Tight quantum security of the Fiat-Shamir transform for commit-and-open identification schemes with applications to post-quantum signature schemes

André Chailloux*[1]

[1]Inria de Paris, EPI COSMIQ

Abstract

Applying the Fiat-Shamir transform on identification schemes is one of the main ways of constructing signature schemes. While the classical security of this transformation is well understood, it is only very recently that generic results for the quantum case have been proposed [DFMS19, LZ19]. These results are asymptotic and therefore can't be used to derive the concrete security of these signature schemes without a significant loss in parameters.

In this paper, we show that if we start from a commit-and-open identification scheme, where the prover first commits to several strings and then as a second message opens a subset of them depending on the verifier's message, then there is a tight quantum reduction for the the Fiat-Shamir transform to special soundness notions. Our work applies to most 3 round schemes of this form and can be used immediately to derive quantum concrete security of signature schemes.

We apply our techniques to several identification schemes that lead to signature schemes such as Stern's identification scheme based on coding problems, the [KTX08] identification scheme based on lattice problems, the [SSH11] identification schemes based on multivariate problems, closely related to the NIST candidate MQDSS, and the PICNIC scheme based on multiparty computing problems, which is also a NIST candidate.

1 Introduction

Each year brings new advances in quantum technologies [ABB+19] and we will soon need to deploy post-quantum cryptography in order to prevent ourselves against the potential construction of a quantum computer capable of running Shor's algorithm [Sho94] and other powerful quantum algorithms. The NIST standardization process of post-quantum cryptographic primitives [NIS17] (specifically encryption schemes, key encapsulation mechanisms and signature schemes) is currently ongoing and it becomes crucial to continue to build trust for these schemes. A first way to build trust is to constantly challenge the post-quantum computational assumptions by designing new quantum algorithms. Another very important aspect is to make sure we have sound security reductions even with quantum computers. In particular, several technical problems arise when

*email: andre.chailloux@inria.fr

translating the Random Oracle Model[1] (ROM) to the Quantum ROM (QROM) and we need to rewrite all the security proofs involving the QROM.

Quantum security reductions for signature schemes

In this paper, we focus on quantum security reductions for signature schemes. There are mainly 2 families of signature schemes that use security reductions in the QROM: (1) Hash and Sign signatures and (2) signatures using the Fiat-Shamir transform on identification schemes. We understand well the security of Hash and Sign signatures in the QROM [Zha12]. For those using the Fiat-Shamir transform, it is only recently that there exists a general proof of its security in the QROM [DFMS19, LZ19].

So is this the end of the story? Not quite. The results of [DFMS19, LZ19] are only asymptotic and are not tight. This means that if you want your signature scheme to have 128 bits of security, you need to choose parameters such that your post-quantum computational assumption has $256, 384$ or often much more bits of security. Several schemes have tight security reductions QROM, for example those based on lossy identification schemes [KLS18] or closely related [ABB+19]. However, several others have only non tight security reductions and some even don't have a post-quantum security reduction, including some NIST candidates[2] Of course, designers that use a non-tight security reduction could take this into account in their parameters but almost no one does this as it would be devastating for their parameters. Instead, designers often have to fix parameters as if the reductions were tight and accept not having concrete security claims. For example, in their latest design specification, the authors of PICNIC write the following:

"One caveat we note is that this generalization comes with a cost in tightness of the reduction. The reduction for the ZKB++ parameter sets looses a factor of q^2, and for KKW the loss is a factor q^6, where q is the number of hash queries. As the results are non-tight, and depend on the asymptotic analysis of [DFMS19], we make no claims about the concrete security of Picnic in the QROM."

In a similar vein, the authors of the MQDSS signature scheme [CHR+20] write in their latest specifications:

"Another weakness of our security proof is that it is not at all tight. This is again an inherent weakness introduced by the rewinding technique of the forking lemma. Therefore, in order to produce a tight security reduction for MQDSS one would have to base the proof on different techniques. At the moment, we are not aware of such techniques that we could use"

This lack of tightness can have real consequences. For example, there has been a recent attack exploiting the non-tightness of the security reduction of the MQDSS signature scheme by Kales and Zaverucha [KZ19]. This was fortunately easily fixable by increasing the parameters without too much harm but this overall situation is unsettling for the trust we have in the parameter sets of these schemes, which is especially problematic since the NIST will soon choose some post-quantum signature schemes to standardize with some fixed parameters. There is therefore an urgent need to find as tight security reductions as possible for signature schemes in the QROM.

Our work in a few words

[1] In the Random Oracle Model, we model a hash function by a truly random function to which we only have black box access. This model is in all generality unrealistic and can be too strong in some corner case scenarios [CGH04] but has been extremely useful for making efficient security reductions [KM15] and is passing well the test of time.

[2] The GeMSS signature scheme described in [CFM+20] doesn't even have a full concrete security claims against classical adversaries for instance.

In this work, we show tight security reduction in the QROM for a large class of identification schemes: namely 3-round commit-and-open identification schemes. We also derive a more precise reduction when considering parallel repetition of commit-and-open identification schemes. We apply our results to existing signature schemes and show their concrete security, while until now, only asymptotic security was known. We consider Stern's signature scheme [Ste93] [3], the 3 round SSH signature scheme, which is a non-optimized version of the MQDSS signature the PICNIC signature scheme and the scheme from [KTX08].

In order to find these tight reductions, we can't use rewinding techniques as they introduce non-tightness. Moreover, we have to be careful with quantum reprogramming techniques since these can also add some non-tightness as we can see from the [DFMS19] results. So how do we proceed? We first extend Unruh's result and show the quantum security of the Fiat-Shamir transform for identification schemes that have some notion of soundness between statistical and computational soundness. Then, at a crucial moment of our proof, we need to replace a random permutation by a pseudorandom permutation which is easily invertible. We use the recent result on the quantum security of Feistel networks to construct this pseudorandom permutation. We present all steps and proof techniques more in detail in Section 2. This work is quite different and complements well the recent work [DFMS19, DFM20] as it is more suited for concrete quantum security claims useful for designers of signature schemes but is less general.

Related work

We briefly presented a few security results in the QROM, let us present a more detailed presentation of related work which will still be far from exhaustive. The QROM was first studied quite late actually in [BDF+11] where it was correctly assessed that in the quantum setting, an adversary making queries to a random oracle should have a quantum access to it, since the hash function it models has a public description. There, they showed the security of some schemes in the QROM, as well as examples where schemes were secure in the ROM but not in the QROM. Other impossibility results showed settings where, in all generality, the quantum Fiat-Shamir transform is not secure [DFG13, ARU14]. On the positive side, [DFG13] proved the security of the quantum Fiat-Shamir transform when oblivious commitments are used. Unruh [Unr15] then showed that it was possible to do a Fiat-Shamir like transform to remove the interaction from identification protocols. This transform is however rather inefficient and was hardly used in practice. More recently, there have been new positive results related to the quantum security of the Fiat-Shamir transform. If an identification scheme is lossy, then [KLS18] showed tight concrete quantum security bounds for the Fiat-Shamir transform. They used this result to prove the security of the Dilithium signature [DKL+17], which is a NIST competitor. Another related result is the security proof of qTESLA [ABB+19]. Unruh [Unr17] showed the quantum security of the Fiat-Shamir transform for identification schemes with statistical security, or using a dual-mode hard instance generator, a property closely related to the lossiness property. Another related work is the the framework of recording quantum queries by Zhandry [Zha19] which is a very powerful tool for studying random functions and the QROM[4].

[3] This scheme actually already has concrete quantum security bounds because the underlying identification scheme can be made lossy[Lei18]. However, this introduces some losses in the parameters that don't arise with our techniques.

[4] In a previous iteration of this submission, we actually tried to use this framework but we had issues with the proofs and we replaced this framework with the use of quantum-secure pseudorandom permutations arising from Feistel networks.

Recently, 2 papers [DFMS19, LZ19] showed generic reduction for the quantum Fiat-Shamir transform. Unlike what was believed before, they show that it is actually possible to perform reprogramming of a quantum random oracle and to follow the classical proofs. Their results are not tight and lose at least a factor of $O(q^2)$ where q is the number of queries to the random function. The results of [LZ19] add even a larger factor of non-tightness but can be applied to more general settings than those of [DFMS19]. Even more recently, another work [DFM20] showed that this $O(q^2)$ loss is tight and showed a large of class of examples where this is necessary. We will discuss this in the next section and show that this is less harmful than it seems for security reductions.

2 State of the art, overview of our results and proof techniques

We will focus on the quantum security of the Fiat-Shamir transform for identification schemes and we will use known results in the QROM to transform this security into the quantum security for resulting signature schemes.

State of the art for identification schemes

In an identification scheme $\mathcal{IS}$, a prover P has a pair of public and secret key (pk, sk) and wants to convince a verifier V (that sees only the public key pk) that he has a valid corresponding secret key sk. In its most standard form, an identification scheme consists of 3 messages: a first message x from P to V, a challenge c from V to P which is a random string and finally a response z from P to V. V finally has a procedure that from (pk, x, c, z) determines whether he is convinced or not. The Fiat-Shamir transform consists of replacing the above interaction with a single message $(x, \mathcal{H}(x), z)$[5] from P to V where $\mathcal{H}$ is a hash function modeled as a truly random function in the QROM.

An adversary, who knows only pk and no corresponding sk, breaks the Fiat-Shamir transform of $\mathcal{IS}$ if he can construct a triplet $(x, \mathcal{H}(x), z)$ that the verifier will accept. Breaking the identification scheme (in the sense of computational soundness) means that an adversary can construct a string x and, when he receives a challenge c, he can construct a string z such that the verifier will accept (pk, x, c, z).

The security of the quantum Fiat-Shamir transform means that we can polynomially relate the above 2 probabilities. For example, the result in [DFMS19] can be stated as follows

$$QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}]}(t, q_{\mathcal{H}}) \leq q_{\mathcal{H}}^2 \cdot QADV_{\mathcal{IS}}(O(t)). \tag{1}$$

On the left side is the quantum probability (or advantage) of breaking the Fiat-Shamir transform of an identification scheme $\mathcal{IS}$ with a quantum adversary running in time t and making $q_{\mathcal{H}}$ quantum queries to $\mathcal{H}$. The right side corresponds to the probability of breaking $\mathcal{IS}$ for an adversary running in time $O(t)$. We can see already the term $q_{\mathcal{H}}^2$ accounting for the non-tightness of this reduction.

There is another source of non-tightness: we often require a bound in terms of the quantum advantage for *special soundness* and not computational soundness. An adversary that breaks the 2-special soundness property is able to construct 2 valid triplets (x, c, z) and (x, c', z') with $c \neq c'$[6](the first message x is the same for both triplets). This can be generalized to γ-special soundness where

[5]The message actually just consists of (x, z) since $\mathcal{H}(x)$ can be constructed from x.

[6]In the asymptotic case, 2-special soundness is often defined with an efficient extractor that takes a pair of triplets and outputs a valid secret key. The current definition is similar in spirit and uses an advantage notion which is more adapted for concrete security bounds.

we require an adversary to create γ valid triplets $(x, c_1, z_1), \ldots, (x, c_\gamma, z_\gamma)$ where the challenges c_i are pairwise distinct. One can relate computational soundness advantage with γ-special soundness advantage but this comes with another big loss in tightness. For example, the authors of [DFMS19] use roughly[7] the following bound:

$$QADV_{\mathcal{IS}}(t) \leq \left[QADV_{\mathcal{IS}}^{\gamma\text{-}sp}(O(t))\right]^{\frac{1}{2\gamma-1}} \tag{2}$$

which, when combined to Equation 1, gives the bound

$$QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}]}(t, q_{\mathcal{H}}) \leq q_{\mathcal{H}}^2 \cdot \left[QADV_{\mathcal{IS}}^{\gamma\text{-}sp}(O(t))\right]^{\frac{1}{2\gamma-1}}. \tag{3}$$

We can see that already with $\gamma = 2$, we have a cubic loss in the exponent because we use special soundness and we lose a power 5 when requiring 3-special soundness, which are the 2 most common cases. In conclusion, while these asymptotic results, as well as those in [LZ19], are extremely important for having post-quantum trust in the Fiat-Shamir transform for identification schemes, the amount of non-tightness is significantly too large to make concrete security claims with decent parameters.

Overview of our results

Our results will remove this non-tightness for an important class of identification schemes, namely commit-and-open identification schemes. In a commit-and-open identification scheme, the prover can extract a string $z = z_1, \ldots, z_n$ from the secret key sk. His first message $x = G(z_1), \ldots, G(z_n)$ consists of committing to all the values z_i with a commitment function G and then in the second message, he reveals a subset of the z_i depending on the challenge c. Several schemes, such as Stern's identification scheme, the Picnic identification scheme and the SSH identification scheme that inspired the MQDSS signature are of this form. They are all even more particular: they consist of a parallel repetition of a commit-and-open identification scheme $\mathcal{IS}$ with challenge size 3 and the advantage of the underlying post-quantum computational assumption is equal to $QADV_{\mathcal{IS}}^{3\text{-}sp}(t)$. Our first theorem deals specifically with the parallel repetition case.

Theorem 1 (Simplified)**.** *Let $\mathcal{IS}$ be a commit-and-open identification scheme that uses a commitment G modeled as a random function. Let $\gamma \geq 2$ be an integer. For any $t, q_{\mathcal{H}}, q_G$, and number of repetition r, we have*

$$QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}^{\otimes r}]}(t, q_{\mathcal{H}}, q_G) \leq QADV_{\mathcal{IS}}^{\gamma\text{-}sp}\left(O(t)\right) + O\left(\frac{q_{\mathcal{H}}^2(\gamma-1)^r}{|C|^r}\right) + O\left(\frac{q_G^3}{|M|}\right)$$

where $|C|$ is the size of the challenge space and $|M|$ is the size of the space of each $x_i = G(z_i)$.

Here, the left hand side is the probability (*i.e.* advantage) that a quantum adversary has of breaking the Fiat-Shamir transform of $\mathcal{IS}^{\otimes r}$, the r-fold parallel repetition of $\mathcal{IS}$. The adversary is running in time t and performs $q_{\mathcal{H}}$ quantum queries to the hash function used in the Fiat-Shamir transform and q_G quantum queries to the commitment function G. We also use the QROM and model G as a truly random function.

[7]The bound is actually slightly worst as Theorem 25 of [DFMS19] (in the eprint version) generalizes Lemma 7 of [Unr12] while it should generalize Lemma 8 in order to account for the fact that the challenges have to be pairwise distinct. The difference is however only minimal and doesn't change the asymptotic behavior, even though it may add some small dependence in the size of the challenge space.

These terms on the right hand side are all necessary. The first term is supposed to be related to the hardness of the computational problem. The term $O\left(\frac{q_{\mathcal{H}}^2(\gamma-1)^r}{|C|^r}\right)$ corresponds to applying Grover's algorithm on the challenge space. This attack appears for example in schemes that have 3-special soundness but where an adversary can easily construct an x for which he can successfully answer 2 of the 3 verifier's challenges. This is also the attack that was presented in [DFM20] with $\gamma = 2$. So indeed, the $q_{\mathcal{H}}^2$ might be necessary but only for the part of advantage related to the challenge attack and crucially, the $O(q_{\mathcal{H}}^2)$ factor loss in [DFMS19] isn't tight in front of the advantage to break the computational problem. What we describe here is also true for the example presented in [DFM20] so their tightness result of the $O(q^2)$ loss factor is much less harmful that what it seems even for schemes where it holds. The third term is also necessary corresponds to attacking the commitment function and breaking the binding property by finding collisions on G. An interesting remark about this theorem is that designers already implicitly used results very similar to Theorem 2 but without a formal proof and used it to determine the value of r[8].

What we omitted in the description of Theorem 1 is that the $O(t)$ hides some additive terms that depend on $|C|$ so they are well suited for parallel repetition of schemes with small challenge but are not suited when these are exponential. To circumvent this, we also generalize the above theorem when we don't have parallel repetition but just a single identification scheme with potentially a large challenge space. We prove the following

Theorem 2 (Simplified)**.** *Let $\gamma \geq 2$ be an integer and let $\mathcal{IS}$ be a commit-and-open identification scheme with a commitment function G modeled as a random function. We have for any running time t and number of queries $q_{\mathcal{H}}, q_G$*

$$QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}]}(t, q_{\mathcal{H}}, q_G) \leq QADV_{\mathcal{IS}}^{\gamma\text{-}osp}(O(t)) + O\left(\frac{q_{\mathcal{H}}^2\gamma}{|C|}\right) + O\left(\frac{q_G^3}{|M|}\right).$$

Here, the $O(\cdot)$ terms do not depend on $|C|$ anymore. This theorem is very similar to Theorem 1 but the reduction is to a weaker notion of special soundness, namely output special soundness (hence the γ-*osp* in the theorem) that we will discuss more in detail in the paper. Informally, we want again the adversary to produce γ valid triplets (x, c_i, z_i) except that he doesn't need to know what are the challenges c_i that correspond to the z_i. The identification schemes we study all can use Theorem 1 but it would be interesting to see if some other schemes could use Theorem 2.

Finally, an important conceptual step of our results is to relate the quantum Fiat-Shamir advantage for any identification scheme (so not necessarily commit and open) to the notion of γ-rigid soundness. This notion can be seen as a computational-statistical notion of soundness meaning that the adversary is computationally bounded when producing the first message x but unbounded when producing the response z (that depends on pk, x, and the challenge c). Informally, an adversary breaks the γ-rigid soundness property if he can construct x such that he will be able to answer in a valid way at least γ different challenges (he is unbounded for this second message). We prove the following

[8]For example, the PICNIC scheme is of the form $\mathcal{IS}^{\otimes r}$ and we have 3-special soundness for $\mathcal{IS}$ (so we pick $\gamma = 3$) and $|C| = 3$. If we want 64 bits of quantum security (so $q_{\mathcal{H}} = 2^{64}$), we want from the challenge attack $\frac{q_{\mathcal{H}}^2 2^r}{3^r} \leq 1$ (omitting the $O(\cdot)$) which implies $r \geq 219$. If we want 128 bits of quantum security, this r has to be doubled. This corresponds exactly to the number of repetitions of the PICNIC scheme respectively for levels 1 and 5 of the NIST security levels.

Proposition 1. *For any integer $\gamma \geq 2$, time t, number of queries $q_{\mathcal{H}}$, and identification scheme $\mathcal{IS}$, we have*

$$QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}]}(t, q_{\mathcal{H}}) \leq QADV^{\gamma\text{-}rs}_{\mathcal{IS}}(t, q_{\mathcal{H}}) + O(\frac{q_{\mathcal{H}}^2 \gamma}{|C|}).$$

This proposition can be seen as a generalization of Unruh's reduction from the quantum advantage of the Fiat-Shamir transform to statistical soundness. The fact that we impose a γ threshold here in our rigid soundness definition makes it easier to related to γ-special soundness without any losses in tightness. We use this proposition for commit-and-open identification schemes but it could have more applications.

Techniques used

How to we achieve our results? The most common ways of proving the quantum security of the Fiat-Shamir transform use techniques such as quantum rewinding or quantum reprogramming. These techniques are very general but introduce some non-tightness that we want to avoid so we have to manage without them. Our starting point is to use Unruh's result on the quantum security of the Fiat-Shamir transform when the underlying identification scheme has statistical soundness. In this case, things are fairly easy and we can invoke quantum lower bounds on the search problem to conclude. As we wrote above, we first introduce the notion of γ-rigid soundness to achieve Proposition 1 that holds for any identification scheme.

We then look more precisely at commit-and-open identification schemes, where during the first message, the prover commits to some values $x = G(z_1), \ldots, G(z_n)$ where G is the commitment function and reveals a subset of those z_i as his second message. We first show that we can replace this function G with a random permutation σ [9]. This comes from the fact that the actual values of $G(z_1), \ldots, G(z_n)$ are used only for computing the challenge $c = \mathcal{H}(G(z_1), \ldots, G(z_n))$. Since $\mathcal{H}$ is also random, we show that this change of G doesn't change the quantum advantage, on average on $\mathcal{H}$.

However, because we want tight results, we are far from done. We can't use generic relations from computational soundness to γ-special soundness (like the one in Equation 2). We need to directly reduce to γ-special soundness without going through computational soundness. To do so, we need from the string $\sigma(z_1), \ldots, \sigma(z_n)$ to be able to recover the whole string $z = z_1, \ldots, z_n$. However, we only have black box access to σ and we don't have access to a inversion oracle. The idea we use to do this is to replace σ with a pseudorandom permutation $\widetilde{\pi}_0$ which doesn't change the security claim but which is easily invertible. From there, we can tightly relate the Fiat-Shamir advantage to a γ-special soundness advantage. How do we construct this function $\widetilde{\pi}_0$? We use recent results on the quantum security of Feistel networks from [HI19]. This result shows how to construct quantum secure random permutations from random functions with black box access. These Feistel networks also have the property that they are easily computable *and invertible*, even when the underlying random function is hard for the preimage finding problem. We use as the underlying pseudorandom function the SHAKE-256 function, which is quantum-secure [CHS19].

Putting this all together, we can relate the quantum Fiat-Shamir to special soundness notions. In order to use the security of the Feistel networks, we have to artificially increase the size of the input space of the commitment scheme and we also replaced the random function G with the function $\widetilde{\pi}_0$. So how we can conclude about special soundness for the original scheme. For

[9] We note here that this replacement is just part of a proof technique. We prove the security of identification schemes for random commitment schemes which are not permutations.

Theorem 2, this is immediate as our transformations do not change the γ-output special soundness advantage. However, this is not true for γ-special soundness. For Theorem 1, we actually reduce to a stronger variant of γ-special soundness which is also invariant under our transformations which immediately implies Theorem 1.

We now dive in the more formal part of this paper.

3 Preliminaries

Basic notations. For an integer $N \in \mathbb{N}^*$, we denote by $[N]$ the set $\{1, \ldots, N\}$. For a (usually probabilistic) algorithm $\mathrm{A}(\cdot)$, $x \leftarrow \mathrm{A}(\cdot)$ means that we run $\mathrm{A}(\cdot)$ with some fresh randomness and get some output x. We will sometimes also use the notation $\mathrm{A}(\cdot) \to x$. We will also use the notation $x \leftarrow D$ when D is a distribution when we sample x from D. For a set S, the notation $x \xleftarrow{\$} S$ means that x is chosen uniformly at random from the set S. Let $\mathcal{F}_Y^X$ be the set of functions from X to Y and let $\mathcal{P}^X$ be the set of permutations acting on X. The notation $\stackrel{\triangle}{=}$ designs an equality which is a definition.

3.1 Quantum query algorithms.

In this work, we will often work with query algorithms that have a black box access to some deterministic function f. A classical access to f means that we can perform queries that on input x outputs $f(x)$. A quantum access to f means that we can perform the unitary U_f in a black box manner, where

$$U_f : |x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle.$$

A quantum query algorithm with classical access to f will be denoted $\mathscr{A}^f$ and a quantum query algorithm with quantum access to f will be denoted $\mathscr{A}^{|f\rangle}$. For any quantum algorithm $\mathscr{A}$, we denote by $|\mathscr{A}|$ it's total running time. We write $|\mathscr{A}^{|f\rangle}| = (t, q_f)$ when $\mathscr{A}^{|f\rangle}$ runs in time t and performs q_f quantum queries to f. We can also write $|\mathscr{A}^{|f\rangle}| = (*, q_f)$ to specify only the number of queries but not the running time. Unless stated otherwise, black box calls to f or U_f are efficient and we fix the running time of a query to be equal to 1.

In the notation $\mathscr{A}^{|f\rangle}$, the behavior of the query algorithm is described by $\mathscr{A}$ and the superscript $|f\rangle$ only indicates which function is queried. This means that the algorithm $\mathscr{A}^{|g\rangle}$ behaves exactly as $\mathscr{A}^{|f\rangle}$ where calls to U_f are replaced with calls to U_g. We can also write $\mathscr{A}$ for a quantum query algorithm where the queried function is not specified.

A query algorithm can perform queries to different functions. For example $\mathscr{A}^{|f\rangle,|g\rangle,|h\rangle}$ has a black box access to the 3 unitaries U_f, U_g, U_h. We write $|\mathscr{A}^{|f\rangle,|g\rangle,|h\rangle}| = (t, q_f, q_g, q_h)$ to denote the fact that $\mathscr{A}^{|f\rangle,|g\rangle,|h\rangle}$ runs in time t, performs q_f queries to U_f, q_g queries to U_g and q_h queries to U_h. Finally, we define the q-query quantum variational distance between 2 distributions D_1, D_2 on functions as

$$\Delta_q(D_1, D_2) \stackrel{\triangle}{=} \max_{\mathscr{A}:|\mathscr{A}|=(*,q)} \left| \Pr_{f \leftarrow D_1}[\mathscr{A}^{|f\rangle}(\cdot) \text{ outputs } 0] - \Pr_{g \leftarrow D_2}[\mathscr{A}^{|g\rangle}(\cdot) \text{ outputs } 0] \right|.$$

3.2 Hash functions and Feistel networks

SHAKE-256. In this work, we will need a quantum secure hash function. We use SHAKE-256 which is a SHA-3 variant [BDPV11] that uses the sponge construction with variable input and

output sizes. We write SHAKE-256$_{X,Y}$ to explicit the input space X and output space Y. The sponge construction is known to be quantum secure [CHS19] and it is standard in the QROM to model SHAKE-256$_{X,Y}$ with a random function in $\mathcal{F}_Y^X$ for which we only have black box access.

Feistel networks. Feistel networks are a generic way to transform pseudorandom functions in pseudorandom permutations. They were first studied by Luby and Rackoff [LR88], and we know well their classical security. Recently, the quantum security was proven for 4 round Feistel networks. Very briefly, the 4 round Feistel network starts with a function $f \in \mathcal{F}_{\{0,1\}^n}^{\{0,1\}^n}$ and constructs a permutation $\mathfrak{Fe}_4(f) \in \mathcal{P}^{\{0,1\}^{2n}}$. $\mathfrak{Fe}_4(f)$ uses 4 black box calls to f and both $\mathfrak{Fe}_4(f)$ and $\mathfrak{Fe}_4(f)^{-1}$ are efficiently computable if we know how to efficiently compute f (but not necessarily f^{-1}). The quantum security of $\mathfrak{Fe}_4$ was recently proven in [HI19]:

Proposition 2 ([HI19])**.** *Let D_1 be the distribution sampled as follows: $f \xleftarrow{\$} \mathcal{F}_{\{0,1\}^n}^{\{0,1\}^n}$, return $\mathfrak{Fe}_4(f)$. We have $\Delta_q(D_1, \mathcal{P}^{\{0,1\}^{2n}}) \leq O(\sqrt{\frac{q^6}{2^n}})$.*

3.3 The (quantum) random oracle model

Suppose in a cryptographic scheme, we use a hash function $\mathcal{H} : \{0,1\}^n \to \{0,1\}^m$ which is fully specified, for example SHAKE-256. In the random oracle model (ROM), we make the following assumption: the function $\mathcal{H}$ can be modeled as a random function from $\{0,1\}^n$ to $\{0,1\}^m$ to which we only have a black box access. In the quantum random oracle model (QROM), we allow a quantum black box access to the function $\mathcal{H}$, meaning that we give access to the unitary

$$U_{\mathcal{H}} : |x\rangle|y\rangle \to |x\rangle|y \oplus \mathcal{H}(x)\rangle.$$

3.4 Quantum lower bounds

We will use a generalization of Grover's lower bound for the search problem.

Lemma 1. *Let X and Y be respectively an input set and an output set. For each $x \in X$, we associate a set $U_x \subseteq Y$ such that $\frac{|U_x|}{|Y|} \leq \varepsilon$. For any quantum query algorithm $\mathscr{A}$ with $|\mathscr{A}| = (*, q)$, we have*

$$\Pr[\mathcal{H}(x) \in U_x : \mathcal{H} \xleftarrow{\$} \mathcal{F}_Y^X, x \leftarrow \mathscr{A}^{|\mathcal{H}\rangle}(\cdot)] \leq O(q^2\varepsilon).$$

The above lemma was implicitly stated and proven in [Unr17, Theorem21]. Another lower bound that we will use is Zhandry's quantum lower bound on distinguishing a random permutation from a random function with small range [Zha15]. We fix a set X, an integer r such that $[r] \subseteq X$, and define the following distribution DSF_r^X on functions in $\mathcal{F}_X^X$, which can be sampled as follows:

- Draw a random function $g \xleftarrow{\$} \mathcal{F}_{[r]}^X$.
- Draw a random injective function h from $[r]$ to X.
- Output $h \circ g$.

Notice that since we imposed $[r] \subseteq X$, we can consider g as an element of $\mathcal{F}_X^X$ and choose for h a random permutation in $\mathcal{P}^X$ which will lead to the same distribution. Also, we can replace $[r]$ with any other set $Y \subseteq X$ with $|Y| = r$. Zhandry's lower bound can be stated as follows:

Proposition 3 ([Zha15])**.** $\Delta_q(DSF_r^X, \mathcal{P}^X) \leq O(\frac{q^3}{r})$.

4 Identification schemes

4.1 First definitions

An identification scheme $\mathcal{IS} = (K_{\mathcal{IS}}, P_{\mathcal{IS}}, V_{\mathcal{IS}}; M, C, R)$, consists of the following:

- A key generation algorithm $K_{\mathcal{IS}}(1^\lambda) \to (pk, sk)$.
- The prover's algorithm $P_{\mathcal{IS}} = (P_1, P_2)$ for constructing his messages. We have $P_1(sk) \to (x, St)$ where $x \in M$ corresponds to the first message and St is some internal state. $P_2(sk, x, c, St) \to z$ where $c \in C$ is the challenge from the verifier and $z \in R$ the prover's response (second message).
- A verification function $V_{\mathcal{IS}}(pk, x, c, z)$ used by the verifier that outputs a bit, 0 corresponds to 'Reject' and 1 to 'Accept'.

Notice that we specify in the description of $\mathcal{IS}$ the sets M, C, R corresponding respectively to the first message space, the challenge space and the second message (*i.e.* response) space. All the different algorithms presented above are efficient and we will usually omit their running times (*i.e.* fix them to 1), in order to reduce the amount of notations we introduce. Even though we deal with concrete security parameters in this paper, we keep the notation $K_{\mathcal{IS}}(1^\lambda)$ with a unary representation of a security parameter λ to remind this implicit efficiency requirement.
We present below more precisely the different steps of an identification scheme.

Identification scheme $\mathcal{IS} = (K_{\mathcal{IS}}, P_{\mathcal{IS}} = (P_1, P_2), V_{\mathcal{IS}}; M, C, R)$

Initialization. $(pk, sk) \leftarrow K_{\mathcal{IS}}(1^\lambda)$. The prover has (pk, sk) and the verifier pk.
Interaction.

1. The prover generates $(x, St) \leftarrow P_1(sk)$ and sends $x \in M$ to the verifier.
2. The verifier picks $c \xleftarrow{\$} C$ and sends c to the prover.
3. The prover generates $z \leftarrow P_2(sk, x, c, St)$ and sends $z \in R$ to the verifier.

Verification. The verifier accepts iff. $V_{\mathcal{IS}}(pk, x, c, z) = 1$.

We denote by $\mathcal{IS}^{\otimes r}$ the r-fold parallel repetition of $\mathcal{IS}$, which consists of the following

Identification scheme $\mathcal{IS}^{\otimes r}$ when $\mathcal{IS} = (K_{\mathcal{IS}}, P_{\mathcal{IS}} = (P_1, P_2), V_{\mathcal{IS}}; M, C, R)$

Initialization. $(pk, sk) \leftarrow K_{\mathcal{IS}}(1^\lambda)$. The prover P has (pk, sk) and the verifier V has pk.
Interaction.

1. P generates $(x^1, St^1), \ldots, (x^r, St^r)$ where for each $i \in [r]$, he generates $(x^i, St^i) \leftarrow P_1(sk)$. He then sends $x = x^1, \ldots, x^r$ to V.
2. V picks a random $c = c^1, \ldots, c^r$ where each $c^i \xleftarrow{\$} C$ and sends c to P.
3. P generates $z = (z^1, \ldots, z^r)$ where for each $i \in [r]$, $z^i \leftarrow P_2(sk, x^i, c^i, St^i)$ and sends z to V.

Verification. The verifier V accepts iff. $\forall i \in [r], V_{\mathcal{IS}}(pk, x^i, c^i, z^i) = 1$.

Now, let's present the properties we want an identification scheme to verify. The first property we want from an identification scheme is that the verifier accepts if a prover runs the scheme honestly.

Definition 1 (Completeness)**.** *An identification scheme $\mathcal{IS} = (K_{\mathcal{IS}}, P_{\mathcal{IS}} = (P_1, P_2), V_{\mathcal{IS}}; M, C, R)$ has perfect completeness if*

$$\Pr\left[V_{\mathcal{IS}}(pk, x, c, z) = 1 \;\middle|\; \begin{matrix} (pk,sk)\leftarrow K_{\mathcal{IS}}(1^\lambda) \\ (x,St)\leftarrow P_1(sk) \\ c\xleftarrow{\$} C \\ z\leftarrow P_2(sk,x,c,St)=1 \end{matrix}\right] = 1.$$

We only consider here perfect completeness but almost perfect completeness where the probability above is very close to 1 could also be used.

The second property we want is honest-verifier zero-knowledge, meaning that an honest verifier cannot extract any information (in particular about the secret key sk), from its interaction with an honest prover.

Definition 2 (HVZK)**.** *An identification scheme $\mathcal{IS} = (K_{\mathcal{IS}}, P_{\mathcal{IS}}, V_{\mathcal{IS}}; M, C, R)$ is ε-HVZK if there exists an efficient simulator Sim such that the 2 distributions D_1 and D_2 sampled as follows:*

- $D_1 : (pk, sk) \leftarrow K_{\mathcal{IS}}(1^\lambda),\ (x, St) \leftarrow P_1(sk), c \xleftarrow{\$} C, z \leftarrow P_2(sk, x, c, St)$, *return* (x, c, z),
- $D_2 : (pk, sk) \leftarrow K_{\mathcal{IS}}(1^\lambda),\ (x', c', z') \leftarrow Sim(pk, 1^\lambda)$, *return* (x', c', z'),

have statistical distance[10] *at most ε.*

Finally, the third property that we require is soundness. We don't want an efficient cheating prover that doesn't know the secret key sk to make the verifier accept. There are different notions of soundness and the interplay between them will play an important role in our proofs.

Different flavors of soundness. We provide here notions of soundness in terms of advantage, which are well suited when dealing with concrete security bounds. We first define the notion of (computational) soundness advantage for a quantum cheating adversary $\mathscr{A}$.

[10]The statistical distance between 2 distributions is defined as $\Delta(D_1, D_2) \triangleq \frac{1}{2} \sum_y |\Pr_{x\leftarrow D_1}[x = y] - \Pr_{x\leftarrow D_2}[x = y]|$.

Definition 3 (Quantum soundness advantage)**.** *Let $\mathcal{IS} = (K_{\mathcal{IS}}, P_{\mathcal{IS}}, V_{\mathcal{IS}}; M, C, R)$ be an identification scheme. For any quantum algorithm (a quantum cheating prover) $\mathscr{A} = (\mathscr{A}_1, \mathscr{A}_2)$, we define*

$$QADV_{\mathcal{IS}}(\mathscr{A}) \stackrel{\triangle}{=} \Pr\left[V_{\mathcal{IS}}(pk, x, c, z) = 1 \,\middle|\, \begin{smallmatrix}(pk,sk)\leftarrow K_{\mathcal{IS}}(1^\lambda)\\ (x,St)\leftarrow \mathscr{A}_1(pk)\\ c\xleftarrow{\$} C\\ z\leftarrow \mathscr{A}_2(pk,x,c,St)\end{smallmatrix}\right]$$

and $QADV_{\mathcal{IS}}(t) \stackrel{\triangle}{=} \max_{\substack{\mathscr{A}=(\mathscr{A}_1,\mathscr{A}_2),\\ |\mathscr{A}_1|+|\mathscr{A}_2|=t}} (QADV_{\mathcal{IS}}(\mathscr{A}))$.

In the context of identification schemes, we define the quantum 2-special soundness advantage as follows

Definition 4. *Let $\mathcal{IS} = (K_{\mathcal{IS}}, P_{\mathcal{IS}}, V_{\mathcal{IS}}; M, C, R)$ be an identification scheme. For any quantum algorithm $\mathscr{A}$, we define*

$$QADV^{2\text{-}sp}_{\mathcal{IS}}(\mathscr{A}) \stackrel{\triangle}{=} \Pr\left[V_{\mathcal{IS}}(pk, x, c, z) = 1 \wedge V_{\mathcal{IS}}(pk, x, c', z') = 1 \wedge c \neq c' \,\middle|\, \begin{smallmatrix}(pk,sk)\leftarrow K_{\mathcal{IS}}(1^\lambda)\\ (x,c,z,c',z')\leftarrow \mathscr{A}(pk)\end{smallmatrix}\right]$$

and $QADV^{2\text{-}sp}_{\mathcal{IS}}(t) \stackrel{\triangle}{=} \max_{\mathscr{A}:|\mathscr{A}|=t} \left(QADV^{2\text{-}sp}_{\mathcal{IS}}(\mathscr{A})\right)$.

A small 2-special soundness advantage means that it is hard for a quantum adversary to construct 2 valid transcripts (x, c, z) and (x, c', z') with $c \neq c'$. This notion can be extended to γ-special soundness, where we require more than 2 transcripts.

Definition 5. *Let $\mathcal{IS} = (K_{\mathcal{IS}}, P_{\mathcal{IS}}, V_{\mathcal{IS}}; M, C, R)$ be an identification scheme. For any quantum algorithm $\mathscr{A}$, we define*

$$QADV^{\gamma\text{-}sp}_{\mathcal{IS}}(\mathscr{A}) = \Pr\Big[\forall j \in [\gamma],\ V_{\mathcal{IS}}(pk, x, c_j, z_j) \stackrel{\triangle}{=} 1 \wedge (c_1, \ldots, c_\gamma \text{ are pairwise distinct}) \,\Big|\, \begin{smallmatrix}(pk,sk)\leftarrow K_{\mathcal{IS}}(1^\lambda)\\ (x,c_1,\ldots,c_\gamma,z_1,\ldots,z_\gamma)\leftarrow \mathscr{A}(pk)\end{smallmatrix}\Big]$$

and $QADV^{\gamma\text{-}sp}_{\mathcal{IS}}(t) \stackrel{\triangle}{=} \max_{\mathscr{A}:|\mathscr{A}|=t} \left(QADV^{\gamma\text{-}sp}_{\mathcal{IS}}(\mathscr{A})\right)$.

4.2 The Fiat-Shamir transform for identification schemes

The Fiat-Shamir transform [FS86] is a major cryptographic construction that converts any Σ-protocol, in our case any identification scheme into an non-interactive protocol. The idea is to use a hash function $\mathcal{H} : M \to C$, and to replace the verifier's challenge $c \in C$ by the string $\mathcal{H}(x)$ where x is the prover's first message. Since the prover can compute $\mathcal{H}(x)$ himself, there is no need for interaction anymore. For any identification scheme $\mathcal{IS}$, we denote by $\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}]$ its Fiat-Shamir transform, for a fixed function $\mathcal{H}$.

Running $\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}]$ for an identification scheme $\mathcal{IS} = (K_{\mathcal{IS}}, P_{\mathcal{IS}}, V_{\mathcal{IS}}; M, C, R)$

Initialization. $(pk, sk) \leftarrow K_{\mathcal{IS}}(1^\lambda)$. The prover P has (pk, sk) and the verifier V has pk.
One-way communication. P generates $(x, St) \leftarrow P_1(sk)$, computes $c = \mathcal{H}(x)$ and generates $z \leftarrow P_2(sk, x, c, St)$. He sends the pair (x, z) to the verifier.
Verification. The verifier accepts iff. $V_{\mathcal{IS}}(pk, x, \mathcal{H}(x), z) = 1$.

The Fiat-Shamir transform is very useful as it can be used (among other things) to construct signature schemes from identification schemes. The quantum Fiat-Shamir advantage for $\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}]$ is defined as follows:

Definition 6. *Let $\mathcal{IS} = (K_{\mathcal{IS}}, P_{\mathcal{IS}}, V_{\mathcal{IS}}; M, C, R)$ be an identification scheme and $\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}]$ its Fiat-Shamir transform. Let $\mathscr{A}$ be a quantum query algorithm. We define*

$$QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}]}(\mathscr{A}^{|\mathcal{H}\rangle}) \triangleq \Pr\left[V(x, \mathcal{H}(x), z) = 1 \,\middle|\, \begin{smallmatrix}(pk,sk)\leftarrow K_{\mathcal{IS}}(1^\lambda)\\ (x,z)\leftarrow \mathscr{A}^{|\mathcal{H}\rangle}(pk)\end{smallmatrix}\right]$$

and $QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}]}(t, q_{\mathcal{H}}) \triangleq \max_{\mathscr{A}:|\mathscr{A}|=(t,q_{\mathcal{H}})} \left(QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}]}(\mathscr{A}^{|\mathcal{H}\rangle})\right)$.

In the QROM, this function $\mathcal{H}$ is modeled as a random function to which we only have black box access. In this model, the quantum Fiat-Shamir advantage that we are interested in is

$$\mathbb{E}_{\mathcal{H}\xleftarrow{\$}\mathcal{F}_C^M}\left(QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}]}(\mathscr{A}^{|\mathcal{H}\rangle})\right).$$

4.3 Signature schemes

All our technical work is on identification scheme but the finality is to prove the security of signature schemes. We discuss signature schemes and how the security of identification schemes implies the security of signature schemes in Appendix A.

4.4 Relating the quantum Fiat-Shamir security to rigid soundness

In this section, we introduce the notion of rigid soundness and to relate the quantum Fiat-Shamir security of any identification scheme to this notion. Throughout this section, we fix an identification scheme $\mathcal{IS} = (K_{\mathcal{IS}}, P_{\mathcal{IS}}, V_{\mathcal{IS}}; M, C, R)$. We first define the set $VC_x^{\mathcal{IS}}$ of valid challenges for $x \in M$ as well as the set $VC_{\geq\gamma}^{\mathcal{IS}}$ of elements having at least γ valid challenges for any $\gamma \in \mathbb{N}$:

$$VC_x^{\mathcal{IS}} \triangleq \{c \in C : \exists z \in R, V_{\mathcal{IS}}(pk, x, c, z) = 1\} \quad ; \quad VC_{\geq\gamma}^{\mathcal{IS}} \triangleq \{x \in M : |VC_x^{\mathcal{IS}}| \geq \gamma\}.$$

We can now define the quantum γ-rigid soundness advantage for a quantum algorithm $\mathscr{A}$ as follows:

Definition 7 (Quantum γ-rigid soundness advantage)**.**

$$QADV^{\gamma\text{-}rs}_{\mathcal{IS}}(\mathscr{A}) \triangleq \Pr\left[x \in VC^{\mathcal{IS}}_{\gamma} \;\middle|\; \begin{smallmatrix}(pk,sk)\leftarrow K_{\mathcal{IS}}(1^\lambda)\\ x\leftarrow\mathscr{A}(pk)\end{smallmatrix}\right] \;;\; QADV^{\gamma\text{-}rs}_{\mathcal{IS}}(t) \triangleq \max_{\mathscr{A}:|\mathscr{A}|=t} QADV^{\gamma\text{-}rs}_{\mathcal{IS}}(\mathscr{A}).$$

We now relate the security of the Fiat-Shamir transform to a rigid soundness advantage.

Proposition 4. *For any query algorithm $\mathscr{A}^{|\mathcal{H}\rangle}$ with $|\mathscr{A}^{|\mathcal{H}\rangle}| = (t, q_{\mathcal{H}})$, for any integer $\gamma \geq 2$, we have*

$$\mathbb{E}_{\mathcal{H}\leftarrow\mathcal{F}^M_C}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}]}(\mathscr{A}^{|\mathcal{H}\rangle})\right] \leq QADV^{\gamma\text{-}rs}_{\mathcal{IS}}(t, q_{\mathcal{H}}) + O(\frac{q^2_{\mathcal{H}}\gamma}{|C|}).$$

Proof. Fix a query algorithm $\mathscr{A}^{|\mathcal{H}\rangle}$ with $|\mathscr{A}^{|\mathcal{H}\rangle}| = (t, q_{\mathcal{H}})$ and an integer $\gamma \geq 2$.

$$\mathbb{E}_{\mathcal{H}\leftarrow\mathcal{F}^M_C}[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}]}(\mathscr{A}^{|\mathcal{H}\rangle})] = \Pr_{\mathcal{H}\leftarrow\mathcal{F}^M_C}\left[V_{\mathcal{IS}}(pk,x,\mathcal{H}(x),z)=1 \;\middle|\; \begin{smallmatrix}(pk,sk)\leftarrow K_{\mathcal{IS}}(1^\lambda)\\ (x,z)\leftarrow\mathscr{A}^{|\mathcal{H}\rangle}(pk)\end{smallmatrix}\right] = P_1 + P_2 \quad (4)$$

$$\begin{aligned}\text{with}\quad P_1 &\triangleq \Pr_{\mathcal{H}\leftarrow\mathcal{F}^M_C}\left[V_{\mathcal{IS}}(pk,x,\mathcal{H}(x),z)=1 \wedge (x\in VC^{\mathcal{IS}}_{\geq\gamma}) \;\middle|\; \begin{smallmatrix}(pk,sk)\leftarrow K_{\mathcal{IS}}(1^\lambda)\\ (x,z)\leftarrow\mathscr{A}^{|\mathcal{H}\rangle}(pk)\end{smallmatrix}\right]\\ P_2 &\triangleq \Pr_{\mathcal{H}\leftarrow\mathcal{F}^M_C}\left[V_{\mathcal{IS}}(pk,x,\mathcal{H}(x),z)=1 \wedge (x\notin VC^{\mathcal{IS}}_{\geq\gamma}) \;\middle|\; \begin{smallmatrix}(pk,sk)\leftarrow K_{\mathcal{IS}}(1^\lambda)\\ (x,z)\leftarrow\mathscr{A}^{|\mathcal{H}\rangle}(pk)\end{smallmatrix}\right].\end{aligned}$$

$\mathscr{A}^{|\mathcal{H}\rangle}$ runs in time t so the probability that it outputs $x \in VC^{\mathcal{IS}}_{\geq\gamma}$ is upper bounded by $QADV^{\gamma\text{-}rs}_{\mathcal{IS}}(t)$ hence $P_1 \leq QADV^{\gamma\text{-}rs}_{\mathcal{IS}}(t)$. If $x \notin VC^{\mathcal{IS}}_{\geq\gamma}$ then $|VC^{\mathcal{IS}}_x| \leq \gamma - 1$. Moreover, if $V_{\mathcal{IS}}(pk,x,\mathcal{H}(x),z) = 1$ then $\mathcal{H}(x) \in VC^{\mathcal{IS}}_x$. Hence:

$$P_2 \leq \Pr_{\mathcal{H}\leftarrow\mathcal{F}^{M^n}_C}\left[\mathcal{H}(x)\in VC^{\mathcal{IS}}_x \wedge \left(|VC^{\mathcal{IS}}_x| \leq (\gamma-1)\right) \;\middle|\; \begin{smallmatrix}(pk,sk)\leftarrow K_{\mathcal{IS}}(1^\lambda)\\ (x,z)\leftarrow\mathscr{A}^{|\mathcal{H}\rangle}(pk)\end{smallmatrix}\right].$$

We can directly use Lemma 1 with $U_x = |VC^{\mathcal{IS}}_x|$ and the fact that $\mathscr{A}^{|\mathcal{H}\rangle}$ perform $q_{\mathcal{H}}$ queries to $|\mathcal{H}\rangle$ to obtain $P_2 \leq O(\frac{q^2_{\mathcal{H}}(\gamma-1)}{|C|}) = O(\frac{q^2_{\mathcal{H}}\gamma}{|C|})$. Putting the bounds on P_1 and P_2 in Equation 4, we obtain the desired result. □

This proposition can be seen as a generalization of Unruh's relation between the Fiat-Shamir security and a statistical soundness advantage, but we replace this statistical soundness with rigid soundness. While some schemes may naturally have the rigid soundness property, it is not a priori clear how to use Proposition 4. As we will see, this Proposition will be very useful when studying commit-and-open identification schemes, which we now define and discuss.

4.5 Commit and open identification schemes

A commit-and-open identification scheme is a specific kind of identification scheme where, for the first message, P commits to some values $z_1, \ldots, z_n$ using some function G and after the verifier's challenge, he reveals a subset of those values. More precisely, a commit-and-open identification scheme $\mathcal{IS} = (K_{\mathcal{IS}}, P_{\mathcal{IS}}, V_{\mathcal{IS}}, G; M, C, R, n)$ consists of the following

- A key generation algorithm $K_{\mathcal{IS}}(1^\lambda) \to (pk, sk)$.
- A function $G : R \to M$ that will act as a commitment scheme.

- The challenge set C where each $c \in C$ has a corresponding set $I_c \subseteq [n]$.
- The prover's algorithm $P_{\mathcal{IS}} = (P_1, P_2)$ for constructing his messages. We have $P_1(sk) \to (x, z)$ where $z = (z_1, \ldots, z_n)$ with each $z_i \in R$ and $x = x_1, \ldots, x_n = G(z_1), \ldots, G(z_n)$ with each $x_i \in M$. $P_2(z, c)$ outputs $z_{I_c} = \{z_i\}_{i \in I_c}$.
- A verification function $V_{\mathcal{IS}}(pk, c, z_{I_c})$. The verifier also checks that the commitments are valid, *i.e.* for each $i \in I_c$, $G(z_i) = x_i$.

Notice that we now denote by M the message space of individual commited values, so the Prover sends actually an element in M^n. Notice also that in the above verification function, we require $V_{\mathcal{IS}}$ to be independent of x, and we check the validity of the commitment separately. All the real identification schemes we will consider have this property.

Commit-and-open Identification scheme $\mathcal{IS} = (K_{\mathcal{IS}}, P_{\mathcal{IS}}, V_{\mathcal{IS}}, G; M, C, R, n)$

Initialization. $(pk, sk) \leftarrow K_{\mathcal{IS}}(1^\lambda)$. The prover has (pk, sk) and the verifier pk.
Interaction.

1. P generates $(z_1, \ldots, z_n, G(z_1), \ldots, G(z_n)) \leftarrow P_1(sk)$ and sends $x_1, \ldots, x_n = G(z_1), \ldots, G(z_n)$ to the verifier.
2. The verifier sends a random $c \xleftarrow{\$} C$ that corresponds to a subset $I_c \subseteq [n]$.
3. P sends z_{I_c} to the verifier.

Verification. The verifier accepts iff. $(\forall i \in I_c, G(z_i) = x_i) \wedge V_{\mathcal{IS}}(pk, c, z_{I_c}) = 1$.

The Quantum Random Oracle Model for commit-and-open identification schemes. As we described in section 4.2, we use the QROM to characterize the quantum security of the Fiat-Shamir transform of $\mathcal{IS}$ using the quantity

$$E_{\mathcal{H} \xleftarrow{\$} \mathcal{F}_C^{M^n}} \left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}]}(t, q_{\mathcal{H}}) \right].$$

We will use again the QROM for the commitment function, and model the function G as a random function in $\mathcal{F}_M^R$. We will write $\mathcal{IS}_G = (K_{\mathcal{IS}}, P_{\mathcal{IS}}, V_{\mathcal{IS}}, G; M, C, R, n)$ to specify the commitment function used in the subscript of $\mathcal{IS}$. The quantum Fiat-Shamir advantage therefore becomes

$$\mathbb{E}_{\substack{\mathcal{H} \xleftarrow{\$} \mathcal{F}_C^{M^n} \\ G \xleftarrow{\$} \mathcal{F}_M^R}} \left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_G]}(t, q_{\mathcal{H}}, q_G) \right],$$

where q_G is the number of queries to the unitary U_G.

For commit-and-open identification schemes, we define 2 variants of γ-special soundness. These variants have the nice property that they are independent of the commitment function used, which is not the case for special soundness. We first define output special soundness

Definition 8. *Let $\mathcal{IS}_G = (K_{\mathcal{IS}}, P_{\mathcal{IS}}, V_{\mathcal{IS}}, G; M, C, R, n)$ be a commit-and-open identification scheme. For any quantum query algorithm $\mathscr{A}$, we define*

$$QADV^{\gamma\text{-}osp}_{\mathcal{IS}_G}(\mathscr{A}) \triangleq \Pr[|\{c : V_{\mathcal{IS}}(pk, c, z_{I_c}) = 1\}| \geq \gamma : (pk, sk) \leftarrow K_{\mathcal{IS}}(1^\lambda), z \leftarrow \mathscr{A}(pk)\Big].$$

where $z = (z_1, \ldots, z_n)$. We also define $QADV^{\gamma\text{-}osp}_{\mathcal{IS}_G}(t) \triangleq \max_{\mathscr{A}:|\mathscr{A}|=t} \left(QADV^{\gamma\text{-}osp}_{\mathcal{IS}_G}(\mathscr{A})\right)$

The idea of output special soundness is that we can generate z (and $x = G(z_1, \ldots, z_n)$ such that there exist γ valid triplets $(x, c_1, z_{I_1}), \ldots, (x, c_\gamma, z_{I_\gamma})$ for pairwise distinct challenges $c_1, \ldots, c_\gamma$. However, the adversary here doesn't need to output these challenges. This notion is incomparable with γ-special soundness.

The second notion is the γ-special+ soundness which is the same as above but the adversary has to output the challenges.

Definition 9. *Let $\mathcal{IS}_G = (K_{\mathcal{IS}}, P_{\mathcal{IS}}, V_{\mathcal{IS}}, G; M, C, R, n)$ be a commit-and-open identification scheme. For any quantum query algorithm $\mathscr{A}$, we define*

$$QADV^{\gamma\text{-}sp+}_{\mathcal{IS}_G}(\mathscr{A}) \triangleq \Pr\Big[\Big(\forall i \in [\gamma], V_{\mathcal{IS}}(pk, c_i, z_{I_{c_i}}) = 1\Big) \wedge \text{ the } c_i \text{ are pairwise distinct } : (pk, sk) \leftarrow K_{\mathcal{IS}}(1^\lambda), (z, c_1, \ldots, c_\gamma) \leftarrow \mathscr{A}(pk)\Big].$$

where $z = (z_1, \ldots, z_n)$. We also define $QADV^{\gamma\text{-}sp+}_{\mathcal{IS}_G}(t) \triangleq \max_{\mathscr{A}:|\mathscr{A}|=t} \left(QADV^{\gamma\text{-}sp+}_{\mathcal{IS}_G}(\mathscr{A})\right)$

This definition is also independent of the commitment used in $\mathcal{IS}$. As the name suggests, this notion is stronger than γ-special soundness in the sense that $QADV^{\gamma\text{-}sp+}_{\mathcal{IS}_G}(t) \leq QADV^{\gamma\text{-}sp}_{\mathcal{IS}_G}(t)$. This comes from the from an adversary a generating $(z, c_1, \ldots, c_\gamma)$ that breaks the γ-special+ soundness property, we can construct explicitly γ valid triplets $(x, c_1, z_{I_1}), \ldots, (x, c_\gamma, z_{I_\gamma})$ with $x = (G(z_1), \ldots, G(z_n))$ and the challenges are pairwise distinct, which breaks the γ-special soundness property.

We are now ready to jump in the proofs of our theorems.

5 The quantum Fiat-Shamir security of commit-and-open identification schemes

5.1 Overview of our theorems and proof strategy

Our main theorems are the following:

Theorem 1. *Let $\mathcal{IS}_G = (K_{\mathcal{IS}}, P_{\mathcal{IS}}, V_{\mathcal{IS}}, G; M, C, R, n)$ be a commit-and-open identification scheme with $G \xleftarrow{\$} \mathcal{F}_M^R$. Let also $\gamma \geq 2$ be an integer. We have for any $t, q_{\mathcal{H}}, q_G$:*

$$\mathbb{E}_{\substack{\mathcal{H} \xleftarrow{\$} \mathcal{F}_C^{M^n} \\ G \xleftarrow{\$} \mathcal{F}_M^R}} \left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_G^{\otimes r}]}(t, q_{\mathcal{H}}, q_G)\right] \leq QADV^{\gamma\text{-}sp+}_{\mathcal{IS}_G}\left(t', q_{\mathcal{H}}\right) + O\left(\frac{q_{\mathcal{H}}^2(\gamma-1)^r}{|C|^r}\right) + O_n\left(\frac{(q_G + q_{\mathcal{H}})^3}{|M|}\right).$$

with $t' = O_n(t) + nr + n|C|$.

One can then use $QADV^{\gamma\text{-}sp+}_{\mathcal{IS}_G}(t', q_{\mathcal{H}}) \leq QADV^{\gamma\text{-}sp}_{\mathcal{IS}_G}(t', q_{\mathcal{H}})$ in order to get a bound in terms of γ-special soundness.

Theorem 2. *Let $\mathcal{IS}_G = (K_{\mathcal{IS}}, P_{\mathcal{IS}}, V_{\mathcal{IS}}, G; M, C, R, n)$ be a commit-and-open identification scheme with $G \xleftarrow{\$} \mathcal{F}_M^R$. Let also $\gamma \geq 2$ be an integer. We have for any $t, q_{\mathcal{H}}, q_G$:*

$$\mathbb{E}_{\substack{\mathcal{H}\xleftarrow{\$}\mathcal{F}_C^{M^n} \\ G\xleftarrow{\$}\mathcal{F}_M^R}}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_G]}(t, q_{\mathcal{H}}, q_G)\right] \leq QADV^{\gamma\text{-}osp}_{\mathcal{IS}_G}(O_n(t), q_{\mathcal{H}}) + O\left(\frac{q_{\mathcal{H}}^2\gamma}{|C|}\right) + O_n\left(\frac{(q_G+q_{\mathcal{H}})^3}{|M|}\right).$$

Proof strategy. We present here informally our proof strategy. We fix a commit-and-open identification scheme $\mathcal{IS}_G = (K_{\mathcal{IS}}, P_{\mathcal{IS}}, V_{\mathcal{IS}}, G; M, C, R, n)$ and a quantum algorithm $\mathscr{A}$ that wants to break the quantum soundness of $\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_G]$. This algorithm outputs $x = (x_1, \ldots, x_n)$ and z_{I_c} such that if we define $c \stackrel{\triangle}{=} \mathcal{H}(x)$, we have $V_{\mathcal{IS}}(pk, c, z_{I_c}) = 1 \wedge \forall i \in I_c, G(z_i) = x_i$. If G were an easily invertible permutation, we could from $x = (x_1, \ldots, x_n)$ extract the full string $z = (G^{-1}(x_1), \ldots, G^{-1}(x_n))$. With such a construction, we can fairly directly relate γ-rigid soundness and γ-output special soundness and then conclude using Proposition 4. However, G is not usually an efficiently invertible random permutation and it can't be if $\mathcal{IS}$ has to be honest verifier zero-knowledge. In order to circumvent this issue, we perform the 4 following steps:

1. We transform $\mathcal{IS}$ into $\widetilde{\mathcal{IS}}$ in order to artificially increase the size of R. This will allow us to work with larger functions with which we will be able to construct pseudorandom permutations using Feistel networks.
2. We start from $G \xleftarrow{\$} \mathcal{F}_M^R$ as our commitment and show that we can replace G with a random permutation $\sigma \in \mathcal{P}^R$.
3. We now have a random permutation σ as our commitment. We show here how to replace σ with a quantum pseudorandom permutation $\widetilde{\pi}_0$ that is easily invertible using Feistel networks.
4. Now, that we have an easily invertible permutation, we relate the quantum Fiat-Shamir advantage to the special+ (or output special) soundness advantage of $\widetilde{\mathcal{IS}}$. We can then go back to $\mathcal{IS}$ since the two soundness advantage notions we consider are independent of the commitment used and are the same for $\mathcal{IS}$ and $\widetilde{\mathcal{IS}}$, which allows us to finish the proof. It is only step 4 that differes for Theorems 1 and 2.

We now present these 4 steps in the next 4 subsections.

5.2 Step 1: Transforming $\mathcal{IS}$ into $\widetilde{\mathcal{IS}}$

We start from a commit-and-open identification $\mathcal{IS}_G = (K_{\mathcal{IS}}, P_{\mathcal{IS}}, V_{\mathcal{IS}}, G; M, C, R, n)$. We consider the smallest set R' of the form $\{0,1\}^{2m}$ with $m \geq 2048$ such that $R \subseteq R'$ and $M \subseteq R'$[11]. With this artificial increase of R, we consider a commitment function $G' : R' \to M$. The idea is that instead of committing to each $z_i \in R$ using the string $G(z_i)$, we commit to these strings via the string $G'(z_i||0\ldots0)$, where $z_i||0\ldots0 \in R'$.

[11]To do this, we increase m so that $|M|, |R| \leq 2^{2m}$. If this doesn't give us the inclusions then we can relabel the elements of M and R so that they are included in $\{0,1\}^{2m}$.

We consider $\widetilde{\mathcal{IS}}_{G'} = (K_{\mathcal{IS}}, P_{\mathcal{IS}}, \widetilde{V_{\mathcal{IS}}}, G'; M, C, R', n)$ that is derived from $\mathcal{IS}_G$ where we changed the space R into R' (and accordingly the function G into G'), as well as $\widetilde{V_{\mathcal{IS}}}$ which is defined as follows:

$$\widetilde{V_{\mathcal{IS}}}(pk, c, z'_{I_c}) = 1 \Leftrightarrow \left(\forall i \in I_c,\ z'_i = z_i||0\dots0 \text{ for some } z_i \in R\right) \wedge V_{\mathcal{IS}}(pk, c, z_{I_c}) = 1.$$

We prove the following proposition

Proposition 5. *For any hash function $\mathcal{H}$, for any $t, q_G, q_{\mathcal{H}}$, we have*

$$\mathbb{E}_{G \xleftarrow{\$} \mathcal{F}_M^R}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_G]}(t, q_{\mathcal{H}}, q_G)\right] \leq \mathbb{E}_{G' \xleftarrow{\$} \mathcal{F}_M^{R'}}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\widetilde{\mathcal{IS}}_{G'}]}(t, q_{\mathcal{H}}, q_G)\right].$$

Proof. For any function $G' \in \mathcal{F}_M^{R'}$, we define the function $C_{G'} \in \mathcal{F}_M^R$ as follows: $C_{G'}(z) \stackrel{\triangle}{=} G'(z||0\dots0)$. Notice that if G' is a random function in $\mathcal{F}_M^{R'}$ then $C_{G'}$ is a random function in $\mathcal{F}_M^R$. Therefore

$$\mathbb{E}_{G \xleftarrow{\$} \mathcal{F}_M^R}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_G]}(\mathscr{A}^{|G\rangle,|\mathcal{H}\rangle})\right] = \mathbb{E}_{G' \xleftarrow{\$} \mathcal{F}_M^{R'}}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_{C_{G'}}]}(\mathscr{A}^{|C_{G'}\rangle,|\mathcal{H}\rangle})\right].$$

Now, let's consider the following algorithm $\mathscr{A}_2^{|C_{G'}\rangle,|\mathcal{H}\rangle} : (x, z_{I_c}) \leftarrow \mathscr{A}^{|C_{G'}\rangle,|\mathcal{H}\rangle}$ with $c = \mathcal{H}(x)$. Return (x, z'_{I_c}) where $\forall i \in I_c,\ z'_i = z_i||0\dots0$. From the definition of $\widetilde{\mathcal{IS}}$, we have

$$\begin{aligned}\mathbb{E}_{G' \xleftarrow{\$} \mathcal{F}_M^{R'}}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_{C_{G'}}]}(\mathscr{A}^{|C_{G'}\rangle,|\mathcal{H}\rangle})\right] &= \mathbb{E}_{G' \xleftarrow{\$} \mathcal{F}_M^{R'}}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\widetilde{\mathcal{IS}}_{G'}]}(\mathscr{A}_2^{|C_{G'}\rangle,|\mathcal{H}\rangle})\right] \\ &\leq \mathbb{E}_{G' \xleftarrow{\$} \mathcal{F}_M^{R'}}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\widetilde{\mathcal{IS}}_{G'}]}(\mathscr{A}_2^{|G'\rangle,|\mathcal{H}\rangle})\right]\end{aligned}$$

where the last inequality comes from the fact that a call to $U_{C_{G'}}$ can be done with a call to $U_{G'}$. Since the running time and number of queries remains unchanged between $\mathscr{A}$ and $\mathscr{A}_2$, we can conclude. □

Notice also from the definitions that we can derive the following equalities, for any γ and $\mathcal{H}$:

$$\begin{aligned}\mathbb{E}_{G \xleftarrow{\$} \mathcal{F}_M^R}\left[QADV^{\gamma\text{-}sp+}_{\mathcal{IS}_G}(t, q_G, q_{\mathcal{H}})\right] &= \mathbb{E}_{G' \xleftarrow{\$} \mathcal{F}_M^{R'}}\left[QADV^{\gamma\text{-}sp+}_{\widetilde{\mathcal{IS}}_{G'}}(t, q_G, q_{\mathcal{H}})\right] \\ \mathbb{E}_{G \xleftarrow{\$} \mathcal{F}_M^R}\left[QADV^{\gamma\text{-}osp}_{\mathcal{IS}_G}(t, q_G, q_{\mathcal{H}})\right] &= \mathbb{E}_{G' \xleftarrow{\$} \mathcal{F}_M^{R'}}\left[QADV^{\gamma\text{-}osp}_{\widetilde{\mathcal{IS}}_{G'}}(t, q_G, q_{\mathcal{H}})\right]\end{aligned}$$

5.3 Step 2: Replacing G with a random permutation

We prove the second step, which corresponds to the following proposition.

Proposition 6. *Let $\mathcal{IS} = (K_{\mathcal{IS}}, P_{\mathcal{IS}}, V_{\mathcal{IS}}, G; M, C, R, n)$ be a commit-and-open identification scheme with $M \subseteq R$. We have for any $t, q_{\mathcal{H}}, q_G$*

$$\mathbb{E}_{\substack{\mathcal{H} \xleftarrow{\$} \mathcal{F}_C^{M^n} \\ G \xleftarrow{\$} \mathcal{F}_M^R}}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_G]}(t, q_{\mathcal{H}}, q_G)\right] \leq \mathbb{E}_{\substack{\mathcal{H} \xleftarrow{\$} \mathcal{F}_C^{M^n} \\ \sigma \xleftarrow{\$} \mathcal{P}^R}}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_\sigma]}(t'', q''_{\mathcal{H}}, q''_G) + O_n\left(\frac{(q_G + q_{\mathcal{H}})^3}{|M|}\right)\right].$$

with $t'' = O_n(t), q''_{\mathcal{H}} = q_{\mathcal{H}}, q''_G = O_n(q_G + q_{\mathcal{H}})$.

Proof. We first show the following lemma, which states that we can replace G with $\pi \circ G$ for any permutation $\pi \in \mathcal{P}^R$. In order to define $\pi \circ G$, we actually need to extend G to a function with image R, which is possible since we considered the case where $M \subseteq R$.

Lemma 2. *For any permutation $\pi \in \mathcal{P}^R$, for which we have an efficient black box access, for any fixed $G \in \mathcal{F}_M^R$ (extended to $G \in \mathcal{F}_R^R$), there exists a quantum query algorithm $\mathscr{B}^{|\mathcal{H}\rangle,|G\rangle,|\pi\rangle}$ of size $|\mathscr{B}^{|\mathcal{H}\rangle,|G\rangle,|\pi\rangle}| \stackrel{\triangle}{=} (t', q'_{\mathcal{H}}, q'_G, q'_\pi)$ such that*

$$\mathbb{E}_{\mathcal{H}\xleftarrow{\$}\mathcal{F}_C^{M^n}}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_G]}(t, q_{\mathcal{H}}, q_G)\right] = \mathbb{E}_{\mathcal{H}\xleftarrow{\$}\mathcal{F}_C^{M^n}}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_{\pi\circ G}]}(\mathscr{B}^{|\mathcal{H}\rangle,|G\rangle,|\pi\rangle})\right].$$

and $t' = O_n(t), q'_{\mathcal{H}} = q_{\mathcal{H}}, q'_G = q_G, q'_\pi = O_n(q_{\mathcal{H}})$.

Proof. Let $\mathscr{A}^{|\mathcal{H}\rangle,|G\rangle}$ be a quantum query algorithm with $|\mathscr{A}^{|\mathcal{H}\rangle,|G\rangle}| = (t, q_{\mathcal{H}}, q_G)$ and $QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_G]}(\mathscr{A}^{|\mathcal{H}\rangle,|G\rangle}) = QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_G]}(t, q_{\mathcal{H}}, q_G)$. Fix also a permutation π. For each function $\mathcal{H} : M^n \to C$, we define $\mathcal{H}_\pi(x_1, \ldots, x_n) \stackrel{\triangle}{=} \mathcal{H}(\pi(x_1), \ldots, \pi(x_n))$. Notice that if $\mathcal{H} \xleftarrow{\$} \mathcal{F}_C^{M^n}$ then $\mathcal{H}_\pi$ is also uniformly random in $\mathcal{F}_C^{M^n}$ for any fixed π. Therefore, we have

$$\mathbb{E}_{\mathcal{H}\xleftarrow{\$}\mathcal{F}_C^{M^n}}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_G]}(\mathscr{A}^{|\mathcal{H}\rangle,|G\rangle})\right] = \mathbb{E}_{\mathcal{H}\xleftarrow{\$}\mathcal{F}_C^{M^n}}\left[QADV_{\mathrm{FS}^{\mathcal{H}_\pi}[\mathcal{IS}_G]}(\mathscr{A}^{|\mathcal{H}_\pi\rangle,|G\rangle})\right]. \tag{5}$$

We now construct the following algorithm $\mathscr{B}^{|\mathcal{H}\rangle,|G\rangle,|\pi\rangle} : (x, z_{I_c}) \leftarrow \mathscr{A}^{|\mathcal{H}_\pi\rangle,|G\rangle}$, return $(\boldsymbol{\pi}(x), z_{I_c})$. where we use the notation $\boldsymbol{\pi}(x) = \pi(x_1), \ldots, \pi(x_n)$. The algorithm $\mathscr{B}^{|\mathcal{H}\rangle,|G\rangle,|\pi\rangle}$ emulates calls to $U_{\mathcal{H}_\pi}$, with calls to $U_{\mathcal{H}}$ and U_π, using each time n calls to U_π and 1 call to $U_{\mathcal{H}}$.

$$\begin{aligned}
\Gamma_1 &\stackrel{\triangle}{=} QADV_{\mathrm{FS}^{\mathcal{H}_\pi}[\mathcal{IS}_{\pi\circ G}]}(\mathscr{A}^{|\mathcal{H}_\pi\rangle,|G\rangle}) \\
&= \Pr\left[V_{\mathcal{IS}}(pk, c, z_{I_c}) = 1 \wedge (\forall i \in I_c, G(z_i) = x_i) \;\middle|\; \begin{smallmatrix}(pk,sk)\leftarrow K_{\mathcal{IS}}(1^\lambda)\\ (x,z_{I_c})\leftarrow\mathscr{A}^{|\mathcal{H}_\pi\rangle,|G\rangle}\\ c=\mathcal{H}_\pi(x)\end{smallmatrix}\right] \\
&= \Pr\left[V_{\mathcal{IS}}(pk, c, z_{I_c}) = 1 \wedge (\forall i \in I_c, (\pi\circ G)(z_i) = \pi(x_i)) \;\middle|\; \begin{smallmatrix}(pk,sk)\leftarrow K_{\mathcal{IS}}(1^\lambda)\\ (x,z_{I_c})\leftarrow\mathscr{A}^{|\mathcal{H}_\pi\rangle,|G\rangle}\\ c=\mathcal{H}(\boldsymbol{\pi}(x))\end{smallmatrix}\right] \\
&= \Pr\left[V_{\mathcal{IS}}(pk, c, z_{I_c}) = 1 \wedge (\forall i \in I_c, (\pi\circ G)(z_i) = \pi(x_i)) \;\middle|\; \begin{smallmatrix}(pk,sk)\leftarrow K_{\mathcal{IS}}(1^\lambda)\\ (\boldsymbol{\pi}(x),z_{I_c})\leftarrow\mathscr{B}^{|\mathcal{H}\rangle,|G\rangle,|\pi\rangle}\\ c=\mathcal{H}(\boldsymbol{\pi}(x))\end{smallmatrix}\right] \\
&= QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_{\pi\circ G}]}(\mathscr{B}^{|\mathcal{H}\rangle,|G\rangle,|\pi\rangle}).
\end{aligned} \tag{6}$$

Combining Equations 5 and 6, we can conclude

$$\begin{aligned}
\mathbb{E}_{\mathcal{H}\xleftarrow{\$}\mathcal{F}_C^{M^n}}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_G]}(\mathscr{A}^{|\mathcal{H}\rangle,|G\rangle})\right] &= \mathbb{E}_{\mathcal{H}\xleftarrow{\$}\mathcal{F}_C^{M^n}}\left[QADV_{\mathrm{FS}^{\mathcal{H}_\pi}[\mathcal{IS}_G]}(\mathscr{A}^{|\mathcal{H}_\pi\rangle,|G\rangle})\right] \\
&= \mathbb{E}_{\mathcal{H}\xleftarrow{\$}\mathcal{F}_C^{M^n}}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_{\pi\circ G}]}(\mathscr{B}^{|\mathcal{H}\rangle,|G\rangle,|\pi\rangle})\right].
\end{aligned}$$

□

We now go back to the proof of Proposition 6. The above lemma holds for any π and G, so we can choose in particular a random function G and random permutation π, which gives us

$$\mathbb{E}_{\substack{\mathcal{H}\xleftarrow{\$}\mathcal{F}_C^{M^n}\\ G\xleftarrow{\$}\mathcal{F}_M^R}}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_G]}(t, q_{\mathcal{H}}, q_G)\right] = \mathbb{E}_{\mathcal{H}\xleftarrow{\$}\mathcal{F}_C^{M^n}}\mathbb{E}_{\substack{G\xleftarrow{\$}\mathcal{F}_M^R\\ \pi\xleftarrow{\$}\mathcal{P}^R}}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_{\pi\circ G}]}(\mathscr{B}^{|\mathcal{H}\rangle,|G\rangle,|\pi\rangle})\right]. \tag{7}$$

Using Zhandry's lower bound on small range functions, it seems we could directly conclude and get Proposition 6. There is a caveat though. The algorithm $\mathscr{B}$ constructed in the above lemma makes calls to $U_{\mathcal{H}}$, U_G and U_π while in order to satisfy the definitions, we would want $\mathscr{B}$ to make calls only to $U_{\mathcal{H}}$ and $U_{\pi\circ G}$.

In order to solve the problem, we use once again the QROM. In the scheme $\mathcal{IS}_{\pi\circ G}$, when taking random π and G, the commitment used $\pi \circ G$ is a random function with small range and we use the QROM to state that we only have black box access to $\pi \circ G$. This implies that an adversary having access to U_G and U_π isn't more powerful than an adversary having access to $U_{\pi\circ G}$ when trying to attack the Fiat-Shamir transform of $\mathcal{IS}_{\pi\circ G}$ in the QROM and motivates the following:

Assumption 1 (The QROM assumption for $\mathcal{IS}_{\pi\circ G}$)**.** [12] *For any quantum query algorithm $\mathscr{B}^{|\mathcal{H}\rangle,|G\rangle,|\pi\rangle}$ with $|\mathscr{B}^{|\mathcal{H}\rangle,|G\rangle,|\pi\rangle}| = (t, q'_{\mathcal{H}}, q'_G, q'_\pi)$, there exists an algorithm $\mathscr{C}^{|\mathcal{H}\rangle,|\pi\circ G\rangle}$ st.*

$$\mathbb{E}_{\substack{G\xleftarrow{\$}\mathcal{F}_M^R \\ \pi\xleftarrow{\$}\mathcal{P}^R}}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_{\pi\circ G}]}(\mathscr{B}^{|\mathcal{H}\rangle,|G\rangle,|\pi\rangle})\right] = \mathbb{E}_{\substack{G\xleftarrow{\$}\mathcal{F}_M^R \\ \pi\xleftarrow{\$}\mathcal{P}^R}}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_{\pi\circ G}]}(\mathscr{C}^{|\mathcal{H}\rangle,|\pi\circ G\rangle})\right].$$

and $|\mathscr{C}^{|\mathcal{H}\rangle,|\pi\circ G\rangle}| = (t', q'_{\mathcal{H}}, q'_G + q'_\pi)$.

Here, we count conservatively and consider that a call to U_G or U_π in $\mathscr{B}^{|\mathcal{H}\rangle,|G\rangle,|\pi\rangle}$ is as powerful as a call to $U_{\pi\circ G}$ in $\mathscr{C}^{|\mathcal{H}\rangle,|\pi\circ G\rangle}$. Also, the above is true for any function $\mathcal{H}$.

We can now go finish the proof of Proposition 7. Fix any algorithm $\mathscr{B}^{|\mathcal{H}\rangle,|G\rangle,|\pi\rangle}$ with $|\mathscr{B}^{|\mathcal{H}\rangle,|G\rangle,|\pi\rangle}| = (t', q'_{\mathcal{H}}, q'_G, q'_\pi)$ and a corresponding $\mathscr{C}^{|\mathcal{H}\rangle,|\pi\circ G\rangle}$ such that the equality of Assumption 1 holds. Recall the definition of DSF of Section 3.4. We get for any $\mathcal{H}$

$$\begin{aligned}\mathbb{E}_{\substack{G\xleftarrow{\$}\mathcal{F}_M^R \\ \pi\xleftarrow{\$}\mathcal{P}^R}}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_{\pi\circ G}]}(\mathscr{B}^{|\mathcal{H}\rangle,|G\rangle,|\pi\rangle})\right] &= \mathbb{E}_{\substack{G\xleftarrow{\$}\mathcal{F}_M^R \\ \pi\xleftarrow{\$}\mathcal{P}^R}}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_{\pi\circ G}]}(\mathscr{C}^{|\mathcal{H}\rangle,|\pi\circ G\rangle})\right] \\ &= \mathbb{E}_{S\leftarrow DSF^R_{|M|}}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_S]}(\mathscr{C}^{|\mathcal{H}\rangle,|S\rangle})\right] \\ &\leq \mathbb{E}_{S\leftarrow DSF^R_{|M|}}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_S]}(t', q'_{\mathcal{H}}, q'_G + q'_\pi)\right] \qquad (8)\end{aligned}$$

We now use Proposition 3 to get for any $\mathcal{H}$:

$$\begin{aligned}\mathbb{E}_{S\leftarrow DSF^R_{|M|}}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_S]}(t', q'_{\mathcal{H}}, q'_G + q'_\pi)\right] \leq \mathbb{E}_{\sigma\xleftarrow{\$}\mathcal{P}^R}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_\sigma]}(t, q'_{\mathcal{H}}, q'_G + q'_\pi)\right] + \\ O\left(\frac{(q'_G + q'_\pi)^3}{|M|}\right). \qquad (9)\end{aligned}$$

[12] The function $\pi \circ G$ has less structure for a random π and random G than say the SHA-3 sponge with a random internal function. In the QROM, the latter is modeled in a black box fashion, so we consider as a mild assumption to also consider this for the former.

Putting Equations 7, 8 and 9, we get

$$\begin{aligned}
\mathbb{E}_{\substack{\mathcal{H}\xleftarrow{\$}\mathcal{F}_C^{M^n}\\ G\xleftarrow{\$}\mathcal{F}_M^R}}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_G]}(t,q_{\mathcal{H}},q_G)\right] &= \mathbb{E}_{\mathcal{H}\xleftarrow{\$}\mathcal{F}_C^{M^n}}\mathbb{E}_{\substack{G\xleftarrow{\$}\mathcal{F}_M^R\\ \pi\xleftarrow{\$}\mathcal{P}^R}}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_{\pi\circ G}]}(\mathscr{B}^{|\mathcal{H}\rangle,|G\rangle,|\pi\rangle})\right]\\
&\leq \mathbb{E}_{\mathcal{H}\xleftarrow{\$}\mathcal{F}_C^{M^n}}\mathbb{E}_{S\xleftarrow{\$}DSF_{|M|}^R}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_S]}(t',q'_{\mathcal{H}},q'_G+q'_\pi)\right]\\
&\leq \mathbb{E}_{\substack{\mathcal{H}\xleftarrow{\$}\mathcal{F}_C^{M^n}\\ \sigma\xleftarrow{\$}\mathcal{P}^R}}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_\sigma]}(t',q'_{\mathcal{H}},q'_G+q'_\pi)\right]+O\left(\frac{(q'_G+q'_\pi)^3}{|M|}\right)\\
&\leq \mathbb{E}_{\substack{\mathcal{H}\xleftarrow{\$}\mathcal{F}_C^{M^n}\\ \sigma\xleftarrow{\$}\mathcal{P}^R}}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_\sigma]}(t'',q''_{\mathcal{H}},q''_G)\right]+O_n\left(\frac{(q_{\mathcal{H}}+q_G)^3}{|M|}\right)
\end{aligned}$$

with $t''=O_n(t), q''_{\mathcal{H}}=q_{\mathcal{H}}, q''_G=O_n(q_G+q_{\mathcal{H}})$ where for the last inequality, we use $t'=O_n(t), q'_{\mathcal{H}}=q_{\mathcal{H}}, q'_G=q_G, q'_\pi=O_n(q_{\mathcal{H}})$. □

5.4 Step 3: Replacing the random permutation σ with an efficiently invertible QPRP

We prove the following proposition

Proposition 7. *Let $\mathcal{IS}=(K_{\mathcal{IS}},P_{\mathcal{IS}},V_{\mathcal{IS}},G;M,C,R,n)$ be a commit-and-open identification scheme with $R=\{0,1\}^{2m}$ for some integer m. In the QROM, there exists a permutation $\widetilde{\pi}_0$ that is efficiently computable and invertible such that for any fixed $\mathcal{H}$:*

$$\mathbb{E}_{\sigma\xleftarrow{\$}\mathcal{P}^R}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_\sigma]}(t,q_{\mathcal{H}},q_G)\right]\leq QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_{\widetilde{\pi}_0}]}(t,q_{\mathcal{H}})+O(\frac{q_G^3}{2^{m/2}}).$$

Proof. In order to prove this proposition, we will use Feistel networks described in Section 3. Our pseudorandom permutation is the following

$$\widetilde{\pi}_0\stackrel{\triangle}{=}\mathfrak{Fe}_4(\text{SHAKE-256}_{\{0,1\}^m,\{0,1\}^m}).$$

Now fix $\mathcal{H}$. We have

$$\begin{aligned}
\mathbb{E}_{\sigma\xleftarrow{\$}\mathcal{P}^R}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_\sigma]}(t,q_{\mathcal{H}},q_G)\right] &\leq \mathbb{E}_{f\xleftarrow{\$}\mathcal{F}_{\{0,1\}^m}^{\{0,1\}^m}}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_{\mathfrak{Fe}_4(f)}]}(t,q_{\mathcal{H}},q_G)\right]+O(\sqrt{\frac{q_G^6}{2^m}})\\
&= QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_{\widetilde{\pi}_0}]}(t,q_{\mathcal{H}})+O(\frac{q_G^3}{2^{m/2}}).
\end{aligned}$$

The first inequality comes from Proposition 2 and the second equality comes from the QROM, where we model the hash function $\text{SHAKE-256}_{\{0,1\}^m,\{0,1\}^m}$ with a random function in $\mathcal{F}_{\{0,1\}^m}^{\{0,1\}^m}$. □

When $m\geq 2048$ (this is the value chosen in Step 1 but it couldn't have been another arbitrary large value), the term $O(\frac{q_G^3}{2^{m/2}})$ will always be tiny and irrelevant for the amounts of security we consider.

5.5 Finishing the proof: step 4 and conclusion

So we managed to replace the commitment function by the pseudorandom permutation $\widetilde{\pi}_0 = \mathfrak{Fe}_4(\text{SHAKE-256}_{\{0,1\}^m,\{0,1\}^m})$ with $|R| = 2^{2m}$. As we described in Section 3, this use of Feistel networks implies that both $\widetilde{\pi}_0$ and $\widetilde{\pi}_0^{-1}$ are efficiently computable without needing to know how to compute preimages for $\text{SHAKE-256}_{\{0,1\}^m,\{0,1\}^m}$. Our goal in this final step is to bound $QADV_{\text{FS}^{\mathcal{H}}[\mathcal{IS}_{\widetilde{\pi}_0}]}(t, q_{\mathcal{H}})$.

5.5.1 Step 4 used for Theorem 2

Proposition 8. *Let $\mathcal{IS}_{\widetilde{\pi}_0} = (K_{\mathcal{IS}}, P_{\mathcal{IS}}, V_{\mathcal{IS}}, \widetilde{\pi}_0; M, C, R, n)$ be a commit-and-open identification scheme. For any integer $\gamma \geq 2$, for any fixed $\mathcal{H}$, we have*

$$QADV_{\text{FS}^{\mathcal{H}}[\mathcal{IS}_{\widetilde{\pi}_0}]}(t, q_{\mathcal{H}}) \leq QADV^{\gamma\text{-}osp}_{\mathcal{IS}_{\widetilde{\pi}_0}}(t + n, q_{\mathcal{H}}) + O(\frac{q_{\mathcal{H}}^2 \gamma}{|C|}).$$

Notice here that since $\widetilde{\pi}_0$ has a known efficient description, we don't consider only black box calls to $U_{\widetilde{\pi}_0}$ but we can perform any computation that depends on the description of $\widetilde{\pi}_0$ and $\widetilde{\pi}_0^{-1}$. Also, the above holds for any efficiently computable and invertible permutation $\widetilde{\pi}_0$.

Proof. Fix a commit-and-open identification scheme $\mathcal{IS}_{\widetilde{\pi}_0} = (K_{\mathcal{IS}}, P_{\mathcal{IS}}, V_{\mathcal{IS}}, \widetilde{\pi}_0; M, C, R, n)$, and an integer $\gamma \geq 2$. Using Proposition 4, we have

$$QADV_{\text{FS}^{\mathcal{H}}[\mathcal{IS}_{\widetilde{\pi}_0}]}(t, q_{\mathcal{H}}) \leq QADV^{\gamma\text{-}rs}_{\mathcal{IS}_{\widetilde{\pi}_0}}(t, q_{\mathcal{H}}) + O(\frac{q_{\mathcal{H}}^2 \gamma}{|C|}). \tag{10}$$

Let $\mathscr{C}^{|\mathcal{H}\rangle}$ be an quantum query algorithm satisfying $|\mathscr{C}^{|\mathcal{H}\rangle}| = (t, q_{\mathcal{H}})$ and $QADV^{\gamma\text{-}rs}_{\mathcal{IS}_{\widetilde{\pi}_0}}(t, q_{\mathcal{H}}) = QADV^{\gamma\text{-}rs}_{\mathcal{IS}_{\widetilde{\pi}_0}}(\mathscr{C}^{|\mathcal{H}\rangle})$. We consider the following algorithm $\mathscr{B}^{|\mathcal{H}\rangle}$:

$$\mathscr{B}^{|\mathcal{H}\rangle}(pk) : x \stackrel{\triangle}{=} (x_1, \ldots, x_n) \leftarrow \mathscr{C}^{|\mathcal{H}\rangle}(pk), z = (\widetilde{\pi}_0^{-1}(x_1), \ldots, \widetilde{\pi}_0^{-1}(x_n)), \text{ return } z.$$

Notice that if $\mathscr{C}^{|\mathcal{H}\rangle}$ outputs a value $x \in VC^{\mathcal{IS}}_{\geq \gamma}$, then $|\{c : V_{\mathcal{IS}}(pk, c, z_{I_c}) = 1\}| \geq \gamma)$. Therefore, $QADV^{\gamma\text{-}rs}_{\mathcal{IS}_{\widetilde{\pi}_0}}(\mathscr{C}^{|\mathcal{H}\rangle}) \leq QADV^{\gamma\text{-}osp}_{\mathcal{IS}_{\widetilde{\pi}_0}}(\mathscr{B}^{|\mathcal{H}\rangle})$. Also $\mathscr{B}^{|\mathcal{H}\rangle}$ runs in time $t + \ n$ (recall that $\widetilde{\pi}_0^{-1}$ can be performed efficiently so we consider here its running time is 1). We can therefore conclude

$$QADV^{\gamma\text{-}rs}_{\mathcal{IS}_{\widetilde{\pi}_0}}(t, q_{\mathcal{H}}) \leq QADV^{\gamma\text{-}osp}_{\mathcal{IS}_{\widetilde{\pi}_0}}(t + n, q_{\mathcal{H}}).$$

□

5.5.2 Theorem 2: putting everything together

We can now show our first main theorem, which is the combination of our 4 steps.

Theorem 2. *Let $\mathcal{IS}_G = (K_{\mathcal{IS}}, P_{\mathcal{IS}}, V_{\mathcal{IS}}, G; M, C, R, n)$ be a commit-and-open identification scheme with $G \stackrel{\$}{\leftarrow} \mathcal{F}_M^R$. Let also $\gamma \geq 2$ be an integer. We have for any $t, q_{\mathcal{H}}, q_G$:*

$$\mathbb{E}_{\substack{\mathcal{H} \stackrel{\$}{\leftarrow} \mathcal{F}_C^{M^n} \\ G \stackrel{\$}{\leftarrow} \mathcal{F}_M^R}} \left[QADV_{\text{FS}^{\mathcal{H}}[\mathcal{IS}_G]}(t, q_{\mathcal{H}}, q_G) \right] \leq QADV^{\gamma\text{-}osp}_{\mathcal{IS}_G}(O_n(t), q_{\mathcal{H}}) + O\left(\frac{q_{\mathcal{H}}^2 \gamma}{|C|}\right) + O_n\left(\frac{(q_G + q_{\mathcal{H}})^3}{|M|}\right).$$

Proof. We start from $\mathcal{IS}_G$ and construct $\widetilde{\mathcal{IS}}_{G'} = (K_{\mathcal{IS}}, P_{\mathcal{IS}}, \widetilde{V_{\mathcal{IS}}}, G'; M, C, R', n)$ as in Proposition 5. We have in particular $M \subseteq R$, which allows us to apply Proposition 6 and $R = \{0,1\}^{2m}$ with $m \geq 2048$. We define $\widetilde{\pi}_0 \stackrel{\triangle}{=} \mathfrak{Fe}_4(\text{SHAKE-256}_{\{0,1\}^m,\{0,1\}^m})$ and write

$$\begin{aligned}
\Gamma_2 &\stackrel{\triangle}{=} \mathbb{E}_{\substack{\mathcal{H}\xleftarrow{\$}\mathcal{F}_C^{M^n} \\ G\xleftarrow{\$}\mathcal{F}_M^R}} \left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}_G]}(t, q_{\mathcal{H}}, q_G)\right] \\
&\leq \mathbb{E}_{\substack{\mathcal{H}\xleftarrow{\$}\mathcal{F}_C^{M^n} \\ G'\xleftarrow{\$}\mathcal{F}_M^{R'}}} \left[QADV_{\mathrm{FS}^{\mathcal{H}}[\widetilde{\mathcal{IS}}_{G'}]}(t, q_G, q_{\mathcal{H}})\right] \\
&\leq \mathbb{E}_{\substack{\mathcal{H}\xleftarrow{\$}\mathcal{F}_C^{M^n} \\ \sigma\xleftarrow{\$}\mathcal{P}^R}} \left[QADV_{\mathrm{FS}^{\mathcal{H}}[\widetilde{\mathcal{IS}}_{\sigma}]}(O_n(t), q_{\mathcal{H}}, O_n(q_G + q_{\mathcal{H}}))\right] + O_n\left(\frac{(q_G + q_{\mathcal{H}})^3}{|M|}\right) \\
&= \mathbb{E}_{\mathcal{H}\xleftarrow{\$}\mathcal{F}_C^{M^n}} \left[QADV_{\mathrm{FS}^{\mathcal{H}}[\widetilde{\mathcal{IS}}_{\widetilde{\pi}_0}]}(O_n(t), q_{\mathcal{H}})\right] + O_n\left(\frac{(q_G + q_{\mathcal{H}})^3}{|M|}\right) \\
&\leq QADV^{\gamma\text{-}osp}_{\widetilde{\mathcal{IS}}_{\widetilde{\pi}_0}}(O_n(t), q_{\mathcal{H}}) + O\left(\frac{q_{\mathcal{H}}^2\gamma}{|C|}\right) + O_n\left(\frac{(q_G + q_{\mathcal{H}})^3}{|M|}\right) \\
&= QADV^{\gamma\text{-}osp}_{\mathcal{IS}_G}(O_n(t), q_{\mathcal{H}}) + O\left(\frac{q_{\mathcal{H}}^2\gamma}{|C|}\right) + O_n\left(\frac{(q_G + q_{\mathcal{H}})^3}{|M|}\right)
\end{aligned}$$

The first 4 lines come from the 4 steps of our proof, namely Propositions 5, 6, 7 and 8. We ignored the term $O_n(\frac{(q_G+q_{\mathcal{H}})^3}{2^{2m}})$ from Proposition 7 which is tiny and absorbed by the other terms for any reasonable security requirement since $m \geq 2024$. The last equality comes the last equalities of Section 5.2. and concludes the proof of Theorem 2. □

5.5.3 Step 4 used for Theorem 1

We prove here the Step 4 that will be used for proving Theorem 1.

Proposition 9. *Let $\mathcal{IS}_{\widetilde{\pi}_0} = (K_{\mathcal{IS}}, P_{\mathcal{IS}}, V_{\mathcal{IS}}, \widetilde{\pi}_0; M, C, R, n)$ be a commit-and-open identification scheme, where $\widetilde{\pi}_0$ is an efficiently computable and invertible permutation. For any integer $\gamma \geq 2$, and $r \in \mathbb{N}^*$, we have*

$$QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}^{\otimes r}_{\widetilde{\pi}_0}]}(t, q_{\mathcal{H}}) \leq QADV^{\gamma\text{-}sp+}_{\mathcal{IS}^{\otimes r}_{\widetilde{\pi}_0}}(t + nr + |C|r, q_{\mathcal{H}}) + O\left(\frac{q_{\mathcal{H}}^2(\gamma-1)^r}{|C|^r}\right).$$

Proof. We first show the following 2 lemmata.

Lemma 3. *Let $S \subseteq |C|^r$. Let $\gamma \geq 2$ be an integer. If $|S| \geq (\gamma-1)^r + 1$ then there exists an index $i \in [r]$, $|\{c_i : \exists c = (c_1, \ldots, c_r), c \in S\}| \geq \gamma$.*

Proof. We prove the contrapositive. Let $T_i \stackrel{\triangle}{=} \{c_i : \exists c = (c_1, \ldots, c_r), c \in S\}$ and assume that $\forall i \in [r],\ |T_i| \leq \gamma - 1$. We immediately have $S \subseteq T_1 \times T_2 \cdots \times T_r$ which implies $|S| \leq \Pi_{i\in r}|T_i| \leq (\gamma-1)^r$. □

For the next lemma, recall the definitions of valid challenges of Section 4.4. We wil now write $\mathcal{IS}^{\otimes r}$ instead of $\mathcal{IS}^{\otimes r}_{\widetilde{\pi}_0}$ to lighten the notations.

Lemma 4. *Let $x = (x^1, \ldots, x^r) \in M^{nr}$ where for each $i \in [r], x^i = (x^i_1, \ldots, x^i_n)$ and each $x^i_j \in M$. Let also $\gamma \geq 2$ be an integer. If $x \in V^{\mathcal{IS}^{\otimes r}}_{\geq (\gamma-1)^r+1}$ then there exists an $i \in [r]$, distinct values $b_1, \ldots, b_\gamma \in C$ such that if we define $z^i \stackrel{\triangle}{=} \widetilde{\boldsymbol{\pi}}_0^{-1}(x^i) = (\widetilde{\pi}_0^{-1}(x^i_1), \ldots, \widetilde{\pi}_0^{-1}(x^i_n))$, we have $\forall j \in [\gamma],\ V_{\mathcal{IS}}(pk, b_j, z^i_{I_{b_j}}) = 1$.*

Proof. Fix $x \in M^{nr}$ and assume $|VC^{\mathcal{IS}^{\otimes r}}_x| \geq (\gamma-1)^r + 1$. Using the previous lemma, let $i \in [r]$ be the index such that $|\{c_i \in C : \exists c = (c_1, \ldots, c_r) \in VC^{\mathcal{IS}^{\otimes r}}_x\}| \geq \gamma$ and we denote by $\{b_1, \ldots, b_\gamma\}$ any γ pairwise distinct values of this set. For each $j \in [\gamma]$, let $c^j \in VC^{\mathcal{IS}^{\otimes r}}_x$ such that $c^j_i = b_j$. Let $z = \widetilde{\boldsymbol{\pi}}_0^{-1}(x)$. This means for each $i \in [r]$, $z^i = \widetilde{\boldsymbol{\pi}}_0^{-1}(x^i)$. Now $\forall j \in [\gamma]$, because the strings $b_i \in VC^{\mathcal{IS}^{\otimes r}}_x$, we have

$$\forall j \in [\gamma],\ V^{\otimes r}_{\mathcal{IS}}(x, c^j, z_{I_{c^j}}) = 1 \quad \Rightarrow \quad \forall j \in [\gamma],\ V_{\mathcal{IS}}(pk, b_j, z^i_{I_{b_j}}) = 1.$$

□

With these 2 lemmata, we can prove Proposition 9. First notice using Proposition 4 that

$$QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}^{\otimes r}_{\widetilde{\pi}_0}]}(t, q_{\mathcal{H}}) \leq QADV^{((\gamma-1)^r+1)\text{-}rs}_{\mathcal{IS}^{\otimes r}_{\widetilde{\pi}_0}}(t, q_{\mathcal{H}}) + O\left(q^2_{\mathcal{H}} \frac{(\gamma-1)^r}{|C|^r}\right). \tag{11}$$

Let $\mathscr{A}^{|\mathcal{H}\rangle}$ be a quantum algorithm running with $|\mathscr{A}^{|\mathcal{H}\rangle}| = (t, q_{\mathcal{H}})$ such that $QADV^{((\gamma-1)^r+1)\text{-}rs}_{\mathcal{IS}^{\otimes r}_{\widetilde{\pi}_0}}(\mathscr{A}^{|\mathcal{H}\rangle}) = QADV^{((\gamma-1)^r+1)\text{-}rs}_{\mathcal{IS}^{\otimes r}_{\widetilde{\pi}_0}}(t, q_{\mathcal{H}})$. We consider the following algorithm $\mathscr{B}^{|\mathcal{H}\rangle}$:

Quantum algorithm $\mathscr{B}^{|\mathcal{H}\rangle}$

1. compute $x = x^1, \ldots, x^r \leftarrow \mathscr{A}^{|\mathcal{H}\rangle}(p_k)$ where for each $i \in [r], x^i = x^i_1, \ldots, x^i_n$.
2. compute for each $i \in [r], j \in [n]$ $z^i_j = \widetilde{\pi}_0^{-1}(x^i_j)$. Similarly as above, we define $z^i = z^i_1, \ldots, z^i_n$ for each $i \in [r]$.
3. Find $i \in [r]$ and distinct values $b_1, \ldots, b_\gamma \in C$ such that for each $j \in [\gamma], V_{\mathcal{IS}}(pk, b_j, z^i_{I_j}) = 1$ if such values exist, else output $\perp$. To do so, we compute $V_{\mathcal{IS}}(pk, b, z^i_{I_b})$ for each $i \in [r]$ and $b \in C$.
4. Output $(b_1, \ldots, b_\gamma, z^i)$.

Using Lemma 4, we have

$$\begin{aligned}
QADV^{((\gamma-1)^r+1)\text{-}rs}_{\mathcal{IS}^{\otimes r}_{\widetilde{\pi}_0}}(\mathscr{A}^{|\mathcal{H}\rangle}) &= \Pr\left[x \in VC^{\mathcal{IS}}_{(\gamma-1)^r+1} \;\middle|\; \begin{smallmatrix}(pk,sk)\leftarrow K_{\mathcal{IS}}(1^\lambda)\\ x\leftarrow\mathscr{A}^{|\mathcal{H}\rangle}(pk)\end{smallmatrix}\right] \\
&\leq \Pr\left[\exists i\in[r], \exists \text{ distinct } b_1,\ldots,b_\gamma \in C : \right. \\
&\qquad \left. \forall j\in[\gamma], V_{\mathcal{IS}}(pk, x^i, b_j, (\widetilde{\pi}_0^{-1}(x^i))_{I_{b_j}}) = 1 \mid \begin{smallmatrix}(pk,sk)\leftarrow K_{\mathcal{IS}}(1^\lambda)\\ x\leftarrow\mathscr{A}^{|\mathcal{H}\rangle}(pk)\end{smallmatrix}\right] \\
&= \Pr\left[\forall j\in[\gamma], V_{\mathcal{IS}}(pk, b_j, z^i_{I_j}) = 1 \;\middle|\; \begin{smallmatrix}(pk,sk)\leftarrow K_{\mathcal{IS}}(1^\lambda)\\ (b_1,\ldots,b_\gamma,z^i)\leftarrow\mathscr{B}^{|\mathcal{H}\rangle}(pk)\end{smallmatrix}\right] \\
&= QADV^{\gamma\text{-}sp+}_{\mathcal{IS}_{\widetilde{\pi}_0}}(\mathscr{B}^{|\mathcal{H}\rangle}) \qquad (12)
\end{aligned}$$

Now, let's compute the running time of $\mathscr{B}^{|\mathcal{H}\rangle}$. Step 1: takes time t. Step 2: makes nr calls to $\widetilde{\pi}_0^{-1}$, which is efficiently computable. Step 3: makes $|C|r$ calls to $V_{\mathcal{IS}}$ which is efficiently computable. This is implies that the total running time of $\mathscr{B}$ is $t + nr + |C|r$. Moreover, $\mathscr{B}^{|\mathcal{H}\rangle}$ makes as much queries to $|\mathcal{H}\rangle$ as $\mathscr{A}^{|\mathcal{H}\rangle}$. Combining Equation 11 and 12, we conclude

$$QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}^{\otimes r}_{\widetilde{\pi}_0}]}(t, q_{\mathcal{H}}) \leq QADV^{\gamma\text{-}sp+}_{\mathcal{IS}_{\widetilde{\pi}_0}}(t + nr + |C|r, q_{\mathcal{H}}) + O\left(\frac{q^2_{\mathcal{H}}(\gamma-1)^r}{|C|^r}\right)$$

□

5.5.4 Finishing the proof of Theorem 1

We finish the proof exactly as we did for Theorem 2 in Section 5.5.2 except we replace Proposition 8 with Proposition 9.

6 Practical instantiations

We now present several application of our results, to present concrete security claims for different identification schemes, from which we can derive claims for signatures schemes. We first present Stern's identification scheme and its security claim in full detail. The reason we do this is that this identification is probably one of the oldest and has inspired many more identification schemes which have a similar stricture, which we then briefly discuss.

6.1 Stern signature scheme

Notations for this section. Matrices are denoted with bold large letters, for eg. $\mathbf{M}$ and line vectors will be denoted with bold small letters, for eg. $\mathbf{v} = (v_1, \ldots, v_n)$. The Hamming weight $|\cdot|_H$ for binary vectors is defined as follows: $|\mathbf{v}|_H = |\{i : v_i = 1\}|$.

Stern's signature scheme is one of the first signature schemes based on a commit-and-open identification scheme. It is a post-quantum signature scheme based on the hardness of the syndrome decoding problem, which is the canonical hard problem for code-based cryptography.

Problem 1 (Syndrome Decoding - SD(n, k, w))**.**

- Instance: *a parity-check matrix* $\mathbf{H} \in \{0,1\}^{(n-k)\times n}$ *of rank* $n-k$*, a syndrome* $\mathbf{s} \in \{0,1\}^{n-k}$*,*

- Output: $\mathbf{e} \in S_w$ *such that* $\mathbf{e}\mathbf{H}^\intercal = \mathbf{s}$ *where* $S_w \stackrel{\triangle}{=} \{\mathbf{e} \in \{0,1\}^n : |\mathbf{e}|_H = w\}$.

We also define the syndrome decoding advantage:

Definition 10 (SD-advantage(n,k,w))**.** *For any algorithm* $\mathscr{A}$*, we define*

$$Adv^{\mathrm{SD}}_{(n,k,w)}(\mathscr{A}) \stackrel{\triangle}{=} \Pr\left(\mathbf{e}\mathbf{H}^\intercal = \mathbf{s} \wedge |\mathbf{e}| = w \,\middle|\, \mathbf{H} \stackrel{\$}{\leftarrow} \mathrm{FR}^{(n-k),n},\ \mathbf{s} \stackrel{\$}{\leftarrow} \{0,1\}^{n-k},\ \mathbf{e} \leftarrow \mathscr{A}(\mathbf{H},\mathbf{s})\right),$$

where $\mathrm{FR}^{(n-k),n} \stackrel{\triangle}{=} \{\mathbf{H} \in \{0,1\}^{(n-k)\times n} : \mathbf{H}$ *has rank* $(n-k)\}$ *is the set of full rank matrices in* $\{0,1\}^{(n-k),n}$*. For any time* t*, we also define,* $Adv^{\mathrm{SD}}_{(n,k,w)}(t) \stackrel{\triangle}{=} \max_{\mathscr{A}:|\mathscr{A}|=t} Adv^{\mathrm{SD}}_{(n,k,w)}(\mathscr{A})$.

We can now describe Stern's identification scheme

Stern's single round Identification scheme
$\mathcal{IS}_{\mathrm{Stern}}(\lambda, G) = (K_{\mathcal{IS}}, P_{\mathcal{IS}} = (P_1, P_2), V_{\mathcal{IS}}, G; M, C = \{1,2,3\}, R, n = 3)$.

Initialization. $K_{\mathcal{IS}}(1^\lambda)$: $\mathbf{H} \stackrel{\$}{\leftarrow} \mathrm{FR}^{(n-k),n}, \mathbf{e} \stackrel{\$}{\leftarrow} S_w, \mathbf{s} \stackrel{\triangle}{=} \mathbf{e}\mathbf{H}^\intercal$ return $pk = (\mathbf{H}, s)$, $sk = e$, where n, k, w depend on the security parameter λ.

Interaction. $P_1 : \sigma \stackrel{\$}{\leftarrow} \mathcal{P}^{[n]}, \mathbf{y} \leftarrow \{0,1\}^n$. Let $\mathbf{s}' \stackrel{\triangle}{=} \mathbf{y}\mathbf{H}^\intercal$. Let also $z_1 \stackrel{\triangle}{=} (\sigma || \mathbf{s}')$; $z_2 \stackrel{\triangle}{=} \sigma(y)$; $z_3 \stackrel{\triangle}{=} \sigma(\mathbf{y} \oplus \mathbf{e})$. Send $(x_1, x_2, x_3) \stackrel{\triangle}{=} (G(z_1), G(z_2), G(z_3))$ to the verifier.
$V : c \stackrel{\$}{\leftarrow} \{1,2,3\}$, send c to the prover.
P_2 : send $z_{c'}$ for the two values c' different from c.

Verification. $V_{\mathcal{IS}}(1, (z_2, z_3)) = 1$ iff. $|z_2 + z_3|_H = w$.
$V_{\mathcal{IS}}(2, (z_1 \stackrel{\triangle}{=} (\sigma, \mathbf{s}'), z_3)) = 1$ iff. $\sigma^{-1}(z_3)\mathbf{H}^\intercal = \mathbf{s} \oplus \mathbf{s}'$.
$V_{\mathcal{IS}}(3, (z_1 \stackrel{\triangle}{=} (\sigma, \mathbf{s}'), z_2)) = 1$ iff. $\sigma^{-1}(z_2)\mathbf{H}^\intercal = \mathbf{s}'$.

One can check completeness. Indeed, in the honest case:

1. $|z_2 + z_3|_H = |\sigma(\mathbf{y}) + \sigma(\mathbf{y} \oplus \mathbf{e})|_H = |\sigma(e)|_H = w$.
2. $\sigma^{-1}(\sigma(\mathbf{y} \oplus \mathbf{e}))\mathbf{H}^\intercal = \mathbf{y}\mathbf{H}^\intercal + \mathbf{e}\mathbf{H}^\intercal$.
3. $\sigma^{-1}(\sigma(\mathbf{y}))\mathbf{H}^\intercal = \mathbf{y}\mathbf{H}^\intercal$.

Moreover, suppose one constructs a triplet $z_1 = (\sigma, \mathbf{s}'), z_2, z_3$ that passes the 3 checks. We show how to easily construct a vector $\mathbf{e}$ such that $\mathbf{e}\mathbf{H}^\intercal = \mathbf{s}$ and $|\mathbf{e}|_H = w$. Indeed, consider the vector $\mathbf{e} = \sigma^{-1}(z_2 \oplus z_3)$. Using the second and third checks, we have $\mathbf{e}\mathbf{H}^\intercal = \sigma^{-1}(z_2 \oplus z_3)\mathbf{H}^\intercal = \mathbf{s} \oplus \mathbf{s}' \oplus \mathbf{s}' = \mathbf{s}$. Also, $|\mathbf{e}|_H = |\sigma^{-1}(z_2 \oplus z_3)|_H = |z_2 \oplus z_3|_H = w$. This means we immediately have

$$QADV^{3\text{-}sp}_{\mathcal{IS}_{\mathrm{Stern}}(\lambda,G)}(t) = QAdv^{\mathrm{SD}}_{(n(\lambda),k(\lambda),w(\lambda))}(t). \tag{13}$$

The above equality is exactly the kind of relations we need in order to prove the quantum security of the Fiat-Shamir transform of identifications schemes and hence of resulting signature schemes. Using Theorem 1, we immediately have

Proposition 10 (Quantum security of the Fiat-Shamir transform for the parallel repetition of Stern's identifications scheme)**.**

$$\mathbb{E}_{\substack{\mathcal{H}\xleftarrow{\$}\mathcal{F}_C^{M^n} \\ G\xleftarrow{\$}\mathcal{F}_M^R}}\left[QADV_{\mathrm{FS}^{\mathcal{H}}[\mathcal{IS}^{\otimes r}_{\mathrm{Stern}}(\lambda,G)]}(t,q_{\mathcal{H}},q_G)\right] \leq QAdv^{\mathrm{SD}}_{(n(\lambda),k(\lambda),w(\lambda))}(O(t)) + O\left(\frac{q_{\mathcal{H}}^2 2^r}{3^r}\right) + O\left(\frac{q_G^3}{|M|}\right).$$

6.2 Other schemes

The above analysis can be similarly applied to other parallel repetition of commit-and-open identification schemes with $|C| = 3, n = 3$ and for which the post-quantum computational problem can be directly related to 3-special+ soundness as in Equation 13. Such schemes include the [KTX08] identification scheme, the [SSH11] identification scheme and the PICNIC identification scheme [CDG+17], for which we can have a similar statement as Proposition 10.

The 5 round schemes, such as MQDSS or the KKW variant of PICNIC seem to require more work but the current techniques seem quite promising for proving tight security reductions for those as well. There are also more complicated schemes that are commit-and-open but with more rounds such as Pigroast/Legroast [BD20]. These multi-round protocols also have asymptotic quantum reductions from the work of [DFM20] and we hope our techniques can be useful here for concrete security. We leave this for future work.

References

[ABB+19] Erdem Alkim, Paulo S. L. M. Barreto, Nina Bindel, Patrick Longa, and Jefferson E. Ricardini. The lattice-based digital signature scheme qTESLA, 2019. `https://eprint.iacr.org/2019/085`.

[ARU14] Andris Ambainis, Ansis Rosmanis, and Dominique Unruh. Quantum attacks on classical proof systems: The hardness of quantum rewinding. In *FOCS '14*, pages 474–483, 2014.

[BD20] Ward Beullens and Cyprien Delpech de Saint Guilhem. Legroast: Efficient post-quantum signatures from the legendre PRF. In *PQCRYPTO 2020*, volume 12100, pages 130–150. Springer, 2020.

[BDF+11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In *ASIACRYPT 2011*, pages 41–69, 2011.

[BDPV11] G. Bertoni, J. Daemen, Michaël Peeters, and Gilles Van Assche. The keccak sha-3 submission, 2011. `https://keccak.team/files/Keccak-submission-3.pdf`.

[CDG+17] Melissa Chase, David Derler, Steven Goldfeder, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger, Daniel Slamanig, and Greg Zaverucha. Post-quantum zero-knowledge and signatures from symmetric-key primitives. In *CCS '17*, pages 1825–1842, 2017.

[CFM+20] A. Casanova, J-C Faugère, G. Matario-Rat, J. Patarin, L. Perret, and J. Ryckeghem. GeMSS: A great multivariate short signature, 2020. `https://www-polsys.lip6.fr/Links/NIST/GeMSS.html`.

[CGH04] Ran Canetti, Oded Goldreich, and Shai Halevi. The random oracle methodology, revisited. *J. ACM*, 51(4):557–594, July 2004.

[CHR+20] Ming-Shing Chen, Andreas Hülsing, Joost Rijneveld, Simona Samardjiska, and Peter Schwabe. MQDSS specifications, 2020. `http://mqdss.org/files/mqdssVer2point1.pdf`.

[CHS19] Jan Czajkowski, Andreas Hülsing, and Christian Schaffner. Quantum indistinguishability of random sponges. In *CRYPTO 2019, pp 296-325*, 2019.

[DFG13] Özgür Dagdelen, Marc Fischlin, and Tommaso Gagliardoni. The fiat–shamir transformation in a quantum world. In Kazue Sako and Palash Sarkar, editors, *ASIACRYPT 2013*, pages 62–81, 2013.

[DFM20] Jelle Don, Serge Fehr, and Christian Majenz. The measure-and-reprogram technique 2.0: Multi-round fiat-shamir and more. Cryptology ePrint Archive, Report 2020/282, 2020. `https://eprint.iacr.org/2020/282`.

[DFMS19] Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner. Security of the fiat-shamir transformation in the quantum random-oracle model. In *CRYPTO 2019*, pages 356–383, 2019.

[DKL+17] Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stéhlé. CRYSTALS-Dilithium, 2017. `https://pq-crystals.org/dilithium/data/dilithium-specification.pdf`,.

[FS86] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *CRYPTO, pp 186-194*, 1986.

[HI19] Akinori Hosoyamada and Tetsu Iwata. 4-round luby-rackoff construction is a qprp. In *ASIACRYPT 2019*, pages 145–174, 2019.

[KLS18] Eike Kiltz, Vadim Lyubashevsky, and Christian Schaffner. A concrete treatment of fiat-shamir signatures in the quantum random-oracle model. In *EUROCRYPT 2018*, pages 552–586, 2018.

[KM15] Neal Koblitz and Alfred Menezes. The random oracle model: a twenty-year retrospective. *Designs, Codes and Cryptography*, 77, 05 2015.

[KTX08] Akinori Kawachi, Keisuke Tanaka, and Keita Xagawa. Concurrently secure identification schemes based on the worst-case hardness of lattice problems. In *ASIACRYPT 2008*, pages 372–389, 2008.

[KZ19] Daniel Kales and Greg Zaverucha. Forgery attacks on MQDSSv2.0, 2019. `:https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-2/official-comments/MQDSS-round2-official-comment.pdf"`.

[Lei18] Dominik Leichtle. Post-quantum signatures from identification schemes, 2018. `https://pure.tue.nl/ws/portalfiles/portal/125545339/Dominik_Leichtle_thesis_final_IAM_307.pdf`.

[LR88] Michael Luby and Charles Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SICOMP*, 17(2):373–386, 1988.

[LZ19] Qipeng Liu and Mark Zhandry. Revisiting post-quantum fiat-shamir. In *CRYPTO 2019*, pages 326–355, 2019.

[NIS17] NIST. Post-quantum cryptography standardization, 2017. `https://csrc.nist.gov/projects/post-quantum-cryptography`.

[Sho94] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *FOCS 94*, pages 124–134, 1994.

[SSH11] Koichi Sakumoto, Taizo Shirai, and Harunaga Hiwatari. Public-key identification schemes based on multivariate quadratic polynomials. In *CRYPTO 2011*, pages 706–723, 2011.

[Ste93] Jacques Stern. A new identification scheme based on syndrome decoding. In *Advances in Cryptology — CRYPTO' 93*, pages 13–21, 1993.

[Unr12] Dominique Unruh. Quantum proofs of knowledge. In *EUROCRYPT 2012*, pages 135–152, 2012.

[Unr15] Dominique Unruh. Non-interactive zero-knowledge proofs in the quantum random oracle model. In *EUROCRYPT 2015*, pages 755–784, 2015.

[Unr17] Dominique Unruh. Post-quantum security of Fiat-Shamir. In *ASIACRYPT (1)*, pages 65–95. Springer, 2017.

[Zha12] Mark Zhandry. Secure identity-based encryption in the quantum random oracle model. In *CRYPTO 2012*, pages 758–775, 2012.

[Zha15] Mark Zhandry. A note on the quantum collision and set equality problems. *Quantum Info. Comput.*, 15(7-8):557–567, May 2015.

[Zha19] Mark Zhandry. How to record quantum queries, and applications to quantum indifferentiability. In *CRYPTO 2019*, pages 239–268, 2019.

A Signature schemes

A signature scheme S consists of 3 algorithms ($\text{S.KEYGEN}, \text{S.SIGN}, \text{S.VERIFY}$):

- $\text{S.KEYGEN}(1^\lambda) \to (pk, sk)$ is the generation of the public key pk and the secret key sk from the security parameter λ.
- $\text{S.SIGN}(m, pk, sk) \to \sigma_m$: generates the signature σ_m of a message m from m, pk, sk.
- $\text{S.VERIFY}(m, \sigma, pk) \to \{0, 1\}$ verifies that σ is a valid signature of m using m, σ, pk. The output 1 corresponds to a valid signature.

Correctness. A signature scheme is correct iff. when we sample $(pk, sk) \leftarrow \text{S.KEYGEN}(1^\lambda)$, we have for each m

$$\text{S.VERIFY}(m, \text{S.SIGN}(m, pk, sk), pk) = 1.$$

Security definitions We consider the standard EUF-CMA security for signature schemes. To define the advantage of an adversary $\mathscr{A}$, we consider the following interaction with a challenger:

Initialize. The challenger generates $(pk, sk) \leftarrow \text{S.KEYGEN}(1^\lambda)$ and sends pk to $\mathscr{A}$.
Query phase. $\mathscr{A}$ can perform sign queries by sending each time a message m to the challenger who generates $\sigma = \text{S.SIGN}(m, pk, sk)$ and sends σ to $\mathscr{A}$. Let $m_1, \ldots, m_{q_S}$ the (not necessarily distinct) queries made by $\mathscr{A}$. The adversary can also make $q_\mathcal{H}$ queries to $\mathcal{H}$.
Output. $\mathscr{A}$ outputs a pair (m^*, σ^*). The advantage $Adv(\mathscr{A})$ for $\mathscr{A}$ is the quantity

$$QADV_\mathcal{S}^{\text{EUF-CMA}}(\mathscr{A}) = \Pr[\mathscr{A} \text{ outputs } (m^*, \sigma^*) \ st. \\ \text{S.VERIFY}(m^*, \sigma^*, pk) = 1 \wedge m^* \neq m_1, \ldots, m_{q_S}],$$

where $m^* \neq m_1, \ldots, m_{q_S}$ means $\forall i,\ m^* \neq m_i$.

Definition 11. *Let $\mathcal{S} = (\text{S.KEYGEN}, \text{S.SIGN}, \text{S.VERIFY})$ be a signature scheme. We define*

$$QADV_\mathcal{S}^{\text{EUF-CMA}}(t, q_\mathcal{H}, q_S) = \max_\mathscr{A} QADV_\mathcal{S}^{\text{EUF-CMA}}(\mathscr{A}).$$

where we maximize over an adversary running in time t, performing $q_\mathcal{H}$ hash queries and q_S sign queries.

We can directly construct a signature scheme from an identification scheme via the Fiat-Shamir transform. From an identification scheme $\mathcal{IS} = (K_\mathcal{IS}, P_\mathcal{IS} = (P_1, P_2), V_\mathcal{IS}; M, C, R)$, we define the following signature scheme
$\mathcal{S}_\mathcal{IS} = (\text{S}_\mathcal{IS}\text{.KEYGEN}, \text{S}_\mathcal{IS}\text{.SIGN}, \text{S}_\mathcal{IS}\text{.VERIFY})$ that uses a random function $\mathcal{H}$:

- $\text{S}_\mathcal{IS}\text{.KEYGEN}(1^\lambda) = K_\mathcal{IS}(1^\lambda)$
- $\text{S}_\mathcal{IS}\text{.SIGN}(m, pk, sk) : (x, St) \leftarrow P_1(pk), c \leftarrow \mathcal{H}(x, m), z \leftarrow P_2(sk, x, c, St)$, output $\sigma = (x, z)$.
- $\text{S}_\mathcal{IS}\text{.VERIFY}(m, \sigma = (x, z), pk) = V(pk, x, \mathcal{H}(x, m), z)$.

Proposition 11. *[KLS18] Let $\mathcal{IS}$ be an identification scheme which is ε-HVZK and has α bits of min-entropy. Let $S_\mathcal{IS}$ the corresponding signature scheme.*

$$QADV_{S_\mathcal{IS}}^{EUF\text{-}CMA}(t, q_\mathcal{H}, q_S) \leq QADV_{\text{FS}^{\mathcal{H}}[\mathcal{IS}]}(t + q_\mathcal{H} + q_\mathcal{S}, q_\mathcal{H}) + q_\mathcal{S} 2^{-\alpha} + q_\mathcal{S}\varepsilon.$$

where we need to average the 2 advantages over the hash function $\mathcal{H}$.

The min-entropy here is the min-entropy of the prover's first message when he in honest. All schemes we consider will have very large min-entropy so the $q_\mathcal{S} 2^{-\alpha}$ will be negligibly small. Notice that in [KLS18], they prove a more general result where the identification scheme $\mathcal{IS}$ allows some aborts. The above proposition shows that we only need to focus on the soundness of the Fiat-Shamir transform in order to build signature schemes, which is what we will do in the paper.