$ to a distribution of $\mathcal{Y}$.

Definition 13. *Let $\mathcal{K}$, $\mathcal{X}$ and $\mathcal{Y}$ be finite sets and λ be the security parameter. A NTCF is a function family $\mathcal{F} : \{f_{k,b} : \mathcal{X} \to \mathcal{D}_\mathcal{Y}\}_{k\in\mathcal{K},b\in\{0,1\}}$ such that*

1. *(Efficient Function Generation.) There exists an efficient sampling algorithm $\mathsf{FuncGen}_\mathcal{F}$ that samples a key $k \in \mathcal{K}$ and a trapdoor t_k.*
2. *(Trapdoor Injective Pair.) For $(k, t_k) \leftarrow \mathsf{FuncGen}_\mathcal{F}$, it holds that:*
   (a) *There exists an efficient deterministic algorithm Inv such that for all $b \in \{0,1\}$, $x \in \mathcal{X}$ and $y \in \mathsf{SUPP}(f_{k,b}(x))$, it holds that $\mathsf{Inv}(t_k, b, y) = x$.*
   (b) *There exists a perfect matching $\mathcal{R}_k \subseteq \mathcal{X}^2$ such that $f_{k,0}(x_0) = f_{k,1}(x_1)$ iff $(x_0, x_1) \in \mathcal{R}_k$.*
   (c) *There exists an efficient classical sampling algorithm such that given t_k and $x \in \mathcal{X}$, it samples $y \leftarrow f_{k,0}(x)$.*
3. *(Efficient Range Superposition.) There exists a function $f'_{k,b} : \mathcal{X} \to \mathcal{D}_\mathcal{Y}$ such that for all $k \in \mathcal{K}$ and $b \in \{0,1\}$:*
   (a) *For all $(x_0, x_1) \in \mathcal{R}_k$ and $y \in \mathsf{SUPP}(f'_{k,b}(x_b))$, it holds that $\mathsf{Inv}(t_k, b, y) = x_b$ and $\mathsf{Inv}(t_k, b \oplus 1, y) = x_{b\oplus 1}$.*
   (b) *There exists an efficient predicate Chk such that $\mathsf{Chk}(k, b, x, y) = 1$ if and only if $y \in \mathsf{SUPP}(f'_{k,b}(x))$. From 3(a), it implies that if $\mathsf{Chk}(k, 0, x_0, y) = \mathsf{Chk}(k, 1, x_1, y) = 1$, then we have $(x_0, x_1) \in \mathcal{R}_k$.*
   (c) *There exists a negligible function δ such that for every $k \in \mathcal{K}$, it holds that*

$$\mathbb{E}_{x \xleftarrow{\$} \mathcal{X}} \left[H^2\big(f_{k,b}(x), f'_{k,b}(x)\big) \right] < \delta(\lambda), \tag{6}$$

   where H^2 denotes the Hellinger distance.
   (d) *There exists an efficient quantum algorithm $\mathsf{Samp}(k)$ that maps*

$$|b\rangle |0\rangle_x |0\rangle_y \mapsto \frac{1}{\sqrt{|\mathcal{X}|}} \sum_{x,y} \sqrt{(f'_{k,b}(x))(y)}\, |b, x, y\rangle .$$

4. *(Claw-free Property.) For any QPT adversary $\mathcal{A}$, there exists a negligible function ϵ such that*

$$\Pr_{(k,t_k)\leftarrow \mathsf{FuncGen}_\mathcal{F}(1^\lambda)} \left[(x_0, x_1) \leftarrow \mathcal{A}(k) : (x_0, x_1) \in \mathcal{R}_k \right] < \epsilon(\lambda).$$

Remark 5. Properties 2(c) is not required in the original definition of NTCFs [12,13], but implicitly hold in their constructions based on LWE and Ring-LWE. It ensures that our scheme can be implemented by a classical algorithm.

B Toolbox

Lemma 4. *Let f_1 and f_2 be two density functions with domain $\mathcal{X}$. Let $|\phi_1\rangle = \sum_{x\in\mathcal{X}} \sqrt{f_1(x)}\,|x\rangle$ and $|\phi_2\rangle = \sum_{x\in\mathcal{X}} \sqrt{f_2(x)}\,|x\rangle$. Then, the trace distance between $|\phi_1\rangle$ and $|\phi_2\rangle$ is*

$$Tr(|\phi_1\rangle - |\phi_2\rangle) := \frac{1}{2}\| \,|\phi_1\rangle - |\phi_2\rangle\,\|_1 \leq \sqrt{1-(1-H^2(f_1,f_2)^2)},$$

where H^2 denotes the Hellinger distance.

Lemma 5. *(Query Extraction Variant of One-way to Hiding Lemma. [2]) Let X and Y be two sets and $S \subset X$ be an arbitrary subset. Let O_1 be a random function mapping to X to Y, and O_S be a random function mapping S to Y. Denote by O_2 the function that: (1) for $\forall x \in S$, $\mathsf{O}_2(x) = O_S(x)$; (2) for $\forall x \notin S$, $\mathsf{O}_2(x) = O_1(x)$. Let inp be arbitrary input. Then, for any (potentially unbounded) quantum algorithm $\mathcal{A}$ that distinguish $\mathsf{O}_1, \mathsf{O}_2$ with q queries, there exists an extractor $\mathsf{Find}_{\mathcal{A}}$ such that*

$$\left|\Pr[\mathcal{A}^{|\mathsf{O}_1\rangle}(inp)] - \Pr[\mathcal{A}^{|\mathsf{O}_2\rangle}(inp)]\right| \leq 2q\sqrt{\Pr[x\in S : x \leftarrow \mathsf{Find}_{\mathcal{A}}^{|\mathsf{O}_1\rangle}(inp)]},$$

where $\mathsf{Find}_{\mathcal{A}}^{|\mathsf{O}_1\rangle}(inp)$ runs as follows: pick $i \xleftarrow{\$} [q]$, run $\mathcal{A}(inp)$ until the i-th query to O_1, measure the i-th query and output the measurement result.

Lemma 6. *(Adaptive Reprogramming Lemma. [30]) Let X and Y be two sets and $\mathsf{O} : X \mapsto Y$ be a random function. For some $x \in X$, $y \in Y$, denote by $\mathsf{O}^{x\mapsto y}$ the function that is the same as O except mapping x to y. Define the adaptive reprogramming game Repro_b as in Figure 5. Let $\rho^{(r)}$ be the r-th input to $\mathsf{Repgoram}$ and $\rho^{(r)}(x)$ be the marginal distribution of $\rho^{(r)}$. For any quantum algorithm $\mathcal{A}$ that has R queries to $\mathsf{Reprogram}$ and q_s queries to O_b, it holds that*

$$\left|\Pr[\mathsf{Repro}_0(\mathcal{A})] - \Pr[\mathsf{Repro}_1(\mathcal{A})] \leq \sum_{r\in[R]} \left(\sqrt{q\rho_{\max}^{(r)}} + \frac{1}{2}q\rho_{\max}^{(r)}\right), \right. \tag{7}$$

where $\rho_{\max}^{(r)} := \mathbb{E}\max_x \rho^{(r)}(x)$.

Game $\mathsf{Repro}_b(\mathcal{A})$	$\mathsf{Reprogram}(\rho)$
$\mathsf{O}_1 := \mathsf{O}_0$	$x \leftarrow \rho, \quad y \xleftarrow{\$} Y$
$b' \leftarrow \mathcal{A}^{\|\mathsf{O}_b\rangle,\mathsf{Reprogram}}$	$\mathsf{O}_1 := \mathsf{O}_1^{x\mapsto y}$
return b'	**return** x

Fig. 5. Adaptive reprogramming games for $b \in \{0,1\}$.

Lemma 7. *(Small-range Distribution Lemma. [11, 48]) Let X and Y be sets and l be some integer. Let $O_1 : X \mapsto Y$ be a random oracle. Pick $y_i \xleftarrow{\$} Y$ for each $i \in [l]$ and a random function $V : X \mapsto [l]$. Let O_2 be the oracle such that $O_2(x) = y_{V(x)}$. Then, for any adversary $\mathcal{A}$ with q queries, it holds that*

$$\left| \Pr[\mathcal{A}^{|O_1\rangle}] - \Pr[\mathcal{A}^{|O_2\rangle}] \right| \leq 27q^3/l.$$

In this paper, we use the random oracles in Lemma 7 to model hash functions, whose input is a string of arbitrary length. Without loss of generality, we assume that X covers $[l]$ (if not, let $X' = X \cup [l]$ and replace the domain of O_1 with X'). Then, O_2 can be expressed by $\mathsf{O}_1(\mathsf{V}(m))$.

Lemma 7 can be generalized to the case that $\mathsf{O}'_1 : X \times Y \mapsto Z$ and O'_2 behaves as $\mathsf{O}'_1(\mathsf{V}(x), y)$ for a random $\mathsf{V} : X \mapsto [l]$. Then, $\mathcal{A}^{|\mathsf{O}'_1\rangle}$ and $\mathcal{A}^{|\mathsf{O}'_2\rangle}$ is also $27q^3/l$-close. We can consider O_1 in Lemma 7 as a map from $x \in X$ to a function $f : Y \mapsto Z$.

Lemma 8. *(Period Finding Algorithm. [43]) Let M be a power of 2. Let f be a function with period $p \in [M/2, M)$. That is, p is the smallest one in $[M]$ such that $f(x) \equiv f(x \mod p)$ holds for all x. Then, there exists a quantum algorithm with quantum queries to f that outputs p with constant probability.*

Lemma 9. *([1]) Let X, Y be non-empty sets and $\epsilon \in [0, 1]$. Let $B_\epsilon \leftarrow \mathsf{Blind}(X, \epsilon)$. Let $f, g : X \mapsto Y$ be functions such that $f(x) = g(x)$ for all $x \notin B_\epsilon$. Let O_f be an oracle computing f and $\mathcal{A}$ be a quantum algorithm that sends q queries to oracle O. It holds that*

$$\mathop{\mathbb{E}}_{B_\epsilon}\left[\Delta\left(\mathcal{A}^{|O_f\rangle}, \mathcal{A}^{|O_g\rangle}\right)\right] \leq 2q\sqrt{\epsilon}.$$

Lemma 10. *([33]) Let X be a non-empty set and $\epsilon \in [0, 1]$. Let $B_\epsilon \leftarrow \mathsf{Blind}(X, \epsilon)$, and $f : X \mapsto \{0, 1\}$ be a Boolean function such that $f(x) = 1$ if and only if $x \in B_\epsilon$. Then for any (potentially unbounded) quantum algorithm $\mathcal{A}$ that has at most q queries to f, it holds that*

$$\Pr_{B_\epsilon}[f(x) = 1 : x \leftarrow \mathcal{A}^{|f\rangle}] \leq 8(q + 1)^2\epsilon.$$

C Security Proof

C.1 Proof of Theorem 1

The non-zero-knowldege has been proven in the sketch, and the post-quantum sound (without given transcripts) is obvious. We only need to prove the multi-HVZK. Let Sim be the simulator of ID, we construct a simulator of $\mathsf{Sim}'(pk)$ of ID' as follows. Run $(a, c, z) \leftarrow \mathsf{Sim}(pk)$ and pick $d \xleftarrow{\$} \{0, 1\}^\lambda$. Return (a, c, z') where $z' = (z, d)$.

The q-time HVZK experiment of ID' for $\mathcal{A}$ is analyzed as follows.

– **Game** G_0: The original multi-HVZK experiment of $\mathcal{A}$. That is, $G_b^0(\mathcal{A})$ denotes q-$\mathsf{HVZK}^b_{\mathsf{ID},\mathsf{Sim}'}(\lambda,\mathcal{A})$.
– **Game** G_1: Replace the $\mathsf{PRF}(k,\cdot)$ with a random function $\mathsf{F}(\cdot)$. Due to the pseudorandomness of PRF, $\Pr[G_1^0(\mathcal{A})]$ and $\Pr[G_0^0(\mathcal{A})]$ are negligibly close (say $\varepsilon_{\mathsf{PRF}}$), and $\Pr[G_1^1(\mathcal{A})] = \Pr[G_0^1(\mathcal{A})]$.
– **Game** G_2: Let $(a_i^{(0)}, c_i^{(0)}, z_i'^{(0)})_{i\in[q]}$ be the honest transcripts. Denote by **Bad** the event that $b=0$ there exist $i \neq j$ such that $c_i^{(0)} \equiv c_j^{(0)} \bmod p$. Let G_2 output 0 if **Bad** happens.
Since $c_i^{(0)}$'s are truly random. $(c_i^{(0)} - c_j^{(0)}) \bmod p$ is uniform distributed in $\mathbb{Z}_p$ for each i and j. For any $b \in \{0,1\}$, it holds that

$$\left|\Pr[G_2^b(\mathcal{A})] - \Pr[G_1^b(\mathcal{A})]\right| \leq \Pr[\mathbf{Bad}] \leq \sum_{s\in[q]} \frac{s-1}{p} < \frac{q^2}{\sqrt{N}},$$

– **Game** G_3: In the key generation, make $\mathsf{IGen}(1^\lambda; \mathsf{G}(\lambda))$ irrelevant to p. That is, picks another (inaccessible) random function G' and replace $\mathsf{IGen}(1^\lambda; \mathsf{G}(p))$ with $\mathsf{IGen}(1^\lambda; \mathsf{G}'(p))$. From Lemma 5, if $\mathcal{A}$ could distinguish the G_3 from G_2, then there exists an extractor $\mathsf{Find}_{\mathcal{A}}$ outputting p. That is, for any $b \in \{0,1\}$

$$\left|\Pr[G_3^b(\mathcal{A})] - \Pr[G_2^b(\mathcal{A})]\right| \leq 2q_G\sqrt{\Pr\left[p \leftarrow \mathsf{Find}_{\mathcal{A}}^{|\mathsf{G}\rangle}(pk)\right]},$$

where the probability is taken over G, b, $p \leftarrow \mathsf{GenPrime}(N)$ and the randomness of ID, Sim and $\mathcal{A}$.
Note that the only information about p in $\mathcal{A}$'s view is that p cannot divide a difference between any two of the challenges from the q transcripts when $b=0$. (When $b=1$, $\mathcal{A}$ cannot obtain *any* information about p.) Note that each difference has at most two prime factors in $[\sqrt{N}/2, \sqrt{N})$. Since there are $\binom{q}{2}$ differences and $\Omega\big(\sqrt{N}/\log\sqrt{N}\big)$ many primes in $[\sqrt{N}/2, \sqrt{N})$. We have

$$\Pr\left[p \leftarrow \mathsf{Find}_{\mathcal{A}}^{|\mathsf{G}\rangle}(pk)\right] \leq \frac{1}{\Omega\big(\sqrt{N}/\log\sqrt{N}\big) - \binom{q}{2}} = O\left(\frac{q^2\log N}{\sqrt{N}}\right).$$

– In G_3, the key generation is independent of p. An adversary $\mathcal{A}$ in G_3 can be used to construct a reduction $\mathcal{B}$ that breaks q-time HVZK of ID. Given pk and q transcripts $(a_i, c_i, z_i)_{i\in[q]}$, $\mathcal{R}$ picks $p \leftarrow \mathsf{GenPrime}(N)$. $\mathcal{R}$ aborts and return 0 if there exists $i \neq j$ such that $c_i \equiv c_j \bmod p$. Then, pick a random function $\mathsf{F} : \mathsf{ChSet} \mapsto \{0,1\}^\lambda$ and computes $d_i = \mathsf{F}(c_i)$, and lets $z_i' := (z_i, d_i)$. Send pk and $(a_i, c_i, z_i')_{i\in[q]}$ to $\mathcal{A}$, and return what $\mathcal{A}$ returns. $\mathcal{B}$ perfectly simulates the input to $\mathcal{A}$ with regard to G_3. We thus have $\left|\Pr[G_3^0(\mathcal{A})] - \Pr[G_3^1(\mathcal{A})]\right| \leq \mathrm{Adv}^{q\text{-}\mathsf{HVZK}}_{\mathsf{ID}}(\mathcal{B})$.
To sum up, we have

$$\begin{aligned}\mathrm{Adv}^{q\text{-}\mathsf{HVZK}}_{\mathsf{ID}}(\mathcal{A}) &= \left|\Pr[G_0^0(\mathcal{A})] - \Pr[G_0^1(\mathcal{A})]\right| \\ &\leq \mathrm{Adv}^{q\text{-}\mathsf{HVZK}}_{\mathsf{ID}}(\mathcal{B}) + 4q_G \cdot O\left(\sqrt{\frac{q^2\log N}{\sqrt{N}}}\right) + \frac{q^2}{\sqrt{N}} + \varepsilon_{\mathsf{PRF}},\end{aligned}$$

which is negligible when q and q_G is polynomial.

Game G_0^b-G_3^b

$p \leftarrow \mathsf{GenPrime}(N)$
$(pk, sk) = \mathsf{IGen}(1^\lambda; \mathsf{G}(p))$ $/\!/G_0$-G_2
$(pk, sk) \leftarrow \mathsf{IGen}(1^\lambda)$ $/\!/G_3$
$k \xleftarrow{\$} \{0,1\}^\kappa$
If $\exists i \neq j$ s.t. $c_i^{(0)} \equiv c_j^{(0)} \bmod p$ $/\!/G_2$-G_3
  return 0
$b' \leftarrow \mathcal{A}\big(pk, (a_i^{(b)}, c_i^{(b)}, z_i^{(b)}, d_i^{(b)})_{i\in[q]}\big)$
return b'

For $i \in [q]$
  $(a_i^{(0)}, St_i^{(0)}) \leftarrow \mathsf{Com}(sk)$
  $c_i^{(0)} \xleftarrow{\$} \mathsf{ChSet}$
  $z_i^{(0)} \leftarrow \mathsf{Resp}(sk, c_i^{(0)}, St_i^{(0)})$
  $d_i^{(0)} := \mathsf{PRF}(k, c_i^{(0)} \bmod p)$ $/\!/G_0$-G_1
  $d_i^{(0)} := \mathsf{F}(c_i^{(0)} \bmod p)$ $/\!/G_2$-G_3
  $(a_i^{(1)}, c_i^{(1)}, z_i^{(1)}) \leftarrow \mathsf{Sim}(pk)$
  $d_i^{(1)} \xleftarrow{\$} \{0,1\}^\lambda$

Fig. 6. Games G_0 to G_3 in the proof of Theorem 1.

C.2 Proof of Theroem 2

Due to Lemma 3, we need to prove the completeness, 2-soundness, strict soundness and weak qsHVZK from the properties in Definition 13.

- **Overwhelming Completeness.** If $c_i = 0$, $\mathsf{Chk}(k, c_i, x_i, y_i) = 1$ immediately holds from property 3(a) and 3(b). We then consider the case that $c_i = 1$. Note that $y_i \leftarrow f_{k,0}(x_0^{(0)})$ for *uniform* $x_0^{(0)}$. Then, the distribution of y_i is the same as $y_i' \leftarrow f_{k,1}(x_i^{(1)})$ for a uniform $x_i^{(1)}$ (since $\mathcal{R}_k$ is a perfect matching), and $x_i = \mathsf{Inv}(t_k, 1, y_i') = x_i^{(1)}$ from property 2(b). Then, from property 3(c), $y_i' \in \mathsf{SUPP}(f'_{k,1}(x_i))$ with overwhelming probability and thus $\mathsf{Chk}(k, 1, x_i, y_i') = 1$ holds.
- **2-soundness.** Let $\mathcal{A}$ be an adversary breaking 2-soundness of ID with non-negligible probability. A successful $\mathcal{A}(pk)$ outputs $(x_{i,0}, x_{i,1}, y_i)$ for some i : $c_i \neq c_i'$ such that $\mathsf{Chk}(k, 0, x_{i,0}, y_i) = \mathsf{Chk}(k, 1, x_{i,1}, y_i) = 1$. It implies that $(x_0, x_1) \in \mathcal{R}_k$ from property 3(b) and it breaks the claw-free property.
- **Strict Soundness.** Let $\mathsf{Ver}(pk, a, c, z) = \mathsf{Ver}(pk, a, c, z') = 1$ where $pk = k$, $a = (y_1, ..., y_\lambda)$, $c = (c_1, ..., c_\lambda)$, $z = (x_1, ..., x_\lambda)$ and $z' = (x_1', ..., x_\lambda')$. It implies that $y_i \in \mathsf{SUPP}(f'_{k,c_i}(x_i)) \cap \mathsf{SUPP}(f'_{k,c_i}(x_i'))$ for any $i \in [\lambda]$. From property 3(a), we have $x_i = \mathsf{Inv}(t_k, c_i, y_i') = x_i'$ and thus $z = z'$.
- **Weak qsHVZK.** We construct a quantum Sim for weak qsHVZK. For simplicity, we show the one-bit challenge version for $i \in [\lambda]$, and it immediately implies the full version.
  1. Taken as input pk and the quantum state $|\phi_0\rangle = \sum_{c_i\in\{0,1\}} \alpha_{c_i} |c_i\rangle$, prepare a state
  $$|\phi_1\rangle = \sum_{c_i\in\{0,1\}} \alpha_{c_i} |c_i\rangle |0\rangle_x |0\rangle_y .$$
  2. Run Samp_k on $|\phi_1\rangle$. We have
  $$|\phi_2\rangle = \frac{1}{\sqrt{|\mathcal{X}|}} \sum_{c_i,x,y} \alpha_{c_i} \sqrt{(f'_{k,c_i}(x))(y)}\, |c_i, x, y\rangle .$$

Due to Lemma 4, it is at trace distance at most $\delta(\lambda)$ from

$$|\phi_2'\rangle = \frac{1}{\sqrt{|\mathcal{X}|}} \sum_{c_i,x,y} \alpha_{c_i} \sqrt{(f_{k,c_i}(x))(y)}\, |c_i, x, y\rangle\,,$$

3. If we measure the third register of $|\phi_2'\rangle$, the result is $y^* \in \mathsf{SUPP}(f_{k,b}(\mathcal{X}))$ with probability

$$\begin{aligned} p_{y^*} =& \left\| \frac{1}{\sqrt{|\mathcal{X}|}} \sum_{c_i, x: y^* \in \mathsf{SUPP}(f_{k,c_i}(x))} \alpha_{c_i} \sqrt{(f_{k,c_i}(x))(y^*)}\, |c_i, x, y^*\rangle \right\| \\ =& \left\| \frac{1}{\sqrt{|\mathcal{X}|}} \sum_{c_i} \alpha_{c_i} \sqrt{(f_{k,c_i}(\mathsf{Inv}(t_k, c_i, y^*)))(y^*)}\, |c_i, \mathsf{Inv}(t_k, c_i, y^*), y^*\rangle \right\| \\ =& \frac{1}{|\mathcal{X}|} \Big(\alpha_0^2 \cdot f_{k,0}\big(\mathsf{Inv}(t_k, 0, y^*)\big)(y^*) + \alpha_1^2 \cdot f_{k,1}\big(\mathsf{Inv}(t_k, 1, y^*)\big)(y^*) \Big). \end{aligned}$$

From property 2(a)(b), we have $\big(x_0^*, x_1^*\big) := \big(\mathsf{Inv}(t_k, 0, y^*), \mathsf{Inv}(t_k, 1, y^*)\big) \in \mathcal{R}_k$ and thus $f_{k,0}(x_0^*) = f_{k,1}(x_1^*)$. Then, we have

$$p_{y^*} = \frac{1}{|\mathcal{X}|} \cdot (\alpha_0^2 + \alpha_1^2) f_{k,0}(x_0^*)(y^*) = \frac{1}{|\mathcal{X}|} \cdot f_{k,0}(x_0^*)(y^*).$$

Note that p_{y^*} is exactly the probability that the *real* Com algorithm outputs y^* as the commitment:

$$\begin{aligned} \Pr[(y^*, y^*) \leftarrow \mathsf{Com}(sk)] =& \sum_x \Pr[x \xleftarrow{\$} \mathcal{X}] \cdot \Pr[y^* \leftarrow f_{k,0}(x)] \\ =& \Pr[x_0^* \xleftarrow{\$} \mathcal{X}] \cdot \Pr[y^* \leftarrow f_{k,0}(x_0^*)] \\ =& \frac{1}{|\mathcal{X}|} \cdot f_{k,0}(x_0^*)(y^*). \end{aligned}$$

After the measurement, the final state is

$$\begin{aligned} |\phi_3'\rangle =& \frac{1}{\sqrt{p_{y^*}}} \frac{1}{\sqrt{|\mathcal{X}|}} \sum_{c_i} \alpha_{c_i} \sqrt{(f_{k,c_i}(\mathsf{Inv}(t_k, c_i, y^*)))(y^*)}\, |c_i, \mathsf{Inv}(t_k, c_i, y^*), y^*\rangle \\ =& \sum_{c_i} \alpha_{c_i}\, |c_i, \mathsf{Inv}(t_k, c_i, y^*)\rangle\, |y^*\rangle\,, \end{aligned}$$

which is the same as the real response of $\mathsf{emTrans}(sk)$ conditioned on $(y^*, y^*) \leftarrow \mathsf{Com}(sk)$.

We can see that the output of Sim (for 1-bit challenge) is at distance at most $\lambda\delta(\lambda)$ from $\mathsf{emTrans}$. Thus, after q queries, any unbounded $\mathcal{A}$ can distinguish the two with probability at most $q\lambda\delta(\lambda)$, which is a negligible function of λ.

C.3 Proof of Theroem 3

As preparation work, we prove a generalized version of Lemma 6.

Lemma 11. *(Generalized Adaptive Reprogramming Lemma.) Let X_1, X_2 and Y be sets and $\mathsf{O} : X_1 \times X_2 \mapsto Y$ be a random function. Let $\mathcal{U}$ be the family of all functions mapping $X_2 \mapsto Y$. Let S be an arbitrary subset of Y_2. For $x \in X_1$ and $\mathsf{U} \in \mathcal{U}$, denote by $\hat{\mathsf{O}} = \mathsf{O}^{(x_1,\cdot)\overset{S}{\mapsto}\mathsf{U}(\cdot)}$ the function that is the same as O except that $\hat{\mathsf{O}}(x_1, x_2) = \mathsf{U}(x_2)$ for all $x_2 \in S \subset X_2$. Define the multiple adaptive reprogramming game MRepro_b as in Figure 7. For any quantum algorithm $\mathcal{A}$ that has R queries to $\mathsf{MReprogram}$ and q queries to O_b, it holds that*

$$\left|\Pr[\mathit{MRepro}_0(\mathcal{A})] - \Pr[\mathit{MRepro}_1(\mathcal{A})]\right| \leq \sum_{r\in[R]} \left(\sqrt{q\rho^{(r)}_{\max}} + \frac{1}{2}q\rho^{(r)}_{\max}\right), \tag{8}$$

where $\rho^{(r)}_{\max} := \mathbb{E}\max_x \rho^{(r)}(x)$.

Game $\mathsf{MRepro}_b(\mathcal{A})$	$\mathsf{MReprogram}(\rho)$
$\mathsf{O}_1 := \mathsf{O}_0$	$x \leftarrow \rho \quad \mathsf{U} \overset{\$}{\leftarrow} \mathcal{U}$
$b' \leftarrow \mathcal{A}^{\lvert\mathsf{O}_b\rangle,\mathsf{MReprogram}}$	$\mathsf{O}_1 := \mathsf{O}_1^{(x,\cdot)\overset{S}{\mapsto}\mathsf{U}(\cdot)}$
return b'	**return** x

Fig. 7. Multiple adaptive reprogramming games for $b \in \{0, 1\}$.

Proof. The proof is straightforward from Lemma 6 by the following observations:

- If there exists an adversary $\mathcal{A}$ that distinguishing MRepro_b with $\mathsf{O} : X_1 \times X_2 \mapsto Y$ and subset $S \subset X_2$, then there exists an adversary $\mathcal{A}'$ that distinguishes MRepro'_b with $\mathsf{O}' : X_1 \times S \mapsto Y$ and subset $S' = S$ with the same probability. It is obvious since $\mathsf{MReprogram}$ makes no sense for $x \notin S$. Formally, $\mathcal{A}'$ runs as follows. Given $\mathsf{O}'_b : X_1 \times S \mapsto Y$, $\mathcal{A}'$ picks a random oracle $\mathsf{O}_{\overline{S}} : X_1 \times \overline{S} \mapsto Y$, where $\overline{S} := X_2 \backslash S$. Then, let $\mathsf{O}_b(x_1, x_2) := \mathsf{O}'_b(x_1, x_2)$ for $x_2 \in S$ and $\mathsf{O}_b(x_1, x_2) := \mathsf{O}_{\overline{S}}(x_1, x_2)$ for $x_2 \in \overline{S}$. When $\mathcal{A}$ queries $\mathsf{MReprogram}(\rho)$, $\mathcal{A}'$ also queries $\mathsf{MReprogram}'(\rho)$ and returns to $\mathcal{A}$ what it obtains. Note that in $\mathsf{MReprogram}'$, the U' is randomly picked from $\mathcal{U}' = \{u' : S \mapsto Y\}$. It is equivalent to randomly picking U from $\mathcal{U}$ and only $x \in S$ is used. $\mathcal{A}'$ perfectly simulates the queries from $\mathcal{A}$ and wins if $\mathcal{A}$ does.
- We then prove the indistinguishability of MRepro'_b. Note that a random function $\mathsf{O}' : X_1 \times S \mapsto Y$ can be written as a random function $\tilde{\mathsf{O}}' : X_1 \mapsto \mathcal{U}'$. that is, a function mapping $x_1 \in X_1$ to a function $u \in \mathcal{U}'$. In other words, O' runs as follows: on input (x_1, x_2), it runs $u = \tilde{\mathsf{O}}'(x_1)$ and returns $u(x_2)$.

Then, MRepro' can be considered a special case of Repro for $\tilde{\mathsf{O}}' : X_1 \mapsto \mathcal{U}'$ in Lemma 6. Note that Equation (7) is not related to the range size of the oracle. We then have Equation (8).

Let $\mathcal{A}$ be an adversary breaking BUF of $\mathsf{FS}[\mathsf{ID}, \mathsf{H}]$, we attempt to construct a reduction to break EUF-NMA of $\mathsf{FS}[\mathsf{ID}, \mathsf{H}]$. We add an additional operation in $\mathsf{BSigO}^{\not\perp}$ with a counter that counts the number of signing queries. The hybrid argument of the BUF experiment of $\mathcal{A}$ is described as follows.

- **Game** G_0: The original BUF experiment of $\mathcal{A}$.
- **Game** G_1: Let $r = (r_1, r_2)$ be the randomness of Com and Resp. The signing oracle is modified as follows. It picks a fresh random oracle F' with the same range as F and defines

$$f(m) := \begin{cases} \mathsf{F}'(m) & \text{if } m \in B_\epsilon \\ 0^{|\sigma|} & \text{if } m \notin B_\epsilon \end{cases}.$$

  Then, it computes $\sigma = \mathsf{Sig}(sk, m; r)$ for all m (instead of $m \notin B_\epsilon$). Finally, it returns $\sigma \oplus f(m)$. That is, the signing oracle computes Sig for each $m \in \mathcal{M}$ rather than only for $m \notin B_\epsilon$, and then "erases" the signatures of $m \in B_\epsilon$ by performing xor with $\mathsf{F}'(m)$.
  Since F is a random function, G_0 and G_1 is perfectly indistinguishable if r is not repeatly used. We have

$$\left|\Pr[G_1(\mathcal{A})] - \Pr[G_0(\mathcal{A})]\right| \leq q_s^2 \cdot 2^{-\lambda} \leq q_s^2 \cdot 2^{-\gamma}. \tag{9}$$

- **Game** G_2: For $j \in [q_s]$, let a_j be the commitment in the j-th query. (Note that a_j can be computed in a classical manner.) The experiment aborts if a_j has appeared in the previous signing queries. We have

$$\left|\Pr[G_2(\mathcal{A})] - \Pr[G_1(\mathcal{A})]\right| \leq q_s^2 \cdot 2^{-\gamma}. \tag{10}$$

  Note that we assume the commitment has at least γ-bit max entropy (which happens with all but probability $2^{-\gamma}$ taken over the randomness of Gen) from this step, and the probability has been included in Equation (10).
- **Game** G_3: In each query with index j, pick a quantum oracle $\mathsf{U}_j : \mathcal{M}_\lambda \mapsto \mathsf{ChSet}$. Then, after computing a_j, reprogram H with $\mathsf{H}^{(a_j,\cdot)\overline{\mapsto}\mathsf{U}_j(\cdot)}$. In other words, after the j-th query, the random oracle $\mathsf{H}(s, a, m)$ additionally checks whether $a = a_j \wedge s = pk$, and if so returns $\mathsf{U}_j(m)$. See Figure 8 for details.
  The difference between G_3 and G_2 is adaptively reprogramming H. Due to the min-entropy of ID, we have $\rho_{\max}^{(r)} \leq 2^{-\gamma}$ for each r in Lemma 11. We have

$$\left|\Pr[G_3(\mathcal{A})] - \Pr[G_2(\mathcal{A})]\right| \leq \frac{3q_s}{2}\sqrt{q_h 2^{-\gamma}}. \tag{11}$$

- **Game** G_4: Replace $c_{m,j} = \mathsf{H}(pk, a_j, m)$ with $c_{m,j} = \mathsf{U}_j(m)$ in the j-th query to $\mathsf{BSigO}^{\not\perp}$. See Figure 8 for details. The only difference appears on

$m \in B_\epsilon$: $z_{m,j}$ is not a valid signature for $m \in B_\epsilon$, since $\mathsf{H}(pk, a_j, m)$ are not reprogrammed by $\mathsf{U}_j(m)$ for $m \in B_\epsilon$. However, it can never be detected by $\mathcal{A}$ since those $z_{m,j}$'s will be eventually erased by plussing a random string $\mathsf{F}'(m)$ in the final step. Thus, the probability of G_4 and G_3 are the same.

– **Game** G_5: Reorder the operations in $\mathsf{BSigO}^{\not\perp}$ as in Figure 8. Formally, (1) let $j = j + 1$; (2) pick U_j; (3) compute $c_{m,j} = \mathsf{U}_j(m)$; (4) compute (a_j, St_j); (5) compute $z_{m,j}$; (6) check whether a_j has appeared and finally (7) reprogram H. Additionally, we instead run Step (4) in a quantum manner and perform an additional measurement on a-register after Step (5). The probability of G_4 and G_3 is the same.

$\mathsf{BSigO}^{\not\perp}(m)$ $/\!/G_3$	$\mathsf{BSigO}^{\not\perp}(m)$ $/\!/G_4$	$\mathsf{BSigO}(m)^{\not\perp}$ $/\!/G_5$
$j = j + 1$	$j = j + 1$	$j = j + 1$
$(r_1, r_2) \xleftarrow{\$} \mathcal{R}_1 \times \mathcal{R}_2$	$(r_1, r_2) \xleftarrow{\$} \mathcal{R}_1 \times \mathcal{R}_2$	$\mathsf{U}_j \xleftarrow{\$} \mathcal{U}$
$(a_j, St_j) = \mathsf{Com}(sk; r_1)$	$(a_j, St_j) = \mathsf{Com}(sk; r_1)$	$c_{m,j} = \mathsf{U}_j(m)$
If $a_j \in \{a_i\}_{i \in [j-1]}$	**If** $a_j \in \{a_i\}_{i \in [j-1]}$	$(r_1, r_2) \xleftarrow{\$} \mathcal{R}_1 \times \mathcal{R}_2$
return $\perp$	**return** $\perp$	$(a_j, St_j) = \mathsf{Com}(sk; r_1)$
$\mathsf{U}_j \xleftarrow{\$} \mathcal{U}$	$\mathsf{U}_j \xleftarrow{\$} \mathcal{U}$	$z_{m,j} = \mathsf{Resp}(sk, c_{m,j}, St_j; r_2)$
$\mathsf{H} := \mathsf{H}^{(pk,a_j,\cdot) \overline{\mapsto}_{\mathsf{f}} \mathsf{U}_j(\cdot)}$	$\mathsf{H} := \mathsf{H}^{(pk,a_j,\cdot) \overline{\mapsto}_{\mathsf{f}} \mathsf{U}_j(\cdot)}$	**If** $a_j \in \{a_i\}_{i \in [j-1]}$
$c_{m,j} = \mathsf{H}(pk, a_j, m)$	$c_{m,j} = \mathsf{U}_j(m)$	**return** $\perp$
$z_{m,j} = \mathsf{Resp}(sk, c_{m,j}, St_j; r_2)$	$z_{m,j} = \mathsf{Resp}(sk, c_{m,j}, St_j; r_2)$	$\mathsf{H} := \mathsf{H}^{(pk,a_j,\cdot) \overline{\mapsto}_{\mathsf{f}} \mathsf{U}_j(\cdot)}$
return $(a_j, z_{m,j}) \oplus f(m)$	**return** $(a_j, z_{m,j}) \oplus f(m)$	**return** $(a_j, z_{m,j}) \oplus f(m)$

Fig. 8. $\mathsf{BSigO}^{\not\perp}$ in Game G_3 to G_5 in Theorem 3.

In G_5, the quantum signing oracle $\mathsf{BSigO}^{\not\perp}$ can be considered as follows:

1. Let $j = j + 1$. Take as input $|\phi_{j,1}\rangle = \sum_{m,t_a,t_z} \alpha^{(j)}_{m,t_1,t_2} |m, t_1, t_2\rangle$, where t_1 and t_2 denotes the a and z parts of t-register respectively.
2. Pick $\mathsf{U}_j \xleftarrow{\$} \mathcal{U}$ as a quantum random oracle. Compute U_j on m-register. Formally,
$$|\phi_{j,2}\rangle = \sum_{m,t_1,t_2} \alpha^{(j)}_{m,t_1,t_2} |m, t_1, t_2, c_{m,j}\rangle ,$$
where $c_{m,j} := \mathsf{U}_j(m)$.
3. Let $\mathsf{Trans}(sk, \cdot)$ be the quantum transcript oracle of ID. Send c-register and t_2-register to $\mathsf{Trans}(sk, \cdot)$ (treating other registers as the local states). We have,
$$|\phi_{j,3}\rangle = \sum_{m,t_1,t_2} \alpha^{(j)}_{m,t_1,t_2} |m, t_1, t_2 \oplus z_{m,j}, c_{m,j}\rangle |a_j\rangle ,$$
where $(a_j, St_j) = \mathsf{Com}(sk, r_1)$ and $z_{m,j} = \mathsf{Resp}(sk, c_{m,j}, St_j; r_2)$.

4. Measure and discard a-register as a_j. Xor a_j to t_1-register. Abort if $a_j \in \{a_i\}_{i\in[j-1]}$.
5. Uncompute U_j from m-register to c-register. We have

$$|\phi_{j,5}\rangle = \sum_{m,t_1,t_2} \alpha^{(j)}_{m,t_1,t_2} |m, t_1 \oplus a_j, t_2 \oplus z_{m,j}\rangle |0\rangle_c .$$

   Discard c-register.
6. Reprogram H with $\mathsf{H}^{(pk,a_j,\cdot)\overline{\in B_\epsilon}\mathsf{U}_j(\cdot)}$.
7. Compute $f = (f_a, f_z)$ from m to (t_1, t_2)-register, we finally have

$$|\phi_{j,7}\rangle = \sum_{m,t_1,t_2} \alpha^{(j)}_{m,t_1,t_2} |m, t_1 \oplus a_j \oplus f_a(m), t_2 \oplus z_{m,j} \oplus f_z(m)\rangle .$$

– **Game** G_6: Replace $\mathsf{Trans}(sk,\cdot)$ in Step 3 with the simulator $\mathsf{Sim}(pk,\cdot)$ of qsHVZK. We have

$$\left|\Pr[G_6(\mathcal{A})] - \Pr[G_5(\mathcal{A})]\right| \leq \mathrm{Adv}^{q_s\text{-}\mathsf{qsHVZK}}_{\mathsf{ID},\mathsf{Sim}}(\mathcal{C}), \tag{12}$$

  for some QPT adversary $\mathcal{C}$.
– In **Game** G_6, $\mathsf{BSigO}^{\not\perp}$ does not require sk any more, and thus an adversary $\mathcal{B}$ can then use $\mathcal{A}$ to attack the EUF-NMA of $\mathsf{FS}[\mathsf{ID},\mathsf{H}]$. Formally, $\mathcal{B}$ is given a public key pk and a random oracle H. Then, $\mathcal{B}$ picks a blind region $B_\epsilon \leftarrow \mathsf{Blind}(\mathcal{M}_\lambda)$ and runs $\mathcal{A}^{|\mathsf{BSigO}^{\not\perp}\rangle,|\mathsf{H}\rangle}(pk)$. $\mathcal{B}$ answers H and $\mathsf{BSigO}^{\not\perp}$ queries as in Game G_5. [11] In this process, $\mathcal{B}$ requires $(q_s + 2q_h)$ queries to its own random oracles, q_s queries to H, and the running time is approximately $\mathrm{Time}(\mathcal{A}) + \Theta(q_s)$, where $\Theta(q_s)$ comes from q_s computations of Sim.

  Finally, $\mathcal{B}$ obtains a forgery $(m^*, (a^*, z^*))$ for some $m^* \in B_\epsilon$ from $\mathcal{A}$. Since $m^* \in B_\epsilon$, $\mathsf{H}(pk, a^*, m^*)$ is never reprogrammed in **Game** G_5. Thus, it is a valid signature for $\mathsf{FS}[\mathsf{ID},\mathsf{H}]$, and the EUF-NMA security is broken. We have $\mathrm{Adv}^{\mathsf{EUF\text{-}NMA}}_{\mathsf{FS}[\mathsf{ID},\mathsf{H}]}(\mathcal{B}) \geq \Pr[G_5(\mathcal{A})]$. From Equation (9),(10), (11) and (12), we complete the proof.

  With the same approach, we can prove the wBUF$^{\not\perp}$ of $\mathsf{FS}[\mathsf{ID},\mathsf{H}]$ with the requirement of $\mathsf{wqsHVZK}$. The only difference is that the t_2 register is initialized by all-zero state. Thus, in Step 3 of **Game** G_4, Trans can be replaced with $\mathsf{emTrans}$, which can be simulated from $\mathsf{wqsHVZK}$ in **Game** G_5.

[11] To decrease the queries to the random oracle from $\mathcal{B}$, we can improve the strategy of answering H as follows. Pick a random oracle $\mathsf{U}' : [q_s] \times \mathcal{M}_\lambda \mapsto \mathsf{ChSet}$ and replace $\mathsf{U}_j(\cdot)$ with $\mathsf{U}'(j,\cdot)$ in Game G_5. Define $\mathsf{Count}(a) = j$ iff $a = a_j$ and otherwise $\mathsf{Count}(a) = 0$. (Note that the behavior of Count is changed after each signing query.) For H-queries, take as input (s, a, m, y) in superposition. If $s = pk$ and $\mathsf{Count}(a) = j > 0$, xor $\mathsf{U}'(\mathsf{Count}(a), m)$ to y. Otherwise, xor $\mathsf{H}(s, a, m)$ to y. In each H-query, $\mathcal{B}$ needs two queries to its own random oracles.

C.4 Proof of Theroem 4

Fix $\epsilon > 0$. Let $p_{\mathcal{A}} := \mathrm{Adv}^{\epsilon\text{-BUF}}_{\mathsf{DFS}[\mathsf{ID},\mathsf{H},\mathsf{PRF}]}(\mathcal{A})$ and Keys_λ be the set of all key pairs $(pk, sk) \leftarrow \mathsf{IGen}(1^\lambda)$. That is

$$\mathbb{E}_{(pk,sk)\leftarrow\mathsf{Keys}_\lambda}\left[\Pr\left[\mathcal{A}(pk) \text{ wins}\right]\right] = p_{\mathcal{A}},$$

where the winning probability of $\mathcal{A}(pk)$ is taken over the choice of H, k and the random tape of $\mathcal{A}, \mathsf{Blind}$.

Denote $\mathsf{Bad}_\lambda = \left\{(pk, sk) \in \mathsf{Keys}_\lambda : \Pr[\mathcal{A}(pk) \text{ wins}] \geq p_{\mathcal{A}}/2\right\}$. It holds that

$$|\mathsf{Bad}_\lambda|/|\mathsf{Keys}_\lambda| \geq p_{\mathcal{A}}/2. \tag{13}$$

Fix some $(pk, sk) \leftarrow \mathsf{IGen}(1^\lambda)$. We discuss the hybrid arguments as follows.

- **Game** $G_0(pk, sk)$: The ϵ-BUF experiment of $\mathsf{DFS}[\mathsf{ID}, \mathsf{H}, \mathsf{PRF}]$ for $\mathcal{A}$ in the case that the keys are given by $(pk, sk) \leftarrow \mathsf{IGen}(1^\lambda)$.
- **Game** $G_1(pk, sk)$: Replace the pseudorandom function with two random oracles $(\mathsf{U}_1, \mathsf{U}_2)$ (see Figure 9). The difference between the winning probability of G_1 and G_2 implies a distinguisher $\mathcal{D}$ of PRF. Here the distinguisher sends $2q_s$ quantum queries to the oracle $(\mathsf{PRF}(k, 0||\cdot), \mathsf{PRF}(k, 1||\cdot))$ or $(\mathsf{U}_1, \mathsf{U}_2)$. Let $\varepsilon_{\mathsf{qPRF}} = \mathrm{Adv}^{\mathsf{Ind\text{-}qPRF}}_{\mathsf{PRF}}(\mathcal{D})$, where $\mathcal{D}$ sends at most $2q_s$ queries. We have

$$|\Pr[G_1(pk, sk)] - \Pr[G_0(pk, sk)]| \leq \varepsilon_{\mathsf{qPRF}}. \tag{14}$$

Game G_1-$G_3(pk, sk)$

$B_\epsilon \leftarrow \mathsf{Blind}(\mathcal{M}_\lambda, \epsilon)$
$(m^*, (a^*, z^*)) \leftarrow \mathcal{A}^{|\mathsf{BSigO}\rangle,|\mathsf{H}\rangle}(pk)$
$c^* = \mathsf{H}(pk, a^*, m^*)$ $\quad /\!/G_1$
$c^* = \mathsf{H}'(pk, a^*, m^*)$ $\quad /\!/G_2$-G_3
If $m^* \in B_\epsilon \wedge \mathsf{IVer}(pk, a^*, c^*, z^*) = 1$
  return 1
return 0

$\mathsf{BSigO}(m)$

If $m \in B_\epsilon$ **return** $\perp$
$(a_m, St_m) = \mathsf{Com}(sk; \mathsf{U}_1(m))$
$c_m = \mathsf{H}(pk, a_m, m)$ $\quad /\!/G_1$-G_2
$c_m = \mathsf{U}(m)$ $\quad /\!/G_3$
$z_m = \mathsf{Resp}(sk, c_m, St_m; \mathsf{U}_2(m))$
return (a_m, z_m)

$\mathsf{H}(s, a, m)$

If $m \in B_\epsilon$ **return** $\mathsf{H}'(s, a, m)$ $\quad /\!/G_2$-G_3
$(a_m, St_m) = \mathsf{Com}(sk; \mathsf{U}_1(m))$ $\quad /\!/G_3$
If $a = a_m \wedge s = pk$ **return** $\mathsf{U}(m)$ $/\!/G_3$
return $\mathsf{H}(s, a, m)$

Fig. 9. Games G_1, G_2 and G_3 in the proof of Theorem 4.

– **Game** $G_2(pk, sk)$: Pick a random oracle H' with the same distribution as H. Program $\mathsf{H}(s, a, m)$ with $\mathsf{H}'(s, a, m)$ if $m \in B_\epsilon$. See Figure 9. The probability is the same as G_1.
– **Game** $G_3(pk, sk)$: Pick a random oracle $\mathsf{U} : \mathcal{M}_\lambda \mapsto \mathsf{ChSet}$. Reprogram $\mathsf{H}(s, a, m)$ for $s = pk \wedge m \notin B_\epsilon$ as follows. Run $(a_m, St_m) = \mathsf{Com}(sk; \mathsf{U}_1(m))$. If $a = a_m$, return $\mathsf{U}(m)$. Otherwise, return $\mathsf{H}(pk, a, m)$. Note that for each $m \notin B_\epsilon$, there is exactly one a_m such that $\mathsf{H}(pk, a_m, m)$ is (non-adaptively) reprogrammed with a uniform element $\mathsf{U}(m)$. Thus, the distribution of H is exactly the same after reprogramming and the probability of G_3 is equal to that of G_2. Note that in the signing queries, $c_m = \mathsf{H}(pk, a_m, m)$ can be replaced with $c_m = \mathsf{U}(m)$.
– **Game** $G_4(pk, sk)$: Let $q = q_s + q_h$ and $l = 54q^3/p_{\mathcal{A}}$.[12] Pick small-range distribution on $(\mathsf{U}_1, \mathsf{U}, \mathsf{U}_2)$. Formally, pick a random oracle V mapping to $[l]$, replace $\mathsf{U}_1(m)$, $\mathsf{U}(m)$ and $\mathsf{U}_2(m)$ with $\mathsf{U}_1(\mathsf{V}(m))$, $\mathsf{U}(\mathsf{V}(m))$ and $\mathsf{U}_2(\mathsf{V}(m))$, respectively. See Figure 10. From Lemma 7, we have

$$\left| \Pr[G_4(pk, sk)] - \Pr[G_3(pk, sk)] \right| < 27q^3/l = p_{\mathcal{A}}/2. \tag{15}$$

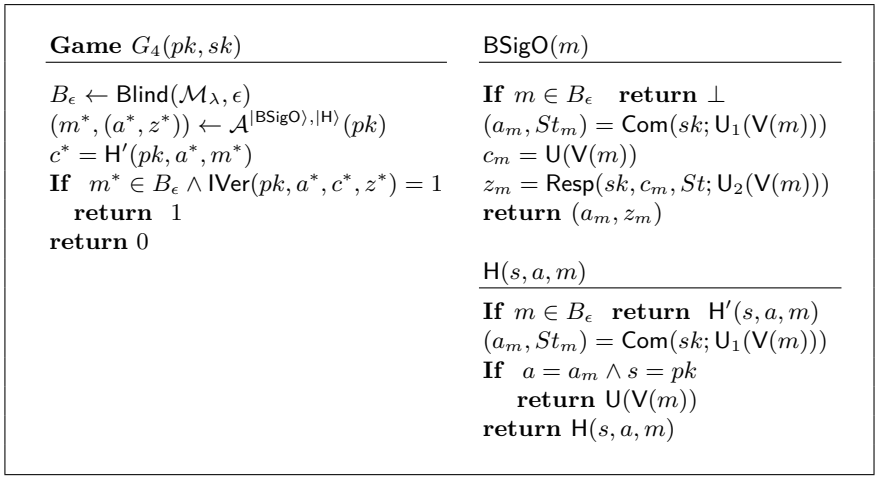

Fig. 10. Game G_4 in the proof of Theorem 4.

– **Game** $G_5(pk, sk)$: Before running $\mathcal{A}$, run $(\tilde{a}_i, \tilde{St}_i) = \mathsf{Com}(sk; \mathsf{U}_1(i))$ and $\tilde{z}_i = \mathsf{Resp}(sk, \mathsf{U}(i), \tilde{St}_i; \mathsf{U}_2(i))$ for $\forall i \in [l]$ in advance. The probability is the same as G_4.
Then, $\mathsf{BSigO}(m)$ (in the non-blind region) can be directly returned with $(\tilde{a}_{\mathsf{V}(m)}, \tilde{z}_{\mathsf{V}(m)})$. In response to H in G_5, it is not necessary to run Com as well. See Figure 11.

[12] Here, $q = q_s + q_h$ because $(\mathsf{U}_1, \mathsf{U}, \mathsf{U}_2)$ is queried q times in G_3. Note that in a computation of BSigO (or H'), $\mathsf{U}_1(m)$, $\mathsf{U}(m)$ and $\mathsf{U}_2(m)$ can be computed with a single query to $(\mathsf{U}_1, \mathsf{U}, \mathsf{U}_2)$.

– **Game** $G_6(pk, sk)$: Replace $(\tilde{a}_i, \tilde{c}_i, \tilde{z}_i)$ with $\mathsf{Sim}(pk)$. Let $\mathsf{Exp}^{l\text{-}\mathsf{HVZK}}_{\mathsf{ID},\mathsf{Sim}}(\mathcal{C}, pk, sk)$ be the specific HVZK experiment for the adversary $\mathcal{C}$ with the key pair (pk, sk). The difference between the probability of G_6 and G_5 implies a distinguisher between $\mathsf{Sim}(pk, \cdot)$ and $\mathsf{Trans}(sk, \cdot)$ with l transcripts. We have

$$\left|\Pr[G_6(pk, sk)] - \Pr[G_5(pk, sk)]\right| \leq \Pr\left[\mathsf{Exp}^{l\text{-}\mathsf{HVZK}}_{\mathsf{ID},\mathsf{Sim}}(\mathcal{C}, pk, sk)\right], \tag{16}$$

where $\mathsf{Exp}^{l\text{-}\mathsf{HVZK}}_{\mathsf{ID},\mathsf{Sim}}(\mathcal{C}, pk, sk)$ denotes the multi-HVZK experiment for $\mathcal{C}$ on condition that $(pk, sk) \leftarrow \mathsf{IGen}$.

– **Game** $G_7(pk, sk)$: As a final step, we try to avoid calculating l transcripts at the beginning of the experiment to decrease the running time of the reduction algorithm. Pick a random oracle U' mapping $[l]$ to the randomness space of Sim. G_7 does not run Sim in advance. Instead, it runs $\mathsf{Sim}(pk; \mathsf{U}'(\mathsf{V}(m)))$ when $(a_{\mathsf{V}(m)}, c_{\mathsf{V}(m)}, z_{\mathsf{V}(m)})$ is required in the signing and hash queries. See Figure 11. The probability of G_7 is the same as G_6.

Game G_5-$G_7(pk, sk)$

$B_\epsilon \leftarrow \mathsf{Blind}(\mathcal{M}_\lambda, \epsilon)$
For $\forall i \in [l]$
  $(\tilde{a}_i, \tilde{St}_i) = \mathsf{Com}(sk; \mathsf{U}_1(i))$ $\quad /\!/G_5$
  $\tilde{c}_i = \mathsf{U}(i)$ $\quad /\!/G_5$
  $\tilde{z}_i = \mathsf{Resp}(sk, \tilde{c}_i, \tilde{St}_i; \mathsf{U}_2(i))$ $\quad /\!/G_5$
  $(\tilde{a}_i, \tilde{c}_i, \tilde{z}_i) \leftarrow \mathsf{Sim}(pk)$ $\quad /\!/G_6$
$(m^*, (a^*, z^*)) \leftarrow \mathcal{A}^{|\mathsf{BSigO}\rangle, |\mathsf{H}\rangle}(pk)$
$c^* = \mathsf{H}(pk, a^*, m^*)$
If $m^* \in B_\epsilon \wedge \mathsf{IVer}(pk, a^*, c^*, z^*) = 1$
  return 1
return 0

$\mathsf{BSigO}(m)$

If $m \in B_\epsilon$ **return** $\perp$
return $(\tilde{a}_{\mathsf{V}(m)}, \tilde{z}_{\mathsf{V}(m)})$ $\quad /\!/G_5$-G_6
$(a_m, c_m, z_m) = \mathsf{Sim}(pk; \mathsf{U}'(\mathsf{V}(m)))$ $\quad /\!/G_7$
return (a_m, z_m) $\quad /\!/G_7$

$\mathsf{H}(s, a, m)$

If $m \in B_\epsilon$ **return** $\mathsf{H}'(s, a, m)$
If $a = \tilde{a}_{\mathsf{V}(m)} \wedge s = pk$ $\quad /\!/G_5$-G_6
  return $\tilde{c}_{\mathsf{V}(m)}$ $\quad /\!/G_5$-G_6
$(a_m, c_m, z_m) = \mathsf{Sim}(pk; \mathsf{U}'(\mathsf{V}(m)))$ $\quad /\!/G_7$
If $a = a_m \wedge s = pk$
  return c_m
return $\mathsf{H}'(s, a, m)$

Fig. 11. Games G_5 to G_7 in the proof of Theorem 4.

– **Game** G_7 does not need the secret key sk in the experiment any more. We use $\mathcal{A}$ breaking **Game** G_7 to construct an adversary breaking EUF-NMA of $\mathsf{FS}[\mathsf{ID}, \mathsf{H}']$. Given pk and access to H', $\mathcal{B}$ treats H' as the position in G_7, and simulates BSigO-queries and H queries for $\mathcal{A}(pk)$ as in G_7. If $\mathcal{A}$ successfully returns (m^*, a^*, z^*), it implies that $\mathsf{IVer}(pk, a^*, \mathsf{H}'(pk, a^*, m^*), z^*) = 1$ and thus it is a valid signature for pk with regard to $\mathsf{FS}[\mathsf{ID}, \mathsf{H}']$. From Equation (13), (14), (15), and (16), we have

$$
\begin{aligned}
&\Pr\left[\mathsf{Exp}^{\mathsf{EUF\text{-}NMA}}_{\mathsf{FS[ID},\mathsf{H}']}(\mathcal{B})\right] \\
\geq &\Pr_{\mathsf{IGen}}\left[(pk,sk)\in\mathsf{Bad}_\lambda\right]\cdot\Pr\left[G_7(pk,sk)\middle|(pk,sk)\in\mathsf{Bad}_\lambda\right] \\
\geq &\frac{p_{\mathcal{A}}}{2}\cdot\left(p_{\mathcal{A}}-\varepsilon_{\mathsf{qPRF}}-\frac{1}{2}p_{\mathcal{A}}-\Pr\left[\mathsf{Exp}^{l\text{-}\mathsf{HVZK}}_{\mathsf{ID},\mathsf{Sim}}(\mathcal{C},pk,sk)=1\middle|pk\in\mathsf{Bad}_\lambda\right]\right) \\
= &\frac{1}{4}p_{\mathcal{A}}^2-\frac{1}{2}p_{\mathcal{A}}\varepsilon_{\mathsf{qPRF}}-\frac{1}{2}p_{\mathcal{A}}\cdot\Pr\left[\mathsf{Exp}^{l\text{-}\mathsf{HVZK}}_{\mathsf{ID},\mathsf{Sim}}(\mathcal{C},pk,sk)=1\middle|pk\in\mathsf{Bad}_\lambda\right]
\end{aligned}
$$

From Markov's inequality, we have

$$
\begin{aligned}
\Pr\left[\mathsf{Exp}^{l\text{-}\mathsf{HVZK}}_{\mathsf{ID}}(\mathcal{C},pk,sk)=1\middle|(pk,sk)\in\mathsf{Bad}_\lambda\right] &\leq \frac{|\mathsf{Keys}_\lambda|}{|\mathsf{Bad}_\lambda|}\cdot\mathrm{Adv}^{l\text{-}\mathsf{HVZK}}_{\mathsf{ID},\mathsf{Sim}}(\mathcal{C}) \\
&\leq \frac{2l^\tau}{p_{\mathcal{A}}}\cdot\varepsilon_{\mathsf{HVZK}}.
\end{aligned}
$$

Thus,

$$
\begin{aligned}
p_{\mathcal{A}}^2 \leq &4\Pr\left[\mathsf{Exp}^{\mathsf{EUF\text{-}NMA}}_{\mathsf{FS[ID},\mathsf{H}']}(\mathcal{B})\right]+2p_{\mathcal{A}}\varepsilon_{\mathsf{qPRF}}+4l^\tau\varepsilon_{\mathsf{HVZK}} \\
= &4\Pr\left[\mathsf{Exp}^{\mathsf{EUF\text{-}NMA}}_{\mathsf{FS[ID},\mathsf{H}']}(\mathcal{B})\right]+2p_{\mathcal{A}}\varepsilon_{\mathsf{qPRF}}+\frac{4\cdot(54q^3)^\tau\varepsilon_{\mathsf{HVZK}}}{p_{\mathcal{A}}^\tau},
\end{aligned}
$$

and

$$
1\leq\frac{4\Pr\left[\mathsf{Exp}^{\mathsf{EUF\text{-}NMA}}_{\mathsf{FS[ID},\mathsf{H}']}(\mathcal{B})\right]}{p_{\mathcal{A}}^2}+\frac{2\varepsilon_{\mathsf{qPRF}}}{p_{\mathcal{A}}}+\frac{4\cdot(54q^3)^\tau\varepsilon_{\mathsf{HVZK}}}{p_{\mathcal{A}}^{\tau+2}}. \tag{17}
$$

If any of the three terms in the right-hand side of Equation (17) is larger than 1, then Equation (1) immediately holds and we are done. Otherwise, we have

$$
1\leq\sqrt{\frac{4\Pr\left[\mathsf{Exp}^{\mathsf{EUF\text{-}NMA}}_{\mathsf{FS[ID},\mathsf{H}']}(\mathcal{B})\right]}{p_{\mathcal{A}}^2}}+\frac{2\varepsilon_{\mathsf{qPRF}}}{p_{\mathcal{A}}}+\sqrt[\tau+2]{\frac{4\cdot(54q^3)^\tau\varepsilon_{\mathsf{HVZK}}}{p_{\mathcal{A}}^{\tau+2}}},
$$

and thus

$$
p_{\mathcal{A}}\leq 2\sqrt{\mathrm{Adv}^{\mathsf{EUF\text{-}NMA}}_{\mathsf{FS[ID},\mathsf{H}']}(\mathcal{B})}+2\varepsilon_{\mathsf{qPRF}}+\left(4\cdot(54q^3)^\tau\varepsilon_{\mathsf{HVZK}}\right)^{\frac{1}{\tau+2}}.
$$

Apart from the only query to $\mathcal{A}$, the reduction $\mathcal{B}$ additionally requires q_h queries to H,H' and (q_s+q_h) queries to $\mathsf{V},\mathsf{U}',\mathsf{Sim}$. We have $\mathrm{Time}(\mathcal{B})\approx\mathrm{Time}(\mathcal{A})+\Theta(q)$, where $\Theta(q)$ comes from (q_s+q_h) quantum computations of Sim.

Remark 6. If we replace $\mathsf{PRF}(k,\cdot)$ with a hash function $\mathsf{G}(k,\cdot)$ modeled as a quantum random oracle, then $\varepsilon_{\mathsf{qPRF}}$ can be replaced with $2q_G\sqrt{2^{-\kappa}}$ from Lemma 2.2 in [42], where q_G be the maximum number of queries to G.

C.5 Proof of Theorem 5

Due to Lemma 10, any (potentially unbounded) adversary can output a message $m \in B_\epsilon$ with probability at most $8(q_s+1)^2\epsilon$ (without considering the forgery). It immediately implies the first bound in Equation (2). Then, we focus on the proof of the second one.

We first show that the access to G is not helpful. The proof sketch is similar to Theorem 5 in [30]. Let $\mathsf{HFS}'[\mathsf{ID},\mathsf{H},\mathsf{G}]$ (and $\mathsf{HFS}''[\mathsf{ID},\mathsf{H},\mathsf{G}]$) be variants of $\mathsf{HFS}[\mathsf{ID},\mathsf{H},\mathsf{G}]$ as follows: Pick another random oracle G' as parts of the secret key. In the j-th query, replace $\mathsf{G}(sk,0||\cdot,n_j)$ and $\mathsf{G}(sk,1||\cdot,n_j)$ with $\mathsf{G}'(sk,0||\cdot,n_j)$ and $\mathsf{G}'(sk,1||\cdot,n_j)$ (and $\mathsf{G}'(sk,0||\cdot,j)$, $\mathsf{G}'(sk,1||\cdot,j)$). In other words, G is indeed not used in the signing algorithm of HFS' and HFS''.

We observe that $\mathrm{Adv}^{\epsilon\text{-BUF-qCMA}}_{\mathsf{HFS}'[\mathsf{ID},\mathsf{H},\mathsf{G}]}(\mathcal{A})$ and $\mathrm{Adv}^{\epsilon\text{-BUF-qCMA}}_{\mathsf{HFS}''[\mathsf{ID},\mathsf{H},\mathsf{G}]}(\mathcal{A})$ differ only if there appears a collision in $n_1,...,n_{q_s}$. Thus, for any $\mathcal{A}$ and ϵ, it holds that

$$\left|\mathrm{Adv}^{\epsilon\text{-BUF-qCMA}}_{\mathsf{HFS}'[\mathsf{ID},\mathsf{H},\mathsf{G}]}(\mathcal{A}) - \mathrm{Adv}^{\epsilon\text{-BUF-qCMA}}_{\mathsf{HFS}''[\mathsf{ID},\mathsf{H},\mathsf{G}]}(\mathcal{A})\right| \leq q_s^2 \cdot 2^{-\kappa}. \tag{18}$$

Then, we show that $\mathrm{Adv}^{\epsilon\text{-BUF-qCMA}}_{\mathsf{HFS}[\mathsf{ID},\mathsf{H},\mathsf{G}]}(\mathcal{A})$ and $\mathrm{Adv}^{\epsilon\text{-BUF-qCMA}}_{\mathsf{HFS}'[\mathsf{ID},\mathsf{H},\mathsf{G}]}(\mathcal{A})$ are close. Let $\mathsf{Exp}^{\epsilon\text{-BUF-CMA}}_{\Gamma}(\mathcal{A},pk,sk)$ be the BUF-qCMA experiment for Γ on condition that $(pk,sk) \leftarrow \mathsf{IGen}$ and $\mathrm{Adv}^{\epsilon\text{-BUF-CMA}}_{\Gamma}(\mathcal{A},pk,sk) := \Pr[\mathsf{Exp}^{\epsilon\text{-BUF-CMA}}_{\Gamma}(\mathcal{A},pk,sk)]$ be the BUF-qCMA experiment for Γ on condition that $(pk,sk) \leftarrow \mathsf{IGen}$. From Lemma 5, we have

$$\left|\mathrm{Adv}^{\epsilon\text{-BUF-CMA}}_{\mathsf{HFS}[\mathsf{ID},\mathsf{H},\mathsf{G}]}(\mathcal{A},pk,sk) - \mathrm{Adv}^{\epsilon\text{-BUF-CMA}}_{\mathsf{HFS}'[\mathsf{ID},\mathsf{H},\mathsf{G}]}(\mathcal{A},pk,sk)\right| \leq 2q_G\sqrt{\Pr[sk \leftarrow \mathsf{Find}'_{\mathcal{A}}(pk)]}, \tag{19}$$

where $\mathsf{Find}'_{\mathcal{A}}$ is the same as $\mathsf{Find}_{\mathcal{A}}$ except that it only output the first $|sk|$ bits.

We construct an adversary $\mathcal{B}'$ to break BUF of HFS' as follows: Given pk, run $\mathsf{Find}'_{\mathcal{A}}(pk)$. That is, pick $i \xleftarrow{\$} [q_G]$, run $\mathcal{A}(pk)$ until the i-th query to G, measure the G-query, and output the first $|sk|$ bits. Then, randomly pick $m^* \xleftarrow{\$} \mathcal{M}_\lambda$, and compute $z^* \leftarrow \mathsf{Sig}(sk,m^*)$. Finally, return (m^*,z^*).

If $\mathsf{Find}'_{\mathcal{A}}(pk)$ succeeds in extracting sk, then $\mathcal{B}'$ can break BUF security with at least probability ϵ. (It is able to forge signatures for any messages, but only the ones in B_ϵ meet the requirement of ϵ-BUF experiment.) That is,

$$\mathrm{Adv}^{\epsilon\text{-BUF-CMA}}_{\mathsf{HFS}'[\mathsf{ID},\mathsf{H},\mathsf{G}]}(\mathcal{B}',pk,sk) \geq \epsilon \cdot \Pr[sk \leftarrow \mathsf{Find}'_{\mathcal{A}}(pk)]. \tag{20}$$

From Equation (18), (19), and (20), we have

$$\begin{aligned}
\mathrm{Adv}^{\epsilon\text{-BUF-CMA}}_{\mathsf{HFS}[\mathsf{ID},\mathsf{H},\mathsf{G}]}(\mathcal{A},pk,sk) &\leq \left(\frac{2q_G}{\sqrt{\epsilon}}+1\right)\sqrt{\mathrm{Adv}^{\epsilon\text{-BUF-CMA}}_{\mathsf{HFS}'[\mathsf{ID},\mathsf{H},\mathsf{G}]}(\mathcal{B}',pk,sk)}, \\
&\leq \left(\frac{2q_G}{\sqrt{\epsilon}}+1\right)\sqrt{\mathrm{Adv}^{\epsilon\text{-BUF-CMA}}_{\mathsf{HFS}''[\mathsf{ID},\mathsf{H},\mathsf{G}]}(\mathcal{B}',pk,sk) + q_s^2 \cdot 2^{-\kappa}},
\end{aligned}$$

where $\mathrm{Time}(\mathcal{B}') \approx \mathrm{Time}(\mathcal{A})$.

Then, we move to bound $\mathrm{Adv}^{\epsilon\text{-BUF-qCMA}}_{\mathsf{HFS}''[\mathsf{ID},\mathsf{H},\mathsf{G}]}(\mathcal{A})$ for any $\mathcal{A}$. (To make the expressions consistent, we still use "$\mathcal{A}$" to denote the adversary for HFS'', which is indeed the $\mathcal{B}'$ in the last paragraph.) Define $p_{\mathcal{A}} := \mathrm{Adv}^{\epsilon\text{-BUF-qCMA}}_{\mathsf{HFS}''[\mathsf{ID},\mathsf{H},\mathsf{G}]}(\mathcal{A})$ and Bad_λ as in the proof of Theorem 4.

- **Game** $G_0(pk, sk)$: The original ϵ-BUF-qCMA experiment of HFS'' for $\mathcal{A}$ conditioned on $(pk, sk) \leftarrow \mathsf{IGen}(1^\lambda)$. Recall that G is never used in HFS'', so we omit the G-queries from $\mathcal{A}$.
- **Game** $G_1(pk, sk)$: Pick two random oracles H' and U_h with the same distribution as H. Program $\mathsf{H}(s, a, m)$ with $\mathsf{H}'(s, a, m)$ for $m \in B_\epsilon$ as in the proof of Theorem 4. Otherwise, let $\mathsf{H}(s, a, m) = \mathsf{U}_h(s, a, m)$. Additionally, let U_1 and U_2 be random oracles mapping to the randomness space of the signing algorithm. We replace $\mathsf{G}'(0||m||n_j)$ and $\mathsf{G}'(1||m||n_j)$ in the signing queries with $\mathsf{U}_1(m||j)$ and $\mathsf{U}_2(m||j)$, respectively. See Figure 12. The probability is the same as G_1.
- **Game** $G_2(pk, sk)$: Let $q = 2q_s + q_h$ and $l = 54q^3/p_{\mathcal{A}}$. Pick a random oracle V mapping $\mathcal{M}_\lambda \times [q_s]$ to $[l]$. Replace $\mathsf{U}_1(m, j)$, $\mathsf{U}_2(m, j)$ and $\mathsf{U}_h(s, a, m)$ with $\mathsf{U}_1(\mathsf{V}(m), j)$, $\mathsf{U}_2(\mathsf{V}(m), j)$, and $\mathsf{U}_h(s, a, \mathsf{V}(m))$, respectively. See Figure 12. From Lemma 7, it holds that

$$\left|\Pr[G_2(pk, sk)] - \Pr[G_1(pk, sk)]\right| \leq \frac{27q^3}{l} = p_{\mathcal{A}}/2. \tag{21}$$

Game G_1-$G_2(pk, sk)$

For $j \in [q_s]$ $\quad n_j \xleftarrow{\$} \mathcal{N}$
If $\exists (j_1, j_2) \in [q_s]^2 : n_{j_1} = n_{j_2} \wedge j_1 \neq j_2$
  return 0
$j = 0$
$B_\epsilon \leftarrow \mathsf{Blind}(\mathcal{M}_\lambda, \epsilon)$
$(m^*, (a^*, z^*)) \leftarrow \mathcal{A}^{|\mathsf{BSigO}\rangle, |\mathsf{H}\rangle}(pk)$
$c^* = \mathsf{H}'(pk, a^*, m^*)$
If $m^* \in B_\epsilon \wedge \mathsf{IVer}(pk, a^*, c^*, z^*) = 1$
  return 1
return 0

$\mathsf{H}(s, a, m)$

If $m \in B_\epsilon$ **return** $\mathsf{H}'(s, a, m)$
return $\mathsf{U}_h(s, a, m)$ $\quad /\!/ G_1$
return $\mathsf{U}_h(s, a, \mathsf{V}(m))$ $\quad /\!/ G_2$

$\mathsf{BSigO}(m)$

$j = j + 1$
If $m \in B_\epsilon$ **return** $\perp$
$(a_m, St_m) = \mathsf{Com}(sk; \mathsf{U}_1(m, j))$ $\quad /\!/ G_1$
$c_m = \mathsf{U}_h(pk, a_m, m)$ $\quad /\!/ G_1$
$z_m = \mathsf{Resp}(sk, c_m, St_m; \mathsf{U}_2(m, j))$ $\quad /\!/ G_1$
$(a_m, St_m) = \mathsf{Com}(sk; \mathsf{U}_1(\mathsf{V}(m), j))$ $\quad /\!/ G_2$
$c_m = \mathsf{U}_h(pk, a_m, \mathsf{V}(m))$ $\quad /\!/ G_2$
$z_m = \mathsf{Resp}(sk, c_m, St; \mathsf{U}_2(\mathsf{V}(m), j))$ $\quad /\!/ G_2$
return (a_m, z_m)

Fig. 12. Games G_1 and G_2 in the proof of Theorem 5.

– **Game** $G_3(pk, sk)$: For any $(i, j) \in [l]\times[q_s]$, runs $(\tilde{a}_{i,j}, \tilde{St}_{i,j}) := \mathsf{Com}(sk; \mathsf{U}_1(i, j))$ before running $\mathcal{A}$. It aborts if there exists $i \in [l]$ and $j_1, j_2 \in [l]$ such that $\tilde{a}_{i,j_1} = \tilde{a}_{i,j_2}$ and $j_1 \neq j_2$. Due to the min-entropy of ID, we have

$$|\Pr[G_3(pk, sk)] - \Pr[G_2(pk, sk)]| \leq l \cdot q_s^2 \cdot 2^{-\gamma} = \frac{54q_s^2q^3}{p_{\mathcal{A}}2^{\gamma}}. \tag{22}$$

– **Game** $G_4(pk, sk)$: Pick a random oracle $\mathsf{U} : [l] \times [q_s] \mapsto \mathsf{ChSet}$. Program $\mathsf{H}(pk, a, m)$ as follows. If $\exists j \in [q_s]$ such that $a = \tilde{a}_{\mathsf{V}(m),j}$, return $\mathsf{U}(\mathsf{V}(m), j)$. (Note that there exists at most one $j \in [l]$ such that $a = \tilde{a}_{\mathsf{V}(m),j}$.) Otherwise, return $\mathsf{U}_h(pk, a, \mathsf{V}(m))$.
For each $i \in [q_s]$, there are exact l number of $\tilde{a}_{i,j}$ such that $\mathsf{U}_h(pk, \tilde{a}_{i,j}, i)$ is reprogrammed with $\mathsf{U}(i, j)$. The probability of G_4 is the same as G_3 since U is a random oracle.
In **Game** G_4, $c_m = \mathsf{U}_h(pk, a_m, \mathsf{V}(m))$ in the j-th query can be replaced with $c_m = \mathsf{U}(\mathsf{V}(m), j)$.
– **Game** G_5: $\tilde{c}_{i,j}$ and $\tilde{z}_{i,j}$ are computed in advance for all $(i, j) \in [l] \times [q_s]$. The probability is the same as G_4. Note that c_m and z_m in the j-th query of BigO can be directly replaced with $\tilde{c}_{\mathsf{V}(m),j}$ and $\tilde{z}_{\mathsf{V}(m),j}$, respectively.
– **Game** G_6: $(\tilde{a}_{i,j}, \tilde{c}_{i,j}, \tilde{z}_{i,j})$ is replaced with $\mathsf{Sim}(pk)$. Similar to the proof of Theorem 4, we have

$$\big|\Pr[G_6(pk, sk)] - \Pr[G_5(pk, sk)]\big| \leq \Pr\big[\mathsf{Exp}^{lq_s\text{-}\mathsf{HVZK}}_{\mathsf{ID},\mathsf{Sim}}(\mathcal{C}, pk, sk)\big]. \tag{23}$$

– **Game** G_7: Similar to the final step in the proof of Theorem 4, we again pick a random oracle $\mathsf{U}' : [l] \times [q_s] \mapsto \mathcal{R}_{\mathsf{Sim}}$ to avoid computing lq_s simulated transcript in advance. However, it is not straightforward since we need to check whether a collision appears in the commitments and triggers aborts. (Formally, check whether there exists (i, j_1, j_2) such that $a_{i,j_1} = a_{i,j_2}$ for distinct j_1 and j_2.) This "bad event" can only be checked after the large number of Sim computations.
Indeed, there is not need to check it in such an explicit manner, since we have already considered the negligible probability of this bad event in the hybrid between G_3 and G_2. Let $\mathsf{BadU}'_{pk} \subset \mathcal{R}^{lq_s}_{\mathsf{Sim}}$ be the set of all the functions $f : [l] \times [q_s] \mapsto \mathcal{R}_{\mathsf{Sim}}$ such that there exists $(i, j_1, j_2) \in [l] \times [q_s]^2$: $\mathsf{Sim}(pk; \mathsf{U}'(i, j_1)) = \mathsf{Sim}(pk; \mathsf{U}'(i, j_2)) \wedge j_1 \neq j_2$. Then, G_7 does not needs to compute lq_s transcripts, but instead checks whether $\mathsf{U} \in \mathsf{BadU}'_{pk}$ and if so returns 0. The probability is the same as G_6
– If the adversary wins G_7 with non-negligible probability, we construct $\mathcal{B}^{\mathcal{A}}$ to break BUF-qCNMA of $\mathsf{FS}[\mathsf{ID}, \mathsf{H}']$. $\mathcal{B}$ randomly picks three random oracles $\mathsf{U}', \mathsf{V}, \mathsf{U}_h$, and runs $\mathcal{A}^{|\mathsf{H}\rangle}$ as in G_7 without checking whether $\mathsf{U}' \in \mathsf{BadU}'_{pk}$ really holds. If $\mathsf{U}' \in \mathsf{BadU}'_{pk}$, then $\mathcal{B}$ perfectly simulates the queries to $\mathcal{A}$, and succeeds if and only if $\mathcal{A}$ succeeds in G_7. Thus,

$$\Pr\left[\mathsf{Exp}^{\mathsf{EUF\text{-}NMA}}_{\mathsf{FS}[\mathsf{ID},\mathsf{H}']}(\mathcal{B})\right] \geq \Pr\left[\mathsf{Exp}^{\mathsf{EUF\text{-}NMA}}_{\mathsf{FS}[\mathsf{ID},\mathsf{H}']}(\mathcal{B}) \wedge \mathsf{U}' \notin \mathsf{BadU}'_{pk}\right] = \Pr[G_7(pk, sk)]. \tag{24}$$

Let $\varepsilon_{\mathsf{Hyb}} = 54q_s^2q^3/p_{\mathcal{A}}2^{\gamma}$. From Equation (21), (22), (23), and (24), we have

Game G_3-$G_6(pk, sk)$

$B_\epsilon \leftarrow \mathsf{Blind}(\mathcal{M}_\lambda, \epsilon)$
If $\exists (j_1, j_2) \in [q_s]^2 : n_{j_1} = n_{j_2} \wedge j_1 \neq j_2$
  return 0
$j = 0$
For $(i, j) \in [l] \times [q_s]$
  $(\tilde{a}_{i,j}, \tilde{St}_{i,j}) = \mathsf{Com}(sk; \mathsf{U}_1(i, j))$
  $\tilde{c}_{i,j} = \mathsf{U}(i, j)$ $/\!/G_5$
  $\tilde{z}_{i,j} = \mathsf{Resp}(sk, \tilde{c}_{i,j}, \tilde{St}_{i,j}; \mathsf{U}_2(i, j))$ $/\!/G_5$
  $(\tilde{a}_{i,j}, \tilde{c}_{i,j}, \tilde{z}_{i,j}) \leftarrow \mathsf{Sim}(pk)$ $/\!/G_6$
If $\exists (i, j_1, j_2) \in [l] \times [q_s]^2 : a_{i,j_1} = a_{i,j_2} \wedge j_1 \neq j_2$
  return 0
$(m^*, (a^*, z^*)) \leftarrow \mathcal{A}^{|\mathsf{BSigO}\rangle, |\mathsf{H}\rangle}(pk)$
$c^* = \mathsf{H}'(pk, a^*, m^*)$
If $m^* \in B_\epsilon \wedge \mathsf{IVer}(pk, a^*, c^*, z^*) = 1$
  return 1
return 0

$\mathsf{BSigO}(m)$

$j = j + 1$
If $m \in B_\epsilon$ **return** $\perp$
$i_m = \mathsf{V}(m)$
$a_m = \tilde{a}_{i_m,j}, \quad St_m = \tilde{St}_{i_m,j}$
$c_m = \mathsf{U}_h(pk, a_m, i_m)$ $/\!/G_3$
$c_m = \mathsf{U}(i_m, j)$ $/\!/G_4$
$z_m = \mathsf{Resp}(sk, c_m, St_m; \mathsf{U}_2(i_m, j))$ $/\!/G_3$-G_4
$z_m = \tilde{z}_{i_m,j}$ $/\!/G_5$-G_6
return (a_m, z_m)

$\mathsf{H}(s, a, m)$

If $m \in B_\epsilon$ **return** $\mathsf{H}'(s, a, m)$
For $j \in [l]$ $/\!/G_4$-G_6
  If $s = pk \wedge a = \tilde{a}_{\mathsf{V}(m),j}$ $/\!/G_4$-G_6
    return $\mathsf{U}(\mathsf{V}(m), j)$ $/\!/G_4$
    return $\tilde{c}_{\mathsf{V}(m),j}$ $/\!/G_5$-G_6
return $\mathsf{U}_h(s, a, m)$

Fig. 13. Games G_3 to G_6 in the proof of Theorem 5

Game $G_7(pk, sk)$

For $j \in [q_s]$ $n_j \xleftarrow{\$} \mathcal{N}$
If $\exists (j_1, j_2) \in [q_s]^2 : n_{j_1} = n_{j_2} \wedge j_1 \neq j_2$
  return 0
$\mathsf{U}' \leftarrow \mathcal{R}_{\mathsf{Sim}}^{lq_s}$
If $\mathsf{U}' \in \mathsf{BadU}'_{pk}$ **return** 0
$B_\epsilon \leftarrow \mathsf{Blind}(\mathcal{M}_\lambda, \epsilon)$
$(m^*, (a^*, z^*)) \leftarrow \mathcal{A}^{|\mathsf{BSigO}\rangle, |\mathsf{H}\rangle}(pk)$
$c^* = \mathsf{H}'(pk, a^*, m^*)$
If $m^* \in B_\epsilon \wedge \mathsf{IVer}(pk, a^*, c^*, z^*) = 1$
  return 1
return 0

$\mathsf{BSigO}(m, n)$

$j = j + 1$
If $m \in B_\epsilon$ **return** $\perp$
$(a_m, c_m, z_m) = \mathsf{Sim}(pk; \mathsf{U}'(\mathsf{V}(m), j))$
return (a, z)

$\mathsf{H}(s, a, m)$

If $m \in B_\epsilon$ **return** $\mathsf{H}'(s, a, m)$
For $j \in [q_s]$
  $(a_{m,j}, c_{m,j}, z_{m,j}) = \mathsf{Sim}(pk; \mathsf{U}'(\mathsf{V}(m), j))$
  If $a = a_{m,j}$ **return** $c_{m,j}$
return $\mathsf{U}_h(s, a, m)$

Fig. 14. Game G_7 in the proof of Theorem 5.

$$
\begin{aligned}
&\mathsf{Adv}^{\mathsf{EUF\text{-}NMA}}_{\mathsf{FS[ID},\mathsf{H}']}(\mathcal{B}) \\
\geq &\Pr_{\mathsf{IGen}}\left[(pk,sk)\in\mathsf{Bad}_\lambda\right]\cdot\Pr\left[G_7(pk,sk)\middle|(pk,sk)\in\mathsf{Bad}_\lambda\right] \\
\geq &\frac{p_{\mathcal{A}}}{2}\cdot\left(p_{\mathcal{A}}-\varepsilon_{\mathsf{Hyb}}-\frac{1}{2}p_{\mathcal{A}}-\Pr\left[\mathsf{Exp}^{lq_s\text{-}\mathsf{HVZK}}_{\mathsf{ID},\mathsf{Sim}}(\mathcal{C},pk,sk)=1\middle|pk\in\mathsf{Bad}_\lambda\right]\right) \\
= &\frac{1}{4}p_{\mathcal{A}}^2-\frac{1}{2}p_{\mathcal{A}}\varepsilon_{\mathsf{Hyb}}-\frac{1}{2}p_{\mathcal{A}}\cdot\Pr\left[\mathsf{Exp}^{lq_s\text{-}\mathsf{HVZK}}_{\mathsf{ID},\mathsf{Sim}}(\mathcal{C},pk,sk)=1\middle|pk\in\mathsf{Bad}_\lambda\right] \\
\geq &\frac{1}{4}p_{\mathcal{A}}^2-\frac{27q_s^2q^3}{2^\gamma}-\left(\frac{54q^3}{p_{\mathcal{A}}}\right)^\tau\varepsilon_{\mathsf{HVZK}}.
\end{aligned}
$$

Thus,

$$
1\leq\frac{4\mathrm{Adv}^{\mathsf{EUF\text{-}NMA}}_{\mathsf{FS[ID},\mathsf{H}']}(\mathcal{B})}{p_{\mathcal{A}}^2}+\frac{27q_s^2q^3}{p_{\mathcal{A}}^2 2^{\gamma-2}}+\frac{4\cdot(54q^3)^\tau}{p_{\mathcal{A}}^{\tau+2}}\varepsilon_{\mathsf{HVZK}},
$$

and

$$
p_{\mathcal{A}}\leq 2\sqrt{\mathrm{Adv}^{\mathsf{EUF\text{-}NMA}}_{\mathsf{FS[ID},\mathsf{H}']}(\mathcal{B})}+q_s\sqrt{\frac{27q^3}{2^{\gamma-2}}}+\left(4\cdot(54q^3)^\tau\varepsilon_{\mathsf{HVZK}}\right)^{\frac{1}{\tau+2}}.
$$

In total, $\mathcal{B}$ needs (q_h+1) queries to H', q_h queries to U_h and $(q_s+q_sq_h)$ queries to $\mathsf{U}',\mathsf{V},\mathsf{Sim}$.

C.6 Proof of Theorem 6

Similar to the proof of Theorem 5, we first define HFS' where $\mathsf{G}(sk,0||\cdot,\cdot)$ and $\mathsf{G}(sk,1||\cdot,\cdot)$ are replaced with $\mathsf{U}_1(\cdot,\cdot)$ and $\mathsf{U}_2(\cdot,\cdot)$, repectively. We have

$$
\mathrm{Adv}^{\epsilon\text{-}\mathsf{BUF\text{-}qCNMA}}_{\mathsf{HFS[ID},\mathsf{H},\mathsf{G}]}(\mathcal{A})\leq\left(\frac{2q_G}{\sqrt{\epsilon}}+1\right)\sqrt{\mathrm{Adv}^{\epsilon\text{-}\mathsf{BUF\text{-}qCNMA}}_{\mathsf{HFS}'\mathsf{[ID},\mathsf{H},\mathsf{G}]}(\mathcal{B}')}.
$$

for some $\mathcal{B}'$ with running time approximately the same as $\mathcal{A}$.
Let $p_{\mathcal{A}}:=\mathrm{Adv}^{\epsilon\text{-}\mathsf{BUF\text{-}qCNMA}}_{\mathsf{HFS}'\mathsf{[ID},\mathsf{H},\mathsf{G}]}(\mathcal{A})$. Define Bad_λ as in the proof of Theorem 5.

- **Game** $G_0(pk,sk)$: The original BUF-qCNMA experiment of HFS' for $\mathcal{A}$ conditioned on $(pk,sk)\leftarrow\mathsf{IGen}(1^\lambda)$. We omit G-queries as above.
- **Game** $G_1(pk,sk)$: Program H with H' for $m\in B_\epsilon$ and otherwise with U_h as in Theorem 5.
- **Game** $G_2(pk,sk)$: Let $q=2q_s+q_h$ and $l=54q^3/p_{\mathcal{A}}$. Pick random oracles V,W mapping to $[l]$. Replace $\mathsf{U}_1(m,n)$ and $\mathsf{U}_2(m,n)$ with $\mathsf{U}_1(\mathsf{V}(m),\mathsf{V}(\mathsf{W}(n))$ and $\mathsf{U}_2(\mathsf{V}(m),\mathsf{V}(\mathsf{W}(n))$, respectively. Replace $\mathsf{U}_h(s,a,m)$ with $\mathsf{U}_h(s,a,\mathsf{V}(m))$. See Figure 15 for detail. From a generalization of Lemma 7, it holds that

$$
|\Pr[G_2(pk,sk)]-\Pr[G_1(pk,sk)]|\leq\frac{27q^3}{l}=p_{\mathcal{A}}/2. \tag{25}
$$

Game G_1-$G_2(pk, sk)$

$B_\epsilon \leftarrow \mathsf{Blind}(\mathcal{M}_\lambda, \epsilon)$
$(m^*, (a^*, z^*)) \leftarrow \mathcal{A}^{|\mathsf{BSigO}\rangle, |\mathsf{H}\rangle}(pk)$
$c^* = \mathsf{H}'(pk, a^*, m^*)$
If $m^* \in B_\epsilon \wedge \mathsf{IVer}(pk, a^*, c^*, z^*) = 1$
  return 1
return 0

$\mathsf{H}(s, a, m)$

If $m \in B_\epsilon$ **return** $\mathsf{H}'(s, a, m)$
return $\mathsf{U}_h(s, a, m)$ $/\!/G_1$
return $\mathsf{U}_h(s, a, \mathsf{V}(m))$ $/\!/G_2$

$\mathsf{BSigO}(m, n)$

If $m \in B_\epsilon$ **return** $\perp$
$(a_{m,n}, St_{m,n}) = \mathsf{Com}(sk; \mathsf{U}_1(m, n))$ $/\!/G_1$
$c_{m,n} = \mathsf{U}_h(pk, a_{m,n}, m)$ $/\!/G_1$
$z_{m,n} = \mathsf{Resp}(sk, c_{m,n}, St_{m,n}; \mathsf{U}_2(m, n))$ $/\!/G_1$
$(a_{m,n}, St_{m,n}) = \mathsf{Com}(sk; \mathsf{U}_1(\mathsf{V}(m), \mathsf{W}(\mathsf{V}(m), n)))$ $/\!/G_2$
$c_{m,n} = \mathsf{U}_h(pk, a_{m,n}, \mathsf{V}(m))$ $/\!/G_2$
$z_{m,n} = \mathsf{Resp}(sk, c_{m,n}, St_{m,n}; \mathsf{U}_2(\mathsf{V}(m), \mathsf{W}(\mathsf{V}(m), n)))$ $/\!/G_2$
return $(a_{m,n}, z_{m,n})$

Fig. 15. Games G_1 and G_2 in the proof of Theorem 6.

– **Game** $G_3(pk, sk)$: For any $(i, j) \in [l]^2$, run $(\tilde{a}_{i,j}, \tilde{St}_{i,j}) := \mathsf{Com}(sk; \mathsf{U}_1(i, j))$ in advance. Abort if there exists $i, j_1, j_2 \in [l]$ such that $\tilde{a}_{i,j_1} = \tilde{a}_{i,j_2}$ and $j_1 \neq j_2$. Due to the min-entropy of ID, we have

$$\left|\Pr[G_3(pk, sk)] - \Pr[G_2(pk, sk)]\right| \leq l^3 \cdot 2^{-\gamma} = \frac{54^3 q^9}{p_{\mathcal{A}}^3 2^\gamma}. \tag{26}$$

– **Game** $G_4(pk, sk)$: Pick a random oracle $\mathsf{U} : [l]^2 \mapsto \mathsf{ChSet}$. Program $\mathsf{H}(pk, a, m)$ as follows. If $\exists j \in [l]$ such that $a = \tilde{a}_{\mathsf{V}(m),j}$, return $\mathsf{U}(\mathsf{V}(m), j)$. Similar to the proof of Theorem 5, the probability of G_4 is the same as G_3.
In G_4, $c_{m,n}$ in SigO can be replaced with $\mathsf{U}(\mathsf{V}(m), \mathsf{W}(\mathsf{V}(m), n))$
– **Game** $G_5(pk, sk)$: $\tilde{c}_{i,j}$ and $\tilde{z}_{i,j}$ are computed in advance for all $(i, j) \in [l]^2$. Then $c_{m,n}$ and $z_{m,n}$ is directly replaced with $\tilde{c}_{i,j}$ and $\tilde{z}_{i,j}$, where $i = \mathsf{V}(m)$ and $j = \mathsf{W}(i, n)$. The probability is the same as G_4.
– **Game** $G_6(pk, sk)$: $(\tilde{a}_{i,j}, \tilde{c}_{i,j}, \tilde{z}_{i,j})$ is replaced with $(\tilde{a}_{i,j}, \tilde{c}_{i,j}, \tilde{z}_{i,j}) \leftarrow \mathsf{Sim}(pk)$. Similar to the proof of Theorem 4, we have

$$\left|\Pr[G_6(pk, sk)] - \Pr[G_5(pk, sk)]\right| \leq \Pr\left[\mathsf{Exp}^{l^2\text{-}\mathsf{HVZK}}_{\mathsf{ID},\mathsf{Sim}}(\mathcal{C}, pk, sk) = 1\right]. \tag{27}$$

– **Game** G_7: Pick a random oracle $\mathsf{U}' : [l]^2 \mapsto \mathcal{R}_{\mathsf{Sim}}$. Replace $(\tilde{a}_{i,j}, \tilde{c}_{i,j}, \tilde{z}_{i,j})$ in BigO and H queries with $\mathsf{Sim}(pk', \mathsf{U}'(i, j))$. Let $\mathsf{BadU}'_{pk} \subset \mathcal{R}_{\mathsf{Sim}}^{l^2}$ be the set of all the functions $f : [l]^2 \mapsto \mathcal{R}_{\mathsf{Sim}}$ such that there exists $(i, j_1, j_2) \in [l]^3 : \mathsf{Sim}(pk; \mathsf{U}'(i, j_1)) = \mathsf{Sim}(pk; \mathsf{U}'(i, j_2)) \wedge j_1 \neq j_2$. If $\mathsf{U}' \in \mathsf{BadU}'_{pk}$, return 0. Then, in G_7, it is not necessary to compute l^2 transcripts before running $\mathcal{A}$. The probability of G_7 is the same as G_6.
– Then, we construct $\mathcal{B}^{\mathcal{A}}$ to break BUF-qCNMA of $\mathsf{FS}[\mathsf{ID}, \mathsf{H}']$. $\mathcal{B}$ randomly picks four random oracles $\mathsf{U}', \mathsf{W}, \mathsf{V}, \mathsf{U}_h$, and runs $\mathcal{A}^{\mathsf{H}'}$ as in G_7 without checking whether $\mathsf{U}' \in \mathsf{BadU}'_{pk}$ exactly holds. If $\mathsf{U}' \in \mathsf{BadU}'_{pk}$, then $\mathcal{B}$ perfectly

Game G_3-$G_6(pk, sk)$

$B_\epsilon \leftarrow \mathsf{Blind}(\mathcal{M}_\lambda, \epsilon)$
For $(i,j) \in [l]^2$
  $(\tilde{a}_{i,j}, \tilde{St}_{i,j}) = \mathsf{Com}(sk; \mathsf{U}_1(i,j))$
  $\tilde{c}_{i,j} = \mathsf{U}(i,j)$ $/\!/G_5$
  $\tilde{z}_{i,j} = \mathsf{Resp}(sk, \tilde{c}_{i,j}, \tilde{St}_{i,j}; \mathsf{U}_2(i,j))$ $/\!/G_5$
  $(\tilde{a}_{i,j}, \tilde{c}_{i,j}, \tilde{z}_{i,j}) \leftarrow \mathsf{Sim}(pk)$ $/\!/G_6$
If $\exists (i, j_1, j_2) \in [l]^3 : \tilde{a}_{i,j_1} = \tilde{a}_{i,j_2} \wedge j_1 \neq j_2$
  return 0
$(m^*, (a^*, z^*)) \leftarrow \mathcal{A}^{|\mathsf{BSigO}\rangle, |\mathsf{H}\rangle}(pk)$
$c^* = \mathsf{H}'(pk, a^*, m^*)$
If $m^* \in B_\epsilon \wedge \mathsf{IVer}(pk, a^*, c^*, z^*) = 1$
  return 1
return 0

$\mathsf{BSigO}(m, n)$

If $m \in B_\epsilon$ **return** $\perp$
$i_{m,n} = \mathsf{V}(m), \quad j_{m,n} = \mathsf{W}(\mathsf{V}(m), n)$
$a_{m,n} = \tilde{a}_{i_{m,n}, j_{m,n}}$
$c_{m,n} = \mathsf{U}_h(pk, a_{m,n}, i_{m,n})$ $/\!/G_3$
$c_{m,n} = \mathsf{U}(i_{m,n}, j_{m,n})$ $/\!/G_4$
$z_{m,n} = \mathsf{Resp}(sk, c_{m,n}, St_{m,n}; \mathsf{U}_2(i_{m,n}, j_{m,n}))$ $/\!/G_3$-G_4
$z_{m,n} = \tilde{z}_{i_{m,n}, j_{m,n}}$ $/\!/G_5$-G_6
return $(a_{m,n}, z_{m,n})$

$\mathsf{H}(s, a, m)$

If $m \in B_\epsilon$ **return** $\mathsf{H}'(s, a, m)$
For $j \in [l]$ $/\!/G_4$-G_6
  If $s = pk \wedge a = \tilde{a}_{\mathsf{V}(m),j}$ $/\!/G_4$-G_6
    return $\mathsf{U}(\mathsf{V}(m), j)$ $/\!/G_4$
    return $\tilde{c}_{\mathsf{V}(m),j}$ $/\!/G_5$-G_6
return $\mathsf{U}_h(s, a, m)$

Fig. 16. Games G_5 to G_6 in the proof of Theorem 6.

simulates the queries to $\mathcal{A}$, and succeeds if and only if $\mathcal{A}$ succeeds in G_7. Thus,

$$\Pr\left[\mathsf{Exp}^{\mathsf{EUF\text{-}NMA}}_{\mathsf{FS[ID,H']}}(\mathcal{B})\right] \geq \Pr\left[\mathsf{Exp}^{\mathsf{EUF\text{-}NMA}}_{\mathsf{FS[ID,H']}}(\mathcal{B}) \wedge \mathsf{U}' \notin \mathsf{BadU}'_{pk}\right] = \Pr[G_7(pk, sk)]. \tag{28}$$

Let $\varepsilon_{\mathsf{Hyb}} = 54^3 q^9 / p_{\mathcal{A}}^3 2^\gamma$. From Equation (25), (26), (27), and (28), we have

$$\begin{aligned}
&\mathsf{Adv}^{\mathsf{EUF\text{-}NMA}}_{\mathsf{FS[ID,H']}}(\mathcal{B}) \\
\geq &\Pr_{\mathsf{IGen}}\left[(pk, sk) \in \mathsf{Bad}_\lambda\right] \cdot \Pr\left[G_7(pk, sk) \middle| (pk, sk) \in \mathsf{Bad}_\lambda\right] \\
\geq &\frac{p_{\mathcal{A}}}{2} \cdot \left(p_{\mathcal{A}} - \varepsilon_{\mathsf{Hyb}} - \frac{1}{2} p_{\mathcal{A}} - \Pr\left[\mathsf{Exp}^{l^2\text{-}\mathsf{HVZK}}_{\mathsf{ID,Sim}}(\mathcal{C}, pk, sk) = 1 \middle| pk \in \mathsf{Bad}_\lambda\right]\right) \\
= &\frac{1}{4} p_{\mathcal{A}}^2 - \frac{1}{2} p_{\mathcal{A}} \varepsilon_{\mathsf{Hyb}} - \frac{1}{2} p_{\mathcal{A}} \cdot \Pr\left[\mathsf{Exp}^{l^2\text{-}\mathsf{HVZK}}_{\mathsf{ID,Sim}}(\mathcal{C}, pk, sk) = 1 \middle| pk \in \mathsf{Bad}_\lambda\right] \\
\geq &\frac{1}{4} p_{\mathcal{A}}^2 - \frac{54^3 q^9}{p_{\mathcal{A}}^2 2^{\gamma-1}} - \left(\frac{54 q^3}{p_{\mathcal{A}}}\right)^{2\tau} \varepsilon_{\mathsf{HVZK}}.
\end{aligned}$$

Thus,

$$1 \leq \frac{4\mathrm{Adv}^{\mathsf{EUF\text{-}NMA}}_{\mathsf{FS[ID,H']}}(\mathcal{B})}{p_{\mathcal{A}}^2} + \frac{54^3 q^9}{p_{\mathcal{A}}^4 2^{\gamma-3}} + \frac{4 \cdot (54 q^3)^{2\tau}}{p_{\mathcal{A}}^{2\tau+2}} \varepsilon_{\mathsf{HVZK}},$$

and

$$p_{\mathcal{A}} \leq 2\sqrt{\mathrm{Adv}^{\mathsf{EUF\text{-}NMA}}_{\mathsf{FS}[\mathsf{ID},\mathsf{H}']}(\mathcal{B})} + \sqrt[4]{\frac{54^3 q^9}{2^{\gamma-3}}} + \left(4 \cdot (54q^3)^{2\tau} \varepsilon_{\mathsf{HVZK}}\right)^{\frac{1}{2\tau+2}}.$$

In total, $\mathcal{B}$ needs $(q_s + q_h)$ queries to V, q_s queries to W, $(q_h + 1)$ queries to H', q_h queries to U_h and $l(q_s + q_h)$ queries to $\mathsf{U}', \mathsf{Sim}$.