Shorter and Faster Identity-Based Signatures with Tight Security in the (Q)ROM from Lattices

Éric Sageloli[1], Pierre Pébereau[1,2], Pierrick Méaux[3], Céline Chevalier[4,5]

[1] Thales SIX
pierre.pebereau, eric.sageloli@thalesgroup.com
[2] Sorbonne Université, CNRS, LIP6, PolSys
pierre.pebereau@lip6.fr
[3] University of Luxembourg, Luxembourg
pierrick.meaux@uni.lu
[4] DIENS, École Normale Supérieure, CNRS, Inria, PSL University, Paris, France,
celine.chevalier@ens.fr
[5] CRED, Université Paris-Panthéon-Assas, Paris, France

Abstract. We provide identity-based signature (IBS) schemes with tight security against adaptive adversaries, in the (classical or quantum) random oracle model (ROM or QROM), in both unstructured and structured lattices, based on the SIS or RSIS assumption. These signatures are short (of size independent of the message length). Our schemes build upon a work from Pan and Wagner (PQCrypto'21) and improve on it in several ways. First, we prove their transformation from non-adaptive to adaptive IBS in the QROM. Then, we simplify the parameters used and give concrete values. Finally, we simplify the signature scheme by using a non-homogeneous relation, which helps us reduce the size of the signature and get rid of one costly trapdoor delegation. On the whole, we get better security bounds, shorter signatures and faster algorithms.

Table of Contents

1 Introduction

Identity-Based Signatures. Secure communication over the Internet heavily relies on the use of digital signatures, which provide authenticity, integrity, and non-repudiation in an asymmetric setting. In textbook schemes, each user needs to generate its own (public key, secret key) pair, and we assume that each user is uniquely identified by its public key. In the real world, this is ensured by the use of public-key infrastructures (PKI) which map public keys to real-world identities such as names or email addresses. This usually involves a hierarchy of trusted certification authorities (CA) that can certify public keys as belonging to a certain user.

To relax the need for such heavy structures, Shamir proposed in his seminal work [30] the use of so-called *identity-based signatures* (IBS), where the public key of a user simply is its identity. The corresponding secret key is issued by a trusted authority, which derives it from a master secret key that only the authority knows, and which is assumed to have a way to verify the identity of the user. This simplifies the requirements on PKI and certificates and opens the way to more efficient schemes. In such a scheme, an honest user with identity id can sign a message μ using its secret key $\mathsf{sk}_{\mathsf{id}}$, and its signature σ can be publicly verified, given the master public key mpk and its identity id.

The usual security notion for IBS is Existential Unforgeability under Chosen Message Attack ($\mathsf{EUF\text{-}CMA}$), where an adversary $\mathcal{A}$ can obtain a set of secret keys associated to some identities and get the signatures associated to a certain number of tuples (identity, message) of its choice. It wins the security game if it is able to produce a new tuple (id, message, signature) for an identity and a message not already queried. We say it is *adaptive* if it can adaptively query the secret keys and signatures ($\mathsf{EUF\text{-}CMA}$), *non-adaptive* otherwise ($\mathsf{EUF\text{-}naCMA}$).

The security of cryptographic schemes is usually proved by reduction, meaning that if a (polynomial-time) adversary $\mathcal{A}$ is able to break the security of the scheme, then we can reduce it to another (probabilistic polynomial time) adversary $\mathcal{B}$ that is able to solve an instance of some hard problem (factoring, discrete logarithm, Short Integer Solution (SIS) [1]...). The success probability of $\mathcal{A}$ is bounded by a factor times the success probability of $\mathcal{B}$. If this factor is a small constant (and does not depend logarithmically, linearly or quadratically on the security parameter), we say that the reduction is *tight*. This is a desirable probability since a cryptographic scheme with tight reduction does not need to increase the key length to compensate a security loss. Furthermore, with the recent advances made on quantum computers, it is desirable to rely on quantum-safe hard problems, such as those based on lattices. It is sometimes possible to rely only on these hard problems, leading to schemes in the so-called *standard* model. But in order to gain efficiency, one usually relies on idealized models, such as the *random oracle model* (ROM). Its quantum equivalent is the quantum ROM (QROM), where a possibly quantum adversary is allowed to quantumly query the oracle. Finally, the goal of this article is thus to present an identity-based signature scheme with tight security, assuming the SIS problem is hard, and relying on the ROM or QROM.

Related Work. There are two main approaches used to construct IBS schemes (see [18] for more details), but none of them is directly applicable to tight post-quantum security (more discussion in [26]). The first one, called the certification approach, transforms a standard signature scheme into an IBS scheme [9,4]. The generic transformation is not tight, but can be shown tightly secure if the underlying signature scheme is tightly secure in the multi-user setting with adaptive corruption [21] (which may be applied to the post-quantum signature scheme designed in [27], but then the obtained IBS would not produce short signatures). The second one is to transform a $2-$level hierarchical IBE (HIBE) [16] tightly to an IBS scheme [18].

Overcoming these difficulties, Pan and Wagner gave in [26] the first identity-based signature scheme with tight security from lattices, and we build upon their construction by improving on

it in several ways. They give two constructions, based on either SIS [1] (unstructured lattices) or Ring-SIS [24] (structured lattices), which are two assumptions believed to be quantum-safe. The latter one offers better efficiency. Their signatures are short, meaning that they contain only a constant number of elements, with a size independent of the message length. They use the Micciancio-Peikert (MP) trapdoor technique [25] and the Bonsai tree technique [6].

They first give a generic transformation trans from a non-adaptive IBS to an adaptive one. They use the known transformation for digital signature schemes [19] using (R)SIS-based chameleon hash [6,12] and extend it to the IBS setting ([26, Theorem 1]). They also give a version in the ROM ([26, Theorem 2]), which is more efficient.

Then, they construct a non-adaptive IBS proved in the ROM and in the QROM, assuming the (R)SIS assumption is hard. In a nutshell, the master public key is a random matrix $\mathbf{A}$ such that the (R)SIS assumption holds, the master secret key is a MP trapdoor $\mathbf{T_A}$ for $\mathbf{A}$ [25], the identity secret key for id is a trapdoor of $(\mathbf{A}\|\mathsf{H}_1(\mathsf{id}))$ obtained through $\mathbf{T_A}$ using the trapdoor delegation operation of MP and a signature of a tuple (id, μ) is a small vector $\mathbf{z}$ computed using the trapdoor such that $(\mathbf{A}\|\mathsf{H}_1(\mathsf{id})\|\mathsf{H}_2(\mathsf{id}, \mu))\,\mathbf{z} = 0$, where H_1 and H_2 are simulated as random oracles in the security proof. This finally gives rise to an adaptive IBS in the ROM, and an adaptive IBS in the QROM assuming chameleon hash. In the proof, the adversary has to output the lists $\mathsf{AskedSk}$ and $\mathsf{AskedSign}$ of secret key queries and signing queries before receiving the master public key (since the scheme is non-adaptive). The key points are that, by programming the random oracles H_1 and H_2, the reduction can embed a MP trapdoor into both $(\mathbf{A}\|\mathsf{H}_1(\mathsf{id}))$ and $(\mathbf{A}\|\mathsf{H}_1(\mathsf{id})\|\mathsf{H}_2(\mathsf{id}, \mu))$ for all elements of these lists, while the other values are programmed on the form $\mathbf{Ax}$ for $\mathbf{x}$ small elements, allowing to construct a SIS solution, with high probability, for any valid signature on (id^*, μ^*) not queried by $\mathcal{A}$. The programming being indistinguishable by $\mathcal{A}$ from random output. This implies that the reduction does not need to guess the forgery (id^*, μ^*), making it tight.

While preparing the final version of this paper, we came across a concurrent paper [31], which also improves the protocol of [26] as one of their contributions, by getting rid of one delegation as we do here. But as compared to our article, they only improve the non-adaptive scheme, only in the ROM case and only based on SIS. As opposed to them, we give here further improvements: We fix some flaws in the proof of [26], propose other choices of distributions, consider QROM and RSIS, lower the number of hash calls needed when applying the transformation from $\mathsf{EUF\text{-}CMA}$ to $\mathsf{EUF\text{-}naCMA}$ on it, and give a practical instantiation with concrete parameters.

Our Contributions. In this article, we improve on the work of Pan and Wagner [26] in several ways. We give here an informal description of these improvements and provide a technical overview in Section 2 for the interested reader.

We prove the generic transformation from non-adaptive to adaptive IBS of [26] in the QROM, making it unnecessary to rely on chameleon hashes in this case, we also provide a proof of this transformation in the strong security setting. We use a former reprogramming result restated in Proposition 6. Our protocols are thus more modular: all the intermediate results (reprogramming lemmas) are proved both in ROM and QROM. Furthermore, we improve the transformation by reducing the number of hash functions to 2 instead of 4, making the final scheme simpler and more efficient.

The set of parameters used is easier, since we harmonize the value of the modulus to $q = 3^k$ in both structured and unstructured case, as opposed to [26] which used q prime in the latter case. The main interest is to simplify the use of the MP trapdoor generation algorithms [25], and in particular to get a simpler gadget matrix (of the form $[\mathsf{I}_n\ 3\mathsf{I}_n\ \ldots\ 3^{k-1}\mathsf{I}_n]$ in the unstructured case). This comes at the cost of a more difficult proof for the smoothness lemma (Lemma 1).

We make an effort to be "concrete" and avoid universal constants and asymptotic parameters, giving parameters in Tables 6 and 7. Note that the two former improvements can be directly applied to the scheme given in [26], which enables us to compare both schemes fairly.

Our scheme is simpler thanks of the use of a non-homogeneous equation for the signature. With the same notations as above, a signature of a tuple (id, μ) is a small vector $\mathbf{z}$ such that $(\mathbf{A} \| \mathsf{H}_1(\mathsf{id}))\,\mathbf{z} = \mathsf{H}_2(\mathsf{id}, \mu)$ (as compared to $(\mathbf{A} \| \mathsf{H}_1(\mathsf{id}) \| \mathsf{H}_2(\mathsf{id}, \mu))\,\mathbf{z} = 0$), again obtained using the trapdoors of [25]. This has two consequences. First, the signature has fewer coordinates. Then, this allows us to manage to avoid the use of one trapdoor delegation operator $\mathsf{DelTrap}$ in Sign, that only consist on a sole application of $\mathsf{SampleD}$. Indeed, we now use the secret matrix to sample the vector $\mathbf{z}$ following a discrete Gaussian distribution, meaning that we can reuse the trapdoor of the secret matrix whereas the scheme in [26] uses a more complex concatenated matrix, forcing them to delegate one more time a trapdoor. This is obtained at the cost of a more difficult proof, especially in the QROM case. More precisely, we give thinner reprogramming lemmas, of independent interest (see Section 4.4). Another improvement of these lemmas is that we do not always reprogram using a Gaussian distribution, but rather a uniform distribution on $\{-1, 0, 1\}$ whenever it is possible. In particular, to obtain the result in the structured case, we give an improved version of Regev's claim [29, Claim 5.3] for more general distributions, in Lemma 18, that is applied in Proposition 1 for our case.

Keeping in mind that one $\mathsf{DelTrap}$ operation roughly corresponds to k $\mathsf{SampleD}$ operations, a first consequence of this simplification is that the time complexity of our signature scheme is at least k times better. Experimentally, this leads to a scheme at least 65 times faster for the same parameters assuming a 128-bit security for our scheme.

A second consequence is that the security we obtain is better, because we get a smaller (R)SIS bound. This implies that the parameters we need to obtain 128-bit security only yields 37-bit security for their improved scheme.

A third consequence is that the signatures generated by our schemes are way shorter than the ones generated in [26], because the use of only one trapdoor delegation yields to a smaller standard deviation for the signature, and that we have k fewer coordinates for the signature by design. Experimentally, this leads to a signature half as big, if we use the same parameters for both schemes. If we consider the same security for both schemes, we even get signatures and keys five times smaller than theirs.

Other contributions of independent interest. We highlight a few contributions made for this article that could be used in other contexts:

- We give an extended version of Regev's claim [29, Claim 5.3], proven for more general distributions and in a module setting. It is stated and proved in Lemma 18.
- We generalize the reprogrammation lemma [5, Lemma 3] in Proposition 7, in order to replace a quantum random oracle by a bounded number of distributions that are close to the random distribution. In the initial lemma, there were only two possible distributions.
- We introduce a lemma applicable to a wide class of indistinguability games, that allows to separate the study of classic and quantum calls to the quantum random oracle, provided the classic calls are made first. It is stated and proved in Section B.5.
- We prove different results regarding the infinity norm of the minimum of (some) unstructured q-lattices with q power of a prime, in Appendix B.3 . Then, we use it to prove a variation of the smoothness lemma [15, Lemma 5.2] for q-ary lattices with q being a power of 3.
- We show a simple characterization of (some) invertibles of $\mathcal{R}_q$ for q being a power of 3, in Appendix B.2.
- To simulate distributions obtained with delegated trapdoors, Proposition 5 and Proposition 4 (such as their counterparts for the structured case, in Appendix B.9) are implicitly used in [26] and needed in our scheme. They have an important role to ensure the ability to simulate the

correct distributions to an adversary against a scheme without master secret key. They are described in Section 4.

Acknowledgements. This work was supported in part by the French ANR projects CryptiQ (ANR-18- CE39-0015) and SecNISQ (ANR-21-CE47-0014). Pierrick Méaux was supported by the ERC Advanced Grant no. 787390.

2 Technical Overview

We focus here on the scheme based on the SIS assumption, the ideas being similar for the scheme based on RSIS.

Following [26], we proceed in two steps: first a generic transformation from an EUF-naCMA IBS scheme to an EUF-CMA scheme and then the construction of an EUF-naCMA IBS scheme.

Generic Transformation.

In [26], the authors show that, using a chameleon hash or in the ROM, the non-adaptive security of an IBS scheme can be tightly transformed into adaptive security.

This implies that the only way to get a scheme secure against a quantum adversary is to use both chameleon hashes and other hash functions simulated as quantum random oracles in the proof. In this article, we extend this generic transformation to the QROM with a compatible-with-ROM case proof, using some adaptive reprogramming results of [17] (restated in Proposition 6).

We can then apply this transformation to our scheme, yielding to a scheme proved in the sole QROM. Furthermore, it is possible to factor these hash functions to reduce their number from four to two, which allows getting a scheme in which fewer queries to hash functions are made.

IBS with Non-Adaptive Security.

In order to exploit the transformation described above, we construct a (weaker) non-adaptively secure IBS scheme, in which an adversary has to commit its user secret key queries and signing queries before receiving the master public key. This weaker security gives rise to a tight construction since in the security proof, the adversary's user secret key queries and signing queries are known in advance. It is thus possible to tightly embed in the reduction the SIS instances in the forgery without having to guess anything.

Description of the Scheme. Similarly to [26], our scheme uses the trapdoor setup of [25] that allows to:

- Instantiate a trapdoor: create a couple of matrix and trapdoor $(\mathbf{A}, \mathbf{T_A})$, where $\mathbf{A}$ looks random (meaning that its statistical distance with the uniform distribution is negligible).
- Delegate a trapdoor: for any matrix $\mathbf{A'}$ and trapdoor $\mathbf{T_A}$ of $\mathbf{A}$, "delegate" the trapdoor $\mathbf{T_A}$ into a trapdoor $\mathbf{T'_A}$ of $(\mathbf{A}\|\mathbf{A'})$, that reveals no information about $\mathbf{T_A}$.
- Perform Gaussian sampling: for any $\mathbf{A}$, trapdoor $\mathbf{T_A}$ of $\mathbf{A}$, vector $\mathbf{u}$ and sufficiently big s, create $\mathbf{x}$ following a discrete Gaussian distribution and verifying $\mathbf{Ax} = \mathbf{u}$. Furthermore, the lower bound of s is linear in the singular value of $\mathbf{T_A}$, up to a negligible term.

Each of these operations is in correspondence with one of the algorithms of our IBS:

- The master public key $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and secret key $\mathbf{T_A} \in \mathbb{Z}_q^{(m-nk)\times nk}$ correspond to the matrix and trapdoor created by the trapdoor instantiation.
- The creation of a secret key for an identity id is done by delegating the trapdoor $\mathbf{T_A} \in \mathbb{Z}_q^{m\times nk}$ of $\mathbf{A}$ into a trapdoor of $\mathbf{T}_{\mathsf{id}}$ of $(\mathbf{A}\|\mathsf{H}_1(\mathsf{id})) \in \mathbb{Z}_q^{n\times(m+nk)}$, for H_1 with values in $\mathbb{Z}_q^{n\times nk}$.
- The signature of a message μ with $\mathsf{sk}_{\mathsf{id}} = \mathbf{T}_{\mathsf{id}}$ corresponds to the Gaussian sampling of a vector $\mathbf{z}$ such that $(\mathbf{A}\|\mathsf{H}_1(\mathsf{id}))\mathbf{z} = \mathsf{H}_2(\mu)$, for H_2 with values in $\mathbb{Z}_q^n$.

The main difference of our scheme as compared to that of [26] is that their signing algorithm requires one more trapdoor delegation operation before doing the Gaussian sampling relatively to this new trapdoor, which explains the better values for parameters and security for our scheme.

More precisely, to sign a message μ for an identity id of secret key $\mathbf{T}_{\mathsf{id}}$, their scheme requires delegating $\mathbf{T}_{\mathsf{id}}$ into a trapdoor $\mathbf{T}_{\mathsf{id},\mu}$ of $(\mathbf{A}\|\mathsf{H}_1(\mathsf{id})\|\mathsf{H}_2(\mathsf{id},\mu))$ (H_2 with values in $\mathbb{Z}_q^{n\times nk}$ in their scheme), then using $\mathbf{T}_{\mathsf{id},\mu}$ to make a Gaussian sampling of a small vector $\mathbf{z}$ such that

$$(\mathbf{A}\|\mathsf{H}_1(\mathsf{id})\|\mathsf{H}_2(\mathsf{id},\mu))\mathbf{z} = 0$$

This makes their signature bigger, on the one hand because it contains an additional component and on the other hand because it uses a bigger delegated matrix $\mathbf{T}''_{\mathbf{A}}$, because of the double delegation. This double delegation also has an impact on the SIS bound in their reduction, which is smaller for our scheme. Finally, the additional delegation operation augments the time complexity of their signature, that can be estimated as at least k time slower than ours, as explained in Section 8.1.

Idea of the Proof. Our tight proof follows the same blueprint for QROM and ROM. We denote the list of all identities id for user secret key queries as $\mathsf{AskedSk}$, and the list of all identity-message pairs (id,μ) for signing queries as $\mathsf{AskedSign}$. An adversary $\mathcal{A}$ has to output these two lists before receiving the master public key. The key step in our proof is that, by programming the random oracles H_1 and H_2, it is possible to simulate the $\mathsf{EUF\text{-}naCMA}$ game for a random $\mathbf{A}$ (without the secret key $\mathbf{T}_{\mathbf{A}}$) by hiding the signatures and secret identity keys in the hash values. More precisely, the idea is to embed a trapdoor $\mathbf{T}_{\mathsf{id}}$ (*i.e.* a secret key for identity id) into the values $\mathsf{H}_1(\mathsf{id})$ for $\mathsf{id} \in \mathsf{AskedSk}$ and a signature of (id,μ), for the values $\mathsf{H}_2(\mu,\mathsf{id})$ for all $(\mu,\mathsf{id}) \in \mathsf{AskedSign}$.

Moreover, for any $\bar{\mathsf{id}} \notin \mathsf{AskedSk}$, $(\tilde{\mathsf{id}},\tilde{\mu}) \notin \mathsf{AskedSign}$, we program $\mathsf{H}(\bar{\mathsf{id}}) = \mathbf{A}\mathbf{R}_{\bar{\mathsf{id}}}$ and $\mathsf{H}(\tilde{\mathsf{id}},\tilde{\mu}) = \mathbf{A}\tilde{\mathbf{z}}_{\mathsf{id},\mu}$ for some small random matrix $\mathbf{R}_{\bar{\mathsf{id}}}$ and vector $\tilde{\mathbf{z}}_{\mathsf{id},\mu}$. Note that we use different distributions than [26], which contributes to lower the size of the SIS bound. Thus, a valid signature $\mathbf{z}^* = (\mathbf{z}_1^*,\mathbf{z}_2^*)$ of $\mathcal{A}$ for a couple of identity and message (id,μ) such that $\mathsf{id} \notin \mathsf{AskedSk}$, $(\mu,\mathsf{id}) \notin \mathsf{AskedSign}$ leads to an SIS solution $\mathbf{x} = \mathbf{z}_1^* + \mathbf{R}_{\mathsf{id}^*}\mathbf{z}_2^* - \mathbf{z}_{\mathsf{id}^*,\mu^*}$ provided that $\mathbf{x} \neq 0$, because, by definition of the signature verification, $\mathbf{A}\mathbf{z}_1^* + \mathsf{H}_1(\mathsf{id})\mathbf{z}_2^*\mathbf{z} = \mathsf{H}_2(\mu)$. Finally, we ensure that $\mathbf{x} = 0$ does not happen more than half of the time by using an indistinguishability technique of [23].

3 Preliminaries

The non-negative integers, integers and reals are respectively denoted by $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{R}$. Unless stated otherwise, we always assume $q = 3^k$ and $d = 2^u$ with $k,u \in \mathbb{N}^*$. Matrices are written as bold capital letters and vectors as low-case bold letters. Vectors should be understood as column vectors. For $a,b \in \mathbb{R}$, we define $[\![a,b]\!] = [a,b] \cap \mathbb{Z}$. For $S \subset \mathbb{R}^n$, we denote by $\mathsf{Span}(S) \subset \mathbb{R}^n$ the $\mathbb{R}$-vector space generated by S. For $\mathbf{x} \in \mathbb{R}^n$, we denote by $\|\mathbf{x}\|$ its Euclidean norm. For a predicate P, we define $[\![P]\!] = 1$ if P is true and 0 otherwise. A function $f(n)$ is negligible, written $f(n) = \mathsf{negl}(n)$, if $\forall c \in \mathbb{N}, f(n) = o(n^{-c})$. We denote log the logarithm in base 2 and $\log_b$ the logarithm in a base $b \in \mathbb{R}^*_{\geq 0}$. For $m \in \mathbb{N}^*, \epsilon > 0$, we define $\mathsf{r}_{m,\epsilon} = \sqrt{\ln\left(2m(1+1/\epsilon)\right)/\pi}$.

Modular arithmetic. For any even (*resp.* odd) $p \in \mathbb{N}^*$ and any $x \in \mathbb{Z}_p$, we will denote by $x \mod^{\pm} p$ the unique representative in $[\![-p/2, p/2]\!]$ (*resp.* $[\![-(p-1)/2, (p-1)/2]\!]$). We extend this definition to vectors and matrices entry-wise. For $x \in \mathbb{Z}_p$, we define $|x| := |x \mod^{\pm} p|$. For any $p,n,m \in \mathbb{N}^*$ and $\mathbf{A} = (a_{i,j}) \in \mathbb{Z}_p^{n\times m}$, we define $\|\mathbf{A}\|_1 = \sum_{i,j}|a_{i,j}|$, $\|\mathbf{A}\| = \sqrt{\sum_{i,j}|a_{i,j}|^2}$, $\|\mathbf{A}\|_\infty = \max_{i,j}|a_{i,j}|$. We extend this definition to vectors, considered as matrices with one column.

The Ring $\mathcal{R}_q$. We will work in $\mathcal{R} = \mathbb{Z}[X]/(X^d+1)$ and $\mathcal{R}_q = \mathbb{Z}_q[X]/(X^d+1)$ for d a power of 2. We define $\mathcal{S}_{\mathsf{R}} = \{\sum_{i=0}^{d-1} a_i X^i \in \mathcal{R} \colon (a_0, \ldots, a_{d-1}) \in \{-4,0,4\}^{d/4} \times \{-1,0,1\}^{d/2} \times \{-4,0,4\}^{d/4}\} \subset \mathcal{R}$. We will consider it as a subset of $\mathcal{R}_{3^k}$ for all $k \geq 2$. For $a \in \mathcal{R}$, we will denote by $\mathsf{Cf}(a) \in \mathbb{Z}^d$ the vector whose coordinates are the coefficients of a and $\mathsf{Rot}(a) \in \mathbb{Z}^{d\times d}$ the matrix whose lines are $\mathsf{Cf}(a), \mathsf{Cf}(Xa), \ldots, \mathsf{Cf}\big(X^{d-1}a\big)$. We extend this definition for matrix $\mathbf{A} \in \mathcal{R}^{n\times m}$, that leads to $\mathsf{Cf}(\mathbf{A}) \in \mathbb{Z}^{n\times dm}$ and $\mathsf{Rot}(\mathbf{A}) \in \mathbb{Z}^{dn\times dm}$. We also extend this definition modulo q by $\mathsf{Cf}(\mathbf{A} \bmod q) := \mathsf{Cf}(\mathbf{A}) \bmod q$.

General Probabilities. In this article, we only consider discrete probability distributions. If Dist is a probability distribution, $x \leftarrow\!\!\$\ \mathsf{Dist}$ denotes that x is sampled from Dist. The support of a probability distribution is the set of x such that $\Pr[\mathsf{Dist} = x] > 0$. Unless specified otherwise, all the probability distributions we work with have finite support. If S is a set, $x \leftarrow\!\!\$\ S$ means that x is sampled uniformly in S and $\mathsf{U}(S)$ denote the uniform distribution on S. For sets $S \subset X$ and Dist a probability distribution with values in X, we denote by $\mathsf{Dist}_{|S}$ the probability distribution $x \leftarrow\!\!\$\ \mathsf{Dist}$ conditioned to $x \in S$. For two probability distributions $\mathsf{Dist}, \mathsf{Dist}'$ with support in a set X, we define their statistical distance $\mathsf{SD}\big(\mathsf{Dist}, \mathsf{Dist}'\big) = \frac{1}{2}\sum_{x\in X} \big|\Pr[\mathsf{Dist} = x] - \Pr\big[\mathsf{Dist}' = x\big]\big|$. To help the reading of the article, some generic results about statistical distance are stated in Appendix A.1. For $r \in]0,1[$, we denote by $\mathcal{P}_r$ the probability distribution such that $\Pr[\mathcal{P}_r = 0] = r, \Pr[\mathcal{P}_r = -1] = \Pr[\mathcal{P}_r = 1] = (1-r)/2$. Finally, we denote by $\mathcal{P}_{\mathcal{R},1/2}$ the probability distribution $4\mathcal{P}_{1/2}^{d/4} \times \mathcal{P}_{1/2}^{d/2} \times 4\mathcal{P}_{1/2}^{d/4}$ with support $\mathcal{S}_{\mathsf{R}}$.

Lattices. A lattice of dimension $k \in \mathbb{N}$ is a $\mathbb{Z}$-submodule $\Lambda \subset \mathbb{R}^k$ that is finitely generated. It is said full rank if $\mathsf{Span}(\Lambda) = \mathbb{R}^k$. A $\mathcal{R}$-lattice of dimension k is defined as a $\mathcal{R}$-submodule of $\Lambda \subset \mathcal{R}^k$. Note that a $\mathcal{R}$-lattice of dimension k becomes a lattice of dimension kd under Cf. We will often identify $\mathcal{R}$-lattices with their associated lattice through Cf and call them (structured) lattices. For $\mathbf{A} \in \mathbb{Z}_q^{n\times k}, \mathbf{u} \in \mathbb{Z}_q^n$, $\mathbf{B} \in \mathcal{R}_q^{n\times k}, \mathbf{v} \in \mathcal{R}_q^n$, we define the following full-rank lattices

$$\Lambda_q(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^n \colon \exists\, \mathbf{s},\ \mathbf{x} = \mathbf{A}\mathbf{s} \bmod q\},\ \Lambda_{\mathbf{u},q}^{\perp}(\mathbf{A}) := \{\mathbf{x} \in \mathbb{Z}^k \colon \mathbf{A}\mathbf{x} = \mathbf{u} \bmod q\}\ ,$$
$$\Lambda_{\mathcal{R},q}(\mathbf{B}) = \{\mathbf{x} \in \mathcal{R}^n \colon \exists\, \mathbf{s},\ \mathbf{x} = \mathbf{B}\mathbf{s} \bmod q\},\ \Lambda_{\mathbf{v},\mathcal{R},q}^{\perp}(\mathbf{B}) = \{\mathbf{x} \in \mathcal{R}^k \colon \mathbf{B}\mathbf{x} = \mathbf{v} \bmod q\}\ .$$

We write $\Lambda_q^{\perp}(\mathbf{A})$ (resp $\Lambda_{\mathcal{R},q}^{\perp}(\mathbf{B})$) if $\mathbf{u} = 0$ (*resp.* $\mathbf{v} = 0$). The dual Λ^* of a full rank lattice Λ of dimension k is the set of all $\mathbf{v} \in \mathbb{R}^k$ such that $\mathbf{x}^\top\mathbf{v} \in \mathbb{Z}$ for all $\mathbf{x} \in \Lambda$. We have $q\Lambda_q^{\perp}(\mathbf{A})^* = \Lambda_q(\mathbf{A}^\top)$.

SIS and RSIS problems. Consider $n, m, \beta, q \in \mathbb{N}^* \times \mathbb{N}^* \times \mathbb{R} \times \mathbb{N}^*$. The $\mathsf{SIS}_{n,m,\beta,q}$ problem is defined as follows: for $\mathbf{A} \leftarrow\!\!\$\ \mathbb{Z}_q^{n\times m}$, find $\mathbf{z} \in \mathbb{Z}_q^m$ such that $\mathbf{A}\mathbf{z} = 0 \bmod q$ and $\|z\| \leq \beta$. The $\mathsf{RSIS}_{n,\beta,q}$ problem is defined as follows: for $\mathbf{A} \leftarrow\!\!\$\ \mathcal{R}_q^{1\times n}$, find $\mathbf{z} \in \mathcal{R}_q^n$ such that $\mathbf{A}\mathbf{z} = 0 \bmod q$ and $\|z\| \leq \beta$.

The SIS and RSIS problems are assumed to be hard to solve for quantum adversaries (*e.g.* [28]).

Discrete Gaussian Distribution. For $\mathbf{x} \in \mathbb{R}^n, s > 0$, we define $\rho_s(x) = \exp\left(-\pi\|\mathbf{x}\|^2/s^2\right)$. For a lattice $\Lambda \subset \mathbb{R}^n$, $\mathbf{c} \in \mathbb{R}^n$ and $s > 0$, the discrete Gaussian distribution $\mathcal{D}_{\Lambda+\mathbf{c},s^2}$ is the probability distribution with support $\Lambda + \mathbf{c}$ such that, for all $\mathbf{x} \in \Lambda + \mathbf{c}$, $\mathcal{D}_{\Lambda+\mathbf{c},s}(x)$ is proportional to $\rho_s(\mathbf{x})$. When $\Lambda + \mathbf{c} \subset \mathbb{Z}^n$, we have $\mathcal{D}_{\Lambda+\mathbf{c},s} = \mathcal{D}^n_{\mathbb{Z},s|\Lambda+\mathbf{c}}$. For a $\mathcal{R}_q$-lattice $\Lambda \subset \mathcal{R}_q^n$, $\mathbf{c} \in \mathcal{R}_q^n$ and $s > 0$ the Gaussian distribution over Λ, denoted by $\mathcal{D}_{\Lambda,\mathbf{c},s}$, is defined as $\mathsf{Cf}^{-1}(\mathcal{D}_{\mathsf{Cf}(\Lambda),\mathsf{Cf}(\mathbf{c}),s})$. For example, $\mathcal{D}_{\mathcal{R},\mathbf{c},s} = \mathsf{Cf}^{-1}(\mathcal{D}^d_{\mathbb{Z},\mathsf{Cf}(\mathbf{c}),s})$. For $\epsilon > 0$, the smoothing parameter of a lattice Λ of dimension n, denoted by $\eta_\epsilon(\Lambda)$, is the smallest s such that $\rho_{1/s}(\Lambda^* - \{0\}) \leq \epsilon$. The smoothing parameter of a $\mathcal{R}$-lattice Λ is defined as $\eta_\epsilon(\mathsf{Cf}(\Lambda))$.

Adversary, games and oracles. PPT stands for "probabilistic polynomial time". We denote by $\mathsf{Adv}^{\mathsf{G}}_{\mathcal{A}}$ the advantage of an adversary $\mathcal{A}$ in game G. If the game is applied to a scheme S, we

write $\mathsf{Adv}^{\mathsf{G}}_{\mathcal{A},\mathsf{S}}$ or $\mathsf{Adv}^{\mathsf{G}}_{\mathcal{A}}$ if it is clear from context. We denote by $\mathcal{A}^{\mathsf{H}}$ (*resp.* $\mathcal{A}^{|\mathsf{H}\rangle}$) an adversary $\mathcal{A}$ that can make classic (*resp.* quantum) queries to a hash function H. For an oracle with possible input x and for an element y, we denote by $\mathcal{O}^{x\to y}$ the oracle defined by $\mathcal{O}^{x\to y}(z) = y$ if $z = x$ and $\mathcal{O}(z)$ otherwise.

Identity-based signature schemes and security. An Identity-Based Signature (IBS) scheme is a tuple of PPT algorithms $\mathsf{IBS} = (\mathsf{Setup}, \mathsf{KeyExt}, \mathsf{Sign}, \mathsf{Verify})$ such that:
- $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}()$ outputs a master public key and master private key.
- $\mathsf{sk}_{\mathsf{id}} \leftarrow \mathsf{KeyExt}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$ outputs a secret key for identity id.
- $\sigma \leftarrow \mathsf{Sign}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{id}}, \mu)$ outputs a signature for a message μ and identity id.
- $b \in \{0,1\} \leftarrow \mathsf{Verify}(\mathsf{mpk}, \sigma, \mu, \mathsf{id})$ is deterministic.

The scheme IBS is (ξ_1, ξ_2)-complete if for all $\mathsf{mpk}, \mathsf{msk}, \mathsf{id}, \mu$, we have

$$\underset{(\mathsf{mpk},\mathsf{msk})\leftarrow\mathsf{Setup}()}{Pr}\Big[Pr\big[\mathsf{Verify}(\mathsf{mpk},\sigma,\mu,\mathsf{id}) = 1 :\ \mathsf{sk}_{\mathsf{id}} \leftarrow \mathsf{KeyExt}(\mathsf{mpk},\mathsf{msk},\mathsf{id}),\ \sigma \leftarrow \mathsf{Sign}(\mathsf{mpk},\mathsf{sk}_{\mathsf{id}},\mu)\big] \geq 1-\xi_1\Big] \geq 1-\xi_2\ .$$

The usual security notion for IBS is Existential Unforgeability under Chosen Message Attack (EUF-CMA) (adaptive or non-adaptive), we depict the corresponding security game in Figure 1. We also define the notion of strong Existential Unforgeability. For $Q_{\mathsf{Corr}}, Q_{\mathsf{S}} \in \mathbb{N}^*$, we measure the $\mathsf{EUF\text{-}CMA}$ (*resp.* $\mathsf{sEUF\text{-}CMA}$) security of a scheme IBS against an adversary $\mathcal{A}$ that can obtain Q_{Corr} identity secret keys and Q_{S} signatures by the advantage $\mathsf{Adv}^{\mathsf{EUFCMA}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}}_{\mathcal{A}} := \Pr\big[1 \leftarrow \mathsf{EUFCMA}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}(\mathcal{A})\big]$ (*resp.* $\mathsf{Adv}^{\mathsf{sEUFCMA}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}}_{\mathcal{A}} := \Pr\big[1 \leftarrow \mathsf{sEUFCMA}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}(\mathcal{A})\big]$). Note that the signatures and keys can be adaptively queried in $\mathsf{EUFCMA}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}$, we speak of adaptive security. We will speak of strong security when using $\mathsf{sEUF\text{-}CMA}$ or $\mathsf{sEUF\text{-}naCMA}$.

$\mathsf{EUFCMA}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}/\mathsf{sEUFCMA}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}(\mathcal{A})$

$(\mathsf{mpk},\mathsf{msk}) \leftarrow \mathsf{Setup}()$
$\mathsf{cpt}_{\mathsf{C}} := 0, \mathsf{cpt}_{\mathsf{S}} := 0$
$\mathsf{AskedSk} \leftarrow \varnothing, \mathsf{AskedSign} \leftarrow \varnothing, \mathsf{sAskedSign} \leftarrow \varnothing$
$(\mathsf{id}^*, \mu^*, \sigma^*) \leftarrow \mathcal{A}^{\mathcal{O}_{\mathsf{Corrupt}},\mathcal{O}_{\mathsf{Sign}}}(\mathsf{mpk})$
if $\mathsf{id}^* \in \mathsf{AskedSk}$
  $\vee\ (\mathsf{id}^*, \mu^*) \in \mathsf{AskedSign}$ // for EUF-CMA
  $\vee\ (\mathsf{id}^*, \mu^*, \sigma^*) \in \mathsf{sAskedSign}$ // for sEUF-CMA
  $\vee\ \mathsf{cpt}_{\mathsf{C}} > Q_{\mathsf{Corr}} \vee \mathsf{cpt}_{\mathsf{S}} > Q_{\mathsf{S}}$ **then**
  return 0
return $\mathsf{Verify}(\mathsf{mpk}, \mathsf{id}^*, \mu^*, \sigma^*)$

$\mathcal{O}_{\mathsf{Sign}}(\mathsf{id}, \mu)$

$\mathsf{cpt}_{\mathsf{S}} := \mathsf{cpt}_{\mathsf{S}} + 1$
$\mathsf{sk}_{\mathsf{id},\mu} \leftarrow \mathsf{KeyExt}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$
$\sigma_{\mathsf{id},\mu} \leftarrow \mathsf{Sign}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{id},\mu}, \mu)$
$\mathsf{AskedSign} = \mathsf{AskedSign} \cup \{(\mathsf{id}, \mu)\}$ // for EUF-CMA
$\mathsf{sAskedSign} = \mathsf{sAskedSign} \cup \{(\mathsf{id}, \mu, \sigma_{\mathsf{id},\mu})\}$ // for sEUF-CMA
return $\sigma_{\mathsf{id},\mu}$

$\mathcal{O}_{\mathsf{Corrupt}}(\mathsf{id})$

$\mathsf{AskedSk} := \mathsf{AskedSk} \cup \{\mathsf{id}\}$
$\mathsf{cpt}_{\mathsf{C}} := \mathsf{cpt}_{\mathsf{C}} + 1$
$\mathsf{sk}_{\mathsf{id}} \leftarrow \mathsf{KeyExt}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$
return $\mathsf{sk}_{\mathsf{id}}$

$\mathsf{EUFnaCMA}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}/\mathsf{sEUFnaCMA}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}(\mathcal{A})$

$(\mathsf{mpk},\mathsf{msk}) \leftarrow \mathsf{Setup}()$
$(\mathsf{AskedSk}, \mathsf{AskedSign}, \mathsf{aux}) \leftarrow \mathcal{A}_1(\mathsf{mpk})$
if $|\mathsf{AskedSk}| > Q_{\mathsf{Corr}}$
  $\vee\ |\mathsf{AskedSign}| > Q_{\mathsf{S}}$ **then**
  return 0
for $\mathsf{id} \in \mathsf{AskedSk}$:
  $\mathsf{sk}_{\mathsf{id}} \leftarrow \mathsf{KeyExt}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$
for $(\mathsf{id}, \mu) \in \mathsf{AskedSign}$:
  $\mathsf{sk}_{\mathsf{id},\mu} \leftarrow \mathsf{KeyExt}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$
  $\sigma_{\mathsf{id},\mu} \leftarrow \mathsf{Sign}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{id},\mu}, \mu)$
$\mathsf{GivenSk} = \{(\mathsf{id}, \mathsf{sk}_{\mathsf{id}}), \mathsf{id} \in \mathsf{AskedSk}\}$
$\mathsf{GivenSign} = \big\{(\mathsf{id}, \mu, \sigma_{\mathsf{id},\mu}),$
  $(\mathsf{id}, \mu) \in \mathsf{AskedSign}\big\}$
$(\mathsf{id}^*, \mu^*, \sigma^*) \leftarrow \mathcal{A}_2(\mathsf{mpk}, \mathsf{GivenSk},$
  $\mathsf{GivenSign}, \mathsf{aux})$
if $\mathsf{id}^* \in \mathsf{AskedSk}$
  $\vee\ (\mathsf{id}^*, \mu^*) \in \mathsf{AskedSign}$ **then** // for EUF-naCMA
  $\vee\ (\mathsf{id}^*, \mu^*, \sigma^*) \in \mathsf{GivenSign}$ **then** // for sEUF-naCMA
  return 0
return $\mathsf{Verify}(\mathsf{mpk}, \mathsf{id}^*, \mu^*, \sigma^*)$

Fig. 1. $\mathsf{EUFCMA}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}/\mathsf{sEUFCMA}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}$ and $\mathsf{EUFnaCMA}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}/\mathsf{sEUFnaCMA}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}$ games.

For $Q_{\mathsf{Corr}}, Q_{\mathsf{S}} \in \mathbb{N}^*$, we measure the EUF-naCMA (*resp.* sEUF-naCMA) security against an adversary $\mathcal{A}$ that can obtain Q_{Corr} identity secret keys and Q_{S} signature by the advantage $\mathsf{Adv}^{\mathsf{EUFnaCMA}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}}_{\mathcal{A}} := \Pr\big[1 \leftarrow \mathsf{EUFnaCMA}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}(\mathcal{A})\big]$ (*resp.* by the advantage $\mathsf{Adv}^{\mathsf{sEUFnaCMA}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}}_{\mathcal{A}} := \Pr\big[1 \leftarrow \mathsf{sEUFnaCMA}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}(\mathcal{A})\big]$). Note that the signatures and keys have to be queried at the beginning in $\mathsf{EUFnaCMA}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}$ (*resp.* $\mathsf{sEUFnaCMA}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}$), we speak of non-adaptive security.

Singular values and bounds on singular values. The singular value $\mathsf{s}_1(\mathbf{A})$ of a matrix $\mathbf{A} \in \mathbb{R}^{n\times m}$ is defined by $\sup_{\mathbf{x}\neq 0} \frac{\|\mathbf{Ax}\|}{\|\mathbf{x}\|}$. We extend the definition of singular values of matrices with coefficients in $\mathbb{R}$ to matrices with coefficients in $\mathcal{R}$ by taking $\mathsf{s}_1(\mathbf{A}) := \mathsf{s}_1(\mathsf{Cf}(\mathbf{A}))$.

4 Preliminary results

In this section we recall notions and provide technical results that are necessary to prove the security of the generic transformation in Section 5 and IBS schemes in Section 6 and Section 7.

4.1 Results on statistical distance

For the security of the IBS scheme, we will use a game-based proof where the statistical distance between uniform distributions and other distributions are crucial for the main argument of the

proof. We define these distributions and bound their probability of being close to the uniform distribution. More precisely, Proposition 1 contains results inspired of [29, Claim 5.3] regarding the leftover hash lemma, we generalize this result and prove it in Appendix B.6. Then, Lemma 1 states variations of smoothness [15, Lemma 5.2] for the structured and unstructured case with $q = 3^k$.

For $s > 0$, $m, n, k, l \in \mathbb{N}$, $\mathbf{A} \in \mathbb{Z}_q^{n\times m}, \mathbf{B} \in \mathcal{R}_q^{1\times l}$, we define:

- $\mathcal{D}^k_{\mathbb{Z},s,\mathbf{A}}$ the probability distribution that outputs $\mathbf{AR}$ for $\mathbf{R} \hookleftarrow \$\ \mathcal{D}^{n\times k}_{\mathbb{Z},s}$ and $\mathcal{D}^k_{\mathcal{R},s,\mathbf{B}}$ the probability distribution that outputs $\mathbf{BR}$ for $\mathbf{R} \hookleftarrow \$\ \mathcal{D}^{n\times k}_{\mathcal{R},s}$ (we omit k in the notation if $k = 1$).
- $\mathcal{U}_{\mathbf{A}}$ the probability distribution that outputs $\mathbf{Ax}$, where $\mathbf{x} \hookleftarrow \$\ \{-1, 0, 1\}^m$ and $\mathcal{U}_{\mathcal{R},\mathbf{B}}$ the probability distribution that outputs $\mathbf{Bx}$ where $\mathbf{x} \hookleftarrow \$\ \mathcal{S}^l_{\mathsf{R}}$ and
- $\mathcal{P}_{\mathbf{A}}$ the probability distribution that outputs $\mathbf{Ax}$, where $\mathbf{x} \hookleftarrow \$\ \mathcal{P}^m_{1/2}$ and $\mathcal{P}_{\mathcal{R},\mathbf{B}}$ the probability distribution that outputs $\mathbf{Bx}$, where $\mathbf{x} \hookleftarrow \$\ \mathcal{P}^l_{\mathcal{R},1/2}$.

Proposition 1 (Proof in Appendix B.6.). *Let $m, n, k, l \in \mathbb{N}, q = 3^k$, with $k \geq 4$, $m \geq 2nk$ and $l \geq \max(2k, 21)$. Then,*

$$\begin{aligned}
&\Pr_{\mathbf{A}\in\mathbb{Z}_q^{n\times m}}\left[\mathsf{SD}\left(\mathsf{U}\left(\mathbb{Z}_q^n\right), \mathcal{U}_{\mathbf{A}}\right) > q^{-\frac{n}{4}}\right] \leq q^{-\frac{n}{4}}, \ \Pr_{\mathbf{A}\in\mathcal{R}_q^{1\times l}}\left[\mathsf{SD}\left(\mathsf{U}\left(\mathcal{R}_q\right), \mathcal{U}_{\mathcal{R},\mathbf{A}}\right) > q^{-\frac{d}{4}}\right] \leq q^{-\frac{d}{4}},\\
&\Pr_{\mathbf{A}\in\mathbb{Z}_q^{n\times m}}\left[\mathsf{SD}\left(\mathsf{U}\left(\mathbb{Z}_q^n\right), \mathcal{P}_{\mathbf{A}}\right) > q^{-0.196n}\right] \leq q^{-0.196n}, \ \Pr_{\mathbf{A}\in\mathbb{Z}_q^{n\times m}}\left[\mathbf{A}\mathbb{Z}_q^m \neq \mathbb{Z}_q^n\right] \leq q^{\frac{n(2k-1)}{4k}},\\
&\Pr_{\mathbf{A}\in\mathcal{R}_q^{1\times l}}\left[\mathsf{SD}\left(\mathsf{U}\left(\mathcal{R}_q\right), \mathcal{P}_{\mathcal{R},\mathbf{A}}\right) > q^{-0.196d}\right] \leq q^{-0.196d}, \ \Pr_{\mathbf{A}\in\mathcal{R}_q^{1\times l}}\left[\mathbf{A}\mathcal{R}_q^l \neq \mathcal{R}_q\right] \leq q^{-\frac{d(k-1)}{2k}} \ .
\end{aligned}$$

Lemma 1 (Smoothness lemma. Proof in Appendix B.3.). *Let $n, m, k \in \mathbb{N}$, $q = 3^k$, $m \geq 2nk$. Let $\epsilon \in]0, 1/2[$ and $s \in \mathbb{R}$ such that $s \geq 12\mathsf{r}_{m,\epsilon}$. Then,*

$$\Pr_{\mathbf{A}\in\mathbb{Z}_q^{n\times m}}\left[\mathsf{SD}\left(\mathcal{D}_{s,\mathbf{A}}, \mathsf{U}\left(\mathbb{Z}_q^n\right)\right) > 2\epsilon\right] \leq 2q^{-n/4} \ . \tag{1}$$

Let d a power of 2, $2k + k/2 \geq l > 2k$ and $s \geq 12\mathsf{r}_{ld,\epsilon}$. Then,

$$\Pr_{\mathbf{A}\in\mathcal{R}_q^{1\times l}}\left[\mathsf{SD}\left(\mathcal{D}_{s,\mathbf{A}}, \mathsf{U}\left(\mathcal{R}_q\right)\right) > 2\epsilon\right] \leq q^{-d/4} + 3^{-d\frac{(2k-l)}{2}} \leq 2 * 3^{-d\frac{(2k-l)}{2}} \ . \tag{2}$$

4.2 Singular values of random matrix

Let $C = 8e^{1+2/e}\sqrt{\ln(9)}/\sqrt{\pi} < 38$ and $f(m, n) = \sqrt{m} + 2\pi\ C\ \left(\sqrt{n} + \sqrt{m\ln(3)}\right)$. We will use $\mathsf{s}_1(\mathsf{Unif})[n, m] := \sqrt{2/3}f(m, n)$, $\mathsf{s}_1(\mathsf{Gauss})[n, m, s] := \frac{s}{\sqrt{2\pi}}f(m, n)$, and $\mathsf{s}_1(\mathsf{Binom})[n, m, r] := \sqrt{(1-r)}f(m, n)$.

Corollary 1 (Corollary of [13, Theorem 6.1] and Lemma 8, proof in Appendix B.1.). *Let $n, m, k \in \mathbb{N}$, $q = 3^k$. Let $s \in]0, 1[, a \in \mathbb{Z}^*$. Then*

$$\begin{aligned}
\Pr_{\mathbf{R}\hookleftarrow\$\mathsf{U}\left(\{-a,0,a\}^{n\times m}\right)}[\mathsf{s}_1(\mathbf{R}) \leq a\mathsf{s}_1(\mathsf{Unif})[n, m]] &\geq 1 - 2 * 3^{-m} \ ,\\
\Pr_{\mathbf{R}\hookleftarrow\$\mathcal{D}^{n\times m}_{\mathbb{Z},s}}[\mathsf{s}_1(\mathbf{R}) \leq a\mathsf{s}_1(\mathsf{Gauss})[n, m, s]] &\geq 1 - 2 * 3^{-m} \ ,\\
\Pr_{\mathbf{R}\hookleftarrow\$\mathcal{P}^{n\times m}_r}[\mathsf{s}_1(\mathbf{R}) \leq a\mathsf{s}_1(\mathsf{Binom})[n, m, r]] &\geq 1 - 2 * 3^{-m} \ .
\end{aligned}$$

This can be applied in the ring case, by sampling from the distributions $\mathsf{U}(\mathcal{S}_{\mathsf{R}})$, $\mathcal{D}_{\mathcal{R},s}$ and $\mathcal{P}_{\mathcal{R},r}$. Note that in order to find an upper bound for $\mathsf{U}(\mathcal{S}_{\mathsf{R}})$ and $\mathcal{P}_{\mathcal{R},r}$, the corollary needs to be applied with respectively products of $\mathsf{U}(\{-4, 0, 4\})$ and products of $4\mathcal{P}_r$.

4.3 Lattice trapdoors

The IBS schemes presented in the article follow the framework of [25] using trapdoor delegation. In this part we recall the results necessary to instantiate the framework, and prove the adaptations for the cases we consider. More precisely, we use Proposition 2 to instantiate the trapdoor used to create the master key. Note that we use the binomial distribution instead of the Gaussian one in [25] for compactness. Then, we use Proposition 3 to delegate trapdoors and perform Gaussian sampling, to create respectively the secret keys of identities and signatures. Finally, we give two propositions (Proposition 4, Proposition 5) necessary for the simulation in the game-based proof, and motivated by the identity-based property of the signature scheme.

Let $\mathbf{g} = (1, 3, \ldots, 3^{k-1}) \in \mathcal{R}^k$ and $\mathbf{G} = [\mathsf{I}_n \; 3\mathsf{I}_n \; \ldots \; 3^{k-1}\mathsf{I}_n] \in \mathbb{Z}^{n \times nk}$. A $\mathbf{G}$-trapdoor of a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ is a matrix $\mathbf{T_A} \in \mathbb{Z}_q^{(m-nk) \times nk}$ such that $\mathbf{A} \begin{pmatrix} -\mathbf{T_A} \\ \mathsf{I}_{nk} \end{pmatrix} = \mathbf{G} \bmod q$. A $\mathbf{g}$-trapdoor of a matrix $\mathbf{A} \in \mathcal{R}_q^{1 \times l}$ is a matrix $\mathbf{T_A} \in \mathcal{R}_q^{(l-k) \times k}$ such that $\mathsf{Rot}(\mathbf{T_A}) \in \mathbb{Z}_q^{d(l-k) \times dk}$ is a $\mathbf{G}$-trapdoor of $\mathsf{Rot}(\mathbf{A}) \in \mathbb{Z}_q^{d \times dl}$. Equivalently, using the definition and properties[6] of Rot, $\mathbf{A} \begin{pmatrix} -\mathbf{T_A} \\ \mathsf{I}_k \end{pmatrix} = \mathbf{g} \bmod q$.

Proposition 2 (Statistical instantiation of trapdoors (adapted from [25, Section 5.2])). *Let $n, m, k \in \mathbb{N}^*$, $q = 3^k$, $m \geq 2kn$. Let $\mathsf{Trap}(n, m, q)$ the algorithm that samples $\overline{\mathbf{A}} \hookleftarrow\$ \mathbb{Z}_q^{n \times (m-nk)}$, $\mathbf{T_A} \hookleftarrow\$ \mathcal{P}_{1/2}^{(m-nk) \times nk}$ and outputs $\left(\mathbf{A} := \left[\overline{\mathbf{A}} \| \mathbf{G} - \overline{\mathbf{A}}\mathbf{T_A}\right], \mathbf{T_A}\right)$. Then, $\mathbf{T_A}$ is a $\mathbf{G}$-trapdoor of $\mathbf{A}$, and $\mathbf{A}$ is distributed with statistical distance at most $nkq^{-0.196n}$ of the uniform distribution.*

Proof. A direct computation shows that $\mathbf{T_A}$ is a $\mathbf{G}$-trapdoor of $\mathbf{A}$. The statistical distance upper bound comes from Proposition 1.

Proposition 3 (Gaussian Sampling and Delegation of trapdoors (adapted from [25, Section 5])). *Let $n, m, k \in \mathbb{N}^*$, $q = 3^k$, $m \geq 2kn$. Let $0 < \epsilon < 1/2$. There exists algorithms $\mathsf{DelTrap}, \mathsf{SampleD}$ such that, for $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, $\mathbf{T_A} \in \mathbb{Z}_q^{(m-nk) \times nk}$ a $\mathbf{G}$-trapdoor and $s \geq \mathsf{r}_{nk,\epsilon} \sqrt{11\left(\mathsf{s}_1(\mathbf{T_A})^2 + 1\right)}$, we have:*

- $\mathsf{SampleD}(\mathbf{A}, \mathbf{u}, \mathbf{T_A}, s)$ *returns $\mathbf{z}$ such that $\mathbf{Az} = \mathbf{u}$ and the statistical distance between the probability distribution of $\mathbf{z}$ and $\mathcal{D}_{\Lambda_{q,\mathbf{u}}^\top(\mathbf{A}),s}$ is bounded by a function $\gamma_{n,m,\epsilon}^{\mathsf{Sample}}$ which is negligible if ϵ is.*
- $\mathsf{DelTrap}(\mathbf{A} \in \mathbb{Z}^{n \times m}, \mathbf{T_A} \in \mathbb{Z}^{(m-nk) \times nk}, \mathbf{A'} \in \mathbb{Z}^{n \times nk}, s)$ *returns a $\mathbf{G}$-trapdoor of $[\mathbf{A} \| \mathbf{A'}]$ (the output $\mathbf{T'_A} \in \mathbb{Z}^{m \times nk}$ satisfies $\mathbf{AT'_A} = \mathbf{A'} - \mathbf{G}$). Moreover, the probability distribution of the output $\mathbf{T'_A}$ is at statistical distance less than $nk\gamma_{n,m,\epsilon}^{\mathsf{Sample}}$ of the distribution $\mathcal{D}_{\mathbb{Z},s}^{m \times nk}$ with output $\mathbf{R}$ conditioned to $\mathbf{AR} = \mathbf{A'} - \mathbf{G}$. More precisely, if we denote by $(\mathbf{u}_1 \| \mathbf{u}_2 \| \cdots \| \mathbf{u}_{nk})$ the columns of $\mathbf{A'} - \mathbf{G}$, the k^{th} column of $\mathbf{T'_A}$ is computed as $\mathsf{SampleD}(\mathbf{A}, \mathbf{u}_k, \mathbf{T_A}, s)$.*

The next proposition will be used to replace some instances of KeyExt (that correspond to $\mathsf{Dist}_{\mathsf{ModKExt}}$) by another algorithm that does not use the master secret key ($\mathbf{T_A}$), of probability distribution $\mathsf{Dist}_{\mathsf{SimModKExt}}$. Note that the proposition allows making multiple replacements of $\mathsf{Dist}_{\mathsf{SimModKExt}}$ by $\mathsf{Dist}_{\mathsf{ModKExt}}$ for the same, fixed, pair of master public and secret keys (output of $\mathsf{Dist}_{\mathsf{KExt}}$). This is important because the adversary of $\mathsf{EUFnaCMA}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}^{\mathsf{IBS}}$ can ask for multiple secret keys of identities in one instance of the game - this can be easily overlooked when applying the framework of [25], designed with simple signature schemes in mind which involve only one pair of keys, to identity-based signature schemes.

[6] More details in Proposition 14 (Appendix B.8).

Proposition 4 (Simulation of delegation of trapdoors. Proof in Appendix B.7.). *Let* $n, m, k \in \mathbb{N}^*$, $q = 3^k$, $m \geq 2kn$. *Let* $s > 0$, $\mathbf{A} \in \mathbb{Z}^{n \times m}$ *and* $\mathbf{T_A} \in \mathbb{Z}_q^{(m-nk)\times nk}$ *a* $\mathbf{G}$*-trapdoor of* $\mathbf{A}$. *We define* $\mathsf{Dist}_{\mathsf{ModKExt}}(\mathbf{A}, \mathbf{T_A}, s)$ *as*

$$\left\{(\mathbf{A}', \mathbf{T}'_{\mathbf{A}}) : \mathbf{R} \hookleftarrow \mathcal{D}_{\mathbb{Z},s}^{m\times nk},\ \mathbf{A}' := \mathbf{AR} + \mathbf{G}, \mathbf{T}'_{\mathbf{A}} \leftarrow \mathsf{DelTrap}\left(\mathbf{A}, \mathbf{T_A}, \mathbf{A}', s\right)\right\} ,$$

and $\mathsf{Dist}_{\mathsf{SimModKExt}}(\mathbf{A}, s)$ *as* $\left\{(\mathbf{A}', \mathbf{R}) : \mathbf{R} \hookleftarrow \mathcal{D}_{\mathbb{Z},s}^{m\times nk},\ \mathbf{A}' := \mathbf{AR} + \mathbf{G}\right\}$.

Then, if $s \geq \sqrt{11}\mathsf{r}_{nk,\epsilon}\sqrt{\mathsf{s}_1(\mathsf{Binom})[m - nk, nk, 1/2]^2 + 1}$, *we have*

$$\underset{(\mathbf{A},\mathbf{T_A})\leftarrow\mathsf{Trap}(n,m,q)}{Pr}\left[\mathsf{SD}(\mathsf{Dist}_{\mathsf{ModKExt}}(\mathbf{A}, \mathbf{T_A}, s), \mathsf{Dist}_{\mathsf{SimModKExt}}(\mathbf{A}, s)) \leq nk\gamma^{\mathsf{Sample}}_{n,m,\epsilon}\right] \geq 1 - 2q^{-n} .$$

The next proposition shows that the probability distribution of the signatures ($\mathsf{Dist}_{\mathsf{Sign}}$) made with a secret key created by KeyExt (of probability distribution $\mathsf{Dist}_{\mathsf{KExt}}$) is close to a Gaussian distribution ($\mathcal{D}_{\mathbb{Z},s}^{m+nk}$). This will be useful to show the completeness of the IBS scheme, and also to replace signatures by Gaussian outputs in the proof of Theorem 2. The proposition allows studying multiple signatures for the same secret key, in a situation where a couple of public and master keys (output of $\mathsf{Dist}_{\mathsf{KExt}}$) has been taken, and multiples secret keys of identities have been created. This is crucial because the adversary of $\mathsf{EUFnaCMA}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}$ can ask for multiple signatures, made by multiple secret keys of identities in one instance of the game.

Proposition 5 (Proof in Appendix B.7.). *Let* $n, m, k \in \mathbb{N}^*$, $q = 3^k$, $m \geq 2kn$. *For* $s > 0, \tilde{s} > 0$, $\mathbf{A} \in \mathbb{Z}^{n\times m}, \mathbf{A}' \in \mathbb{Z}^{n\times nk}$ *and* $\mathbf{T}'_{\mathbf{A}} \in \mathbb{Z}^{m\times nk}$ *a* $\mathbf{G}$*-trapdoor of* $[\mathbf{A}\|\mathbf{A}']$. *We define*

$$\mathsf{Dist}_{\mathsf{KExt}}(\mathbf{A}, \mathbf{T_A}, s) := \left\{(\mathbf{A}', \mathbf{T}'_{\mathbf{A}}) : \ \mathbf{A}' \hookleftarrow \mathbb{Z}_q^{n\times nk}, \mathbf{T}'_{\mathbf{A}} \leftarrow \mathsf{DelTrap}\left(\mathbf{A}, \mathbf{T_A}, \mathbf{A}', s\right)\right\} ,$$

$$\mathsf{Dist}_{\mathsf{Sign}}(\mathbf{A}, \mathbf{A}', \mathbf{T}'_{\mathbf{A}}, \tilde{s}) = \{\mathbf{z} \colon \mathbf{z} \leftarrow \mathsf{SampleD}([\mathbf{A}\|\mathbf{A}'], \mathbf{u}, \mathbf{T}'_{\mathbf{A}}, \tilde{s}), \mathbf{u} \hookleftarrow \mathbb{Z}_q^n\} ,$$

$$\nu_1 := 2q^{-n} + nk(2\epsilon + \gamma^{\mathsf{Sample}}_{n,m,\epsilon}) + \sqrt{2}q^{-n/8} = \mathsf{negl}(n) ,$$

$$\nu_2 := 2nkq^{-0.196n} + 4q^{-n/4} + \sqrt{2}q^{-n/8} = \mathsf{negl}(n) .$$

Then, for $s \geq \max\left(\sqrt{11}\mathsf{r}_{nk,\epsilon}\sqrt{\mathsf{s}_1(\mathsf{Binom})[m - nk, nk, 1/2]^2 + 1},\ 12\mathsf{r}_{m,\epsilon}\right)$ *and* $\tilde{s} \geq \max\left(\sqrt{11}\mathsf{r}_{nk,\epsilon}\sqrt{\mathsf{s}_1(\mathsf{Gauss})[m, nk, s]^2 + 1},\ 12\mathsf{r}_{m+nk,\epsilon}\right)$, *we have*

$$\underset{(\mathbf{A},\mathbf{T_A})\leftarrow\$\mathsf{Trap}(n,m,q)}{Pr}\Bigg[\underset{(\mathbf{A}',\mathbf{T}'_{\mathbf{A}})\leftarrow\$\mathsf{Dist}_{\mathsf{KExt}}(\mathbf{A},\mathbf{T_A},s)}{Pr}\left[\mathsf{SD}(\mathsf{Dist}_{\mathsf{Sign}}(\mathbf{A}, \mathbf{A}', \mathbf{T_A}, \tilde{s}), \mathcal{D}_{\mathbb{Z},\tilde{s}}^{m+nk}) \leq \gamma^{\mathsf{Sample}}_{n,m+nk,\epsilon}\right] \geq 1 - \nu_1\Bigg] \geq 1 - \nu_2 . \tag{3}$$

The ring equivalent to Proposition 4 is stated and proved in Appendix B.7.

The $\mathcal{R}_q$ versions of the functions $\mathsf{Trap}, \mathsf{SampleD}, \mathsf{DelTrap}$ are denoted by $\mathsf{Trap}_{\mathcal{R}}, \mathsf{SampleD}_{\mathcal{R}}, \mathsf{DelTrap}_{\mathcal{R}}$ and the ring equivalent of Propositions 2,3,4 are stated and proved in Appendix B.9.

4.4 Hash reprogramming in the ROM and the QROM

This section gives two generic lemmas that enable the reprogramming of a hash function, in both the ROM and the QROM (the latter requiring more effort).

The first one is one of the main results of [17], it deals with the tedious problem of adaptive hash reprogramming in the QROM, for specific situations where only a chunk of the input is controlled by the adversary; the other chunk being chosen uniformly at random. It will be of great use for the ROM and the QROM reductions from $\mathsf{EUFCMA}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}$ to $\mathsf{EUFnaCMA}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}$ of Section 5.

The second one is a generalization of [5, Lemma 3], that allows the challenger to replace the value $\mathsf{H}(x)$, by the output of probability distributions Dist_i close (in statistical distance) to the uniform distribution. The probability distribution used depending on which set X_i contains x, for $(X_i)_i$ a partition of the input set, with a bounded number of elements. It will be used for the proof of the EUF-naCMA security of the schemes.

Proposition 6 ([17, Proposition 1], with added ROM case). *Let $m, n \in \mathbb{N}^*, X = \{0,1\}^m, Y = \{0,1\}^n$ and $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ be any algorithm issuing at most R queries to* ReprogramOracleOne *and Q quantum queries to $\mathcal{O}_b$ as defined in Figure 2. Then, it can be shown that the advantage defined by $\frac{1}{2}\left|\Pr[1 \leftarrow\$ \mathsf{AdaptReprog}_0(\mathcal{A})] - \Pr[1 \leftarrow\$ \mathsf{AdaptReprog}_1(\mathcal{A})]\right|$ is upper bounded by $\frac{3R}{4}\sqrt{\frac{Q}{|X_1|}}$. If the queries to $\mathcal{O}_b$ are classical, the upper bound becomes $\frac{QR}{|X_1|}$.*

Proof. The QROM case is proved in [17, Proposition 1]. We only prove the ROM case. The only way $\mathcal{A}$ can differentiate $\mathcal{O}_0$ from $\mathcal{O}_1$ is to obtain different values from multiple queries to $\mathcal{O}_b$ with the same input. If we denote by (x_1, x_2) this input, this implies that one of the R query to ReprogramOracleOne sampled x_1. Because ReprogramOracleOne is queried less than R times and $\mathcal{O}_b$ less than Q times, this event has a probability less than $\frac{RQ}{|X_1|}$.

$\mathsf{AdaptReprog}_b(\mathcal{A})$		$\mathsf{ReprogramOracleOne}(x_2)$
$\mathcal{O}_0 \leftarrow\$ Y^{X_1 \times X_2}$	$\mathsf{ORACLES} = \{\|\mathcal{O}_b\rangle, \mathsf{ReprogramOracleOne}\}$	$(x_1, y) \leftarrow\$ X_1 \times Y$
$\mathcal{O}_1 := \mathcal{O}_0$	$\tilde{b} \leftarrow \mathcal{A}^{\mathsf{ORACLES}}$	$\mathcal{O}_1 := \mathcal{O}_1^{(x_1 \| x_2) \to y}$
	return $\tilde{b}$	**return** x_1

Fig. 2. Adaptive reprogramming games $\mathsf{AdaptReprog}_b$ for bit $b \in \{0,1\}$. The adversary only decide the chunk in X_2 of the input

Proposition 7 (generalization of [5, Lemma 3] and addition of the ROM case. Proof in Appendix B.5.). *Let $m \in \mathbb{N}^*, Y = \{0,1\}^m$ and $\mathcal{S}_{\mathsf{dist}}$ a (possibly infinite) set of independent probability distributions with values in Y. We assume that for each $\mathsf{Dist} \in \mathcal{S}_{\mathsf{dist}}$, $\mathsf{SD}(\mathsf{U}(Y), \mathsf{Dist}) \leq \epsilon$. We consider the game* NoAdaptReprog *of Figure 3, with some fixed parameter $P \in \mathbb{N}^*$. Then, for any quantum adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ such that $\mathcal{A}_2$ make less than Q_c classical queries to H_b and $\mathcal{A}_3$ less than Q_q queries to $|\mathsf{H}_b\rangle$, we have,*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{NoAdaptReprog}} := \left|\Pr[1 \leftarrow \mathsf{NoAdaptReprog}(\mathcal{A}) \mid b = 1] - \frac{1}{2}\right| \leq Q_c\epsilon + 4Q_q^2\sqrt{P\epsilon} \ .$$

5 Generic transformation from EUF-naCMA (*resp.* sEUF-naCMA) to EUF-CMA security (*resp.* sEUF-CMA) in the ROM and the QROM

In [26] the authors exhibit two tight transformations from non-adaptive to adaptive IBS schemes:
- With chameleon hash functions [26, Figure 2].
- With hash functions in the ROM [26, Figure 5], as described in Figure 4.

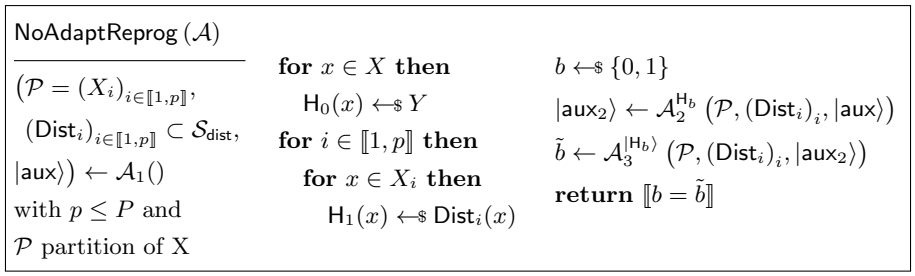

Fig. 3. Game NoAdaptReprog $(\mathcal{A})$ for $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$.

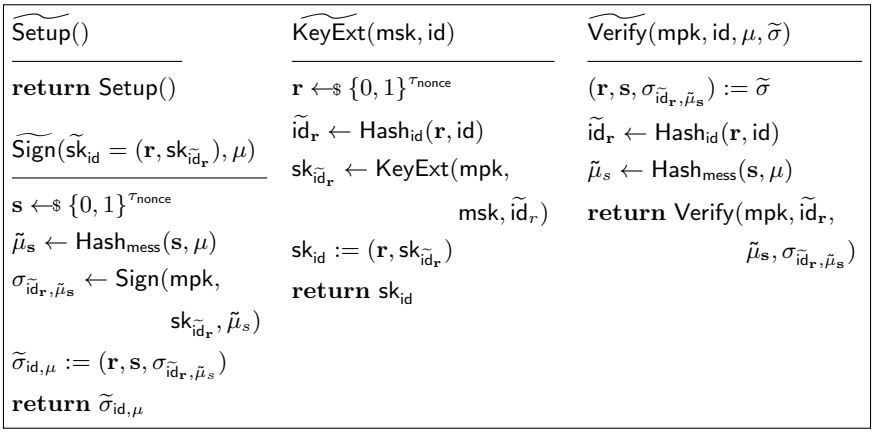

Fig. 4. Adaptively secure IBS $\mathsf{adapt}(\mathsf{IBS})$ from a non-adaptively secure IBS IBS. The codomains of $\mathsf{Hash}_{\mathsf{mess}}$ and $\mathsf{Hash}_{\mathsf{mess}}$ are respectively SetMess and SetId.

In this section we prove that the transformation of Figure 4 is also secure in the QROM. Moreover, the proof is modular, it also applies to the ROM. Afterwards, the transformation will be used to prove the security in the ROM and the QROM of our schemes $\mathsf{IBS}_\mathbb{Z}$ (Figure 5) and $\mathsf{IBS}_\mathcal{R}$ (Section 7, Figure 7) respectively linked to non-adaptive IBS schemes $\mathsf{IBS}_{\mathsf{NA},\mathbb{Z}}$ (Figure 6) and $\mathsf{IBS}_{\mathsf{NA},\mathcal{R}}$ (Section 7, Figure 8). We also show that this transformation work in the strong security setting, but this will not be used to prove the security of our schemes. Finally, note that the transformation does not modify the completeness.

Theorem 1 (Adaptive security of $\mathsf{adapt}(\mathsf{IBS})$ in the ROM and the QROM provided IBS is non-adaptively secure, with or without strong security). *We assume that* $\mathsf{SetId} = \{0,1\}^{\tau_{\mathsf{id}}}$, $\mathsf{SetMess} = \{0,1\}^{\tau_{\mathsf{mess}}}$ *for* $\tau_{\mathsf{id}}, \tau_{\mathsf{mess}} \in \mathbb{N}^*$. *Let* $Q_{\mathsf{Corr}}, Q_{\mathsf{S}} \in \mathbb{N}^*$. *For* $a, b, Q \in \mathbb{N}^*$, *we denote by* $\mathsf{FindCol}_{\mathsf{Q}}(a,b)_Q$ *the game of finding a collision for a random function* $\mathsf{H} : \{0,1\}^a \to \{0,1\}^b$ *with access to at most* Q *quantum queries to* H. *In order to simplify the notations, we define the security game* FindColId *by* $\mathsf{FindCol}_{\mathsf{Q}}(\tau_{\mathsf{nonce}}+\tau_{\mathsf{id}}, \tau_{\mathsf{id}})_{Q_{\mathsf{Hash}_{\mathsf{id}}}+Q_{\mathsf{Corr}}+Q_{\mathsf{S}}}$ *and we also define the security game* FindColMess *by* $\mathsf{FindCol}_{\mathsf{Q}}(\tau_{\mathsf{nonce}}+\tau_{\mathsf{mess}}, \tau_{\mathsf{mess}})_{Q_{\mathsf{Hash}_{\mathsf{mess}}}+Q_{\mathsf{S}}}$. *Let* $(\mathsf{GameSign}, \mathsf{GamenaSign}) \in \{(\mathsf{EUFCMA}, \mathsf{EUFnaCMA}), (\mathsf{sEUFCMA}, \mathsf{sEUFnaCMA})\}$. *Then for each PPT adversary* $\mathcal{A}$ *against* $\mathsf{GameSign}^{\mathsf{adapt}(\mathsf{IBS})}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}$ *that makes* $Q_{\mathsf{Hash}_{\mathsf{id}}}$ *quantum queries to* $\mathsf{Hash}_{\mathsf{id}}$ *and* $Q_{\mathsf{Hash}_{\mathsf{mess}}}$ *quantum queries to* $\mathsf{Hash}_{\mathsf{mess}}$, *there exists PPT adversaries* $\mathcal{C}$ *against* $\mathsf{GamenaSign}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}$, $\mathcal{B}_{\mathsf{id}}$ *against* FindColId *and* $\mathcal{B}_\mu$ *against*

$\mathsf{FindColMess}$ *such that* $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{GameSign}^{\mathsf{adapt(IBS)}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}}$ *is upper bounded by*

$$\mathsf{Adv}_{\mathcal{C}}^{\mathsf{GamenaSign}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}} + 3 * 2^{-\frac{\tau_{\mathsf{nonce}}+4}{2}} \left(\sqrt{Q_{\mathsf{Hash_{id}}}}(Q_{\mathsf{Corr}}+Q_{\mathsf{S}}) + \sqrt{Q_{\mathsf{Hash_{mess}}}}\, Q_{\mathsf{S}}\right) + \mathsf{Adv}_{\mathcal{B}_{\mathsf{id}}}^{\mathsf{FindColId}} + \mathsf{Adv}_{\mathcal{B}_{\mu}}^{\mathsf{FindColMess}} \ .$$

Remark 1. Using [32, Theorem 3.1], we know that there exists a universal constant $\mathsf{C_{coll}}$ such that the advantage $\mathsf{Adv}_{\mathcal{B}_{\mathsf{id}}}^{\mathsf{FindColId}} + \mathsf{Adv}_{\mathcal{B}_{\mu}}^{\mathsf{FindColMess}}$ can be upper bounded by $\mathsf{C_{coll}}\left[2^{-\tau_{\mathsf{id}}}\left(Q_{\mathsf{Hash_{id}}}+Q_{\mathsf{S}}+Q_{\mathsf{Corr}}+1\right)^3 + 2^{-\tau_{\mathsf{mess}}}\left(Q_{\mathsf{Hash_{mess}}}+Q_{\mathsf{S}}+1\right)^3\right]$. If all queries are classical, $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{GameSign}^{\mathsf{adapt(IBS)}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}}$ is upper bounded by

$$\mathsf{Adv}_{\mathcal{C}}^{\mathsf{GamenaSign}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}} + 2^{-\tau_{\mathsf{nonce}}}\left(Q_{\mathsf{Hash_{id}}}+1\right)(Q_{\mathsf{Corr}}+Q_{\mathsf{S}}) + \left(Q_{\mathsf{Hash_{mess}}}+1\right)Q_{\mathsf{S}} + 2^{-\tau_{\mathsf{id}}}(Q_{\mathsf{Hash_{id}}}+Q_{\mathsf{S}}+Q_{\mathsf{Corr}}+1) + 2^{-\tau_{\mathsf{mess}}}(Q_{\mathsf{Hash_{mess}}}+Q_{\mathsf{S}}+1) \ .$$

Proof. We sum up the changes between games in Table 1.

Hop	Change	Security loss
G_0 to G_1	Prohibition of some collisions.	ROM $2^{-\tau_{\mathsf{id}}}\left(Q_{\mathsf{Hash_{id}}}+1\right)\left(Q_{\mathsf{Corr}}+Q_{\mathsf{S}}\right) + 2^{-\tau_{\mathsf{mess}}}\left(Q_{\mathsf{Hash_{mess}}}+1\right)Q_{\mathsf{S}}$ QROM $\mathsf{Adv}_{\mathcal{B}_{\mathsf{id}}}^{\mathsf{FindColId}} + \mathsf{Adv}_{\mathcal{B}_{\mu}}^{\mathsf{FindColMess}}$
G_1 to G_2	Reprogramming of hash function when $\mathcal{O}_{\mathsf{Sign}}$ or $\mathcal{O}_{\mathsf{Corrupt}}$ is queried.	ROM $2^{-\tau_{\mathsf{nonce}}}\left(Q_{\mathsf{Hash_{id}}}\left(Q_{\mathsf{Corr}}+Q_{\mathsf{S}}\right)+Q_{\mathsf{Hash_{mess}}}\,Q_{\mathsf{S}}\right)$ QROM $2^{-\frac{\tau_{\mathsf{nonce}}+4}{2}}\ 3\left(\sqrt{Q_{\mathsf{Hash_{id}}}}(Q_{\mathsf{Corr}}+Q_{\mathsf{S}}) + \sqrt{Q_{\mathsf{Hash_{mess}}}}\,Q_{\mathsf{S}}\right)$
G_2 to G_3	Precomputation of identities, messages, keys and signatures.	0
Minoration of advantage of last game:		$\leq \mathsf{Adv}_{\mathcal{C}}^{\mathsf{GamenaSign}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}}$

Table 1. Summary of the changes between the games used for the proof of Theorem 1. Complete games are in Appendix C. We use $\mathsf{FindCol}_{\mathsf{Q}}(\tau_{\mathsf{nonce}}=\tau_{\mathsf{id}},\tau_{\mathsf{id}})_{Q_{\mathsf{Hash_{id}}}=Q_{\mathsf{Corr}}=Q_{\mathsf{S}}=1}=\mathsf{FindColId}$ and $\mathsf{FindCol}_{\mathsf{Q}}(\tau_{\mathsf{nonce}}=\tau_{\mathsf{mess}},\tau_{\mathsf{mess}})_{Q_{\mathsf{Hash_{mess}}}=Q_{\mathsf{S}}=1}=\mathsf{FindColMess}$ for compactness.

From $\mathsf{G}_0 = \mathsf{GameSign}^{\mathsf{adapt(IBS)}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}$ to G_1:
We denote by $(\tilde{\sigma}^* = (\mathbf{t}^*, s^*, \sigma^*), \mathsf{id}^*, \mu^*)$ the output of $\mathcal{A}$. We abort the game if one of these two events happens

$$\mathsf{fail}_1 := \text{"}\exists(\mathbf{r},\mathsf{id}) \in \mathsf{NoncesSk} : \mathsf{Hash_{id}}(\mathbf{r},\mathsf{id}) = \mathsf{Hash_{id}}(\mathbf{t}^*,\mathsf{id}^*)\text{"} \ ,$$
$$\mathsf{fail}_2 := \text{"}\exists(\mathbf{t},\mathsf{id},\mathbf{s},\mu) \in \mathsf{NoncesSign} : \ (\mathbf{t},\mathsf{id},\mathbf{s},\mu) \neq (\mathbf{t}^*,\mathsf{id}^*,\mathbf{s}^*,\mu^*) \wedge \mathsf{Hash_{id}}(\mathbf{t},\mathsf{id}) = \mathsf{Hash_{id}}(\mathbf{t}^*,\mathsf{id}^*) \wedge \mathsf{Hash_{mess}}(\mathbf{s},\mu) = \mathsf{Hash_{mess}}(\mathbf{s}^*,\mu^*)\text{"} \ .$$

Where $\mathsf{NoncesSk}$ (*resp.* $\mathsf{NoncesSign}$) contains the nonces and identities asked to and created by the oracle $\mathcal{O}_{\mathsf{Corrupt}}$ (*resp.* nonces, messages and identities asked to and created by the oracle $\mathcal{O}_{\mathsf{Sign}}$). Note that $(\mathbf{t}^*,\mathsf{id}^*,\mathbf{s}^*,\mu^*) \in \mathsf{NoncesSign}$ can led to a valid forgery only in the strong case. In the QROM case, we can create $\mathcal{B}$, playing the game of finding a collision on $\mathsf{Hash_{id}}$ or $\mathsf{Hash_{mess}}$. $\mathcal{B}$ uses an adversary $\mathcal{A}$ against $\mathsf{GameSign}^{\mathsf{adapt(IBS)}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}$ in order to:

- Find a collision on $\mathsf{Hash_{id}}$ if $\mathcal{A}$ wins and fail_1 is realized. $\mathcal{B}$ uses at most $Q_{\mathsf{Hash_{id}}} + Q_{\mathsf{Corr}} + Q_{\mathsf{S}}$ queries to $\mathsf{Hash_{id}}$.

– Find a collision on $\mathsf{Hash}_{\mathsf{id}}$ or $\mathsf{Hash}_{\mathsf{mess}}$ if $\mathcal{A}$ wins and fail_2 is realized. $\mathcal{B}$ uses at most $Q_{\mathsf{Hash}_{\mathsf{mess}}} + Q_{\mathsf{S}}$ queries to $\mathsf{Hash}_{\mathsf{mess}}$.

Using $\mathcal{B}$, we can then create two adversaries $\mathcal{B}_{\mathsf{id}}$ and $\mathcal{B}_{\mu}$ that respectively play to FindColId and FindColMess, and such that the advantage of $\mathcal{B}$ is bounded by $\mathsf{Adv}^{\mathsf{FindColId}}_{\mathcal{B}_{\mathsf{id}}} + \mathsf{Adv}^{\mathsf{FindColMess}}_{\mathcal{B}_{\mu}}$. We give a better bound in the ROM case than the bound for a collision by noticing that the collisions founds are specific. Indeed, The collision with $\mathsf{Hash}_{\mathsf{id}}$ (*resp.* $\mathsf{Hash}_{\mathsf{mess}}$) is searched with the constraint that one of the two elements is on the set NoncesSk (*resp.* a set linked to NoncesSign) of $Q_{\mathsf{Corr}} + Q_{\mathsf{S}}$ (*resp.* Q_{S}) elements while the other is not and can be found using $Q_{\mathsf{Hash}_{\mathsf{id}}} + 1$ (*resp.* $Q_{\mathsf{Hash}_{\mathsf{mess}}} + 1$) Hash queries (the "+1" is for the case where the value is output by the adversary without being queried). The advantage is bounded by $2^{-\tau_{\mathsf{id}}}(Q_{\mathsf{Hash}_{\mathsf{id}}} + 1)\,(Q_{\mathsf{Corr}} + Q_{\mathsf{S}})$ (*resp.* $2^{-\tau_{\mathsf{mess}}}(Q_{\mathsf{Hash}_{\mathsf{mess}}} + 1)Q_{\mathsf{S}}$).

G_1 to G_2: We use the reprogramming algorithm of Proposition 6 for $\mathsf{Hash}_{\mathsf{id}}$ when $\mathcal{O}_{\mathsf{Sign}}$ or $\mathcal{O}_{\mathsf{Corrupt}}$ is queried and for $\mathsf{Hash}_{\mathsf{mess}}$ when $\mathcal{O}_{\mathsf{Sign}}$ is queried. For example, when the reprogramming oracle for $\mathsf{Hash}_{\mathsf{mess}}$ is queried for a message μ, a nonce $\mathbf{s}$ is uniformly sampled in $\{0,1\}^{\tau_{\mathsf{nonce}}}$ and the Hash value $\mathsf{Hash}_{\mathsf{mess}}(\mathbf{s}, \mu)$ is programmed to a uniform value of SetMess.

A double application of Proposition 6 shows that $\left|\mathsf{Adv}^{\mathsf{G}_1}_{\mathcal{A}} - \mathsf{Adv}^{\mathsf{G}_2}_{\mathcal{A}}\right|$ is upper bounded by $2^{-\frac{\tau_{\mathsf{nonce}}+4}{2}}\, 3\left(\sqrt{Q_{\mathsf{Hash}_{\mathsf{id}}}}(Q_{\mathsf{Corr}} + Q_{\mathsf{S}}) + \sqrt{Q_{\mathsf{Hash}_{\mathsf{mess}}}\, Q_{\mathsf{S}}}\right)$ if the hash queries are quantum and $2^{-\tau_{\mathsf{nonce}}}\left(Q_{\mathsf{Hash}_{\mathsf{id}}}\,(Q_{\mathsf{Corr}} + Q_{\mathsf{S}}) + Q_{\mathsf{Hash}_{\mathsf{mess}}}\, Q_{\mathsf{S}}\right)$ if they are classical.

G_2 to G_3: In this game, the identities and messages that are sampled by the reprogramming oracles for H_1 and $\mathsf{Hash}_{\mathsf{mess}}$ are precomputed at the beginning of the game. It is thus possible to precompute the secret keys of identities and signatures computed by $\mathcal{O}_{\mathsf{Corrupt}}$ and $\mathcal{O}_{\mathsf{Sign}}$. The advantage suffers no loss since the distribution of each of these elements remains the same.

Reduction from $\mathsf{GamenaSign}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}$ to G_3: We use the fact that the signatures and keys of $\mathcal{O}_{\mathsf{Corrupt}}$ and $\mathcal{O}_{\mathsf{Sign}}$ are precomputed in G_3 to create an adversary $\mathcal{C}$ of the $\mathsf{GamenaSign}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}$ of IBS that uses $\mathcal{A}$.

Thanks to the event fail_1 and fail_2 that were added in G_1, we observe that $\mathcal{C}$ wins the $\mathsf{GamenaSign}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}$ game for IBS each time that $\mathcal{A}$ wins G_3. Thus, $\mathsf{Adv}^{\mathsf{G}_3}_{\mathcal{A}} \leq \mathsf{Adv}^{\mathsf{GamenaSign}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}}_{\mathcal{C}}$.

6 IBS Scheme in the ROM and the QROM, based on SIS

The scheme is defined in Figure 5. The parameters and the conditions they must follow are summarized in Table 2.

$\mathsf{Setup}(n,m)$	$\mathsf{Sign}(\mathsf{mpk}, (\mathbf{r}, \mathsf{id}, \mathbf{T}_{\mathsf{id}}), \mu)$	$\mathsf{Verify}\,(\mathsf{mpk}, \mathsf{id}, \mu, (\mathbf{r}, \mathbf{s}, \mathbf{z}))$
$(\mathbf{A}, \mathbf{T}_{\mathbf{A}}) \leftarrow \mathsf{Trap}(n,m,q)$	$\mathbf{s} \leftarrow\!\$\ \{0,1\}^{\tau_{\mathsf{nonce}}}$	**if** $\mathbf{z} = \mathbf{0} \vee [\mathbf{A} \Vert \mathsf{H}_1(\mathbf{r}, \mathsf{id})]\,\mathbf{z}$
return $(\mathbf{A}, \mathbf{T}_{\mathbf{A}})$	$\mathbf{u} \leftarrow \mathsf{H}_2\,(\mathbf{r}, \mathbf{s}, \mathsf{id}, \mu)$	$\neq \mathsf{H}_2(\mathbf{r}, \mathbf{s}, \mathsf{id}, \mu)$
	$\mathbf{z} \leftarrow \mathsf{SampleD}\big([\mathbf{A} \Vert \mathsf{H}_1(\mathbf{r}, \mathsf{id})]\,,$	**then return** 0
$\mathsf{KeyExt}(\mathbf{A}, \mathbf{T}_{\mathbf{A}}, \mathsf{id})$	$\mathbf{T}_{\mathsf{id}}, \mathbf{u}, s_{\mathsf{sign}}\big)$	$/\!/\ \mathbf{z} = (\mathbf{z}_1, \mathbf{z}_2) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^{nk}$
$\mathbf{r} \leftarrow\!\$\ \{0,1\}^{\tau_{\mathsf{nonce}}}$	**return** $(\mathbf{r}, \mathbf{s}, \mathbf{z})$	**return** $[\![\Vert\mathbf{z}_1\Vert \leq \mathsf{Bound}_1$
$\mathbf{T}_{\mathsf{id}} \leftarrow \mathsf{DelTrap}\big(\mathbf{A}, \mathbf{T}_{\mathbf{A}},$		$\wedge\ \Vert\mathbf{z}_2\Vert \leq \mathsf{Bound}_2]\!]$
$\mathsf{H}_1(\mathbf{r}, \mathsf{id}), s_{\mathsf{id}}\big)$		
return $(\mathbf{r}, \mathbf{T}_{\mathsf{id}})$		

Fig. 5. Scheme $\mathsf{IBS}_{\mathbb{Z}}$.

The proof of completeness will use the tail inequality.

Notation	Description
$q := 3^k$	modulus, power of 3 for $k \in \mathbb{N}, k \geq 1$
SetId	Set of identities, of the form $\{0,1\}^{\tau_{\mathsf{id}}}$ for some integer τ_{id}
$\mathsf{SetMess}$	Set of messages, of the form $\{0,1\}^{\tau_{\mathsf{mess}}}$ for some integer τ_{mess}
$\mathsf{SetNonces}$	Set of nonces, of the form $\{0,1\}^{\tau_{\mathsf{nonce}}}$ for some integer τ_{nonce}
n, m	number of rows and columns of $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, $m \geq 2nk$
ϵ	used in $\mathsf{r}_{x,\epsilon} = \sqrt{\ln\left(2x(1+1/\epsilon)\right)/\pi}$, we take $\epsilon = \epsilon(n) = \mathsf{negl}(n)$
$\mathsf{H}_1, \mathsf{H}_2$	hash functions with respective values in $\mathbb{Z}_q^{n \times nk}$ and $\mathbb{Z}_q^n$
$s_{\mathsf{id}}, s_{\mathsf{sign}}$	standard deviations, with
	$s_{\mathsf{id}} \geq \max\left(\sqrt{11}\mathsf{r}_{nk,\epsilon}\sqrt{\mathsf{s}_1(\mathsf{Binom})[m-nk, nk, 1/2]^2 + 1},\ 12\mathsf{r}_{m,\epsilon}\right)$.
	$s_{\mathsf{sign}} \geq \max\left(\sqrt{11}\mathsf{r}_{nk,\epsilon}\sqrt{\mathsf{s}_1(\mathsf{Gauss})[m, nk, s_{\mathsf{id}}]^2 + 1},\ 12\mathsf{r}_{m+nk,\epsilon}\right)$.
Bound_1	bound of $\|\mathbf{z}_1\|$ for signatures $\mathbf{z}$=$(\mathbf{z}_1, \mathbf{z}_2) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^{nk}$, $\mathsf{Bound}_1 \geq \sqrt{2m}\, s_{\mathsf{sign}}$
Bound_2	bound of $\|\mathbf{z}_2\|$ for signatures $\mathbf{z}$=$(\mathbf{z}_1, \mathbf{z}_2) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^{nk}$, $\mathsf{Bound}_2 \geq \sqrt{2nk}\, s_{\mathsf{sign}}$

Table 2. Parameters of $\mathsf{IBS}_{\mathbb{Z}}$ and required conditions.

Lemma 2 (Tail inequality (*e.g.* [3])). *Let $m \in \mathbb{N}$, $\sigma > 1$. Then,* $\Pr_{\mathbf{z} \leftarrow \$ \mathcal{D}_{\mathbb{Z},\sigma}^m}\left[\|\mathbf{z}\| > \sqrt{2m}\sigma\right] < 2^{-\frac{m}{4}}$.

Proposition 8 (completeness). *Consider the scheme $\mathsf{IBS}_{\mathbb{Z}}$ with the parameters of Table 2. Then, $\mathsf{IBS}_{\mathbb{Z}}$ is (ξ_1, ξ_2)-complete with $\xi_1 = 2q^{-n} + nk(2\epsilon + \gamma_{n,m,\epsilon}^{\mathsf{Sample}}) + 4\sqrt{2}q^{-n/8} + 2^{-\frac{(nk-1)}{4}} = \mathsf{negl}(n)$, and $\xi_2 = nkq^{-0.196n} + 4q^{-n/4} + \sqrt{2}q^{-n/8} = \mathsf{negl}(n)$.*

Proof. Direct consequence of Proposition 5 and Lemma 2 that shows that

$$Pr_{(\mathbf{z}_1,\mathbf{z}_2) \leftarrow \$ \mathcal{D}_{\mathbb{Z},s_{\mathsf{sign}}}^m \times \mathcal{D}_{\mathbb{Z},s_{\mathsf{sign}}}^{nk}}\left[\|\mathbf{z}_1\| > \sqrt{2m}s_{\mathsf{sign}} \vee \|\mathbf{z}_2\| > \sqrt{2nk}\sigma\right] < 2^{-\frac{m}{4}} + 2^{-\frac{nk}{4}} < 2^{-\frac{(nk-1)}{4}}\ .$$

From adaptive security to non-adaptive security. In this part we show the adaptive security of the scheme $\mathsf{IBS}_{\mathbb{Z}}$ (Figure 5). It consists in three steps. First, we prove the $\mathsf{EUF\text{-}naCMA}$ property of the scheme $\mathsf{IBS}_{\mathsf{NA},\mathbb{Z}}$ in Theorem 2 of Section 6. Then, the $\mathsf{EUF\text{-}naCMA}$ property of $\mathsf{IBS}_{\mathsf{NA},\mathbb{Z}}$ implies the $\mathsf{EUF\text{-}CMA}$ property of $\mathsf{adapt}(\mathsf{IBS}_{\mathsf{NA},\mathbb{Z}})$ through Theorem 1. Finally, Proposition 9 proves that the $\mathsf{EUF\text{-}CMA}$ property of $\mathsf{adapt}(\mathsf{IBS}_{\mathsf{NA},\mathbb{Z}})$ implies the $\mathsf{EUF\text{-}CMA}$ property of $\mathsf{IBS}_{\mathbb{Z}}$.

$\mathsf{Setup}(n, m)$	$\mathsf{Sign}(\mathsf{mpk}, (\mathsf{id}, \mathbf{T}_{\mathsf{id}}), \mu)$	$\mathsf{Verify}(\mathsf{mpk}, \mathsf{id}, \mu, \mathbf{z})$
$(\mathbf{A}, \mathbf{T}_{\mathbf{A}}) \leftarrow \mathsf{Trap}(n, m, q)$	$\mathbf{u} := \mathsf{H}_2(\mathsf{id}, \mu)$	**if** $\mathbf{z} = 0 \vee [\mathbf{A} \| \mathsf{H}_1(\mathsf{id})]\,\mathbf{z}$
return $(\mathbf{A}, \mathbf{T}_{\mathbf{A}})$	$\mathbf{z} \leftarrow \mathsf{SampleD}\big([\mathbf{A} \| \mathsf{H}_1(\mathsf{id})], \mathbf{T}_{\mathsf{id}}, \mathbf{u}, s_{\mathsf{sign}}\big)$	$\neq \mathsf{H}_2(\mathsf{id}, \mu)$
$\mathsf{KeyExt}(\mathbf{A}, \mathbf{T}_{\mathbf{A}}, \mathsf{id})$	**return** $\mathbf{z}$	**then return** 0
$\mathbf{T}_{\mathsf{id}} \leftarrow \mathsf{DelTrap}\big(\mathbf{A}, \mathbf{T}_{\mathbf{A}}, \mathsf{H}_1(\mathsf{id}), s_{\mathsf{id}}\big)$		$/\!/\ \mathbf{z} = (\mathbf{z}_1, \mathbf{z}_2) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^{nk}$
return $(\mathsf{id}, \mathbf{T}_{\mathsf{id}})$		**return** $[\![\|\mathbf{z}_1\| \leq \mathsf{Bound}_1 \wedge \|\mathbf{z}_2\| \leq \mathsf{Bound}_2]\!]$

Fig. 6. Scheme $\mathsf{IBS}_{\mathsf{NA},\mathbb{Z}}$.

Proposition 9 ($\mathsf{EUF\text{-}CMA}$ security of $\mathsf{adapt}(\mathsf{IBS}_{\mathbb{Z}})$ implies the security of $\mathsf{IBS}_{\mathbb{Z}}$.). *Let $Q_{\mathsf{Corr}}, Q_{\mathsf{S}} \in \mathbb{N}$ and $\mathcal{A}$ a PPT adversary of $\mathsf{EUFCMA}^{\mathsf{IBS}_{\mathbb{Z}}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}$ (Figure 5) that makes Q_{Corr} queries to $\mathcal{O}_{\mathsf{Corrupt}}$, Q_{S} queries to $\mathcal{O}_{\mathsf{Sign}}$, Q_{H_1} quantum (resp. classical) queries to H_1 and Q_{H_2} quantum*

(resp. classical) queries to H_2*. Then, there exists a PPT adversary* $\mathcal{B}$ *of* $\mathsf{EUFCMA}^{\mathsf{adapt}(\mathsf{IBS}_{\mathbb{Z}})}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}$ *that makes* Q_{H_1} *quantum (resp. classical) queries to* H_1*,* Q_{H_2} *quantum (resp. classical) queries to* H_2*,* $2(Q_{\mathsf{H}_1}+Q_{\mathsf{H}_2})$ *quantum (resp.* $Q_{\mathsf{H}_1}+Q_{\mathsf{H}_2}$ *classical) queries to* $\mathsf{Hash}_{\mathsf{id}}$*, and* $2Q_{\mathsf{H}_2}$ *quantum (resp.* Q_{H_2} *classical) queries to* $\mathsf{Hash}_{\mathsf{mess}}$*, such that* $\mathsf{Adv}^{\mathsf{EUFCMA}^{\mathsf{IBS}_{\mathbb{Z}}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}}_{\mathcal{A}} = \mathsf{Adv}^{\mathsf{EUFCMA}^{\mathsf{adapt}(\mathsf{IBS}_{\mathbb{Z}})}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}}_{\mathcal{B}}$ *.*

Proof. We can see the functions

$$\tilde{\mathsf{H}_1}(\mathbf{r},\mathsf{id}) := \mathsf{H}_1(\mathsf{Hash}_{\mathsf{id}}(\mathbf{r},\mathsf{id})) \quad \tilde{\mathsf{H}_2}(\mathbf{r},\mathbf{s},\mathsf{id},\mu) := \mathsf{H}_1\left(\mathsf{Hash}_{\mathsf{id}}(\mathbf{r},\mathsf{id}),\mathsf{Hash}_{\mathsf{mess}}(\mathbf{s},\mu)\right) \ ,$$

are functions if $\mathsf{H}_1,\mathsf{H}_2,\mathsf{Hash}_{\mathsf{id}},\mathsf{Hash}_{\mathsf{mess}}$ are. The adversary $\mathcal{B}$ can then use the random functions $\tilde{\mathsf{H}_1}$ and $\tilde{\mathsf{H}_2}$ for the game that is playing $\mathcal{A}$. This is sufficient to conclude if $\mathcal{A}$ make classical queries.

If $\mathcal{A}$ make quantum queries, we furthermore need to show that $\mathcal{B}$ can simulate queries to $|\mathsf{H}_1(\mathsf{Hash}_{\mathsf{id}}(\cdot,\cdot))\rangle$ and $|\mathsf{H}_1\left(\mathsf{Hash}_{\mathsf{id}}(\cdot,\cdot),\mathsf{Hash}_{\mathsf{mess}}(\cdot,\cdot)\right)\rangle$ using queries to $|\mathsf{H}_1\rangle$, $|\mathsf{H}_2\rangle$, $|\mathsf{Hash}_{\mathsf{mess}}\rangle$ and $|\mathsf{Hash}_{\mathsf{id}}\rangle$. This is shown by Lemmas 13 and 15 of Appendix B.4.

Non-adaptive security in the ROM and the QROM. The non-adaptive security of $\mathsf{IBS}_{\mathsf{NA},\mathbb{Z}}$ is, as for the IBS scheme of [26], an "IBS version" of the proof of the signature scheme of [23], with the added difficulty of dealing with delegated trapdoors. It is made in two steps:

- The first step consists in replacing $\mathsf{EUFnaCMA}^{\mathsf{IBS}_{\mathsf{NA},\mathbb{Z}}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}$, in an indistinguishable way for the adversary $\mathcal{A}$, by a game G_5 that does not use the trapdoor $\mathbf{T_A}$ and where $\mathbf{A}$ is uniform. It is done by reprogramming H_1 and H_2, to give outputs indistinguishable from a random function, but that contain "planted" trapdoors, enabling the challenger to respond to secret key and signature queries. Here, we need a more subtle method than the one used in [26]: it was using [5, Lemma 3], which corresponds to a particular case of Proposition 7 with partitions of size 2. However, in our games, the size of the partitions is only bounded by $Q_{\mathsf{IdSign}}+1$ where Q_{IdSign} is the number of distinct identities for which the adversary queries a signature. Also note that, contrary to [26] that uses distributions of the form $\mathcal{D}_{\mathbb{Z},s,\mathbf{A}}$ for reprogramming, we use reprogramming with $\mathcal{U}_{\mathbf{A}}$ whenever it is possible.
- The second step is a reduction from SIS to G_5 that is similar to what is done in [23] and [26]. Note that we find a better SIS bound than [26], partly thanks or use of $\mathcal{U}_{\mathbf{A}}$ for the reprogramming.

Theorem 2 (EUF-naCMA security of $\mathsf{IBS}_{\mathsf{NA},\mathbb{Z}}$). *Consider a set of parameters respecting the conditions listed in Table 2. Let* $Q_{\mathsf{Corr}},Q_{\mathsf{S}}\in\mathbb{N}$ *and* $\mathcal{A}$ *a PPT adversary of* $\mathsf{EUFnaCMA}^{\mathsf{IBS}_{\mathsf{NA},\mathbb{Z}}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}$ *that makes* Q_{H_1} *quantum queries to* H_1*,* Q_{H_2} *quantum queries to* H_2 *and such that at most* Q_{IdSign} *signatures are queried for the same identity. Let* $\mathsf{Bound}_{\mathsf{SIS}}=\mathsf{Bound}_1+\mathsf{s}_1(\mathsf{Unif})[m,nk]\,\mathsf{Bound}_2+\sqrt{m}$ *and* $\mathsf{mx}=\max(2\epsilon,q^{-n/4})=\mathsf{negl}(n)$*. Then, there exists a PPT adversary* $\mathcal{B}$ *of* $\mathsf{SIS}_{n,m,\mathsf{Bound}_{\mathsf{SIS}},q}$ *such that* $\mathsf{Adv}^{\mathsf{EUFnaCMA}^{\mathsf{IBS}_{\mathsf{NA},\mathbb{Z}}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}}_{\mathcal{A}}$ *is upper bounded by*

$$\begin{aligned}
&\frac{2\mathsf{Adv}^{\mathsf{SIS}_{n,m,\mathsf{Bound}_{\mathsf{SIS}},q}}_{\mathcal{B}}}{1-q^{-n}}+4Q_{\mathsf{H}_1}^2\sqrt{2nk\mathsf{mx}}+4Q_{\mathsf{H}_2}^2\sqrt{Q_{\mathsf{IdSign}}+1}\sqrt{\mathsf{mx}}\\
&+Q_{\mathsf{Corr}}nk\left(\mathsf{mx}+\gamma^{\mathsf{Sample}}_{n,m,\epsilon}\right)+Q_{\mathsf{S}}\left(\gamma^{\mathsf{Sample}}_{n,m+nk,\epsilon}+nk(2\epsilon+\gamma^{\mathsf{Sample}}_{n,m,\epsilon})+4q^{-n/8}+(nk+2)\mathsf{mx}\right)\\
&+Q_{\mathsf{IdSign}}\left(2q^{-\frac{n}{4}}+\mathsf{mx}\right)+5nkq^{-0.196n}+11q^{-\frac{n}{4}}+\frac{4q^{-n}}{1-q^{-n}} \ ,
\end{aligned}$$

where $\gamma^{\mathsf{Sample}}_{n,m,\epsilon}$ *is negligible and is defined in Section 4.3. If the queries to* Q_{H_1} *and* Q_{H_2} *are classical, first line of the upper bound becomes* $\frac{2}{1-q^{-n}}\mathsf{Adv}^{\mathsf{SIS}_{n,m,\mathsf{Bound}_{\mathsf{SIS}},q}}_{\mathcal{B}}+Q_{\mathsf{H}_1}nk\mathsf{mx}+Q_{\mathsf{H}_2}\mathsf{mx}$*.*

Hop	Change	Security loss
G_0 to G_1	Reprogramming of H_1.	ROM: $(Q_{\mathsf{H}_1}+Q_{\mathsf{Corr}})\,nk\mathsf{mx}+nkq^{-0.196n}+3q^{-n/4}$ QROM: $Q_{\mathsf{Corr}}\,nk\mathsf{mx}+4Q_{\mathsf{H}_1}^2\sqrt{2nk\mathsf{mx}}+nkq^{-0.196n}+3q^{-n/4}$
G_1 to G_2	Reprogramming of H_2.	ROM: $(Q_{\mathsf{H}_2}+Q_{\mathsf{S}})\,\mathsf{mx}+Q_{\mathsf{IdSign}}(2q^{-n/4}+\mathsf{mx})+nkq^{-0.196}$ QROM: $Q_{\mathsf{S}}\,\mathsf{mx}+4Q_{\mathsf{H}_2}^2\sqrt{(Q_{\mathsf{IdSign}}+1)\mathsf{mx}}$ $+Q_{\mathsf{IdSign}}(2q^{-n/4}+\mathsf{mx})+nkq^{-0.196}$
G_2 to G_3	$\mathbf{T_A}$ no more used for $\mathcal{O}_{\mathsf{Corrupt}}$ queries.	$Q_{\mathsf{Corr}}nk\gamma^{\mathsf{Sample}}_{n,m,\epsilon}+2q^{-n}$
G_3 to G_4	$\mathbf{T_A}$ no more used for $\mathcal{O}_{\mathsf{Sign}}$ queries.	$Q_{\mathsf{S}}\big(\gamma^{\mathsf{Sample}}_{n,m+nk,\epsilon}+nk(2\epsilon+\gamma^{\mathsf{Sample}}_{n,m,\epsilon})+4q^{-n/8}$ $+(1+nk)\mathsf{mx}\big)+2nkq^{-0.196n}+6q^{-n/8}$
G_4 to G_5	$\mathbf{A}$ is taken uniformly.	$nkq^{-0.196n}$

Minoration of advantage of last game: $\mathsf{Adv}^{\mathsf{G}_5}_{\mathcal{A}} \le \left(\frac{2}{1-q^{-n}}\right)\mathsf{Adv}^{\mathsf{SIS}_{n,m,\mathsf{Bound}_{\mathsf{SIS}},q}}_{\mathcal{B}}+\frac{4q^{-n}}{1-q^{-n}}$

Table 3. Summary of the changes between the games used for the proof of Theorem 2. Complete games are given in Appendix D.2.

Proof. We sum up the changes between games in Table 3.

From $\mathsf{G}_0 = \mathsf{EUFnaCMA}^{\mathsf{IBS}_{\mathsf{NA},\mathbb{Z}}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}$ to G_1: In G_1, the probability distribution of outputs of H_1, $\mathsf{U}\left(\mathbb{Z}_q^{n\times nk}\right)$, is replaced by $\mathcal{D}^{nk}_{\mathbb{Z},s_{\mathsf{id}},\mathbf{A}}+\mathbf{G}$ for $\mathsf{id}\in\mathsf{AskedSk}$ and $\mathcal{U}^{nk}_{\mathbf{A}}$ else. Moreover, we abort if the matrix $\mathbf{A}$ is sampled in the set fail_1 defined as $\left\{\mathbf{A}:\ \mathsf{SD}\Big(\mathcal{D}_{\mathbb{Z},s_{\mathsf{id}},\mathbf{A}},\mathsf{U}\left(\mathbb{Z}_q^n\right)\Big)>\epsilon\vee\mathsf{SD}\big(\mathcal{U}_{\mathbf{A}},\mathsf{U}\left(\mathbb{Z}_q^n\right)\big)>q^{-n/4}\right\}$. Using Lemma 1, Proposition 1 and Proposition 2 we see that $\Pr[\mathsf{fail}_1]\le nkq^{-0.196n}+3q^{-n/4}$. Moreover, when fail_1 is not realized, we have

$$\mathsf{SD}\Big(\mathcal{D}^{nk}_{\mathbb{Z},s_{\mathsf{id}},\mathbf{A}}+\mathbf{G},\mathsf{U}\left(\mathbb{Z}_q^{n\times nk}\right)\Big)=\mathsf{SD}\Big(\mathcal{D}^{nk}_{\mathbb{Z},s_{\mathsf{id}},\mathbf{A}},\mathsf{U}\left(\mathbb{Z}_q^{n\times nk}\right)\Big)\le 2nk\epsilon\ ,$$
$$\mathsf{SD}\Big(\mathcal{U}^{nk}_{\mathbf{A}},\mathsf{U}\left(\mathbb{Z}_q^{n\times nk}\right)\Big)\le nkq^{-n/4}\ .$$

Proposition 7 implies that $\left|\mathsf{Adv}^{\mathsf{G}_0}_{\mathcal{A}}-\mathsf{Adv}^{\mathsf{G}_1}_{\mathcal{A}}\right|$ is less than the upper bound indicated in Table 3.

From G_1 to G_2: In G_2, the probability distribution of outputs of H_2, $\mathsf{U}\left(\mathbb{Z}_q^n\right)$, is replaced by $\mathcal{D}_{\mathbb{Z},s_{\mathsf{sign}},(\mathbf{A}\|\mathsf{H}_1(\mathsf{id}))}$ for $(\mathsf{id},\mu)\in\mathsf{AskedSign}$ and $\mathcal{U}_{\mathbf{A}}$ else. Moreover, with the notation $\mathsf{IdAskedForSign}=\{\mathsf{id}\in\mathsf{SetId}:\ \exists\mu\in\mathsf{SetMess},(\mathsf{id},\mu)\in\mathsf{AskedSign}\}$, so $|\mathsf{IdAskedForSign}|=Q_{\mathsf{IdSign}}$, we abort if the event fail_2 happens, where fail_2 is defined as $\left\{\exists\mathsf{id}\in\mathsf{IdAskedForSign}:\ \mathsf{SD}\Big(\mathcal{D}_{\mathbb{Z},s_{\mathsf{sign}},(\mathbf{A}\|\mathsf{H}_1(\mathsf{id}))},\mathsf{U}\left(\mathbb{Z}_q^n\right)\Big)>2\epsilon\right\}$.

We will use Proposition 7 with the size of partitions bounded by $Q_{\mathsf{IdSign}}+1$. We note that $\Pr[\mathsf{fail}_2:\ \mathbf{A}\leftarrow\mathsf{Trap}(n,m,q)\wedge\mathsf{H}_1\text{ as in }\mathsf{G}_1]$ is upper bounded by

$$\begin{aligned}
&\Pr\Big[\exists\mathsf{id}\in\mathsf{IdAskedForSign},\mathsf{SD}\Big(\mathcal{D}_{\mathbb{Z},s_{\mathsf{sign}},(\mathbf{A}\|\mathsf{H}_1(\mathsf{id}))},\mathsf{U}\left(\mathbb{Z}_q^n\right)\Big)>2\epsilon\colon {\scriptstyle\mathbf{A}\leftarrow\mathsf{Trap}(n,m,q)\atop\mathsf{H}_1\text{ as in }\mathsf{G}_1}\Big]\\
&\le\Pr\Big[\exists\mathsf{id}\in\mathsf{IdAskedForSign},\mathsf{SD}\Big(\mathcal{D}_{\mathbb{Z},s_{\mathsf{sign}},((\mathbf{A}\|\mathsf{H}_1(\mathsf{id}))},\mathsf{U}\left(\mathbb{Z}_q^n\right)\Big)>2\epsilon\colon {\scriptstyle\mathbf{A}\leftarrow\$\mathbb{Z}_q^{n\times m}\atop\forall\mathsf{id}\colon\mathsf{H}_1(\mathsf{id})\leftarrow\$\mathbb{Z}_q^{nk}}\Big]\\
&\quad+Q_{\mathsf{IdSign}}\,\mathsf{mx}+nkq^{-0.196n}\quad\text{by definition of }\mathsf{fail}_1\text{ and Proposition 2}\\
&\le Q_{\mathsf{IdSign}}(2q^{-n/4}+\mathsf{mx})+nkq^{-0.196n}\quad\text{by Corollary 5.}
\end{aligned}$$

We can then apply Proposition 7 to deduce that $\left|\mathsf{Adv}^{\mathsf{G}_1}_{\mathcal{A}}-\mathsf{Adv}^{\mathsf{G}_2}_{\mathcal{A}}\right|$ is less than the upper bounds indicated in Table 3.

From G_2 to G_3: In G_3, for $\mathsf{id} \in \mathsf{AskedSk}$, the secret key $\mathsf{sk}_{\mathsf{id}}$, is defined as the value $\mathbf{R}_{\mathsf{id}}$ of $\mathsf{H}_1(\mathsf{id}) := \mathbf{A}\mathbf{R}_{\mathsf{id}} + \mathbf{G}$, instead of being created by $\mathsf{DelTrap}$. Using Proposition 4, we conclude that $\left|\mathsf{Adv}^{\mathsf{G}_2}_{\mathcal{A}} - \mathsf{Adv}^{\mathsf{G}_3}_{\mathcal{A}}\right| \leq Q_{\mathsf{Corr}} nk\gamma^{\mathsf{Sample}}_{n,m,\epsilon} + 2q^{-n}$.

From G_3 to G_4: In game G_4, for $(\mathsf{id}, \mu) \in \mathsf{AskedSign}$, the signatures $\mathbf{z}_{\mathsf{id},\mu}$, are defined as the $\mathbf{z}$ used to create the hash value $\mathsf{H}_2(\mathsf{id}, \mu) = [\mathbf{A}|\mathsf{H}_1(\mathsf{id})]\mathbf{z}$, instead of being computed by Sign applied to a secret key computed with KeyExt. Thus, the probability distribution of a signature is now $\mathcal{D}^{m+nk}_{\mathbb{Z},s_{\mathsf{sign}}}$.

Using Proposition 5 and the definitions of fail_1 and fail_2, we conclude that $\left|\mathsf{Adv}^{\mathsf{G}_3}_{\mathcal{A}} - \mathsf{Adv}^{\mathsf{G}_4}_{\mathcal{A}}\right|$ is less than the upper bound indicated in Table 3.

From G_4 to G_5: We replace the $\mathbf{A}$ made by Trap by a matrix $\mathbf{A} \hookleftarrow\$\ \mathbb{Z}_q^{n\times m}$. This is possible because the trapdoor $\mathbf{T}_{\mathbf{A}}$ is not used in G_4. We use Proposition 2 to conclude that $\left|\mathsf{Adv}^{\mathsf{G}_4}_{\mathcal{A}} - \mathsf{Adv}^{\mathsf{G}_5}_{\mathcal{A}}\right| \leq nkq^{-0.196n}$.

From G_5 to $\mathsf{SIS}_{n,m,\mathsf{Bound}_{\mathsf{SIS}},q}$: Thanks to the definition of G_5, we can simulate an instance of G_5 to $\mathcal{A}$ from an instance $\mathbf{A}$ of the $\mathsf{SIS}_{n,m,\mathsf{Bound}_{\mathsf{SIS}},q}$ problem.

Suppose $\mathcal{A}$ wins an instance of the game with the answer $(\mathbf{z}^* = (\mathbf{z}_1^*, \mathbf{z}_2^*), \mathsf{id}^*, \mu^*)$. This implies that $[\mathbf{A} \mid \mathsf{H}_1(\mathsf{id})]\mathbf{z}^* = \mathsf{H}_2(\mathsf{id}^*, \mu^*)$, $\|\mathbf{z}_1^*\| \leq \mathsf{Bound}_1$, $\|\mathbf{z}_2^*\| \leq \mathsf{Bound}_2$, $\mathsf{id}^* \notin \mathsf{AskedSk}$ and $(\mathsf{id}^*, \mu^*) \notin \mathsf{AskedSign}$. Thus:

- There exists $\mathbf{R}_{\mathsf{id}^*}$ which has been sampled uniformly in $\{-1, 0, 1\}^{m\times nk}$ such that $\mathsf{H}_1(\mathsf{id}) = \mathbf{A}\mathbf{R}_{\mathsf{id}}$.
- There exists $\mathbf{z}_{\mathsf{id}^*,\mu^*}$ which has been sampled uniformly in $\{-1, 0, 1\}^m$ such that $\mathsf{H}_2(\mathsf{id}, \mu) = \mathbf{A}\mathbf{z}_{\mathsf{id}^*,\mu^*}$.

This implies that $\mathbf{A}\left[\mathbf{z}_1^* + \mathbf{R}_{\mathsf{id}^*}\mathbf{z}_2^* - \mathbf{z}_{\mathsf{id}^*,\mu^*}\right] = 0$. Moreover, using Corollary 1 and the bounds on $\mathbf{z}_1^*, \mathbf{z}_2^*$, we know that with a probability less than at least $1 - 2q^{-n}$ on $\mathbf{R}_{\mathsf{id}^*}$, we have

$$\begin{aligned}\left\|\mathbf{z}_1^* + \mathbf{R}_{\mathsf{id}^*}\mathbf{z}_2^* - \mathbf{z}_{\mathsf{id}^*,\mu^*}\right\| &\leq \|\mathbf{z}_1^*\| + \mathsf{s}_1(\mathbf{R}_{\mathsf{id}^*})\,\|\mathbf{z}_2^*\| + \left\|\mathbf{z}_{\mathsf{id}^*,\mu^*}\right\| \\ &\leq \mathsf{Bound}_1 + \mathsf{s}_1(\mathsf{Unif})[m, nk]\,\mathsf{Bound}_2 + \sqrt{m} = \mathsf{Bound}_{\mathsf{SIS}}\ .\end{aligned}$$

If $\mathbf{z}_1^* + \mathbf{R}_{\mathsf{id}^*}\mathbf{z}_2^* \neq \mathbf{z}_{\mathsf{id}^*,\mu^*}$, it is a valid solution of the SIS problem.

We show that, for an overwhelming number of $\mathbf{A}$, the case where $\mathbf{z}_1^* + \mathbf{R}_{\mathsf{id}^*}\mathbf{z}_2^* = \mathbf{z}_{\mathsf{id}^*,\mu^*}$ happens with lower probability than the previous case, which implies that the attack fails with probability at most $1/2$. Assume that $\mathbf{z}_1^* + \mathbf{R}_{\mathsf{id}^*}\mathbf{z}_2^* = \mathbf{z}_{\mathsf{id}^*,\mu^*}$. From the point of view of $\mathcal{A}$, the instance of the game G_5 it is playing is identical for each $\tilde{\mathbf{z}}_{\mathsf{id}^*,\mu^*} \in \{-1, 0, 1\}^m$ such that $\mathbf{A}\tilde{\mathbf{z}}_{\mathsf{id}^*,\mu^*} = \mathbf{A}\mathbf{z}_{\mathsf{id}^*,\mu^*}$. Moreover, Lemma 21 shows that, with a probability more that $1 - q^{-n}$ in $\mathbf{z}_{\mathsf{id}^*,\mu^*}$, an element $\tilde{\mathbf{z}}_{\mathsf{id}^*,\mu^*} \in \{-1, 0, 1\}^m$, $\mathbf{z}_{\mathsf{id}^*,\mu^*} \neq \tilde{\mathbf{z}}_{\mathsf{id}^*,\mu^*}$, such that $\mathbf{A}\mathbf{z}_{\mathsf{id}^*,\mu^*} = \mathbf{A}\tilde{\mathbf{z}}_{\mathsf{id}^*,\mu^*}$, could have been taken with the same probability as $\mathbf{z}_{\mathsf{id}^*,\mu^*}$ for the computation of $\mathsf{H}_2(\mathsf{id}, \mu)$. Such an element would satisfy $\mathbf{z}_1^* + \mathbf{R}_{\mathsf{id}^*}\mathbf{z}_2^* \neq \tilde{\mathbf{z}}_{\mathsf{id}^*,\mu^*}$. Therefore, from the point of view of the adversary, the probability that $\mathbf{z}_1^* + \mathbf{R}_{\mathsf{id}^*}\mathbf{z}_2^* \neq \mathbf{z}_{\mathsf{id}^*,\mu^*}$ is at least $1/2$.

We conclude that $\mathsf{Adv}^{\mathsf{SIS}_{n,m,\mathsf{Bound}_{\mathsf{SIS}},q}}_{\mathcal{B}}$ is more than $\left(\frac{1-q^{-n}}{2}\right)\mathsf{Adv}^{\mathsf{G}_5}_{\mathcal{A}} + 2q^{-n}$, which leads to the upper bound indicated in Table 3.

7 IBS Scheme in ROM and the QROM, based on RSIS

The scheme is defined in Figure 7. The parameters and the conditions they must follow are on Table 4.

The proof of completeness will use the tail inequality.

Lemma 3 (Tail inequality, ring case (*e.g.* [3])). *Let $l \in \mathbb{N}$, $\sigma > 1$, then* $\Pr_{\mathbf{z}\hookleftarrow\$\mathcal{D}^l_{\mathcal{R},\sigma}}\left[\|\mathbf{z}\| > \sqrt{2dl}\sigma\right] < 2^{-\frac{dl}{4}}$.

$\mathsf{Setup}(n, m)$	$\mathsf{Sign}(\mathsf{mpk}, (\mathbf{r}, \mathsf{id}, \mathbf{T}_{\mathsf{id}}), \mu)$	$\mathsf{Verify}\,(\mathsf{mpk}, \mathsf{id}, \mu, (\mathbf{r}, \mathbf{s}, \mathbf{z}))$
$(\mathbf{A}, \mathbf{T_A}) \leftarrow \mathsf{Trap}_{\mathcal{R}}(l, q)$	$\mathbf{s} \leftarrow\!\!\$\ \{0,1\}^{\tau_{\mathsf{nonce}}}$	**if** $\mathbf{z} = \mathbf{0} \vee [\mathbf{A} \Vert \mathsf{H}_1(\mathbf{r}, \mathsf{id})]\,\mathbf{z}$
return $(\mathbf{A}, \mathbf{T_A})$	$\mathbf{u} \leftarrow \mathsf{H}_2\,(\mathbf{r}, \mathbf{s}, \mathsf{id}, \mu)$	$\neq \mathsf{H}_2(\mathbf{r}, \mathbf{s}, \mathsf{id}, \mu)$
$\mathsf{KeyExt}(\mathbf{A}, \mathbf{T_A}, \mathsf{id})$	$\mathbf{z} \leftarrow \mathsf{SampleD}_{\mathcal{R}}\big(\,[\mathbf{A} \Vert \mathsf{H}_1(\mathbf{r}, \mathsf{id})]\,,$ $\mathbf{T}_{\mathsf{id}}, \mathbf{u}, s_{\mathsf{sign}}\big)$	**then return** 0
		$/\!/\ \mathbf{z} = (\mathbf{z}_1, \mathbf{z}_2) \in \mathcal{R}_q^l \times \mathcal{R}_q^k$
$\mathbf{r} \leftarrow\!\!\$\ \{0,1\}^{\tau_{\mathsf{nonce}}}$	**return** $(\mathbf{r}, \mathbf{s}, \mathbf{z})$	**return** $[\![\Vert\mathbf{z}_1\Vert \leq \mathsf{Bound}_{\mathcal{R},1}$
$\mathbf{T}_{\mathsf{id}} \leftarrow \mathsf{DelTrap}_{\mathcal{R}}(\mathbf{A}, \mathbf{T_A},$		$\wedge\ \Vert\mathbf{z}_2\Vert \leq \mathsf{Bound}_{\mathcal{R},2}]\!]$
$\mathsf{H}_1(\mathbf{r}, \mathsf{id}), s_{\mathsf{id}})$		
return $(\mathbf{r}, \mathbf{T}_{\mathsf{id}})$		

Fig. 7. Scheme $\mathsf{IBS}_{\mathcal{R}}$.

Notation	Description
$q := 3^k$	modulus, power of 3 for $k \in \mathbb{N}, k \geq 4$
SetId	Set of identities, of the form $\{0,1\}^{\tau_{\mathsf{id}}}$ for some integer τ_{id}
$\mathsf{SetMess}$	Set of messages, of the form $\{0,1\}^{\tau_{\mathsf{mess}}}$ for some integer τ_{mess}
$\mathsf{SetNonces}$	Set of nonces, of the form $\{0,1\}^{\tau_{\mathsf{nonce}}}$ for some integer τ_{nonce}
l	number of columns of the matrix $\mathbf{A} \in \mathcal{R}_q^{1\times l}$, $2k + k/2 \geq l > \max(2k, 21)$
ϵ	used in $\mathsf{r}_{x,\epsilon} = \sqrt{\ln\left(2x(1+1/\epsilon)\right)/\pi}$, we take $\epsilon = \epsilon(d) = \mathsf{negl}(d)$
H_1	hash function 1, with values in $\mathcal{R}_q^{1\times k}$
H_2	hash function 2, with values in $\mathcal{R}_q$
s_{id}	standard deviation, $s_{\mathsf{id}} \geq \max\left(\sqrt{11}\mathsf{r}_{dk,\epsilon}\sqrt{16d\mathsf{s}_1(\mathsf{Binom})[l-k, dk, 1/2]^2 + 1},\ 12\mathsf{r}_{dl,\epsilon}\right)$.
s_{sign}	standard deviation, $s_{\mathsf{sign}} \geq \max\left(\sqrt{11}\mathsf{r}_{dk,\epsilon}\sqrt{d\mathsf{s}_1(\mathsf{Gauss})[l, dk, s_{\mathsf{id}}]^2 + 1},\ 12\mathsf{r}_{d(l+k),\epsilon}\right)$.
$\mathsf{Bound}_{\mathcal{R},1}$	bound of $\Vert\mathbf{z}_1\Vert$ for signatures $\mathbf{z}$=$(\mathbf{z}_1, \mathbf{z}_2) \in \mathcal{R}_q^l \times \mathcal{R}_q^k$, $\mathsf{Bound}_{\mathcal{R},1} \geq \sqrt{2dl}s_{\mathsf{sign}}$
$\mathsf{Bound}_{\mathcal{R},2}$	bound of $\Vert\mathbf{z}_2\Vert$ for signatures $\mathbf{z}$=$(\mathbf{z}_1, \mathbf{z}_2) \in \mathcal{R}_q^l \times \mathcal{R}_q^k$,$\mathsf{Bound}_{\mathcal{R},2} \geq \sqrt{2dk}s_{\mathsf{sign}}$

Table 4. Parameters of $\mathsf{IBS}_{\mathcal{R}}$ and required conditions.

Proposition 10 (completeness). *Consider the scheme $\mathsf{IBS}_{\mathcal{R}}$ with the parameters of Table 4. Then, it is (ξ_1, ξ_2)-complete with $\xi_1 = k(2\epsilon + \gamma^{\mathsf{Sample}}_{d,dl,\epsilon}) + 3^{\left(-d\frac{(2k-l)}{4}+\frac{3}{2}\right)} + 2^{-\frac{(dk-1)}{4}} = \mathsf{negl}(d)$ and $\xi_2 = 2kq^{-0.196d} + 3^{\left(-d\frac{(2k-l)}{4}+3\right)} = \mathsf{negl}(d)$.*

Proof. Direct consequence of Proposition 21 and Lemma 3 that shows that

$$Pr_{(\mathbf{z}_1,\mathbf{z}_2)\leftarrow\!\!\$\mathcal{D}^l_{\mathcal{R},s_{\mathsf{sign}}}\times\mathcal{D}^k_{\mathcal{R},s_{\mathsf{sign}}}}\left[\Vert\mathbf{z}_1\Vert > \sqrt{2ld}\sigma \vee \Vert\mathbf{z}_2\Vert > \sqrt{2dk}\sigma\right] < 2^{-\frac{dl}{4}} + 2^{-\frac{dk}{4}} < 2^{-\frac{(dk-1)}{4}}\ .$$

From adaptive security to non-adaptive security.

Proposition 11 ($\mathsf{EUF\text{-}CMA}$ security of $\mathsf{adapt}(\mathsf{IBS}_{\mathcal{R}})$ implies the $\mathsf{EUF\text{-}CMA}$ security of $\mathsf{IBS}_{\mathcal{R}}$). *Consider a set of parameters with the conditions indicated in Table 4. Let $Q_{\mathsf{Corr}}, Q_{\mathsf{S}} \in \mathbb{N}$ and $\mathcal{A}$ a PPT adversary of $\mathsf{EUFCMA}^{\mathsf{IBS}_{\mathcal{R}}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}$ (Figure 7) that makes Q_{H_1} quantum (resp. classical) queries to H_1 and Q_{H_2} quantum (resp. classical) queries to H_2. Then, there exists an adversary $\mathcal{B}$ of $\mathsf{EUFCMA}^{\mathsf{adapt}(\mathsf{IBS}_{\mathcal{R}})}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}$ that makes Q_{H_1} quantum (resp. classical) queries to H_1, Q_{H_2} quantum (resp. classical) queries to H_2, $2(Q_{\mathsf{H}_1} + Q_{\mathsf{H}_2})$ quantum (resp. $Q_{\mathsf{H}_1} + Q_{\mathsf{H}_2}$ classical) queries to $\mathsf{Hash}_{\mathsf{id}}$, and $2Q_{\mathsf{H}_2}$ quantum (resp. Q_{H_2} classical) queries to $\mathsf{Hash}_{\mathsf{mess}}$, such that $\mathsf{Adv}^{\mathsf{EUFCMA}^{\mathsf{IBS}_{\mathcal{R}}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}}_{\mathcal{A}} = \mathsf{Adv}^{\mathsf{EUFCMA}^{\mathsf{adapt}(\mathsf{IBS}_{\mathcal{R}})}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}}_{\mathcal{B}}$.*

Proof. Proof is similar to the proof of Proposition 9.

$\mathsf{Setup}()$	$\mathsf{Sign}(\mathsf{mpk}, (\mathsf{id}, \mathbf{T}_{\mathsf{id}}), \mu)$	$\mathsf{Verify}(\mathsf{mpk}, \mathsf{id}, \mu, \mathbf{z})$
$(\mathbf{A}, \mathbf{T_A}) \leftarrow \mathsf{Trap}_{\mathcal{R}}(l, q)$	$\mathbf{u} := \mathsf{H}_2(\mathsf{id}, \mu)$	**if** $\mathbf{z} = 0$ **then**
return $(\mathbf{A}, \mathbf{T_A})$	$\mathbf{z} \leftarrow \mathsf{SampleD}_{\mathcal{R}}\big([\mathbf{A} \Vert \mathsf{H}_1(\mathsf{id})], \mathbf{T}_{\mathsf{id}}, \mathbf{u}, s_{\mathsf{sign}}\big)$	**return** 0
$\mathsf{KeyExt}(\mathbf{A}, \mathbf{T_A}, \mathsf{id})$	**return** $\mathbf{z}$	**if** $[\mathbf{A} \Vert \mathsf{H}_1(\mathsf{id})]\,\mathbf{z} \neq \mathsf{H}_2(\mathsf{id}, \mu)$ **then**
$\mathbf{T}_{\mathsf{id}} \leftarrow \mathsf{DelTrap}_{\mathcal{R}}(\mathbf{A}, \mathbf{T_A}, \mathsf{H}_1(\mathsf{id}), s_{\mathsf{id}})$		**return** 0
return $(\mathsf{id}, \mathbf{T}_{\mathsf{id}})$		$/\!/\ \mathbf{z} = (\mathbf{z}_1, \mathbf{z}_2) \in \mathcal{R}_q^l \times \mathcal{R}_q^k$
		return $[\![\Vert\mathbf{z}_1\Vert \leq \mathsf{Bound}_{\mathcal{R},1} \wedge \Vert\mathbf{z}_2\Vert \leq \mathsf{Bound}_{\mathcal{R},2}]\!]$

Fig. 8. Scheme $\mathsf{IBS}_{\mathsf{NA},\mathcal{R}}$.

Non-adaptive Security in the ROM and the QROM.

Theorem 3 ($\mathsf{EUF\text{-}naCMA}$ **security of** $\mathsf{IBS}_{\mathsf{NA},\mathcal{R}}$**).** *Consider a set of parameters with the conditions indicated in Table 4. Let* $Q_{\mathsf{Corr}}, Q_{\mathsf{S}} \in \mathbb{N}$ *and* $\mathcal{A}$ *a PPT adversary of* $\mathsf{EUFnaCMA}^{\mathsf{IBS}_{\mathsf{NA},\mathcal{R}}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}$ *that makes* Q_{H_1} *quantum queries to* H_1*,* Q_{H_2} *quantum queries to* H_2 *and such that at most* Q_{IdSign} *signatures are queried for the same identity. Let also, take* $\mathsf{Bound}_{\mathsf{RSIS}} = \mathsf{Bound}_{\mathcal{R},1} + 4\sqrt{d}\mathsf{s}_1(\mathsf{Unif})[l, dk]\,\mathsf{Bound}_{\mathcal{R},2} + \sqrt{17/2}\sqrt{ld}$ *and* $\mathsf{mx} = \max(2\epsilon, q^{-d/4}) = \mathsf{negl}(d)$*. Then, there exists a PPT adversary* $\mathcal{B}$ *of* $\mathsf{RSIS}_{l,\mathsf{Bound}_{\mathsf{RSIS}},q}$ *such that* $\mathsf{Adv}^{\mathsf{EUFnaCMA}^{\mathsf{IBS}_{\mathsf{NA},\mathcal{R}}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}}_{\mathcal{A}}$ *is upper bounded by*

$$\begin{aligned}
&\frac{2\mathsf{Adv}^{\mathsf{RSIS}_{l,\mathsf{Bound}_{\mathsf{RSIS}},q}}_{\mathcal{B}}}{1-q^{-d}} + 4Q_{\mathsf{H}_1}^2\sqrt{2k\mathsf{mx}} + 4Q_{\mathsf{H}_2}^2\sqrt{Q_{\mathsf{IdSign}}+1}\sqrt{\mathsf{mx}} \\
&+Q_{\mathsf{Corr}}k\left(\mathsf{mx}+\gamma^{\mathsf{Sample}}_{d,dl,\epsilon}\right)+5kq^{-0.196d}+3^{\left(-d\frac{2k-l}{4}+4\right)}+Q_{\mathsf{IdSign}}\left(2*3^{-d\frac{(2k-l)}{2}}+\mathsf{mx}\right) \\
&+Q_{\mathsf{S}}\left(\gamma^{\mathsf{Sample}}_{d,d(k+l)\epsilon}+k(2\epsilon+\gamma^{\mathsf{Sample}}_{d,dl,\epsilon})+3^{\left(-d\frac{(2k-l)}{4}+\frac{3}{2}\right)}+(k+2)\mathsf{mx}\right)+\frac{4q^{-d}}{1-q^{-d}}\ ,
\end{aligned}$$

where $\gamma^{\mathsf{Sample}}_{d,dl,\epsilon}$ *is negligible and is defined in Section B.9.*

If the queries to Q_{H_1} *and* Q_{H_2} *are classical, the upper bound becomes*

$$\begin{aligned}
&\frac{2\mathsf{Adv}^{\mathsf{RSIS}_{l,\mathsf{Bound}_{\mathsf{RSIS}},q}}_{\mathcal{B}}}{1-q^{-d}} + Q_{\mathsf{H}_1}k\mathsf{mx} + Q_{\mathsf{H}_2}\mathsf{mx} \\
&+Q_{\mathsf{Corr}}k\left(\mathsf{mx}+\gamma^{\mathsf{Sample}}_{d,dl,\epsilon}\right)+5kq^{-0.196d}+3^{\left(-d\frac{2k-l}{4}+4\right)}+Q_{\mathsf{IdSign}}\left(2*3^{-d\frac{(2k-l)}{2}}+\mathsf{mx}\right) \\
&+Q_{\mathsf{S}}\left(\gamma^{\mathsf{Sample}}_{d,d(k+l)\epsilon}+k(2\epsilon+\gamma^{\mathsf{Sample}}_{d,dl,\epsilon})+3^{\left(-d\frac{(2k-l)}{4}+\frac{3}{2}\right)}+(k+2)\mathsf{mx}\right)+\frac{4q^{-d}}{1-q^{-d}}\ .
\end{aligned}$$

Proof. We sum up the changes between games in Table 5.

From $\mathsf{G}_0 = \mathsf{EUFnaCMA}^{\mathsf{IBS}_{\mathsf{NA},\mathcal{R}}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}$ **to** G_1**:** In G_1, the probability distribution of outputs of H_1, $\mathsf{U}\left(\mathcal{R}_q^{1\times k}\right)$, is replaced by $\mathcal{D}^k_{\mathcal{R},s_{\mathsf{id}},\mathbf{A}} + \mathbf{G}$ for $\mathsf{id} \in \mathsf{AskedSk}$ and $\mathcal{U}^k_{\mathcal{R},\mathbf{A}}$ else. Moreover, we abort if $\mathbf{A}$ is sampled in the set

$$\mathsf{fail}_1 = \left\{\mathbf{A} :\ \mathsf{SD}\big(\mathcal{D}_{\mathcal{R},s_{\mathsf{id}},\mathbf{A}}, \mathsf{U}\left(\mathcal{R}_q\right)\big) > \epsilon \vee \mathsf{SD}\big(\mathcal{U}_{\mathcal{R},\mathbf{A}}, \mathsf{U}\left(\mathcal{R}_q\right)\big) > q^{-d/4}\right\}\ .$$

Hop	Change	Security loss
G_0 to G_1	reprogramming of H_1.	ROM: $(Q_{\mathsf{H}_1}+Q_{\mathsf{Corr}})\,k\mathsf{mx}+kq^{-0.196d}+3^{-d\frac{(2k-l)}{2}+1}$ QROM: $Q_{\mathsf{Corr}}\,k\mathsf{mx}+4Q_{\mathsf{H}_1}^2\sqrt{2k\mathsf{mx}}+kq^{-0.196d}+3^{-d\frac{(2k-l)}{2}+1}$
G_1 to G_2	reprogramming of H_2.	ROM: $(Q_{\mathsf{H}_2}+Q_{\mathsf{S}})\,\mathsf{mx}+Q_{\mathsf{IdSign}}(2*3^{-d\frac{(2k-l)}{2}}+\mathsf{mx})+kq^{-0.196d}$ QROM: $Q_{\mathsf{S}}\,\mathsf{mx}+4Q_{\mathsf{H}_2}^2\sqrt{(Q_{\mathsf{IdSign}}+1)\mathsf{mx}}$ $+Q_{\mathsf{IdSign}}(2*3^{-d\frac{(2k-l)}{2}}+\mathsf{mx})+kq^{-0.196d}$
G_2 to G_3	$\mathbf{T_A}$ no more used for $\mathcal{O}_{\mathsf{Corrupt}}$ queries.	$Q_{\mathsf{Corr}}k\gamma^{\mathsf{Sample}}_{d,dl,\epsilon}+2q^{-d}$
G_3 to G_4	$\mathbf{T_A}$ no more used for $\mathcal{O}_{\mathsf{Sign}}$ queries.	$Q_{\mathsf{S}}\big(\gamma^{\mathsf{Sample}}_{d,d(k+l)\epsilon}+k(2\epsilon+\gamma^{\mathsf{Sample}}_{d,dl,\epsilon})+3^{-d\frac{(2k-l)}{4}+\frac{3}{2}}$ $+(k+1)\mathsf{mx}\big)+2kq^{-0.196d}+3^{-d\frac{2k-l}{4}+3}$.
G_4 to G_5	$\mathbf{A}$ is taken uniformly.	$kq^{-0.196d}$
Minoration of advantage of last game: $\mathsf{Adv}^{\mathsf{G}_5}_{\mathcal{A}}\leq\left(\frac{2}{1-q^{-d}}\right)\mathsf{Adv}^{\mathsf{RSIS}_{l,\mathsf{Bound}_{\mathsf{RSIS}},q}}_{\mathcal{B}}+\frac{4q^{-d}}{1-q^{-d}}$		

Table 5. Summary of the changes between the games used for the proof of Theorem 3. Complete games are similar of the ones of the proof of Theorem 2.

Using Lemma 1, Proposition 1 and Proposition 18 we see that $\Pr[\mathsf{fail}_1]\leq kq^{-0.196d}+3^{-d\frac{(2k-l)}{2}+1}$. Moreover, when fail_1 is not realized, we have

$$\mathsf{SD}\Big(\mathcal{D}^k_{\mathcal{R},s_{\mathsf{id}},\mathbf{A}}+\mathbf{G},\mathsf{U}\left(\mathcal{R}_q^{1\times k}\right)\Big)=\mathsf{SD}\Big(\mathcal{D}^k_{\mathcal{R},s_{\mathsf{id}},\mathbf{A}},\mathsf{U}\left(\mathcal{R}_q^{1\times k}\right)\Big)\leq 2k\epsilon\ ,$$
$$\mathsf{SD}\Big(\mathcal{U}^k_{\mathcal{R},\mathbf{A}},\mathsf{U}\left(\mathcal{R}_q^{1\times k}\right)\Big)\leq kq^{-d/4}\ .$$

Proposition 7 implies that $\left|\mathsf{Adv}^{\mathsf{G}_0}_{\mathcal{A}}-\mathsf{Adv}^{\mathsf{G}_1}_{\mathcal{A}}\right|$ is less than

$$\text{in the ROM: } (Q_{\mathsf{H}_1}+Q_{\mathsf{Corr}})\,k\mathsf{mx}+kq^{-0.196d}+3^{-d\frac{(2k-l)}{2}+1}\ ,$$
$$\text{in the QROM: } Q_{\mathsf{Corr}}k\mathsf{mx}+4Q_{\mathsf{H}_1}^2\sqrt{2k\mathsf{mx}}+kq^{-0.196d}+3^{-d\frac{(2k-l)}{2}+1}\ .$$

From G_1 to G_2: In G_2, the probability distribution of outputs of H_2, $\mathsf{U}(\mathcal{R}_q)$, is replaced by $\mathcal{D}_{\mathcal{R},s_{\mathsf{sign}},(\mathbf{A}\|\mathsf{H}_1(\mathsf{id}))}$ for $(\mathsf{id},\mu)\in\mathsf{AskedSign}$ and $\mathcal{U}_{\mathcal{R},\mathbf{A}}$ else. Moreover, with notation $\mathsf{IdAskedForSign}=\{\mathsf{id}\in\mathsf{SetId}:\ \exists\mu\in\mathsf{SetMess},(\mathsf{id},\mu)\in\mathsf{AskedSign}\}$, so $|\mathsf{IdAskedForSign}|=Q_{\mathsf{IdSign}}$, we abort if the event fail_2 happens, where

$$\mathsf{fail}_2=\left\{\exists\mathsf{id}\in\mathsf{IdAskedForSign}:\ \mathsf{SD}\Big(\mathcal{D}_{s_{\mathsf{sign}},(\mathbf{A}\|\mathsf{H}_1(\mathsf{id}))},\mathsf{U}\left(\mathcal{R}_q\right)\Big)>2\epsilon\right\}\ .$$

We use Proposition 7 with the size of partitions bounded by $Q_{\mathsf{IdSign}}+1$.
We note that

$$\begin{aligned}
&\Pr[\mathsf{fail}_2\ :\ \mathbf{A}\leftarrow\mathsf{Trap}_{\mathcal{R}}(l,q)\wedge\mathsf{H}_1\text{programmed as in }\mathsf{G}_1]\\
&=\Pr\Big[\exists\mathsf{id}\in\mathsf{IdAskedForSign}:\ \mathsf{SD}\Big(\mathcal{D}_{\mathcal{R},s_{\mathsf{sign}},(\mathbf{A}\|\mathsf{H}_1(\mathsf{id}))},\mathsf{U}\left(\mathcal{R}_q\right)\Big)>2\epsilon\ :\ \substack{\mathbf{A}\leftarrow\mathsf{Trap}_{\mathcal{R}}(l,q)\\ \mathsf{H}_1\text{ as in }\mathsf{G}_1}\Big]\\
&\leq\Pr\Big[\exists\mathsf{id}\in\mathsf{IdAskedForSign}:\ \mathsf{SD}\Big(\mathcal{D}_{\mathcal{R},s_{\mathsf{sign}},(\mathbf{A}\|\mathsf{H}_1(\mathsf{id}))},\mathsf{U}\left(\mathcal{R}_q\right)\Big)>2\epsilon\ :\ \substack{\mathbf{A}\leftarrow\$\,\mathcal{R}_q^{n\times m}\\ \forall\mathsf{id}:\,\mathsf{H}_1(\mathsf{id})\leftarrow\$\,\mathcal{R}_q^k}\Big]\\
&\quad+Q_{\mathsf{IdSign}}\,\mathsf{mx}+kq^{-0.196d}\quad\text{by definition of }\mathsf{fail}_1\text{ and Proposition 18}\\
&\leq Q_{\mathsf{IdSign}}(2*3^{-d\frac{(2k-l)}{2}}+\mathsf{mx})+kq^{-0.196d}\quad\text{by Corollary 5.}
\end{aligned}$$

We can then apply Proposition 7 to deduce that $\left|\mathsf{Adv}^{\mathsf{G}_1}_{\mathcal{A}} - \mathsf{Adv}^{\mathsf{G}_2}_{\mathcal{A}}\right|$ is less than

$$\text{in the ROM: } (Q_{\mathsf{H}_2}+Q_{\mathsf{S}})\,\mathsf{mx}+Q_{\mathsf{IdSign}}(2*3^{-d\frac{(2k-l)}{2}}+\mathsf{mx})+kq^{-0.196d}\ ,$$
$$\text{in the QROM: } Q_{\mathsf{S}}\,\mathsf{mx}+4Q^2_{\mathsf{H}_2}\sqrt{(Q_{\mathsf{IdSign}}+1)\mathsf{mx}}+Q_{\mathsf{IdSign}}(2*3^{-d\frac{(2k-l)}{2}}+\mathsf{mx})+kq^{-0.196d}\ .$$

From G_2 to G_3:

In G_3, for $\mathsf{id} \in \mathsf{AskedSk}$, the secret key $\mathsf{sk}_{\mathsf{id}}$, instead of being created by $\mathsf{DelTrap}_{\mathcal{R}}$, is defined as the value $\mathbf{R}_{\mathsf{id}}$ of $\mathsf{H}_1(\mathsf{id}) := \mathbf{A}\mathbf{R}_{\mathsf{id}}+\mathbf{G}$. Using Proposition 20, we conclude that $\left|\mathsf{Adv}^{\mathsf{G}_2}_{\mathcal{A}} - \mathsf{Adv}^{\mathsf{G}_3}_{\mathcal{A}}\right| \leq Q_{\mathsf{Corr}}k\gamma^{\mathsf{Sample}}_{d,dl,\epsilon} + 2q^{-d}$.

From G_3 to G_4: In game G_4, for $(\mathsf{id},\mu) \in \mathsf{AskedSign}$, the signatures $\mathbf{z}_{\mathsf{id},\mu}$, instead of being computed by Sign applied to a secret key computed with KeyExt, are now being defined as the $\mathbf{z}$ used to create the hash value $\mathsf{H}_2(\mathsf{id},\mu) = [\mathbf{A}|\mathsf{H}_1(\mathsf{id})]\mathbf{z}$. Thus, the probability distribution of a signature is now $\mathcal{D}^{l+k}_{\mathcal{R},s_{\mathsf{sign}}}$. Using Proposition 21 and the definitions of fail_1 and fail_2, we conclude that $\left|\mathsf{Adv}^{\mathsf{G}_3}_{\mathcal{A}} - \mathsf{Adv}^{\mathsf{G}_4}_{\mathcal{A}}\right|$ is less than the upper bound indicated in Table 5.

From G_4 to G_5: We replace the $\mathbf{A}$ made by Trap by a matrix $\mathbf{A} \hookleftarrow \mathcal{R}_q^{1\times l}$. This is possible because the trapdoor $\mathbf{T_A}$ is not used in G_4 . We use Proposition 2 to conclude that $\left|\mathsf{Adv}^{\mathsf{G}_4}_{\mathcal{A}} - \mathsf{Adv}^{\mathsf{G}_5}_{\mathcal{A}}\right| \leq kq^{-0.196d}$.

From G_5 to $\mathsf{RSIS}_{l,\mathsf{Bound}_{\mathsf{RSIS}},q}$: Thanks to the definition of G_5, we can simulate an instance of G_5 to $\mathcal{A}$ from an instance $\mathbf{A}$ of the $\mathsf{RSIS}_{l,\mathsf{Bound}_{\mathsf{RSIS}},q}$ problem.

Suppose $\mathcal{A}$ wins an instance of the game with the answer $(\mathbf{z}^* = (\mathbf{z}_1^*, \mathbf{z}_2^*), \mathsf{id}^*, \mu^*)$. This implies that

$$[\mathbf{A} \mid \mathsf{H}_1(\mathsf{id})]\mathbf{z}^* = \mathsf{H}_2(\mathsf{id}^*,\mu^*),\ \|\mathbf{z}_1^*\| \leq \mathsf{Bound}_{\mathcal{R},1},\ \|\mathbf{z}_2^*\| \leq \mathsf{Bound}_{\mathcal{R},2}\ , \tag{4}$$

and $\mathsf{id}^* \notin \mathsf{AskedSk}$, $(\mathsf{id}^*,\mu^*) \notin \mathsf{AskedSign}$. Thus:

- There exists $\mathbf{R}_{\mathsf{id}^*}$ that has been sampled uniformly in $\mathcal{S}^{l\times k}_{\mathsf{R}}$ such that $\mathsf{H}_1(\mathsf{id}) = \mathbf{A}\mathbf{R}_{\mathsf{id}}$.
- There exists $\mathbf{z}_{\mathsf{id}^*,\mu^*}$ that has been sampled uniformly in $\mathcal{S}^{l}_{\mathsf{R}}$ such that $\mathsf{H}_2(\mathsf{id},\mu) = \mathbf{A}\mathbf{z}_{\mathsf{id}^*,\mu^*}$.

We write $\mathbf{z}^* = (\mathbf{z}_1^*, \mathbf{z}_2^*) \in \mathcal{R}_q^m \times \mathcal{R}_q^k$. Equation (4) becomes $\mathbf{A}\left[\mathbf{z}_1^* + \mathbf{R}_{\mathsf{id}^*}\mathbf{z}_2^* - \mathbf{z}_{\mathsf{id}^*,\mu^*}\right] = 0$. Moreover, using Corollary 1 and Proposition 15, we know that with a probability less that at least $1-2q^{-d}$ on $\mathbf{R}_{\mathsf{id}^*}$, we have

$$\begin{aligned}\left\|\mathbf{z}_1^* + \mathbf{R}_{\mathsf{id}^*}\mathbf{z}_2^* - \mathbf{z}_{\mathsf{id}^*,\mu^*}\right\| &\leq \|\mathbf{z}_1^*\| + \sqrt{d}\mathsf{s}_1(\mathbf{R}_{\mathsf{id}^*})\,\|\mathbf{z}_2^*\| + \left\|\mathbf{z}_{\mathsf{id}^*,\mu^*}\right\| \\ &\leq \mathsf{Bound}_{\mathcal{R},1} + 4\sqrt{d}\mathsf{s}_1(\mathsf{Unif})[l,dk]\,\mathsf{Bound}_{\mathcal{R},2} + \sqrt{dl}\sqrt{17/2} \\ &= \mathsf{Bound}_{\mathsf{RSIS}}\ ,\end{aligned}$$

where we use $\left\|\mathcal{S}^l_{\mathsf{R}}\right\| \leq \sqrt{d(l/2)(4^2+1)} = \sqrt{dl}\sqrt{17/2}$.

If $\mathbf{z}_1^* + \mathbf{R}_{\mathsf{id}^*}\mathbf{z}_2^* \neq \mathbf{z}_{\mathsf{id}^*,\mu^*}$, it is a valid solution of the RSIS problem.

We show that, for an overwhelming number of $\mathbf{A}$, the case where $\mathbf{z}_1^* + \mathbf{R}_{\mathsf{id}^*}\mathbf{z}_2^* = \mathbf{z}_{\mathsf{id}^*,\mu^*}$ happens with lower probability than the previous case, which implies that the attack fails with probability at most $1/2$. Assume that $\mathbf{z}_1^* + \mathbf{R}_{\mathsf{id}^*}\mathbf{z}_2^* = \mathbf{z}_{\mathsf{id}^*,\mu^*}$.

From the point of view of $\mathcal{A}$, the instance of the game G_5 it is playing is identical for each $\tilde{\mathbf{z}}_{\mathsf{id}^*,\mu^*} \in \mathcal{S}^l_{\mathsf{R}}$ such that $\mathbf{A}\tilde{\mathbf{z}}_{\mathsf{id}^*,\mu^*} = \mathbf{A}\mathbf{z}_{\mathsf{id}^*,\mu^*}$. Moreover, Lemma 22 shows that, with a probability more that $1-q^{-d}$ in $\mathbf{z}_{\mathsf{id}^*,\mu^*}$, an element $\tilde{\mathbf{z}}_{\mathsf{id}^*,\mu^*} \in \mathcal{S}^l_{\mathsf{R}}$, $\mathbf{z}_{\mathsf{id}^*,\mu^*} \neq \tilde{\mathbf{z}}_{\mathsf{id}^*,\mu^*}$, such that $\mathbf{A}\mathbf{z}_{\mathsf{id}^*,\mu^*} = \mathbf{A}\tilde{\mathbf{z}}_{\mathsf{id}^*,\mu^*}$, could have been taken with the same probability as $\mathbf{z}_{\mathsf{id}^*,\mu^*}$ for the computation of $\mathsf{H}_2(\mathsf{id},\mu)$. Such an element would satisfy $\mathbf{z}_1^* + \mathbf{R}_{\mathsf{id}^*}\mathbf{z}_2^* \neq \tilde{\mathbf{z}}_{\mathsf{id}^*,\mu^*}$. Therefore, from the point of view of the adversary, the probability that $\mathbf{z}_1^* + \mathbf{R}_{\mathsf{id}^*}\mathbf{z}_2^* \neq \mathbf{z}_{\mathsf{id}^*,\mu^*}$ is at least $1/2$.

We conclude that $\mathsf{Adv}^{\mathsf{RSIS}_{l,\mathsf{Bound}_{\mathsf{RSIS}},q}}_{\mathcal{B}}$ is more thant $\left(\frac{1-q^{-d}}{2}\right)\mathsf{Adv}^{\mathsf{G}_5}_{\mathcal{A}} - 2q^{-d}$, which leads to the upper bound indicated in Table 5.

8 Conclusion

8.1 Parameters (proof of concept) and discussion

We propose parameters to give a rough idea of the efficiency of our IBS scheme. The parameters are not optimized; the main motivation of this proof of concept is to observe the impact of the tight reduction on concrete parameters. We describe the principle behind our parameter selection in the following. First, we only study $\mathsf{IBS}_{\mathcal{R}}$ since it will be more efficient than $\mathsf{IBS}_{\mathbb{Z}}$ for the same security. Then, we reduce the study of $\mathsf{IBS}_{\mathcal{R}}$ to the study of $\mathsf{IBS}_{\mathsf{NA},\mathcal{R}}$ since the tightness of the transformation between $\mathsf{IBS}_{\mathcal{R}}$ and $\mathsf{IBS}_{\mathsf{NA},\mathcal{R}}$ provides only negligible changes of size (only nonces are added, that is, less than 1Ko) and of speed (only hash evaluations are added). It also allows us to directly compare with the non-adaptive scheme $\mathsf{IBS}_{\mathsf{NA},\mathsf{PW}}$ [26, Figure 8]. Finally, we take into account the experimental estimations of C (Section 4.2) made in [13, Section 6] in order to set $C = \frac{1}{2\pi}$ or $\frac{1}{4\pi}$ depending on the distribution. More precisely, we make the comparison with an improved version $\mathsf{IBS}^{+}_{\mathsf{NA},\mathsf{PW}}$ of $\mathsf{IBS}_{\mathsf{NA},\mathsf{PW}}$, where coefficients of the master secret key $\mathbf{T_A}$ are sampled with $\mathcal{P}_{\mathcal{R},1/2}$, as in our scheme (this method was already suggested for the unstructured case in [25] as an example of "statistical instantiation"), and setting $l = 2k + 2$ instead of $l \geq 2\lceil \log(q) \rceil + 2$ as in our scheme.

We present in Table 6 two sets of parameters, each one giving 128 bits of security for one of the two schemes. Table 7 displays the sizes and security related to the schemes $\mathsf{IBS}_{\mathsf{NA},\mathcal{R}}$ and $\mathsf{IBS}^{+}_{\mathsf{NA},\mathsf{PW}}$ for these two sets of parameters. We include in Appendix E the script we use to compute sizes and security bounds for the two schemes, and summarize the principle in the following. Regarding RSIS concrete security against a quantum adversary, we use the security estimation scripts of [10] whose initial aim was to assess the security of Kyber [2] and Dilithium [11] schemes. For $\mathsf{IBS}_{\mathsf{NA},\mathcal{R}}$ the parameters values and security bounds directly come from Table 4 and Theorem 3 while the sizes are found by direct computation. For $\mathsf{IBS}_{\mathsf{NA},\mathsf{PW}}$ the parameters values and security bounds are given in [26, Section 5.2] while the sizes of signatures and keys are given in [26, Page 25]. However, in [26] the authors use universal constants and asymptotic bounds, that cannot directly give concrete parameters, thus for a fair comparison we instantiate each asymptotic value by the one obtained from our results (that is, the same as for $\mathsf{IBS}_{\mathsf{NA},\mathcal{R}}$).

	k	d	l	$-\log(\epsilon)$	$\log(s_{\mathsf{id}})$=$\log(s)$	$\log(s_{\mathsf{sign}})$=$\log(s')$	$\log(s'')$
ParamI	65	2048	132	200	20.65	38.92	57.19
ParamII	153	2048	308	200	21.27	40.16	59.05

Table 6. Parameter set for $\mathsf{IBS}_{\mathsf{NA},\mathcal{R}}$ and $\mathsf{IBS}^{+}_{\mathsf{NA},\mathsf{PW}}$. $s_{\mathsf{id}}, s_{\mathsf{sign}}$ are the standard deviations for $\mathsf{IBS}_{\mathsf{NA},\mathcal{R}}$ while s, s', s'' are the standard deviations for $\mathsf{IBS}^{+}_{\mathsf{NA},\mathsf{PW}}$.

Scheme	Security	Signature	mpk	msk	$\mathsf{sk}_{\mathsf{id}}$
$\mathsf{IBS}_{\mathsf{NA},\mathcal{R}}$ (ParamI)	129bits	20Mo	28Mo	14Mo	699Mo
$\mathsf{IBS}^{+}_{\mathsf{NA},\mathsf{PW}}$ (ParamI)	37bits	41Mo	28Mo	14Mo	699Mo
$\mathsf{IBS}_{\mathsf{NA},\mathcal{R}}$ (ParamII)	371bits	48Mo	153Mo	77Mo	3940Mo
$\mathsf{IBS}^{+}_{\mathsf{NA},\mathsf{PW}}$ (ParamII)	127bits	100Mo	153Mo	77Mo	3940Mo

Table 7. Security and size for $\mathsf{IBS}_{\mathsf{NA},\mathcal{R}}$ and $\mathsf{IBS}^{+}_{\mathsf{NA},\mathsf{PW}}$ with parameters of Table 6

From Table 7 we can conclude that we obtain shorter parameter sizes than with $\mathsf{IBS}^{+}_{\mathsf{NA},\mathsf{PW}}$ (and thus $\mathsf{IBS}_{\mathsf{NA},\mathsf{PW}}$) for the same security level. More precisely, sizes are around 5 times smaller for the same estimated level of security. Then, regarding time complexity by definition of DelTrap,

it uses one call to $\mathsf{SampleD}$ to compute each column of the delegated trapdoor, one signature of $\mathsf{IBS}^{+}_{\mathsf{NA,PW}}$ (*resp.* $\mathsf{IBS}_{\mathsf{NA,PW}}$) needs to use k times $\mathsf{SampleD}$ with the same (*resp.* a bigger) standard deviation as the one for $\mathsf{IBS}_{\mathbb{Z}}/\mathsf{IBS}_{\mathsf{NA},\mathcal{R}}$. We can thus estimate that the signature algorithm, the slowest part in $\mathsf{IBS}_{\mathsf{NA,PW}}/\mathsf{IBS}^{+}_{\mathsf{NA,PW}}$ scheme, is k times faster in our schemes. For a concrete use of IBS scheme, we observe that these sizes are still several orders of magnitude bigger than the optimized lattice-based signature proposed for the NIST standardization contest: 3 for the signatures and public keys for a comparison with Dilithium ([11, Table 1]). Since $\mathsf{IBS}_{\mathbb{Z}}$ scheme relies on tight security, is not optimized and has the identity-based property, this efficiency difference is expected, however there are different interesting improvements that could reduce the gap. We detail some of them in the following part.

8.2 Future work

One of the main improvements on the scheme could come from improving the matrix delegation. Indeed, the size of the delegated trapdoor is responsible for the big size of the secret key of identities. Moreover, the singular value of a delegated trapdoor is directly linked to the size of signatures because it is used to make a lower bound on the standard deviations appearing in our scheme. The use of subgaussian sampling instead of Gaussian one following the work of [14] seems to be promising in this direction. Then, it would be interesting to investigate how the notions of approximate trapdoors [8] could also be used in order to have smaller delegated trapdoor. Finally, we also think the condition on l, $l \geq 2k\log(q)$, could be greatly improved and thus directly lead to more competitive sizes.

References

1. Ajtai, M. Generating hard instances of lattice problems (extended abstract). In *28th Annual ACM Symposium on Theory of Computing* (Philadephia, PA, USA, May 22–24, 1996), ACM Press, pp. 99–108.
2. Avanzi, R., Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., Schwabe, P., Seiler, G., , and Stehlé, D. CRYSTALS-Kyber (version 3.02) – submission to round 3 of the nist post-quantum project. Specification document (update from August 2021). 2021-08-04, `https://pq-crystals.org/kyber/data/kyber-specification-round3-20210804.pdf`.
3. Banaszczyk, W. New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen, 296* (1993), 625–635.
4. Bellare, M., Namprempre, C., and Neven, G. Security proofs for identity-based identification and signature schemes. In *Advances in Cryptology – EUROCRYPT 2004* (Interlaken, Switzerland, May 2–6, 2004), C. Cachin and J. Camenisch, Eds., vol. 3027 of *Lecture Notes in Computer Science*, Springer, Heidelberg, Germany, pp. 268–286.
5. Boneh, D., Dagdelen, Ö., Fischlin, M., Lehmann, A., Schaffner, C., and Zhandry, M. Random oracles in a quantum world. In *Advances in Cryptology – ASIACRYPT 2011* (Seoul, South Korea, Dec. 4–8, 2011), D. H. Lee and X. Wang, Eds., vol. 7073 of *Lecture Notes in Computer Science*, Springer, Heidelberg, Germany, pp. 41–69.
6. Cash, D., Hofheinz, D., Kiltz, E., and Peikert, C. Bonsai trees, or how to delegate a lattice basis. In *Advances in Cryptology – EUROCRYPT 2010* (French Riviera, May 30 – June 3, 2010), H. Gilbert, Ed., vol. 6110 of *Lecture Notes in Computer Science*, Springer, Heidelberg, Germany, pp. 523–552.
7. Cesa-Bianchi, N., and Lugosi, G. Prediction, learning and games. *Cambridge University Press* (2006).
8. Chen, Y., Genise, N., and Mukherjee, P. Approximate trapdoors for lattices and smaller hash-and-sign signatures. In *Advances in Cryptology – ASIACRYPT 2019, Part III* (Kobe, Japan, Dec. 8–12, 2019), S. D. Galbraith and S. Moriai, Eds., vol. 11923 of *Lecture Notes in Computer Science*, Springer, Heidelberg, Germany, pp. 3–32.
9. Dodis, Y., Katz, J., Xu, S., and Yung, M. Strong key-insulated signature schemes. In *PKC 2003: 6th International Workshop on Theory and Practice in Public Key Cryptography* (Miami, FL, USA, Jan. 6–8, 2003), Y. Desmedt, Ed., vol. 2567 of *Lecture Notes in Computer Science*, Springer, Heidelberg, Germany, pp. 130–144.
10. Ducas, L. Github repository pq-crystals/security-estimates. Accessed January 1, 2023, `https://github.com/pq-crystals/security-estimates`.

11. Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., , and Stehlé, D. CRYSTALS-Dilithium – algorithm specifications and supporting documentation (version 3.1). Specification document (update from February 2021). 2021-02-08, `https://pq-crystals.org/dilithium/data/dilithium-specification-round3-20210208.pdf`.
12. Ducas, L., and Micciancio, D. Improved short lattice signatures in the standard model. In *Advances in Cryptology – CRYPTO 2014, Part I* (Santa Barbara, CA, USA, Aug. 17–21, 2014), J. A. Garay and R. Gennaro, Eds., vol. 8616 of *Lecture Notes in Computer Science*, Springer, Heidelberg, Germany, pp. 335–352.
13. Genise, N., Micciancio, D., Peikert, C., and Walter, M. Improved discrete gaussian and subgaussian analysis for lattice cryptography. In *PKC 2020: 23rd International Conference on Theory and Practice of Public Key Cryptography, Part I* (Edinburgh, UK, May 4–7, 2020), A. Kiayias, M. Kohlweiss, P. Wallden, and V. Zikas, Eds., vol. 12110 of *Lecture Notes in Computer Science*, Springer, Heidelberg, Germany, pp. 623–651.
14. Genise, N., Micciancio, D., and Polyakov, Y. Building an efficient lattice gadget toolkit: Subgaussian sampling and more. In *Advances in Cryptology – EUROCRYPT 2019, Part II* (Darmstadt, Germany, May 19–23, 2019), Y. Ishai and V. Rijmen, Eds., vol. 11477 of *Lecture Notes in Computer Science*, Springer, Heidelberg, Germany, pp. 655–684.
15. Gentry, C., Peikert, C., and Vaikuntanathan, V. Trapdoors for hard lattices and new cryptographic constructions. Cryptology ePrint Archive, Report 2007/432, 2007. `https://eprint.iacr.org/2007/432`.
16. Gentry, C., and Silverberg, A. Hierarchical ID-based cryptography. In *Advances in Cryptology – ASIACRYPT 2002* (Queenstown, New Zealand, Dec. 1–5, 2002), Y. Zheng, Ed., vol. 2501 of *Lecture Notes in Computer Science*, Springer, Heidelberg, Germany, pp. 548–566.
17. Grilo, A. B., Hövelmanns, K., Hülsing, A., and Majenz, C. Tight adaptive reprogramming in the QROM. In *Advances in Cryptology – ASIACRYPT 2021, Part I* (Singapore, Dec. 6–10, 2021), M. Tibouchi and H. Wang, Eds., vol. 13090 of *Lecture Notes in Computer Science*, Springer, Heidelberg, Germany, pp. 637–667.
18. Kiltz, E., and Neven, G. Identity-based signatures. In *Identity-Based Cryptography*, M. Joye and G. Neven, Eds., vol. 2 of *Cryptology and Information Security Series*. IOS Press, 2009, pp. 31–44.
19. Krawczyk, H., and Rabin, T. Chameleon signatures. In *ISOC Network and Distributed System Security Symposium – NDSS 2000* (San Diego, CA, USA, Feb. 2–4, 2000), The Internet Society.
20. Langlois, A., and Stehlé, D. Worst-case to average-case reductions for module lattices. Cryptology ePrint Archive, Report 2012/090, 2012. `https://eprint.iacr.org/2012/090`.
21. Lee, Y., Park, J. H., Lee, K., and Lee, D. H. Tight security for the generic construction of identity-based signature (in the multi-instance setting). *Theor. Comput. Sci. 847* (2020), 122–133.
22. Lyubashevsky, V. Lattice signatures without trapdoors. Cryptology ePrint Archive, Report 2011/537, 2011. `https://eprint.iacr.org/2011/537`.
23. Lyubashevsky, V. Lattice signatures without trapdoors. In *Advances in Cryptology – EUROCRYPT 2012* (Cambridge, UK, Apr. 15–19, 2012), D. Pointcheval and T. Johansson, Eds., vol. 7237 of *Lecture Notes in Computer Science*, Springer, Heidelberg, Germany, pp. 738–755.
24. Micciancio, D. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions from worst-case complexity assumptions. In *43rd Annual Symposium on Foundations of Computer Science* (Vancouver, BC, Canada, Nov. 16–19, 2002), IEEE Computer Society Press, pp. 356–365.
25. Micciancio, D., and Peikert, C. Trapdoors for lattices: Simpler, tighter, faster, smaller. In *Advances in Cryptology – EUROCRYPT 2012* (Cambridge, UK, Apr. 15–19, 2012), D. Pointcheval and T. Johansson, Eds., vol. 7237 of *Lecture Notes in Computer Science*, Springer, Heidelberg, Germany, pp. 700–718.
26. Pan, J., and Wagner, B. Short identity-based signatures with tight security from lattices. In *Post-Quantum Cryptography - 12th International Workshop, PQCrypto 2021* (Daejeon, South Korea, July 20–22, 2021), J. H. Cheon and J.-P. Tillich, Eds., Springer, Heidelberg, Germany, pp. 360–379.
27. Pan, J., and Wagner, B. Lattice-based signatures with tight adaptive corruptions and more. In *Public-Key Cryptography - PKC 2022 - 25th IACR International Conference on Practice and Theory of Public-Key Cryptography, Virtual Event, March 8-11, 2022, Proceedings, Part II* (2022), G. Hanaoka, J. Shikata, and Y. Watanabe, Eds., vol. 13178 of *Lecture Notes in Computer Science*, Springer, pp. 347–378.
28. Peikert, C. A decade of lattice cryptography. Cryptology ePrint Archive, Report 2015/939, 2015. `https://eprint.iacr.org/2015/939`.
29. Regev, O. On lattices, learning with errors, random linear codes, and cryptography. In *37th Annual ACM Symposium on Theory of Computing* (Baltimore, MA, USA, May 22–24, 2005), H. N. Gabow and R. Fagin, Eds., ACM Press, pp. 84–93.
30. Shamir, A. Identity-based cryptosystems and signature schemes. In *Advances in Cryptology – CRYPTO'84* (Santa Barbara, CA, USA, Aug. 19–23, 1984), G. R. Blakley and D. Chaum, Eds., vol. 196 of *Lecture Notes in Computer Science*, Springer, Heidelberg, Germany, pp. 47–53.
31. Wang, Y., Wang, B., Lai, Q., and Zhan, Y. Identity-based matchmaking encryption with stronger security and instantiation on lattices. Cryptology ePrint Archive, Paper 2022/1718, 2022. `https://eprint.iacr.org/2022/1718`.

32. Zhandry, M. A note on the quantum collision and set equality problems. *Quantum Inf. Comput. 15*, 7&8 (2015), 557–567. https://doi.org/10.26421/QIC15.7-8-2.

A Generic probability results

A.1 Results about the statistical distance

Lemma 4. *Let A, B two sets, X, Y two independent random variables with values in A and $f : A \to B$ a function. Then,* $\mathsf{SD}(f(X), f(Y)) \leq \mathsf{SD}(X, Y)$.

Proof.

$$\begin{aligned}
\mathsf{SD}(f(X), f(Y)) &= \sum_{z \in f(\mathcal{X})} |\Pr[f(X) = z] - \Pr[f(Y) = z]| \\
&= \sum_{z \in f(\mathcal{X})} \left|\Pr\left[X \in f^{-1}(z)\right] - \Pr\left[Y \in f^{-1}(z)\right]\right| \\
&= \sum_{z \in f(\mathcal{X})} \left| \sum_{t \in f^{-1}(z)} \Pr[X = t] - \Pr[Y = t] \right| \\
&\leq \sum_{z \in f(\mathcal{X})} \sum_{t \in f^{-1}(z)} |\Pr[X = t] - \Pr[Y = t]| \\
&= \sum_{t \in f^{-1}(f(\mathcal{X}))} |\Pr[X = t] - \Pr[Y = t]| \ .
\end{aligned}$$

Since $f^{-1}(f(X)) \subset \mathcal{X}$, this yields,

$$\sum_{t \in f^{-1}(f(\mathcal{X}))} |\Pr[X = t] - \Pr[Y = t]| \leq \sum_{t \in \mathcal{X}} |\Pr[X = t] - \Pr[Y = t]| \ .$$

Therefore, $\mathsf{SD}(f(X), f(Y)) \leq \mathsf{SD}(X, Y)$.

Lemma 5. *Let A, B two sets, X, Y two independent random variables with values in A and a function $f : A \to B$. Then for any random variable Z independent with both X, Y, we have*

$$\mathsf{SD}(f(X, Z), f(Y, Z)) \leq \mathsf{SD}(X, Y) \, .$$

Proof. $\mathsf{SD}(f(X, Z), f(Y, Z)) \leq \mathsf{SD}((X, Z), (Y, Z))$ by the previous lemma. Since the variables are independent, $\mathsf{SD}((X, Z), (Y, Z)) = \mathsf{SD}(X, Y)$.

Lemma 6. *Let $m \geq 1$ and $X_1, \ldots, X_m, Y_1, \ldots, Y_m$ some independent random variables. Let $X = (X_1, \ldots, X_m), Y = (Y_1, \ldots, Y_m)$. Then,* $\mathsf{SD}(X, Y) \leq \sum_{i=1}^{m} \mathsf{SD}(X_i, Y_i)$.

Proof. For $m = 2$, the result holds. By induction, assume the property holds for some $m > 1$. Consider $X = (X_1, \ldots, X_{m+1}), Y = (Y_1, \ldots, Y_{m+1})$.
Then by triangle inequality

$$\begin{aligned}
\mathsf{SD}(X, Y) &\leq \mathsf{SD}(X, (X_1, \ldots, X_m, Y_{m+1})) + \mathsf{SD}((X_1, \ldots, X_m, Y_{m+1}), Y) \\
&\leq \mathsf{SD}(X_{m+1}, Y_{m+1}) + \mathsf{SD}((X_1, \ldots, X_m), (Y_1, \ldots Y_m)) \ .
\end{aligned}$$

By induction, this shows $\mathsf{SD}(X, Y) \leq \mathsf{SD}(X_{m+1}, Y_{m+1}) + \sum_{i=1}^{m} \mathsf{SD}(X_i, Y_i)$.

A.2 Other probability results

Proposition 12. *Let X, Y two independent random variables with values on sets A and B respectively. Let $f : A \times B \to \{0,1\}$ a function. Suppose that there exists $\epsilon > 0$ such that $\Pr_{(a,b)\leftarrow\$(X,Y)}[f(a,b)=1] \geq 1-\epsilon$. Then, for all $\lambda \in [0,1[$,*

$$\Pr_{a\leftarrow\$X}[\Pr_{b\leftarrow\$Y}[f(a,b)=1] \geq 1-\lambda] \geq 1-\frac{\epsilon}{\lambda} \ .$$

In particular, with $\lambda = \sqrt{\epsilon}$,

$$\Pr_{a\leftarrow\$X}\left[\Pr_{b\leftarrow\$Y}[f(a,b)=1] \geq 1-\sqrt{\epsilon}\right] \geq 1-\sqrt{\epsilon} \ .$$

Proof. We define $\mathsf{E}(\lambda) = \{a \in A : \ \Pr_{b\leftarrow\$Y}[f(a,b)=1] \geq 1-\lambda\}$. We have

$$\begin{aligned}
1-\epsilon &\leq \Pr_{(a,b)\leftarrow\$(X,Y)}[f(a,b)=1] \\
&= \sum_{a\in\mathsf{E}(\lambda)} \Pr[X=a]\Pr_{b\leftarrow\$Y}[f(a,b)=1] \\
&\quad + \sum_{a\notin\mathsf{E}(\lambda)} \Pr[X=a]\Pr_{b\leftarrow\$Y}[f(a,b)=1] \\
&\leq \Pr[X\in\mathsf{E}(\lambda)] + (1-\Pr[X\in\mathsf{E}(\lambda)])\,(1-\lambda) \\
&= \lambda\Pr[X\in\mathsf{E}(\lambda)] + (1-\lambda) \\
&= \lambda\Pr_{a\leftarrow\$X}[\Pr_{b\leftarrow\$Y}[f(a,b)=1] \geq 1-\lambda] + (1-\lambda) \ .
\end{aligned}$$

We can then conclude.

Lemma 7. *Let* Dist *a random variable with values in a set A and a function $f : A \to B$. Then, the following probability distributions are equal*

$$\begin{aligned}
\mathsf{Dist}_1 &= \{(f(a),a) : a \leftarrow\$ \ \mathsf{Dist}\} \ , \\
\mathsf{Dist}_2 &= \{(b,a) : b \leftarrow\$ \ f(\mathsf{Dist}), a \leftarrow\$ \ \mathsf{Dist}_{|f^{-1}(\{b\})}\} \ .
\end{aligned}$$

Proof. For $b \in f(X), a \in A$, we have

$$\begin{aligned}
\Pr[\mathsf{Dist}_2=(b,a)] &= \Pr\left[f(\mathsf{Dist})=b \wedge \mathsf{Dist}_{|f^{-1}(\{b\})}=a\right] \\
&= \Pr\left[\mathsf{Dist}\in f^{-1}(\{b\}) \wedge \mathsf{Dist}_{|f^{-1}(\{b\})}=a\right] \\
&= \Pr\left[\mathsf{Dist}\in f^{-1}(\{b\})\right]\ \Pr\left[\mathsf{Dist}_{|f^{-1}(\{b\})}=a\right] \\
&= \Pr\left[\mathsf{Dist}\in f^{-1}(\{b\})\right]\ \frac{\Pr\left[\mathsf{Dist}\in f^{-1}(\{b\})\in\{a\}\right]}{\Pr[\mathsf{Dist}\in f^{-1}(\{b\})]} \\
&= \Pr\left[\mathsf{Dist}\in f^{-1}(\{b\})\cap\{a\}\right] \\
&= \begin{cases} \Pr[\mathsf{Dist}=a] & \text{if } f(a)=b \\ 0 & \text{else} \end{cases} \\
&= \Pr[\mathsf{Dist}_1=(b,a)] \ .
\end{aligned}$$

B Proofs of Section 4

B.1 Bound on singular values of random matrices

A random variable X over $\mathbb{R}$ is subgaussian with parameter $s>0$ if for each $t\in\mathbb{R}$, $\mathbb{E}\left[e^{2\pi tX}\right] \leq e^{\pi s^2t^2}$.

For $k\in\mathbb{N}^*$, a random variable X over $\mathbb{R}^k$ is subgaussian with parameter $s>0$ if for each $i\in[\![1,k]\!]$, the i$^{\text{th}}$ component of X is subgaussian with parameter s.

Lemma 8. *Let $n, a \in \mathbb{N}^*$. The probability distribution $\mathcal{D}^n_{\mathbb{Z},s}$ is subgaussian with parameter s. The uniform distribution $\mathsf{U}(\{-a, 0, a\})$ is subgaussian with parameter $a\sqrt{\frac{4\pi}{3}}$. The uniform distribution $a\mathcal{P}_r$ is subgaussian with parameter $a\sqrt{2\pi(1-r)}$.*

Proof. The first claim is from [25, Lemma 2.8]. For the last two claims, the proof is an adaptation of the proof of Hoeffding's lemma in [7, Lemma A.1]. For example, for $\mathsf{U}(\{-a, 0, a\})$, we have, $\mathbb{E}\left[e^{2\pi tX}\right] = \frac{1}{3}\left(e^{2\pi ta} + e^{-2\pi ta} + 1\right) = e^{\phi(u)}$ with $u = 2\pi at$ and $\phi(u) = \ln\left(\frac{1}{3}\right) + \ln\left(e^u + e^{-u} + 1\right)$ A direct computation and analysis shows that $\phi(0) = \phi'(0) = 0 \quad \forall v \in \mathbb{R}, \phi''(v) \leq \phi''(0) = \frac{2}{3}$.

Thus, by Taylor's Theorem, $\forall v, \phi(v) \leq \frac{u^2}{2}\phi''(0) = \frac{1}{3}u^2$. We then conclude that

$$\mathbb{E}\left[e^{2\pi tX}\right] \leq e^{\frac{1}{3}(2\pi at)^2} = e^{\pi\left(a\sqrt{\frac{4\pi}{3}}\right)^2 t^2} \ .$$

Proof of Corollary 1. We want to apply [13, Theorem 6.1] with $t = \sqrt{m\ln(3)}$, which will show in both cases that with probability $1 - 2e^{-t^2} = 1 - 2 * 3^{-m}$

$$\mathsf{s}_1(\mathbf{R}) \leq \sigma\left[\sqrt{m} + C(s^2/\sigma^2)\left(\sqrt{n} + \sqrt{\ln(3)m}\right)\right] \ ,$$

where the rows $\mathbf{r}_i$ are independent, identically distributed, zero-mean, and such that $\mathbb{E}\left[\mathbf{r}_i\mathbf{r}_i^\top\right] = \sigma^2\mathsf{I}$. In both cases of the corollary, the coordinates are independent, identically distributed and zero-mean, thus $\mathbb{E}\left[\mathbf{r}_i\mathbf{r}_i^\top\right] = \sigma^2\mathsf{I}$ where σ is the standard deviation. Lemma 8 and a direct computation of the standard deviation show that:

- For the distribution $\mathcal{D}_{\mathbb{Z},s}$, $\sigma = s/\sqrt{2\pi}$ and s is the subgaussian parameter.
- For the distribution $\mathsf{U}(\{-a, 0, a\})$, $\sigma = a\sqrt{\frac{2}{3}}$ and $s = a\sqrt{\frac{4\pi}{3}}$.
- For the distribution $a\mathcal{P}_r$, $\sigma = a\sqrt{(1-r)}$ and $s = a\sqrt{2\pi(1-r)}$.

We then apply Theorem 6.1 with these values.

The ring case can be deduced from this corollary thanks to the definition of singular norm in the ring case.

B.2 Invertible elements of $\mathcal{R}_q$

In this part we provide a simple condition on the invertibility of $\mathcal{R}_q$ elements, for $q = 3^k$.

Proposition 13 (Simple condition to be invertible in $\mathcal{R}_q$). *We consider $\mathcal{R}_q = \mathbb{Z}_q[X]/X^d + 1$ for $d \geq 2$ a power of 2 and $q = 3^k$ for $k \geq 1$. Let $\mathcal{C}_0, \mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ subsets of $[\![-(q-1)/4, (q-1)/4]\!]$ such that*

$$(-\mathcal{C}_0) \cap \mathcal{C}_1 \cap \mathcal{C}_2 \subset \{0\} \ , \tag{5}$$

$$\mathcal{C}_0 \cap \mathcal{C}_1 \cap (-\mathcal{C}_2) \subset \{0\} \ , \tag{6}$$

$$\min_{x \in \mathcal{C}_3 - \{0\}} |x| > \frac{\|\mathcal{C}_1\|_\infty + \|\mathcal{C}_2\|_\infty}{2} \ . \tag{7}$$

Let $P \in \mathbb{Z}[X]$ of degree $< d$ such that $P \neq 0 \mod 3$ and

$$\mathsf{Cf}(P) \mod^{\pm} \in \mathcal{C}_0 \times \mathcal{C}_1 \times \mathcal{C}_2 \times \mathcal{C}_3 \ .$$

Then, P is invertible as an element of $\mathcal{R}_q$.

Proof. We define $P = C_0 + C_1X^{d/4} + C_2X^{d/2} + C_3X^{3d/4}$ with each $C_i \in \mathbb{Z}[X]$ of degree strictly less than d/4. We define $Q_1(X) = X^{d/2} + X^{d/4} - 1, Q_2(X) = X^{d/2} - X^{d/4} - 1$ and set $I_1 = (Q_1), I_2 = (Q_2)$, In the proof of [12, Lemma 7] it is observed that the non-zero ideals of $\mathcal{R}_q$ are

$$\begin{aligned} &\mathcal{R}_q \text{ itself} && I_1 \supset 3I_1 \supset \ldots \supset 3^{k-1}I_1 \ , \\ &I_2 \supset 3I_2 \supset \ldots \supset 3^{k-1}I_2 \ , && (3) \supset (3^2) \supset \ldots \supset (3^{k-1}) \ . \end{aligned}$$

Thus, P is invertible as an element of $\mathcal{R}_q$ if and only if

$$P \neq 0 \mod (I_1, 3^k) \quad P \neq 0 \mod (I_2, 3^k) \quad P \neq 0 \mod 3 \ .$$

Furthermore, we see that

$$\begin{aligned} & P = 0 \mod (I_1, 3^k) \\ \Leftrightarrow\ & C_0 + C_1X^{d/4} + (1 - X^{d/4})(C_2 + C_3X^{d/4}) = 0 \mod (I_1, 3^k) \\ \Leftrightarrow\ & (C_0 + C_2) + (C_1 + C_3 - C_2)X^{d/4} - X^{d/2}C_3 = 0 \mod (I_1, 3^k) \\ \Leftrightarrow\ & (C_0 + C_2 - C_3) + (C_1 + 2C_3 - C_2)X^{d/4} = 0 \mod 3^k \\ \Leftrightarrow\ & C_0 + C_2 - C_3 = 0 \mod 3^k \quad \wedge \quad C_1 + 2C_3 - C_2 = 0 \mod 3^k \\ \Leftrightarrow\ & C_0 + C_2 = C_3 \quad \wedge \quad 2C_3 = C_2 - C_1 \quad \text{because coefficients of P are} \\ & \qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{in } [\![-(q-1)/4, (q-1)/4]\!] \\ \Rightarrow\ & C_3 = 0 \ \wedge\ C_0 = -C_2 \ \wedge\ C_2 = C_1 \quad \text{by equation (7)} \\ \Rightarrow\ & P = 0 \quad \text{by equation (5)} \ , \end{aligned}$$

Moreover, we can show with the same method, using Equations (7) and (6), that $P = 0 \mod (I_2, 3^k)$ implies $P = 0$. Thus, P is invertible as an element of $\mathcal{R}_q$ if and only if $P \neq 0 \mod 3$.

Corollary 2 (of Proposition 13). *Let $k \geq 4, q = 3^k$. We consider $\mathcal{S}_{\mathsf{R}}$ as a subset of $\mathcal{R}_q$. Then*

$$\overline{\mathcal{S}_{\mathsf{R}}} = \{a - a' \ \ a, a' \in \mathcal{S}_{\mathsf{R}}, a \neq a'\} \subset (\mathcal{R}_q)^\times$$

Proof. Note that $\overline{\mathcal{S}_{\mathsf{R}}}$ is equal to

$$\left\{P \in \mathcal{R}_q \colon \mathsf{Cf}(P) \in \{-8, -4, 0, 4, 8\}^{d/4} \times \{-2, -1, 0, 1, 2\}^{d/2} \times \{-8, -4, 0, 4, 8\}^{d/4}\right\} \ .$$

The proposition can be directly applied.

B.3 Proof of smoothing lemma (Lemma 1)

Unstructured case (Equation (1))

In order to prove it, we introduce Lemmas 9 and 10.

Lemma 9. *Let $m, k \in \mathbb{N}^*$ b prime and $q = b^k$. For each $r > 0$, let $\mathcal{B}_\infty^m(r) = \{x \in \mathbb{Z}^m : \|x\|_\infty < r\}$, $\mathcal{B}_{q,\infty}^m(r) = \{x \in \mathbb{Z}_q^m : \|x\|_\infty < r\}$. Then,*

$$\forall 0 \leq l < k, \qquad \left| b^l\mathbb{Z}_q^m \cap (\mathcal{B}_\infty^m(q/4b) \mod q) \right| \leq \left(\frac{q}{b^{1+l}}\right)^m \ . \tag{8}$$

Proof. Let $\mathsf{Rep} = [\![-(q-1)/2, (q-1)/2]\!]$ if b odd and $\mathsf{Rep} =]\!] - q/2, q/2]\!]$ if $b = 2$. The infinity norm of $x \in \mathbb{Z}_q$ is the infinity norm of the unique representative of x in Rep.

We will first show that

$$b^l\mathbb{Z}_q^m \cap \mathcal{B}_{q,\infty}^m(q/4b) = \left(b^l\mathbb{Z}^m \cap \mathcal{B}_\infty^m(q/4b)\right) \bmod q \ . \tag{9}$$

The inclusion "$\subset$" comes from the fact that $\mathcal{B}_\infty^m(q/4b) \subset \mathsf{Rep}^m$, which implies that $\mathcal{B}_{q,\infty}^m(q/4b) = \mathcal{B}_\infty(q/4b)^m \mod q$. We now show the reverse inclusion "$\supset$". Let $\mathbf{x} \in b^l\mathbb{Z}_q^m \cap (\mathcal{B}_\infty^m(q/4b) \mod q)$ and let $\tilde{\mathbf{x}}$ the representative of $\mathbf{x}$ in Rep^m. Because $\mathbf{x} \in b^l\mathbb{Z}_q^m$, there exists $\mathbf{y} \in \mathbb{Z}^m$ such that

$$q = b^k | \ \tilde{\mathbf{x}} - b^l\mathbf{y} \ \Rightarrow b^l \mid \left(\tilde{\mathbf{x}} - b^l\mathbf{y}\right) \Rightarrow b^l | \tilde{\mathbf{x}} \quad \text{because } l \leq k \ .$$

We can write $\tilde{\mathbf{x}} = b^l\hat{\mathbf{x}}$ for $\hat{\mathbf{x}} \in \mathbb{Z}^m$. We know that $\tilde{\mathbf{x}} = \mathbf{z} \bmod q$ for some $\mathbf{z} \in \mathcal{B}_\infty^m(q/4b)$ (because $\mathcal{B}_{q,\infty}^m(q/4b) = \mathcal{B}_\infty^m(q/4b) \mod q$). But $\mathcal{B}_\infty^m(q/4b) \subset \mathsf{Rep}^m$ implies that $z = \tilde{\mathbf{x}}$, and therefore $x \in \mathcal{B}_{q,\infty}^m(q/4b)$. This proves the inclusion and therefore Equation (9).

Observe that $\mathcal{B}_\infty^m(q/b) \subset \mathsf{Rep}^m$ implies that

$$\left|\left(b^l\mathbb{Z}^m \cap \mathcal{B}_\infty^m(q/4b)\right)\right| = \left|\left(b^l\mathbb{Z}^m \cap \mathcal{B}_\infty^m(q/4b)\right) \bmod q\right| \tag{10}$$

Notice that

$$\mathbf{x} \in \mathcal{B}_\infty^m\left(q/4b^{l+1}\right) \mapsto b^l\mathbf{x} \in b^l\mathbb{Z}^m \cap \mathcal{B}_\infty^m(q/4b)$$

is a bijection. We can then use Equations (9) and (10) to see that

$$\left|\left(b^l\mathbb{Z}^m \cap \mathcal{B}_\infty^m(q/b)\right) \bmod q\right| = \left|\mathcal{B}_\infty^m\left(q/4b^{l+1}\right)\right|$$

Finally, we show that $\left|\mathcal{B}_\infty^m\left(q/4b^{l+1}\right)\right| \leq \left(\frac{q}{b^{1+l}}\right)^m$. If $l = k-1$, we have $\left|\mathcal{B}_\infty^m\left(q/4b^{l+1}\right)\right| = |\{0\}| = 1$ and thus $\left|\mathcal{B}_\infty^m\left(q/4b^{l+1}\right)\right| \leq 1 = \left(\frac{q}{b^{1+l}}\right)^m$. If $l < k-1$, we have

$$\begin{aligned}
\left|\mathcal{B}_\infty^m\left(q/4b^{l+1}\right)\right| &= \left(2\left\lceil\frac{q}{4b^{1+l}}\right\rceil - 1\right)^m \\
&\leq \left(\frac{q}{2b^{1+l}} + 1\right)^m \\
&\leq \left(\frac{q}{b^{1+l}}\right)^m \text{ because } q/2b^{1+l} \geq q/2b^{k-1} = b/2 \geq 1.
\end{aligned}$$

Lemma 10. *Let $k, b \in \mathbb{N}^*$, b prime. Let $m, n \in \mathbb{N}^*$, such that $m \geq 2nk$. Then,*

$$\Pr_{\mathbf{A} \in \mathbb{Z}^{m \times n}}[\lambda^\infty(\Lambda(\mathbf{A})) \geq q/4b] \geq 1 - q^{-n}.$$

Proof. As in Lemma 9, for each $r > 0$, we define $\mathcal{B}_\infty^m(r) = \{x \in \mathbb{Z}^m : \|x\|_\infty < r\}$, $\mathcal{B}_{q,\infty}^m(r) = \{x \in \mathbb{Z}_q^m : \|x\|_\infty < r\}$.

Notice that for any non-zero $\mathbf{s} \in \mathbb{Z}_q^n$, there exists $0 \leq l < k$ such that $\mathbf{s} = b^l \tilde{\mathbf{s}}$ for $\tilde{\mathbf{s}}$ with one invertible coordinate, and we have

$$\begin{aligned}
&\Pr_{\mathbf{A} \in \mathbb{Z}_q^{n \times m}} \left[\left\| \mathbf{A}^\top \mathbf{s} \right\|_\infty < q/4b \right] \\
&= \Pr_{\mathbf{A} \in \mathbb{Z}_q^{n \times m}} \left[\mathbf{A}^\top \mathbf{s} \in \mathcal{B}_{q,\infty}^m (q/4b) \right] \quad \text{because } q/4b \leq q/2 \\
&= \Pr_{\mathbf{A} \in \mathbb{Z}_q^{n \times m}} \left[b^l \mathbf{A}^\top \tilde{\mathbf{s}} \in \mathcal{B}_{q,\infty}^m (q/4b) \right] \quad \text{because } \mathbf{s} = b^l \tilde{\mathbf{s}} \\
&= \Pr_{\mathbf{a} \in \mathbb{Z}_q^m} \left[b^l \mathbf{a} \in \mathcal{B}_{q,\infty}^m (q/4b) \right] \quad \text{because } \tilde{\mathbf{s}} \text{ has an invertible coordinate} \\
&= \Pr_{\mathbf{x} \in b^l \mathbb{Z}_q^m} \left[\mathbf{x} \in \mathcal{B}_{q,\infty}^m (q/4b) \right] \\
&= \frac{\left| b^l \mathbb{Z}_q^m \cap \mathcal{B}_{q,\infty}^m (q/4b) \right|}{\left| b^l \mathbb{Z}_q^m \right|} \\
&= \frac{\left| b^l \mathbb{Z}_q^m \cap \mathcal{B}_{q,\infty}^m (q/4b) \right|}{(q/b^l)^m} \quad q \text{ being a power of } b \text{ and bigger than } b^l \\
&\leq \left(\frac{\frac{q}{b^{1+l}}}{(q/b^l)} \right)^m \quad \text{by Lemma 9} \\
&= \left(\frac{1}{b} \right)^m .
\end{aligned}$$

Thus, taking the union for all non-zero $\mathbf{s}$

$$\begin{aligned}
&\Pr_{\mathbf{A} \in \mathbb{Z}_q^{n \times m}} \left[\exists \mathbf{s} \in \mathbb{Z}_q^n - \{\mathbf{0}\} : \left\| \mathbf{A}^\top \mathbf{s} \right\|_\infty < q/b \right] \\
&\leq q^n \left(\frac{1}{b} \right)^m = q^{(n - \frac{m}{k})} \quad \text{because } q = b^k \\
&\leq q^{-n} \quad \text{because } m \geq 2nk .
\end{aligned}$$

Lemma 11. *Let $n, m, k \in \mathbb{N}$, b prime, $q = b^k$, with $m \geq 2nk$ and $\epsilon > 0$, then*

$$\Pr_{\mathbf{A} \in \mathbb{Z}_q^{n \times m}} \left[\eta_\epsilon(\Lambda^\perp(\mathbf{A})) \leq 4b \mathsf{r}_{m,\epsilon} \right] \geq 1 - q^{-n} .$$

Proof. Lemma 10 and the fact that $\Lambda^\perp(\mathbf{A})^* = q^{-1} \Lambda(\mathbf{A}^\top)$ shows that

$$\Pr_{\mathbf{A} \in \mathbb{Z}_q^{n \times m}} \left[\lambda_1^\infty \left(\Lambda^\perp(\mathbf{A})^* \right) \geq 1/(4b) \right] \geq 1 - q^{-n} .$$

Moreover, [20, Lemma 2.5] shows that, since $\Lambda^\perp(\mathbf{A})$ is of dimension m, $\eta_\epsilon(\Lambda^\perp(\mathbf{A})) \leq \mathsf{r}_{m,\epsilon} \cdot 1/\lambda_1^\infty \left(\Lambda^\perp(\mathbf{A})^* \right)$.

Proof of unstructured case ((Equation* (1)*)). This is an adaptation of the demonstration of [15, Lemma 5.2]. Suppose that $\mathbf{A}\mathbb{Z}_q^m = \mathbb{Z}_q^n$ and $s \geq \eta_\epsilon(\Lambda_q^\perp(\mathbf{A}))$. We recall that $\Lambda_q^\perp(\mathbf{A}) \subset \mathbb{Z}_q^m$ is a full-rank lattice. Thus, by [15, Corollary 2.8]

$$\mathsf{SD}\Big(\mathcal{D}_{\mathbb{Z},s}^m \mod \Lambda_q^\perp(\mathbf{A}), \mathsf{U}\left(\mathbb{Z}_q^n\right) \mod \Lambda_q^\perp(\mathbf{A}) \Big) < 2\epsilon .$$

Then, because $\mathbf{A}\mathbb{Z}_q^m = \mathbb{Z}_q^n$, the application $\mathbb{Z}^m \mod \Lambda_q^\perp(\mathbf{A}) \to \mathbb{Z}_q^n$ that send $\mathbf{e} + \Lambda_q^\perp(\mathbf{A})$ to $\mathbf{A}\mathbf{e}$ is an isomorphism and we can thus conclude. We thus need $\mathbf{A}\mathbb{Z}_q^m = \mathbb{Z}_q^n$ and $s \geq \eta_\epsilon(\Lambda_q^\perp(\mathbf{A}))$. This is done with Corollary and Lemma 11.

Proof of unstructured part of Lemma 1 (Equation* (1)*). This is an adaptation of the demonstration of [15, Lemma 5.2]. Suppose that $\mathbf{A}\mathbb{Z}_q^m = \mathbb{Z}_q^n$ and $s \geq \eta_\epsilon(\Lambda_q^\perp(\mathbf{A}))$. We recall that $\Lambda_q^\perp(\mathbf{A}) \subset \mathbb{Z}_q^m$ is a full-rank lattice. Thus, by [15, Corollary 2.8]

$$\mathsf{SD}\Big(\mathcal{D}_{\mathbb{Z},s}^m \mod \Lambda_q^\perp(\mathbf{A}), \mathsf{U}\left(\mathbb{Z}_q^n\right) \mod \Lambda_q^\perp(\mathbf{A})\Big) < 2\epsilon \ .$$

Then, because $\mathbf{A}\mathbb{Z}_q^m = \mathbb{Z}_q^n$, the application $\mathbb{Z}^m \mod \Lambda_q^\perp(\mathbf{A}) \to \mathbb{Z}_q^n$ that send $\mathbf{e} + \Lambda_q^\perp(\mathbf{A})$ to $\mathbf{A}\mathbf{e}$ is an isomorphism. We thus need to see when these conditions happen and to estimate $\eta_\epsilon(\Lambda^\perp(\mathbf{A}))$. This is done with Proposition 1 and Lemma 11 and we can conclude.

Structured case (Equation (2)**)**

We need the following lemma for the proof.

Lemma 12 (Part of [12, Lemma 7] with reformulation and bound improvement). *Let d a power of 2, $q = 3^k$ a power of 3 and $l > 2k$. We have*

$$\Pr_{\mathbf{A} \in \mathcal{R}_q^{1\times l}}\left[\eta_\epsilon(\Lambda_{\mathcal{R},q}^\perp(\mathbf{A})) \leq 12\mathsf{r}_{ld,\epsilon}\right] \geq 1 - 3^{-d\frac{(2k-l)}{2}} \ .$$

Proof. This proof is a adaptation of the proof of [12, Lemma 7] with the condition $l > 2k$ instead of $l > 2\log(q) = 2\log_2(3)k$.

The lemma [20, Lemma 2.5] shows that, since $\Lambda^\perp(\mathbf{A})$ is of dimension dl,

$$\eta_\epsilon(\Lambda^\perp(\mathbf{A})) \leq \mathsf{r}_{dl,\epsilon} \cdot 1/\lambda_1^\infty\left(\Lambda^\perp(\mathbf{A})\right) \ .$$

Thus, using Proposition 4 and the fact that the distribution of $\mathbf{A}^* \in \mathcal{R}_q^{l\times 1}$ is uniform if the one of $\mathbf{A} \in \mathcal{R}_q^{1\times l}$ is, we see that it is sufficient to prove that

$$\Pr_{\mathbf{B} \in \mathcal{R}_q^{l\times 1}}[\Lambda_{\mathcal{R},q}(\mathbf{B})) \geq q/12] \geq 1 - 3^{-d\frac{(2k-l)}{2}} \ .$$

We define $Q_1(X) = X^{d/2} + X^{d/4} - 1, Q_2(X) = X^{d/2} - X^{d/4} - 1$ and we set $I_1 = (Q_1), I_2 = (Q_2)$. We observe that the non-zero ideals of $\mathcal{R}_q$ are

$$\begin{array}{ll} \mathcal{R}_q \text{ itself} & I_1 \supset 3I_1 \supset \ldots \supset 3^{k-1}I_1 \ , \\ I_2 \supset 3I_2 \supset \ldots \supset 3^{k-1}I_2 \ , & (3) \supset (3^2) \supset \ldots \supset (3^{k-1}) \ . \end{array}$$

Let $\mathcal{C} = \{\mathbf{v} \in \mathcal{R}_q^d : \|\mathbf{v}\|_\infty < q/12\}$. Fix some $\mathbf{x} \in \mathcal{R}_q^d \setminus \{0\}$ and set $\mathcal{J} = (\mathbf{x})$. It is one of the nonzero ideal listed above. We want to estimate $\Pr_{\mathbf{B} \leftarrow\$ \mathcal{R}_q^{l\times 1}}[\mathbf{B}\mathbf{x} \in \mathcal{C}]$. Since the function $\mathbf{B} \in \mathcal{R}_q^{1\times l} \to \mathbf{B}\mathbf{x} \in \mathcal{J}$ is a morphism between additive groups, of image $\mathcal{J}^l$, it can be seen that the distribution of $\mathbf{B}x$ is uniform over $\mathcal{J}^l$ and thus

$$\Pr_{\mathbf{B} \leftarrow\$ \mathcal{R}_q^{1\times l}}[\mathbf{B}\mathbf{x} \in \mathcal{C}] = \left(\frac{|\mathcal{C} \cap \mathcal{J}|}{|\mathcal{J}|}\right)^l$$

We proceed by bounding the ratio $\frac{|\mathcal{C}\cap\mathcal{J}|}{|\mathcal{J}|}$, by disjunction of cases.

Case 1: ($\mathcal{J} = (3^h)$ for $h \in \{0, \ldots, k-1\}$). Observe that

$$
\begin{aligned}
|\mathcal{C} \cap \mathcal{J}| &\leq \left|\Big((3^h)\mathbb{Z} \cap [\![-q/12, q/12]\!]\Big)\right|^d \\
&\leq \left(\left\lceil \frac{3^{k-h}}{6} \right\rceil\right)^d \\
&\leq \begin{cases} 1 \text{ if } h = k-1 \quad \text{(it is actually equal).} \\ \left(3^{k-h}/6+1\right)^d \leq 3^{d(k-h-1)} \quad \text{if } h \in [\![0, \ldots, k-2]\!] \end{cases}
\end{aligned}
$$

Thus,

$$
\frac{|\mathcal{C} \cap \mathcal{J}|}{|\mathcal{J}|} \leq \left(\left\lceil \frac{3^{k-h}}{6} \right\rceil \frac{1}{3^{k-h}}\right)^d \leq \begin{cases} \left(1/3^{k-h}\right)^d \text{ if } h = k-1 \\ \left(\frac{3^{k-h-1}}{3^{k-h}}\right)^d \text{ if } h \in [\![0, \ldots, k-2]\!] \text{ and } k \geq 2. \\ \leq 3^{-d} \ . \end{cases}
$$

Case 2: ($\mathcal{J} = (3^h Q_i)$ for $h \in \{0, \ldots, k-1\}$,$i \in \{1, 2\}$). Start by noting that any element e of $\mathcal{J}$ can be uniquely written $e = Q_i(X)\, s$ where $s = \sum_{i=0}^{d/2-1} s_i X^i \in (3^k) \subset \mathcal{R}$ is a polynomial of degree strictly less than $d/2$. Also note that $\|e\|_\infty < q/12$ implies $\|s\|_\infty < q/12$. Indeed, for $i \in \{0, \ldots, n/4-1\}$ we have $e_i = -s_i$ and for $i \in \{n/4, \ldots, n/2-1\}$, we have $e_{i+n/2} = s_i$. This fact and the unicity of the s in the decomposition of e imply that

$$
\frac{|\mathcal{J} \cap \mathcal{C}|}{|\mathcal{J}|} \leq \frac{\left|\left\{(3^h)\mathbb{Z} \cap [\![-q/12, q/12]\!]\right\}^{d/2}\right|}{3^{-\frac{d(k-h)}{2}}} \leq \left(\left\lceil \frac{3^{d(k-h)}}{6} \right\rceil \frac{1}{3^{k-h}}\right)^{d/2} \leq 3^{-d/2} \ ,
$$

where the last inequalities are proved as for case 1.

We thus deduce that for any $\mathbf{x} \in \mathcal{R}_x - \{0\}$,

$$
\mathrm{Pr}_{\mathbf{B} \leftarrow\$ \mathcal{R}_q^{1 \times l}}[\mathbf{B}\mathbf{x} \in \mathcal{C}] =\leq 3^{-\frac{dl}{2}}
$$

Taking the union bound over all nonzero $\mathbf{x} \in \mathcal{R}_q$ we conclude that

$$
\mathrm{Pr}_{\mathbf{B} \leftarrow\$ \mathcal{R}_q^{1 \times l}}[\mathbf{B}\mathbf{x} \in \mathcal{C}] \leq q^d 3^{-\frac{dl}{2}} = 3^{d\left(\frac{2k-l}{2}\right)}
$$

Proof of structured part of Lemma 1 (Equation (2)***).*** This is an adaptation of the demonstration of [15, Lemma 5.2]. Assume $\mathbf{A}\mathcal{R}_q^l = \mathcal{R}_q$ and $s \geq \eta_\epsilon(\Lambda^\perp(\mathbf{A}))$. We recall that $\Lambda_q^\perp(\mathbf{A}) \subset \mathbb{Z}^{ld}$ is a full-rank lattice. Thus, by [15, Corollary 2.8]

$$
\mathsf{SD}\Big(\mathcal{D}_{\mathbb{Z},s}^{ld} \mod \Lambda_{\mathcal{R},q}^\perp(\mathbf{A}), \mathsf{U}\left(\mathbb{Z}_q^{ld}\right) \mod \Lambda_{\mathcal{R},q}^\perp(\mathbf{A})\Big) < 2\epsilon \ .
$$

Then, since $\mathbf{A}\mathcal{R}_q^l = \mathcal{R}_q$, the application: $\mathbb{Z}^{ld} \bmod \Lambda_{\mathcal{R},q}^\perp(\mathbf{A}) \to \mathcal{R}_q$ that sends $\mathbf{e} + \Lambda_{\mathcal{R},q}^\perp(\mathbf{A})$ to $\mathbf{A}\mathsf{Cf}^{-1}(\mathbf{e})$ is an isomorphism.

We estimate $\eta_\epsilon(\Lambda_{\mathcal{R},q}^\perp(\mathbf{A}))$ with Lemma 12 and establish the conditions for our assumptions to hold with Lemma 1, which yields the conclusion.

B.4 Results about the quantum queries of a classical function

For $l, m \in \mathbb{N}^*$ and $f : \{0,1\}^l \to \{0,1\}^m$ a function, we denote by $|f\rangle$ the function

$$
|f\rangle \left(\sum_{(x,y) \in \{0,1\}^n \times \{0,1\}^m} \alpha_{x,y} |x, y\rangle\right) = \sum_{(x,y) \in \{0,1\}^n \times \{0,1\}^m} \alpha_{x,y} |x, y \oplus f(x)\rangle \ .
$$

It is the usual way to embed classical functions into quantum ones. In particular, a quantum query to a hash function H is a query of $|\mathsf{H}\rangle$.

In this section, we will see how, given quantum access to $|f\rangle$ and $|g\rangle$, we can compute:

- $|g \circ f\rangle$ (for f and g composable), see Lemma 13.
- $|g \times f\rangle$ (for f and g with same domain) Lemma 14.
- $|g_{|X_g} \sqcup f_{|X_f}\rangle$ (for $f, g : X_g \sqcup X_f \to Y$, and $g_{|X_g} \sqcup f_{|Y_f}(x)$ equal to $g(x)$ if $x \in X_g$ and $f(x)$ if $x \in X_f$), see Lemma 15.

Lemma 13 (Composition of functions). *Let $l, m, n \in \mathbb{N}^*$, $f : \{0,1\}^l \to \{0,1\}^m$ and $g : \{0,1\}^m \to \{0,1\}^n$, it is possible to implement $|g \circ f\rangle$ using 2 queries to $|f\rangle$ and one query to $|g\rangle$. More precisely, $|g \circ f\rangle$ can be implemented as the following quantum algorithm,*

$$\frac{\mathsf{Comp}_{|f\rangle,|g\rangle}\left(|\phi\rangle = \sum_{(x,z)\in\{0,1\}^l\times\{0,1\}^n} \alpha_{x,z}\,|x,z\rangle\right)}{\begin{array}{ll}
\textit{Insertion of separable qubit } |0^m\rangle\textit{:} & \displaystyle\sum_{(x,z)\in\{0,1\}^l\times\{0,1\}^n} \alpha_{x,z}\,|x,0^m,z\rangle,\\
\textit{Application of } |f\rangle\otimes\mathsf{id}\textit{ :} & \displaystyle\sum_{(x,z)\in\{0,1\}^l\times\{0,1\}^n} \alpha_{x,z}\,|x,f(x),z\rangle,\\
\textit{Application of } \mathsf{id}\otimes|g\rangle\textit{ :} & \displaystyle\sum_{(x,z)\in\{0,1\}^l\times\{0,1\}^n} \alpha_{x,z}\,|x,f(x),z\oplus(g\circ f)(x)\rangle,\\
\textit{Application of } |f\rangle\otimes\mathsf{id}\textit{ :} & \displaystyle\sum_{(x,z)\in\{0,1\}^l\times\{0,1\}^n} \alpha_{x,z}\,|x,0^m,z\oplus(g\circ f)(x)\rangle,\\
\textit{This is a separate state, we return:} & \displaystyle\sum_{(x,z)\in\{0,1\}^l\times\{0,1\}^n} \alpha_{x,z}\,|x,z\oplus(g\circ f)(x)\rangle = |g\circ f\rangle(|\phi\rangle).
\end{array}}$$

Proof. The algorithm shows the result of each step of the calculus.

Lemma 14 (Product of functions). *Let $l, m, n \in \mathbb{N}^*$, $f : \{0,1\}^l \to \{0,1\}^m$ and $g : \{0,1\}^l \to \{0,1\}^n$. It is possible to implement $|g \times f\rangle$ using one query to $|f\rangle$ and one query to $|g\rangle$.*

More precisely. Let V the function

$$\sum_{(x,y)\in\{0,1\}^l\times\{0,1\}^m} \alpha_{x,y}|x,y\rangle \longrightarrow \sum_{(x,y)\in\{0,1\}^l\times\{0,1\}^m} \alpha_{x,y}|y,x\rangle \ .$$

Then, $|f \times g\rangle = (\mathsf{id}\otimes\mathsf{V}\otimes\mathsf{id})\circ(|f\rangle\otimes|g\rangle)\circ(\mathsf{id}\otimes\mathsf{V}\otimes\mathsf{id})$.

Proof. Shown by direct computation.

Lemma 15 (Conditional union of functions). *Let $m, n \in \mathbb{N}^*$, $f, g : \{0,1\}^m \to \{0,1\}^n$ and a partition $\{0,1\}^m = X_g \sqcup X_f$. It is possible to implement $|f_{|X_f} \sqcup g_{|X_g}\rangle$ using one query to $|f\rangle$*

and one query to $|g\rangle$.

$$\frac{\mathsf{CondUnion}_{|f\rangle,X_f,|g\rangle,X_g}\left(|\phi\rangle = \sum_{(x,z)\in\{0,1\}^m\times\{0,1\}^n}\alpha_{x,z}\,|x,z\rangle\right)}{}$$

Insertion of separable qubit $|0^m\rangle$: $\displaystyle\sum_{(x,z)\in\{0,1\}^m\times\{0,1\}^n}\alpha_{x,z}\,|x,0^m,z\rangle$,

Application of $|\mathsf{id}\rangle\otimes\mathsf{id}$: $\displaystyle\sum_{(x,z)\in\{0,1\}^m\times\{0,1\}^n}\alpha_{x,x,z}\,|x,x,z\rangle$,

Application of $|f\rangle$ *in the last* $m+n$ *qubit controlled by the first* m *qubits with the condition* $x\in X_f$: $\displaystyle\sum_{(x,z)\in\{0,1\}^m\times\{0,1\}^n}\alpha_{x,z}\,|x,x,z\oplus\left(f_{|X_f}\sqcup\mathsf{id}_{|X_g}\right)(x)\rangle$,

Application of $|g\rangle$ *in the last* $m+n$ *qubit controlled by the first* m *qubits with the condition* $x\in X_g$: $\displaystyle\sum_{(x,z)\in\{0,1\}^m\times\{0,1\}^n}\alpha_{x,z}\,|x,x,z\oplus\left(f_{|X_f}\sqcup g_{|X_g}\right)(x)\rangle$,

Application of $|\mathsf{id}\rangle\otimes\mathsf{id}$: $\displaystyle\sum_{(x,z)\in\{0,1\}^m\times\{0,1\}^n}\alpha_{x,z}\,|x,0^m,z\oplus\left(f_{|X_f}\sqcup g_{|X_g}\right)(x)\rangle$,

This is a separate state, we return: $\displaystyle\sum_{(x,z)\in\{0,1\}^m\times\{0,1\}^n}\alpha_{x,z}\,|x,z\oplus(f_{|X_f}\sqcup g_{|X_g})(x)\rangle$

$$= |f_{|X_f}\sqcup g_{|X_g}\rangle(|\phi\rangle).$$

Proof. The algorithm shows the result of each step of the calculus.

B.5 Missing proofs of reprogramming Hash lemmas

A lemma to separate classical from quantum queries

Lemma 16. *Let* $m,n\in\mathbb{N}^*$. *We consider a probabilistic algorithm* Setup *that, for an input* $\mathsf{in}_{\mathsf{setup}}$, *outputs two functions* $\mathsf{H}_0,\mathsf{H}_1 : X=\{0,1\}^m\to Y=\{0,1\}^n$ *and an auxiliary output* $\mathsf{aux}_{\mathsf{setup}}$. *We suppose that:*

- *The output* $\mathsf{aux}_{\mathsf{setup}}$ *is determinist in the input* $\mathsf{in}_{\mathsf{setup}}$*: only the computation of* H_0 *and* H_1 *is probabilistic.*
- *For each input* $\mathsf{in}_{\mathsf{setup}}$ *and* $b\in\{0,1\}$, *the distributions* $(p_{b,x})_{x\in X}$, *where* $p_{b,x}$ *is defined by* $\mathsf{H}_b(x)\colon(\mathsf{H}_0,\mathsf{H}_1)\leftarrow\mathsf{Setup}(\mathsf{in}_{\mathsf{setup}})$, *are independent.*

Let consider $Q_c,Q_q\in\mathbb{N}$. *Let denote by* $\mathsf{FindHash}_{Q_c,Q_q}$ *the following game, applied to quantum adversaries* $\mathcal{A}=(\mathcal{A}_1,\mathcal{A}_2,\mathcal{A}_3)$.

$\mathsf{FindHash}_{Q_c,Q_q}(\mathcal{A}=(\mathcal{A}_1,\mathcal{A}_2,\mathcal{A}_3))$

1: $\mathsf{in}_{\mathsf{setup}}\leftarrow\mathcal{A}_1()$
2: $(\mathsf{H}_0,\mathsf{H}_1,\mathsf{aux}_{\mathsf{setup}})\leftarrow\mathsf{Setup}(\mathsf{in}_{\mathsf{setup}})$
3: $b\leftarrow\$\,\{0,1\}$
4: $|\mathsf{aux}\rangle\leftarrow\mathcal{A}_2^{\mathsf{H}_b}(\mathsf{in}_{\mathsf{setup}},\mathsf{aux}_{\mathsf{setup}})$
5: $\tilde{b}\leftarrow\mathcal{A}_3^{|\mathsf{H}_b\rangle}(|\mathsf{aux}\rangle)$
6: **if** $\mathcal{A}_2$ *used* H_b *more than* Q_c *times*
7: $\quad\vee$ $\mathcal{A}_3$ *used* $|\mathsf{H}_b\rangle$ *more than* Q_q *times* **then**
8: $\quad\tilde{b}\leftarrow\$\,\{0,1\}$
9: **return** $[\![b=\tilde{b}]\!]$

We omit $\mathcal{A}_2$ *is* $Q_c=0$ *and* $\mathcal{A}_3$ *if* $Q_q=0$.

Finally, Let

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{FindHash}_{Q_c,Q_q}} = \left|\Pr\left[1\leftarrow\mathsf{FindHash}_{Q_c,Q_q}(\mathcal{A})\right]-\frac{1}{2}\right| .$$

Then, there exist quantum PPT adversaries $\mathcal{A}_{\mathsf{CQueries}}, \mathcal{A}_{\mathsf{QQueries}}$ *such that,*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{FindHash}_{Q_c,Q_q}} \leq \mathsf{Adv}_{\mathcal{A}_{\mathsf{CQueries}}}^{\mathsf{FindHash}_{Q_c,0}} + \mathsf{Adv}_{\mathcal{A}_{\mathsf{QQueries}}}^{\mathsf{FindHash}_{0,Q_q}} \quad .$$

$\mathsf{G}_{1,Q_c,Q_q}\ (\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3))$

$\mathsf{in}_{\mathsf{setup}} \leftarrow \mathcal{A}_1()$
$(\mathsf{H}_0, \mathsf{H}_1, \mathsf{aux}_{\mathsf{setup}}) \leftarrow \mathsf{Setup}(\mathsf{in}_{\mathsf{setup}})$
$b \leftarrow\!\$\ \{0,1\}$
$|\mathsf{aux}\rangle \leftarrow \mathcal{A}_2^{\mathsf{H}_b}(\mathsf{in}_{\mathsf{setup}}, \mathsf{aux}_{\mathsf{setup}})$
// Let $S \subset X$ the set of element queried by $\mathcal{A}_2$
// $\mathsf{zero} : X \to Y$ the constant function to $0^n \in Y$
// and $\mathsf{H}_b^{\mathsf{withoutCQueries}} = \mathsf{H}_{b|X-S} \sqcup \mathsf{zero}_{|S}$
$\tilde{b} \leftarrow \mathcal{A}_3^{|\mathsf{H}_b^{\mathsf{withoutCQueries}}\rangle}(|\mathsf{aux}\rangle)$
if $\mathcal{A}_2$ used H_b more than Q_c times
$\vee$ $\mathcal{A}_3$ used $|\mathsf{H}_b^{\mathsf{withoutCQueries}}\rangle$
more than Q_q times **then**
if $\mathcal{A}_2$ used H_b more than Q_c times
$\vee$ $\mathcal{A}_3$ used $|\mathsf{H}_b\rangle$ more than Q_q times **then**
$\tilde{b} \leftarrow\!\$\ \{0,1\}$
return $[\![b = \tilde{b}]\!]$

$\tilde{\mathsf{G}}_{1,Q_c,Q_q}\ (\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3))$

$\mathsf{in}_{\mathsf{setup}} \leftarrow \mathcal{A}_1()$
$(\mathsf{H}_0, \mathsf{H}_1, \mathsf{aux}_{\mathsf{setup}}) \leftarrow \mathsf{Setup}(\mathsf{in}_{\mathsf{setup}})$
$b_c \leftarrow\!\$\ \{0,1\}, b_q \leftarrow\!\$\ \{0,1\}$
$|\mathsf{aux}\rangle \leftarrow \mathcal{A}_2^{\mathsf{H}_{b_c}}(\mathsf{in}_{\mathsf{setup}}, \mathsf{aux}_{\mathsf{setup}})$
// Let $S \subset X$ the set of element queried by $\mathcal{A}_2$,
// $\mathsf{zero} : X \to Y$ the constant function to $0^n \in Y$
// and $\mathsf{H}_{b_q}^{\mathsf{withoutCQueries}} = \mathsf{H}_{b_q|X-S} \sqcup \mathsf{zero}_{|S}$
$\tilde{b} \leftarrow \mathcal{A}_3^{|\mathsf{H}_{b_q}^{\mathsf{withoutCQueries}}\rangle}(|\mathsf{aux}\rangle)$
if $\mathcal{A}_2$ used H_{b_c} more than Q_c times
$\vee$ $\mathcal{A}_3$ used $|\mathsf{H}_{b_q}^{\mathsf{withoutCQueries}}\rangle$ more
than Q_q times **then**
$\tilde{b} \leftarrow\!\$\ \{0,1\}$
return $\tilde{b}$

Fig. 9. Games $\mathsf{G}_1, \tilde{\mathsf{G}}_1$ of proof of Lemma 16.

Proof. **From** FindHash **to** G_1**:** Using the notations of the game G_1 of Figure 9, we define $\mathsf{H}_b^{\mathsf{CQueries}} = \mathsf{H}_{b|S} \sqcup \mathsf{zero}_{|X-S}$.

We create an adversary $\tilde{\mathcal{A}} = (\mathcal{A}_1, \tilde{\mathcal{A}}_2, \tilde{\mathcal{A}}_3)$ of G_1 such that

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{G}_{0,Q_c,Q_q}} \leq \mathsf{Adv}_{\tilde{\mathcal{A}}}^{\mathsf{G}_{1,Q_c,Q_q}} \quad ,$$

$\tilde{\mathcal{A}}_2$, $\tilde{\mathcal{A}}_3$ are described in Figure 10.

Note that $\tilde{\mathcal{A}}_3$ can simulate each query to $|\mathsf{H}_b\rangle$ by using one query to $|\mathsf{H}_b^{\mathsf{withoutCQueries}}\rangle$. Indeed, it can use the knowledge of classical queries and answers $(q_s, r_s)_{s \in S}$ to construct

$$\mathsf{H}_b^{\mathsf{CQueries}}(x) = \begin{cases} r_s \text{ if } x = q_s \text{ for } s \in S \\ \mathsf{zero}(x) \text{ else} \end{cases} \quad .$$

Then, it uses the Lemma 15 with $\mathsf{H}_b = \mathsf{H}_b^{\mathsf{withoutCQueries}}{}_{|X-S} \sqcup \mathsf{H}^{\mathsf{CQueries}}{}_{|S}$ in order to simulate each query to $|\mathsf{H}_b\rangle$ with one query to $|\mathsf{H}_b^{\mathsf{withoutCQueries}}\rangle$ and one query to $|\mathsf{H}_b^{\mathsf{CQueries}}\rangle$.

$\tilde{\mathcal{A}}_2^{\mathsf{H}_b}(\mathsf{in}_{\mathsf{setup}}, \mathsf{aux}_{\mathsf{setup}})$

1 : $|\mathsf{aux}\rangle \leftarrow \mathcal{A}_2^{\mathsf{H}_b}(\mathsf{in}_{\mathsf{setup}}, \mathsf{aux}_{\mathsf{setup}})$
2 : // Let $S \subset X$ the set of element queried by $\mathcal{A}_2$
3 : // and $(\mathsf{in}_s, \mathsf{out}_s), s \in S$ the (query,response) tuples
4 : // asked by $\mathcal{A}_2$ to H_b
5 : $|\tilde{\mathsf{aux}}\rangle \leftarrow |\mathsf{aux}\rangle \cup (\mathsf{in}_s, \mathsf{out}_s)_{s\in S}$
6 : **return** $\tilde{\mathsf{aux}}$

$\tilde{\mathcal{A}}_3^{\mathsf{H}_b^{\mathsf{withoutCQueries}}}(|\mathsf{aux}\rangle)$

1 : $\mathsf{in}_{\mathsf{setup}} \leftarrow \mathcal{A}_3^{|\mathsf{H}_b\rangle\rangle}()$
2 : // where $\mathsf{H}_b = \mathsf{H}_b^{\mathsf{withoutCQueries}}{}_{|X-S} \sqcup \mathsf{H}_{b|S}$
3 : // so each query of $|\mathsf{H}_b\rangle$ can be computed by $\tilde{\mathcal{A}}_3$
4 : // using one query of $|\mathsf{H}_b^{\mathsf{withoutCQueries}}\rangle$
5 : // and the knowledge of $S, \mathsf{H}_b^{\mathsf{CQueries}}$
6 : **return** $\tilde{b}$

Fig. 10. Adversary $\tilde{\mathcal{A}}$ of proof of Lemma 16 ($\tilde{\mathcal{A}}_1 = \mathcal{A}_1$).

Analysis of G_1: we see that,

$$
\begin{aligned}
&\mathsf{Adv}_{\mathcal{A}}^{\mathsf{G}_{1,Q_c,Q_q}} \\
&= \frac{1}{2}\left|\Pr\left[\tilde{b}{=}0 \text{ in } \mathsf{G}_{1,Q_c,Q_q} \;\middle|\; b{=}1\right] - \Pr\left[\tilde{b}{=}0 \text{ in } \mathsf{G}_{1,Q_c,Q_q} \;\middle|\; b{=}1\right]\right| \\
&= \frac{1}{2}\left|\Pr\left[\tilde{b}{=}0 \text{ in } \tilde{\mathsf{G}}_{1,Q_c,Q_q}(\mathcal{A}) \;\middle|\; (b_c,b_q){=}(0,0)\right] - \Pr\left[\tilde{b}{=}0 \text{ in } \mathsf{G}_{1,Q_c,Q_q}(\mathcal{A}) \;\middle|\; (b_c,b_q){=}(1,1)\right]\right| \\
&\leq \frac{1}{2}\left|\Pr\left[\tilde{b}{=}0 \text{ in } \tilde{\mathsf{G}}_{1,Q_c,Q_q}(\mathcal{A}) \;\middle|\; (b_c,b_q){=}(0,0)\right] - \Pr\left[\tilde{b}{=}0 \text{ in } \mathsf{G}_{1,Q_c,Q_q}(\mathcal{A}) \;\middle|\; (b_c,b_q){=}(0,1)\right]\right| \\
&\quad + \frac{1}{2}\left|\Pr\left[\tilde{b}{=}0 \text{ in } \tilde{\mathsf{G}}_{1,Q_c,Q_q}(\mathcal{A}) \;\middle|\; (b_c,b_q){=}(0,1)\right] - \Pr\left[\tilde{b}{=}0 \text{ in } \mathsf{G}_{1,Q_c,Q_q}(\mathcal{A}) \;\middle|\; (b_c,b_q){=}(1,1)\right]\right| \\
&= \frac{1}{2}\left|\Pr\left[\tilde{b}{=}0 \text{ in } \mathsf{FindHash}_{0,Q_q}(\mathcal{A}_{\mathsf{QQueries}}) \;\middle|\; b{=}0\right] - \Pr\left[\tilde{b}{=}0 \text{ in } \mathsf{FindHash}_{0,Q_q}(\mathcal{A}_{\mathsf{QQueries}}) \;\middle|\; b{=}1\right]\right| \\
&\quad + \frac{1}{2}\left|\Pr\left[\tilde{b}{=}0 \text{ in } \mathsf{FindHash}_{Q_c,0}(\mathcal{A}_{\mathsf{CQueries}}) \;\middle|\; b{=}0\right] - \Pr\left[\tilde{b}{=}0 \text{ in } \mathsf{FindHash}_{Q_c,0}(\mathcal{A}_{\mathsf{CQueries}}) \;\middle|\; b{=}1\right]\right| \\
&= \mathsf{Adv}_{\mathcal{A}_{\mathsf{QQueries}}}^{\mathsf{FindHash}_{0,Q_q}} + \mathsf{Adv}_{\mathcal{A}_{\mathsf{CQueries}}}^{\mathsf{FindHash}_{Q_c,0}} \;,
\end{aligned}
$$

Where the adversary $\mathcal{A}_{\mathsf{QQueries}}$ is $(\mathcal{A}_1, \mathcal{A}_{\mathsf{QQueries},2})$ ($\mathcal{A}_{\mathsf{QQueries},2}$ is described in Figure 11) and the adversary $\mathcal{A}_{\mathsf{CQueries}}$ is $(\mathcal{A}_1, \mathcal{A}_{\mathsf{CQueries},2})$ ($\mathcal{A}_{\mathsf{CQueries},2}$ is described in Figure 11). Note that the two hypotheses about Setup are used in order to have

$$
\begin{aligned}
&\frac{1}{2}\left|\Pr\left[\tilde{b} = 0 \text{ in } \mathsf{FindHash}_{Q_c,0}(\mathcal{A}_{\mathsf{CQueries}}) \;\middle|\; b = 0\right] - \Pr\left[\tilde{b} = 0 \text{ in } \mathsf{FindHash}_{Q_c,0}(\mathcal{A}_{\mathsf{CQueries}}) \;\middle|\; b = 1\right]\right| \\
&= \mathsf{Adv}_{\mathcal{A}_{\mathsf{CQueries}}}^{\mathsf{FindHash}_{Q_c,0}} \;.
\end{aligned}
$$

$$
\begin{aligned}
&\frac{1}{2}\left|\Pr\left[\tilde{b} = 0 \text{ in } \mathsf{FindHash}_{0,Q_q}(\mathcal{A}_{\mathsf{QQueries}}) \;\middle|\; b = 0\right] - \Pr\left[\tilde{b} = 0 \text{ in } \mathsf{FindHash}_{0,Q_q}(\mathcal{A}_{\mathsf{QQueries}}) \;\middle|\; b = 1\right]\right| \\
&= \mathsf{Adv}_{\mathcal{A}_{\mathsf{QQueries}}}^{\mathsf{FindHash}0,Q_q} \;.
\end{aligned}
$$

Proof of Proposition 7 about non-adaptative reprogramming

Lemma 17 (Lemma 9 of [5]). *Let A be a quantum algorithm that makes at most Q queries to a quantum random oracle $\mathcal{O}$ with codomain $\{0,1\}^m$ ($m \in \mathbb{N}^*$). Fix y in the codomain of $\mathcal{O}$. The expected value of the total query probability of all x such that $\mathcal{O}(x) = y$ is at most $\frac{2Q^3}{2^m}$.*

Proof of Proposition 7. We use Lemma 16 in order to study separately the case were only classical (ROM) or quantum (QROM) queries are made.

$\mathcal{A}^{|\mathsf{H}_b\rangle}_{\mathsf{QQueries},2}(\mathsf{in}_{\mathsf{setup}}, \mathsf{aux}_{\mathsf{setup}})$

$(\tilde{\mathsf{H}}_0, \tilde{\mathsf{H}}_1, \mathsf{aux}_{\mathsf{setup}}) \leftarrow \mathsf{Setup}(\mathsf{in}_{\mathsf{setup}})$
$|\mathsf{aux}\rangle \leftarrow \mathcal{A}_2^{\tilde{\mathsf{H}}_0}(\mathsf{in}_{\mathsf{setup}}, \mathsf{aux}_{\mathsf{setup}})$
// queries to $\tilde{\mathsf{H}}_0$ answered by $\mathcal{A}_{\mathsf{QQueries},2}$
// We note $S \subset X$ the set of element
// queried by $\mathcal{A}_2$, and
// $\mathsf{H}_b^{\mathsf{withoutCQueries}} = \mathsf{H}_{b|X-S} \sqcup \mathsf{zero}_{|S}$
$\tilde{b} \leftarrow \mathcal{A}_3^{|\mathsf{H}_b^{\mathsf{withoutCQueries}}\rangle}(|\mathsf{aux}\rangle)$
// queries are answered by$\mathcal{A}_{\mathsf{CQueries},2}$
// that ask a query of $|\mathsf{H}_b\rangle$ and use
// the knowledge of S and $|\mathsf{zero}\rangle$
// in order to compute $|\mathsf{H}_b^{\mathsf{withoutCQueries}}\rangle$
return $\tilde{b}$

$\mathcal{A}^{\mathsf{H}_b}_{\mathsf{CQueries},2}(\mathsf{in}_{\mathsf{setup}}, \mathsf{aux}_{\mathsf{setup}})$

$(\tilde{\mathsf{H}}_0, \tilde{\mathsf{H}}_1, \mathsf{aux}_{\mathsf{setup}}) \leftarrow \mathsf{Setup}(\mathsf{in}_{\mathsf{setup}})$
$|\mathsf{aux}\rangle \leftarrow \mathcal{A}_2^{\mathsf{H}_b}(\mathsf{in}_{\mathsf{setup}}, \mathsf{aux}_{\mathsf{setup}})$
// queries are directly asked by $\mathcal{A}_{\mathsf{CQueries},2}$ to H_b
// We note $S \subset X$ the set of element queried by $\mathcal{A}_2$,
// and $\tilde{\mathsf{H}}_1^{\mathsf{withoutCQueries}} = \tilde{\mathsf{H}}_{1|X-S} \sqcup \mathsf{zero}_S$
$\tilde{b} \leftarrow \mathcal{A}_3^{|\tilde{\mathsf{H}}_1^{\mathsf{withoutCQueries}}\rangle}(|\mathsf{aux}\rangle)$
// queries are answered by $\mathcal{A}_{\mathsf{CQueries},2}$
// that knows $\mathsf{H}_1^{\mathsf{withoutCQueries}}$
return $\tilde{b}$

Fig. 11. Adversaries $\mathcal{A}_{\mathsf{CQueries},2}$ and $\mathcal{A}_{\mathsf{QQueries},2}$ of proof of Lemma 16.

Proof of the ROM case
We will show that for each fixed partition $\mathcal{P} = (X_i)_{i\in[\![1,p]\!]}$, $p \leq P$ and family of probability distributions $(\mathsf{Dist}_i)_{i\in[\![1,p]\!]}$ such that for each $i \in [\![1,p]\!]$, $\mathsf{SD}(\mathsf{Dist}_i, \mathsf{U}(Y)) < \epsilon$, the advantage of $\mathcal{A}$, making only classical queries, is less that $\epsilon\, Q$.

We suppose that $\mathcal{A}$ makes Q_i queries on X_i, $Q = \sum_i Q_i$. We create the following games:
- G_0 is the game where the oracle is always set to H_1.
- For $k \in [\![1,p]\!]$, G_k is like G_{k-1} except for the modification of the oracle where Dist_k is replaced by $\mathsf{U}(Y)$.

We then see that,

$$\begin{aligned}\mathsf{Adv}^{\mathsf{G}_0}_{\mathcal{A}} &= \big|\Pr[0 \leftarrow \mathcal{A} \text{ in } \mathsf{G}_0] - \Pr[0 \leftarrow \mathcal{A} \text{ in } \mathsf{G}_p]\big| \\ &\leq \sum_{i=1}^{p} \big|\Pr[0 \leftarrow \mathcal{A} \text{ in } \mathsf{G}_i] - \Pr[0 \leftarrow \mathcal{A} \text{ in } \mathsf{G}_{i-1}]\big| \\ &\leq \sum_{i=1}^{p} Q_i \mathsf{SD}(\mathsf{U}(Y), \mathsf{Dist}_i) \leq Q\,\epsilon\ .\end{aligned}$$

Proof of the QROM case
The proof is an adaptation of the demonstration of [5, Lemma 3] in our more general situation. We will show that for each fixed partition $\mathcal{P} = (X_i)_{i\in[\![1,p]\!]}$, $p \leq P$ and family of probability distributions $(\mathsf{Dist}_i)_{i\in[\![1,p]\!]}$ such that for each $i \in [\![1,p]\!]$, $\mathsf{SD}(\mathsf{Dist}_i, \mathsf{U}(Y)) < \epsilon$, the advantage of $\mathcal{A}$ to distinguish the uniform oracle H_0 and H_1 is less that $4Q^2\sqrt{P\epsilon}$.

We first remark that H_0 is the random oracle. Then, as in the demonstration of Lemma [5, Lemma 3], we will describe another way to construct H_1 as follows. For each $i \in [\![1,p,]\!]$, we define $\epsilon_i = \mathsf{SD}(\mathsf{Dist}_i, \mathsf{U}(Y)) \leq \epsilon$ and for each i such that $\epsilon_i > 0$, we define Dist'_i by :
- If $\Pr[y = \mathsf{Dist}_i] < 2^{-m}$, then $\Pr\big[y = \mathsf{Dist}'_i\big] = 0$,
- If $\Pr[y = \mathsf{Dist}_i] \geq 2^{-m}$, then $\Pr\big[y = \mathsf{Dist}'_i\big] = (\Pr[y = \mathsf{Dist}_i] - 2^{-m})\,\frac{2}{\epsilon_i}$,

The demonstration of [5, Lemma 3] shows that it is a probability distribution using the fact that

$$\frac{\epsilon_i}{2} = \sum_{y:\Pr[y=\mathsf{Dist}_i]\geq 2^{-m}} \big(\Pr[y = \mathsf{Dist}_i] - 2^{-m}\big) = \sum_{y:\Pr[y=\mathsf{Dist}_i]<2^{-m}} \big(2^{-m} - \Pr[y = \mathsf{Dist}_i]\big)$$

It also shows that H_1 can be described as:

$\mathsf{H}_1(x)$

```
1 :  y ←$ H_0(x)   (i.e, sampled with U({0,1}^m))
2 :    // we recall that Y = {0,1}^m
3 :  for i ∈ [[1, p]]
4 :      if x ∈ X_i ∧ Pr[y = Dist_i] < 2^{-m} then
5 :    // Note that this condition never happens if ε_i = 0
6 :          with probability 1 − 2^m Pr[y = Dist_i]:
7 :              y' ←$ Dist'_i
8 :              return y'
9 :  return y
```

Now, we bound the expected query magnitude of the $x \in X$ such that the oracle changed. Lemma 17 shows that the expected total query probability of any x such that $\mathsf{H}_0(x) = y$ is $2Q^3 2^{-m}$. Let σ be the query magnitude of points x at which we changed the oracle. The alternative construction of H_1 shows that the only elements x where $\mathsf{H}_1(x)$ can differ from H_0 are the ones where the condition of line 4 is verified. Thus,

$$
\begin{aligned}
&\mathbb{E}[\sigma] \\
&= \sum_{i=1}^{p} \mathbb{E}\left[\sum_{\substack{x \in X_i : \\ \Pr[\mathsf{H}_0(x)=\mathsf{Dist}_i]<2^{-m}}} (1 - 2^m \Pr[\mathsf{H}_0(x) = \mathsf{Dist}_i]) \times (\text{total query magnitude of x}) \right] \\
&= \sum_{i=1}^{p} \sum_{\substack{y \in Y : \\ \Pr[y=\mathsf{Dist}_i]<2^{-m}}} (1 - 2^m \Pr[y = \mathsf{Dist}_i]) \times \mathsf{E}\left[\begin{matrix} \text{total query magnitude of all} \\ x \in X_i \text{ s.t } \mathsf{H}_0(x) = y \end{matrix} \right] \\
&\leq \sum_{i=1}^{p} \sum_{y \in Y : \Pr[y=\mathsf{Dist}_i]<2^{-m}} (1 - 2^m \Pr[y = \mathsf{Dist}_i]) \times 2Q^3 2^{-m} \quad \text{by Lemma 17} \\
&= 2Q^3 \sum_{i=1}^{p} \sum_{y \in Y : \Pr[y=\mathsf{Dist}_i]<2^{-m}} \left(2^{-m} - \Pr[y = \mathsf{Dist}_i]\right) \\
&= Q^3 \sum_{i=1}^{p} \mathsf{SD}(\mathsf{U}(Y), \mathsf{Dist}_i) \\
&\leq Q^3 p\epsilon \leq Q^3 P\epsilon \quad \text{by hypothesis on } \mathsf{SD}(\mathsf{U}(Y), \mathsf{Dist}_i) \text{ and p.}
\end{aligned}
$$

Thus, the expected Euclidean distance is

$$\mathbb{E}\left[\sqrt{Q\sigma}\right] \leq \sqrt{Q\,\mathbb{E}[\sigma]} \leq \sqrt{Q \times PQ^3\epsilon} = Q^2\sqrt{P\epsilon}\ .$$

We then conclude as in the demonstration of [5, Lemma 3] that the expected statistical distance of the output probability distributions is thus at most $4Q^2\sqrt{P\epsilon}$ and therefore the probability distribution of outputs when the oracle is H_0 is at most $4Q^2\sqrt{P\epsilon}$ away from the probability distribution of outputs when the oracle is H_1.

B.6 Generalization of [29, Claim 5.3] and proof of Proposition 1

Lemma 18 (Generalization of [29, Claim 5.3]). *Let $(A, +, x, 0, 1)$ be a commutative ring, M an A-module and* Dist *a probability distribution of A such that*

$$\varnothing \neq \overline{\mathrm{Supp}(\mathsf{Dist})} := \{a - a' : a, a' \in \mathrm{Supp}(\mathsf{Dist}), a \neq a'\} \subset A^\times \ .$$

Let $m \geq 1$. For $\mathbf{a} = (a_i)_{i \in [\![1,m]\!]} \in A^m$, and $\mathbf{m} = (m_i)_{i \in [\![1,m]\!]} \in M^m$, let $\langle \mathbf{a}, \mathbf{m} \rangle = \sum_i a_i m_i$. For $\mathbf{m} \in M^m$, let $\chi_{\mathbf{m},\mathsf{Dist}}$ the probability distribution that outputs $\langle \mathbf{a}, \mathbf{m} \rangle$ for $\mathbf{a} \leftarrow\!\$\ \mathsf{Dist}^m$. Then, $\mathbb{E}_{\mathbf{m} \in M^m}[\mathsf{SD}(\mathsf{U}(M), \chi_{\mathbf{m},\mathsf{Dist}})] \leq \mathsf{Col}(\mathsf{Dist})^{m/2}\sqrt{|M|}$, where $\mathsf{Col}(\mathsf{Dist}) := \Pr_{x,y \leftarrow \mathsf{Dist}}[x = y] = \sum_{x \in \mathrm{Supp}(\mathsf{Dist})} \Pr[\mathsf{Dist} = x]^2$. In particular

$$\Pr_{\mathbf{m} \in M^k}\left[\mathsf{SD}(\mathsf{U}(M), \chi_{\mathbf{m},\mathsf{Dist}}) > \mathsf{Col}(\mathsf{Dist})^{m/4}|M|^{1/4}\right] \leq \mathsf{Col}(\mathsf{Dist})^{k/4}|M|^{1/4} \ .$$

Moreover, if $\mathsf{Col}(\mathsf{Dist})^m < |M|^{-5}$, then,

$$\Pr_{\mathbf{m} \in M^k}[\mathbf{a} \in \mathrm{Supp}(\mathsf{Dist}) \to \langle \mathbf{a}, \mathbf{m} \rangle \in M \text{ is surjective}] \geq 1 - \mathsf{Col}(\mathsf{Dist})^{m/4}|M|^{1/4} \ .$$

Proof. We have

$$\begin{aligned}
&\sum_{h \in M} \Pr\left[\chi_{\mathbf{m},\mathrm{Supp}(\mathsf{Dist})} = h\right]^2 = \sum_{h \in M} \Pr_{\mathbf{a} \leftarrow\!\$ \mathsf{Dist}^m}[\langle \mathbf{a}, \mathbf{m} \rangle = h]^2 \\
&= \Pr_{(\mathbf{a},\mathbf{a}') \leftarrow\!\$ \mathsf{Dist}^{2m}}\left[\langle \mathbf{a}, \mathbf{m} \rangle = \langle \mathbf{a}', \mathbf{m} \rangle\right] \\
&\leq \Pr_{(\mathbf{a},\mathbf{a}') \leftarrow\!\$ \mathsf{Dist}^{2m}}\left[\mathbf{a} = \mathbf{a}'\right] + \Pr_{(\mathbf{a},\mathbf{a}') \leftarrow\!\$ \mathsf{Dist}^{2m}}\left[\langle \mathbf{a} - \mathbf{a}', \mathbf{m} \rangle = 0 \ \middle|\ \mathbf{a} \neq \mathbf{a}'\right] \\
&= \sum_{\mathbf{a} \in \mathrm{Supp}(D)^k} \Pr[\mathsf{Dist}^m = \mathbf{a}]^2 + \Pr_{(\mathbf{a},\mathbf{a}') \leftarrow\!\$ \mathsf{Dist}^{2m}}\left[\langle \mathbf{a} - \mathbf{a}', \mathbf{m} \rangle = 0 \ \middle|\ \mathbf{a} \neq \mathbf{a}'\right] \\
&\leq \sum_{(a_1,\ldots,a_m) \in \mathrm{Supp}(\mathsf{Dist})^m} \left(\prod_{i=1}^m \Pr[\mathsf{Dist} = a_i]^2\right) + \underset{(\mathbf{a},\mathbf{a}') \leftarrow\!\$ \mathsf{Dist}^{2m}}{Pr}\left[\langle \mathbf{a} - \mathbf{a}', \mathbf{m} \rangle = 0 \mid \mathbf{a} \neq \mathbf{a}'\right] \\
&= \prod_{i=1}^m \left(\sum_{a \in \mathrm{Supp}(\mathsf{Dist})} \Pr[\mathsf{Dist} = a]^2\right) + \underset{(\mathbf{a},\mathbf{a}') \leftarrow\!\$ \mathsf{Dist}^{2m}}{Pr}\left[\langle \mathbf{a} - \mathbf{a}', \mathbf{m} \rangle = 0 \mid \mathbf{a} \neq \mathbf{a}'\right] \\
&= \mathsf{Col}(\mathsf{Dist})^m + \underset{(\mathbf{a},\mathbf{a}') \leftarrow\!\$ \mathsf{Dist}^{2m}}{Pr}\left[\langle \mathbf{a} - \mathbf{a}', \mathbf{m} \rangle = 0 \mid \mathbf{a} \neq \mathbf{a}'\right] \ .
\end{aligned}$$

Taking the expectation in $\mathbf{m}$,

$$
\begin{aligned}
&\mathbb{E}_{\mathbf{m}}\left[\sum_{h\in M}\Pr\left[\chi_{\mathbf{m},\mathrm{Supp}(\mathsf{Dist})}=h\right]^2\right]\\
&\leq \mathsf{Col}(\mathsf{Dist})^m+\mathbb{E}_{\mathbf{m}}\left[\Pr_{(\mathbf{a},\mathbf{a}')\leftarrow\$\mathsf{Dist}^{2m}}\left[\left\langle \mathbf{a}-\mathbf{a}',\mathbf{m}\right\rangle=0 \;\middle|\; \mathbf{a}\neq\mathbf{a}'\right]\right]\\
&= \mathsf{Col}(\mathsf{Dist})^m+\sum_{\mathbf{m}\in M^m}\frac{1}{|M|^m}\Pr_{(\mathbf{a},\mathbf{a}')\leftarrow\$\mathsf{Dist}^{2m}}\left[\left\langle \mathbf{a}-\mathbf{a}',\mathbf{m}\right\rangle=0 \;\middle|\; \mathbf{a}\neq\mathbf{a}'\right]\\
&= \sum_{\mathbf{m}\in M^m}\Pr_{\mathbf{m}'\leftarrow\$M^m}\left[\mathbf{m}'=\mathbf{m}\right]\;\Pr_{(\mathbf{a},\mathbf{a}')\leftarrow\$\mathsf{Dist}^{2m}}\left[\left\langle \mathbf{a}-\mathbf{a}',\mathbf{m}\right\rangle=0 \;\middle|\; \mathbf{a}\neq\mathbf{a}'\right]\\
&=\Pr_{\substack{\mathbf{m}\leftarrow\$M^m\\(\mathbf{a},\mathbf{a}')\leftarrow\$\mathsf{Dist}^{2m}}}\left[\left\langle \mathbf{a}-\mathbf{a}',\mathbf{m}\right\rangle=0 \;\middle|\; \mathbf{a}\neq\mathbf{a}'\right]\\
&= \mathsf{Col}(\mathsf{Dist})^m+\sum_{\substack{\mathbf{a},\mathbf{a}'\in\mathrm{Supp}(\mathsf{Dist})^m\\\mathbf{a}\neq\mathbf{a}'}}\Pr[\mathsf{Dist}^m=\mathbf{a}]\Pr\left[\mathsf{Dist}^m=\mathbf{a}'\right]\underset{\mathbf{m}\in M^m}{Pr}\left[\left\langle \mathbf{a}-\mathbf{a}',\mathbf{m}\right\rangle=0\right]\\
&= \mathsf{Col}(\mathsf{Dist})^m+\sum_{\substack{\mathbf{a},\mathbf{a}'\in\mathrm{Supp}(\mathsf{Dist})^m\\\mathbf{a}\neq\mathbf{a}'}}\Pr[\mathsf{Dist}^m=\mathbf{a}]\Pr\left[\mathsf{Dist}^m=\mathbf{a}'\right]\frac{\mathsf{Ker}(\phi_{\mathbf{a}-\mathbf{a}'})}{|M|^m}\ . \qquad (11)
\end{aligned}
$$

where $\phi_{\mathbf{a}-\mathbf{a}'}: M^m\to M$ is defined by $\phi_{\mathbf{a}-\mathbf{a}'}(\mathbf{m})=\langle \mathbf{a}-\mathbf{a}',\mathbf{m}\rangle$.

In order to evaluate this last probability, we will show that $\phi_{\mathbf{a}-\mathbf{a}'}$ is surjective. Because $\mathbf{a},\mathbf{a}'\in\mathrm{Supp}(\mathsf{Dist})^m$ and $\mathbf{a}\neq\mathbf{a}'$, there exists i such that $a_i-a'_i\in\overline{\mathsf{Dist}}\subset A^\times$. For $m\in M$, We denote by $\hat{\mathbf{m}}$ the vector such that $\hat{\mathbf{m}}_i=m$ and $\hat{\mathbf{m}}_l=0$ for $l\neq i$. We can see that for each $m\in M$, $m=\phi\left((a_i-a'_i)^{-1}\hat{\mathbf{m}}\right)$. Thus ϕ is surjective.

We deduce that

$$
|\mathsf{Ker}(\phi_{\mathbf{a}-\mathbf{a}'})|\simeq\frac{|M|^m}{|\mathsf{Im}(\phi_{\mathbf{a}-\mathbf{a}'})|}=\frac{|M|^m}{|M|}=|M|^{m-1}\ ,
$$

and that, using Equation (11),

$$
\begin{aligned}
&\mathbb{E}_{\mathbf{m}}\left[\sum_{h\in M}\Pr\left[\chi_{\mathbf{m},\mathrm{Supp}(\mathsf{Dist})}=h\right]^2\right]\\
&= \mathsf{Col}(\mathsf{Dist})^m+\sum_{\substack{\mathbf{a},\mathbf{a}'\in\mathrm{Supp}(\mathsf{Dist})^m\\\mathbf{a}\neq\mathbf{a}'}}\frac{\Pr[\mathsf{Dist}^m=\mathbf{a}]\Pr[\mathsf{Dist}^m=\mathbf{a}']}{|M|}\\
&= \mathsf{Col}(\mathsf{Dist})^m+\frac{1}{|M|}\ . \qquad (12)
\end{aligned}
$$

Thus,

$$\begin{aligned}
&\mathbb{E}_{\mathbf{m}}\left[\sum_{h\in M}\left|\Pr\left[\chi_{\mathbf{m},\mathsf{Supp}(\mathsf{Dist})}=h\right]-\frac{1}{|M|}\right|\right]\\
&\leq \mathbb{E}_{\mathbf{m}}\left[|M|^{\frac{1}{2}}\left(\sum_{h}\left(\Pr\left[\chi_{\mathbf{m},\mathsf{Supp}(\mathsf{Dist})}=h\right]-\frac{1}{|M|}\right)^2\right)^{\frac{1}{2}}\right]\\
&= \sqrt{|M|}\,\mathbb{E}_{\mathbf{m}}\left[\left(\sum_{h}\left(\Pr\left[\chi_{\mathbf{m},\mathsf{Supp}(\mathsf{Dist})}=h\right]-\frac{1}{|M|}\right)^2\right)^{\frac{1}{2}}\right]\\
&\leq \sqrt{|M|}\left(\mathbb{E}_{\mathbf{m}}\left[\sum_{h}\Pr\left[\chi_{\mathbf{m},\mathsf{Supp}(\mathsf{Dist})}=h\right]^2\right]-\frac{1}{|M|}\right)^{\frac{1}{2}}\\
&\leq \mathsf{Col}(\mathsf{Dist})^{m/2}\sqrt{|M|}\quad \text{by equation (12).}
\end{aligned}$$

Finally, if $\mathsf{Col}(\mathsf{Dist})^m < |M|^{-5}$, we have $\frac{1}{|M|} - \mathsf{Col}(\mathsf{Dist})^{m/4}|M|^{1/4} > 0$ and thus

$$\begin{aligned}
&\mathsf{SD}(\mathsf{U}(M), \chi_{\mathbf{m},\mathsf{Dist}}) \leq \mathsf{Col}(\mathsf{Dist})^{m/4}|M|^{1/4}\\
&\Rightarrow \forall x\in M,\quad \Pr[\chi_{\mathbf{m},\mathsf{Dist}}=x] \geq \frac{1}{|M|} - \mathsf{Col}(\mathsf{Dist})^{m/4}|M|^{1/4} > 0\\
&\Rightarrow \forall x\in M,\quad x\in \mathrm{Supp}(\chi_{\mathbf{m},\mathsf{Dist}})\\
&\Rightarrow \mathbf{a}\in\mathrm{Supp}(\mathsf{Dist}) \to \langle \mathbf{a},\mathbf{m}\rangle \in M \text{ is surjective .}
\end{aligned}$$

Corollary 3. *Let $m,n,l,k,h,d\in\mathbb{N}^*$, $\mathcal{R}=\mathbb{Z}[X]/(X^d+1)$, $d=2^h$, $q=3^k$. If $k\geq 4$, $m\geq 5n+1$ and $l\geq 21$, then,*

$$\Pr_{\mathbf{A}\in\mathcal{R}_q^{1\times l}}\left[\mathbf{A}\mathcal{R}_q^l=\mathcal{R}_q\right]\geq 1-3^{-(m-n)/4},\ \Pr_{\mathbf{A}\in\mathbb{Z}_q^{n\times m}}\left[\mathbf{A}\mathbb{Z}_q^m=\mathbb{Z}_q^n\right]\geq 1-3^{-\left(\frac{d(l-4)}{4}\right)}\ .$$

Proof. It can be shown by induction on $k\geq 4$ than $\mathbf{A}\mathcal{R}_{3^4}^l=\mathcal{R}_{3^4}\Rightarrow \mathbf{A}\mathcal{R}_q^l=\mathcal{R}_q$ and $\mathbf{A}\mathbb{Z}_3^m=\mathbb{Z}_3^n\Rightarrow \mathbf{A}\mathbb{Z}_q^m=\mathbb{Z}_q^n$. For example, if we have already shown that $\mathbf{A}\mathcal{R}_{3^u}^l=\mathcal{R}_{3^u}$ for some $u\geq 4$, we write any $\mathbf{y}\in\mathcal{R}_{3^{u+1}}$ as $\mathbf{y}=3\mathbf{y}_u+\mathbf{y}_3 \mod q$ with $\mathsf{Cf}(\mathbf{y}_u)\in\{0,3^u-1\}^l, \mathsf{Cf}(\mathbf{y}_3)\in\{0,3-1\}^l$ and can thus write $\mathbf{y}=\mathbf{A}(3\mathbf{x}_1+\mathbf{x}_2)$ with $\mathbf{x}_u$ and $\mathbf{x}_u$ found using the induction hypothesis that $\mathbf{A}\mathcal{R}_{3^u}^l=\mathcal{R}_{3^u}$. We then use Lemma 18 with:

- $A=\mathbb{Z}_3$, $M=\mathbb{Z}_3^n, m=m, \mathsf{Dist}=\mathsf{U}(\llbracket -1,1\rrbracket)$. The condition $\mathsf{Col}(\mathsf{Dist})^m<|M|^{-5}$ becomes $\frac{1}{3^m}<3^{-5n}$ and if satisfied if $m\geq 5n+1$.
- $A=M=\mathcal{R}_{3^4}$, $\mathsf{Dist}=\mathsf{U}(\mathcal{S}_{\mathsf{R}})$ where $\mathcal{S}_{\mathsf{R}}=\{\sum_{i=0}^{d-1}a_iX^i\in\mathcal{R}_{3^4}\colon (a_0,\ldots,a_{d-1})\in\{-4,0,4\}^{d/4}\times\{-1,0,1\}^{d/2}\times\{-4,0,4\}^{d/4}\}\subset\mathcal{R}_{3^4}$ The distribution satisfies the condition of the lemma by Proposition 13. Moreover, The condition $\mathsf{Col}(\mathsf{Dist})^l<|M|^{-5}$ becomes $\frac{1}{3^{dl}}<3^{-20d}$ and if satisfied if $l\geq 21$.

Proof of Proposition 1. The inequalities about statistical distance are consequences of Lemma 18 with:

- $A=\mathbb{Z}_q$, $M=\mathbb{Z}_q^n$ and m elements of M.
- $A=M=\mathcal{R}_q$, with l elements of M. Corollary 2 is used to ensure the distributions satisfy the invertibility condition.

The two other inequalities are consequences of Corollary 3.

B.7 Proof of Propositions 4 and 5 about matrix delegation

Lemma 19. *Let $m, n, q \in \mathbb{N}^*, 0 < \epsilon < 1/2, s > 0, \mathbf{A} \in \mathbb{Z}^{n\times m}$. If $\mathbf{A}\mathbb{Z}^m = \mathbb{Z}^n \mod q$, then, the two following probability distributions are equal*

$$\mathsf{Dist}_1 : \mathbf{z} \hookleftarrow\$\, \mathcal{D}_{\Lambda_q^\perp(\mathbf{A})+\mathbf{x},s}, \mathbf{x} \hookleftarrow\$\, \mathbb{Z}^m\ , \quad \mathsf{Dist}_2 : \mathbf{z} \hookleftarrow\$\, \mathcal{D}_{\Lambda_{\mathbf{u},q}^\perp(\mathbf{A}),s}, \mathbf{u} \hookleftarrow\$\, \mathbb{Z}^n\ .$$

Moreover, if $s \geq \eta_\epsilon(\Lambda_q^\perp(\mathbf{A}))$, $\mathsf{SD}\Big(\mathsf{Dist}_1, \mathcal{D}_{\mathbb{Z},s}^m\Big) \leq 2\epsilon$.

Proof. If $\mathbf{A}\mathbb{Z}_q^m = \mathbb{Z}_q^n$, we can consider it as a surjective morphism between groups $((\mathbb{Z}_q^m, \mathbf{0}, +) \to (\mathbb{Z}_q^n, \mathbf{0}, +))$ to deduce that the probability distribution $\mathbf{Ax}, \mathbf{x} \hookleftarrow\$\, \mathbb{Z}_q^m$ is uniform on $\mathbb{Z}_q^n$. Using in addition $\Lambda_{q,\mathbf{Ax}}^\perp(\mathbf{A}) = \Lambda_q^\perp(\mathbf{A}) + \mathbf{x}$, we conclude that $\mathsf{Dist}_1 = \mathsf{Dist}_2$. Note now that Dist_1 and $\mathcal{D}_{\mathbb{Z},s}^m$ can be expressed as

$$\mathcal{D}_{\mathbb{Z},s}^m \colon \mathbf{z} \hookleftarrow\$\, \mathcal{D}_{\Lambda_q^\perp(\mathbf{A})+\mathbf{x},s}, \Lambda_q^\perp(\mathbf{A}) + \mathbf{x} \hookleftarrow\$\, \Big(\mathcal{D}_{\mathbb{Z},s}^m \mod \Lambda_q^\perp(\mathbf{A})\Big)\ ,$$
$$\mathsf{Dist}_1 \colon \mathbf{z} \hookleftarrow\$\, \mathcal{D}_{\Lambda_q^\perp(\mathbf{A})+\mathbf{x},s}, \mathbf{x} \hookleftarrow\$\, \Big(\mathbb{Z}^m \mod \Lambda_q^\perp(\mathbf{A})\Big)\ .$$

With this observation and [15, Corollary 2.8], we see

$$\mathsf{SD}\big(\mathsf{Dist}_1, \mathcal{D}_{\mathbb{Z},s}^m\big) \leq \mathsf{SD}\Big(\mathsf{U}\left(\mathbb{Z}^m \mod \Lambda_q^\perp(\mathbf{A})\right), \mathcal{D}_{\mathbb{Z},s}^m \mod \Lambda_q^\perp(\mathbf{A})\Big) \leq 2\epsilon\ .$$

Proof of Proposition 4. We will use an intermediate probability distribution Dist_1.

$\mathsf{Dist}_{\mathsf{ModKExt}}(\mathbf{A}, \mathbf{T_A}, s)$	$\mathsf{Dist}_1(\mathbf{A})$	$\mathsf{Dist}_{\mathsf{SimModKExt}}(\mathbf{A})$
$\mathbf{R} \hookleftarrow\$\, \mathcal{D}_{\mathbb{Z},s}^{m\times nk}$	$\mathbf{R} \hookleftarrow\$\, \mathcal{D}_{\mathbb{Z},s}^{m\times nk}$	$\mathbf{R} \hookleftarrow\$\, \mathcal{D}_{\mathbb{Z},s}^{m\times nk}$
$\mathbf{A}' := \mathbf{AR} + \mathbf{G}$	$\mathbf{A}' := \mathbf{AR} + \mathbf{G}$	$\mathbf{A}' := \mathbf{AR} + \mathbf{G}$
$\mathbf{T}'_\mathbf{A} \leftarrow \mathsf{DelTrap}(\mathbf{A}, \mathbf{T_A}, \mathbf{A}', s)$	$\tilde{\mathbf{R}} \leftarrow \mathcal{D}_{\mathbb{Z},s}^{m\times nk}$ conditionned to $\mathbf{A}\tilde{\mathbf{R}} = \mathbf{A}' - \mathbf{G}(= \mathbf{AR})$	$\mathbf{T}'_\mathbf{A} := \mathbf{R}$
return $(\mathbf{A}', \mathbf{T}'_\mathbf{A})$	$\mathbf{T}'_\mathbf{A} := \tilde{\mathbf{R}}$	**return** $(\mathbf{A}', \mathbf{T}'_\mathbf{A})$
	return $(\mathbf{A}', \mathbf{T}'_\mathbf{A})$	

We study the statistical distance between $\mathsf{Dist}_{\mathsf{KExt}}$ and Dist_1: Proposition 3 shows that if $s \geq \mathsf{r}_{nk,\epsilon}\sqrt{11\left(\mathsf{s}_1(\mathbf{T_A})^2 + 1\right)}$, then

$$\mathsf{SD}\Big(\mathsf{Dist}_{\mathsf{ModKExt}}(\mathbf{A}, \mathbf{T_A}, s), \mathsf{Dist}_1(\mathbf{A})\Big) \leq nk\gamma_{n,m,\epsilon}^{\mathsf{Sample}}\ . \tag{13}$$

We show that Dist_1 and $\mathsf{Dist}_{\mathsf{SimModKExt}}$ are equal: Dist_1 and $\mathsf{Dist}_{\mathsf{SimModKExt}}$ are equals because, for any $\mathbf{A}$, the two following probability distributions are equals

$$\{(\mathbf{AR}, \mathbf{R}) :\ \mathbf{R} \hookleftarrow\$\, \mathcal{D}_{\mathbb{Z},s}^{m\times nk}\}\ ,$$
$$\{(\mathbf{AR}, \mathbf{R}') :\ \mathbf{R} \hookleftarrow\$\, \mathcal{D}_{\mathbb{Z},s}^{m\times nk}, \mathbf{R}' \hookleftarrow\$\, \mathcal{D}_{\mathbb{Z},s}^{m\times nk} \text{ conditioned to } \mathbf{AR} = \mathbf{AR}'\}\ .$$

This equality comes from a general probability fact proved in Appendix A (Lemma 7).

We analyze when $s \geq \mathsf{r}_{nk,\epsilon}\sqrt{11\left(\mathsf{s}_1(\mathbf{T_A})^2 + 1\right)}$: Proposition 2, Corollary 1 and the condition $s \geq \sqrt{11}\mathsf{r}_{nk,\epsilon}\sqrt{\mathsf{s}_1(\mathsf{Binom})[m - nk, nk, 1/2]^2 + 1}$ show that

$$\Pr_{(\mathbf{A},\mathbf{T_A})\hookleftarrow\$\mathsf{Trap}(n,m,q)}\left[s \geq \mathsf{r}_{nk,\epsilon}\sqrt{11\left(\mathsf{s}_1(\mathbf{T_A})^2 + 1\right)}\right] \geq 1 - 2q^{-n}\ . \tag{14}$$

Conclusion: Using Equations (13), (14) and the equality $\mathsf{Dist}_1 = \mathsf{Dist}_{\mathsf{SimModKExt}}$, we can conclude that

$$\begin{aligned}&\Pr_{(\mathbf{A},\mathbf{T_A})\leftarrow\$\mathsf{Trap}(n,m,q)}\Big[\mathsf{SD}(\mathsf{Dist}_{\mathsf{SimModKExt}}(\mathbf{A}),\mathsf{Dist}_{\mathsf{ModKExt}}(\mathbf{A},\mathbf{T_A},s))\leq nk\gamma^{\mathsf{Sample}}_{n,m,\epsilon}\Big]\\&\geq 1-2q^{-n}\ .\end{aligned}$$

Proof of Proposition 5. The part of Proposition 3 about SampleD and Lemma 19 implies that, when

$$\begin{aligned}&\text{(i)}\quad \tilde{s}\geq\eta_\epsilon\left(\Lambda_q^\perp(\mathbf{A}\|\mathbf{A}')\right)\ ,\\&\text{(ii)}\quad (\mathbf{A}\|\mathbf{A}')\mathbb{Z}^{m+nk}=\mathbb{Z}^n\mod q\ ,\\&\text{(iii)}\quad \mathsf{s}_1\big(\mathbf{T}'_\mathbf{A}\big)\leq\mathsf{s}_1(\mathsf{Gauss})[m,nk,s]\quad\left(\Rightarrow\tilde{s}\geq\mathsf{r}_{nk,\epsilon}\sqrt{11\left(\mathsf{s}_1\big(\mathbf{T}'_\mathbf{A}\big)^2+1\right)}\right)\ ,\end{aligned}$$

we have

$$\mathsf{SD}\Big(\mathsf{Dist}_{\mathsf{Sign}}(\mathbf{A},\mathbf{A}',\mathbf{T}'_\mathbf{A},\tilde{s}),\mathcal{D}^{m+nk}_{\mathbb{Z},\tilde{s}}\Big)\leq\gamma^{\mathsf{Sample}}_{n,m+nk,\epsilon}+2\epsilon\ . \tag{15}$$

We now study these three conditions.

Study of the conditions (i), (ii)

Lemma 11 and Proposition 1 show that

$$\begin{aligned}&\underset{(\mathbf{A},\mathbf{A}')\leftarrow\$\mathbb{Z}_q^{n\times m}\times\mathbb{Z}_q^{n\times nk}}{Pr}\Big[s\geq\eta_\epsilon\left(\Lambda_q^\perp(\mathbf{A}\|\mathbf{A}')\right)\wedge(\mathbf{A}\|\mathbf{A}')\mathbb{Z}^{m+nk}=\mathbb{Z}^n\mod q\Big]\\&\geq 1-2q^{-n/4}\ .\end{aligned}$$

This implies, by a general probability fact, shown in additional appendix in Proposition 12, that

$$\begin{aligned}&Pr_{\mathbf{A}\leftarrow\$\mathbb{Z}_q^{n\times m}}\Big[Pr_{\mathbf{A}'\leftarrow\$\mathbb{Z}_q^{n\times nk}}\big[s\geq\eta_\epsilon(\Lambda_q^\perp(\mathbf{A}\|\mathbf{A}'))\\&\qquad\qquad\wedge(\mathbf{A}\|\mathbf{A}')\mathbb{Z}^{m+nk}=\mathbb{Z}^n\bmod q\big]\geq 1-\sqrt{2}q^{-n/8}\Big]\\&\geq 1-\sqrt{2}q^{-n/8}\ .\end{aligned}\tag{16}$$

Using the equation (16), the fact that the output $\mathbf{A}'$ of $\mathsf{Dist}_{\mathsf{KExt}}$ is uniform and Proposition 2, we have

$$\begin{aligned}&\underset{(\mathbf{A},\mathbf{T_A})\leftarrow\$\mathsf{Trap}(n,m,q)}{Pr}\Big[\underset{(\mathbf{A}',\mathbf{T}'_\mathbf{A})\leftarrow\$\mathsf{Dist}_{\mathsf{KExt}}(\mathbf{A},\mathbf{T_A},s)}{Pr}\big[\text{(i) and (ii) true}\big]\geq 1-\sqrt{2}q^{-n/8}\Big]\\&\geq 1-\left(\sqrt{2}q^{-n/8}+nkq^{-0.196n}\right)\ .\end{aligned}\tag{17}$$

Study of the condition (iii)

Lemma 19 (applied nk times) and Proposition 3 shows that if:

$$\begin{aligned}&\text{(a)}\quad s\geq\eta_\epsilon(\Lambda_q^\perp(\mathbf{A}))\text{,}\\&\text{(b)}\quad \mathbf{A}\mathbb{Z}^m=\mathbb{Z}^n\mod q\\&\text{(c)}\quad \mathsf{s}_1(\mathbf{T_A})\leq\mathsf{s}_1(\mathsf{Binom})[m-nk,nk,1/2]\quad\left(\Rightarrow s\geq\mathsf{r}_{nk,\epsilon}\sqrt{11\left(\mathsf{s}_1(\mathbf{T_A})^2+1\right)}\right)\ ,\end{aligned}$$

ten,

$$\mathsf{SD}\Big(\mathbf{T}'_{\mathbf{A}} : (\mathbf{A}', \mathbf{T}'_{\mathbf{A}}) \leftarrow \mathsf{Dist}_{\mathsf{KExt}}(\mathbf{A}, \mathbf{T}_{\mathbf{A}}, s), \mathcal{D}_{\mathbb{Z},s}^{m\times nk}\Big) \leq nk\left(2\epsilon + \gamma_{n,m,\epsilon}^{\mathsf{Sample}}\right) \ . \tag{18}$$

Moreover, Corollary 1 shows that

$$Pr_{\mathbf{R}\leftarrow\$\mathcal{D}_{\mathbb{Z},s}^{m\times nk}}\left[\mathsf{s}_1(\mathbf{R}) > \mathsf{s}_1(\mathsf{Gauss})[m, nk, s]\right] \leq 2q^{-n} \ . \tag{19}$$

Thus, Equations (18) and (19) implies that when $(\mathsf{a}), (\mathsf{b}), (\mathsf{c})$ are verified,

$$\begin{aligned} Pr_{(\mathbf{A}',\mathbf{T}'_{\mathbf{A}})\leftarrow\mathsf{Dist}_{\mathsf{KExt}}(\mathbf{A},\mathbf{T}_{\mathbf{A}},s)}\left[\mathsf{s}_1\left(\mathbf{T}'_{\mathbf{A}}\right) \leq \mathsf{s}_1(\mathsf{Gauss})[m, nk, s]\right] \\ \geq 1 - \left(2q^{-n} + nk(2\epsilon + \gamma_{n,m,\epsilon}^{\mathsf{Sample}})\right) \ . \end{aligned} \tag{20}$$

Finally, Proposition 1, Proposition 2, Lemma 11 and Corollary 1 show

$$\underset{(\mathbf{A},\mathbf{T}_{\mathbf{A}})\leftarrow\$\mathsf{Trap}(n,m,q)}{Pr}\left[(\mathsf{a}), (\mathsf{b}) \text{ and } (\mathsf{c}) \text{ true}\right] \geq 1 - \left(4q^{-n/4} + nkq^{-0.196n}\right) \ . \tag{21}$$

We thus have, by equations (20) and (21)

$$\begin{aligned} &\underset{(\mathbf{A},\mathbf{T}_{\mathbf{A}})\leftarrow\$\mathsf{Trap}(n,m,q)}{Pr}\Big[Pr_{(\mathbf{A}',\mathbf{T}'_{\mathbf{A}})\leftarrow\mathsf{Dist}_{\mathsf{KExt}}(\mathbf{A},\mathbf{T}_{\mathbf{A}},s)}\left[(\mathsf{iii}) \text{ true}\right] \\ &\qquad\qquad \geq 1 - \left(2q^{-n} + nk(2\epsilon + \gamma_{n,m,\epsilon}^{\mathsf{Sample}})\right)\Big] \\ &\geq 1 - \left(4q^{-n/4} + nkq^{-0.196n}\right) \ . \end{aligned} \tag{22}$$

Conclusion
We conclude, with equations (15), (17), (22) and with Proposition 2 that

$$\begin{aligned} &\underset{(\mathbf{A},\mathbf{T}_{\mathbf{A}})\leftarrow\mathsf{Trap}(n,m,q)}{Pr}\Bigg[\underset{(\mathbf{A}',\mathbf{T}'_{\mathbf{A}})\leftarrow\mathsf{Dist}_{\mathsf{KExt}}(\mathbf{A},\mathbf{T}_{\mathbf{A}})}{Pr}\left[\mathsf{SD}\Big(\mathsf{Dist}_{\mathsf{Sign}}(\mathbf{A}, \mathbf{A}', \mathbf{T}_{\mathbf{A}}, \tilde{s}), \mathcal{D}_{\mathbb{Z},\tilde{s}}^{m+nk}\Big) \leq \gamma_{n,m+nk,\epsilon}^{\mathsf{Sample}} + 2\epsilon\right] \\ &\qquad\qquad \geq 1 - \left(2q^{-n} + nk(2\epsilon + \gamma_{n,m,\epsilon}^{\mathsf{Sample}}) + \sqrt{2}q^{-n/8}\right)\Bigg] \\ &\geq 1 - \left(2nkq^{-0.196n} + 4q^{-n/4} + \sqrt{2}q^{-n/8}\right) \ . \end{aligned}$$

B.8 Links between lattices and $\mathcal{R}$-lattices

We will use the functions $\mathsf{Cf} : \mathcal{R}_q^{a\times b} \to \mathbb{Z}_q^{a\times db}$ and $\mathsf{Rot} : \mathcal{R}_q^{a\times b} \to \mathbb{Z}_q^{da\times db}$ defined in Section 3. We define the dual of an element $a = \sum_{i=0}^{d-1} a_i X^i \in \mathcal{R}$ as $a^* := a_0 + \sum_{i=1}^{d-1} a_{d-i} X^i$. The dual of a matrix $\mathbf{B} = (b_{i,j}) \in \mathcal{R}^{n\times m}$ is defined as $\mathbf{B}^* := (b_{j,i}^*) \in \mathcal{R}^{m\times n}$. We note that $(\mathbf{B}^*)^* = \mathbf{B}$ and $\left(\mathbf{B}^\top\right)^* = (\mathbf{B}^*)^\top$.

Proposition 14. Cf *and* Rot *are* $\mathbb{Z}$*-linear. Moreover, for all* $\mathbf{A} \in \mathcal{R}^{n\times m}, \mathbf{B} \in \mathcal{R}^{m\times l}$*, we have*

$$\mathsf{Cf}(\mathbf{AB})=\mathsf{Cf}(\mathbf{A})\,\mathsf{Rot}(\mathbf{B}) \quad \mathsf{Rot}(\mathbf{AB})=\mathsf{Rot}(\mathbf{A})\,\mathsf{Rot}(\mathbf{B}) \quad \mathsf{Rot}(\mathbf{A}^*)=\mathsf{Rot}(\mathbf{A})^\top \ .$$

Proof. The fact that Cf and Rot are $\mathbb{Z}$-linear is verified by direct computation.

First, a direct calculus shows that for each $a, b \in \mathcal{R}_q$ $\mathsf{Cf}(ab) = \mathsf{Cf}(a)\mathsf{Rot}(b)$. Then, for $1 \leq i \leq n$, the i$^{\text{th}}$ line of $\mathsf{Cf}(\mathbf{AB})$ is

$$\begin{aligned}\mathsf{Cf}\left(\sum_{j=1}^{m} a_{i,j}b_{j,1}, \ldots, \sum_{j=1}^{m} a_{i,j}b_{j,l}\right) &= \left(\sum_{j=1}^{m} \mathsf{Cf}(a_{i,j}b_{j,1}), \ldots, \sum_{j=1}^{m} \mathsf{Cf}(a_{i,j}b_{j,l})\right) , \\ &= \left(\sum_{j=1}^{m} \mathsf{Cf}(a_{i,j})\mathsf{Rot}(b_{j,1}), \ldots, \sum_{j=1}^{m} \mathsf{Cf}(a_{i,j})\mathsf{Rot}(b_{j,l})\right) , \\ &= \big(\mathsf{Cf}(a_{i,1})\|\ldots\|\mathsf{Cf}(a_{i,m})\big)\,\mathsf{Rot}(\mathbf{B}) \ ,\end{aligned}$$

which is equal to the i$^{\text{th}}$ line of $\mathsf{Cf}(\mathbf{A})\mathbf{B}$. The second equation in a direct consequence of the fact that, for $a, b \in \mathcal{R}$, $\mathsf{Rot}(ab) = \mathsf{Rot}(a)\mathsf{Rot}(b)$. To see that, we note that for $1 \leq i \leq d$ the i$^{\text{th}}$ lines of $\mathsf{Rot}(ab)$ and $\mathsf{Rot}(a)\mathsf{Rot}(b)$ are, by definition, respectively $\mathsf{Cf}(X^i ab)$ and $\mathsf{Cf}(X^i a)\mathsf{Rot}(b)$: they are thus equal by an application of the first equality of the proposition.

The third equation is a direct consequence of the fact that for all $a \in \mathcal{R}$, $\mathsf{Rot}(a^*) = \mathsf{Rot}(a)^\top$, and the definitions of Rot and the dual of a matrix in $\mathcal{R}$.

Proposition 15. *For $\mathbf{A} \in \mathcal{R}^{n\times m}$ and $\mathbf{B} \in \mathcal{R}^{m\times l}$, we have $\|\mathbf{AB}\| \leq \sqrt{d}\ \mathsf{s}_1(\mathbf{A})\,\|\mathbf{B}\|$.*

Proof. We note that $\|\mathsf{Cf}(\mathbf{A})\| = \|\mathbf{A}\|$, the norm being taken in their respective spaces. We note that $\|\mathsf{Rot}(\mathbf{B})\| = \sqrt{d}\|\mathbf{B}\|$. We also note that $\mathsf{Cf}(\mathbf{AB}) = \mathsf{Cf}(\mathbf{A})\,\mathsf{Rot}(\mathbf{B})$. Thus,

$$\begin{aligned}\|\mathbf{AB}\| = \|\mathsf{Cf}(\mathbf{AB})\| &= \|\mathsf{Cf}(\mathbf{A})\,\mathsf{Rot}(\mathbf{B})\| \leq \mathsf{s}_1(\mathsf{Cf}(\mathbf{A}))\,\|\,\mathsf{Rot}(\mathbf{B})\| \ , \\ &= \mathsf{s}_1(\mathbf{A})\,\|\,\mathsf{Rot}(\mathbf{B})\| \leq \sqrt{d}\,\mathsf{s}_1(\mathbf{A})\,\|\mathbf{B}\| \ .\end{aligned}$$

Proposition 16. *For $\mathbf{A} \in \mathcal{R}^{n\times m}$, $\mathsf{s}_1(\mathsf{Rot}(\mathbf{A})) \leq \sqrt{d}\,\mathsf{s}_1(\mathbf{A})$*

Proof. For all $1 \leq i \leq d-1$, we have $\mathsf{s}_1\big(\mathsf{Cf}(X^i\mathbf{A})\big) = \mathsf{s}_1(\mathsf{Cf}(\mathbf{A}))$. Thus, for any $\mathbf{x} \in \mathcal{R}^{dm}$, we have,

$$\begin{aligned}\|\mathsf{Rot}(\mathbf{A})\mathbf{x}\| &= \left\|\Big(\mathsf{Cf}(\mathbf{A})\mathbf{x}, \mathsf{Cf}(X\mathbf{A})\mathbf{x}, \cdots, \mathsf{Cf}(X^{d-1}\mathbf{A})\mathbf{x}\Big)\right\| \\ &= \sqrt{\sum_{i=0}^{d-1} \|\mathsf{Cf}(X^i\mathbf{A})\mathbf{x}\|^2} \\ &\leq \sqrt{\sum_{i=0}^{d-1} \mathsf{s}_1(\mathsf{Cf}(X^i\mathbf{A}))^2\,\|\mathbf{x}\|^2} \\ &= \sqrt{d\,\mathsf{s}_1(\mathsf{Cf}(\mathbf{A}))^2\,\|\mathbf{x}\|^2} = \sqrt{d}\,\mathsf{s}_1(\mathsf{Cf}(\mathbf{A}))\,\|\mathbf{x}\|\end{aligned}$$

Proposition 17. *For $\mathbf{A} \in \mathcal{R}_q^{m\times n}, \mathbf{x} \in \mathcal{R}_q^n, \mathbf{u} \in \mathcal{R}_q^m$, we have*

$$\mathsf{Cf}\left(\Lambda^\top_{\mathbf{u},\mathcal{R},q}(\mathbf{A})\right) = \Lambda^\top_{\mathsf{Cf}(\mathbf{u})}\left(\mathsf{Rot}\left(\mathbf{A}^\top\right)^\top\right) \quad \mathsf{Cf}\left(\Lambda_{\mathcal{R},q}(\mathbf{A})\right) = \Lambda_q\left(\mathsf{Rot}\left(\mathbf{A}^\top\right)^\top\right) \ ,$$

$$\mathcal{D}_{\Lambda^\top_{\mathbf{u},\mathcal{R},q}(\mathbf{A})+\mathbf{x},s} = \mathsf{Cf}^{-1}\left(\mathcal{D}_{\Lambda^\top_{\mathsf{Cf}(\mathbf{u})}(\mathsf{Rot}(\mathbf{A}))+\mathsf{Cf}(\mathbf{x}),s}\right) \ .$$

Proof. We will need some properties about Rot and Cf that are shown in Appendix B.8, Proposition 14. The first equality is proved by

$$\begin{aligned}\mathbf{x} \in \Lambda^{\top}_{\mathbf{u},\mathcal{R}}(\mathbf{A}) \Leftrightarrow \mathbf{x}^{\top}\mathbf{A}^{\top} = \mathbf{u}^{\top} &\Leftrightarrow \mathsf{Cf}\left(\mathbf{x}^{\top}\mathbf{A}^{\top}\right) = \mathsf{Cf}(\mathbf{u}^{\top}) \\ &\Leftrightarrow \mathsf{Cf}(\mathbf{x}^{\top})\mathsf{Rot}(\mathbf{A}^{\top}) = \mathsf{Cf}(\mathbf{u}^{\top}) \\ &\Leftrightarrow \mathsf{Cf}(\mathbf{x}) \in \Lambda^{\top}_{\mathsf{Cf}(\mathbf{u})}\left(\mathsf{Rot}\left(\mathbf{A}^{\top}\right)^{\top}\right) \ .\end{aligned}$$

The second by

$$\begin{aligned}\mathbf{x} \in \Lambda_{\mathcal{R},q}(\mathbf{A}) &\Leftrightarrow \exists \mathbf{s} \colon \mathbf{x} = \mathbf{A}\mathbf{s} \\ &\Leftrightarrow \mathsf{Cf}(\mathbf{x}^{\top}) = \mathsf{Cf}\left(\mathbf{s}^{\top}\mathbf{A}^{\top}\right) \\ &\Leftrightarrow \mathsf{Cf}(\mathbf{x}^{\top}) = \mathsf{Cf}(\mathbf{s}^{\top})\mathsf{Rot}(\mathbf{A}^{\top}) \\ &\Leftrightarrow \mathsf{Cf}(\mathbf{x}) = \mathsf{Rot}(\mathbf{A}^{\top})^{\top}\mathsf{Cf}(\mathbf{s}) \\ &\Leftrightarrow \mathsf{Cf}(\mathbf{x}) \in \Lambda_q\left(\mathsf{Rot}\left(\mathbf{A}^{\top}\right)^{\top}\right) \ .\end{aligned}$$

The equality of probability distributions is a direct consequence of the first equality.

Corollary 4. *For all $\mathbf{B} \in \mathcal{R}^{n\times m}$, we have $q\,\mathsf{Cf}\left(\Lambda^{\perp}_{\mathcal{R},q}(\mathbf{B})\right)^{*} = \mathsf{Cf}\left(\Lambda_{\mathcal{R},q}(\mathbf{B}^{*})\right)$.*

Proof. We use Propositions 17 and 14 for

$$\begin{aligned}q\,\mathsf{Cf}\left(\Lambda^{\perp}_{\mathcal{R},q}(\mathbf{B})\right)^{*} &= q\left(\Lambda^{\perp}_{q}\left(\mathsf{Rot}\left(\mathbf{B}^{\top}\right)^{\top}\right)\right)^{*} \quad \text{by Proposition 17} \\ &= \Lambda_q\left(\mathsf{Rot}\left(\mathbf{B}^{\top}\right)\right) \ \text{ because for } \mathbf{A} \in \mathbb{Z}^{m\times n},\ q\left(\Lambda^{\perp}_{q}(\mathbf{A})\right)^{*} = \Lambda_q\left(\mathbf{A}^{\top}\right) \\ &= \Lambda_q\left(\mathsf{Rot}\left((\mathbf{B}^{*})^{\top}\right)^{\top}\right) \quad \text{by Proposition 14} \\ &= \mathsf{Cf}\left(\Lambda_{\mathcal{R},q}(\mathbf{B}^{*})\right) \quad \text{by Proposition 17.}\end{aligned}$$

B.9 Lattice trapdoors over $\mathcal{R}_q$

In this section we provide the definitions of the algorithms $\mathsf{Trap}_{\mathcal{R}}$,$\mathsf{DelTrap}_{\mathcal{R}}$ and $\mathsf{SampleD}_{\mathcal{R}}$ evoked in Section 4.3. We give the propositions and proofs relative to instantiations on rings, they are the equivalent (on structured lattices) of the ones presented in Section 4.3 on unstructured lattices. We will make an extensive use of the propositions of Appendix B.8 in order to pass from the unstructured to the structured case.

Let $\mathbf{g} = (1, 3, \ldots, 3^{k-1}) \in \mathcal{R}^{k}$ and $\mathbf{G} = [\mathsf{I}_n \ 3\mathsf{I}_n \ \ldots \ 3^{k-1}\mathsf{I}_n] \in \mathbb{Z}^{n\times nk}$. We recall that a $\mathbf{g}$-trapdoor of a matrix $\mathbf{A} \in \mathcal{R}_q^{1\times l}$ is a matrix $\mathbf{T_A} \in \mathcal{R}_q^{(l-k)\times k}$ such that $\mathsf{Rot}(\mathbf{T_A}) \in \mathbb{Z}_q^{d(l-k)\times dk}$ is a $\mathbf{G}$-trapdoor (defined in Section 4.3) of $\mathsf{Rot}(\mathbf{A}) \in \mathbb{Z}_q^{d\times dl}$. Equivalently, $\mathbf{A}\begin{pmatrix} -\mathbf{T_A} \\ \mathsf{I}_k \end{pmatrix} = \mathbf{g} \bmod q$.

Proposition 18 (Statistical instantiation of trapdoors (from [25, Section 5.2]), ring version). *Let $l > 2k$. We denote by $\mathsf{Trap}_{\mathcal{R}}(l, q)$ the algorithm that samples $\overline{\mathbf{A}} \hookleftarrow\$\ \mathcal{R}_q^{1\times(l-k)}$, $\mathbf{T_A} \hookleftarrow\$\ \mathcal{P}_{\mathcal{R},1/2}^{(l-k)\times k}$ and outputs the couple $\left(\mathbf{A} := \left[\overline{\mathbf{A}} \| \mathbf{g} - \overline{\mathbf{A}}\mathbf{T_A}\right], \mathbf{T_A}\right)$. Then, $\mathbf{T_A}$ is a $\mathbf{g}$-trapdoor of $\mathbf{A}$, and $\mathbf{A}$ has a probability distribution with statistical distance at most $kq^{-0.196d} = \mathsf{negl}(d)$ from uniform distribution.*

Proof. A direct computation shows that $\mathbf{T_A}$ is a $\mathbf{G}$-trapdoor of $\mathbf{A}$. The statistical distance upper bound comes from Proposition 1.

Proposition 19 ([25], Ring version). *Let $l, k \in \mathbb{N}^*$, $q = 3^k$, $l > 2k$. Let $0 < \epsilon < 1/2$. We consider $\mathbf{g} = (1, 3, \cdots, 3^{k-1})$ as an element of $\mathcal{R}_q^k$. There exists algorithms $\mathsf{DelTrap}_{\mathcal{R}}, \mathsf{SampleD}_{\mathcal{R}}$ such that, for $\mathbf{A} \in \mathcal{R}_q^{1\times l}$, $\mathbf{T_A} \in \mathcal{R}_q^{(l-k\times k)}$ a $\mathbf{g}$-trapdoor and $s \geq \mathsf{r}_{dk,\epsilon}\sqrt{11\left(d\,\mathsf{s}_1(\mathbf{T_A})^2+1\right)}$, we have:*

- $\mathsf{SampleD}_{\mathcal{R}}(\mathbf{A}, \mathbf{u}, \mathbf{T_A}, s)$ *returns $\mathbf{z} \in \mathcal{R}_q^k$ such that $\mathbf{Az} = \mathbf{u}$ and the statistical distance between the probability distribution of $\mathbf{z}$ and $\mathcal{D}_{\Lambda^\top_{\mathcal{R},q,\mathbf{u}}(\mathbf{A}),s}$ is upper bounded by the function*[7] $\gamma^{\mathsf{Sample}}_{d,dl,\epsilon}$ *which is negligible if ϵ is.*
- $\mathsf{DelTrap}(\mathbf{A} \in \mathcal{R}^{1\times l}, \mathbf{T_A} \in \mathcal{R}^{(l-k)\times k}, \mathbf{A}' \in \mathcal{R}^{1\times k}, s)$ *returns a $\mathbf{g}$-trapdoor of $[\mathbf{A}\|\mathbf{A}']$ (the output $\mathbf{T}'_\mathbf{A} \in \mathcal{R}^{l\times k}$ satisfies $\mathbf{AT}'_\mathbf{A} = \mathbf{A}' - \mathbf{g}$). Moreover, the probability distribution of the output $\mathbf{T}'_\mathbf{A}$ is at statistical distance less than $k\gamma^{\mathsf{Sample}}_{d,dl,\epsilon}$ of the distribution $\mathcal{D}^{l\times k}_{\mathcal{R},s}$ with output $\mathbf{R}$ conditioned to $\mathbf{AR} = \mathbf{A}' - \mathbf{g}$. More precisely, with notation $\mathbf{A}' - \mathbf{g} = (\mathbf{u}_1, \mathbf{u}_2, \cdots, \mathbf{u}_k) \in \mathcal{R}^k$, the i^{th} column of $\mathbf{T}'_\mathbf{A}$ is computed as $\mathsf{SampleD}(\mathbf{A}, \mathbf{u}_i, \mathbf{T_A}, s)$.*

Proof. We apply Proposition 3 to $\mathsf{Rot}(\mathbf{A})$ with the help of the results of Section B.8. For example, we use the bound $\mathsf{s}_1(\mathsf{Rot}(\mathbf{T_A})) \leq \sqrt{d}\mathsf{s}_1(\mathbf{A})$ of Proposition 16 and the proposition 17 is used to see that

$$\mathcal{D}_{\Lambda^\top_{\mathbf{u},\mathcal{R},q}(\mathbf{A}),s} = \mathsf{Cf}^{-1}\left(\mathcal{D}_{\Lambda^\top_{\mathsf{Cf}(\mathbf{u})}(\mathsf{Rot}(\mathbf{A})),s}\right) .$$

Lemma 20. *Let $l \in \mathbb{N}^*$, $q \in \mathbb{N}^*$, $0 < \epsilon < 1/2, s > 0$ and $\mathbf{A} \in \mathcal{R}_q^{1\times l}$. If $\mathbf{A}\mathcal{R}_q^l = \mathcal{R}_q$ Then, the two following probability distributions are equals*

$$\mathsf{Dist}_1 : \mathbf{z} \hookleftarrow\$\, \mathcal{D}_{\Lambda^\perp_{\mathcal{R},q}(\mathbf{A})+\mathbf{x},s}, \mathbf{x} \hookleftarrow\$\, \mathcal{R}^l , \quad \mathsf{Dist}_2 : \mathbf{z} \hookleftarrow\$\, \mathcal{D}_{\Lambda^\perp_{\mathcal{R},\mathbf{u},q}(\mathbf{A}),s}, \mathbf{u} \hookleftarrow\$\, \mathcal{R} .$$

Moreover, if $s \geq \eta_\epsilon(\Lambda^\perp_{\mathcal{R},q}(\mathbf{A}))$, then $\mathsf{SD}\Big(\mathsf{Dist}_1, \mathcal{D}^l_{\mathcal{R},s}\Big) \leq 2\epsilon$

Proof. Similar to the demonstration of Lemma 19.

Proposition 20 (Simulation of delegation of trapdoors). *For $s > 0$, $\mathbf{A} \in \mathcal{R}^{1\times l}$ and $\mathbf{T_A} \in \mathcal{R}^{(l-k)\times k}$ a $\mathbf{g}$-trapdoor of $\mathbf{A}$. We define*

$$\mathsf{Dist}_{\mathcal{R},\mathsf{ModKExt}}(\mathbf{A}, \mathbf{T_A}, s) := \big\{(\mathbf{A}', \mathbf{T}'_\mathbf{A}) : \mathbf{R} \hookleftarrow\$\, \mathcal{D}^{l\times k}_{\mathcal{R},s},\ \mathbf{A}' := \mathbf{AR} + \mathbf{G} ,\ \mathbf{T}'_\mathbf{A} \leftarrow \mathsf{DelTrap}_{\mathcal{R}}\left(\mathbf{A}, \mathbf{T_A}, \mathbf{A}', s\right)\big\} ,$$

$$\mathsf{Dist}_{\mathcal{R},\mathsf{SimModKExt}}(\mathbf{A}, s) := \Big\{(\mathbf{A}', \mathbf{R}) : \mathbf{R} \hookleftarrow\$\, \mathcal{D}^{l\times k}_{\mathcal{R},s},\ \mathbf{A}' := \mathbf{AR} + \mathbf{g}\Big\} .$$

Then, if $s \geq \sqrt{11}\mathsf{r}_{dk,\epsilon}\sqrt{16d\mathsf{s}_1(\mathsf{Binom})[l-k, dk, 1/2]^2 + 1}$, we have

$$Pr_{(\mathbf{A},\mathbf{T_A})\leftarrow\mathsf{Trap}_{\mathcal{R}}(l,q)}\left[\mathsf{SD}(\mathsf{Dist}_{\mathcal{R},\mathsf{ModKExt}}(\mathbf{A}, \mathbf{T_A}), \mathsf{Dist}_{\mathcal{R},\mathsf{SimModKExt}}(\mathbf{A})) \leq dk\gamma^{\mathsf{Sample}}_{d,dl,\epsilon}\right] \geq 1 - 2q^{-d} .$$

Proof. We will use an intermediate probability distribution Dist_1.

$\mathsf{Dist}_{\mathcal{R},\mathsf{ModKExt}}(\mathbf{A}, \mathbf{T_A}, s)$	$\mathsf{Dist}_1(\mathbf{A})$	$\mathsf{Dist}_{\mathcal{R},\mathsf{SimModKExt}}(\mathbf{A})$
$\mathbf{R} \hookleftarrow\$\, \mathcal{D}^{l\times k}_{\mathcal{R},s}$	$\mathbf{R} \hookleftarrow\$\, \mathcal{D}^{l\times k}_{\mathcal{R},s}$	$\mathbf{R} \hookleftarrow\$\, \mathcal{D}^{l\times k}_{\mathcal{R},s}$
$\mathbf{A}' := \mathbf{AR} + \mathbf{G}$	$\mathbf{A}' := \mathbf{AR} + \mathbf{G}$	$\mathbf{A}' := \mathbf{AR} + \mathbf{G}$
$\mathbf{T}'_\mathbf{A} \leftarrow \mathsf{DelTrap}_{\mathcal{R}}(\mathbf{A}, \mathbf{T_A}, \mathbf{A}', s)$	$\tilde{\mathbf{R}} \leftarrow \mathcal{D}^{l\times k}_{\mathcal{R},s}$ condi:ionned to $\mathbf{A}\tilde{\mathbf{R}} = \mathbf{A}' - \mathbf{G}(= \mathbf{AR})$	$\mathbf{T}'_\mathbf{A} := \mathbf{R}$
return $(\mathbf{A}', \mathbf{T}'_\mathbf{A})$	$\mathbf{T}'_\mathbf{A} := \tilde{\mathbf{R}}$	**return** $(\mathbf{A}', \mathbf{T}'_\mathbf{A})$
	return $(\mathbf{A}', \mathbf{T}'_\mathbf{A})$	

[7] The same as in Proposition 3.

We study the statistical distance between $\mathsf{Dist}_{\mathcal{R},\mathsf{KExt}}$ and Dist_1: Proposition 3 shows that if $s \geq \mathsf{r}_{dk,\epsilon}\sqrt{11\left(d\mathsf{s}_1(\mathbf{T_A})^2+1\right)}$

$$\mathsf{SD}\Big(\mathsf{Dist}_{\mathcal{R},\mathsf{ModKExt}}(\mathbf{A},\mathbf{T_A},s),\mathsf{Dist}_1(\mathbf{A})\Big) \leq lk\gamma^{\mathsf{Sample}}_{d,dl,\epsilon} \ . \tag{23}$$

We show that Dist_1 and $\mathsf{Dist}_{\mathcal{R},\mathsf{SimModKExt}}$ are equal: Dist_1 and $\mathsf{Dist}_{\mathcal{R},\mathsf{SimModKExt}}$ are equals because, for any $\mathbf{A}$, the two following probability distributions are equals

$$\{(\mathbf{AR},\mathbf{R}) : \ \mathbf{R} \hookleftarrow\$\ \mathcal{D}^{l\times k}_{\mathcal{R},s}\}$$
$$\{(\mathbf{AR},\mathbf{R}') : \ \mathbf{R} \hookleftarrow\$\ \mathcal{D}^{l\times k}_{\mathcal{R},s}, \mathbf{R}' \hookleftarrow\$\ \mathcal{D}^{l\times k}_{\mathcal{R},s} \text{ conditioned to } \mathbf{AR}=\mathbf{AR}'\} \ .$$

This equality comes from a general probability fact proved in Appendix A (Lemma 7).

We analyze when $s \geq \mathsf{r}_{dk,\epsilon}\sqrt{11\left(\mathsf{s}_1(\mathbf{T_A})^2+1\right)}$: Proposition 18, Corollary 1 and the condition $s \geq \sqrt{11}\mathsf{r}_{dk,\epsilon}\sqrt{16d\mathsf{s}_1(\mathsf{Binom})[l-k,dk,1/2]^2+1}$ show that

$$\Pr_{(\mathbf{A},\mathbf{T_A})\hookleftarrow\$\mathsf{Trap}(l,q)}\left[s \geq \mathsf{r}_{dk,\epsilon}\sqrt{11\left(d\mathsf{s}_1(\mathbf{T_A})^2+1\right)}\right] \geq 1-2q^{-d} \ . \tag{24}$$

Conclusion: Using Equations (23), (24) and the equality $\mathsf{Dist}_1 = \mathsf{Dist}_{\mathcal{R},\mathsf{SimModKExt}}$, we can conclude that

$$\underset{(\mathbf{A},\mathbf{T_A})\hookleftarrow\$\mathsf{Trap}(l,q)}{Pr}\left[\mathsf{SD}(\mathsf{Dist}_{\mathcal{R},\mathsf{SimModKExt}}(\mathbf{A},s),\mathsf{Dist}_{\mathcal{R},\mathsf{ModKExt}}(\mathbf{A},\mathbf{T_A},s)) \leq dk\gamma^{\mathsf{Sample}}_{d,dl,\epsilon}\right] \geq 1-2q^{-d} \ .$$

Proposition 21. *For $s>0, \tilde{s}>0$, $\mathbf{A}\in\mathcal{R}^{1\times l}, \mathbf{A}'\in\mathcal{R}^{1\times k}$ and $\mathbf{T}'_{\mathbf{A}}\in\mathcal{R}^{l\times k}$ a $\mathbf{g}$-trapdoor of $[\mathbf{A}\|\mathbf{A}']$, We define*

$$\mathsf{Dist}_{\mathcal{R},\mathsf{KExt}}(\mathbf{A},\mathbf{T_A},s) := \left\{(\mathbf{A}',\mathbf{T}'_{\mathbf{A}}) : \ \mathbf{A}' \hookleftarrow\$\ \mathcal{R}^{l\times k}_q, \mathbf{T}'_{\mathbf{A}} \leftarrow \mathsf{DelTrap}_{\mathcal{R}}\left(\mathbf{A},\mathbf{T_A},\mathbf{A}',s\right)\right\}$$
$$\mathsf{Dist}_{\mathsf{Sign}}(\mathbf{A},\mathbf{A}',\mathbf{T}'_{\mathbf{A}},\tilde{s}) = \{\mathbf{z}\colon \mathbf{z}\leftarrow \mathsf{SampleD}_{\mathcal{R}}([\mathbf{A}\|\mathbf{A}'],\mathbf{u},\mathbf{T}'_{\mathbf{A}},\tilde{s}), \mathbf{u}\hookleftarrow\$\ \mathcal{R}^n_q\}$$
$$\nu_1 := k(2\epsilon+\gamma^{\mathsf{Sample}}_{d,dl,\epsilon}) + 3^{-d\frac{(2k-l)}{4}+\frac{3}{2}}$$
$$\nu_2 := 2kq^{-0.196d} + 3^{-d\frac{(2k-l)}{4}+3} = \mathsf{negl}(d) \ .$$

Then, for $s \geq \max\left(\sqrt{11}\mathsf{r}_{dk,\epsilon}\sqrt{16d\mathsf{s}_1(\mathsf{Binom})[l-k,dk,1/2]^2+1},\ 12\mathsf{r}_{dl,\epsilon}\right)$ and $\tilde{s} \geq \max\left(\sqrt{11}\mathsf{r}_{dk,\epsilon}\sqrt{d\mathsf{s}_1(\mathsf{Gauss})[l,dk,s]^2+1},\ 12\mathsf{r}_{d(l+k),\epsilon}\right)$, we have

$$\underset{(\mathbf{A},\mathbf{T_A})\hookleftarrow\$\mathsf{Trap}_{\mathcal{R}}(l,q)}{Pr}\Big[\underset{(\mathbf{A}',\mathbf{T}'_{\mathbf{A}})\hookleftarrow\$\mathsf{Dist}_{\mathcal{R},\mathsf{KExt}}(\mathbf{A})}{Pr}\left[\mathsf{SD}\Big(\mathsf{Dist}_{\mathsf{Sign}}(\mathbf{A},\mathbf{A}',\mathbf{T_A},\tilde{s}),\mathcal{D}^{d(l+k)}_{\mathcal{R},\tilde{s}}\Big) \leq \gamma^{\mathsf{Sample}}_{d,d(k+l)\epsilon}\right] \geq 1-\nu_1\Big] \geq 1-\nu_2 \ . \tag{25}$$

Proof. The part of Proposition 3 about $\mathsf{SampleD}_{\mathcal{R}}$ and the lemma 19 imply that, when

(i) $\tilde{s} \geq \eta_\epsilon\left(\Lambda^{\perp}_{\mathcal{R},q}(\mathbf{A}\|\mathbf{A}')\right)$,

(ii) $(\mathbf{A}\|\mathbf{A}')\mathcal{R}^{l+k} = \mathcal{R} \mod q$,

(iii) $\mathsf{s}_1\left(\mathbf{T}'_{\mathbf{A}}\right) \leq d\mathsf{s}_1(\mathsf{Gauss})[l,dk,s] \quad \left(\Rightarrow \tilde{s} \geq \mathsf{r}_{dk,\epsilon}\sqrt{11\left(d\mathsf{s}_1\left(\mathbf{T}'_{\mathbf{A}}\right)^2+1\right)}\right)$,

we have

$$\mathsf{SD}\Big(\mathsf{Dist}_{\mathcal{R},\mathsf{Sign}}(\mathbf{A},\mathbf{A}',\mathbf{T}_{\mathbf{A}},\tilde{s}),\mathcal{D}^{l+k}_{\mathcal{R},\tilde{s}}\Big) \leq \gamma^{\mathsf{Sample}}_{d,d(k+l)\epsilon} + 2\epsilon \ . \tag{26}$$

We now study these three conditions.

Study of the conditions (i), (ii) Lemma 12 and Proposition 1 show that

$$\begin{aligned} \underset{(\mathbf{A},\mathbf{A}')\leftarrow\$\mathcal{R}_q^{1\times l}\times\mathcal{R}_q^{1\times k}}{Pr}\Big[s \geq \eta_\epsilon\left(\Lambda^{\perp}_{\mathcal{R},q}(\mathbf{A}\|\mathbf{A}')\right) \wedge (\mathbf{A}\|\mathbf{A}')\mathcal{R}^{l+k} = \mathcal{R} \mod q\Big] &\geq 1 - 3 * 3^{-d\frac{(2k-l)}{2}} \\ &= 1 - 3^{-d\frac{(2k-l)}{2}+1} \ . \end{aligned}$$

This implies, by a general probability fact, shown in additional appendix in Proposition 12, that

$$\begin{aligned} &Pr_{\mathbf{A}\leftarrow\$\mathcal{R}_q^{1\times l}}\Big[Pr_{\mathbf{A}'\leftarrow\$\mathcal{R}_q^{1\times k}}\big[s \geq \eta_\epsilon(\Lambda^{\perp}_{\mathcal{R},q}(\mathbf{A}\|\mathbf{A}')) \\ &\qquad\qquad \wedge (\mathbf{A}\|\mathbf{A}')\mathcal{R}^{l+k} = \mathcal{R} \mod q\big] \geq 1 - 3^{-d\frac{(2k-l)}{4}+\frac{1}{2}}\Big] \\ &\geq 1 - 3^{-d\frac{(2k-l)}{4}+\frac{1}{2}} \ . \end{aligned} \tag{27}$$

Using the equation (27), the fact that the output $\mathbf{A}'$ of $\mathsf{Dist}_{\mathcal{R},\mathsf{KExt}}$ is uniform and Proposition 18, we have

$$\begin{aligned} &\underset{(\mathbf{A},\mathbf{T}_{\mathbf{A}})\leftarrow\$\mathsf{Trap}(n,m,q)}{Pr}\Big[\underset{(\mathbf{A}',\mathbf{T}'_{\mathbf{A}})\leftarrow\$\mathsf{Dist}_{\mathsf{KExt}}(\mathbf{A},\mathbf{T}_{\mathbf{A}},s)}{Pr}\big[\text{(i) and (ii) true}\big] \geq 1 - 3^{-d\frac{(2k-l)}{4}+\frac{1}{2}}\Big] \\ &\geq 1 - \left(3^{-d\frac{(2k-l)}{4}+\frac{1}{2}} + kq^{-0.196d}\right) \ . \end{aligned} \tag{28}$$

Study of the condition (iii)

Lemma 20 (applied k times) and Proposition 19 show that if

(a) $s \geq \eta_\epsilon(\Lambda^{\perp}_{\mathcal{R},q}(\mathbf{A}))$

(b) $\mathbf{A}\mathcal{R}^l = \mathcal{R} \mod q$

(c) $\mathsf{s}_1(\mathbf{T}_{\mathbf{A}}) \leq 4\mathsf{s}_1(\mathsf{Binom})[l-k,dk,1/2]\left(\Rightarrow s \geq \mathsf{r}_{dk,\epsilon}\sqrt{11\left(d\,\mathsf{s}_1(\mathbf{T}_{\mathbf{A}})^2+1\right)}\right)$,

then,

$$\mathsf{SD}\Big(\mathbf{T}'_{\mathbf{A}} \colon (\mathbf{A}',\mathbf{T}'_{\mathbf{A}}) \leftarrow \mathsf{Dist}_{\mathcal{R},\mathsf{KExt}}(\mathbf{A},\mathbf{T}_{\mathbf{A}},s),\mathcal{D}^{l\times k}_{\mathcal{R},s}\Big) \leq k\left(2\epsilon + \gamma^{\mathsf{Sample}}_{d,dl,\epsilon}\right) \ . \tag{29}$$

Moreover, Corollary 1 shows that

$$Pr_{\mathbf{R}\leftarrow\$\mathcal{D}^{l\times k}_{\mathcal{R},s}}\big[\mathsf{s}_1(\mathbf{R}) > \mathsf{s}_1(\mathsf{Gauss})[l,dk,s]\big] \leq 2q^{-d} \ . \tag{30}$$

Thus, Equations (29) and (30) implies that when (a), (b), (c) are verified,

$$\begin{aligned} Pr_{(\mathbf{A}',\mathbf{T}'_{\mathbf{A}})\leftarrow\mathsf{Dist}_{\mathcal{R},\mathsf{KExt}}(\mathbf{A},\mathbf{T}_{\mathbf{A}})}\big[\mathsf{s}_1(\mathbf{T}'_{\mathbf{A}}) \leq \mathsf{s}_1(\mathsf{Gauss})[l,dk,s]\big] \\ \geq 1 - \left(2q^{-d} + k(2\epsilon + \gamma^{\mathsf{Sample}}_{d,dl,\epsilon})\right) \ . \end{aligned} \tag{31}$$

Finally, Proposition 1 Proposition 18, Lemma 12 and Corollary 1 show

$$\underset{(\mathbf{A},\mathbf{T}_{\mathbf{A}})\leftarrow\$\mathsf{Trap}_{\mathcal{R}}(n,m,q)}{Pr}\big[(\mathsf{a}),(\mathsf{b}) \text{ and } (\mathsf{c}) \text{ true}\big] \geq 1 - \left(3q^{-d/4} + 3^{-d\frac{(2k-l)}{2}} + 2kq^{-0.196d}\right) \tag{32}$$

$$\geq 1 - \left(3^{-d\frac{(2k-l)}{2}+2} + 2kq^{-0.196d}\right) \tag{33}$$

We thus have, by equations (31) and (33)

$$\begin{aligned}
&\underset{(\mathbf{A},\mathbf{T_A})\leftarrow\$\mathsf{Trap}_{\mathcal{R}}(n,m,q)}{Pr} \Big[Pr_{(\mathbf{A}',\mathbf{T'_A})\leftarrow\mathsf{Dist}_{\mathcal{R},\mathsf{KExt}}(\mathbf{A},\mathbf{T_A},s)}\big[(\mathsf{iii})\ \text{true}\big] \\
&\qquad\qquad \geq 1-\Big(2q^{-d}+k(2\epsilon+\gamma^{\mathsf{Sample}}_{d,dl,\epsilon})\Big)\Big] \\
&\geq 1-\Big(3^{-d\frac{(2k-l)}{2}+2}+kq^{-0.196d}\Big)\ . \qquad (34)
\end{aligned}$$

Conclusion
We conclude, with equations (26), (28), (34) Proposition 18 and the fact that $2q^{-d}\leq 3^{-d\frac{(2k-l)}{4}}$,

$$\begin{aligned}
&\underset{(\mathbf{A},\mathbf{T_A})\leftarrow\mathsf{Trap}_{\mathcal{R}}(l,q)}{Pr}\Bigg[\underset{(\mathbf{A}',\mathbf{T'_A})\leftarrow\mathsf{Dist}_{\mathcal{R},\mathsf{KExt}}(\mathbf{A},\mathbf{T_A})}{Pr}\Big[\mathsf{SD}\Big(\mathsf{Dist}_{\mathcal{R},\mathsf{Sign}}(\mathbf{A},\mathbf{A}',\mathbf{T_A},\tilde{s}),\mathcal{D}^{l+k}_{\mathcal{R},\tilde{s}}\Big)\leq\gamma^{\mathsf{Sample}}_{d,d(k+l)\epsilon}+\epsilon\Big] \\
&\qquad\qquad \geq 1-\Big(k(2\epsilon+\gamma^{\mathsf{Sample}}_{d,dl,\epsilon})+3^{-d\frac{(2k-l)}{4}+\frac{3}{2}}\Big)\Bigg] \\
&\geq 1-\Big(2kq^{-0.196d}+3^{-d\frac{(2k-l)}{2}+2}+3^{-d\frac{(2k-l)}{4}+\frac{1}{2}}\Big) \\
&\geq 1-\Big(2kq^{-0.196d}+3^{-d\frac{(2k-l)}{4}+3}\Big)\ .
\end{aligned}$$

C Detailed games for the proof of Theorem 1 of Section 5

$\mathsf{G}_1(\mathcal{A})$

1 : $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}()$
2 : $\mathsf{cpt_C} := 0, \mathsf{cpt_S} := 0$
3 : $\mathsf{Hash_{id}} \leftarrow\!\!\$\ \mathsf{SetId}^{\{0,1\}^{\tau_{\mathsf{nonce}}} \times \mathsf{SetId}}$
4 : $\mathsf{Hash_{mess}} \leftarrow\!\!\$\ \mathsf{SetMess}^{\{0,1\}^{\tau_{\mathsf{nonce}}} \times \mathsf{SetMess}}$
5 : $\mathsf{NoncesSk} \leftarrow \varnothing, \mathsf{NoncesSign} \leftarrow \varnothing$
6 : $\mathsf{AskedSk} \leftarrow \varnothing, \mathsf{AskedSign} \leftarrow \varnothing, \mathsf{sAskedSign} \leftarrow \varnothing$
7 : $\mathsf{ORACLES} = \{\mathcal{O}_{\mathsf{Corrupt}}, \mathcal{O}_{\mathsf{Sign}}, |\mathsf{Hash_{id}}\rangle, |\mathsf{Hash_{mess}}\rangle\}$
8 : $(\tilde{\sigma}^* = (\mathbf{t}^*, s^*, \sigma^*), \mathsf{id}^*, \mu^*) \leftarrow \mathcal{A}^{\mathsf{ORACLES}}(\mathsf{mpk})$
9 : **if** $\mathsf{id}^* \in \mathsf{AskedSk}$
10 : $\quad \vee\, (\mathsf{id}^*, \mu^*) \in \mathsf{AskedSign}$ **then** // for EUF-CMA
11 : $\quad \vee\, (\mathsf{id}^*, \mu^*, \sigma^*) \in \mathsf{sAskedSign}$ **then** // for sEUF-CMA
12 : $\quad$ **return** 0
13 : $\mathsf{fail}_1 :=$ "$\exists (\mathbf{r}, \mathsf{id}) \in \mathsf{NoncesSk}$:
14 : $\quad \mathsf{Hash_{id}}(\mathbf{r}, \mathsf{id}) = \mathsf{Hash_{id}}(\mathbf{t}^*, \mathsf{id}^*)$"
15 : $\mathsf{fail}_2 :=$ "$\exists (\mathbf{t}, \mathsf{id}, \mathbf{s}, \mu) \in \mathsf{NoncesSign}$:
16 : $\quad (\mathbf{t}, \mathsf{id}, \mathbf{s}, \mu) \neq (\mathbf{t}^*, \mathsf{id}^*, \mathbf{s}^*, \mu^*)$
17 : $\quad \wedge\ \mathsf{Hash_{id}}(\mathbf{t}, \mathsf{id}) = \mathsf{Hash_{id}}(\mathbf{t}^*, \mathsf{id}^*)$
18 : $\quad \wedge\ \mathsf{Hash_{mess}}(\mathbf{s}, \mu) = \mathsf{Hash_{mess}}(\mathbf{s}^*, \mu^*)$"
19 : **if** $\mathsf{cpt_C} > Q_{\mathsf{Corr}} \vee \mathsf{cpt_S} > Q_{\mathsf{S}}$ **then**
20 : $\quad$ **return** 0
21 : **if** $\mathsf{fail}_1 \vee \mathsf{fail}_2$ **then**
22 : $\quad$ **return** 0
23 : **return** $\mathsf{Verify}\big(\mathsf{mpk}, \mathsf{Hash_{id}}(\mathbf{t}^*, \mathsf{id}^*),$
24 : $\qquad\qquad \mathsf{Hash_{mess}}(\mathbf{s}^*, \mu^*), \sigma^*\big)$

$\mathcal{O}_{\mathsf{Sign}}(\mathsf{id}, \mu)$

1 : $\mathsf{cpt_S} := \mathsf{cpt_S} + 1$
2 : $\mathbf{t} \leftarrow\!\!\$\ \{0,1\}^{\tau_{\mathsf{nonce}}}$
3 : $\mathbf{s} \leftarrow\!\!\$\ \{0,1\}^{\tau_{\mathsf{nonce}}}$
4 : $\tilde{\mathsf{id}} := \mathsf{Hash_{id}}(\mathbf{t}, \mathsf{id})$
5 : $\tilde{\mu} := \mathsf{Hash_{mess}}(\mathbf{s}, \mu)$
6 : $\mathsf{NoncesSign} := \mathsf{NoncesSign}$
7 : $\qquad\qquad \cup \{(\mathbf{t}, \mathsf{id}, \mathbf{s}, \mu)\}$
8 : $\mathsf{sk}_{\tilde{\mathsf{id}}, \tilde{\mu}} \leftarrow \mathsf{KeyExt}(\mathsf{msk}, \tilde{\mathsf{id}})$
9 : $\sigma_{\tilde{\mathsf{id}}, \tilde{\mu}} \leftarrow \mathsf{Sign}(\mathsf{sk}_{\tilde{\mathsf{id}}, \tilde{\mu}}, \tilde{\mu})$
10 : $\widetilde{\sigma}_{\mathsf{id}, \mu} = (\mathbf{t}, \mathbf{s}, \sigma_{\tilde{\mathsf{id}}, \tilde{\mu}})$
11 : $\quad$ // for EUF-CMA:
12 : $\mathsf{AskedSign} = \mathsf{AskedSign} \cup \{(\mathsf{id}, \mu)\}$
13 : $\quad$ // for sEUF-CMA:
14 : $\mathsf{sAskedSign} = \mathsf{sAskedSign} \cup \{(\mathsf{id}, \mu, \widetilde{\sigma}_{\mathsf{id}, \mu})\}$
15 : **return** $\widetilde{\sigma}_{\mathsf{id}, \mu}$

$\mathcal{O}_{\mathsf{Corrupt}}(\mathsf{id})$

1 : $\mathsf{AskedSk} = \mathsf{AskedSk} \cup \{\mathsf{id}\}$
2 : $\mathsf{cpt_C} := \mathsf{cpt_C} + 1$
3 : $\mathbf{r} \leftarrow\!\!\$\ \{0,1\}^{\tau_{\mathsf{nonce}}}$
4 : $\mathsf{NoncesSk} := \mathsf{NoncesSk} \cup \{(\mathbf{r}, \mathsf{id})\}$
5 : $\tilde{\mathsf{id}} := \mathsf{Hash_{id}}(\mathbf{r}, \mathsf{id})$
6 : $\mathsf{sk}_{\tilde{\mathsf{id}}} \leftarrow \mathsf{KeyExt}(\mathsf{msk}, \tilde{\mathsf{id}})$
7 : $\mathsf{sk_{id}} := (\mathbf{r}, \mathsf{sk}_{\tilde{\mathsf{id}}})$
8 : **return** $\mathsf{sk_{id}}$

Fig. 12. Game G_1 of proof of Theorem 1.

Union of $\mathsf{FindCol}_{\mathsf{Q}}\left(\tau_{\mathsf{nonce}}+\tau_{\mathsf{id}},\tau_{\mathsf{id}}\right)_{Q_{\mathsf{Hash}_{\mathsf{id}}}+Q_{\mathsf{Corr}}+Q_{\mathsf{S}}}$
and $\mathsf{FindCol}_{\mathsf{Q}}\left(\tau_{\mathsf{nonce}}+\tau_{\mathsf{mess}},\tau_{\mathsf{mess}}\right)_{Q_{\mathsf{Hash}_{\mathsf{mess}}}+Q_{\mathsf{S}}}$

$\mathsf{Hash}_{\mathsf{id}} \leftarrow\!\!\$\ \mathsf{SetId}^{\{0,1\}^{\tau_{\mathsf{nonce}}}\times\mathsf{SetId}}$
$\mathsf{Hash}_{\mathsf{mess}} \leftarrow\!\!\$\ \mathsf{SetMess}^{\{0,1\}^{\tau_{\mathsf{nonce}}}\times\mathsf{SetId}}$
$(u,v) \leftarrow \mathcal{B}^{|\mathsf{Hash}_{\mathsf{id}}\rangle,|\mathsf{Hash}_{\mathsf{mess}}\rangle}$
if $\mathsf{Hash}_{\mathsf{id}}(u)=\mathsf{Hash}_{\mathsf{id}}(v)$
  $\vee\ \mathsf{Hash}_{\mathsf{mess}}(u)=\mathsf{Hash}_{\mathsf{mess}}(v)$ **then**
  return 1
return 0

$\mathcal{B}()$

$\mathsf{Hash}_{\mathsf{mess}} \leftarrow\!\!\$\ \mathsf{SetMess}^{\{0,1\}^{\tau_{\mathsf{nonce}}}\times\mathsf{SetMess}}$
$\mathsf{mpk},\mathsf{msk} \leftarrow \mathsf{Setup}()$
$\mathsf{cpt}_{\mathsf{C}} := 0, \mathsf{cpt}_{\mathsf{S}} := 0$
$\mathsf{NoncesSk} \leftarrow \varnothing, \mathsf{NoncesSign} \leftarrow \varnothing$
$\mathsf{AskedSk} \leftarrow \varnothing, \mathsf{AskedSign} \leftarrow \varnothing, \mathsf{sAskedSign} \leftarrow \varnothing$
$\mathsf{ORACLES} = \{\mathcal{O}_{\mathsf{Corrupt}}, \mathcal{O}_{\mathsf{Sign}}, |\mathsf{Hash}_{\mathsf{id}}\rangle, |\mathsf{Hash}_{\mathsf{mess}}\rangle\}$
$(\tilde{\sigma}^* = (\mathbf{t}^*, s^*, \sigma^*), \mathsf{id}^*, \mu^*) \leftarrow \mathcal{A}^{\mathsf{ORACLES}}(\mathsf{mpk})$
  // Any classical or quantum query to $\mathsf{Hash}_{\mathsf{id}}$ or $\mathsf{Hash}_{\mathsf{mess}}$
  // is made by $\mathcal{B}$ for $\mathcal{A}$
if $\mathsf{id}^* \in \mathsf{AskedSk}$
  $\vee\ (\mathsf{id}^*, \mu^*) \in \mathsf{AskedSign}$ **then** // for EUF-CMA
  $\vee\ (\mathsf{id}^*, \mu^*, \sigma^*) \in \mathsf{sAskedSign}$ **then** // for sEUF-CMA
  return 0
if $\mathsf{cpt}_{\mathsf{C}} > Q_{\mathsf{Corr}} \vee \mathsf{cpt}_{\mathsf{S}} > Q_{\mathsf{S}}$ **then**
  return 0
if $\exists(\mathbf{r},\mathsf{id}) \in \mathsf{NoncesSk}$ **such that**
    $\mathsf{Hash}_{\mathsf{id}}(\mathbf{r},\mathsf{id}) = \mathsf{Hash}_{\mathsf{id}}(\mathbf{t}^*,\mathsf{id}^*)$ **then**
  return $((\mathbf{r},\mathsf{id}),(\mathbf{t}^*,\mathsf{id}^*))$
if $\exists(\mathbf{t},\mathsf{id},\mathbf{s},\mu) \in \mathsf{NoncesSign}$ **such that**
    $(\mathbf{t},\mathsf{id},\mathbf{s},\mu) \neq (\mathbf{t}^*,\mathsf{id}^*,\mathbf{s}^*,\mu^*)$
    $\wedge\ \mathsf{Hash}_{\mathsf{id}}(\mathbf{t},\mathsf{id}) = \mathsf{Hash}_{\mathsf{id}}(\mathbf{t}^*,\mathsf{id}^*)$
    $\wedge\ \mathsf{Hash}_{\mathsf{mess}}(\mathbf{s},\mu) = \mathsf{Hash}_{\mathsf{mess}}(\mathbf{s}^*,\mu^*)$ **then**
  if $(\mathbf{t},\mathsf{id}) \neq (\mathbf{t}^*,\mathsf{id}^*)$ **then**
    return $((\mathbf{t},\mathsf{id}),(\mathbf{r}^*,\mathsf{id}^*))$
  else then
    return $((\mathbf{s},\mu),(\mathbf{s}^*,\mu^*))$
  return $\perp$

$\mathcal{O}_{\mathsf{Sign}}(\mathsf{id},\mu)$

$\mathsf{cpt}_{\mathsf{S}} := \mathsf{cpt}_{\mathsf{S}} + 1$
$\mathbf{t} \leftarrow\!\!\$\ \{0,1\}^{\tau_{\mathsf{nonce}}}$
$\mathbf{s} \leftarrow\!\!\$\ \{0,1\}^{\tau_{\mathsf{nonce}}}$
$\tilde{\mathsf{id}} := \mathsf{Hash}_{\mathsf{id}}(\mathbf{t},\mathsf{id})$
$\tilde{\mu} := \mathsf{Hash}_{\mathsf{mess}}(\mathbf{s},\mu)$
$\mathsf{NoncesSign} := \mathsf{NoncesSign} \cup \{(\mathbf{t},\mathsf{id},\mathbf{s},\mu)\}$
$\mathsf{sk}_{\tilde{\mathsf{id}},\tilde{\mu}} \leftarrow \mathsf{KeyExt}(\mathsf{msk},\tilde{\mathsf{id}})$
$\sigma_{\tilde{\mathsf{id}},\tilde{\mu}} \leftarrow \mathsf{Sign}(\mathsf{sk}_{\tilde{\mathsf{id}},\tilde{\mu}},\tilde{\mu})$
$\widetilde{\sigma}_{\mathsf{id},\mu} = (\mathbf{t},\mathbf{s},\sigma_{\tilde{\mathsf{id}},\tilde{\mu}})$
  // for EUF-CMA:
$\mathsf{AskedSign} = \mathsf{AskedSign} \cup \{(\mathsf{id},\mu)\}$
  // for sEUF-CMA:
$\mathsf{sAskedSign} = \mathsf{sAskedSign} \cup \{(\mathsf{id},\mu,\widetilde{\sigma}_{\mathsf{id},\mu})\}$
return $\widetilde{\sigma}_{\mathsf{id},\mu}$

$\mathcal{O}_{\mathsf{Corrupt}}(\mathsf{id})$

$\mathsf{AskedSk} = \mathsf{AskedSk} \cup \{\mathsf{id}\}$
$\mathsf{cpt}_{\mathsf{C}} := \mathsf{cpt}_{\mathsf{C}} + 1$
$\mathbf{r} \leftarrow\!\!\$\ \{0,1\}^{\tau_{\mathsf{nonce}}}$
$\mathsf{NoncesSk} := \mathsf{NoncesSk} \cup \{(\mathbf{r},\mathsf{id})\}$
$\tilde{\mathsf{id}} := \mathsf{Hash}_{\mathsf{id}}(\mathbf{r},\mathsf{id})$
$\mathsf{sk}_{\tilde{\mathsf{id}}} \leftarrow \mathsf{KeyExt}(\mathsf{msk},\tilde{\mathsf{id}})$
$\mathsf{sk}_{\mathsf{id}} := (\mathbf{r},\mathsf{sk}_{\tilde{\mathsf{id}}})$
return $\mathsf{sk}_{\mathsf{id}}$

Fig. 13. Reduction to the search of a collision for $\mathsf{Hash}_{\mathsf{id}}$ or $\mathsf{Hash}_{\mathsf{mess}}$, for proof of Theorem 1.

$\mathsf{G}_2(\mathcal{A})$

$(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(\lambda)$
$\mathsf{cpt}_\mathsf{C} := 0, \mathsf{cpt}_\mathsf{S} := 0$
$\mathsf{Hash}_{\mathsf{id}} \leftarrow\!\!\$\ \mathsf{SetId}^{\{0,1\}^{\tau_{\mathsf{nonce}}} \times \mathsf{SetId}}$
$\mathsf{Hash}_{\mathsf{mess}} \leftarrow\!\!\$\ \mathsf{SetMess}^{\{0,1\}^{\tau_{\mathsf{nonce}}} \times \mathsf{SetMess}}$
$\mathsf{NoncesSk} \leftarrow \varnothing, \mathsf{NoncesSign} \leftarrow \varnothing$
$\mathsf{AskedSk} \leftarrow \varnothing, \mathsf{AskedSign} \leftarrow \varnothing, \mathsf{sAskedSign} \leftarrow \varnothing$
$\mathsf{ORACLES} = \{\mathcal{O}_{\mathsf{Corrupt}}, \mathcal{O}_{\mathsf{Sign}}, |\mathsf{Hash}_{\mathsf{id}}\rangle, |\mathsf{Hash}_{\mathsf{mess}}\rangle\}$
$(\tilde{\sigma}^* = (\mathbf{t}^*, s^*, \sigma^*), \mathsf{id}^*, \mu^*) \leftarrow \mathcal{A}^{\mathsf{ORACLES}}(\mathsf{mpk})$
if $\mathsf{id}^* \in \mathsf{AskedSk}$
  $\vee\ (\mathsf{id}^*, \mu^*) \in \mathsf{AskedSign}$ **then** // for EUF-CMA
  $\vee\ (\mathsf{id}^*, \mu^*, \sigma^*) \in \mathsf{sAskedSign}$ **then** // for sEUF-CMA
  return 0
if $\mathsf{cpt}_\mathsf{C} > Q_{\mathsf{Corr}} \vee \mathsf{cpt}_\mathsf{S} > Q_\mathsf{S}$ **then**
  return 0
$\mathsf{fail}_1 :=$ "$\exists (\mathbf{r}, \mathsf{id}) \in \mathsf{NoncesSk}$:
    $\mathsf{Hash}_{\mathsf{id}}(\mathbf{r}, \mathsf{id}) = \mathsf{Hash}_{\mathsf{id}}(\mathbf{t}^*, \mathsf{id}^*)$"
$\mathsf{fail}_2 :=$ "$\exists (\mathbf{t}, \mathsf{id}, \mathbf{s}, \mu) \in \mathsf{NoncesSign}$:
    $(\mathbf{t}, \mathsf{id}, \mathbf{s}, \mu) \neq (\mathbf{t}^*, \mathsf{id}^*, \mathbf{s}^*, \mu^*)$
    $\wedge\ \mathsf{Hash}_{\mathsf{id}}(\mathbf{t}, \mathsf{id}) = \mathsf{Hash}_{\mathsf{id}}(\mathbf{t}^*, \mathsf{id}^*)$
    $\wedge\ \mathsf{Hash}_{\mathsf{mess}}(\mathbf{s}, \mu) = \mathsf{Hash}_{\mathsf{mess}}(\mathbf{s}^*, \mu^*)$"
if $\mathsf{fail}_1 \vee \mathsf{fail}_2$ **then**
  return 0
return $\mathsf{Verify}(\mathsf{mpk}, \mathsf{Hash}_{\mathsf{id}}(\mathbf{t}^*, \mathsf{id}^*), \mathsf{Hash}_{\mathsf{mess}}(\mathbf{s}^*, \mu^*), \sigma^*)$

// $\mathsf{ReprogramOracleOne}_1^{\mathsf{Cor}}$ and $\mathsf{ReprogramOracleOne}_1^{\mathsf{Sign}}(\mathsf{id})$
// correspond to the same reprogramming of H_1.
// It is more convenient to write it in
// two parts for next games.

$\mathsf{ReprogramOracleOne}_1^{\mathsf{Cor}}(\mathsf{id})$

$\mathbf{r} \leftarrow\!\!\$\ \{0,1\}^{\tau_{\mathsf{nonce}}}$
$\tilde{\mathsf{id}} \leftarrow\!\!\$\ \mathsf{SetId}$
$\mathsf{Hash}_{\mathsf{id}} := \mathsf{Hash}_{\mathsf{id}}^{(\mathbf{r}, \mathsf{id}) \to \tilde{\mathsf{id}}}$
return $\mathbf{r}$

$\mathsf{ReprogramOracleOne}_1^{\mathsf{Sign}}(\mathsf{id})$

$\mathbf{t} \leftarrow\!\!\$\ \{0,1\}^{\tau_{\mathsf{nonce}}}$
$\tilde{\mathsf{id}} \leftarrow\!\!\$\ \mathsf{SetId}$
$\mathsf{Hash}_{\mathsf{id}} := \mathsf{Hash}_{\mathsf{id}}^{(\mathbf{t}, \mathsf{id}) \to \tilde{\mathsf{id}}}$
return $\mathbf{t}$

$\mathsf{ReprogramOracleOne}_2(\mu)$

$\mathbf{s} \leftarrow\!\!\$\ \{0,1\}^{\tau_{\mathsf{nonce}}}$
$\tilde{\mu} \leftarrow\!\!\$\ \mathsf{SetMess}$
$\mathsf{Hash}_{\mathsf{mess}} := \mathsf{Hash}_{\mathsf{mess}}^{(\mathbf{s}, \mu) \to \tilde{\mu}}$
return $\mathbf{s}$

$\mathcal{O}_{\mathsf{Sign}}(\mathsf{id}, \mu)$

$\mathsf{cpt}_\mathsf{S} := \mathsf{cpt}_\mathsf{S} + 1$
$\mathbf{t} \leftarrow\!\!\$\ \mathsf{ReprogramOracleOne}_1^{\mathsf{Sign}}(\mathsf{id})$
$\mathbf{s} \leftarrow\!\!\$\ \mathsf{ReprogramOracleOne}_2(\mu)$
$\tilde{\mathsf{id}} := \mathsf{Hash}_{\mathsf{id}}(\mathbf{t}, \mathsf{id})$
$\tilde{\mu} := \mathsf{Hash}_{\mathsf{mess}}(\mathbf{s}, \mu)$
$\mathsf{NoncesSign} := \mathsf{NoncesSign} \cup \{(\mathbf{t}, \mathsf{id}, \mathbf{s}, \mu)\}$
$\mathsf{sk}_{\tilde{\mathsf{id}}, \tilde{\mu}} \leftarrow \mathsf{KeyExt}(\mathsf{msk}, \tilde{\mathsf{id}})$
$\sigma_{\tilde{\mathsf{id}}, \tilde{\mu}} \leftarrow \mathsf{Sign}(\mathsf{sk}_{\tilde{\mathsf{id}}, \tilde{\mu}}, \tilde{\mu})$
$\widetilde{\sigma}_{\mathsf{id}, \mu} = (\mathbf{t}, \mathbf{s}, \sigma_{\tilde{\mathsf{id}}, \tilde{\mu}})$
// for EUF-CMA:
$\mathsf{AskedSign} = \mathsf{AskedSign} \cup \{(\mathsf{id}, \mu)\}$
// for sEUF-CMA:
$\mathsf{sAskedSign} = \mathsf{sAskedSign} \cup \{(\mathsf{id}, \mu, \widetilde{\sigma}_{\mathsf{id}, \mu})\}$
return $\widetilde{\sigma}_{\mathsf{id}, \mu}$

$\mathcal{O}_{\mathsf{Corrupt}}(\mathsf{id})$

$\mathsf{AskedSk} = \mathsf{AskedSk} \cup \{\mathsf{id}\}$
$\mathsf{cpt}_\mathsf{C} := \mathsf{cpt}_\mathsf{C} + 1$
$\mathbf{r} \leftarrow\!\!\$\ \mathsf{ReprogramOracleOne}_1^{\mathsf{Cor}}(\mathsf{id})$
$\mathsf{NoncesSk} := \mathsf{NoncesSk} \cup \{(\mathbf{r}, \mathsf{id})\}$
$\tilde{\mathsf{id}} := \mathsf{Hash}_{\mathsf{id}}(\mathbf{r}, \mathsf{id})$
$\mathsf{sk}_{\tilde{\mathsf{id}}} \leftarrow \mathsf{KeyExt}(\mathsf{msk}, \tilde{\mathsf{id}})$
$\mathsf{sk}_{\mathsf{id}} := (\mathbf{r}, \mathsf{sk}_{\tilde{\mathsf{id}}})$
return $\mathsf{sk}_{\mathsf{id}}$

Fig. 14. Game G_2 of proof of Theorem 1.

$\mathsf{G}_3(\mathcal{A})$

1 : $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(\lambda)$
2 : $\mathsf{cpt_C} := 0, \mathsf{cpt_S} := 0$
3 : $\mathsf{Hash_{id}} \leftarrow\!\$\ \mathsf{SetId}^{\{0,1\}^{\tau_{\mathsf{nonce}}} \times \mathsf{SetId}}$
4 : $\mathsf{Hash_{mess}} \leftarrow\!\$\ \mathsf{SetMess}^{\{0,1\}^{\tau_{\mathsf{nonce}}} \times \mathsf{SetMess}}$
5 : **for** $i \in [\![1, Q_{\mathsf{Corr}}]\!]$ **then**
6 : $\quad \mathsf{id}_i^{\mathbf{r}} \leftarrow\!\$\ \mathsf{SetId}$
7 : $\quad \mathsf{sk}_i^{\mathbf{r}} \leftarrow \mathsf{KeyExt}(\mathsf{msk}, \mathsf{id}_i^{\mathbf{r}})$
8 : **for** $j \in [\![1, Q_{\mathsf{S}}]\!]$ **then**
9 : $\quad \mathsf{id}_j^{\mathbf{t}} \leftarrow\!\$\ \mathsf{SetId}$
10 : $\quad \mu_j^{\mathbf{s}} \leftarrow\!\$\ \mathsf{SetMess}$
11 : $\quad \mathsf{sk}_j^{\mathbf{t}} \leftarrow \mathsf{KeyExt}(\mathsf{msk}, \mathsf{id}_j^{\mathbf{t}})$
12 : $\quad \sigma_j^{\mathbf{s}} \leftarrow \mathsf{Sign}(\mathsf{mpk}, \mathsf{sk}_j^{\mathbf{t}}, \mu_j^{\mathbf{s}})$
13 : $\mathsf{NoncesSk} \leftarrow \varnothing, \mathsf{NoncesSign} \leftarrow \varnothing$
14 : $\mathsf{AskedSk} \leftarrow \varnothing, \mathsf{AskedSign} \leftarrow \varnothing, \mathsf{sAskedSign} \leftarrow \varnothing$
15 : $\mathsf{ORACLES} = \{\mathcal{O}_{\mathsf{Corrupt}}, \mathcal{O}_{\mathsf{Sign}}, |\mathsf{Hash_{id}}\rangle, |\mathsf{Hash_{mess}}\rangle\}$
16 : $(\tilde{\sigma}^* = (\mathbf{t}^*, s^*, \sigma^*), \mathsf{id}^*, \mu^*) \leftarrow \mathcal{A}^{\mathsf{ORACLES}}(\mathsf{mpk})$
17 : **if** $\mathsf{id}^* \in \mathsf{AskedSk}$
18 : $\quad \vee\ (\mathsf{id}^*, \mu^*) \in \mathsf{AskedSign}$ **then** // for EUF-CMA
19 : $\quad \vee\ (\mathsf{id}^*, \mu^*, \sigma^*) \in \mathsf{sAskedSign}$ **then** // for sEUF-CMA
20 : $\quad$ **return** 0
21 : **if** $\mathsf{cpt_C} > Q_{\mathsf{Corr}} \vee \mathsf{cpt_S} > Q_{\mathsf{S}}$ **then**
22 : $\quad$ **return** 0
23 : $\mathsf{fail}_1 :=$ "$\exists (\mathbf{r}, \mathsf{id}) \in \mathsf{NoncesSk}$:
24 : $\qquad \mathsf{Hash_{id}}(\mathbf{r}, \mathsf{id}) = \mathsf{Hash_{id}}(\mathbf{t}^*, \mathsf{id}^*)$"
25 : $\mathsf{fail}_2 :=$ "$\exists (\mathbf{t}, \mathsf{id}, \mathbf{s}, \mu) \in \mathsf{NoncesSign}$:
26 : $\qquad (\mathbf{t}, \mathsf{id}, \mathbf{s}, \mu) \neq (\mathbf{t}^*, \mathsf{id}^*, \mathbf{s}^*, \mu^*)$
27 : $\qquad \wedge\ \mathsf{Hash_{id}}(\mathbf{t}, \mathsf{id}) = \mathsf{Hash_{id}}(\mathbf{t}^*, \mathsf{id}^*)$
28 : $\qquad \wedge\ \mathsf{Hash_{mess}}(\mathbf{s}, \mu) = \mathsf{Hash_{mess}}(\mathbf{s}^*, \mu^*)$"
29 : **if** $\mathsf{fail}_1 \vee \mathsf{fail}_2$ **then**
30 : $\quad$ **return** 0
31 : **return** $\mathsf{Verify}(\mathsf{mpk}, \mathsf{Hash_{id}}(\mathbf{t}^*, \mathsf{id}^*), \mathsf{Hash_{mess}}(\mathbf{s}^*, \mu^*), \sigma^*)$

$\mathsf{ReprogramOracleOne}_1^{\mathsf{Cor}}(\mathsf{id})$

1 : $\mathbf{r} \leftarrow\!\$\ \{0,1\}^{\tau_{\mathsf{nonce}}}$
2 : $\tilde{\mathsf{id}} := \mathsf{id}_{\mathsf{cpt_C}}^{\mathbf{r}}$
3 : $\mathsf{Hash_{id}} := \mathsf{Hash_{id}}^{(\mathbf{r}, \mathsf{id}) \to \tilde{\mathsf{id}}}$
4 : **return** $\mathbf{r}$

$\mathsf{ReprogramOracleOne}_1^{\mathsf{Sign}}(\mathsf{id})$

1 : $\mathbf{t} \leftarrow\!\$\ \{0,1\}^{\tau_{\mathsf{nonce}}}$
2 : $\tilde{\mathsf{id}} := \mathsf{id}_{\mathsf{cpt_S}}^{\mathbf{t}}$
3 : $\mathsf{Hash_{id}} := \mathsf{Hash_{id}}^{(\mathbf{t}, \mathsf{id}) \to \tilde{\mathsf{id}}}$
4 : **return** $\mathbf{t}$

$\mathcal{O}_{\mathsf{Sign}}(\mathsf{id}, \mu)$

1 : $\mathsf{cpt_S} := \mathsf{cpt_S} + 1$
2 : $\mathbf{t} \leftarrow\!\$\ \mathsf{ReprogramOracleOne}_1^{\mathsf{Sign}}(\mathsf{id})$
3 : $\mathbf{s} \leftarrow\!\$\ \mathsf{ReprogramOracleOne}_2(\mu)$
4 : $\tilde{\mathsf{id}} := \mathsf{Hash_{id}}(\mathbf{t}, \mathsf{id})$
5 : $\tilde{\mu} := \mathsf{Hash_{mess}}(\mathbf{s}, \mu)$
6 : $\mathsf{NoncesSign} := \mathsf{NoncesSign}$
7 : $\qquad \cup \{(\mathbf{t}, \mathsf{id}, \mathbf{s}, \mu)\}$
8 : // We use the precomputed values
9 : $\widetilde{\sigma}_{\mathsf{id},\mu} = (\mathbf{t}, \mathbf{s}, \sigma_{\mathsf{cpt_S}}^{\mathbf{t}}, \mu_j^{\mathbf{s}})$
10 : // for EUF-CMA:
11 : $\mathsf{AskedSign} = \mathsf{AskedSign} \cup \{(\mathsf{id}, \mu)\}$
12 : // for sEUF-CMA:
13 : $\mathsf{sAskedSign} = \mathsf{sAskedSign} \cup \{(\mathsf{id}, \mu, \widetilde{\sigma}_{\mathsf{id},\mu})\}$
14 : **return** $\widetilde{\sigma}_{\mathsf{id},\mu}$

$\mathcal{O}_{\mathsf{Corrupt}}(\mathsf{id})$

1 : $\mathsf{AskedSk} = \mathsf{AskedSk} \cup \{\mathsf{id}\}$
2 : $\mathsf{cpt_C} := \mathsf{cpt_C} + 1$
3 : $\mathbf{r} \leftarrow\!\$\ \mathsf{ReprogramOracleOne}_1^{\mathsf{Cor}}(\mathsf{id})$
4 : $\mathsf{NoncesSk} := \mathsf{NoncesSk} \cup \{(\mathbf{r}, \mathsf{id})\}$
5 : $\tilde{\mathsf{id}} := \mathsf{Hash_{id}}(\mathbf{r}, \mathsf{id})$
6 : // We use the precomputed values
7 : $\mathsf{sk_{id}} := (\mathbf{r}, \mathsf{sk}_{\mathsf{cpt_C}}^{\mathbf{r}})$
8 : **return** $\mathsf{sk_{id}}$

$\mathsf{ReprogramOracleOne}_2(\mu)$

1 : $\mathbf{s} \leftarrow\!\$\ \{0,1\}^{\tau_{\mathsf{nonce}}}$
2 : $\tilde{\mu} := \mu_{\mathsf{cpt_S}}^{\mathbf{s}}$
3 : $\mathsf{Hash_{mess}} := \mathsf{Hash_{mess}}^{(\mathbf{s}, \mu) \to \tilde{\mu}}$
4 : **return** $\mathbf{s}$

Fig. 15. Game G_3 of proof of Theorem 1.

$\mathsf{EUFnaCMA}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}/\mathsf{sEUFnaCMA}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}\ (\mathcal{C}=(\mathcal{C}_1,\mathcal{C}_2))$

The game shown in Figure 1

$\mathcal{C}_1(\mathsf{mpk})$

for $i \in [\![1, Q_{\mathsf{Corr}}]\!]$ **then**
  $\mathsf{id}^{\mathbf{r}}_i \leftarrow\!\$\ \mathsf{SetId}$
$\mathsf{AskedSk} := \{\mathsf{id}^{\mathbf{r}}_i : i \in [\![1, Q_{\mathsf{Corr}}]\!]\}$
for $j \in [\![1, Q_{\mathsf{S}}]\!]$ **then**
  $\mathsf{id}^{\mathbf{t}}_j \leftarrow\!\$\ \mathsf{SetId}$
  $\mu^{\mathbf{s}}_j \leftarrow\!\$\ \mathsf{SetMess}$
$\mathsf{AskedSign} := \{(\mathsf{id}^{\mathbf{t}}_j, \mu^{\mathbf{s}}_j) : j \in [\![1, Q_{\mathsf{S}}]\!]\}$
$\mathsf{aux} := \varnothing$
return $(\mathsf{AskedSk}, \mathsf{AskedSign}, \mathsf{aux})$

$\mathcal{C}_2(\mathsf{mpk}, \mathsf{GivenSk}, \mathsf{GivenSign}, \mathsf{aux} = \varnothing)$

// We define:
// $\mathsf{GivenSk} = \{(\mathsf{id}^{\mathbf{r}}_i, \mathsf{sk}^{\mathbf{r}}_i) : i \in [\![1, Q_{\mathsf{Corr}}]\!]\}$
// $\mathsf{GivenSign} = \{(\mathsf{id}^{\mathbf{t}}_j, \mu^{\mathbf{s}}_j, \sigma^{\mathbf{s}}_j) : j \in [\![1, Q_{\mathsf{S}}]\!]\}$
$\mathsf{AskedSk} := \{\mathsf{id}^{x}_i : i \in [\![1, Q_{\mathsf{Corr}}]\!]\}$
$\mathsf{Hash}_{\mathsf{id}} \leftarrow\!\$\ \mathsf{SetId}^{\{0,1\}^{\tau_{\mathsf{nonce}}} \times \mathsf{SetId}}$
$\mathsf{Hash}_{\mathsf{mess}} \leftarrow\!\$\ \mathsf{SetMess}^{\{0,1\}^{\tau_{\mathsf{nonce}}} \times \mathsf{SetMess}}$
$\mathsf{cpt}_{\mathsf{C}} := 0, \mathsf{cpt}_{\mathsf{S}} := 0$
$\mathsf{NoncesSk} \leftarrow \varnothing, \mathsf{NoncesSign} \leftarrow \varnothing$
$\mathsf{AskedSk} \leftarrow \varnothing, \mathsf{AskedSign} \leftarrow \varnothing$
$\mathsf{ORACLES} = \{\mathcal{O}_{\mathsf{Corrupt}}, \mathcal{O}_{\mathsf{Sign}}, |\mathsf{Hash}_{\mathsf{id}}\rangle, |\mathsf{Hash}_{\mathsf{mess}}\rangle\}$
// Oracles are simulated by $\mathcal{C}_2$ in order to
// simulate the $\mathsf{GameSign}^{\mathsf{adapt}(\mathsf{IBS})}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}$ for $\mathcal{A}$
$(\tilde{\sigma}^* = (\mathbf{t}^*, s^*, \sigma^*), \mathsf{id}^*, \mu^*) \leftarrow \mathcal{A}^{\mathsf{ORACLES}}(\mathsf{mpk})$
if $\mathsf{id}^* \in \mathsf{AskedSk}$
  $\vee\ (\mathsf{id}^*, \mu^*) \in \mathsf{AskedSign}$ **then** // for EUF-CMA
  $\vee\ (\mathsf{id}^*, \mu^*, \sigma^*) \in \mathsf{GivenSign}$ **then** // for sEUF-CMA
  return 0
if $\mathsf{cpt}_{\mathsf{C}} > Q_{\mathsf{Corr}} \vee \mathsf{cpt}_{\mathsf{S}} > Q_{\mathsf{S}}$ **then**
  return 0
$\mathsf{fail}_1 :=$ "$\exists(\mathbf{r}, \mathsf{id}) \in \mathsf{NoncesSk} :$
    $\mathsf{Hash}_{\mathsf{id}}(\mathbf{r}, \mathsf{id}) = \mathsf{Hash}_{\mathsf{id}}(\mathbf{t}^*, \mathsf{id}^*)$"
$\mathsf{fail}_2 :=$ "$\exists(\mathbf{t}, \mathsf{id}, \mathbf{s}, \mu) \in \mathsf{NoncesSign} :$
    $(\mathbf{t}, \mathsf{id}, \mathbf{s}, \mu) \neq (\mathbf{t}^*, \mathsf{id}^*, \mathbf{s}^*, \mu^*)$
    $\wedge\ \mathsf{Hash}_{\mathsf{id}}(\mathbf{t}, \mathsf{id}) = \mathsf{Hash}_{\mathsf{id}}(\mathbf{t}^*, \mathsf{id}^*)$
    $\wedge\ \mathsf{Hash}_{\mathsf{mess}}(\mathbf{s}, \mu) = \mathsf{Hash}_{\mathsf{mess}}(\mathbf{s}^*, \mu^*)$"
if $\mathsf{fail}_1 \vee \mathsf{fail}_2$ **then**
  return 0
return $(\mathsf{Hash}_{\mathsf{id}}(\mathbf{t}^*, \mathsf{id}^*), \mathsf{Hash}_{\mathsf{mess}}(\mathbf{s}^*, \mu^*), \sigma^*)$

$\mathcal{O}_{\mathsf{Sign}}(\mathsf{id}, \mu)$

$\mathsf{AskedSign} = \mathsf{AskedSign} \cup \{(\mathsf{id}, \mu)\}$
$\mathsf{cpt}_{\mathsf{S}} := \mathsf{cpt}_{\mathsf{S}} + 1$
$\mathbf{t} \leftarrow\!\$\ \mathsf{ReprogramOracleOne}^{\mathsf{Sign}}_1(\mathsf{id})$
$\mathbf{s} \leftarrow\!\$\ \mathsf{ReprogramOracleOne}_2(\mu)$
$\tilde{\mathsf{id}} := \mathsf{Hash}_{\mathsf{id}}(\mathbf{t}, \mathsf{id})$
$\tilde{\mu} := \mathsf{Hash}_{\mathsf{mess}}(\mathbf{s}, \mu)$
$\mathsf{NoncesSign} := \mathsf{NoncesSign}$
  $\cup \{(\mathbf{t}, \mathsf{id}, \mathbf{s}, \mu)\}$
// We use the precomputed values
$\widetilde{\sigma}_{\mathsf{id},\mu} = (\mathbf{t}, \mathbf{s}, \sigma^{\mathbf{t}}_{\mathsf{cpt}_{\mathsf{S}}}, \mu^{\mathbf{s}}_j)$
return $\widetilde{\sigma}_{\mathsf{id},\mu}$

$\mathcal{O}_{\mathsf{Corrupt}}(\mathsf{id})$

$\mathsf{AskedSk} = \mathsf{AskedSk} \cup \{\mathsf{id}\}$
$\mathsf{cpt}_{\mathsf{C}} := \mathsf{cpt}_{\mathsf{C}} + 1$
$\mathbf{r} \leftarrow\!\$\ \mathsf{ReprogramOracleOne}^{\mathsf{Cor}}_1(\mathsf{id})$
$\mathsf{NoncesSk} := \mathsf{NoncesSk} \cup \{(\mathbf{r}, \mathsf{id})\}$
$\tilde{\mathsf{id}} := \mathsf{Hash}_{\mathsf{id}}(\mathbf{r}, \mathsf{id})$
// We use the precomputed values
$\mathsf{sk}_{\mathsf{id}} := (\mathbf{r}, \mathsf{sk}^{\mathbf{r}}_{\mathsf{cpt}_{\mathsf{C}}})$
return $\mathsf{sk}_{\mathsf{id}}$

$\mathsf{ReprogramOracleOne}_2(\mu)$

$\mathbf{s} \leftarrow\!\$\ \{0,1\}^{\tau_{\mathsf{nonce}}}$
$\tilde{\mu} := \mu^{\mathbf{s}}_{\mathsf{cpt}_{\mathsf{S}}}$
$\mathsf{Hash}_{\mathsf{mess}} := \mathsf{Hash}^{(\mathbf{s},\mu)\to\tilde{\mu}}_{\mathsf{mess}}$
return $\mathbf{s}$

$\mathsf{ReprogramOracleOne}^{\mathsf{Cor}}_1(\mathsf{id})$

$\mathbf{r} \leftarrow\!\$\ \{0,1\}^{\tau_{\mathsf{nonce}}}$
$\tilde{\mathsf{id}} := \mathsf{id}^{\mathbf{r}}_{\mathsf{cpt}_{\mathsf{C}}}$
$\mathsf{Hash}_{\mathsf{id}} := \mathsf{Hash}^{(\mathbf{r},\mathsf{id})\to\tilde{\mathsf{id}}}_{\mathsf{id}}$
return $\mathbf{r}$

$\mathsf{ReprogramOracleOne}^{\mathsf{Sign}}_1(\mathsf{id})$

$\mathbf{t} \leftarrow\!\$\ \{0,1\}^{\tau_{\mathsf{nonce}}}$
$\tilde{\mathsf{id}} := \mathsf{id}^{\mathbf{t}}_{\mathsf{cpt}_{\mathsf{S}}}$
$\mathsf{Hash}_{\mathsf{id}} := \mathsf{Hash}^{(\mathbf{t},\mathsf{id})\to\tilde{\mathsf{id}}}_{\mathsf{id}}$
return $\mathbf{t}$

Fig. 16. Reduction from G_3 to $\mathsf{GamenaSign}^{\mathsf{IBS}}_{Q_{\mathsf{Corr}},Q_{\mathsf{S}}}$ for proof of Theorem 1.

D Proofs of Section 6

D.1 Some intermediary results for the proof of Theorems 2 and 3

Lemma 21 (Adapted from [22, Lemma 4.2]). *Let $m, n, k \in \mathbb{N}^*, m \geq 2nk, q = 3^k,$. We have*

$$\Pr_{\mathbf{z} \leftarrow \$\{-1,0,1\}^m}\left[\Pr_{\bar{z}\{-1,0,1\}^m}[\bar{\mathbf{z}} = \mathbf{z} \mid \mathbf{A}\mathbf{z} = \mathbf{A}\bar{\mathbf{z}}] \leq \frac{1}{2}\right] \geq 1 - q^{-n} \ .$$

Proof. We first see that, for $\bar{\mathbf{z}} \in \{-1,0,1\}^m$ if $\exists \mathbf{z} \neq \bar{\mathbf{z}} \in \{-1,0,1\}^m$ such that $\mathbf{A}\mathbf{z} = \mathbf{A}\bar{\mathbf{z}}$, then $\Pr_{\bar{\mathbf{z}} \leftarrow \$\{-1,0,1\}^k}\left[\bar{\mathbf{z}} = \mathbf{z} \;\middle|\; \mathbf{A}\mathbf{z} = \mathbf{A}\bar{\mathbf{z}}\right] \leq \frac{1}{2}$. Consider $\mathbf{A}$ as a map $\mathbb{Z}_q^m \to \mathbb{Z}_q^n$. We want to find a bound of the number of $\mathbf{z}$ in $\{-1,0,1\}^m$ such that there is no other element in $\{-1,0,1\}^m$ with image $\mathbf{A}\mathbf{z} \in \mathbb{Z}_q^n$. In the worst case, $q^n - 1$ elements of $\{-1,0,1\}^m$ have this property and all the other elements have the same value through multiplication by $\mathbf{A}$. Thus,

$$\begin{aligned}
&\Pr_{\mathbf{z} \in \{-1,0,1\}}\left[\exists \mathbf{z}' \in \{-1,0,1\} : \ \mathbf{z}' \neq \mathbf{z} \wedge \mathbf{A}\mathbf{z} = \mathbf{A}\mathbf{z}' \mod q\right] \\
&\geq 1 - \frac{q^n - 1}{3^m} \geq 1 - 3^{kn-m} \geq 1 - q^{-n} \ ,
\end{aligned}$$

the later inequality using $m \geq 2nk$.

Lemma 22 (Structured version of Lemma 21). *Let $l, k \in \mathbb{N}^*, q = 3^k, l \geq 2k, \mathcal{R}_q = \mathbb{Z}_q/(X^d + 1), \mathbf{A} \in \mathcal{R}_q^{1 \times l}$. We have*

$$\Pr_{z \leftarrow \$\mathcal{S}_{\mathsf{R}}^l}\left[\Pr_{\bar{z} \leftarrow \$\mathcal{S}_{\mathsf{R}}^l}\left[\bar{z} = z \;\middle|\; \mathbf{A}z = \mathbf{A}\bar{z}\right] \leq \frac{1}{2}\right] \geq 1 - q^{-d} \ .$$

Proof. We first see that, for $\bar{\mathbf{z}} \in \mathcal{S}_{\mathsf{R}}^m$ if $\exists \mathbf{z} \neq \bar{\mathbf{z}} \in \mathcal{S}_{\mathsf{R}}^m$ such that $\mathbf{A}\mathbf{z} = \mathbf{A}\bar{\mathbf{z}}$, then we have $\Pr_{\bar{\mathbf{z}} \leftarrow \$\mathcal{S}_{\mathsf{R}}^l}\left[\bar{\mathbf{z}} = \mathbf{z} \;\middle|\; \mathbf{A}\mathbf{z} = \mathbf{A}\bar{\mathbf{z}}\right] \leq \frac{1}{2}$. Consider $\mathbf{A}$ as a map $\mathcal{R}_q^l \to \mathcal{R}_q$. We want to find a bound of the number of $\mathbf{z}$ in $\mathcal{S}_{\mathsf{R}}^l$ such that there is no other element in $\mathcal{S}_{\mathsf{R}}^l$ with image $\mathbf{A}\mathbf{z} \in \mathcal{R}_q$. In the worst case, $q^d - 1$ elements of $\mathcal{S}_{\mathsf{R}}^l$ have this property and all the other elements have the same value through multiplication by $\mathbf{A}$. Thus,

$$\begin{aligned}
&\Pr_{\mathbf{z} \in \{-1,0,1\}}\left[\exists \mathbf{z}' \in \mathcal{S}_{\mathsf{R}}^l : \ \mathbf{z}' \neq \mathbf{z} \wedge \mathbf{A}\mathbf{z} = \mathbf{A}\mathbf{z}' \mod q\right] \\
&\geq 1 - \frac{q^d - 1}{3^l} \geq 1 - 3^{kd-ld} \geq 1 - 3^{-kd} \ ,
\end{aligned}$$

the later inequality using $l \geq 2k$.

Corollary 5 (of Lemma 1). *Let $n, m, k, u \in \mathbb{N}^*$, $q = 3^k$, $m \geq 2nk$. Let $\epsilon \in]0, 1/2[$ and $s \in \mathbb{R}$ such that $s \geq 3\mathsf{r}_{m,\epsilon}$. Then,*

$$\Pr\left[\exists i \in [\![1,u]\!] : \ \mathsf{SD}\Big(\mathcal{D}_{s,(\mathbf{A}\|\mathbf{B}_i)}, \mathsf{U}\left(\mathbb{Z}_q^n\right)\Big) > 2\epsilon \ : \ \begin{smallmatrix}\mathbf{A} \leftarrow \$\mathbb{Z}_q^{n \times m} \\ \forall i \in [\![1,u]\!], \mathbf{B}_i \leftarrow \$\mathbb{Z}_q^{n \times l}\end{smallmatrix}\right] \leq 2uq^{-n/4} \ .$$

Let d a power of 2, $l \geq 2\log(q) + 1$ and $s \geq 12\mathsf{r}_{ld,\epsilon}$. Then,

$$\begin{aligned}
&\Pr\left[\exists i \in [\![1,u]\!] : \ \mathsf{SD}\Big(\mathcal{D}_{s,(\mathbf{A}\|\mathbf{B}_i)}, \mathsf{U}\left(\mathbb{Z}_q^n\right)\Big) > 2\epsilon \ : \ \begin{smallmatrix}\mathbf{A} \leftarrow \$\mathbb{Z}_q^{n \times m} \\ \forall i \in [\![1,u]\!], \mathbf{B}_i \leftarrow \$\mathbb{Z}_q^{n \times l}\end{smallmatrix}\right] \\
&\leq 2\,u\,3^{-d\frac{(2k-l)}{2}} \ .
\end{aligned}$$

Proof. The proofs of the two inequalities are similar. We prove the first one. Let μ the probability we want to bound. Let Bad the set of matrices $\mathbf{X} \in \mathbb{Z}_q^{n\times(m+l)}$ such that $\mathsf{SD}\Big(\mathcal{D}_{s,\mathbf{X}}, \mathsf{U}\left(\mathbb{Z}_q^n\right)\Big) > 2\epsilon$. We note that, by Lemma 1,

$$\Pr_{\mathbf{X}\in\mathbb{Z}_q^{n\times(m+k}}[\mathbf{X} \in \mathsf{Bad}] \leq 2q^{-n/4} \ . \tag{35}$$

Thus,

$$\begin{aligned}
\mu &= \Pr\Big[\exists i \in [\![1,u]\!](\mathbf{A}\|\mathbf{B}_i) \in \mathsf{Bad} \ : \ \substack{\mathbf{A}\leftarrow\$\mathbb{Z}_q^{n\times m} \\ \text{for } i\in[\![1,u]\!],\mathbf{B}_i\leftarrow\$\mathbb{Z}_q^{n\times l}}\Big] \\
&= q^{-nm} \sum_{\mathbf{A}\in\mathbb{Z}_q^{m\times n}} \Pr\Big[\exists i \in [\![1,u]\!](\mathbf{A}\|\mathbf{B}_i) \in \mathsf{Bad} \ : \ \text{for } i \in [\![1,u]\!], \mathbf{B}_i \leftarrow\$\ \mathbb{Z}_q^{n\times l}\Big] \\
&\leq u\, q^{-nm} \sum_{\mathbf{A}\in\mathbb{Z}_q^{m\times n}} \Pr\Big[(\mathbf{A}\|\mathbf{B}) \in \mathsf{Bad} \ : \ \mathbf{B} \leftarrow\$\ \mathbb{Z}_q^{n\times l}\Big] \\
&= u\ \Pr_{(\mathbf{A}\|\mathbf{B})\leftarrow\$\mathbb{Z}_q^{n\times(m+l)}}[(\mathbf{A}\|\mathbf{B}) \in \mathsf{Bad}] \leq 2uq^{-n/4} \quad \text{by equation (35).}
\end{aligned}$$

D.2 Detailed games for the proof of Theorem 2 of Section 6

$\mathsf{G}_0\ (\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2))$

1 : $(\mathbf{A}, \mathbf{T}_\mathbf{A}) \leftarrow \mathsf{Trap}(n, m, q)$
2 : $\mathsf{H}_1 \leftarrow\$\ \left(\mathbb{Z}_q^{n\times nk}\right)^{\mathsf{SetId}}$
3 : $\mathsf{H}_2 \leftarrow\$\ \left(\mathbb{Z}_q^{n}\right)^{\mathsf{SetId}\times\mathsf{SetMess}}$
4 : $(\mathsf{AskedSk}, \mathsf{AskedSign}, |\mathsf{aux}\rangle) \leftarrow \mathcal{A}_1(\mathbf{A})$
5 : **if** $|\mathsf{AskedSk}| > Q_{\mathsf{Corr}}$
6 : $\quad \vee\ |\mathsf{AskedSign}| > Q_\mathsf{S}$ **then**
7 : $\quad$ **return** 0
8 : **for** $\mathsf{id} \in \mathsf{AskedSk}$:
9 : $\quad \mathbf{T}_\mathsf{id} \leftarrow \mathsf{KeyExt}(\mathbf{A}, \mathbf{T}_\mathbf{A}, \mathsf{id})$
10 : **for** $(\mathsf{id}, \mu) \in \mathsf{AskedSign}$:
11 : $\quad \mathbf{T}_{\mathsf{id},\mu} \leftarrow \mathsf{KeyExt}(\mathbf{A}, \mathbf{T}_\mathbf{A}, \mathsf{id})$
12 : $\quad \mathbf{z}_{\mathsf{id},\mu} \leftarrow \mathsf{Sign}(\mathsf{id}, \mathbf{T}_{\mathsf{id},\mu}, \mu)$
13 : $\mathsf{GivenSk} := \{\mathbf{T}_\mathsf{id}, \mathsf{id} \in \mathsf{AskedSk}\}$
14 : $\mathsf{GivenSign} := \{\mathbf{z}_{\mathsf{id},\mu}, (\mathsf{id}, \mu) \in \mathsf{AskedSign}\}$
15 : $(\mathbf{z}^*, \mathsf{id}^*, \mu^*) \leftarrow \mathcal{A}_2^{|\mathsf{H}_1\rangle,|\mathsf{H}_2\rangle}(\mathbf{A}, \mathsf{GivenSk}, \mathsf{GivenSign}, |\mathsf{aux}\rangle)$
16 : **if** $\mathsf{id}^* \in \mathsf{AskedSk} \vee (\mathsf{id}^*, \mu^*) \in \mathsf{AskedSign}$ **then**
17 : $\quad$ **return** 0
18 : **return** $\mathsf{Verify}(\mathsf{id}^*, \mu^*, \mathbf{z}^*)$

$\mathsf{KeyExt}(\mathbf{A}, \mathbf{T}_\mathbf{A}, \mathsf{id})$

1 : $\mathbf{T}_\mathsf{id} \leftarrow\$\ \mathsf{DelTrap}\left(\mathbf{A}, \mathbf{T}_\mathbf{A}, \mathsf{H}_1(\mathsf{id}), s_\mathsf{id}\right)$
2 : **return** $\mathbf{T}_\mathsf{id}$

$\mathsf{Verify}(\mathsf{id}, \mu, \mathbf{z})$

1 : **if** $\mathbf{z} = 0$ **then**
2 : $\quad$ **return** 0
3 : **if** $(\mathbf{A}\|\mathsf{H}_1(\mathsf{id}))\,\mathbf{z} \neq \mathsf{H}_2(\mathsf{id}, \mu)$ **then**
4 : $\quad$ **return** 0
5 : $\quad$ // we write $\mathbf{z} = (\mathbf{z}_1, \mathbf{z}_2) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^{nk}$
6 : **return** $[\![\|\mathbf{z}_1\| \leq \mathsf{Bound}_1 \wedge \|\mathbf{z}_2\| \leq \mathsf{Bound}_2]\!]$

$\mathsf{Sign}(\mathsf{id}, \mathbf{T}_\mathsf{id}, \mu)$

1 : $\mathbf{u} := \mathsf{H}_2(\mathsf{id}, \mu)$
2 : $\mathbf{z} \leftarrow \mathsf{SampleD}\left((\mathbf{A}\|\mathsf{H}_1(\mathsf{id}))\,, \mathbf{T}_\mathsf{id}, \mathbf{u}, s_\mathsf{sign}\right)$
3 : **return** $\mathbf{z}$

Fig. 17. Game $\mathsf{G}_0 = \mathsf{EUFnaCMA}^{\mathsf{IBS}_\mathbb{Z}}_{Q_\mathsf{Corr},Q_\mathsf{S}}$, of proof of Theorem 2.

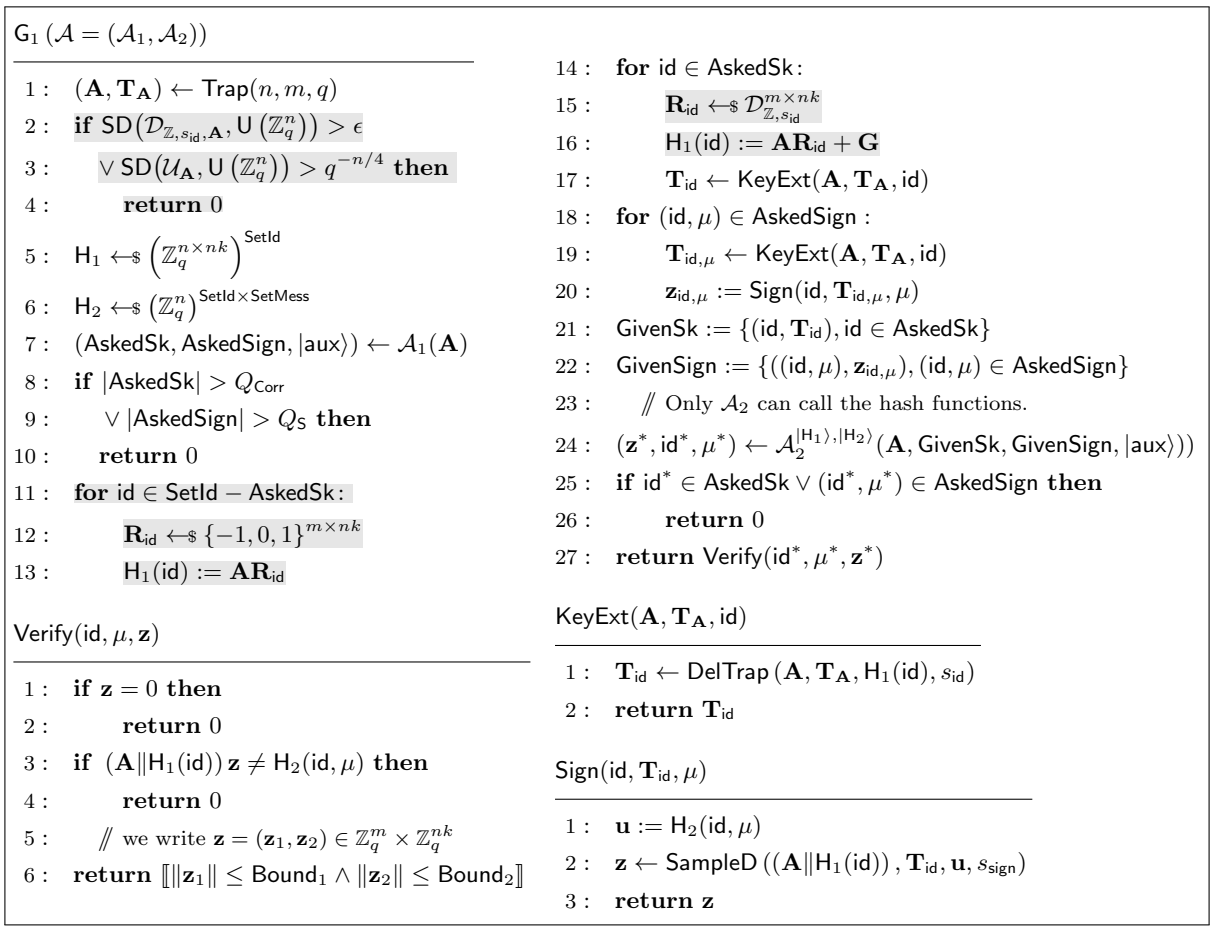

Fig. 18. Game G_1 of proof of Theorem 2.

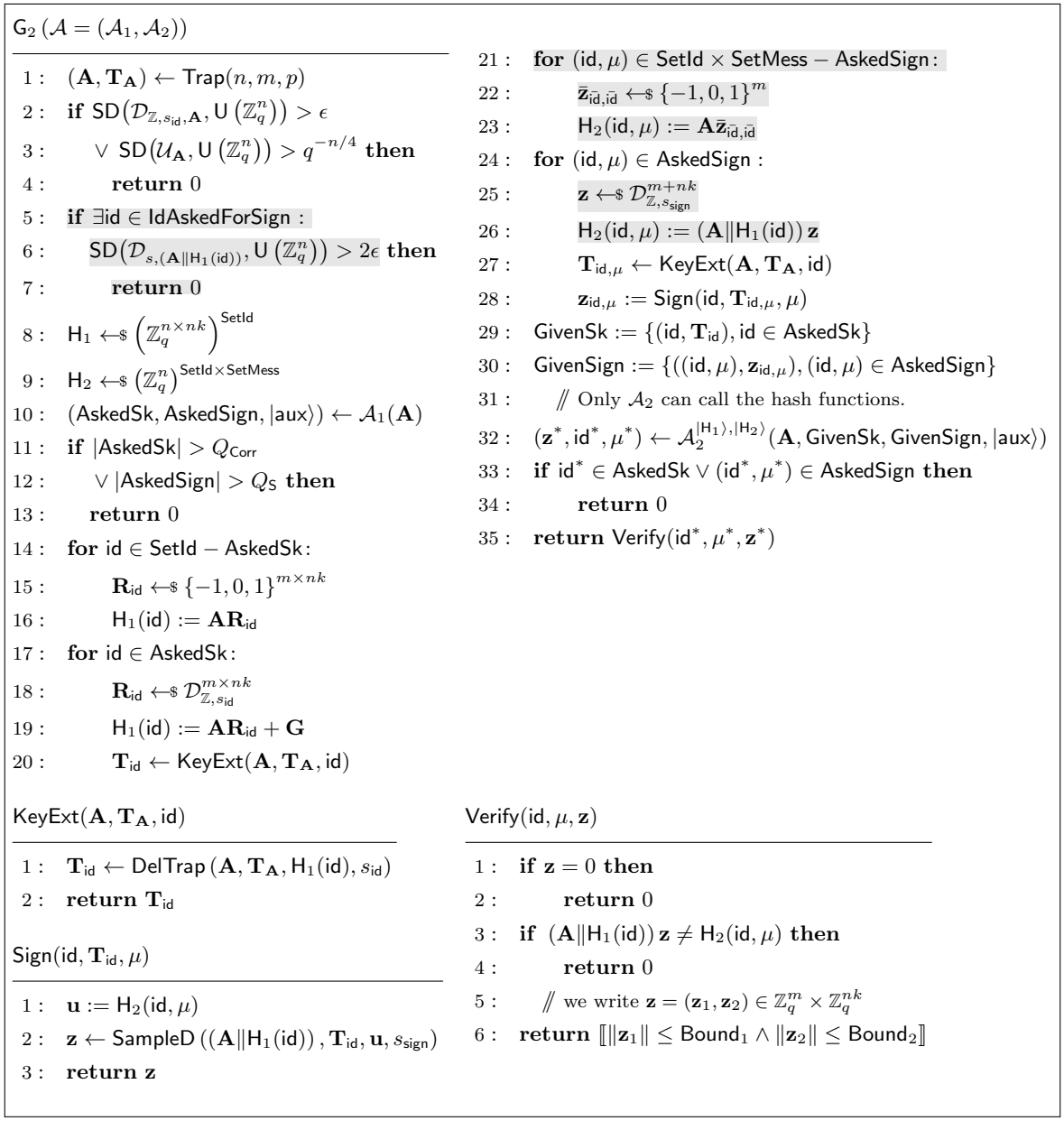

Fig. 19. Game G_2 of proof of Theorem 2.

$\mathsf{G}_3\,(\mathcal{A}=(\mathcal{A}_1,\mathcal{A}_2))$

$(\mathbf{A},\mathbf{T_A}) \leftarrow \mathsf{Trap}(n,m,p)$
if $\mathsf{SD}\big(\mathcal{D}_{\mathbb{Z},s_{\mathsf{id}},\mathbf{A}},\mathsf{U}\left(\mathbb{Z}_q^n\right)\big) > \epsilon$
  $\vee\ \mathsf{SD}\big(\mathcal{U}_{\mathbf{A}},\mathsf{U}\left(\mathbb{Z}_q^n\right)\big) > q^{-n/4}$ **then**
    return 0
if $\exists \mathsf{id} \in \mathsf{IdAskedForSign}$:
  $\mathsf{SD}\big(\mathcal{D}_{s,(\mathbf{A}\|\mathsf{H}_1(\mathsf{id}))},\mathsf{U}\left(\mathbb{Z}_q^n\right)\big) > 2\epsilon$ **then**
    return 0
$\mathsf{H}_1 \leftarrow\!\$ \left(\mathbb{Z}_q^{n\times nk}\right)^{\mathsf{SetId}}$
$\mathsf{H}_2 \leftarrow\!\$ \left(\mathbb{Z}_q^{n}\right)^{\mathsf{SetId}\times\mathsf{SetMess}}$
$(\mathsf{AskedSk},\mathsf{AskedSign},|\mathsf{aux}\rangle) \leftarrow \mathcal{A}_1(\mathbf{A})$
if $|\mathsf{AskedSk}| > Q_{\mathsf{Corr}}$
  $\vee\ |\mathsf{AskedSign}| > Q_{\mathsf{S}}$ **then**
  return 0
for $\mathsf{id} \in \mathsf{SetId} - \mathsf{AskedSk}$:
    $\mathbf{R}_{\mathsf{id}} \leftarrow\!\$ \{-1,0,1\}^{m\times nk}$
    $\mathsf{H}_1(\mathsf{id}) := \mathbf{A}\mathbf{R}_{\mathsf{id}}$
for $\mathsf{id} \in \mathsf{AskedSk}$:
    $\mathbf{R}_{\mathsf{id}} \leftarrow\!\$ \mathcal{D}^{m\times nk}_{\mathbb{Z},s_{\mathsf{id}}}$
    $\mathsf{H}_1(\mathsf{id}) := \mathbf{A}\mathbf{R}_{\mathsf{id}} + \mathbf{G}$
    $\mathbf{T}_{\mathsf{id}} := \mathbf{R}_{\mathsf{id}}$
  // note that KeyExt is not used here
for $(\mathsf{id},\mu) \in \mathsf{SetId}\times\mathsf{SetMess} - \mathsf{AskedSign}$:
    $\bar{\mathbf{z}}_{\bar{\mathsf{id}},\bar{\mathsf{id}}} \leftarrow\!\$ \{-1,0,1\}^m$
    $\mathsf{H}_2(\mathsf{id},\mu) := \mathbf{A}\bar{\mathbf{z}}_{\bar{\mathsf{id}},\bar{\mathsf{id}}}$
for $(\mathsf{id},\mu) \in \mathsf{AskedSign}$:
    $\mathbf{z} \leftarrow\!\$ \mathcal{D}^{m+nk}_{\mathbb{Z},s_{\mathsf{sign}}}$
    $\mathsf{H}_2(\mathsf{id},\mu) := (\mathbf{A}\|\mathsf{H}_1(\mathsf{id}))\,\mathbf{z}$
  // note that KeyExt is still used here
    $\mathbf{T}_{\mathsf{id},\mu} \leftarrow \mathsf{KeyExt}(\mathbf{A},\mathbf{T_A},\mathsf{id})$
    $\mathbf{z}_{\mathsf{id},\mu} := \mathsf{Sign}(\mathsf{id},\mathbf{T}_{\mathsf{id},\mu},\mu)$
$\mathsf{GivenSk} := \{(\mathsf{id},\mathbf{T}_{\mathsf{id}}),\mathsf{id} \in \mathsf{AskedSk}\}$
$\mathsf{GivenSign} := \{((\mathsf{id},\mu),\mathbf{z}_{\mathsf{id},\mu}),(\mathsf{id},\mu) \in \mathsf{AskedSign}\}$
  // Only $\mathcal{A}_2$ can call the hash functions.
$(\mathbf{z}^*,\mathsf{id}^*,\mu^*) \leftarrow \mathcal{A}_2^{|\mathsf{H}_1\rangle,|\mathsf{H}_2\rangle}(\mathbf{A},\mathsf{GivenSk},\mathsf{GivenSign},|\mathsf{aux}\rangle)$
if $\mathsf{id}^* \in \mathsf{AskedSk} \vee (\mathsf{id}^*,\mu^*) \in \mathsf{AskedSign}$ **then**
    return 0
return $\mathsf{Verify}(\mathsf{id}^*,\mu^*,\mathbf{z}^*)$

$\mathsf{Sign}(\mathsf{id},\mathbf{T}_{\mathsf{id}},\mu)$

$\mathbf{u} := \mathsf{H}_2(\mathsf{id},\mu)$
$\mathbf{z} \leftarrow \mathsf{SampleD}\left((\mathbf{A}\|\mathsf{H}_1(\mathsf{id}))\,,\mathbf{T}_{\mathsf{id}},\mathbf{u},s_{\mathsf{sign}}\right)$
return $\mathbf{z}$

$\mathsf{KeyExt}(\mathbf{A},\mathbf{T_A},\mathsf{id})$

$\mathbf{T}_{\mathsf{id}} \leftarrow \mathsf{DelTrap}\left(\mathbf{A},\mathbf{T_A},\mathsf{H}_1(\mathsf{id}),s_{\mathsf{id}}\right)$
return $\mathbf{T}_{\mathsf{id}}$

$\mathsf{Verify}(\mathsf{id},\mu,\mathbf{z})$

    return 0
if $(\mathbf{A}\|\mathsf{H}_1(\mathsf{id}))\,\mathbf{z} \neq \mathsf{H}_2(\mathsf{id},\mu)$ **then**
    return 0
  // we write $\mathbf{z} = (\mathbf{z}_1,\mathbf{z}_2) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^{nk}$
return $[\![\|\mathbf{z}_1\| \le \mathsf{Bound}_1 \wedge \|\mathbf{z}_2\| \le \mathsf{Bound}_2]\!]$

Fig. 20. Game G_3 of proof of Theorem 2..

$\mathsf{G}_4\,(\mathcal{A}=(\mathcal{A}_1,\mathcal{A}_2))$

$(\mathbf{A},\mathbf{T}_\mathbf{A}) \leftarrow \mathsf{Trap}(n,m,p)$
// note that $\mathbf{T}_\mathbf{A}$ won't be used
if $\mathsf{SD}\big(\mathcal{D}_{\mathbb{Z},s_{\mathsf{id}},\mathbf{A}},\mathsf{U}\left(\mathbb{Z}_q^n\right)\big) > \epsilon$
  $\vee\ \mathsf{SD}\big((\mathcal{U}_\mathbf{A}),\mathsf{U}\left(\mathbb{Z}_q^n\right)\big) > q^{-n/4}$ **then**
  return 0
if $\exists \mathsf{id} \in \mathsf{IdAskedForSign}$:
  $\mathsf{SD}\big(\mathcal{D}_{s,(\mathbf{A}\|\mathsf{H}_1(\mathsf{id}))},\mathsf{U}\left(\mathbb{Z}_q^n\right)\big) > 2\epsilon$ **then**
  return 0
$\mathsf{H}_1 \leftarrow\!\$ \left(\mathbb{Z}_q^{n\times nk}\right)^{\mathsf{SetId}}$
$\mathsf{H}_2 \leftarrow\!\$ \left(\mathbb{Z}_q^{n}\right)^{\mathsf{SetId}\times\mathsf{SetMess}}$
$(\mathsf{AskedSk},\mathsf{AskedSign},|\mathsf{aux}\rangle) \leftarrow \mathcal{A}_1(\mathbf{A})$
if $|\mathsf{AskedSk}| > Q_{\mathsf{Corr}}$
  $\vee\ |\mathsf{AskedSign}| > Q_\mathsf{S}$ **then**
  return 0
for $\mathsf{id} \in \mathsf{SetId} - \mathsf{AskedSk}$:
  $\mathbf{R}_\mathsf{id} \leftarrow\!\$ \{-1,0,1\}^{m\times nk}$
  $\mathsf{H}_1(\mathsf{id}) := \mathbf{A}\mathbf{R}_\mathsf{id}$
for $\mathsf{id} \in \mathsf{AskedSk}$:
  $\mathbf{R}_\mathsf{id} \leftarrow\!\$ \mathcal{D}_{\mathbb{Z},s_\mathsf{id}}^{m\times nk}$
  $\mathsf{H}_1(\mathsf{id}) := \mathbf{A}\mathbf{R}_\mathsf{id} + \mathbf{G}$
  $\mathbf{T}_\mathsf{id} := \mathbf{R}_\mathsf{id}$
// note that KeyExt is not used here
for $(\mathsf{id},\mu) \in \mathsf{SetId} \times \mathsf{SetMess} - \mathsf{AskedSign}$:
  $\bar{\mathbf{z}}_{\bar{\mathsf{id}},\bar{\mathsf{id}}} \leftarrow\!\$ \{-1,0,1\}^m$
  $\mathsf{H}_2(\mathsf{id},\mu) := \mathbf{A}\bar{\mathbf{z}}_{\bar{\mathsf{id}},\bar{\mathsf{id}}}$
for $(\mathsf{id},\mu) \in \mathsf{AskedSign}$:
  $\mathbf{z} \leftarrow\!\$ \mathcal{D}_{\mathbb{Z},s_{\mathsf{sign}}}^{m+nk}$
  $\mathsf{H}_2(\mathsf{id},\mu) := (\mathbf{A}\|\mathsf{H}_1(\mathsf{id}))\,\mathbf{z}$
  $\mathbf{z}_{\mathsf{id},\mu} := \mathbf{z}$
// note that KeyExt and Sign are not used here
$\mathsf{GivenSk} := \{(\mathsf{id},\mathbf{T}_\mathsf{id}), \mathsf{id} \in \mathsf{AskedSk}\}$
$\mathsf{GivenSign} := \{((\mathsf{id},\mu),\mathbf{z}_{\mathsf{id},\mu}), (\mathsf{id},\mu) \in \mathsf{AskedSign}\}$
// Only $\mathcal{A}_2$ can call the hash functions.
$(\mathbf{z}^*,\mathsf{id}^*,\mu^*) \leftarrow \mathcal{A}_2^{|\mathsf{H}_1\rangle,|\mathsf{H}_2\rangle}(\mathbf{A},\mathsf{GivenSk},\mathsf{GivenSign},|\mathsf{aux}\rangle)$
if $\mathsf{id}^* \in \mathsf{AskedSk} \vee (\mathsf{id}^*,\mu^*) \in \mathsf{AskedSign}$ **then**
  return 0
return $\mathsf{Verify}(\mathsf{id}^*,\mu^*,\mathbf{z}^*)$

$\mathsf{Verify}(\mathsf{id},\mu,\mathbf{z})$

return 0
if $(\mathbf{A}\|\mathsf{H}_1(\mathsf{id}))\,\mathbf{z} \neq \mathsf{H}_2(\mathsf{id},\mu)$ **then**
  return 0
// we write $\mathbf{z} = (\mathbf{z}_1,\mathbf{z}_2) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^{nk}$
return $[\![\|\mathbf{z}_1\| \le \mathsf{Bound}_1 \wedge \|\mathbf{z}_2\| \le \mathsf{Bound}_2]\!]$

// Sign and KeyExt are no more used

Fig. 21. Game G_4 of proof of Theorem 2.

$\mathsf{G}_5\,(\mathcal{A}=(\mathcal{A}_1,\mathcal{A}_2))$

$\mathbf{A} \leftarrow\!\$ \mathbb{Z}_q^{n\times m}$
There is no other changes.

Fig. 22. Game G_5 of proof of Theorem 2.

$\mathcal{B}(\mathbf{A})$

$\mathsf{H}_1 \leftarrow\$ \left(\mathbb{Z}_q^{n\times nk}\right)^{\mathsf{SetId}}$
$\mathsf{H}_2 \leftarrow\$ \left(\mathbb{Z}_q^{n}\right)^{\mathsf{SetId}\times\mathsf{SetMess}}$
$(\mathsf{AskedSk}, \mathsf{AskedSign}, |\mathsf{aux}\rangle) \leftarrow \mathcal{A}_1(\mathbf{A})$
if $|\mathsf{AskedSk}| > Q_{\mathsf{Corr}}$
  $\vee\ |\mathsf{AskedSign}| > Q_{\mathsf{S}}$ **then**
  return 0
for $\mathsf{id} \in \mathsf{SetId} - \mathsf{AskedSk}$:
  $\mathbf{R}_{\mathsf{id}} \leftarrow\$ \{-1,0,1\}^{m\times nk}$
  $\mathsf{H}_1(\mathsf{id}) := \mathbf{A}\mathbf{R}_{\mathsf{id}}$
for $\mathsf{id} \in \mathsf{AskedSk}$:
  $\mathbf{R}_{\mathsf{id}} \leftarrow\$ \mathcal{D}^{m\times nk}_{\mathbb{Z},s_{\mathsf{id}}}$
  $\mathsf{H}_1(\mathsf{id}) := \mathbf{A}\mathbf{R}_{\mathsf{id}} + \mathbf{G}$
  $\mathbf{T}_{\mathsf{id}} := \mathbf{R}_{\mathsf{id}}$
for $(\mathsf{id},\mu) \in \mathsf{SetId}\times\mathsf{SetMess} - \mathsf{AskedSign}$:
  $\bar{\mathbf{z}}_{\bar{\mathsf{id}},\bar{\mathsf{id}}} \leftarrow\$ \{-1,0,1\}^{m}$
  $\mathsf{H}_2(\mathsf{id},\mu) := \mathbf{A}\bar{\mathbf{z}}_{\bar{\mathsf{id}},\bar{\mathsf{id}}}$
for $(\mathsf{id},\mu) \in \mathsf{AskedSign}$:
  $\mathbf{z} \leftarrow\$ \mathcal{D}^{m+nk}_{\mathbb{Z},s_{\mathsf{sign}}}$
  $\mathsf{H}_2(\mathsf{id},\mu) := (\mathbf{A}\|\mathsf{H}_1(\mathsf{id}))\,\mathbf{z}$
  $\mathbf{z}_{\mathsf{id},\mu} := \mathbf{z}$
$\mathsf{GivenSk} := \{(\mathsf{id}, \mathbf{T}_{\mathsf{id}}), \mathsf{id} \in \mathsf{AskedSk}\}$
$\mathsf{GivenSign} := \{((\mathsf{id},\mu), \mathbf{z}_{\mathsf{id},\mu}), (\mathsf{id},\mu) \in \mathsf{AskedSign}\}$
$(\mathbf{z}^*, \mathsf{id}^*, \mu^*) \leftarrow \mathcal{A}^{|\mathsf{H}_1\rangle,|\mathsf{H}_2\rangle}(\mathbf{A}, \mathsf{GivenSk}, \mathsf{GivenSign}, |\mathsf{aux}\rangle)$
if $\mathsf{id}^* \in \mathsf{AskedSk} \vee (\mathsf{id}^*,\mu) \in \mathsf{AskedSign}$ **then**
  return 0
return $(\mathsf{I}_m\|\mathbf{R}_{\mathsf{id}^*})\,\mathbf{z}^* - \bar{\mathbf{z}}_{\mathsf{id}^*,\mu^*}$

$\mathsf{SIS}_{n,m,\mathsf{Bound}_{\mathsf{SIS}},q}(\mathcal{B})$

$\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n\times m}$
$\mathbf{u} \leftarrow \mathcal{B}(\mathbf{A})$
return $[\![0 < \|\mathbf{u}\| < \mathsf{Bound}_{\mathsf{SIS}} \wedge \mathbf{A}\mathbf{u} = 0]\!]$

Fig. 23. Reduction from G_5 to $\mathsf{SIS}_{n,m,\mathsf{Bound}_{\mathsf{SIS}},q}$ for proof of Theorem 2.

E Script for the computation of parameters of $\mathsf{IBS}_{\mathsf{NA},\mathcal{R}}$ and $\mathsf{IBS}^{+}_{\mathsf{NA},\mathsf{PW}}$

```
from math import *
# MSIS_security can be found in [10].
from MSIS_security import *

# we use the experimental approximation of C for Discrete
# Gaussians # and Uniforms in {-1,1} made in [13, Section 6.1]
CGaussUnif = 1 / (2*pi)
# we use the experimental approximation of C for P_{1/2}
# made in [13, Section 6.1]
CBinom = 1 / (4*pi)

# auxilliary functions
def f(m, n, C):
  return sqrt(m) + 2 * pi * C * (
      sqrt(n) + sqrt(m * log(3)))
def s1unif(n, m):
  return sqrt(2 / 3) * f(m, n, CGaussUnif)
def s1gauss(n, m, s):
  return (s / sqrt(2 * pi)) * f(m, n, CGaussUnif)
def s1binom(n, m):
  return sqrt(1 / 2) * f(m, n, CBinom)
def r(m, eps):
  return sqrt(log(2 * m * (1 + 1/eps)) / pi)
def compute_sid(k, d, l, eps):
  return max(
```

```
      sqrt(11) * r(d * k, eps) * 4 *
      sqrt(d * s1binom(l - k, d * k)**2 + 1),
      12 * r(d * l, eps))
def compute_ssign(k, d, l, eps, sid):
  return max(
      sqrt(11) * r(d * k, eps) *
      sqrt(d * s1gauss(l, d * k, sid)**2 + 1),
      12 * r(d * (l+k), eps))
  # s_PW is taken as sid :
  # it is smaller than if we took the formulae of
  # [26, Section 5.2].
  # and it simplifies our estimations
def compute_s_PW(k, d, l, eps):
  return compute_sid(k, d, l, eps)
def compute_sp_PW(k, d, l, eps, s_PW):
  return compute_ssign(k, d, l, eps, s_PW)
def compute_spp_PW(k, d, l, eps, sp_PW):
  return max(
      sqrt(11) * r(d * k, eps) *
      sqrt(d * s1gauss(l + k, d * k, sp_PW)**2 +
           1), 12 * r(d * (l + 2*k), eps))

class IBSParameterSet:
  # _PW : specific to IBSPW scheme ([26, Figure 8]))
  def __init__(self, k, d, l, eps):
    self.k = k # the modulus is equal to q=3^k
    self.d = d # Ring dimesion
    self.l = l # Dimension of A
    self.eps = eps # epsilon

    # Note that :
    # - IBSPW does not use the probability P_(1/2)
    #   but gaussian distribution # to create T_A
    # - (see their [26, Lemma 12]).
    #   The use of P_(1/2) led to smaller trapdoor
    #   and thus better # results : we use P_(1/2) for both,
    #   wich make a better standard deviation s for IBSPanWan.
    #   (see equations at [26, Section 5.2])
    # - We use our estimations of singular values of matrix
    #   for both IBSR and IBSPW because the ones
    #   of IBSPW included universal constants.
    self.sid = compute_sid(k, d, l, eps)
    self.ssign = compute_ssign(k, d, l, eps,
                               self.sid)
    # the standard deviations s, s', s''.
    self.s_PW = compute_s_PW(k, d, l, eps)
    self.sp_PW = compute_sp_PW(k, d, l, eps,
                               self.s_PW)
    self.spp_PW = compute_spp_PW(k, d, l, eps,
```

```
                                self.sp_PW)
# sProof_PW is our estimation of the standard
# deviation tilde{s}  they used for Hash reprogramming
# in the proof of [26, Theorem 4].
# We used Lemma 1 to
# estimate it (it gives a conditon on std such that
# A*(Discrete Gaussian(std)) is near
# the uniform distribution")
self.sProof_PW = 12 * r(d * l, eps)
self.signBoundI = sqrt(2 * d * l) * self.ssign
self.signBoundII = sqrt(
    2 * d * k) * self.ssign
# Bound of the solution, see (([26, Figure 8]
self.signBound_PW = sqrt(
    d * (l + 2*k)) * s1gauss(l, d * k,
                                self.spp_PW)
# RSIS Bound of IBSR,  from 3
self.RSISBound = self.signBoundI + 4 * sqrt(
    d) * s1unif(
        l, d * k) * self.signBoundII + sqrt(
            17 / 2) * sqrt(l * d)
# RSIS Bound of IBSPW, constructed by looking at the
# demonstration of [26, Theorem 4]),
self.RSISBound_PW = (
    1 + 2 * sqrt(d) *
    s1gauss(l, d * k, self.sProof_PW)
) * self.signBound_PW
# Creation of MSISParams for IBSR and IBSPan
#in order to use MSIS_summarize_attacks
self.MSISParams_PW = MSISParameterSet(
    d, l, 1, self.RSISBound_PW, 3**k, "l2")
self.MSISParams = MSISParameterSet(
    d, l, 1, self.RSISBound, 3**k, "l2")
self.size_sign = ceil(
    l * d * log(2 * self.signBoundI, 2) +
    k * d * log(2 * self.signBoundII, 2))
# With notation z=(z_1,z_2) we use the fact that
# by definition of the scheme (Figure 7)
# |sign_1|_infty \leq |sign_1|_2 \leq signBoundI
# |sign_2|_infty \leq |sign_2|_2 \leq signBoundII
# so they can be stored respectively modulo 2*signBoundI
# and 2*signBoundII
self.size_sign_PW = ceil(
    (l + 2*k) * d *
    log(min(2 * self.signBound_PW, 3**k), 2))
# We use the fact that
# by definition # ([26, Figure 8]):
# |sign|_infty \leq |sign|_2 \leq signBound_PW
# so it can be stored modulo min(2*signBound_PW, 3**k)
```

```
  self.size_pk = ceil(l * d * log(3**k, 2))
  self.size_sk = ceil((l-k) * k * d * log(3, 2))
  self.size_sk_id = ceil(
      (l+k) * k * d *
      log(sqrt(2 * d) * self.sid, 2))
  # We use the fact that the ouput is close to discrete
  # gaussian with standard deviation sid
  #(see for example Equation~(29))
  # and the tail inequality (Lemma~3) to each coordonate
  self.size_sk_id_naive = ceil(
      (l+k) * k * d * log(3**k, 2))

def secu(self):
  MSISsecu_PW = MSIS_summarize_attacks(
      self.MSISParams_PW)
  secu_PW = MSISsecu_PW[-2]
  # -1 because of the factor 2 in the reduction to RSIS
  print(
      "\nSecurity of IBSPW (cost with cost_svp): "
      + str(secu_PW - 1))
  MSISsecu = MSIS_summarize_attacks(
      self.MSISParams)
  secu = MSISsecu[-2]
  # -1 because of the factor 2 in the reduction to RSIS
  print(
      "\nSecurity of IBSR (cost with cost_svp): "
      + str(secu - 1))
  return secu

def print_params(self):
  txt = "k=" + str(self.k)
  txt += ", log(3**k, 2)=" + str(
      round(log(3**self.k, 2), 2))
  txt += ", d=" + str(self.d)
  txt += ", l=" + str(self.l)
  txt += ",log(epsilon,2)=" + str(
      round(log(self.eps, 2), 2)) + "\n"
  txt += "Standard deviations for IBSR:\n"
  txt += "s_id=" + str(self.sid)
  txt += ", log(s_sid,2)=" + str(
      round(log(self.sid, 2), 2)) + "\n"
  txt += "s_sig=" + str(self.ssign)
  txt += ", log(s_sid,2)=" + str(
      round(log(self.ssign, 2), 2)) + "\n"
  txt += "Standard deviations for IBSPW:\n"
  txt += "s_PW=" + str(self.sid)
  txt += ", log(s_PW,2)=" + str(
      round(log(self.s_PW, 2), 2)) + "\n"
  txt += "sp_PW=" + str(self.sid)
```

```
    txt += ", log(sp_PW,2)=" + str(
        round(log(self.sp_PW, 2), 2)) + "\n"
    txt += "spp_PW=" + str(self.ssign)
    txt += ", log(spp_PW,2)=" + str(
        round(log(self.spp_PW, 2), 2))
    print(txt)

  def print_sizes(self):
    txt = "SIGNATURE SIZES: "
    txt += "IBSR=" + str(
        round(self.size_sign / 10**6, 2)) + "Mo"
    txt += " IBSRPW=" + str(
        round(self.size_sign_PW / 10**6,
              2)) + "Mo"
    txt += "\nPUBLIC KEY SIZE: "
    txt += "mpk=" + str(
        round(self.size_pk / 10**6, 2)) + "Mo"
    txt += "\nSECRET KEY SIZES: "
    txt += "msk=" + str(
        round(self.size_sk / 10**6, 2)) + "Mo, "
    txt += "sk_id=" + str(
        round(self.size_sk_id / 10**6, 2)) + "Mo"
    txt += "\nRSIS bounds: "
    txt += "IBSR=" + str(self.RSISBound)
    txt += ", of log=" + str(
        round(log(self.RSISBound, 2), 2))
    txt += "IBSPW=" + str(self.RSISBound_PW)
    txt += ", of log=" + str(
        round(log(self.RSISBound_PW, 2), 2))
    print(txt)

  def summary(self):
    print("PARAMETERS SUMMARY:\n")
    self.print_params()
    print("SIZES SUMMARY:\n")
    self.print_sizes()
    print("SECURITY SUMMARY:\n")
    self.secu()

# create the set of parameters
paramsI = IBSParameterSet(65, 2048, 132,
                          2**(-200))
paramsII = IBSParameterSet(153, 2048, 308,
                           2**(-200))
# Make a summary of parameters values,
print("Summary for paramsI:\n")
paramsI.summary()
print("Summary for paramsII:\n")
paramsII.summary()
```