Short Signatures from DDH without Pairings or Random Oracles

Dario Catalano[1], Valentina Frasca[1], Emanuele Giunta[2]

[1] Dipartimento di Matematica e Informatica, Università di Catania, Italy.
dario.catalano@unict.it
valentina.frasca@phd.unict.it
[2] ETH Zurich, Zurich, Switzerland.
emanuele.giunta@inf.ethz.ch

Abstract. We present two constructions of short signature schemes based on the polynomial hardness of decisional Diffie Hellman. Our simplest scheme guarantees *selective* security (i.e. the adversary has to commit to the forged message ahead of time) while the second one realizes full fledged existential unforgeability. Remarkably, our schemes can be implemented over standard prime order groups (no pairings needed) and can be proven secure without resorting to the random oracle heuristic.

Table of Contents

1 Introduction **4**
- 1.1 Technical Overview . . . 5
- 1.2 Other Related Work . . . 9

2 Preliminaries **10**
- 2.1 Notation . . . 10
- 2.2 Statistical Distance . . . 10
- 2.3 Universal Hash Functions . . . 11
- 2.4 Strongly Universal Function . . . 12
- 2.5 Exceptional Sets of Binary Matrices . . . 12
- 2.6 Prime Order Groups . . . 13
- 2.7 Digital Signatures . . . 14

3 Distance Function **14**
- 3.1 Definition and Properties . . . 14
- 3.2 Rejection Sampling . . . 16
- 3.3 Domain Sampler . . . 17
- 3.4 Preimage Sampler . . . 18

4 Selectively Secure Short Signatures from DDH **20**
- 4.1 Construction . . . 20
- 4.2 Correctness . . . 21
- 4.3 Unforgeability . . . 23

5 Adaptively Secure Short Signatures from DDH **28**
- 5.1 Construction . . . 28
- 5.2 Correctness . . . 29
- 5.3 Unforgeability . . . 30

A Further Preliminaries **33**
- A.1 Statistical Distance . . . 33
- A.2 Min-Entropy . . . 36

B Postponed Proofs: Preliminaries **36**
- B.1 Balanced Functions . . . 36
- B.2 Min-Entropy . . . 38
- B.3 Universal Hash Functions . . . 39
- B.4 Exceptional Sets of Binary Matrices . . . 40
- B.5 Prime Order Groups . . . 40

C Postponed Proofs: Distance Function **42**
C.1 Properties 42
C.2 Rejection Sampling 43
C.3 Domain Sampling 44
C.4 Preimage Sampling 46

D Postponed Proofs: Constructions **50**
D.1 Selectively Secure Scheme: Claims 50
D.2 Adaptively Secure Scheme: Correctness 54
D.3 Adaptively Secure Scheme: Unforgeability 55
D.4 Adaptively Secure Scheme: Claims 64

1 Introduction

Digital signatures are among the most fundamental primitives in cryptography. They allow reassuring the receiver of a digital content that it originates from a specific sender. Moreover, such guarantee can be transferred to any third party (non-repudiation). Because of their centrality, it is of fundamental importance to realize signature schemes that are both secure and efficient.

Security for digital signatures was formally introduced in the seminal paper by Goldwasser *et al.* [GMR88] along with a concrete scheme realizing it. Numerous other works (see below) later improved on it both in terms of concrete efficiency and weaker computational assumptions.

As per the second direction, an important line of research focused on identifying the minimal assumptions needed to realize secure digital signatures. The constructions from [GMR88] rely on *trapdoor claw free permutations*. Subsequently, Bellare and Micali [BM92] demonstrated that any trapdoor permutation would suffice. A major advance was achieved by Naor and Yung [NY89], who proved that secure digital signatures can be constructed from one-way permutations, thereby eliminating the need for the trapdoor assumption, initially thought to be essential. Finally, Rompel [Rom90] further reduced the requirement to the sole existence of one-way functions, which is clearly the minimal necessary assumption.

All the schemes mentioned above, however, fall short in terms of signature size. For instance, [GMR88] is based on a binary tree of height d, resulting in a signature size $\Omega(d \cdot \lambda)$. Here, the parameter d is selected so that 2^d exceeds the total number of messages the signer may ever produce. In particular, no scheme with *short* signature length $\Theta(\lambda)$ is known from symmetric primitives.

Currently, short signatures have been realized from several public-key assumptions such as CDH [Wat05], RSA [HW09] and SIS [DM14]. However, with no exception, all constructions in the known prime order group setting either rely on pairings (e.g. [BB04, CL04, Wat05]) or the random oracle heuristic ([Sch90, PS96]), or are proven under ad-hoc assumptions [JMV01].

Our Contributions. We provide the first short and stateless signature schemes that are provably secure under the decisional Diffie Hellman assumption and that do not rely on pairings or random oracles. We list our contributions below.

- Our first scheme guarantees *selective security* (i.e. the adversary has to provide the message to forge ahead of time) and produces signatures that can be as short as 7 scalars (225B at 128 bits of security).
- Our second scheme instead achieves full EUF-CMA security, although with larger public key, and signatures as short as 9 scalars (290B at 128 bits of security).

Exact signature and verification key sizes are reported in Table 1. Both our schemes rely on novel techniques to produce (and simulate in the proof of security) signatures. We consider these among the main contributions of this paper.

Scheme	$\lvert\sigma\rvert$	$\lvert\mathsf{vk}\rvert$	Security
First	$6\lambda + 4\log q + \log(4\lambda)$	$O(\lambda^2)\ \mathbb{G} + O(\lambda^5 \log \lambda)$	Selective
Second	$6\lambda + 6\log q + \log(4\lambda)$	$O(\lambda^3)\ \mathbb{G} + O(\lambda^6 \log \lambda)$	Adaptive

Table 1: Parameters achieved by our constructions. λ is the security parameter, $\mathbb{G}$ is a group of prime order q.

On the concrete efficiency of our schemes. We stress both our schemes are mainly of theoretical interest. They are only meant to demonstrate the feasibility of short signature under plain DDH, and feature public key size and running times that are impractical by all means. However, such high costs stem from our reliance on heavy information-theoretical tools and distance functions over groups [BGI16]. This is in sharp contrast with inefficiency arising from the usage of non black box techniques (such as garbled circuits and iO), leaving room for hope. We therefore leave open the problem of standard model realizations of *practical* short signatures from the Diffie Hellman assumption.

Strong Puncturability. Due to our proof techniques, both schemes are also *strongly puncturable* [ADM+24, GVW19], meaning that the verification key can be generated so that for prescribed messages there exists no valid signature with high probability. Specifically, our first scheme support puncturing in a single point, whereas our second construction, with message space $\mathbb{F}_2^\mu$, can be constrained over any linear subspace. Note the notion in [GVW19] is a stronger than that of [BSW16, CPW20, JDS22] (realizable from OWFs), where given a punctured *secret key* it is infeasible (as opposed to statistically impossible) to find a signature for punctured messages. To the best of our knowledge, strongly puncturable signatures were only known from RSA, LWE, pairings and simulation sound NIZKs, and our constructions are the first to realize this primitive from the polynomial hardness of DDH.

1.1 Technical Overview

Blueprint. Both our schemes follow similar strategies. The verification key contains parameters defining a family of functions $F_m : \mathcal{X} \to \mathcal{Y}$, one per message m, such that:

1. F_m is efficiently computable.
2. For a (set of) m^*, programmable in the parameters, F_{m^*} is *very lossy*[3].
3. The parameters hide the message(s) m^*.
4. For any other m, F_m is preimage-sampleable given a trapdoor.

[3] Precisely, we will need that $|\mathrm{Im}\,(F_{m^*})| \ll |\mathcal{Y}|$.

Such a family yields a signature as follows. Initially a target $t \in \mathcal{Y}$ is chosen. A signature for a message m is a preimage σ of t and the verifier simply checks $F_m(\sigma) = t$. For most messages such a signature is efficiently computable if F_m is preimage-sampleable. However, if F_{m^*} is very lossy, with high probability $t \notin \mathrm{Im}(F_{m^*})$ and so no signature exists. This gives us selective security when m^*, the message an adversary attempts to forge, is known in advance, as we can *puncture* it without having the adversary realize we did so. To argue adaptive security instead we would need F to be puncturable in a set of messages specified by a partitioning scheme, e.g. an admissible hash [BB04].

Straw man example. As a stepping stone we present a simple first attempt at instantiating our blue-print, aiming for selective security. The subtle but fundamental reasons why this fails represent the core challenges solved by our schemes.

Key Generation. Key generation consists in the following steps. Given a group $\mathbb{G}$[4] of prime order q where DDH is hard, one chooses $\mathbf{a}_1, \mathbf{a}_2, \mathbf{u} \in \mathbb{F}_q^n$ and $\mathbf{t} \in \{0,1\}^n$, where n is a parameter, and sets[5] $A_i \leftarrow \mathbf{u} \otimes \mathbf{a}_i$, for $i = 1, 2$. Notice A_1, A_2 are rank-1. Next, a random key k for a PRF $f_k : \mathbb{G} \to \{0,1\}$ is chosen. The verification key is

$$\mathsf{vk} = ([A_1], [A_2], [\mathbf{u}], \mathbf{t}, k)$$

while the secret signing key is $\mathbf{a}_1, \mathbf{a}_2$. The underlying family of functions F_m for $m \in \mathbb{F}_q$ maps two *short* vectors $\mathbf{x}_1, \mathbf{x}_2 \in \{0, \ldots, \ell - 1\}^n$ with $\ell = \mathsf{poly}(\lambda)$ and a field element $z \in \mathbb{F}_q$ into a bit string of length n as follows:

$$F_m(\mathbf{x}_1, \mathbf{x}_2, z) = f_k([A_1\mathbf{x}_1 + A_2\mathbf{x}_2 + z\mathbf{u} + m(\mathbf{x}_1 + \mathbf{x}_2)])$$

where we assume f_k to be applied entry-wise. Following the blue-print, a signature for m would be $\sigma = (\mathbf{x}_1, \mathbf{x}_2, z)$ with $\mathbf{x}_i$ short such that $F_m(\sigma) = \mathbf{t}$. This is efficiently verifiable, as F_m can be computed efficiently.

Signing. Our approach to sign, i.e. how to preimage-sample each F_m, is inspired by lock-picking[6]. As is, changing one entry in $\mathbf{x}_1$ affects all output bits due to the term $A_1\mathbf{x}_1$. We wish to reach a state where fixing z and $\mathbf{x}_2$, changing $x_{1,i}$ only affects the i-th entry. This is possible through equivocation: since $A_1 = \mathbf{u} \otimes \mathbf{a}_1$ then the term $A_1\mathbf{x}_1 + z\mathbf{u} = (\mathbf{a}_1^\top \mathbf{x}_1 + z)\mathbf{u}$ is a Chameleon Hash [KR00]. The idea is then to first fix some valid $z^*, \mathbf{x}_2$, brute-force entry-wise $\mathbf{x}_1$ such that $f_k([A_2\mathbf{x}_2 + z^*\mathbf{u} + \mathbf{x}_1]) = \mathbf{t}$ and finally recover the term $A_1\mathbf{x}_1$ by finding a collision, done setting $z = z^* - \mathbf{a}_1^\top \mathbf{x}_1$. Note that, for this to work, one only needs to know $\mathbf{a}_1$. This is summarized in the following steps:

[4] See section 2.1 for notation.

[5] $\otimes$ denotes the Kronecker product, i.e. for $\mathbf{u} \in \mathbb{F}_q^n$, $\mathbf{v} \in \mathbb{F}_q^m$ then $\mathbf{u} \otimes \mathbf{v} = (u_i v_j) \in \mathbb{F}_q^{n,m}$.

[6] When picking a physical lock, trying all possible combinations of pin elevations would require exponential time. However, in some cases, applying pressure makes it possible to test each pin's correct elevation *individually* and *independently* from other pins, thus only requiring linear time.

1. Sample $z^* \leftarrow^{\$} \mathbb{F}_q$ and $\mathbf{x}_2 \leftarrow^{\$} \{0, \ldots, \ell - 1\}^n$;
2. Call $(H_1, \ldots, H_n) = [A_2\mathbf{x}_2 + z^*\mathbf{u} + m\mathbf{x}_2]$; // $H_i \in \mathbb{G}$
3. For $i = 1, \ldots, n$:
4. Sample $x_{1,i} \leftarrow^{\$} \{y \ : \ f_k(H_i + my \cdot G) = t_i \ \wedge \ 0 \leq y \leq \ell - 1\}$;
5. If any of the above sets is empty start again with a different $z^*, \mathbf{x}_2$;
6. Set $z = z^* - \mathbf{a}_1^\top \mathbf{x}_1$ and $\sigma = (\mathbf{x}_1, \mathbf{x}_2, z)$;

Puncturing. Finally we illustrate how security could be argued. As per the blueprint, we wish to setup A_1, A_2 so that m^* cannot be signed *statistically*. We may do so setting $A_1 = \mathbf{u} \otimes \mathbf{a}_1 - m^* I$ and $A_2 = \mathbf{u} \otimes \mathbf{a}_2 - m^* I$ with I the $n \times n$ identity matrix. In this way the function F_m becomes

$$\begin{aligned} F_m(\mathbf{x}_1, \mathbf{x}_2, z) &= f_k([A_1\mathbf{x}_1 + A_2\mathbf{x}_2 + z\mathbf{u} + m(\mathbf{x}_1 + \mathbf{x}_2)]) \\ &= f_k(\big[(\mathbf{a}_1^\top \mathbf{x}_1 + \mathbf{a}_2^\top \mathbf{x}_2 + z)\mathbf{u} + (m - m^*) \cdot (\mathbf{x}_1 + \mathbf{x}_2)\big]). \end{aligned}$$

For $m \neq m^*$, signatures can be pre-sampled as before. However when $m = m^*$ the second term vanishes and f_k is applied to elements in $\mathbb{G}^n$ lying in the linear span of $[\mathbf{u}]$. As there are only $|\mathbb{G}| = q$ many of them, setting $n \gg \log q$ (e.g. $n = \log q + \lambda$) we have that with high probability $\mathbf{t} \notin \mathrm{Im}\,(F_{m^*})$.

Technical Challenges. To conclude we must argue "regular" and "punctured" keys are indistinguishable. Using DDH this could seemingly be done through 7 hybrids: Initially we only sign with $\mathbf{a}_1$. In H_1 we transform A_2 into a random matrix by DDH[7]. In H_2 we set A_2 as a random matrix minus $m^* I$, which gives the same distribution of H_1. In H_3 we use DDH on reverse, and set $A_2 = \mathbf{u} \otimes \mathbf{a}_1 - m^* I$. Finally in H_4 we switch key, so that $\mathbf{a}_2$ is now used to sign messages, and mirror the previous steps in H_5, H_6, H_7 for the matrix A_1.

Sadly this simple strategy fails in the key-switching hybrid (H_3 - H_4). The issue is that signatures generated with $\mathbf{a}_1$ or $\mathbf{a}_2$ may not have close distributions. Specifically, it can be shown that the i-th output bit of F_m now depends *only* on z and $x_{1,i}, x_{2,i}$ (as a consequence of our equivocation approach). Therefore one would need to argue that, fixed z, sampling one randomly and brute-forcing the other produces close distributions. However, both $x_{1,i}$, $x_{2,i}$ lie on polynomially small sets, leaving only two options: either f_k is extremely balanced[8] over the sets of group elements spanned by $x_{1,i}, x_{2,i}$ for most $z \in \mathbb{F}_q$, or even the smallest bias causes the statistical distance to be at least inverse polynomial.

Our Selectively Secure Construction. We overcome the issue above replacing f_k with a function that is perfectly balanced under some conditions, that is the *distance function* introduced in [BGI16]. Informally, given a set $S \subseteq \mathbb{G}$, the

[7] Here we would actually use Matrix-DDH (also referred to as Rank-DDH), stating rank-1 and random matrices are indistinguishable. This is equivalent to DDH.

[8] Specifically, arranging the points $[zu_i + mx_{1,i} + (m - m^*)x_{2,i}]$ on an $\ell \times \ell$ matrix, we would need f_k to be perfectly balanced when restricted to each row and column.

distance function $\delta : \mathbb{G} \to \mathbb{N}$ on $H \in \mathbb{G}$ measures the smallest $d \in \mathbb{N}$ for which $H + dG \in S$. δ_2, measuring the *parity* of δ (i.e. $\delta_2 = \delta \mod 2$) is then perfectly balanced since $\delta_2(H)$ and $\delta_2(H + G)$ are distinct, at least when $\delta(H) > 0$. Note this further means it now suffices to take $\mathbf{x}_1, \mathbf{x}_2$ as vectors of *bits*, i.e. we can set $\ell = 2$. However, these benefits come at the cost of new technical challenges.

Rejection Sampling. The most notable is that δ_2 is perfectly balanced on $H, H + G$ only when H has positive distance (or else H and $H + G$ may lie in different buckets), and smaller than some bound $T = \mathsf{poly}(\lambda)$ (or else computing $\delta(H)$ may take super-polynomial time). This implies that an inverse-polynomial fraction of group elements breaks δ_2. We solve the issue through a rejection sampling strategy: when signing, we reject all values of $z^*, \mathbf{x}_2$ leading to group elements $[A_2\mathbf{x}_2 + z^*\mathbf{u}]$ with either too small or too large (entry-wise) distance.

Message Embedding. Another issue is that previously, to support exponentially many messages, we added a term $m\mathbf{x}_1 + m\mathbf{x}_2$, which after puncturing becomes of the form $(m - m^*)\mathbf{x}_1 + (m - m^*)\mathbf{x}_2$. However such an approach is incompatible with δ_2. The issue is that when signing, given $H_1, \ldots, H_n \in \mathbb{G}^n$ with good distance, we would need to find $x_{1,i} \in \{0, 1\}$ such that $\delta_2(H_i + (m - m^*)x_{1,i}) = t_i$. This fails to make δ_2 balanced if $(m - m^*)$ is even, or if $(m - m^*)$ is too large (as H_i and $H_i + (m - m^*)G$ fall in different "buckets").

We solve this relying on an exponentially large family of *short* matrices M_m with entries in $\{0, 1\}$ so that the difference of any two distinct ones is invertible modulo 2 (i.e. a large exceptional set). Our main function F_m becomes

$$F_m(\mathbf{x}_1, \mathbf{x}_2, z) \;=\; \delta_2([A_1\mathbf{x}_1 + A_2\mathbf{x}_2 + z\mathbf{u} + \mathbf{x}_1 + M_m\mathbf{x}_2)]).$$

where we eventually choose not to add the factor M_m to $\mathbf{x}_1$ for technical reasons[9]. Since M_m is short, if $[A_1\mathbf{x}_1 + A_2\mathbf{x}_2 + z\mathbf{u}]$ has large enough distance it can be shown the above function equals

$$F_m(\mathbf{x}_1, \mathbf{x}_2, z) \;=\; \delta_2([A_1\mathbf{x}_1 + A_2\mathbf{x}_2 + z\mathbf{u}]) \oplus M_m\mathbf{x}_2 \oplus \mathbf{x}_1. \tag{1}$$

The first term can now be drawn equivocating $z^* = z + \mathbf{a}_1^\top \mathbf{x}_1$ (resp. $z^* = z + \mathbf{a}_2^\top \mathbf{x}_2$), while $\mathbf{x}_1$ (resp. $\mathbf{x}_2$) mapping to $\mathbf{t}$ is found solving a linear system over $\mathbb{F}_2$.

Key Switching Lemma. Finally, to show δ_2 resolves the initial issue, we introduce the *key switching lemma*, which we see as an independent technical contributions. At a high level our lemma addresses the following problem: two functions $f_1 : \mathcal{X}_1 \to \mathcal{Y}$ and $f_2 : \mathcal{X}_2 \to \mathcal{Y}$ are given. One wishes to sample a *collision* by setting x_1 uniformly in $\mathcal{X}_1$ and x_2 from $f_2^{-1}(f_1(x_1))$, or vice-versa (i.e. x_2 uniformly in $\mathcal{X}_2$ and x_1 in $f_1^{-1}(f_2(x_2))$). Then our lemma ensures the two distributions are close if both functions are ε-balanced[10].

[9] This is both to reduce the required minimum distance, and to allow signing 0 even though $M_0 = \Omega$ will not be invertible in our construction.

[10] i.e. they preserve the uniform distribution within distance ε.

To see how this relates to the sampling done for F_m, observe first that a side effect of δ_2 is that F_m *splits* as the xor of two functions (see equation 1). Letting z absorb the term $A_1\mathbf{x}_1$, (i.e. by applying a linear transformation mapping $z \mapsto z - \mathbf{a}_1^\top \mathbf{x}_1$) separates the variables $(\mathbf{x}_2, z)$ from $\mathbf{x}_1$. To avoid confusion, we will use z^* to refer to the shifting of z. Finding a preimage for $\mathbf{t}$ in this shifted domain is then the same as finding a collision for the two functions

$$\begin{aligned} f_1 &: \mathbb{F}_2^n \to \mathbb{F}_2^n \qquad & f_1(\mathbf{x}_1) &= \mathbf{x}_1 \oplus \mathbf{t}; \\ f_2 &: \mathcal{U}^* \to \mathbb{F}_2^n \qquad & f_2(\mathbf{x}_2, z^*) &= \delta_2\left([A_2\mathbf{x}_2 + z^*\mathbf{u}]\right) \oplus M_m\mathbf{x}_2, \end{aligned}$$

where $\mathcal{U}^*$ is the set of group elements where $\delta(A_2\mathbf{x}_2 + z^*\mathbf{u})$ is large enough. Our key-switching lemma then ensures keys can be switched as long as both functions are balanced (or *regular*).

Adaptively Secure Construction. To achieve full adaptive security we augment the selective secure scheme with an algebraic hash, as in [Wat05], so to allow partitioning. This further increases the public key size, but has no effect on signature size. The new verification key contains now (encoding of) $2\mu + 2$ matrices (with μ the message bit-length) and $\mu + 1$ vectors, that are used to map the message to sign into matrices $[A_i^{(m)}] = [A_{i,0} + m_1 A_{i,1} + \ldots + m_\mu A_{i,\mu}]$ and vector $\mathbf{u}^{(m)}$. Interestingly this allows to instantiate partitioning from conceptually simpler objects (i.e. $\mathbb{F}_2$-linear universal hash functions). This is in contrast to more involved simulation strategies such as the artificial abort of [Wat05]. We defer the details to Section 4.1.

1.2 Other Related Work

As mentioned in the introduction, efficient stateless signature schemes have already been constructed in the Random Oracle Model (e.g. [BR93, Sch90, BLS01, GJ03], [KW03, AFLT12]). In the standard model, known constructions of short signatures from prime order groups rely on pairings (e.g. [Wat05], [BB04]). Even if not truly short, it is also worth mentioning the signature schemes of [DN94] and [CD96]: in their work, the authors realize signatures from RSA using *flat* n-ary trees, as opposed to the binary tree of [GMR88]. A variant of [CD96] from (a variant of) the factoring problem was proposed in [CG05].

The widely recognized hardness of realizing (short) signatures in the standard model from pairing-free groups also fueled a line of research investigating inherent limitations. In [DHH+21, CFGG22] it is shown that no signature schemes can be proven secure in Maurer's generic group model (GGM) [Mau94]. These results however rule out constructions making even basic non-black-box usage of the group, including relying on group element representation. Notably, our constructions overcome both results precisely exploiting group element representation through the distance function. A similar picture is observed in the context of several related primitives, e.g. NIZK which are impossible in Maurer's GGM [Giu23] but realizable when the representation is exploited [JJ21].

We also mention that *non-short* signatures from pairing free groups exist. Beyond generic constructions from OWFs, [BKKP15] discuss a tree based scheme from a chameleon hash, which exists if the discrete logarithm problem is hard. The same construction can also be derived through Naor's trick [BF01] from the IBE in [DG17].

2 Preliminaries

2.1 Notation

λ is the security parameter. A non-negative function $f : \mathbb{N} \to \mathbb{R}$ is negligible if it vanishes faster than the inverse of any polynomial. For a prime power q, $\mathbb{F}_q$ is the finite field of order q. Given $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n$, then $\mathbf{u}^\top \mathbf{v}$ is their inner product. $\otimes$ denotes the Kronecker product, so that for $\mathbf{u} \in \mathbb{F}_q^n$, $\mathbf{v} \in \mathbb{F}_q^m$ then $\mathbf{u} \otimes \mathbf{v} = (u_i v_j) \in \mathbb{F}_q^{n,m}$. Note this implies that $(\mathbf{u} \otimes \mathbf{v}) \cdot \mathbf{x} = (\mathbf{v}^\top \mathbf{x}) \cdot \mathbf{u}$. Given $B \in \mathbb{F}^{n,m}$ with $n \leq m$ and $\mathsf{rk}(B) = n$ we denote B^+ a canonical right inverse of B, i.e. such that $BB^+ = I_n$

With abuse of notation we identify $\mathbb{F}_2$ with $\{0, 1\} \subseteq \mathbb{Z}$. For $x, y \in \mathbb{F}_2$, $x + y$ is their sum in $\mathbb{Z}$, while $x \oplus y = (x + y) \mod 2$ is their sum in $\mathbb{F}_2$. We use $\cdot$ to denote both products in $\mathbb{Z}$ and $\mathbb{F}_2$ as there is no ambiguity. Given a group $\mathbb{G}$ of prime order q with generator G, we use the additive notation over $\mathbb{G}$ and we denote $[a] = a \cdot G$ for $a \in \mathbb{F}_q$. We extend the notation to vectors and matrices entry-wise.

Given a probabilistic Turing machine $\mathcal{A}$ the notation $y \leftarrow \mathcal{A}(x; r)$, or equivalently $\mathcal{A}(x; r) \to y$, means that y is its output on input x and random tape r. We write $y \leftarrow \mathcal{A}(x)$ if $\mathcal{A}$ is deterministic. Moreover $y \leftarrow^{\$} \mathcal{A}(x)$ denotes the random variable $y \leftarrow \mathcal{A}(x; r)$ for a uniformly sampled tape r. Given S a set, $x \leftarrow^{\$} S$ means x is sampled uniformly from S. We adopt the convention that $x \leftarrow^{\$} \varnothing$ means $x = \perp$.

Provided discrete random variables x, y and event E, we denote $\mathrm{H}_\infty(x)$, $\mathrm{H}_\infty(x \,|\, E)$ and $\mathrm{H}_\infty(x \,|\, y)$ respectively the min-entropy of x, the conditional min-entropy of x given E and the average min-entropy of x given y. We defer definitions and known bounds to the appendix, Section A.2.

2.2 Statistical Distance

Here we recall the definition of statistical distance, and introduce the class of *balanced* functions as those that preserve the uniform distribution up to small statistical distance. Further basic results are deferred to the appendix, Section A.1.

Definition 1. *Let X_1, X_2 be two random variables over a finite set $\mathcal{X}$. The* statistical distance *between X_1 and X_2 is defined as*

$$\Delta(X_1, X_2) \coloneqq \frac{1}{2} \sum\nolimits_{x_0 \in \mathcal{X}} |\Pr[X_1 = x_0] - \Pr[X_2 = x_0]|.$$

Definition 2. *A function $f : \mathcal{X} \to \mathcal{Y}$ is* ε-balanced *if for $x \leftarrow^{\$} \mathcal{X}$ and $y \leftarrow^{\$} \mathcal{Y}$, it holds $\Delta(f(x), y) \leq \varepsilon$.*

We now state our key switching lemma, proof of which appears in the appendix, Section B.1. Recall that by our convention (see Section 2.1), sampling from the empty set always returns $\perp$.

Lemma 1 (Key Switching). *Let $f_1 : \mathcal{X}_1 \to \mathcal{Y}$ be a ε_1-balanced function and let $f_2 : \mathcal{X}_2 \to \mathcal{Y}$ be a ε_2-balanced function. Let $x_1, x_2, \widehat{x}_1, \widehat{x}_2$ be defined as follows:*

- $x_1 \leftarrow^{\$} \mathcal{X}_1$ *and* $x_2 \leftarrow^{\$} f_2^{-1}(f_1(x_1))$*;*
- $\widehat{x}_2 \leftarrow^{\$} \mathcal{X}_2$ *and* $\widehat{x}_1 \leftarrow^{\$} f_1^{-1}(f_2(\widehat{x}_2))$.

Then their statistical distance is bounded by $\Delta((x_1, x_2), (\widehat{x}_1, \widehat{x}_2)) \leq \varepsilon_1 + \varepsilon_2$.

2.3 Universal Hash Functions

Universal Hash Functions (UHF) [CW77] are families of compressing functions. Their security guarantee is that collisions on inputs distributed *independently* from a uniformly sampled UHF key are unlikely (although collisions may be easy to find adaptively). Throughout this paper we rely on families of linear UHF both due to their effectiveness as randomness extractor (see Theorem 1), and their ability to instantiate partitioning schemes (Lemma 2).

Definition 3. *Let $\mathcal{X}$ and $\mathcal{Y}$ be finite sets. A family $\mathcal{H} \subseteq \{f : \mathcal{X} \to \mathcal{Y}\}$ is a* universal hash function *(UHF) family if, for any $x_1, x_2 \in \mathcal{X}$ such that $x_1 \neq x_2$ and for any $h \leftarrow^{\$} \mathcal{H}$, it holds $\Pr[h(x_1) = h(x_2)] \leq |\mathcal{Y}|^{-1}$.*

Proposition 1. *For any prime $q \in \mathbb{N}$, and integers $n > m$ in $\mathbb{N}$ the family $\mathrm{Hom}(\mathbb{F}_q^n, \mathbb{F}_q^m) = \{f : \mathbb{F}_q^n \to \mathbb{F}_q^m \ : \ f \ \mathbb{F}_q\text{-linear}\}$ is a UHF. Moreover, the subset $\mathcal{H} \subseteq \mathrm{Hom}(\mathbb{F}_q^n, \mathbb{F}_q^m)$ of surjective functions[11] is a UHF.*

In light of the proposition above we will occasionally abuse notation by identifying $\mathbb{F}_q^{m,n}$ with $\mathrm{Hom}(\mathbb{F}_q^n, \mathbb{F}_q^m)$, and call $\mathbb{F}_q^{m,n}$ a set of linear UHF.

Theorem 1 (Leftover Hash Lemma [DORS08]). *Let X and Y be random variables over $\mathcal{X}$ and $\mathcal{Y}$ respectively, $m \in \mathbb{N}$ and $\mathcal{H} \subseteq \{f : \mathcal{X} \to \{0,1\}^m\}$ a UHF family. If $\mathrm{H}_\infty(X|Y) \geq m + 2\log(1/\varepsilon)$, sampling $h \leftarrow^{\$} \mathcal{H}$, $U \leftarrow^{\$} \{0,1\}^m$, it holds*

$$\Delta((h, h(X), Y), (h, U, Y)) \leq \varepsilon.$$

Beyond being useful as randomness extractors, universal hash functions are also an effective tool to instantiate admissible hash functions [BB04]. This is formally implied by the following Lemma. A proof can be found in the appendix, Section B.3.

Lemma 2. *Let $\mathcal{H} \subseteq \{f : \{0,1\}^n \to \{0,1\}^\ell\}$ a UHF family, $h \leftarrow^{\$} \mathcal{H}$, $y \leftarrow^{\$} \{0,1\}^\ell$, and $m_1, \ldots, m_\vartheta, m^*$ random variables in $\{0,1\}^n$ and independent from (h, y). Calling $\mathsf{Coll} \coloneqq (m_1 = m^* \vee \ldots \vee m_\vartheta = m^*)$, if $\ell = \log(2\vartheta)$ and E is an event mutually independent from (h, y) then*

$$\Pr\left[h(m^*) = y \wedge \left(\wedge_{i=1}^{\vartheta} h(m_i) \neq y\right) \wedge E\right] \ \geq \ \frac{1}{4\vartheta} \cdot \Pr\left[\neg\mathsf{Coll} \wedge E\right].$$

[11] Since $n > m$, these are all those functions whose associated matrix is full rank.

2.4 Strongly Universal Function

If universal hash functions could be seen as the information-theoretic analog of a collision resistant hash, *strongly* universal functions (or K-universal) [WC81] are the statistical analog of pseudorandom functions. Informally, the defining property of K-universal functions is being "locally random". That is, given a randomly drawn key, then the output of its associated function on any set of at most K distinct points is truly random. In the following we mildly adapt the original definition to consider *ensembles* of SUFs, parametrized by λ.

Definition 4. *Given $K : \mathbb{N} \to \mathbb{N}$, two ensembles of finite sets $(\mathcal{X}_\lambda, \mathcal{Y}_\lambda)_{\lambda\in\mathbb{N}}$ and a pair of* PPT *algorithms* $(\mathsf{SUF.Gen}, \mathsf{SUF.Eval})$ *such that*

- $\mathsf{SUF.Gen}(1^\lambda) \xrightarrow{\$} k$ *returns a function key;*
- $\mathsf{SUF.Eval}(k, x) \to y$ *for $x \in \mathcal{X}$ and $y \in \mathcal{Y}$.*

then $(\mathsf{SUF.Gen}, \mathsf{SUF.Eval})$ *is K-universal if for all $\lambda \in \mathbb{N}$, given $k \leftarrow^{\$} \mathsf{SUF.Gen}(1^\lambda)$ and $x_1, \ldots, x_{K(\lambda)} \in \mathcal{X}_\lambda$ distinct points, setting $y_i \leftarrow \mathsf{SUF.Eval}(k, x_i)$ then $(y_1, \ldots, y_{K(\lambda)})$ is uniform in $\mathcal{Y}_\lambda^{K(\lambda)}$.*

We denote $f_k(\cdot)$ the function $\mathsf{SUF.Eval}(k, \cdot)$. A simple example of K-universal functions is given by the class of polynomials in $\mathbb{F}_{2^n}$ of degree at most $K - 1$. Up to identifying $\mathbb{F}_{2^n}$ and $\{0,1\}^n$ as sets, and truncating the function output, this implies unconditionally the existence of a K-universal function family from $\{0,1\}^n$ to $\{0,1\}^m$ for any K, n, m polynomially bounded. For simplicity we will also denote $\mathcal{K}_\lambda = \mathsf{Supp}(\mathsf{SUF.Gen}(1^\lambda))$ the set of possible SUF keys.

2.5 Exceptional Sets of Binary Matrices

A core tool in our construction is a large *exceptional set* in $\mathbb{F}_2^{n,n}$. A set $\mathcal{E} \subseteq \mathbb{F}_2^{n,n}$ is said to be exceptional if for any two distinct $A, B \in \mathcal{E}$ their difference $A - B$ is invertible. In this section we revisit a construction of an $\mathbb{F}_2$-linear immersion $P^{(\ell)} : \mathbb{F}_2^\ell \to \mathbb{F}_2^{n,n}$ for any $\ell \leq n$ whose image forms an exceptional set.

Up to canonically identifying $\mathbb{F}_2^{n,n}$ with $\mathrm{End}(\mathbb{F}_2^n)$ the ring of linear maps from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$, we will actually describe $P^{(\ell)} : \mathbb{F}_2^\ell \to \mathrm{End}(\mathbb{F}_{2^n})$. To this aim, for every $\ell \leq n$, let us introduce the following functions:

- $\psi^{(\ell)} : \mathbb{F}_2^\ell \to \mathbb{F}_2^n$ the immersion s.t. $\psi^{(\ell)}(x_1, \ldots, x_\ell) = (x_1, \ldots, x_\ell, 0, \ldots, 0)$;
- $\phi : \mathbb{F}_2^n \to \mathbb{F}_{2^n}$ an isomorphism of $\mathbb{F}_2$-vector spaces.

Given the above, we can define for any $\mathbf{x} \in \mathbb{F}_2^\ell$, $P_{\mathbf{x}}^{(\ell)} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ such that

$$P_{\mathbf{x}}^{(\ell)}(\mathbf{y}) \;=\; \phi^{-1}\left(\phi(\mathbf{y}) \cdot \phi(\psi^{(\ell)}(\mathbf{x}))\right).$$

Where the dot $\cdot$ denotes the product in $\mathbb{F}_{2^n}$. We prove the following theorem in the appendix, Section B.4.

Theorem 2. *For any $\ell \leq n$ positive integers, the map $P^{(\ell)} : \mathbb{F}_2^\ell \to \mathrm{End}(\mathbb{F}_2^n)$ assigning $\mathbf{x} \mapsto P_{\mathbf{x}}^{(\ell)}$ is a well defined $\mathbb{F}_2$-linear map. Moreover*

$$\mathbf{x} \neq \mathbf{0} \;\Rightarrow\; P_{\mathbf{x}}^{(\ell)} \text{ is invertible.}$$

Remark 1. When ℓ is clear from context, e.g. it can be inferred by the length of $\mathbf{x}$, we will omit it and simply write $P_{\mathbf{x}} = P_{\mathbf{x}}^{(\ell)}$.

2.6 Prime Order Groups

In this section we recall notation for cryptographic prime order groups, along with the decisional Diffie-Hellman problem and equivalent formulations up to logarithmic loss in the instance size.

Definition 5. *A cryptographic prime order group is a* PPT *algorithm* $\mathsf{G.Gen}$ *such that for all $\lambda \in \mathbb{N}$, $\mathsf{G.Gen}(1^\lambda) \xrightarrow{\$} (\mathbb{G}, G, q)$ where $\mathbb{G}$ is a group with efficiently computable operation and membership test, $G \in \mathbb{G}$ is a generator and $q = |\mathbb{G}|$ is prime.*

Without loss of generality we will assume G, q to be embedded in $\mathbb{G}$. Moreover, we will denote $\mathcal{G}_\lambda = \mathsf{Supp}(\mathsf{G.Gen}(1^\lambda))$ the set of possible group descriptions.

Definition 6. *The decisional Diffie-Hellman (DDH) problem is hard in* $\mathsf{G.Gen}$ *if for any* PPT *adversary $\mathcal{A}$ there exists a negligible ε such that for all $\lambda \in \mathbb{N}$, sampling $(\mathbb{G}, G, q) \leftarrow^{\$} \mathsf{G.Gen}(1^\lambda)$, $a, b, c \leftarrow^{\$} \mathbb{F}_q$ then $\mathsf{Adv}^{\mathsf{ddh}}_{\mathsf{G},\mathcal{A}}(\lambda) :=$*

$$\left|\Pr\left[1 \leftarrow \mathcal{A}(\mathbb{G}, [a], [b], [ab])\right] - \Pr\left[1 \leftarrow \mathcal{A}(\mathbb{G}, [a], [b], [c])\right]\right| \;\leq\; \varepsilon(\lambda).$$

Definition 7. *The (n, m)-Matrix Diffie-Hellman problem, or (n, m)-MDDH, for $n \leq m$ polynomially bounded functions, is hard for* $\mathsf{G.Gen}$ *if for any* PPT *adversary $\mathcal{A}$ there exists a negligible ε such that for all $\lambda \in \mathbb{N}$, sampling matrices $A \leftarrow^{\$} \mathbb{F}_q^{n(\lambda), m(\lambda)}$ and $B \leftarrow^{\$} \mathbb{F}_q^{n(\lambda), m(\lambda)}$ with $\mathsf{rk}(A) = n(\lambda)$ and $\mathsf{rk}(B) = 1$ then,*

$$\mathsf{Adv}^{\mathsf{rank}}_{\mathsf{G},\mathcal{A}}(\lambda) \;:=\; \left|\Pr\left[1 \leftarrow \mathcal{A}(\mathbb{G}, [A])\right] - \Pr\left[1 \leftarrow \mathcal{A}(\mathbb{G}, [B])\right]\right| \;\leq\; \varepsilon(\lambda).$$

Note that the DDH problem and the (n, m)-MDDH problem are equivalent for all polynomially bounded n, m. An elegant and optimal reduction of (n, m)-MDDH to DDH losing only a factor $\log_2 n$ is given in [Vil12].

In order to simplify the analysis in our reductions, we will often consider the above decisional problem with mildly different distributions. Specifically, in Section B.5 of the appendix we quantify the statistical loss when sampling A uniformly in $\mathbb{F}_q^{n,m}$ and B as $\mathbf{u} \otimes (1, \mathbf{v})$ or $\mathbf{u} \otimes \mathbf{w}$ for uniformly sampled vectors of matching dimensions.

2.7 Digital Signatures

The standard security notion for digital signature is existential unforgeability against chosen message attacks [GMR88], recalled in this section. However, in this paper we further consider a *selective* variant where the adversary has to choose the forged message before seeing the public parameters. Note our first (more efficient) construction will be proven selectively secure, whereas our second one achieves EUF-CMA security.

Definition 8. *A signature scheme is a triplet of* PPT *algorithms* $(\mathsf{S.Gen}, \mathsf{S.Sign}, \mathsf{S.Vfy})$ *along with an ensemble of sets* $(\mathcal{M}_\lambda)_{\lambda\in\mathbb{N}}$ *(the message space) such that:*

- $\mathsf{S.Gen}(1^\lambda) \xrightarrow{\$} (\mathsf{vk}, \mathsf{sk})$ *generates a verification key and a signing key;*
- $\mathsf{S.Sign}(\mathsf{sk}, m) \xrightarrow{\$} \sigma$ *returns the signature of a message* $m \in \mathcal{M}_\lambda$*;*
- $\mathsf{S.Vfy}(\mathsf{vk}, m, \sigma) \to 0/1$ *verifies the validity of* σ *for* m*.*

Without loss of generality, up to relying on the hash-and-sign paradigm, we can always assume $\mathcal{M}_\lambda = \{0,1\}^{2\lambda}$.

Definition 9. *A signature scheme* $(\mathsf{S.Gen}, \mathsf{S.Sign}, \mathsf{S.Vfy})$ *is correct if there exists a negligible function* ε *such that for all messages* $m \in \mathcal{M}_\lambda$*, then*

$$\Pr\left[\mathsf{S.Vfy}(\mathsf{vk}, m, \sigma) \to 0 \;\middle|\; \begin{array}{r}(\mathsf{vk},\mathsf{sk}) \xleftarrow{\$} \mathsf{S.Gen}(1^\lambda)\\ \sigma \xleftarrow{\$} \mathsf{S.Sign}(\mathsf{sk}, m)\end{array}\right] \;\leq\; \varepsilon(\lambda).$$

Definition 10. *A signature scheme* S *is selectively unforgeable under chosen message attack (SUF-CMA) if for any* PPT *adversary* $\mathcal{A}$ *executed in the experiment in Figure 1 (left) there exists a negligible* ε *such that*

$$\mathsf{Adv}^{\mathsf{suf\text{-}cma}}_{\mathsf{S},\mathcal{A}}(\lambda) \;\coloneqq\; \Pr\left[\mathsf{Exp}^{\mathsf{suf\text{-}cma}}_{\mathsf{S},\mathcal{A}}(\lambda) = 1\right] \;\leq\; \varepsilon(\lambda).$$

Analogously S *is existentially unforgeable under chosen message attacks (EUF-CMA) if for any* PPT *adversary* $\mathcal{A}$ *executed in the experiment in Figure 1 (right) there exists a negligible* ε *such that*

$$\mathsf{Adv}^{\mathsf{euf\text{-}cma}}_{\mathsf{S},\mathcal{A}}(\lambda) \;\coloneqq\; \Pr\left[\mathsf{Exp}^{\mathsf{euf\text{-}cma}}_{\mathsf{S},\mathcal{A}}(\lambda) = 1\right] \;\leq\; \varepsilon(\lambda).$$

3 Distance Function

3.1 Definition and Properties

In this section we recall the definition of distance function over a group $\mathbb{G}$, a tool originally introduced in the context of homomorphic secret sharing [BGI16]. Given a subset $S \subseteq \mathbb{G}$, a distance function measures how far a given group H element is from S. This is the smallest $d \in \mathbb{N}$ such that $H + dG \in S$. Concretely, S must be efficiently representable and decidable. Moreover, for the distance to be

$\mathsf{Exp}^{\mathsf{suf\text{-}cma}}_{\mathsf{S},\mathcal{A}}(\lambda)$:

1 : $m^* \leftarrow \mathcal{A}(1^\lambda);\ Q \leftarrow \varnothing$
2 : $(\mathsf{vk}, \mathsf{sk}) \leftarrow^{\$} \mathsf{S.Gen}(1^\lambda)$
3 : $\sigma^* \leftarrow^{\$} \mathcal{A}^{\mathcal{O}_{\mathsf{sk},Q}}(1^\lambda, \mathsf{vk})$
4 : $b_1 \leftarrow (m^* \notin Q)$
5 : $b_2 \leftarrow (\mathsf{S.Vfy}(\mathsf{vk}, m^*, \sigma^*) = 1)$
6 : **Return** $b_1 \wedge b_2$

$\mathcal{O}_{\mathsf{sk},Q}(m)$:

1 : Update $Q \leftarrow Q \cup \{m\}$
2 : **Return** $\sigma \leftarrow \mathsf{S.Sign}(\mathsf{sk}, m)$

$\mathsf{Exp}^{\mathsf{euf\text{-}cma}}_{\mathsf{S},\mathcal{A}}(\lambda)$:

1 : $Q \leftarrow \varnothing$
2 : $(\mathsf{vk}, \mathsf{sk}) \leftarrow^{\$} \mathsf{S.Gen}(1^\lambda)$
3 : $(m^*, \sigma^*) \leftarrow^{\$} \mathcal{A}^{\mathcal{O}_{\mathsf{sk},Q}}(1^\lambda, \mathsf{vk})$
4 : $b_1 \leftarrow (m^* \notin Q)$
5 : $b_2 \leftarrow (\mathsf{S.Vfy}(\mathsf{vk}, m^*, \sigma^*) = 1)$
6 : **Return** $b_1 \wedge b_2$

Fig. 1: Selective unforgeability (left) and existential unforgeability (right) game under chosen message attacks, for scheme S and adversary $\mathcal{A}$.

computable in PPT-time, S should not have many *large* gaps. All these properties can be achieved through a SUF[12]: given k a key for $f_k : \mathbb{G} \to \{0,1\}^L$, simply let $S = f_k^{-1}(0)$. Choosing $L = O(\log \lambda)$ then ensures that the average element has distance proportional to $2^L = \mathsf{poly}(\lambda)$, which can be measured via brute force search. This is formalized in Definition 11, where we assume $(\mathsf{SUF.Gen}, \mathsf{SUF.Eval})$ to be a strongly universal function family so that f_k for $k \in \mathcal{K}_\lambda$ is well defined over all $\mathbb{G} \subseteq \{0,1\}^*$ with $(\mathbb{G}, G, q) \in \mathcal{G}_\lambda$.

Definition 11. *Given $(\mathbb{G}, G, q) \in \mathcal{G}_\lambda$, $k \in \mathcal{K}_\lambda$ and $L, T = \mathsf{poly}(\lambda)$, we define the distance function $\delta_{\mathsf{dp}} : \mathbb{G} \to \mathbb{N} \cup \{\perp\}$ as the output of the algorithm in Figure 2, where $\mathsf{dp} = (\mathbb{G}, G, q, k, L, T)$.*

$\delta_{\mathsf{dp}}(H)$:

1 : Parse $\mathsf{dp} = (\mathbb{G}, G, q, k, L, T)$
2 : **For** $i \in \{0, \ldots, T-1\}$:
3 : **If** $f_k(H + i \cdot G) = 0^L$: **Return** i
4 : **Return** $\perp$

Fig. 2: Distance function with $f_k : \mathbb{G} \to \{0,1\}^L$ a SUF and $H \in \mathbb{G}$.

When clear from the context, we will omit dp and write $\delta : \mathbb{G} \to \mathbb{N} \cup \{\perp\}$. Given a distance function δ, we extend it to $\mathbb{G}^n$ by applying it entry-wise, i.e.

$$\delta : \mathbb{G}^n \to (\mathbb{N} \cup \{\perp\})^n \qquad \delta(H_1, \ldots, H_n) \ = \ (\delta(H_1), \ldots, \delta(H_n)).$$

[12] Previous work (e.g. [BGI16], [DGI+19]) relied on pseudorandom functions instead. We opt for strongly universal functions instead for the sake of a simpler analysis.

Moreover, the following associated functions will be useful:

$$\begin{aligned} \delta_{\mathsf{min}} : \mathbb{G}^n \to \mathbb{N} \cup \{\perp\} \qquad & \delta_{\mathsf{min}}(H_1, \ldots, H_n) = \min_{i=1}^{n} \delta(H_i) \\ \delta_2 : \mathbb{G}^n \to (\mathbb{F}_2 \cup \{\perp\})^n \qquad & \delta_2(H_1, \ldots, H_n) = \delta(H_1, \ldots, H_n) \mod 2. \end{aligned}$$

where we assume that min returns $\perp$ if at least one of its arguments is $\perp$, and that $\perp$ modulo 2 is mapped to $\perp$. To avoid explicitly requiring the distance to be an integer, throughout the paper we also assume that $\perp \not\leq d$ and $\perp \not\geq d$ for any integer d. In particular $\delta_{\mathsf{min}}(\mathbf{H}) \geq d$ also means $\delta_{\mathsf{min}}(\mathbf{H}) \neq \perp$.

Finally, the main property of the distance function is its restricted homomorphism, as formally stated in the following propositions. Their proofs appear in the appendix, Section C.1.

Lemma 3. *Let* $\mathsf{dp} = (\mathbb{G}, G, q, k, L, T)$ *as in Definition 11. For any* $\mathbf{H} \in \mathbb{G}^n$ *with* $\delta_{\mathsf{min}}(\mathbf{H}) \geq d$ *and vector* $\mathbf{x} \in \mathbb{N}^n$ *with* $\|\mathbf{x}\|_\infty \leq d$ *we have*

$$\delta(\mathbf{H} + \mathbf{x} \cdot G) \;=\; \delta(\mathbf{H}) - \mathbf{x}.$$

In particular, under the same assumptions $\delta_2(\mathbf{H} + \mathbf{x}G) = \delta_2(\mathbf{H}) \oplus \mathbf{x}$.

Corollary 1. *Let* $\mathsf{dp} = (\mathbb{G}, G, q, k, L, T)$ *as in Definition 11. For any* $\mathbf{H} \in \mathbb{G}^n$ *and pair of vectors* $\mathbf{x}_1, \mathbf{x}_2 \in \mathbb{N}^n$ *such that* $\delta_{\mathsf{min}}(\mathbf{H} - \mathbf{x}_1 G) \geq \max(\|\mathbf{x}_1\|_\infty, \|\mathbf{x}_2\|_\infty)$ *then*

$$\delta(\mathbf{H} - \mathbf{x}_1 G + \mathbf{x}_2 G) \;=\; \delta(\mathbf{H}) + \mathbf{x}_1 - \mathbf{x}_2.$$

In particular, under the same assumptions $\delta_2(\mathbf{H} - \mathbf{x}_1 G + \mathbf{x}_2 G) \;=\; \delta_2(\mathbf{H}) \oplus \mathbf{x}_1 \oplus \mathbf{x}_2$.

3.2 Rejection Sampling

Many primitives built from distance functions (e.g. [DGI+19]) require a large fraction of elements in $\mathbb{G}$ to have sufficiently high distance. In light of Lemma 3 this enables powerful manipulations. However, it also introduces an inverse-polynomial failure probability, since a significant fraction of group elements will either be too far (so that distance cannot be measured) or too close. This limitation seems inherent in many applications such as [DGI+19] where group elements of interest are generated by parties who cannot themselves check their distance. In order to avoid high error rate, we propose a simple rejection sampling procedure. In other words, given a specified distribution on $\mathbb{G}^n$, we draw independent samples from it until one achieves the desired minimum distance. Notably, this is possible for signatures (and not for Trapdoor Hash Functions and related primitives) since the signer holds all secret information and has no limitation in testing the resulting distance.

In this section we present the main theorem (Theorem 3) detailing the relation between desired distance and distance function parameters. Remarkably, although we adapt from [BGI16], their results only consider a *fixed* group element and make the error probability depend only on the PRF/SUF key choice. In our case instead we must crucially rely on samples being mutually independent and sufficiently spread out over $\mathbb{G}$. To formally capture the last requirement we first introduce the following *near collision* event.

Definition 12. *Given a group $(\mathbb{G}, G, q) \in \mathcal{G}_\lambda$, random variables $H_{i,j} \in \mathbb{G}$ for $i \in \{1, \ldots, \nu\}$ and $j \in \{1, \ldots, n\}$ and an integer $T \in \mathbb{N}^+$, we define the near-collision event of $\mathbf{H}$ for distance T as* $\mathsf{Near}(\mathbf{H}, T) =$

$$\exists i_1, i_2 \in \{1, \ldots, \nu\},\ \ j_1, j_2 \in \{1, \ldots, n\},\ \ \gamma \in \{0, \ldots, T-1\}\ : \\ (i_1, j_1) \neq (i_2, j_2)\ \wedge\ H_{i_1,j_1} = H_{i_2,j_2} + \gamma G.$$

Theorem 3. *Let $(\mathbb{G}, G, q) \in \mathcal{G}_\lambda$, $k \leftarrow^{\$} \mathsf{SUF.Gen}(1^\lambda)$ and $H_{i,j}$ random variables in $\mathbb{G}$ distributed independently from k, for $i \in \{1, \ldots, \nu\}$ and $j \in \{1, \ldots, n\}$. For any $d \in \mathbb{N}^+$ let $L, T \in \mathbb{N}$ be such that*

$$L \geq \log(5nd), \qquad T \geq 2^L \cdot (1 + \ln(n)) + d.$$

If SUF *is $(\nu n T)$-universal (see Definition 4), then*

$$\Pr\left[\nexists i : \delta_{\mathsf{min}}(H_{i,1}, \ldots, H_{i,n}) \geq d\right]\ \leq\ 2^{-\nu} + \Pr\left[\mathsf{Near}(\mathbf{H}, T)\right].$$

The proof appears in the appendix, Section C.2.

3.3 Domain Sampler

Using Theorem 3 we will show that, for a sensible choice of the distance parameters, a specific subset of $\mathbb{F}_2^{\eta_2} \times \mathbb{F}_q$ consisting of vectors whose distance is at least d is efficiently sampleable. Concretely, for η_1, η_2, η_3 integers[13], given a matrix $A \in \mathbb{F}_q^{\eta_3, \eta_2}$, a vector $\mathbf{u} \in \mathbb{F}_q^{\eta_3}$ and distance parameters dp, the set we need to sample from is defined as

$$\mathcal{U}^*\ :=\ \{(\mathbf{x}_0, z_0) \in \mathbb{F}_2^{\eta_2} \times \mathbb{F}_q\ :\ \delta_{\mathsf{min}}\left([A\mathbf{x}_0 + z_0\mathbf{u}]\right) \geq d\}.$$

To do so, we apply a rejection sampling strategy: a sequence of ν elements $(\mathbf{x}_1, z_1), \ldots, (\mathbf{x}_\nu, z_\nu)$ is sampled uniformly from $\mathbb{F}_2^{\eta_2} \times \mathbb{F}_q$, and the first one satisfying $\delta_{\mathsf{min}}([A\mathbf{x}_i + z_i\mathbf{u}]) \geq d$ is returned. This is formally described in Figure 3. Proofs for the following theorems are deferred to the appendix, Section C.3.

$\mathsf{Samp}([A], [\mathbf{u}], d, \mathsf{dp})$: // $\delta = \delta_{\mathsf{dp}}$

1 : **For** $i \in \{1, \ldots, \nu\}$:
2 : $\quad \mathbf{x}_i \leftarrow^{\$} \mathbb{F}_2^{\eta_2},\ z_i \leftarrow^{\$} \mathbb{F}_q$
3 : $\quad$ **If** $\delta_{\mathsf{min}}\left([A\mathbf{x}_i + z_i\mathbf{u}]\right) \geq d$: **Return** $(\mathbf{x}_i, z_i)$
4 : **Return** $\perp$ // Give up after ν attempts

Fig. 3: Domain sampler with $A \in \mathbb{F}_q^{\eta_3, \eta_2}$, $\mathbf{u} \in \mathbb{F}_q^{\eta_3}$, $d \in \mathbb{N}$, $\mathsf{dp} = (\mathbb{G}, G, q, k, L, T)$.

[13] Looking ahead, we will set $\eta_1 = n_1$, $\eta_2 = n_2$, $\eta_3 = n_1$ in the first construction (see Table 2), while for the second one we set $\eta_1 = n_1$, $\eta_2 = n_2$, $\eta_3 = n_2$ (see Table 3)

Theorem 4. *For any $k \in \mathcal{K}_\lambda$, $(\mathbb{G}, G, q) \in \mathcal{G}_\lambda$, $[A] \in \mathbb{G}_q^{\eta_3,\eta_2}$, $[\mathbf{u}] \in \mathbb{G}^{\eta_3}$ and any L, T, d integers, let $(\mathbf{x}, z) \leftarrow^{\$} \mathsf{Samp}([A], [\mathbf{u}], d, \mathsf{dp})$ with $\mathsf{dp} = (\mathbb{G}, G, q, k, L, T)$. Then conditioning on $(\mathbf{x}, z) \neq \perp$ we have that $(\mathbf{x}, z)$ is uniform over*

$$\mathcal{U}^* = \{(\mathbf{x}_0, z_0) \in \mathbb{F}_2^{\eta_2} \times \mathbb{F}_q : \delta_{\mathsf{min}}([A\mathbf{x}_0 + z_0\mathbf{u}]) \geq d\}.$$

Theorem 5. *For all $(\mathbb{G}, G, q) \in \mathcal{G}_\lambda$, $[A] \in \mathbb{G}^{\eta_3,\eta_2}$, $[\mathbf{u}] \in \mathbb{G}^{\eta_3}$ such that $(0 \neq u_i \neq u_j \ \forall i \neq j)$ and $d = \mathsf{poly}(\lambda)$, setting*

$$L \geq \log(5\eta_3 d), \qquad T \geq 2^L \cdot (1 + \ln(\eta_3)) + d$$

there exist $\varepsilon_1(\lambda)$ and a set of SUF keys $\mathcal{K}_1^* \subseteq \mathcal{K}_\lambda$:

1. $\varepsilon_1(\lambda) = \sqrt{\frac{1}{2^\nu} + \frac{\nu^2 \eta_3^2 T}{q}}$;
2. $k \leftarrow^{\$} \mathsf{SUF.Gen}(1^\lambda) \Rightarrow \Pr[k \notin \mathcal{K}_1^*] \leq \varepsilon_1(\lambda)$;
3. $k_0 \in \mathcal{K}_1^*, \ \mathsf{dp} = (\mathbb{G}, G, q, k_0, L, T) \Rightarrow \Pr[\mathsf{Samp}([A], [\mathbf{u}], d, \mathsf{dp}) = \perp] \leq \varepsilon_1(\lambda)$.

Note that the set $\mathcal{K}_1^*$ depends on all inputs of Samp except the SUF key. While this will suffice for our first construction, the second one will require more flexibility on the set of *good* SUF keys. The following Theorem shows how to achieve that at the price of mildly worse parameters, when A is of the form $\mathbf{u} \otimes \mathbf{a} - M$, with M a short matrix. A proof appears in the appendix, Section C.3.

Theorem 6. *For all $(\mathbb{G}, G, q) \in \mathcal{G}_\lambda$, $[\mathbf{u}] \in \mathbb{G}^{\eta_3}$ such that $(0 \neq u_i \neq u_j \ \forall i \neq j)$, $\mathbf{a} \in \mathbb{F}_q^{\eta_2}$ and $d = \mathsf{poly}(\lambda)$, setting*

$$L \geq \log(10\eta_3 d) \qquad T \geq 2^L \cdot (1 + \ln(\eta_3)) + 2d \qquad \nu \geq 2\lambda$$

there exists $\varepsilon_1(\lambda)$ and a set of SUF keys $\widehat{\mathcal{K}}_1^* \subseteq \mathcal{K}_\lambda$:

1. $\varepsilon_1(\lambda) = \sqrt{\frac{1}{2^\nu} + \frac{\nu^2 \eta_3^2 T}{q}}$;
2. $k \leftarrow^{\$} \mathsf{SUF.Gen}(1^\lambda) \Rightarrow \Pr\left[k \notin \widehat{\mathcal{K}}_1^*\right] \leq \varepsilon_1(\lambda)$;
3. *Setting $k_0 \in \widehat{\mathcal{K}}_1^*, \ \mathsf{dp} = (\mathbb{G}, G, q, k_0, L, T)$, for all $\alpha \in \mathbb{F}_q \setminus \{0\}$, and all $M \in \mathbb{F}_q^{\eta_3,\eta_2}$ such that $\|M\|_\infty \leq d$, then*

$$\Pr[\mathsf{Samp}([\mathbf{u} \otimes \mathbf{a} - M], [\alpha\mathbf{u}], d, \mathsf{dp}) = \perp] \leq \varepsilon_1(\lambda).$$

3.4 Preimage Sampler

With the key-switching lemma in mind, $\mathcal{U}^*$ from the previous section represents the domain of one among the two functions we split our (shifted) verification equation into. As informally discussed in the intro, when keys are switched in the security proof, the verification equation takes the following form[14]:

$$B \cdot \delta_2([A_1\mathbf{x}_1 + A_2\mathbf{x}_2 + z\mathbf{u} + \mathbf{x}_1 + M_2\mathbf{x}_2]) = \mathbf{t},$$

[14] in our first scheme, $B = I_{n_1}$ and can be ignored here. In our second scheme instead, B will be a universal hash function in $\mathbb{F}_2^{n_1,n_2}$

where $A_2 = \mathbf{u} \otimes \mathbf{a}_2 - M_1$ and M_1 is chosen in the reduction so that for the punctured message(s) $M_1 \oplus M_2$ is not invertible. Applying Lemma 3, due to $M_1, M_2, \mathbf{x}_1, \mathbf{x}_2$ being short, if the group elements have sufficiently large distance this splits into:

$$B\delta_2([A_1\mathbf{x}_1 + A_2\mathbf{x}_2 + z\mathbf{u}]) \oplus BM_2\mathbf{x}_2 = \mathbf{x}_1 \oplus \mathbf{t}.$$

The goal of this section is to show how to sample $(\mathbf{x}_2, z)$ in a way that is consistent with Samp, provided $\mathbf{a}_2$ (i.e. the second key), and $\mathbf{x}_1$ (which now would be sampled uniformly at random in $\mathbb{F}_2^{\eta_1}$). We call such procedure $\mathsf{PreSamp}$ (detailed in Figure 4) or *preimage sampler* as it returns a uniformly sampled preimage of $\mathbf{x}_1 \oplus \mathbf{t}$ for

$$\begin{aligned} f_2 &: \{(\mathbf{x}_2, z) \in \mathbb{F}_2^{\eta_2} \times \mathbb{F}_q \ : \ \delta_{\mathsf{min}}([\mathbf{v} + A_2\mathbf{x}_2 + z\mathbf{u}]) \geq d\} \to \mathbb{F}_2^{\eta_1} \\ f_2(\mathbf{x}_2, z) \ &= \ B \cdot \delta_2([\mathbf{v} + A_2\mathbf{x}_2 + z\mathbf{u} + M_2\mathbf{x}_2]). \end{aligned}$$

$\mathsf{PreSamp}([\mathbf{v}], [\mathbf{u}], \mathbf{a}, M_1, M_2, B, \mathbf{t}, d, \mathsf{dp})$:

1 : **For** $i \in \{1, \ldots, \nu\}$:
2 : $\quad z_i^* \leftarrow^{\$} \mathbb{F}_q$
3 : $\quad$ // Default to $\mathbf{s}_i = \mathbf{0}$ so line 9 can fail
4 : $\quad$ **If** $\delta_{\mathsf{min}}([\mathbf{v} + z_i^*\mathbf{u}]) = \perp$: $\ \mathbf{s}_i \leftarrow \mathbf{0}$
5 : $\quad$ **If** $\delta_{\mathsf{min}}([\mathbf{v} + z_i^*\mathbf{u}]) \neq \perp$: $\ \mathbf{s}_i \leftarrow \delta_2([\mathbf{v} + z_i^*\mathbf{u}])$
6 : $\quad S_i \coloneqq \{\mathbf{x}_0 \in \mathbb{F}_2^{\eta_2} \ : \ B(M_1 \oplus M_2)\mathbf{x}_0 = B\mathbf{s}_i \oplus \mathbf{t}\}$
7 : $\quad$ **If** $S_i = \varnothing$: **Return** $\perp$
8 : $\quad \mathbf{x}_i \leftarrow^{\$} S_i$
9 : $\quad$ **If** $\delta_{\mathsf{min}}([\mathbf{v} + z_i^*\mathbf{u} - M_1\mathbf{x}_i]) \geq d$:
10 : $\quad\quad$ // Accept the sample, up to shifting z_i^*
11 : $\quad\quad$ **Return** $(\mathbf{x}, z) \leftarrow (\mathbf{x}_i, z_i^* - \mathbf{a}^\top\mathbf{x}_i)$
12 : **Return** $\perp$

Fig. 4: Preimage sampler with $\mathsf{dp} = (\mathbb{G}, G, q, k, L, T)$, $\mathbf{v}, \mathbf{u} \in \mathbb{F}_q^{\eta_3}$, $\mathbf{a} \in \mathbb{F}_q^{\eta_2}$, $M_1, M_2 \in \mathbb{F}_2^{\eta_3, \eta_2}$, $\mathbf{t} \in \mathbb{F}_2^{\eta_1}$ and $d \in \mathbb{N}$.

The proofs of the following theorems appear in appendix, Section C.4.

Theorem 7. *For all $\eta_1 \leq \eta_3 \leq \eta_2$, $(\mathbb{G}, G, q) \in \mathcal{G}_\lambda$, $[\mathbf{u}] \in \mathbb{G}^{\eta_3}$ such that $(0 \neq u_{j_0} \neq u_{j_1} \ \forall j_0 \neq j_1)$, $\mathbf{a} \in \mathbb{F}_q^{\eta_2}$, $d \in \mathbb{N}$, setting*

$$L \geq \log(10\eta_3 d), \qquad T \geq 2^L \cdot (1 + \ln(\eta_3)) + 2d, \qquad \nu \geq 2\lambda$$

there exists $\varepsilon_2(\lambda)$ and a set of SUF keys $\mathcal{K}_2^* \subseteq \mathcal{K}_\lambda$:

1. $\varepsilon_2(\lambda) = \sqrt{\frac{1}{2^\nu} + \frac{\nu^2 \eta_3^2 T}{q}}$
2. $k \leftarrow^{\$} \mathsf{SUF.Gen}(1^\lambda) \Rightarrow \Pr[k \notin \mathcal{K}_2^*] \leq \varepsilon_2(\lambda)$
3. *Setting* $k_0 \in \mathcal{K}_2^*$ *and* $\mathsf{dp} = (\mathbb{G}, G, q, k_0, L, T)$*, then for all* $M_1, M_2 \in \mathbb{N}^{\eta_3, \eta_2}$ *such that* $M_1 \oplus M_2$ *is full rank in* $\mathbb{F}_2^{\eta_3, \eta_2}$ *and* $d \geq \max(\|M_1\|_\infty, \|M_2\|_\infty)$ *, for all* $B \in \mathbb{F}_2^{\eta_1, \eta_3}$ *of rank* η_1 *and for all* $\alpha_1, \alpha_2 \in \mathbb{F}_q$ *(with* $\alpha_2 \neq 0$*),* $\mathbf{t} \in \mathbb{F}_2^{\eta_1}$

$$\Pr[\mathsf{PreSamp}([\alpha_1 \mathbf{u}], [\alpha_2 \mathbf{u}], \mathbf{a}, M_1, M_2, B, \mathbf{t}, d, \mathsf{dp}) = \perp] \leq \varepsilon_2(\lambda).$$

Theorem 8. *For any* $\eta_1 \leq \eta_3 \leq \eta_2$*,* $k \in \mathcal{K}_\lambda$*,* $(\mathbb{G}, G, q) \in \mathcal{G}_\lambda$*,* $[\mathbf{v}], [\mathbf{u}] \in \mathbb{G}^{\eta_3}$*,* $\mathbf{a} \in \mathbb{F}_q^{\eta_2}$*,* $M_1, M_2 \in \mathbb{N}^{\eta_3, \eta_2}$ *such that* $M_1 \oplus M_2$ *is full rank modulo* 2*,* $B \in \mathbb{F}_2^{\eta_1, \eta_3}$ *full rank,* $\mathbf{t} \in \mathbb{F}_2^{\eta_1}$*,* $L, T = \mathsf{poly}(\lambda)$ *and* $d \geq \max(\|M_1\|_\infty, \|M_2\|_\infty)$*, let* $(\mathbf{x}, z) \leftarrow^{\$} \mathsf{PreSamp}([\mathbf{v}], [\mathbf{u}], \mathbf{a}, M_1, M_2, B, \mathbf{t}, d, \mathsf{dp})$*. Then conditioning on* $(\mathbf{x}, z) \neq \perp$ *we have that* $(\mathbf{x}, z)$ *is uniform over*

$$\left\{ (\mathbf{x}_0, z_0) \in \mathbb{F}_2^{\eta_2} \times \mathbb{F}_q \;\middle|\; \begin{array}{l} \delta_{\mathsf{min}}([\mathbf{v} + A\mathbf{x}_0 + z_0 \mathbf{u}]) \geq d \\ B\delta_2([\mathbf{v} + A\mathbf{x}_0 + z_0 \mathbf{u} + M_2 \mathbf{x}_0]) = \mathbf{t} \end{array} \right\}$$

where $A = \mathbf{u} \otimes \mathbf{a} - M_1 \in \mathbb{F}_q^{\eta_3, \eta_2}$*.*

4 Selectively Secure Short Signatures from DDH

4.1 Construction

We are now ready to present our *selectively secure* construction based on DDH. The scheme, detailed in Figure 5, is based on a family of functions F_m (defined by a set of public parameters in the verification key) such that

- F_m is preimage sampleable for all but one m;
- public parameters can be generated so that for a secret m^*, F_{m^*} has image size *sparse* in its domain.

We abuse terminology and refer to the second property as F_{m^*} being *lossy*[15] Given such F_m and a target output $\mathbf{t}$ in vk, a signature for m is a preimage of $\mathbf{t}$ for F_m. The verifier simply checks $F_m(\sigma) = \mathbf{t}$. Security is argued by programming F_{m^*} to be lossy, with m^* being the message selected by the adversary, so that w.h.p. no preimage for $\mathbf{t}$ exists. More in details, the function F_m is determined by: a group $\mathbb{G}$; a vector $\mathbf{u} \in \mathbb{F}_q^{n_1}$; two matrices with *large* entries $A_1, A_2 \in \mathbb{F}_q^{n_1, n_2}$ of the form $A_i = \mathbf{u} \otimes \mathbf{a}_i$; two *binary* matrices B_1, B_2 acting as UHF (see Section 2.3); a distance function δ. Given these $F_m : \mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \mathbb{F}_q \to \mathbb{F}_2^{n_1}$ is defined as

$$F_m(\mathbf{x}_1, \mathbf{x}_2, z) \;=\; \delta_2([A_1 \mathbf{x}_1 + A_2 \mathbf{x}_2 + z\mathbf{u} + \mathbf{x}_1 + M\mathbf{x}_2])$$

where $M = B_1 \oplus (P_m B_2)$, see Section 2.5 for the definition of P_m. All the parameters are specified in Table 2.

[15] For all m in fact F_m is an (almost) surjective function which already loses some information. However F_{m^*} crucially loses $\Theta(\lambda)$ additional bits.

Par.	Value	Description
λ	–	security parameter
μ	2λ	supported message length
q	–	group order
n_1	$\lambda + \log q$	first trapdoor bit length
n_2	$5\lambda + 2\log q + \log(4\lambda)$	second trapdoor bit length
ν	2λ	rejection-sampling repetitions
L	$\log(10n_1d)$	SUF output length for δ
T	$10n_1d \cdot (1 + \ln(n_1)) + 2d$	maximum supported distance in δ
d	$n_2 + 1$	distance

Table 2: parameters for the *selectively* secure scheme.

Preimage sampling. In order to find a preimage for a vector $\mathbf{t}$ we rely on the homomorphic properties of δ_2 and the fact that $[A_1], [A_2], [\mathbf{u}]$ defines a chameleon hash. The goal will be to disentangle $\mathbf{x}_1$ from $\mathbf{x}_2, z$. To do so, let us restrict the domain of F_m to those inputs for which $A_1\mathbf{x}_1 + A_2\mathbf{x}_2 + z\mathbf{u}$ has large enough minimum distance w.r.t. δ. Then F_m can be rewritten as

$$F_m(\mathbf{x}_1, \mathbf{x}_2, z) \;=\; \delta_2\left([A_1\mathbf{x}_1 + A_2\mathbf{x}_2 + z\mathbf{u}]\right) \oplus M\mathbf{x}_2 \oplus \mathbf{x}_1$$

Next, knowing $\mathbf{a}_1$, we can consider the following domain shift $z^* = z + \mathbf{a}_1^\top \mathbf{x}_1$. Calling F_m^* the function

$$F_m^*(\mathbf{x}_1, \mathbf{x}_2, z) \;=\; \delta_2\left([A_2\mathbf{x}_2 + z\mathbf{u}]\right) \oplus M\mathbf{x}_2 \oplus \mathbf{x}_1,$$

we can see that $F_m^*(\mathbf{x}_1, \mathbf{x}_2, z^*) = F_m(\mathbf{x}_1, \mathbf{x}_2, z)$. In order to find a preimage for $\mathbf{t}$ then it suffices to sample $(\mathbf{x}_2, z^*)$ with a large enough minimum distance through Samp (see Section 3.3), find the right $\mathbf{x}_1$ that makes $F_m^*(\mathbf{x}_1, \mathbf{x}_2, z^*) = \mathbf{t}$, and finally undo the shift by setting $z = z^* - \mathbf{a}_1^\top \mathbf{x}_1$.

Lossier mode in one point. Given m^*, we can program the public parameters so that F_{m^*} is lossier. To do so, we set $A_1 = \mathbf{u} \otimes \mathbf{a}_1 - I$ and $A_2 = \mathbf{u} \otimes \mathbf{a}_2 - M^*$ where $M^* = B_1 \oplus (P_{m^*}B_2)$. This parameter choice gives us that $F_{m^*}(\mathbf{x}_1, \mathbf{x}_2, z) =$

$$\begin{aligned} &= \delta_2\left([(\mathbf{u} \otimes \mathbf{a}_1 \cdot \mathbf{x}_1 + \mathbf{u} \otimes \mathbf{a}_2 \cdot \mathbf{x}_2 + z\mathbf{u})]\right) \\ &= \delta_2\left(\left[(\mathbf{a}_1^\top \mathbf{x}_1 + \mathbf{a}_2^\top \mathbf{x}_2 + z) \cdot \mathbf{u}\right]\right) \end{aligned}$$

which has image size at most q. Setting $\mathbf{t} \in \mathbb{F}_2^{n_1}$ to have length $\log q + \lambda$, the image of F_{m^*} is indeed sparse. Showing how to simulate signatures with this new key relies on a combination of DDH hybrids to adapt each matrix and the Key Switching Lemma (Lemma 1), we defer the details to the proof of Theorem 10.

4.2 Correctness

Theorem 9. *If* SUF *is* $(\nu n_1 T)$*-universal, then the signature scheme in Figure 5 with parameters as in Table 2 is correct.*

$\mathsf{S.Gen}(1^\lambda)$:

1 : $(\mathbb{G}, G, q) \leftarrow^{\$} \mathsf{G.Gen}(1^\lambda)$
2 : $\mathbf{u} \leftarrow^{\$} \mathbb{F}_q^{n_1}$
3 : $\mathbf{a}_1 \leftarrow^{\$} \mathbb{F}_q^{n_1}$, $\mathbf{a}_2 \leftarrow^{\$} \mathbb{F}_q^{n_2}$
4 : $A_i \leftarrow \mathbf{u} \otimes \mathbf{a}_i$
5 : $\mathbf{t} \leftarrow^{\$} \mathbb{F}_2^{n_1}$
6 : $B_1, B_2 \leftarrow^{\$} \mathbb{F}_2^{n_1, n_2}$
7 : $k \leftarrow^{\$} \mathsf{SUF.Gen}(1^\lambda)$
8 : $\mathsf{vk} = ([A_1], [A_2], [\mathbf{u}], \mathbf{t}, B_1, B_2, k, \mathbb{G})$
9 : $\mathsf{sk} = (\mathsf{vk}, \mathbf{a}_1)$
10 : **Return** $(\mathsf{vk}, \mathsf{sk})$

$\mathsf{S.Sign}(\mathsf{sk}, m)$: // $m \in \mathbb{F}_2^\mu$

1 : Set $\mathsf{dp} = (\mathbb{G}, G, q, k, L, T)$, $\delta = \delta_{\mathsf{dp}}$.
2 : Set $M = B_1 \oplus (P_m B_2)$ // $\in \mathbb{F}_2^{n_1, n_2}$
3 : $(\mathbf{x}_2, z^*) \leftarrow^{\$} \mathsf{Samp}([A_2], [\mathbf{u}], d, \mathsf{dp})$
4 : **If** $(\mathbf{x}_2, z^*) = \perp$: **Return** $\perp$
5 : $\mathbf{x}_1 \leftarrow \delta_2([A_2\mathbf{x}_2 + z^*\mathbf{u}]) \oplus M\mathbf{x}_2 \oplus \mathbf{t}$
6 : $z \leftarrow z^* - \mathbf{a}_1^\top \mathbf{x}_1$
7 : **Return** $\sigma = (\mathbf{x}_1, \mathbf{x}_2, z)$

$\mathsf{S.Vfy}(\mathsf{vk}, m, \sigma)$:

1 : Set $\mathsf{dp} = (\mathbb{G}, G, q, k, L, T)$, $\delta = \delta_{\mathsf{dp}}$ and $M = B_1 \oplus (P_m B_2)$
2 : Parse $\sigma = (\mathbf{x}_1, \mathbf{x}_2, z)$ // $\in \mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \mathbb{F}_q$
3 : $b \leftarrow (\delta_2([A_1\mathbf{x}_1 + A_2\mathbf{x}_2 + z\mathbf{u} + \mathbf{x}_1 + M\mathbf{x}_2]) == \mathbf{t})$
4 : **Return** b

Fig. 5: Selectively secure signature from DDH. f_k is $(\nu n_1 T)$-universal.

Proof. The proof consists of three parts: (1) use the results in Section 3.4 to identify a set of good SUF keys; (2) show that a signature is accepting unless $(\mathbf{x}_2, z^*) = \perp$ in the signing procedure, line 4; (3) prove the latter event occurs with negligible probability that is independent from the given message.

Regarding the first step, as per Table 2 we have $L > \log(5n_1 d)$ and $T > 2^L \cdot (1 + \ln(n_1)) + d$. Given $(\mathsf{vk}, \mathsf{sk}) \leftarrow^{\$} \mathsf{S.Gen}(1^\lambda)$, up to negligible probability we have $0 \neq u_i \neq u_j$ for all $i \neq j$. Therefore, conditioning on $\mathbf{u}$ satisfying the above conditions, there exist a negligible $\varepsilon_1(\lambda)$ and a set $\mathcal{K}_1^* \subseteq \mathcal{K}_\lambda$ satisfying the three conditions of Theorem 5. Next we observe that for any $m \in \mathcal{M}_\lambda$ and $\sigma \leftarrow^{\$} \mathsf{S.Sign}(\mathsf{sk}, m)$, if $\sigma \neq \perp$ then the verifier accepts. Indeed by Theorem 4 $(\mathbf{x}_2, z^*) \neq \perp$ implies that $\delta([A_2\mathbf{x}_2 + z^*\mathbf{u}]) \geq d$. Calling $\sigma = (\mathbf{x}_1, \mathbf{x}_2, z)$ and $M = B_1 \oplus P_m B_2$ then we get by construction that

$$\begin{aligned}
\delta_2([A_1\mathbf{x}_1 + A_2\mathbf{x}_2 + z\mathbf{u} + M\mathbf{x}_2 + \mathbf{x}_1]) &= \delta_2([(\mathbf{u} \otimes \mathbf{a}_1)\mathbf{x}_1 + A_2\mathbf{x}_2 + z\mathbf{u} + M\mathbf{x}_2]) \\
&= \delta_2(\left[A_2\mathbf{x}_2 + (\mathbf{a}_1^\top \mathbf{x}_1 + z)\mathbf{u} + M\mathbf{x}_2 + \mathbf{x}_1\right]) \\
&= \delta_2([A_2\mathbf{x}_2 + z^*\mathbf{u} + M\mathbf{x}_2 + \mathbf{x}_1]) \\
&= \delta_2([A_2\mathbf{x}_2 + z^*\mathbf{u}]) \oplus M\mathbf{x}_2 \oplus \mathbf{x}_1 \;=\; \mathbf{t}
\end{aligned}$$

where the first equality follows as $A_1 = \mathbf{u} \otimes \mathbf{a}_1$, the second by definition of $\otimes$ (see Section 2.1), the third by the definition of z. Fourth equality is by Lemma 3 as $\|M\mathbf{x}_2 + \mathbf{x}_1\|_\infty \leq n_2 + 1 = d$. The last follows by construction of $\mathbf{x}_1$. Hence $\mathsf{S.Vfy}(\mathsf{vk}, \sigma, m) \to 1$ if $\sigma \neq \perp$. For ease of notation, let Good be the set of "good"

vectors $\mathbf{u}$, i.e. the vectors satisfying $u_i \neq 0$ for all i and $u_i \neq u_j$ for all $i \neq j$. We can bound $\Pr[\mathsf{S.Vfy}(\mathsf{vk}, \sigma, m) = 0] \leq \Pr[\sigma = \perp] \leq$

$$\leq \sum_{\bar{A}_2} \sum_{\bar{\mathbf{u}} \in \mathsf{Good}} \Pr\left[\sigma = \perp | A_2 = \bar{A}_2, \mathbf{u} = \bar{\mathbf{u}}\right] \Pr\left[A_2 = \bar{A}_2, \mathbf{u} = \bar{\mathbf{u}}\right] + \Pr[\mathbf{u} \notin \mathsf{Good}].$$

Due to Theorem 5, for fixed $\bar{A}_2$ and $\bar{\mathbf{u}}$ we bound $\Pr\left[\sigma = \perp | A_2 = \bar{A}_2, \mathbf{u} = \bar{\mathbf{u}}\right] \leq$

$$\Pr\left[\sigma = \perp | A_2 = \bar{A}_2, \mathbf{u} = \bar{\mathbf{u}}, k \in \mathcal{K}_1^*\right] + \Pr[k \notin \mathcal{K}_1^*] \leq 2\varepsilon_1(\lambda)$$

whereas $\Pr[\mathbf{u} \notin \mathsf{Good}]$ can be bounded above by $\frac{n_1(n_1+1)}{2q}$. Considering that $\varepsilon_1(\lambda)$ does not depend on $\bar{A}_2$ or $\bar{\mathbf{u}}$ can thus bound the probability of failure by

$$2\varepsilon_1(\lambda) + n_1(n_1+1)/2q. \qquad \square$$

4.3 Unforgeability

Theorem 10. *If DDH is hard for* $\mathsf{G.Gen}$ *and* SUF *is* $(\nu n_1 T)$*-universal, then the signature scheme in Figure 5 with parameters as in Table 2 is selectively unforgeable under chosen message attacks.*

Proof. We prove the theorem through a sequence of hybrids. Informally, we can break up the proof into four main steps, calling m^* the message our selective adversary tries to forge. Initially, using $\mathbf{a}_1$ trapdoor for A_1 to sign, we *puncture* A_2 in m^*. Next, we switch to a signing procedure that relies on $\mathbf{a}_2$ trapdoor for A_2 to sign all messages but m^*. Third, we modify A_1 so that *no message* can be signed using its trapdoor (while all but m^* can still be signed with A_2). Finally, we show that up to negligible probability there exists no valid signature for m^* in the last hybrid. For the two transformation of A_2 and A_1 we make use of MDDH along with Lemma 9 and 10.

Formally, given a PPT adversary $\mathcal{A}$, we define the following hybrids:

- H_1: Real SUF-CMA game;
- H_2: As H_1, but sample A_2 uniformly in $\mathbb{F}_q^{n_1, n_2}$;
- H_3: As H_2, but, after $m^* \leftarrow^{\$} \mathcal{A}(1^\lambda)$, set in the signature's verification key $A_2 \leftarrow \mathbf{u} \otimes \mathbf{a}_2 - M^*$ with $M^* = B_1 + P_{m^*} B_2$;
- H_4: As H_3, but $\mathsf{sk}^* = (\mathsf{vk}, \mathbf{a}_1, \mathbf{a}_2)$ and $\mathcal{O}_{\mathsf{sk}^*, Q}(m)$ returns $\mathsf{S.Sign}((\mathsf{vk}, \mathbf{a}_1), m)$;
- H_5: As H_4, but $\mathcal{O}_{\mathsf{sk}^*, Q}(m)$ returns $\sigma \leftarrow^{\$} \mathsf{S.Sign2}(\mathsf{sk}^*, m^*, m)$ as in Figure 6;
- H_6: As H_5, but sample A_1 uniformly in $\mathbb{F}_q^{n_1, n_1}$;
- H_7: As H_6, but set $A_1 \leftarrow \mathbf{u} \otimes \mathbf{a}_1 - I$;

In the following we will show $\mathsf{H}_1, \mathsf{H}_2, \mathsf{H}_3$ are computationally indistinguishable under the MDDH assumption (Definition 7), $\mathsf{H}_3, \mathsf{H}_4$ are identical up to syntactical changes, $\mathsf{H}_4, \mathsf{H}_5$ are statistically indistinguishable, while $\mathsf{H}_5, \mathsf{H}_6, \mathsf{H}_7$ are indistinguishable again under the MDDH assumption. Finally we will prove that up to negligible probability, there exists no valid signature for m^* in H_7.

$\mathsf{S.Sign2}(\mathsf{sk}^*, m^*, m)$:

1 : Parse $\mathsf{sk}^* = (\mathsf{vk}, \mathbf{a}_1, \mathbf{a}_2)$
2 : Parse $\mathsf{vk} = ([A_1], [A_2], [\mathbf{u}], \mathbf{t}, B_1, B_2, k, \mathbb{G})$
3 : $\mathsf{dp} \leftarrow (\mathbb{G}, G, q, k, L, T)$ // deriving G, q from $\mathbb{G}$
4 : $\mathbf{x}_1 \leftarrow^{\$} \mathbb{F}_2^{n_1}$
5 : $\mathbf{v} \leftarrow A_1\mathbf{x}_1$ // $\in \mathbb{F}_q^{n_1}$
6 : $M^* \leftarrow B_1 \oplus P_{m^*}B_2$ // $\in \mathbb{F}_2^{n_1,n_2}$
7 : $M \leftarrow B_1 \oplus P_mB_2$ // $\in \mathbb{F}_2^{n_1,n_2}$
8 : $(\mathbf{x}_2, z) \leftarrow^{\$} \mathsf{PreSamp}([\mathbf{v}], [\mathbf{u}], \mathbf{a}_2, M^*, M, I, \mathbf{t} \oplus \mathbf{x}_1, d, \mathsf{dp})$ // $I \in \mathbb{F}_2^{n_1,n_1}$
9 : **Return** $\sigma = (\mathbf{x}_1, \mathbf{x}_2, z)$

Fig. 6: Alternative signature scheme using $\mathbf{a}_2$ to sign any $m \neq m^*$.

Indistinguishability of $\mathsf{H}_1, \mathsf{H}_2$. Let $\mathcal{D}$ be a distinguisher for $\mathsf{H}_1, \mathsf{H}_2$. In Figure 7 we describe a reduction $\mathcal{B}_1(\mathbb{G}, [C])$ to $(n_1, n_2 + 1)$-MDDH. Initially, it executes $\mathcal{D}$ and waits for m^*. Next, in order to generate vk, sk, it sets $[\mathbf{u}]$ as the first column of $[C]$ and $[A_2]$ as the remaining n_2 columns. $[A_1]$ is set as $[\mathbf{u} \otimes \mathbf{a}_1]$, which can be computed given only $[\mathbf{u}]$ and sampling $\mathbf{a}_1$. The remaining public key entries are sampled as per $\mathsf{S.Gen}$, and signing queries are answered via $\mathsf{S.Sign}((\mathsf{vk}, \mathbf{a}_1), m)$. Note neither $\mathbf{u}$ nor $\mathbf{a}_2$ are required to sign. Finally it returns the same bit returned by $\mathcal{D}$.

$\mathcal{B}_1(\mathbb{G}, [C])$: // $[C] \in \mathbb{G}^{n_1,n_2+1}$

1 : Run $m^* \leftarrow^{\$} \mathcal{D}(1^\lambda)$
2 : Derive $(\mathbb{G}, G, q)$ from $\mathbb{G}$ and parse $[C] = [\mathbf{u}], [A_2] \in \mathbb{G}^{n_1} \times \mathbb{G}^{n_1,n_2}$
3 : $\mathbf{a}_1 \leftarrow^{\$} \mathbb{F}_q^{n_1}$, $[A_1] \leftarrow [\mathbf{u} \otimes \mathbf{a}_1]$, $\mathbf{t} \leftarrow^{\$} \mathbb{F}_2^{n_1}$, $B_1, B_2 \leftarrow^{\$} \mathbb{F}_2^{n_1,n_2}$ and $k \leftarrow^{\$} \mathsf{SUF.Gen}(1^\lambda)$
4 : $\mathsf{vk} = ([A_1], [A_2], [\mathbf{u}], \mathbf{t}, B_1, B_2, k, \mathbb{G})$ and $\mathsf{sk} = (\mathsf{vk}, \mathbf{a}_1)$
5 : Run $\mathcal{D}(1^\lambda, \mathsf{vk})$
6 : **When** $\mathcal{D}$ queries $m \in \{0,1\}^\mu$: Send $\sigma \leftarrow^{\$} \mathsf{S.Sign}(\mathsf{sk}, m)$ to $\mathcal{D}$
7 : **When** $\mathcal{D}$ returns b: **Return** b

Fig. 7: Reduction of the indistinguishability of $\mathsf{H}_1, \mathsf{H}_2$ to $(n_1, n_2 + 1)$-MDDH.

Using Lemma 9 and 10, it suffices to study the advantage of $\mathcal{B}_1$ in distinguishing a uniform C_0 from C_1 of the form $\mathbf{u} \otimes (1, \mathbf{v})$ with uniform $\mathbf{u} \in \mathbb{F}_q^{n_1}$, $\mathbf{v} \in \mathbb{F}_q^{n_2}$. First, when $C = C_0$ is uniform, so is $\mathbf{u}$ and A_2 as in H_2. The remaining components of the verification key and secret key $\mathbf{a}_1, \mathbf{t}, B_1, B_2, k$ are sampled correctly and independently from $\mathbf{u}, A_2$, and $A_1 = \mathbf{u} \otimes \mathbf{a}_1$. Hence

$$\Pr\left[1 \leftarrow \mathcal{B}_1(\mathbb{G}, [C_0])\right] \;=\; \Pr\left[1 \leftarrow \mathcal{D}^{\mathsf{H}_2}(1^\lambda)\right].$$

Conversely, when $C = C_1$ then $C = (\mathbf{u}, \mathbf{u} \otimes \mathbf{a}_2)$ for uniformly sampled $\mathbf{u}, \mathbf{a}_2$. In particular $[\mathbf{u}]$ and $[A_2] = [\mathbf{u} \otimes \mathbf{a}_2]$ are correctly distributed as in H_1. As before, the remaining public and secret key components, as well as signature queries, are also correctly sampled. Thus $\Pr[1 \leftarrow \mathcal{B}_1(\mathbb{G}, [C_1])] = \Pr\left[1 \leftarrow \mathcal{D}^{\mathsf{H}_1}(1^\lambda)\right]$ implies that $\mathsf{Adv}^{\mathsf{H}_1,\mathsf{H}_2}_{\mathcal{D}}(\lambda) = \mathsf{Adv}_{\mathcal{B}_1}(\lambda) \leq \mathsf{negl}(\lambda)$.

Indistinguishability of $\mathsf{H}_2, \mathsf{H}_3$. We again reduce a distinguisher $\mathcal{D}$ to an adversary $\mathcal{B}_2$ for (n_1, n_2+1)-MDDH. Initially it gets m^* the challenge message from $\mathcal{D}(1^\lambda)$. Then, it samples all public and secret key component $\mathbf{a}_1, \mathbf{t}, B_1, B_2, k$ with the exception of $[\mathbf{u}], [A_1], [A_2]$. To complete vk, given $[C] \in \mathbb{G}^{n_1,n_2+1}$, it separates the first column from the rest, i.e. parsing $C = \mathbf{c}_0 || C^*$ with $\mathbf{c}_0 \in \mathbb{F}_q^{n_1}$ and $C^* \in \mathbb{F}_q^{n_1,n_2}$. The first column is set to $[\mathbf{u}] = [\mathbf{c}_0]$, while $[A_2] = [C^* - M^*]$ with $M^* = B_1 \oplus (P_{m^*} B_2)$. Finally $[A_1] = [\mathbf{u} \otimes \mathbf{a}_1]$. Signature queries are then answered with $\mathsf{sk} = (\mathsf{vk}, \mathbf{a}_1)$ as prescribed in both games.

$\mathcal{B}_2(\mathbb{G}, [C])$: // $[C] \in \mathbb{G}^{n_1,n_2+1}$

1 : Run $m^* \leftarrow^{\$} \mathcal{D}(1^\lambda)$
2 : Derive $(\mathbb{G}, G, q)$ from $\mathbb{G}$
3 : $\mathbf{t} \leftarrow^{\$} \mathbb{F}_2^{n_1}$, $B_1, B_2 \leftarrow^{\$} \mathbb{F}_2^{n_1,n_2}$ and $k \leftarrow^{\$} \mathsf{SUF.Gen}(1^\lambda)$, $M^* \leftarrow B_1 \oplus (P_{m^*} B_2)$
4 : Parse $[C] = [\mathbf{c_0}], [C^*] \in \mathbb{G}^{n_1} \times \mathbb{G}^{n_1,n_2}$. Set $[\mathbf{u}] = [\mathbf{c}_0]$ and $[A_2] = [C^* - M^*]$
5 : $\mathbf{a}_1 \leftarrow^{\$} \mathbb{F}_q^{n_1}$, $[A_1] \leftarrow [\mathbf{u} \otimes \mathbf{a}_1]$
6 : $\mathsf{vk} = ([A_1], [A_2], [\mathbf{u}], \mathbf{t}, B_1, B_2, k, \mathbb{G})$ and $\mathsf{sk} = (\mathsf{vk}, \mathbf{a}_1)$
7 : Run $\mathcal{D}(1^\lambda, \mathsf{vk})$
8 : **When** $\mathcal{D}$ queries $m \in \{0,1\}^\mu$: Send $\sigma \leftarrow^{\$} \mathsf{S.Sign}(\mathsf{sk}, m)$ to $\mathcal{D}$
9 : **When** $\mathcal{D}$ returns b: **Return** b

Fig. 8: Reduction of the indistinguishability of $\mathsf{H}_2, \mathsf{H}_3$ to $(n_1, n_2 + 1)$-MDDH.

It is easy to see that in both game, $\mathbf{a}_1, \mathbf{t}, B_1, B_2, k, \mathbb{G}$ are identically distributed, and $[A_1] = [\mathbf{u} \otimes \mathbf{a}_1]$ is computed as prescribed. Using Lemma 9 and 10 it suffices to study the advantage with which $\mathcal{B}_2$ distinguishes a uniform C_0 from $C_1 = (\mathbf{u} \otimes (1, \mathbf{v}))$ for uniform $\mathbf{u}, \mathbf{v}$. When $C = C_0$ is uniformly distributed, then so are both $\mathbf{c}_0$ and C^*. In particular $\mathbf{u}, A_2 = C^* - M^*$ are uniformly distributed (note C_0 and (m^*, B_1, B_2) are independently distributed). Thus $\mathcal{B}_1$ perfectly simulates H_2. Conversely, when $C = C_1 = (\mathbf{u}, \mathbf{u} \otimes \mathbf{a}_2)$ we have that $[\mathbf{u}]$ and $[A_2] = (\mathbf{u} \otimes \mathbf{a}_2) - M^*$ are computed as prescribed. Thus $\mathcal{B}_2$ perfectly simulates H_3 in this case. In particular

$$\mathsf{Adv}^{\mathsf{H}_2,\mathsf{H}_3}_{\mathcal{D}}(\lambda) \;\leq\; \mathsf{Adv}_{\mathcal{B}_2}(\lambda) \;\leq\; \mathsf{negl}(\lambda).$$

Indistinguishability of $\mathsf{H}_3, \mathsf{H}_4$. The change is only syntactic as both vk and the signatures distribution are not affected by the larger secret key.

Indistinguishability of $\mathsf{H}_4, \mathsf{H}_5$. Let $\mathcal{D}$ be a possibly unbounded distinguisher for the two games. Without loss of generality, we assume it to always make exactly $\vartheta = \mathsf{poly}(\lambda)$ signature queries. The final bit it returns interacting with either H_4 or H_5 is a *deterministic* function of its view, that is respectively

$$\begin{aligned}\mathsf{H}_4 &: (\rho, [A_1], [A_2], [\mathbf{u}], \mathbf{t}, B_1, B_2, k, \mathbb{G}, \sigma_1, \ldots, \sigma_\vartheta),\\ \mathsf{H}_5 &: \left(\widehat{\rho}, [\widehat{A}_1], [\widehat{A}_2], [\widehat{\mathbf{u}}], \widehat{\mathbf{t}}, \widehat{B}_1, \widehat{B}_2, \widehat{k}, \widehat{\mathbb{G}}, \widehat{\sigma}_1, \ldots, \widehat{\sigma}_\vartheta\right)\end{aligned}$$

where $\rho, \widehat{\rho}$ are $\mathcal{D}$'s random coins. To show $\mathsf{Adv}^{\mathsf{H}_4,\mathsf{H}_5}_{\mathcal{D}}(\lambda)$ is negligible, it then suffices to show that the two views have negligible statistical distance. To further simplify our task we study the vectors

$$\begin{aligned}\mathsf{view} &\coloneqq (\rho, \mathbf{a}_1, \mathbf{a}_2, \mathbf{u}, \mathbf{t}, M^*, B_2, k, \mathbb{G}, \sigma_1, \ldots, \sigma_\vartheta)\\ \widehat{\mathsf{view}} &\coloneqq \left(\widehat{\rho}, \widehat{\mathbf{a}}_1, \widehat{\mathbf{a}}_2, \widehat{\mathbf{u}}, \widehat{\mathbf{t}}, \widehat{M^*}, \widehat{B}_2, \widehat{k}, \widehat{\mathbb{G}}, \widehat{\sigma}_1, \ldots, \widehat{\sigma}_\vartheta\right)\end{aligned}$$

Note the actual view is a function of the above, as m^* is a deterministic function of ρ, $M^* = B_1 \oplus (P_{m^*} B_2)$, $[A_1] = [\mathbf{u} \otimes \mathbf{a}_1]$, $[A_2] = [\mathbf{u} \otimes \mathbf{a}_2 - M^*]$. Hence $\Delta(\mathsf{view}, \widehat{\mathsf{view}})$ upper bound the statistical distance of the vectors above.

We now proceed via Lemma 4 studying the entries of view one by one.

$\mathsf{H}_4 \approx_s \mathsf{H}_5$*: Trivial Components.* First, we observe that in both games $\rho, \widehat{\rho}$ follows the same distribution, and, conditioning on $\rho = \rho_0 = \widehat{\rho}$, m^* becomes a constant and therefore $\mathbf{a}_1, \mathbf{a}_2, \mathbf{u}, M^*, \mathbf{t}, \mathbb{G}$ are identically distributed. For ease of notation, define a "partial view" vector $\mathsf{pv}^* = (\rho, \mathbf{a}_1, \mathbf{a}_2, \mathbf{u}, \mathbf{t}, M^*, \mathbb{G})$ and $\widehat{\mathsf{pv}}^* = (\widehat{\rho}, \widehat{\mathbf{a}}_1, \widehat{\mathbf{a}}_2, \widehat{\mathbf{u}}, \widehat{\mathbf{t}}, \widehat{M^*}, \widehat{\mathbb{G}})$. To proceed we condition on $\mathsf{pv}^* = \mathsf{pv}^*_0 = \widehat{\mathsf{pv}}^*$ such that $\mathbf{u}$ satisfies $u_i \neq u_j \neq 0$. Since $\mathbf{u}$ is uniformly sampled and independent from the other components

$$\Pr\left[\exists i : u_i = 0 \ \vee \ \exists i \neq j : u_i = u_j\right] \ \leq \ n_1(n_1+1)/2q.$$

$\mathsf{H}_4 \approx_s \mathsf{H}_5$*: SUF key.* $k, \widehat{k}$ both follow the distribution induced by $\mathsf{SUF.Gen}(1^\lambda)$ and are independent from the components in $\mathsf{pv}^*, \widehat{\mathsf{pv}}^*$. To proceed we condition on a set of good keys, which we hit with overwhelming probability. Let $\mathcal{K}^*_1, \mathcal{K}^*_2$ respectively be as per Theorem 5 and Theorem 7, and respectively uniquely defined given $([A_2], [\mathbf{u}], d, \mathsf{dp})$ in the first case and $([\mathbf{u}], \mathbf{a}_2, d, \mathsf{dp})$ in the second. Then we proceed conditioning on $k = k_0 = \widehat{k}$ with $k_0 \in \mathcal{K}^*_1 \cap \mathcal{K}^*_2$. By Theorem 5 and 7 $\Pr\left[k \notin \mathcal{K}^*_1 \cap \mathcal{K}^*_2 \mid \mathsf{pv}^* = \mathsf{pv}^*_0\right] =$

$$= \ \Pr\left[k \notin \mathcal{K}^*_1 \cap \mathcal{K}^*_2\right] \ \leq \ \Pr\left[k \notin \mathcal{K}^*_1\right] + \Pr\left[k \notin \mathcal{K}^*_2\right] \ \leq \ \varepsilon_1(\lambda) + \varepsilon_2(\lambda).$$

$\mathsf{H}_4 \approx_s \mathsf{H}_5$*: UHF keys.* Next, given $\mathsf{pv}^* = \mathsf{pv}_0 = \widehat{\mathsf{pv}}^*$ and $k = k_0 = \widehat{k}$ with the previous constraints, we study the distribution of $B_2, \widehat{B}_2$. Both are independently distributed from $\rho, \mathbf{a}_1, \mathbf{a}_2, \mathbf{u}, k$. Moreover, since $B_1, \widehat{B}_1$ are uniformly random, they are independent from $M^* = B_1 \oplus P_{m^*} B_2$ and $\widehat{M^*} = \widehat{B}_1 \oplus P_{m^*} \widehat{B}_2$ respectively. Thus, under the above conditions, they have zero statistical distance.

Finally, we define the following sets:

$$\begin{aligned}
\mathcal{U}^* &= \{(\mathbf{x}, z^*) \in \mathbb{F}_2^{n_2} \times \mathbb{F}_q \,:\, \delta_{\mathsf{min}}([A_2\mathbf{x} + z^*\mathbf{u}]) \geq d\} \\
\mathcal{B}_1 &= \{B \in \mathbb{F}_2^{n_1,n_2} \,:\, \mathsf{rk}(B) = n_1\} \\
\mathcal{B}_2 &= \left\{ B \in \mathbb{F}_2^{n_1,n_2} \,:\, \begin{array}{l} (\mathbf{x}, z^*) \leftarrow^{\$} \mathcal{U}^*,\ \mathbf{s} \leftarrow^{\$} \mathbb{F}_2^{n_1} \\ \Delta((\mathbf{a}_2^\top \mathbf{x} + z^*, B\mathbf{x}), (\mathbf{a}_2^\top \mathbf{x} + z^*, \mathbf{s})) \leq 2^{-\lambda} \end{array} \right\}
\end{aligned}$$

Using the Leftover Hash Lemma we can prove B_2 almost always lies in $\mathcal{B}_2$. The full argument appears in the appendix, Section D.1.

Claim 1. $\Pr\left[B_2 \notin \mathcal{B}_2 | \mathsf{pv}^* = \mathsf{pv}_0^*,\ k = k_0\right] \leq 2^{-\lambda}$

We conclude that $\Pr\left[B_2 \notin \mathcal{B}_1 \cap \mathcal{B}_2 \,|\, \mathsf{pv}^* = \mathsf{pv}_0^*,\ k = k_0\right] \leq$

$$\begin{aligned}
&\leq \Pr\left[B_2 \notin \mathcal{B}_1 \,|\, \mathsf{pv}^* = \mathsf{pv}_0^*,\ k = k_0\right] + \Pr\left[B_2 \notin \mathcal{B}_2 \,|\, \mathsf{pv}^* = \mathsf{pv}_0^*,\ k = k_0\right] \\
&\leq 2^{n_2 - n_1} + 2^{-\lambda} \ \leq\ 2 \cdot 2^{-\lambda}
\end{aligned}$$

where in the second inequality, the upper bound on the first term follows by Lemma 9, while the last inequality holds as by construction $n_2 \geq n_1 + \lambda$. We can therefore condition on $B_2 = B_{2,0} = \widehat{B}_2 \in \mathcal{B}_1 \cap \mathcal{B}_2$.

$\mathsf{H}_4 \approx_s \mathsf{H}_5$*: Signatures.* Let $\mathsf{pv}_i = (\mathsf{pv}^*, k, B_2, \sigma_1, \ldots, \sigma_{i-1})$ and analogously $\widehat{\mathsf{pv}}_i = (\widehat{\mathsf{pv}}^*, \widehat{k}, \widehat{B}_2, \widehat{\sigma}_1, \ldots, \widehat{\sigma}_{i-1})$. We will show that for any $\sigma_{1,0}, \ldots, \sigma_{i-1,0}$, and $\mathsf{pv}_0^*, k_0, B_{2,0}$ as before, then calling $\mathsf{pv}_{i,0} = (\mathsf{pv}_0^*, k_0, B_{2,0}, \sigma_{1,0}, \ldots, \sigma_{i-1,0})$ we claim (see the Appendix, Section D.1 for a proof).

Claim 2. $\Delta(\sigma_{i|\mathsf{pv}_i = \mathsf{pv}_{i,0}}, \widehat{\sigma}_{i|\widehat{\mathsf{pv}}_i = \widehat{\mathsf{pv}}_{i,0}}) \ \leq\ \varepsilon_1(\lambda) + \varepsilon_2(\lambda) + 2^{-\lambda}$.

Indeed, given the claim, it can be derived by induction that the distance of $(\sigma_1, \ldots, \sigma_\vartheta)$ and $(\widehat{\sigma}_1, \ldots, \widehat{\sigma}_\vartheta)$ given $\mathsf{pv}^* = \mathsf{pv}_0^* = \widehat{\mathsf{pv}}^*$, $k = k_0 = \widehat{k}$ and $B_2 = B_{2,0} = \widehat{B}_2$ it is smaller than $\vartheta(\varepsilon_1 + \varepsilon_2 + 2^{-\lambda})$. This concludes the indistinguishability of $\mathsf{H}_4, \mathsf{H}_5$ as $\mathsf{Adv}_{\mathcal{D}}^{\mathsf{H}_4, \mathsf{H}_5}(\lambda) \leq$

$$\leq\ \Delta(\mathsf{pv}_{\vartheta+1}, \widehat{\mathsf{pv}}_{\vartheta+1}) \ \leq\ \frac{n_1(n_1+1)}{2q} + 2^{-\lambda} + (\vartheta+1)(\varepsilon_1(\lambda) + \varepsilon_2(\lambda) + 2^{-\lambda}).$$

Indistinguishability of $\mathsf{H}_5, \mathsf{H}_6$. The reduction to (n_1, n_1+1)-MDDH is analogous to that of $\mathsf{H}_1, \mathsf{H}_2$. Specifically, given $\mathbb{G}$ and $[\mathbf{c}_0 | C^*] \in \mathbb{G}^{n_1} \times \mathbb{G}^{n_1, n_1}$, the reduction completes the verification key by setting $[\mathbf{u}] = [\mathbf{c}_0]$, $[A_1] = [C^*]$ and $[A_2] = [\mathbf{c}_0 \otimes \mathbf{a}_2 - M^*]$ where $M^* = B_1 \oplus P_{m^*} B_2$ as prescribed.

Indistinguishability of $\mathsf{H}_6, \mathsf{H}_7$. The reduction to (n_1, n_1+1)-MDDH is analogous to that of $\mathsf{H}_2, \mathsf{H}_3$. Specifically, given $\mathbb{G}$ and $[\mathbf{c}_0 | C^*] \in \mathbb{G}^{n_1} \times \mathbb{G}^{n_1, n_2}$, the reduction completes the verification key setting $[\mathbf{u}] = [\mathbf{c}_0]$, $[A_1] = [C^* - I]$ and $[A_2] = [\mathbf{c}_0 \otimes \mathbf{a}_2 - M^*]$ where again $M^* = B_1 \oplus (P_{m^*} B_2)$ as prescribed.

Hardness of H_7. By the definition of $\mathsf{S.Vfy}$, a valid forgery $(\mathbf{x}_1, \mathbf{x}_2, z)$ for m^* in H_7 must satisfy, for $M = B_1 \oplus (P_{m^*} B_2) = M^*$,

$$\begin{aligned}
\mathbf{t} &= \delta_2\left([A_1\mathbf{x}_1 + A_2\mathbf{x}_2 + z\mathbf{u} + \mathbf{x}_1 + M^*\mathbf{x}_2]\right) \\
&= \delta_2\left([(\mathbf{u}\otimes\mathbf{a}_1 - I)\mathbf{x}_1 + (\mathbf{u}\otimes\mathbf{a}_2 - M^*)\mathbf{x}_2 + z\mathbf{u} + \mathbf{x}_1 + M^*\mathbf{x}_2]\right) \\
&= \delta_2\left(\left[(\mathbf{a}_1^\top\mathbf{x}_1)\cdot\mathbf{u} + (\mathbf{a}_2^\top\mathbf{x}_2)\cdot\mathbf{u} + z\cdot\mathbf{u}\right]\right) \\
&= \delta_2\left(\left[(\mathbf{a}_1^\top\mathbf{x}_1 + \mathbf{a}_2^\top\mathbf{x}_2 + z)\cdot\mathbf{u}\right]\right).
\end{aligned}$$

Notice that the function ψ mapping $(\mathbf{x}_1, \mathbf{x}_2, z)$ to $\delta_2(\left[(\mathbf{a}_1^\top\mathbf{x}_1 + \mathbf{a}_2^\top + z)\cdot\mathbf{u}\right])$ takes at most q non-$\perp$ values in $\mathbb{F}_2^{n_1}$. Since $\mathbf{t}$ is uniformly sampled, then

$$\Pr\left[\mathbf{t} \in \operatorname{Im}\psi\right] \;=\; \frac{|\operatorname{Im}\psi \cap \mathbb{F}_2^{n_1}|}{|\mathbb{F}_2^{n_1}|} \;\leq\; \frac{q}{2^{n_1}} \;\leq\; \frac{1}{2^{\lambda}}$$

where we used $n_1 \geq \log q + \lambda$ by definition. Finally, when $\mathbf{t}$ is not in $\operatorname{Im}\psi$, no valid signature for m^* exists, implying the adversary has advantage at most $2^{-\lambda}$. $\square$

5 Adaptively Secure Short Signatures from DDH

5.1 Construction

Building on our selectively secure construction, we now present an improved scheme achieving EUF-CMA security from the polynomial hardness of DDH. The main idea is to combine our previous strategy with an algebraic hash, as in [Wat05], in order to embed a partitioning scheme. We do so at the price of an increased public key size.

Specifically, we now let vk contain matrices $A_{1,0}, \ldots, A_{1,\mu}$, $A_{2,0} \ldots, A_{2,\mu}$ and vectors $\mathbf{u}_0, \ldots, \mathbf{u}_\mu$ in the exponent, such that these vectors all lies in a one-dimensional space and $A_{j,i} = \mathbf{u}_i \otimes \mathbf{a}_j$. Moreover, as before, vk contains a PRF key k which defines a distance function δ over $\mathbb{G}$, and a (single) UHF $B \in \mathbb{F}_q^{n_1, n_2}$. To sign $m = (m_1, \ldots, m_\mu) \in \mathbb{F}_2^\mu$ we first evaluate the algebraic hash setting

$$A_j^{(m)} = A_{j,0} + m_1 A_{j,1} + \ldots + m_\mu A_{j,\mu}, \qquad \mathbf{u}^{(m)} = \mathbf{u}_0 + m_1\mathbf{u}_1 + \ldots + m_\mu\mathbf{u}_\mu.$$

and then consider the function F_m defined as

$$F_m(\mathbf{x}_1, \mathbf{x}_2, z) = B \cdot \delta_2\left([A_1^{(m)}\mathbf{x}_1 + A_2^{(m)}\mathbf{x}_2 + z\mathbf{u}^{(m)} + B^+\mathbf{x}_1]\right),$$

where B^+ is a (canonical) right inverse of B. Note we deviate from the previous scheme, where the last term in the exponent was $M\mathbf{x}_1$ with $M = (B_0 \oplus P_m B_1)$. We do so to have the message only being used in the algebraic hash evaluation. For technical reasons, this change also requires the UHF evaluation to be performed after evaluating the distance function[16].

[16] This is to ensure that uniformly sampled $(\mathbf{x}_2, z^*)$ s.t. $\delta_{\mathsf{min}}([A^{(m)}\mathbf{x}_1 + z^*\mathbf{u}^{(m)}]) \geq d$ are independent from B in all the hybrids we introduce in the security proof.

As before a signature is a preimage σ to a fixed target $\mathbf{t}$ for F_m as F_m is still efficiently preimage-sampleable given $\mathbf{a}_1$. The challenge lies in setting up the partitioning scheme.

We rely on UHF due to their $\mathbb{F}_2$-linearity, which interacts nicely with δ_2. Informally, our simulator will set up a UHF $h : \mathbb{F}_2^\mu \to \mathbb{F}_2^\ell$ and a random image $y \in \mathbb{F}_2^\ell$, so that F_m is lossier only when $h(m) = y$. This could be embedded in vk by performing the following changes in the public key generation[17]

1. $A_{1,0}$ is sampled as $\mathbf{u}_0 \otimes \mathbf{a}_1 - I$ to cancel out $\mathbf{x}_1$;
2. $A_{2,0}$ is set to $\mathbf{u}_0 \otimes \mathbf{a}_1 - P_y$;
3. $A_{2,i}$ is set to $\mathbf{u}_i \otimes \mathbf{a}_1 - P_{h(\mathbf{e}_i)}$.

where $\mathbf{e}_1, \ldots, \mathbf{e}_\mu$ is the canonical base of $\mathbb{F}_2^\mu$. The core idea is that, up to ensuring large enough distance, the function F_m takes the following form: $F_m(\mathbf{x}_1, \mathbf{x}_2, z) =$

$$= \delta_2\left([(\mathbf{a}_1^\top \mathbf{x}_1 + \mathbf{a}_2^\top \mathbf{x}_2 + z) \cdot \mathbf{u}^{(m)}]\right) \oplus (P_y \oplus m_1 P_{h(\mathbf{e}_1)} \oplus \ldots \oplus m_\mu P_{h(\mathbf{e}_\mu)}).$$

The first part is lossy as in the first construction. The second term instead, using the $\mathbb{F}_2$-linearity of P (see Theorem 2) is equal to $P_{y \oplus h(m)}$, which is the zero matrix iff $h(m) = y$. We detail the full scheme in Figure 9 and provide a summary of all the parameters and their values in Table 3.

Par.	Value	Description
λ	–	security parameter
μ	2λ	supported message length
q	–	group order
n_1	$\lambda + \log q$	first trapdoor bit length
n_2	$5\lambda + 2\log q + \log 4\lambda + \boldsymbol{2\mu}$	second trapdoor bit length
ν	2λ	rejection-sampling repetitions
L	$\log(10 n_2 d)$	SUF output length for δ
T	$10 n_2 d \cdot (1 + \ln(n_2)) + 2d$	maximum supported distance in δ
d	$(\boldsymbol{\mu} + \mathbf{1}) \cdot n_2 + n_1$	distance

Table 3: Parameters for the *adaptively* secure scheme. Differences from Table 2 are highlighted.

5.2 Correctness

Theorem 11. *If* SUF *is* $(\nu n_2 T)$*-universal, then the scheme in Figure 9 with the parameters in Table 3 is correct.*

A full proof appears in the Appendix, Section D.2.

[17] in the proof we use a mildly different approach in order to ensure the key-switching Lemma can be applied later on.

$\mathsf{S.Gen}(1^\lambda)$:

$(\mathbb{G}, G, q) \leftarrow^{\$} \mathsf{G.Gen}(1^\lambda)$
$\mathbf{u} \leftarrow^{\$} \mathbb{F}_q^{n_2}$
$\mathbf{a}_1 \leftarrow^{\$} \mathbb{F}_q^{n_1},\ \mathbf{a}_2 \leftarrow^{\$} \mathbb{F}_q^{n_2}$
$\alpha_0, \ldots, \alpha_\mu \leftarrow^{\$} \mathbb{F}_q$
$\mathbf{u}_i \leftarrow \alpha_i \cdot \mathbf{u}$
$A_{j,i} \leftarrow \mathbf{u}_i \otimes \mathbf{a}_j$ for $j \in \{1, 2\}$
$\mathbf{t} \leftarrow^{\$} \mathbb{F}_2^{n_1},\ k \leftarrow^{\$} \mathsf{SUF.Gen}(1^\lambda)$
$B \leftarrow^{\$} \mathbb{F}_2^{n_1, n_2}$ such that $\mathsf{rk}(B) = n_1$
$\mathsf{vk} = (([A_{1,i}], [A_{2,i}], [\mathbf{u}_i])_{i=0}^{\mu}, \mathbf{t}, k, B, \mathbb{G})$
$\mathsf{sk} = (\mathsf{vk}, \mathbf{a}_1)$
Return $(\mathsf{vk}, \mathsf{sk})$

$\mathsf{S.Sign}(\mathsf{sk}, m)$:

Set $\mathsf{dp} = (\mathbb{G}, G, q, k, L, T),\ \delta = \delta_{\mathsf{dp}}$.
Parse $m = (m_1, \ldots, m_\mu) \in \mathbb{F}_2^\mu$
$[\mathbf{u}^{(m)}] \leftarrow \left[\mathbf{u}_0 + \sum_{i=1}^{\mu} m_i \mathbf{u}_i\right]$
$[A_2^{(m)}] \leftarrow \left[A_{2,0} + \sum_{i=1}^{\mu} m_i A_{2,i}\right]$
If $[\mathbf{u}^{(m)}] = [\mathbf{0}]$: **Return** $\sigma = \mathbf{0}$
$(\mathbf{x}_2, z^*) \leftarrow^{\$} \mathsf{Samp}([A_2^{(m)}], [\mathbf{u}^{(m)}], d, \mathsf{dp})$
If $(\mathbf{x}_2, z^*) = \perp$: **Return** $\perp$
$\mathbf{x}_1 \leftarrow B \cdot \delta_2([A_2^{(m)}\mathbf{x}_2 + z^*\mathbf{u}^{(m)}]) \oplus \mathbf{t}$
$z \leftarrow z^* - \mathbf{a}_1^\top \mathbf{x}_1$
Return $\sigma = (\mathbf{x}_1, \mathbf{x}_2, z)$

$\mathsf{S.Vfy}(\mathsf{vk}, m, \sigma)$:

Set $\mathsf{dp} = (\mathbb{G}, G, q, k, L, T),\ \delta = \delta_{\mathsf{dp}}$
Parse $\sigma = (\mathbf{x}_1, \mathbf{x}_2, z)$ // $\in \mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \mathbb{F}_q$
Parse $m = (m_1, \ldots, m_\mu) \in \mathbb{F}_2^\mu$
$[\mathbf{u}^{(m)}] \leftarrow \left[\mathbf{u}_0 + \sum_{i=1}^{\mu} m_i \mathbf{u}_i\right],\ [A_j^{(m)}] \leftarrow \left[A_{j,0} + \sum_{i=1}^{\mu} m_i A_{j,i}\right]$ for $j \in \{1, 2\}$
If $[\mathbf{u}^{(m)}] = [\mathbf{0}]$: **Return** 1 // Accept any signature for bad messages
$b_1 \leftarrow (\delta_{\mathsf{min}}([A_1^{(m)}\mathbf{x}_1 + A_2^{(m)}\mathbf{x}_2 + z\mathbf{u}^{(m)}]) \geq d)$
$b_2 \leftarrow (B \cdot \delta_2([A_1^{(m)}\mathbf{x}_1 + A_2^{(m)}\mathbf{x}_2 + z\mathbf{u}^{(m)} + B^+\mathbf{x}_1]) == \mathbf{t})$ // $B^+\mathbf{x}_1 \in \mathbb{Z}^{n_2}$
Return $b_1 \wedge b_2$

Fig. 9: Adaptively secure signature from DDH.

5.3 Unforgeability

Theorem 12. *If DDH is hard for* $\mathsf{G.Gen}$*, then the scheme in Figure 9 with parameter as per Table 3 is existentially unforgeable under chosen message attacks.*

A full proof appears in the Appendix, Section D.3.

Acknowledgements. This study has been supported by the PIAno di inCEntivi per la Ricerca di Ateneo 2024/2026, linea di intervento 1. It was also supported by the project "PrepAring cRypTograpHy for privacy-awarE blockchaiN applicatiONs (PARTHENON)" - PRIN 2022 - Finanziato dall'Unione europea - Next Generation EU, Missione 4 Componente 1 - CUP: E53D23007990006.

References

ADM+24. Gennaro Avitabile, Nico Döttling, Bernardo Magri, Christos Sakkas, and Stella Wohnig. Signature-based witness encryption with compact cipher-

text. In Kai-Min Chung and Yu Sasaki, editors, *ASIACRYPT 2024, Part I*, volume 15484 of *LNCS*, pages 3–31. Springer, Singapore, December 2024.

AFLT12. Michel Abdalla, Pierre-Alain Fouque, Vadim Lyubashevsky, and Mehdi Tibouchi. Tightly-secure signatures from lossy identification schemes. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 572–590. Springer, Berlin, Heidelberg, April 2012.

BB04. Dan Boneh and Xavier Boyen. Short signatures without random oracles. In Christian Cachin and Jan Camenisch, editors, *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 56–73. Springer, Berlin, Heidelberg, May 2004.

BF01. Dan Boneh and Matthew K. Franklin. Identity-based encryption from the Weil pairing. In Joe Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 213–229. Springer, Berlin, Heidelberg, August 2001.

BGI16. Elette Boyle, Niv Gilboa, and Yuval Ishai. Breaking the circuit size barrier for secure computation under DDH. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part I*, volume 9814 of *LNCS*, pages 509–539. Springer, Berlin, Heidelberg, August 2016.

BKKP15. Olivier Blazy, Saqib A. Kakvi, Eike Kiltz, and Jiaxin Pan. Tightly-secure signatures from chameleon hash functions. In Jonathan Katz, editor, *PKC 2015*, volume 9020 of *LNCS*, pages 256–279. Springer, Berlin, Heidelberg, March / April 2015.

BLS01. Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the Weil pairing. In Colin Boyd, editor, *ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 514–532. Springer, Berlin, Heidelberg, December 2001.

BM92. Mihir Bellare and Silvio Micali. How to sign given any trapdoor function. *Journal of the ACM*, 39(1):214–233, January 1992.

BR93. Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, Ravi S. Sandhu, and Victoria Ashby, editors, *ACM CCS 93*, pages 62–73. ACM Press, November 1993.

BSW16. Mihir Bellare, Igors Stepanovs, and Brent Waters. New negative results on differing-inputs obfuscation. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part II*, volume 9666 of *LNCS*, pages 792–821. Springer, Berlin, Heidelberg, May 2016.

CD96. Ronald Cramer and Ivan Damgård. New generation of secure and practical RSA-based signatures. In Neal Koblitz, editor, *CRYPTO'96*, volume 1109 of *LNCS*, pages 173–185. Springer, Berlin, Heidelberg, August 1996.

CFGG22. Dario Catalano, Dario Fiore, Rosario Gennaro, and Emanuele Giunta. On the impossibility of algebraic vector commitments in pairing-free groups. In Eike Kiltz and Vinod Vaikuntanathan, editors, *TCC 2022, Part II*, volume 13748 of *LNCS*, pages 274–299. Springer, Cham, November 2022.

CG05. Dario Catalano and Rosario Gennaro. Cramer-Damgård signatures revisited: Efficient flat-tree signatures based on factoring. In Serge Vaudenay, editor, *PKC 2005*, volume 3386 of *LNCS*, pages 313–327. Springer, Berlin, Heidelberg, January 2005.

CL04. Jan Camenisch and Anna Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In Matthew Franklin, editor, *CRYPTO 2004*, volume 3152 of *LNCS*, pages 56–72. Springer, Berlin, Heidelberg, August 2004.

CPW20. Suvradip Chakraborty, Manoj Prabhakaran, and Daniel Wichs. Witness maps and applications. In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, *PKC 2020, Part I*, volume 12110 of *LNCS*, pages 220–246. Springer, Cham, May 2020.

CW77. J Lawrence Carter and Mark N Wegman. Universal classes of hash functions. In *Proceedings of the ninth annual ACM symposium on Theory of computing*, pages 106–112, 1977.

DG17. Nico Döttling and Sanjam Garg. Identity-based encryption from the Diffie-Hellman assumption. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part I*, volume 10401 of *LNCS*, pages 537–569. Springer, Cham, August 2017.

DGI+19. Nico Döttling, Sanjam Garg, Yuval Ishai, Giulio Malavolta, Tamer Mour, and Rafail Ostrovsky. Trapdoor hash functions and their applications. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part III*, volume 11694 of *LNCS*, pages 3–32. Springer, Cham, August 2019.

DHH+21. Nico Döttling, Dominik Hartmann, Dennis Hofheinz, Eike Kiltz, Sven Schäge, and Bogdan Ursu. On the impossibility of purely algebraic signatures. In Kobbi Nissim and Brent Waters, editors, *TCC 2021, Part III*, volume 13044 of *LNCS*, pages 317–349. Springer, Cham, November 2021.

DM14. Léo Ducas and Daniele Micciancio. Improved short lattice signatures in the standard model. In Juan A. Garay and Rosario Gennaro, editors, *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 335–352. Springer, Berlin, Heidelberg, August 2014.

DN94. Cynthia Dwork and Moni Naor. An efficient existentially unforgeable signature scheme and its applications. In Yvo Desmedt, editor, *CRYPTO'94*, volume 839 of *LNCS*, pages 234–246. Springer, Berlin, Heidelberg, August 1994.

DORS08. Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM journal on computing*, 38(1):97–139, 2008.

Giu23. Emanuele Giunta. On the impossibility of algebraic NIZK in pairing-free groups. In Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Part IV*, volume 14084 of *LNCS*, pages 702–730. Springer, Cham, August 2023.

GJ03. Eu-Jin Goh and Stanislaw Jarecki. A signature scheme as secure as the Diffie-Hellman problem. In Eli Biham, editor, *EUROCRYPT 2003*, volume 2656 of *LNCS*, pages 401–415. Springer, Berlin, Heidelberg, May 2003.

GMR88. Shafi Goldwasser, Silvio Micali, and Ronald L. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on Computing*, 17(2):281–308, April 1988.

GVW19. Rishab Goyal, Satyanarayana Vusirikala, and Brent Waters. Collusion resistant broadcast and trace from positional witness encryption. In Dongdai Lin and Kazue Sako, editors, *PKC 2019, Part II*, volume 11443 of *LNCS*, pages 3–33. Springer, Cham, April 2019.

HW09. Susan Hohenberger and Brent Waters. Short and stateless signatures from the RSA assumption. In Shai Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 654–670. Springer, Berlin, Heidelberg, August 2009.

JDS22. Mei Jiang, Dung Hoang Duong, and Willy Susilo. Puncturable signature: A generic construction and instantiations. In Vijayalakshmi Atluri, Roberto

Di Pietro, Christian Damsgaard Jensen, and Weizhi Meng, editors, *ESORICS 2022, Part II*, volume 13555 of *LNCS*, pages 507–527. Springer, Cham, September 2022.

JJ21. Abhishek Jain and Zhengzhong Jin. Non-interactive zero knowledge from sub-exponential DDH. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part I*, volume 12696 of *LNCS*, pages 3–32. Springer, Cham, October 2021.

JMV01. Don Johnson, Alfred Menezes, and Scott Vanstone. The elliptic curve digital signature algorithm (ecdsa). *International journal of information security*, 1(1):36–63, 2001.

KR00. Hugo Krawczyk and Tal Rabin. Chameleon signatures. In *NDSS 2000*. The Internet Society, February 2000.

KW03. Jonathan Katz and Nan Wang. Efficiency improvements for signature schemes with tight security reductions. In Sushil Jajodia, Vijayalakshmi Atluri, and Trent Jaeger, editors, *ACM CCS 2003*, pages 155–164. ACM Press, October 2003.

Mau94. Ueli M. Maurer. Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete algorithms. In Yvo Desmedt, editor, *CRYPTO'94*, volume 839 of *LNCS*, pages 271–281. Springer, Berlin, Heidelberg, August 1994.

NY89. Moni Naor and Moti Yung. Universal one-way hash functions and their cryptographic applications. In *21st ACM STOC*, pages 33–43. ACM Press, May 1989.

PS96. David Pointcheval and Jacques Stern. Security proofs for signature schemes. In Ueli M. Maurer, editor, *EUROCRYPT'96*, volume 1070 of *LNCS*, pages 387–398. Springer, Berlin, Heidelberg, May 1996.

Rom90. John Rompel. One-way functions are necessary and sufficient for secure signatures. In *22nd ACM STOC*, pages 387–394. ACM Press, May 1990.

Sch90. Claus-Peter Schnorr. Efficient identification and signatures for smart cards. In Gilles Brassard, editor, *CRYPTO'89*, volume 435 of *LNCS*, pages 239–252. Springer, New York, August 1990.

Vil12. Jorge Luis Villar. Optimal reductions of some decisional problems to the rank problem. In Xiaoyun Wang and Kazue Sako, editors, *ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 80–97. Springer, Berlin, Heidelberg, December 2012.

Wat05. Brent R. Waters. Efficient identity-based encryption without random oracles. In Ronald Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 114–127. Springer, Berlin, Heidelberg, May 2005.

WC81. Mark N Wegman and J Lawrence Carter. New hash functions and their use in authentication and set equality. volume 22, pages 265–279. Elsevier, 1981.

A Further Preliminaries

A.1 Statistical Distance

In this section we recall additional facts regarding the statistical distance. First of all, we present a tool to study the distance of joint distributions.

Lemma 4. *Let (X_1, Y_1) and (X_2, Y_2) be random variables over $\mathcal{X} \times \mathcal{Y}$. Calling $\mathcal{X}^+ = \{x_0 \in X \ : \ \Pr[X_i = x_0] > 0 \ \ \forall i \in \{1, 2\}\}$, then*

$$\Delta((X_1, Y_1), (X_2, Y_2)) \ \leq \ \Delta(X_1, X_2) + \sum_{x_0 \in \mathcal{X}^+} \Pr[X_1 = x_0] \cdot \Delta(Y_1|_{X_1=x_0}, Y_2|_{X_2=x_0}).$$

In particular, if there exists a set $A \subseteq \mathcal{X}$ and $\varepsilon_1, \varepsilon_2, \varepsilon_3$ such that $\forall x_0 \in \mathcal{X}^+ \setminus A$

$$\Pr[x_1 \in A] \leq \varepsilon_1, \quad \Delta(X_1, X_2) \leq \varepsilon_2, \quad \Delta(Y_{1|X_1=x_0}, Y_{2|X_2=x_0}) \leq \varepsilon_3,$$

then $\Delta((X_1, Y_1), (X_2, Y_2)) \leq \varepsilon_1 + \varepsilon_2 + \varepsilon_3$.

Next, we observe that two distributions (X, Y_1), (X, Y_2) being close only means that Y_1, Y_2 are close when conditioning to X *on average*. In our arguments this is often not enough as we need the conditional distance to be small for most values of X. The following lemma provides a Markov-like bound in this direction.

Lemma 5. *Let X be a random variable over $\mathcal{X}$ and Y_0, Y_1 be random variables over $\mathcal{Y}$. If $\Delta((X, Y_0), (X, Y_1)) \leq \varepsilon_1\varepsilon_2$, then*

$$\Pr[X \in \{x_0 : \Delta(Y_0|_{X=x_0}, Y_1|_{X=x_0}) \geq \varepsilon_1\}] \leq \varepsilon_2.$$

Proof. By definition, we have

$$\Delta((X, Y_0), (X, Y_1)) \coloneqq \frac{1}{2} \sum_{x_0 \in \mathcal{X}} \sum_{y_0 \in \mathcal{Y}} \left|\Pr[X = x_0, Y_0 = y_0] - \Pr[X = x_0, Y_1 = y_0]\right|.$$

This can be written as

$$\frac{1}{2} \sum_{x_0 \in \mathcal{X}} \Pr[X = x_0] \sum_{y_0 \in \mathcal{Y}} \left|\Pr[Y_0 = y_0 | X = x_0] - \Pr[Y_1 = y_0 | X = x_0]\right|$$

which is in turn equal to $\mathbb{E}[\Delta(Y_0|_{X=x_0}, Y_1|_{X=x_0})]$, where the expected value is taken with respect to X. Due to our hypothesis, this is bounded above by $\varepsilon_1\varepsilon_2$. Then, by Markov's inequality we get

$$\Pr[\Delta(Y_0|_{X=x_0}, Y_1|_{X=x_0}) \geq \varepsilon_1] \leq \frac{\mathbb{E}[\Delta(Y_0|_{X=x_0}, Y_1|_{X=x_0})]}{\varepsilon_1} \leq \frac{\varepsilon_1\varepsilon_2}{\varepsilon_1} = \varepsilon_2. \quad \square$$

Next, for completeness, we present simple facts we use in the analysis of our rejection-sampling procedures. The first shows that, conditioning on the sampling's success, then the resulting distribution is uniform over the desired subset.

Lemma 6. *Let $\mathcal{X}$ be a finite set and let $\mathcal{Z} \subseteq \mathcal{X}$. Sampling $x_1 \leftarrow^{\$} \mathcal{X}, \ldots, x_n \leftarrow^{\$} \mathcal{X}$, let I be:*

$$I = \begin{cases} \min\{i : x_i \in \mathcal{Z}\} & \text{if } \exists j : x_j \in \mathcal{Z} \\ \perp & \text{otherwise} \end{cases}.$$

Then $(x_I)_{|I\neq\perp}$ *is uniform over* $\mathcal{Z}$.

Proof. For any $a \in \mathcal{Z}$, it holds

$$\Pr[x_I = a | I \neq \perp] = \sum_{i=1}^{n} \Pr[x_i = a | I = i] \Pr[I = i | I \neq \perp].$$

Therefore, we begin by computing $\Pr[x_i = a | I = i]$ for $i = 1, \ldots, n$. We have

$$\begin{aligned}
\Pr[x_i = a | I = i] &= \Pr[x_i = a | x_i \in \mathcal{Z} \wedge (x_j \notin \mathcal{Z} \quad \forall j = 1, \ldots, i-1)] \\
&= \frac{\Pr[x_i = a \wedge x_i \in \mathcal{Z} \wedge (x_j \notin \mathcal{Z} \quad \forall j = 1, \ldots, i-1)]}{\Pr[x_i \in \mathcal{Z} \wedge (x_j \notin \mathcal{Z} \quad \forall j = 1, \ldots, i-1)]} \\
&= \frac{\Pr[x_i = a] \Pr[x_j \notin \mathcal{Z} \quad \forall j = 1, \ldots, i-1]}{\Pr[x_i \in \mathcal{Z}] \Pr[x_j \notin \mathcal{Z} \quad \forall j = 1, \ldots, i-1]} \\
&= \frac{1}{|\mathcal{X}|} \frac{|\mathcal{X}|}{|\mathcal{Z}|} = \frac{1}{|\mathcal{Z}|}.
\end{aligned}$$

The first equality comes from the definition of I; the second one is just the definition of conditional probability; the third one holds because all x_i are independently distributed and, since a belongs to $\mathcal{Z}$, we have $\Pr[x_i = a \wedge x_i \in \mathcal{Z}] = \Pr[x_i = a]$. If we substitute this in the first line, we obtain

$$\begin{aligned}
\Pr[x_I = a | I \neq \perp] &= \sum_{i=1}^{n} \frac{1}{|\mathcal{Z}|} \Pr[I = i | I \neq \perp] \\
&= \frac{1}{|\mathcal{Z}|} \sum_{i=1}^{n} \Pr[I = i | I \in \{1, \ldots, n\}] = \frac{1}{|\mathcal{Z}|}
\end{aligned}$$

meaning that x_I, conditioned on $I \neq \perp$, is uniformly distributed over $\mathcal{Z}$. □

The second one is more relevant for preimage sampling. It shows that conditioning a uniformly distributed random variable to lie in a given subset, then the resulting distribution is uniform over that subset.

Lemma 7. *Let* $\mathcal{X}, \mathcal{Y}$ *be finite sets. Let* $f : \mathcal{X} \to \mathcal{Y}$, $x \leftarrow^{\$} \mathcal{X}$ *and* $y_0 \in \mathrm{Im}(f)$. *Then, taking* $u \leftarrow^{\$} f^{-1}(y_0)$, *we have*

$$\Delta(x|_{f(x)=y_0}, u) = 0.$$

Proof. We need to prove that x, conditioned on $f(x) = y_0$, is uniformly distributed over $f^{-1}(y_0)$. First of all, notice that for any $x_0 \notin f^{-1}(y_0)$, we have $\Pr[x = x_0 | f(x) = y_0] = 0$. On the other hand, for any $x_0 \in f^{-1}(y_0)$, we have

$$\begin{aligned}
\Pr[x = x_0 | f(x) = y_0] &= \frac{\Pr[x = x_0 \wedge f(x) = y_0]}{\Pr[f(x) = y_0]} = \frac{\Pr[x = x_0]}{\Pr[f(x) = y_0]} \\
&= \frac{1}{|\mathcal{X}|} \frac{|\mathcal{X}|}{|f^{-1}(y_0)|} = \frac{1}{|f^{-1}(y_0)|},
\end{aligned}$$

which proves our claim. □

A.2 Min-Entropy

Min-entropy informally measures the hardness to statistically guess the output of a given distribution. Our min-entropy analysis will only be aimed to justify usage of the generalized Leftover Hash Lemma, stated in Section 2.3.

Definition 13. *Let X, Y be a random variable over finite sets $\mathcal{X}, \mathcal{Y}$ and E an event. The min-entropy of X, the min-entropy of X given E and the average min-entropy of X given Y are respectively defined as:*

$$\begin{aligned} \mathrm{H}_\infty(X) &\coloneqq -\log \max_{x_0 \in \mathcal{X}} (\Pr[X = x_0]) \\ \mathrm{H}_\infty(X|E) &\coloneqq -\log \left(\max_{x_0 \in \mathcal{X}} \Pr[X = x_0 | E] \right) \\ \mathrm{H}_\infty(X|Y) &\coloneqq -\log \left(\sum\nolimits_{y_0 \in \mathcal{Y}} \Pr[Y = y_0] \max_{x_0 \in \mathcal{X}} \Pr[X = x_0 | Y = y_0] \right). \end{aligned}$$

Theorem 13 ([DORS08]). *Let X, Y, Z be random variables over $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$ and let E be an event. Then the followings hold:*

1. $\mathrm{H}_\infty(X) \leq \log |\mathcal{X}|$;
2. $\mathrm{H}_\infty(X|Z) \leq \mathrm{H}_\infty(X, Y|Z)$;
3. $\mathrm{H}_\infty(X|Y, Z) \leq \mathrm{H}_\infty(X|Z)$;
4. $\mathrm{H}_\infty(X|Y, Z) \geq \mathrm{H}_\infty(X, Y|Z) - \log |\mathcal{Y}|$;
5. $\mathrm{H}_\infty(X|Y, Z) = \mathrm{H}_\infty(X|Z)$ *if X, Y are conditionally independent given Z;*
6. $\mathrm{H}_\infty(X|E) \geq H(X) + \log \Pr[E]$.

Theorem 14 (Data processing inequalities). *Let X and Y be random variables over $\mathcal{X}$ and $\mathcal{Y}$, respectively. Let $f : \mathcal{X} \to \mathcal{T}$ and $g : \mathcal{Y} \to \mathcal{S}$. Then:*

1. $\mathrm{H}_\infty(f(X)|Y) \leq \mathrm{H}_\infty(X|Y)$;
2. $\mathrm{H}_\infty(X|g(Y)) \geq \mathrm{H}_\infty(X|Y)$.

As informally discussed in the introduction, our signature schemes heavily involve rejection sampling to draw elements from the domain or the preimage of certain functions. The following lemma provides a bound on the min-entropy loss such rejection sampling entails. The proof appears in the Appendix, Section B.2.

Lemma 8. *Let $\mathcal{X}$ be a finite set and let $X_1, \ldots, X_n \leftarrow^{\$} \mathcal{X}$. Moreover, let I be distributed over $\{\perp, 1, \ldots, n\}$. Then, setting $X_\perp = \perp$, we have*

$$\mathrm{H}_\infty(X_I | I \neq \perp) \geq \log(|\mathcal{X}|) - \log(n) + \log(\Pr[I \neq \perp]).$$

B Postponed Proofs: Preliminaries

B.1 Balanced Functions

Proof of Lemma 1. Before proceeding with the proof, we will need the following general fact. The proof appears later in this section.

Claim 3. *Given $f : \mathcal{X} \to \mathcal{Y}$ an ε-balanced function, let $x \leftarrow^{\$} \mathcal{X}$, $y \leftarrow^{\$} \mathcal{Y}$ and $z \leftarrow^{\$} f^{-1}(y)$. Then $\Delta(x, z) \leq \varepsilon$.*

We begin bounding $\Delta(x_1, \widehat{x}_1)$. Let $\widehat{y} \leftarrow^{\$} \mathcal{Y}$ and set $\widehat{z} \leftarrow^{\$} f_1^{-1}(\widehat{y})$. By Claim 3, since f_1 is ε_1-balanced, it follows that $\Delta(x_1, \widehat{z}) \leq \varepsilon_1$. On the other hand, since f_2 is ε_2-balanced, by definition $\Delta(f_2(\widehat{x}_2), \widehat{y}) \leq \varepsilon_2$ which implies $\Delta(\widehat{x}_1, \widehat{z}) \leq \varepsilon_2$. The final bound holds because $\widehat{x}_1, \widehat{z}_1$ are the output of the same (randomized) function, returning a random preimage under f_1, applied to $f_2(\widehat{x}_2)$ and $\widehat{y}$ respectively. Thus, we get

$$\Delta(x_1, \widehat{x}_1) \leq \Delta(x_1, \widehat{z}) + \Delta(\widehat{z}, \widehat{x}_1) \leq \varepsilon_1 + \varepsilon_2.$$

Let us call $\mathcal{Z} \coloneqq f_1^{-1}(\mathrm{Im}\,(f_2)) \subseteq \mathcal{X}_1$. Notice that $\mathcal{Z} = \{\alpha \in \mathcal{X}_1 : \Pr[\widehat{x}_1 = \alpha] \neq 0\}$. We claim that

Claim 4. *For any $\alpha \in \mathcal{Z}$, it holds that $\Delta(x_2|_{x_1=\alpha}, \widehat{x}_2|_{\widehat{x}_1=\alpha}) = 0$.*

It is then possible to bound $\Delta((x_1, x_2), (\widehat{x}_1, \widehat{x}_2)) \leq$

$$\begin{aligned}
&\leq\ \Delta(x_1, \widehat{x}_1) + \sum_{\alpha \in \mathcal{X}_1} \Pr[\widehat{x}_1 = \alpha]\, \Delta(x_2|_{x_1=\alpha}, \widehat{x}_2|_{\widehat{x}_1=\alpha}) \\
&\leq\ \Delta(x_1, \widehat{x}_1) + \sum_{\alpha \in \mathcal{Z}} \Delta(x_2|_{x_1=\alpha}, \widehat{x}_2|_{\widehat{x}_1=\alpha}) + \sum_{\alpha \in \mathcal{X}_1 \setminus \mathcal{Z}} \Pr[\widehat{x}_1 = \alpha] \\
&=\ \Delta(x_1, \widehat{x}_1)\ \leq\ \varepsilon_1 + \varepsilon_2.
\end{aligned}$$

The first inequality holds by Lemma 4; the second inequality comes from splitting the sum over $\mathcal{X}_1$ as a sum over $\mathcal{Z}$ and $\mathcal{X}_1 \setminus \mathcal{Z}$ and then bounding respectively $\Pr[\widehat{x}_1 = \alpha]$ in the first sum and $\Delta(x_2|_{x_1=\alpha}, \widehat{x}_2|_{\widehat{x}_1=\alpha})$ in the second sum by 1; the equality holds since the first sum is equal to 0 as a consequence of Claim 4, while the second sum is equal to 0 by definition of $\mathcal{Z}$. □

Proof of Claim 3. First of all, notice that our hypothesis yields $\varepsilon \geq \Delta(f(x), y) =$

$$= \frac{1}{2} \sum_{y_0 \in \mathcal{Y}} |\Pr[f(x) = y_0] - \Pr[y = y_0]| \ =\ \frac{1}{2} \sum_{y_0 \in \mathcal{Y}} \left| \frac{|f^{-1}(y_0)|}{|\mathcal{X}|} - \frac{1}{|\mathcal{Y}|} \right|.$$

We have to study $\Delta(x, z) = \frac{1}{2} \sum_{x_0 \in \mathcal{X}} |\Pr[x = x_0] - \Pr[z = x_0]|$. Since x is uniformly distributed over $\mathcal{X}$, we have that $\Pr[x = x_0] = |\mathcal{X}|^{-1}$. As for the other term, for a fixed $x_0 \in \mathcal{X}$, we have

$$\Pr[z = x_0] \ =\ \Pr[z = x_0 | y = f(x_0)] \Pr[y = f(x_0)] \ =\ \frac{1}{|f^{-1}(f(x_0))|} \frac{1}{|\mathcal{Y}|}.$$

where the first equality holds since $\Pr[z = x_0 \,|\, y \neq f(x_0)] = 0$. Moreover, we can partition $\mathcal{X}$ as the union of $f^{-1}(y_0)$ for $y_0 \in \mathcal{Y}$ and thus express $\Delta(x, z)$ as

$$\begin{aligned}
\Delta(x, z) \ &=\ \frac{1}{2} \sum_{y_0 \in \mathrm{Im}\,(f)} \sum_{x_0 \in f^{-1}(y_0)} \left| \frac{1}{|\mathcal{X}|} - \frac{1}{|f^{-1}(f(x_0))|} \frac{1}{|\mathcal{Y}|} \right| \\
&=\ \frac{1}{2} \sum_{y_0 \in \mathrm{Im}\,(f)} \left| \frac{|f^{-1}(y_0)|}{|\mathcal{X}|} - \frac{1}{|\mathcal{Y}|} \right| \ \leq\ \frac{1}{2} \sum_{y_0 \in \mathcal{Y}} \left| \frac{|f^{-1}(y_0)|}{|\mathcal{X}|} - \frac{1}{|\mathcal{Y}|} \right| \ \leq\ \varepsilon.
\end{aligned}$$

The first inequality holds because we are summing over a possibly bigger set, while the last one is true due to our remark at the beginning of the proof. □

Proof of Claim 4. Let us call $\gamma \coloneqq f_1(\alpha)$. By construction, $x_2|_{x_1=\alpha}$ is uniform over $f_2^{-1}(\gamma)$, hence for any $\beta \in f_2^{-1}(\gamma)$ we have

$$\Pr\left[x_2 = \beta | x_1 = \alpha\right] = \frac{1}{|f_2^{-1}(\gamma)|}.$$

Next, we study $\Pr\left[\widehat{x}_2 = \beta | \widehat{x}_1 = \alpha\right]$. Using Bayes' Theorem, we get

$$\begin{aligned}\Pr\left[\widehat{x}_2 = \beta | \widehat{x}_1 = \alpha\right] &= \Pr\left[\widehat{x}_1 = \alpha | \widehat{x}_2 = \beta\right] \cdot \frac{\Pr\left[\widehat{x}_2 = \beta\right]}{\Pr\left[\widehat{x}_1 = \alpha\right]} \\ &= \frac{1}{|f_1^{-1}(\gamma)|} \frac{1}{|\mathcal{X}_2|} \frac{1}{\Pr\left[\widehat{x}_1 = \alpha\right]}\end{aligned}$$

where we used the fact that $\Pr\left[\widehat{x}_1 = \alpha | \widehat{x}_2 = \beta\right] = |f_1^{-1}(\gamma)|^{-1}$ since $f_2(\beta) = \gamma$. To conclude we need to determine $\Pr\left[\widehat{x}_1 = \alpha\right]$. We have

$$\begin{aligned}\Pr\left[\widehat{x}_1 = \alpha\right] &= \sum_{\beta \in \mathcal{X}_2} \Pr\left[\widehat{x}_1 = \alpha | \widehat{x}_2 = \beta\right] \Pr\left[\widehat{x}_2 = \beta\right] \\ &= \sum_{\beta \in f_2^{-1}(\gamma)} \Pr\left[\widehat{x}_1 = \alpha | \widehat{x}_2 = \beta\right] \frac{1}{|\mathcal{X}_2|} \\ &= \sum_{\beta \in f_2^{-1}(\gamma)} \frac{1}{|f_1^{-1}(\gamma)|} \frac{1}{|\mathcal{X}_2|} = \frac{|f_2^{-1}(\gamma)|}{|f_1^{-1}(\gamma)|} \frac{1}{|\mathcal{X}_2|}.\end{aligned}$$

By substituting, we obtain that for any $\beta \in f_2^{-1}(\gamma)$

$$\Pr\left[\widehat{x}_2 = \beta | \widehat{x}_1 = \alpha\right] = \frac{1}{|f_1^{-1}(\gamma)|} \frac{1}{|\mathcal{X}_2|} \frac{|\mathcal{X}_2||f_1^{-1}(\gamma)|}{|f_2^{-1}(\gamma)|} = \frac{1}{|f_2^{-1}(\gamma)|},$$

which concludes our proof. □

B.2 Min-Entropy

Proof of Lemma 8. First of all, notice that $\Pr[X_I = \perp | I \neq \perp] = 0$, as $X_1, \ldots, X_n$ take values in $\mathcal{X}$. Then, for any $\alpha \in \mathcal{X}$ we have that

$$\Pr[X_I = \alpha | I \neq \perp] \leq \sum_{i=1}^{n} \Pr[X_i = \alpha | I \neq \perp].$$

However $\Pr[X_i = \alpha] \geq \Pr[X_i = \alpha \wedge I \neq \perp] = \Pr[X_i = \alpha | I \neq \perp] \Pr[I \neq \perp]$, which implies that

$$\Pr[X_i = \alpha | I \neq \perp] \leq \frac{\Pr[X_i = \alpha]}{\Pr[I \neq \perp]}.$$

By combining the inequalities above, we get that

$$\Pr[X_I = \alpha | I \neq \perp] \;\leq\; \sum_{i=1}^{n} \frac{\Pr[X_i = \alpha]}{\Pr[I \neq \perp]} \;=\; \frac{n}{|\mathcal{X}| \Pr[I \neq \perp]}$$

and so the same inequality holds for $\max_{\alpha \in \mathcal{X}} \Pr[X_I = \alpha | I \neq \perp]$. We can thus conclude that $\mathrm{H}_\infty(X_I | I \neq \perp) \geq$

$$\geq -\log\left(n \cdot \frac{1}{|\mathcal{X}|} \cdot \frac{1}{\Pr[I \neq \perp]}\right) = \log|\mathcal{X}| - \log n + \log \Pr[I \neq \perp]. \qquad \square$$

B.3 Universal Hash Functions

Proof of Lemma 2. Developing the probability in the lemma,

$$\begin{aligned}
&\Pr\left[h(m^*) = y \wedge \left(\wedge_{i=1}^{\vartheta} h(m_i) \neq y\right) \wedge E\right] \\
&= \Pr\left[h(m^*) = y \wedge \left(\wedge_{i=1}^{\vartheta} h(m_i) \neq h(m^*)\right) \wedge \neg\mathsf{Coll} \wedge E\right] \\
&= \Pr\left[h(m^*) = y\right] \cdot \left(\Pr\left[\neg\mathsf{Coll} \wedge E\right] - \Pr\left[\neg\mathsf{Coll} \wedge E \wedge \left(\vee_{i=1}^{\vartheta} h(m_i) = h(m^*)\right)\right]\right) \\
&\geq \frac{1}{2^\ell} \cdot \left(\Pr\left[\neg\mathsf{Coll} \wedge E\right] - \sum\nolimits_{i=1}^{\vartheta} \Pr\left[h(m_i) = h(m^*) \wedge \neg\mathsf{Coll} \wedge E\right]\right).
\end{aligned}$$

The first equality follows as $h(m^*) = y \neq h(m_i)$ implies $m^* \neq m_i$ for all i, that is $\neg\mathsf{Coll}$, and in particular the two events are equivalent, the second one since y is independent from other variables, while the inequality hold for the first factor since y is uniformly random, while for the second factors we applied a union bound. Next we study each term in the summation. Let $M = \{0,1\}^n$, and $C \subseteq M^{\vartheta+1}$ the set of tuples $(\bar{m}_1, \ldots, \bar{m}_\vartheta, \bar{m}^*) \in M^{\vartheta+1}$ such that $\exists i : \bar{m}_i = \bar{m}_i^*$ and $\bar{C} = M \setminus C$. Furthermore call $\mathbf{m} = (m_1, \ldots, m_\vartheta, m^*) \in M^{\vartheta+1}$. Then

$$\begin{aligned}
&\Pr\left[h(m_i) = h(m^*) \wedge \neg\mathsf{Coll} \wedge E\right] \\
&= \sum\nolimits_{\bar{\mathbf{m}} \in M^{\vartheta+1}} \Pr\left[h(m_i) = h(m^*) \wedge \neg\mathsf{Coll} \wedge E \wedge \mathbf{m} = \bar{\mathbf{m}}\right] \\
&= \sum\nolimits_{\bar{\mathbf{m}} \in \bar{C}} \Pr\left[h(\bar{m}_i) = h(\bar{m}^*) \wedge E \wedge \mathbf{m} = \bar{\mathbf{m}}\right] \\
&= \sum\nolimits_{\bar{\mathbf{m}} \in \bar{C}} \Pr\left[h(\bar{m}_i) = h(\bar{m}^*)\right] \cdot \Pr\left[E \wedge \mathbf{m} = \bar{\mathbf{m}}\right] \\
&\leq \frac{1}{2^\ell} \cdot \sum\nolimits_{\bar{\mathbf{m}} \in \bar{C}} \Pr\left[E \wedge \mathbf{m} = \bar{\mathbf{m}}\right] \\
&= \frac{1}{2^\ell} \cdot \Pr\left[E \wedge \mathbf{m} \in \bar{C}\right] \;=\; \frac{1}{2^\ell} \cdot \Pr\left[E \wedge \neg\mathsf{Coll}\right]
\end{aligned}$$

where the first inequality is by the total probability theorem, the second one since for all $\bar{\mathbf{m}} \in C$ the corresponding term is 0, while for $\bar{\mathbf{m}} \notin C$, then $\neg\mathsf{Coll}$ always holds. The third follows as h and $E, \mathbf{m}$ are independently distributed. The inequality follows as h is a UHF with image in $\{0,1\}^\ell$, while the last equality follows by definition of C and Coll.

Combining this result with the above we conclude

$$\begin{aligned}
&\Pr\left[h(m^*) = y \wedge (\wedge_{i=1}^{\vartheta} h(m_i) \neq y) \wedge E\right] \\
&\geq \frac{1}{2^\ell} \cdot \left(\Pr\left[\neg\mathsf{Coll} \wedge E\right] - \frac{\vartheta}{2^\ell}\Pr\left[\neg\mathsf{Coll} \wedge E\right]\right) \\
&\geq \Pr\left[\neg\mathsf{Coll} \wedge E\right] \cdot \frac{1}{2\vartheta} \cdot \left(1 - \frac{\vartheta}{2\vartheta}\right) \;=\; \Pr\left[\neg\mathsf{Coll} \wedge E\right] \cdot \frac{1}{4\vartheta}.
\end{aligned}$$

where we used the fact that $2^\ell = 2\vartheta$. □

B.4 Exceptional Sets of Binary Matrices

Proof of Theorem 2. For any fixed $\mathbf{x} \in \mathbb{F}_2^n$, since ϕ^{-1}, ϕ and the multiplication by $\phi(\psi^{(\ell)}(\mathbf{x}))$ in $\mathbb{F}_{2^n}$ are all $\mathbb{F}_2$ linear, so is their composition. Thus $P_{\mathbf{x}}^{(\ell)} \in \mathrm{End}(\mathbb{F}_2^n)$ and P^ℓ is well defined. Moreover, for any fixed $\mathbf{y} \in \mathbb{F}_2^n$, as $\psi^{(\ell)}, \phi$, the multiplication by $\phi(\mathbf{y})$ in $\mathbb{F}_{2^n}$ and ϕ^{-1} are all $\mathbb{F}_2$-linear, we have that $P_{\mathbf{x}_1 \oplus \mathbf{x}_2}^{(\ell)}(\mathbf{y}) = P_{\mathbf{x}_1}^{(\ell)}(\mathbf{y}) \oplus P_{\mathbf{x}_2}^{(\ell)}(\mathbf{y})$. In particular $P_{\mathbf{x}_1 \oplus \mathbf{x}_2}^{(\ell)} = P_{\mathbf{x}_1}^{(\ell)} \oplus P_{\mathbf{x}_2}^{(\ell)}$, meaning that $P^{(\ell)}$ is $\mathbb{F}_2$ linear.

Finally, For any $\mathbf{x} \neq 0$, let $\alpha = \phi(\psi^{(\ell)}(\mathbf{x})) \in \mathbb{F}_{2^n}$. Since $\mathbf{x}$ is non-zero and $\phi, \psi^{(\ell)}$ are injective, $\alpha \neq 0$, and in particular it has a multiplicative inverse in $\mathbb{F}_{2^n}$. Then consider $Q : \mathbb{F}_2^n \to \mathbb{F}_2^n$ the map such that $Q(\mathbf{y}) = \phi^{-1}\left(\phi(\mathbf{y}) \cdot \alpha^{-1}\right)$. We have for all $\mathbf{y} \in \mathbb{F}_2^n$ that

$$P_{\mathbf{x}}^{(\ell)} \circ Q(\mathbf{y}) \;=\; \phi^{-1}\left(\phi(\mathbf{y}) \cdot \alpha^{-1} \cdot \alpha\right) \;=\; \phi^{-1}(\phi(\mathbf{y})) \;=\; \mathbf{y}$$

and in particular $P_{\mathbf{x}}^{(\ell)}$ is invertible with inverse Q. □

B.5 Prime Order Groups

Lemma 9. *Let $A \leftarrow^{\$} \mathbb{F}_q^{n,m}$ and $B \leftarrow^{\$} \mathbb{F}_q^{n,m}$ with $n \geq m$ such than $\mathsf{rk}(B) = m$. Then $\Delta(A, B) \leq q^{m-n}/(q-1)$.*

Proof. By definition, we have

$$\Delta(A, B) \;=\; \frac{1}{2} \sum_{M \in \mathbb{F}_q^{n,m}} |\Pr\left[A = M\right] - \Pr\left[B = M\right]|.$$

Let us denote $\mathbb{F}_q^{n,m;k}$ the set of matrices in $\mathbb{F}_q^{n,m}$ of rank k. Since A is uniform over $\mathbb{F}_q^{n,m}$ and B is uniform over $\mathbb{F}_q^{n,m;m}$, the above statistical distance can be written as

$$\begin{aligned}
&\frac{1}{2} \sum_{\mathbb{F}_q^{n,m;m}} \left|\frac{1}{q^{nm}} - \frac{1}{|\mathbb{F}_q^{n,m;m}|}\right| + \frac{1}{2} \sum_{\mathbb{F}_q^{n,m} \setminus \mathbb{F}_q^{n,m;m}} \frac{1}{q^{nm}} \\
&= \frac{1}{2}|\mathbb{F}_q^{n,m;m}|\left(\frac{1}{|\mathbb{F}_q^{n,m;m}|} - \frac{1}{q^{nm}}\right) + \frac{1}{2}(q^{nm} - |\mathbb{F}_q^{n,m;m}|)\frac{1}{q^{nm}} \\
&= 1 - \frac{|\mathbb{F}_q^{n,m;m}|}{q^{nm}}.
\end{aligned}$$

We can now observe that the above quantity is exactly the probability that a matrix drawn uniformly from $\mathbb{F}_q^{n,m}$ is not full rank. Therefore, in order to conclude, it suffices find an upper bound for this probability. If $C \coloneqq (\mathbf{c}_1, \ldots, \mathbf{c}_m) \leftarrow^{\$} \mathbb{F}_q^{nm}$, we have $\Pr[\mathsf{rk}(C) < m] =$

$$
\begin{aligned}
&= \Pr[\exists i : \mathbf{c}_i \in \mathrm{span}(\mathbf{c}_1, \ldots, \mathbf{c}_{i-1})] \\
&= \Pr[\exists i : (\mathbf{c}_i \in \mathrm{span}(\mathbf{c}_1, \ldots, \mathbf{c}_{i-1}) \wedge \dim(\mathrm{span}(\mathbf{c}_1, \ldots, \mathbf{c}_{i-1})) = i-1)] \\
&\leq \sum_{i=1}^{m} \Pr[\mathbf{c}_i \in \mathrm{span}(\mathbf{c}_1, \ldots, \mathbf{c}_{i-1}) \wedge \dim(\mathrm{span}(\mathbf{c}_1, \ldots, \mathbf{c}_{i-1})) = i-1] \\
&= \sum_{i=1}^{m} \frac{q^{i-1}}{q^n} \;=\; \frac{1}{q^n}\frac{q^m-1}{q-1} \;\leq\; \frac{q^{m-n}}{q-1}.
\end{aligned}
$$

□

Lemma 10. *If* $A \leftarrow^{\$} \mathbb{F}_q^{n,m+1}$ *such that* $\mathsf{rk}(A) = 1$, $\mathbf{u} \leftarrow^{\$} \mathbb{F}_q^n$ *and* $\mathbf{v} \leftarrow^{\$} \mathbb{F}_q^m$, *assuming* $q = \Omega(2^\lambda)$ *then* $\Delta(A, \mathbf{u} \otimes (1, \mathbf{v})) \leq \mathsf{negl}(\lambda)$.

Proof. By definition, using the same notation as Lemma 9, we have

$$
\Delta(A, \mathbf{u} \otimes (1, \mathbf{v})) \;=\; \frac{1}{2} \sum_{M \in \mathbb{F}_q^{n,m+1;1}} |\Pr[A = M] - \Pr[\mathbf{u} \otimes (1, \mathbf{v}) = M]| + \frac{1}{2q^n},
$$

where the term $\frac{1}{q^n}$ is the probability that $\mathbf{u} \otimes (1, \mathbf{v})$ is the null matrix (which is simply the probability that $\mathbf{u}$ is the null vector). Since M is a rank-1 matrix, it can be written as $\mathbf{u} \otimes (1, \mathbf{v})$ in a unique way. Moreover, A is uniformly distributed over $\mathbb{F}_q^{n,m+1;1}$. Therefore we obtain that the above statistical distance is equal to

$$
\begin{aligned}
&\frac{1}{2} \sum_{M \in \mathbb{F}_q^{n,m+1;1}} \left| \frac{1}{|\mathbb{F}_q^{n,m+1;1}|} - \frac{1}{q^{n+m}} \right| + \frac{1}{2q^n} \\
&= \frac{1}{2} |\mathbb{F}_q^{n,m+1;1}| \left(\frac{1}{|\mathbb{F}_q^{n,m+1;1}|} - \frac{1}{q^{n+m}} \right) + \frac{1}{2q^n} \\
&= \frac{1}{2} \left(1 - \frac{|\mathbb{F}_q^{n,m+1;1}|}{q^{n+m}} + \frac{1}{q^n} \right)
\end{aligned}
$$

In order to conclude the proof, we just need to compute $|\mathbb{F}_q^{n,m+1;1}|$. We can compute this quantity by considering the following map

$$
\begin{aligned}
\mathbb{F}_q^n \setminus \{\mathbf{0}_n\} \times \mathbb{F}_q^{m+1} \setminus \{\mathbf{0}_{m+1}\} &\to \mathbb{F}_q^{n,m+1;1} \\
(\mathbf{a}, \mathbf{b}) &\mapsto \mathbf{a} \otimes \mathbf{b}.
\end{aligned}
$$

It can be easily checked that this map is well defined and surjective and that any matrix in $\mathbb{F}_q^{n,m+1;1}$ has exactly $q-1$ preimages, implying that

$$
|\mathbb{F}_q^{n,m+1;1}| \;=\; \frac{|\mathbb{F}_q^n \setminus \{\mathbf{0}_n\}| \times |\mathbb{F}_q^{m+1} \setminus \{\mathbf{0}_{m+1}\}|}{q-1} \;=\; \frac{(q^n-1)(q^{m+1}-1)}{q-1}
$$

By substituting in the above statistical distance and doing some computation, we obtain

$$\frac{1}{2}\left(\frac{q^{n+m}-q^n-q^{m+1}+1}{q^{n+m}(q-1)}+\frac{1}{q^n}\right)=\frac{1}{2q-2}\left(1-\frac{1}{q^m}-\frac{1}{q^{n-1}}+\frac{1}{q^{n+m}}\right)+\frac{1}{2q^n}$$
$$\leq \frac{1}{2}\left(\frac{1}{q-1}+\frac{1}{q^n}\right),$$

which is a negligible function of λ for $q=\Omega(2^\lambda)$. □

Corollary 2. *If* $A \leftarrow^{\$} \mathbb{F}_q^{n,m}$ *such that* $\mathsf{rk}(A)=1$, $\mathbf{u} \leftarrow^{\$} \mathbb{F}_q^n$, $\mathbf{v} \leftarrow^{\$} \mathbb{F}_q^m$, *assuming* $q=\Omega(2^\lambda)$ *then* $\Delta(A, \mathbf{u}\otimes\mathbf{v}) \leq \mathsf{negl}(\lambda)$.

C Postponed Proofs: Distance Function

C.1 Properties

Proof of Lemma 3. Let i be some fixed index in $\{1,\ldots,n\}$. Define

$$S_i \coloneqq \{\alpha \in \{0,\ldots,T-1\} : f_k(H_i+\alpha G)=0^L\}$$

and let $\alpha_i=\min(S_i)$. Since $\delta_{\mathsf{min}}(\mathbf{H}) \neq \perp$, it must be $S_i \neq \emptyset$ and $\alpha_i=\delta(H_i)$ by construction. Since we supposed that $\delta_{\mathsf{min}}(\mathbf{H}) \geq d$, it must be $\alpha_i \geq d$, hence $\alpha_i - x_i \geq \alpha_i - d \geq 0$. Consider now the set

$$T_i \coloneqq \{\beta \in \{0,\ldots,T-1\} : f_k(H_i+x_iG+\beta G)=0^L\}.$$

Again, $T_i \neq \varnothing$, since $\alpha_i - x_i \in T_i$. We claim that $\alpha_i - x_i = \min(T_i)$.
If $\beta \in T_i$ is such that $\beta \leq \alpha_i - x_i$, then $0 \leq \beta + x_i \leq \alpha_i \leq T-1$. Therefore, $\beta + x_i \in S_i$ and, since $\alpha_i=\min(S_i)$, it must be $\alpha_i \leq \beta + x_i$, i.e. $\alpha_i - x_i \leq \beta$. Since we assumed that $\beta \leq \alpha_i - x_i$, we get that $\beta = \alpha_i - x_i$, thus proving our claim. Finally, we have

$$\delta(H_i) - x_i = \alpha_i - x_i = \min(T_i) = \delta(H_i + x_iG).$$

Since this holds for any $i \in \{1,\ldots,n\}$, we obtain the claimed equality. □

Proof of Corollary 1. We will apply Lemma 3 twice. First, since $\delta_{\mathsf{min}}(\mathbf{H}-\mathbf{x}_1G) \geq \|\mathbf{x}_2\|_\infty$ we have that

$$\delta(\mathbf{H}-\mathbf{x}_1G+\mathbf{x}_2G) \;=\; \delta(\mathbf{H}-\mathbf{x}_1G)-\mathbf{x}_2.$$

Next, because $\delta_{\mathsf{min}}(\mathbf{H}-\mathbf{x}_1G) \geq \|\mathbf{x}_1\|_\infty$

$$\delta(\mathbf{H}) \;=\; \delta(\mathbf{H}-\mathbf{x}_1G+\mathbf{x}_1G) \;=\; \delta(\mathbf{H}-\mathbf{x}_1G)-\mathbf{x}_1.$$

Combining the two equations proves the corollary. □

C.2 Rejection Sampling

Proof of Theorem 3. Conditioning on $\neg\mathsf{Near}$, all νnT group elements of the form $H_{i,j}+\gamma G$ for $\gamma \in \{0,\dots,T-1\}$ are distinct and so the random variables $f_k(H_{i,j}+\gamma G)$ are all uniform in $\{0,1\}^L$ and independent due to f_k being (νnT)-universal. First, observe that by our construction of δ

$$\begin{aligned}\delta(H_{i,j}) \geq d \iff & (f_k(H_{i,j}+\gamma G) \neq 0^L \quad \forall \gamma \in \{0,\dots,d-1\}) \wedge \\ & \neg(f_k(H_{i,j}+\gamma G) \neq 0^L \quad \forall \gamma \in \{d,\dots,T-1\}).\end{aligned}$$

Each of the events $\delta(H_{i,j}) \geq d$ only depends on $f_k(H_{i,j}+\gamma G)$. Conditioning on $\neg\mathsf{Near}$ then these are all independent since $f_k(H_{i,j}+\gamma G)$ are. In particular, calling $\mathbf{H}_i \coloneqq (H_{i,j})_{j=1}^n$,

$$\begin{aligned}\Pr\left[\nexists i : \delta_{\mathsf{min}}(\mathbf{H}_i) \geq d \,|\, \neg\mathsf{Near}\right] &= \prod_{i=1}^{\nu} \Pr[\neg(\delta_{\mathsf{min}}(\mathbf{H}_i) \geq d) \,|\, \neg\mathsf{Near}] \\ &= \prod_{i=1}^{\nu} (1 - \Pr[\delta_{\mathsf{min}}(\mathbf{H}_i) \geq d \,|\, \neg\mathsf{Near}]) \\ &= \prod_{i=1}^{\nu} \left(1 - \Pr\left[\bigwedge_{j=1}^{n} \delta(H_{i,j}) \geq d \,\middle|\, \neg\mathsf{Near}\right]\right) \\ &= \prod_{i=1}^{\nu} \left(1 - \prod_{j=1}^{n} \Pr[\delta(H_{i,j}) \geq d \,|\, \neg\mathsf{Near}]\right).\end{aligned}$$

Next, we proceed expanding the term $\Pr[\delta(H_{i,j}) \geq d|\neg\mathsf{Near}] =$

$$\begin{aligned}&= \left(\prod_{\gamma=0}^{d-1} \Pr[f_k(H_{i,j}+\gamma G) \neq 0^L]\right)\left(1 - \prod_{\gamma=d}^{T-1} \Pr[f_k(H_{i,j}+\gamma G) \neq 0^L]\right) = \\ &= \left(1-2^{-L}\right)^d \left(1 - \left(1-2^{-L}\right)^{T-d}\right)\end{aligned}$$

where we used our characterization of $\delta(H_{i,j}) \geq d$. Thus

$$\begin{aligned}\prod_{j=1}^{n} \Pr[\delta(H_{i,j}) \geq d|\neg\mathsf{Near}] &= \left(1-2^{-L}\right)^{dn} \left(1 - \left(1-2^{-L}\right)^{T-d}\right)^n \geq \\ &\geq \left(1 - \frac{nd}{2^L}\right)\left(1 - \exp\left(-\frac{T-d}{2^L}\right)\right)^n \geq \\ &\geq \left(1 - \frac{nd}{5nd}\right)\left(1 - n\exp\left(-\frac{2^L(1+\ln(n))}{2^L}\right)\right) = \\ &= \left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{e}\right) \geq \frac{1}{2},\end{aligned}$$

where we used (multiple times) the following general inequalities:

- $(1-\beta)^\alpha \geq 1 - \alpha\beta \qquad \forall \beta \geq 0,\ \forall \alpha \geq 1;$
- $1 - x \leq \exp(-x) \Rightarrow (1 - 1/n) \leq \exp(-1/n) \Rightarrow (1-1/n)^m \leq \exp(-m/n).$

We then conclude that

$$\begin{aligned}\Pr\left[\nexists i : \delta_{\mathsf{min}}(\mathbf{H}_i) \geq d\right] &\leq \Pr[\nexists i : \delta_{\mathsf{min}}(\mathbf{H}_i) \geq d)|\neg\mathsf{Near}] + \Pr\left[\mathsf{Near}\right] \leq \\ &\leq \prod_{i=1}^{\nu}\left(1 - \frac{1}{2}\right) + \Pr\left[\mathsf{Near}\right] = \frac{1}{2^\nu} + \Pr\left[\mathsf{Near}\right]. \qquad \square\end{aligned}$$

C.3 Domain Sampling

Proof of Theorem 4. This result is a direct consequence of Lemma 6 by considering $\mathcal{X} = \mathbb{F}_2^{\eta_2} \times \mathbb{F}_q$ and $\mathcal{Z} = \mathcal{U}^*$. □

Proof of Theorem 5. Let us parse A as $A^\top = (\mathbf{a}_1, \ldots, \mathbf{a}_{\eta_3}) \in \mathbb{F}_q^{\eta_3, \eta_2}$. We want to apply the result of Theorem 3 on the group elements $H_{i,j} = \left[\mathbf{a}_j^\top \mathbf{x}_i + z_i u_j\right]$. Let us study the near collision probability by distinguishing between two cases and using the fact that all $\mathbf{x}_i$, z_i are sampled independently.

- **Same round collision.** For any $i \in \{1, \ldots, \nu\}$, $j_0 \neq j_1 \in \{1, \ldots, \eta_3\}$ and $\gamma \in \{0, \ldots, T-1\}$, the near-collision probability of H_{i,j_0}, H_{i,j_1} is

$$\begin{aligned}\Pr\left[H_{i,j_0} = H_{i,j_1} + \gamma G\right] &= \Pr\left[\mathbf{a}_{j_0}^\top \mathbf{x}_i + z_i u_{j_0} = \mathbf{a}_{j_1}^\top \mathbf{x}_i + z_i u_{j_1} + \gamma\right] = \\ &= \Pr\left[z_i = \frac{\gamma - \mathbf{a}_{j_0}^\top \mathbf{x}_i + \mathbf{a}_{j_1}^\top \mathbf{x}_i}{u_{j_0} - u_{j_1}}\right] = \frac{1}{q}.\end{aligned}$$

- **Different round collision.** For any $i_0 \neq i_1 \in \{1, \ldots, \nu\}$, $j_0 \neq j_1 \in \{1, \ldots, \eta_3\}$, $\gamma \in \{0, \ldots, T-1\}$,

$$\begin{aligned}\Pr\left[H_{i_0,j_0} = H_{i_1,j_1} + \gamma G\right] &= \Pr\left[\mathbf{a}_{j_0}^\top \mathbf{x}_{i_0} + z_{i_0} u_{j_0} = \mathbf{a}_{j_1}^\top \mathbf{x}_{i_1} + z_{i_1} u_{j_1} + \gamma\right] = \\ &= \Pr\left[z_{i_0} = \frac{\mathbf{a}_{j_0}^\top \mathbf{x}_{i_1} - \mathbf{a}_{j_0}^\top \mathbf{x}_{i_0} + z_{i_1} u_{j_1} + \gamma}{u_{j_0}}\right] = \frac{1}{q}.\end{aligned}$$

The collision probability then satisfies $\Pr[\mathsf{Near}] \leq \nu^2 \eta_3^2 T/q$ via a union bound. Now, since all the hypothesis of Theorem 3 are satisfied, we have

$$\begin{aligned}\Pr\left[\mathsf{Samp}([A], [\mathbf{u}], d, \mathsf{dp}) = \perp\right] &= \Pr[\nexists i : \delta_{\mathsf{min}}([A\mathbf{x}_i + z_i \mathbf{u}]) \geq d] \\ &\leq \frac{1}{2^\nu} + \frac{\nu^2 \eta_3^2 T}{q} =: \varepsilon_1(\lambda)^2,\end{aligned}$$

where the probability is taken with respect to $(\mathbf{x}_i, z_i)_{i=1}^\nu$ and $k \leftarrow^{\$} \mathsf{SUF.Gen}(1^\lambda)$. To conclude the proof we rely on an averaging argument through Markov. For ease of notation we denote with Bad the event $\mathsf{Samp}([A], [\mathbf{u}], d, \mathsf{dp}) = \perp$. Let

$$\mathcal{K}_1^* \coloneqq \{k_0 \in \mathcal{K}_\lambda \ : \ \Pr[\mathsf{Bad} \mid k = k_0] \leq \varepsilon_1(\lambda)\}.$$

Considering the function mapping $k_0 \mapsto \Pr[\mathsf{Bad} \mid k = k_0]$, where the probability is taken over $(\mathbf{x}_i, z_i)_{i=1}^\nu$, we have that $\Pr[\mathsf{Bad}] = \mathbb{E}_k\left[\Pr[\mathsf{Bad} \mid k = k_0]\right] \leq \varepsilon_1(\lambda)^2$. By Markov then $\Pr[k \notin \mathcal{K}_1^*] \leq \varepsilon_1(\lambda)$. □

Proof of Theorem 6. The proof of this theorem follows the same blueprint of that of Theorem 5. However, there are some additional details to take into consideration. This time need to make sure that the set $\widehat{\mathcal{K}}_1^*$ exists independently of M, $\mathbf{a}$ and α. For this reason, we will define the set $\widehat{\mathcal{K}}_1^*$ using a stronger condition and then prove that it satisfies the three required properties.

Definition of $\widehat{\mathcal{K}}_1^*$. For a random $k \leftarrow^{\$} \mathsf{SUF.Gen}(1^\lambda)$, for random $\rho_1, \ldots, \rho_\nu \in \mathbb{F}_q$ and given $\mathbf{u}$, d as above, we begin studying the probability that for no $i \in \{1, \ldots, \nu\}$ it is the case that $\delta_{\mathsf{min}}([\rho_i \mathbf{u} - d \cdot \mathbf{1}]) \geq 2d$. Calling $H_{i,j} \coloneqq [\rho_i u_j - d]$, we study the near-collision probability (as per Theorem 3) for these group elements, by distinguishing among two cases:

- **Same round collision.** For any $i \in \{1, \ldots, \nu\}$, $j_0 \neq j_1 \in \{1, \ldots, \eta_3\}$ and $\gamma \in \{0, \ldots, T-1\}$, the near-collision probability of H_{i,j_0}, H_{i,j_1} is

$$\Pr\left[H_{i,j_0} = H_{i,j_1} + \gamma G\right] \;=\; \Pr\left[\rho_i = \frac{\gamma}{u_{j_0} - u_{j_1}}\right] \;=\; \frac{1}{q}$$

- **Different round collision.** For any $i_0 \neq i_1 \in \{1, \ldots, \nu\}$, $j_0 \neq j_1 \in \{1, \ldots, \eta_3\}$, $\gamma \in \{0, \ldots, T-1\}$,

$$\Pr\left[H_{i_0,j_0} = H_{i_1,j_1} + \gamma G\right] \;=\; \Pr\left[\rho_{i_0} = \frac{\rho_{i_1} + \gamma}{u_{j_0}}\right] \;=\; \frac{1}{q}$$

where we used the fact the $\rho_1, \ldots, \rho_\nu$ are uniformly and independently distributed and the assumption that $0 \neq u_{j_0} \neq u_{j_1}$ for any pair of distinct indices $j_0 \neq j_1$. Via a union bound, then $\Pr[\mathsf{Near}] \leq (\nu^2 \eta_3^2 T)/q$, with $\mathsf{Near} = \mathsf{Near}(\mathsf{H}, T)$ being as in Definition 12. In particular, by Theorem 3, we have

$$\Pr\left[\nexists i : \delta_{\mathsf{min}}([\rho_i \mathbf{u} - d \cdot \mathbf{1}] \geq 2d)\right] \leq \frac{1}{2^\nu} + \frac{\nu^2 \eta_3^2 T}{q} =: \varepsilon_1(\lambda)^2.$$

We can now define the set $\widehat{\mathcal{K}}_1^*$ as the set of keys which make the above event happen with probability at most $\varepsilon_1(\lambda)$, namely

$$\widehat{\mathcal{K}}_1^* \coloneqq \{k_0 \in \mathcal{K}_\lambda : \Pr\left[\nexists i : \delta_{\mathsf{min}}([\rho_i \mathbf{u} - d \cdot \mathbf{1}]) \geq 2d \,|\, k = k_0\right] \leq \varepsilon_1(\lambda)\},$$

where the probability is taken over the choice of $\rho_1, \ldots, \rho_\nu \leftarrow^{\$} \mathbb{F}_q$. As argued in the proof of Theorem 5, by Markov inequality we have that if $k \leftarrow^{\$} \mathsf{SUF.Gen}(1^\lambda)$, then $\Pr[k \notin \widehat{\mathcal{K}}_1^*] \leq \varepsilon_1(\lambda)$, which proves that the first two conditions are satisfied. Moreover, if $z_1, \ldots, z_\nu \leftarrow^{\$} \mathbb{F}_q$, $\mathbf{x}_i \leftarrow^{\$} \mathbb{F}_2^{\eta_2}$, $\mathbf{a} \in \mathbb{F}_q^{\eta_2}$, $\alpha \in \mathbb{F}_q$, then $\mathbf{a}^\top \mathbf{x}_i + z_i \alpha$ are still uniformly and independently distributed over $\mathbb{F}_q$ (this is true since all z_i and x_i are independently distributed and α is non-zero), implying that for any $k_0 \in \widehat{\mathcal{K}}_1^*$ it holds that

$$\begin{aligned}
&\Pr\left[\nexists i : \delta_{\mathsf{min}}([(\mathbf{u} \otimes \mathbf{a})\mathbf{x}_i + z_i \cdot \alpha \mathbf{u} - d \cdot \mathbf{1}]) \geq 2d \,|\, k = k_0\right] \\
&= \Pr\left[\nexists i : \delta_{\mathsf{min}}(\left[(\mathbf{a}^\top \mathbf{x}_i + z_i \alpha)\mathbf{u} - d \cdot \mathbf{1}\right]) \geq 2d \,\middle|\, k = k_0\right] \\
&\leq \varepsilon_1(\lambda).
\end{aligned}$$

In order to conclude our proof, we just need to prove the following claim.

Claim 5. *With the previous notation, if* $\delta_{\mathsf{min}}([(\mathbf{u} \otimes \mathbf{a})\mathbf{x}_i + z_i \alpha \mathbf{u} - d \cdot \mathbf{1}]) \geq 2d$, *then it holds that* $\delta_{\mathsf{min}}([(\mathbf{u} \otimes \mathbf{a} - M)\mathbf{x}_i + z_i \alpha \mathbf{u}]) \geq d$.

Indeed, given that the claim is true, we derive that for any $k_0 \in \widehat{\mathcal{K}}_1^*$

$$\begin{aligned}
&\Pr\left[\mathsf{Samp}([\mathbf{u}\otimes\mathbf{a}-M],[\alpha\mathbf{u}],d,\mathsf{dp})=\perp\right]\\
&=\ \Pr\left[\nexists i:\delta_{\mathsf{min}}([(\mathbf{u}\otimes\mathbf{a}-M)\mathbf{x}_i+z_i\alpha\mathbf{u}])\geq d\right]\\
&\leq\ \Pr\left[\nexists i:\delta_{\mathsf{min}}([(\mathbf{u}\otimes\mathbf{a})\mathbf{x}_i+z_i\alpha\mathbf{u}-d\cdot\mathbf{1}])\geq 2d\right]\\
&\leq\ \varepsilon_1(\lambda). \qquad\qquad \square
\end{aligned}$$

Proof of Claim 5. Let $\mathbf{w}\in\mathbb{Z}^{\eta_3}$ be defined as $\mathbf{w}\coloneqq d\cdot\mathbf{1}-M\mathbf{x}_i$. First of all, notice that $\mathbf{w}$ belongs to $\{0,\ldots,d\}^{\eta_3}$. Indeed, by hypothesis $d\geq\|M\|_\infty\geq\|M\mathbf{x}_i\|_\infty$, since $\|x_i\|_\infty\leq 1$. In particular, each entry of $M\mathbf{x}_i$ is smaller than d, implying that $\mathbf{w}$ has non-negative entries; on the other hand, $M\mathbf{x}_i$ has non negative entries, implying also that each entry of $\mathbf{w}$ is also smaller then d.
Next, as by hypothesis $\delta_{\mathsf{min}}([(\mathbf{u}\otimes\mathbf{a})\mathbf{x}_i+z_i\alpha\mathbf{u}-d\cdot\mathbf{1}])\geq 2d\geq d$, applying Lemma 3, we have that

$$\begin{aligned}
\delta([(\mathbf{u}\otimes\mathbf{a}-M)\mathbf{x}_i+z_i\alpha\mathbf{u}])\ &=\ \delta([(\mathbf{u}\otimes\mathbf{a})\mathbf{x}_i+z_i\alpha\mathbf{u}-d\cdot\mathbf{1}+\mathbf{w}])\\
&=\ \delta([(\mathbf{u}\otimes\mathbf{a})\mathbf{x}_i+z_i\alpha\mathbf{u}-d\cdot\mathbf{1}])-\mathbf{w},
\end{aligned}$$

which implies that

$$\delta_{\mathsf{min}}([(\mathbf{u}\otimes\mathbf{a}-M)\mathbf{x}_i+z_i\mathbf{u}])\geq\delta_{\mathsf{min}}([(\mathbf{u}\otimes\mathbf{a})\mathbf{x}_i+z_i\alpha\mathbf{u}-d\cdot\mathbf{1}])-\|\mathbf{w}\|_\infty\geq d.\ \square$$

C.4 Preimage Sampling

Proof of Theorem 7. The proof is inspired by that of Theorem 5, although additional care is required. Specifically, we need to ensure the set $\mathcal{K}_2^*$ exists *independently* from $M_1, M_2, B, \mathbf{v}=\alpha_1\mathbf{u}$ and $\mathbf{t}$, as they are intentionally quantified later. To cleanly achieve this goal, we first derive the set $\mathcal{K}_2^*$ through an averaging argument on the probability that a stronger condition (which does not depend on M_1, M_2, B) than the one in line 9 is satisfied. Next, we prove $\mathcal{K}_2^*$ to satisfy the three required properties.

Definition of $\mathcal{K}_2^*$. For a random $k\leftarrow^{\$}\mathsf{SUF.Gen}(1^\lambda)$, $\rho_1,\ldots,\rho_\nu\leftarrow^{\$}\mathbb{F}_q$ and given $\mathbf{u},\mathbf{a},d$ as above we begin studying the probability that for no $i\in\{1,\ldots,\nu\}$ it is the case that $\delta_{\mathsf{min}}([\rho_i\mathbf{u}-d\cdot\mathbf{1}])\geq 2d$. Calling $H_{i,j}=[\rho_i u_j-d]$, we study the near collision of these group elements (as per Theorem 3) probability in two cases:

- **Same round collision.** For any $i\in\{1,\ldots,\nu\}$, $j_0,j_1\in\{1,\ldots,\eta_3\}$ with $j_0\neq j_1$ and $\gamma\in\{0,\ldots,T-1\}$,

$$\Pr[H_{i,j_0}=H_{i,j_1}+\gamma G]\ =\ \Pr\left[\rho_i=\frac{\gamma}{u_{j_0}-u_{j_1}}\right]\ =\ \frac{1}{q};$$

- **Different round collision.** For any $i_0,i_1\in\{1,\ldots,\nu\}$ with $i_0\neq i_1$, any $j_0,j_1\in\{1,\ldots,\eta_3\}$ and $\gamma\in\{0,\ldots,T-1\}$,

$$\Pr[H_{i_0,j_0}=H_{i_1,j_1}+\gamma G]=\Pr\left[\rho_{i_0}=\frac{\rho_{i_1}u_{j_1}+\gamma}{u_{j_0}}\right]=\frac{1}{q};$$

where we used the uniform and mutually independent distribution of $\rho_1, \ldots, \rho_\nu$, and the assumption that $0 \neq u_{j_0} \neq u_{j_1}$ for any pair of distinct indices $j_0 \neq j_1$. Via a union bound then $\Pr[\mathsf{Near}] \leq (\nu^2\eta_3^2 T)/q$, with $\mathsf{Near} = \mathsf{Near}(\mathbf{H}, T)$ being as in Definition 12. In particular, by Theorem 3

$$\Pr[\nexists i : \delta_{\mathsf{min}}([\rho_i \mathbf{u} - d \cdot \mathbf{1}]) \geq 2d] \;\leq\; \frac{1}{2^\nu} + \frac{\nu^2\eta_3^2 T}{q} \;=:\; \varepsilon_2(\lambda)^2.$$

We can now define $\mathcal{K}_2^*$ as the set of keys that make the event above happen with probability at most $\varepsilon_2(\lambda)$. Formally,

$$\mathcal{K}_2^* \;=\; \{k_0 \in \mathcal{K}_\lambda \;:\; \Pr[\nexists i : \delta_{\mathsf{min}}([\rho_i \mathbf{u} - d \cdot \mathbf{1}]) \geq 2d \,|\, k = k_0] \leq \varepsilon_2(\lambda)\},$$

where the probability is taken over the choice of $\rho_1, \ldots, \rho_\nu \leftarrow^{\$} \mathbb{F}_q$. As argued in the proof of Theorem 5, by Markov inequality we have that if $k \leftarrow^{\$} \mathsf{SUF.Gen}(1^\lambda)$ then $\Pr[k \notin \mathcal{K}_2^*] \leq \varepsilon_2(\lambda)$. This proves points 1 and 2. Moreover, let $z_1^*, \ldots, z_\nu^* \leftarrow^{\$} \mathbb{F}_q$ and $\rho \in \mathbb{F}_q$ constant. Then $\alpha_1 + z_i^* \alpha_2$ are still uniformly and independently distributed over $\mathbb{F}_q$, since $\alpha_2 \neq 0$. This implies that, if $k_0 \in \mathcal{K}_\lambda$, then

$$\Pr[\nexists i : \delta_{\mathsf{min}}([\alpha_2 \mathbf{u} + z_i^* \alpha_2 \mathbf{u} - d \cdot \mathbf{1}]) \geq 2d \,|\, k = k_0] \leq \varepsilon_2(\lambda).$$

Correct termination. We now focus on proving point 3. For ease of notation Bad denotes the event $\mathsf{PreSamp}([\alpha_1 \mathbf{u}], [\alpha_2 \mathbf{u}], \mathbf{a}, M_1, M_2, B, \mathbf{t}, d, \mathsf{dp}) = \perp$. By the checks performed at line 7 and 9 this is equivalent to

$$\mathsf{Bad} \quad \Leftrightarrow \quad (\exists i : S_i = \varnothing) \;\vee\; (\nexists i : \delta_{\mathsf{min}}([\alpha_1 \mathbf{u} + z_i^* \alpha_2 \mathbf{u} - M_1 \mathbf{x}_i]) \geq d).$$

First, notice that as we assumed $M_1 \oplus M_2$ and B to be full rank modulo 2, and $\eta_1 \leq \eta_2$, then the space of solution $\mathbf{x}_0$ such that $B(M_1 \oplus M_2)\mathbf{x}_0 = B\mathbf{s}_i \oplus \mathbf{t}$ has dimension $\eta_2 - \eta_1$ and in particular is always non-empty. Hence Bad is equivalent to second clause above. We conclude with the following consequence of Lemma 3:

Claim 6. *With the previous notation, if* $\delta_{\mathsf{min}}([\alpha_1 \mathbf{u} + z_i^* \alpha_2 \mathbf{u} - d \cdot \mathbf{1}]) \geq 2d$ *then it holds that* $\delta_{\mathsf{min}}([\alpha_1 \mathbf{u} + z_i^* \alpha_2 \mathbf{u} - M_1 \mathbf{x}_i]) \geq d$.

Given the claim, we derive that for any $k_0 \in \mathcal{K}_2^*$

$$\begin{aligned}
\Pr[\mathsf{Bad} \,|\, k = k_0] \;&=\; \Pr[\nexists i : \delta_{\mathsf{min}}([\alpha_1 \mathbf{u} + z_i^* \alpha_2 \mathbf{u} - M_1 \mathbf{x}_i]) \geq d \,|\, k = k_0] \\
&\leq\; \Pr[\nexists i : \delta_{\mathsf{min}}([\alpha_1 \mathbf{u} + z_i^* \alpha_2 \mathbf{u} - d \cdot \mathbf{1}]) \geq 2d \,|\, k = k_0] \\
&\leq\; \varepsilon_2(\lambda).
\end{aligned}$$

which concludes the proof. □

Proof of Claim 6. Let $\mathbf{w} \in \mathbb{Z}^{\eta_3}$ be the vector $d \cdot \mathbf{1} - M_1 \mathbf{x}_i$. The first step is to show $\mathbf{w} \in \mathbb{N}^{\eta_3}$ with norm $\|\mathbf{w}\|_\infty \leq d$. Indeed, by hypothesis $d \geq \|M_1\|_\infty \geq \|M_1 \mathbf{x}_i\|_\infty$, because $\|\mathbf{x}_i\|_\infty \leq 1$. In particular each entry of $M_1 \mathbf{x}_i$ is smaller than d, implying $\mathbf{w}$ has non-negative entries. Moreover, since $M_1 \mathbf{x}_i$ also has non negative entries when computed over the integers, each entry of $\mathbf{w}$ is upper-bounded by d. Hence $\|\mathbf{w}\|_\infty \leq d$.

Next, as by hypothesis $\delta_{\mathsf{min}}([\alpha_1\mathbf{u} + z_i^*\alpha_2\mathbf{u} - d\cdot\mathbf{1}]) \geq d$, applying Lemma 3

$$\begin{aligned}\delta([\alpha_1\mathbf{u} + z_i^*\alpha_2\mathbf{u} - M_1\mathbf{x}_i]) &= \delta([\alpha_1\mathbf{u} + z_i^*\alpha_2\mathbf{u} - d\cdot\mathbf{1} + \mathbf{w}]) \\ &= \delta([\alpha_1\mathbf{u} + z_i^*\alpha_2\mathbf{u} - d\cdot\mathbf{1}]) - \mathbf{w}\end{aligned}$$

implying $\delta_{\mathsf{min}}([\alpha_1\mathbf{u} + z_i^*\alpha_2\mathbf{u} - M_1\mathbf{x}_i]) \geq \delta_{\mathsf{min}}([\alpha_1\mathbf{u} + z_i^*\alpha_2\mathbf{u} - d\cdot\mathbf{1}]) - \|\mathbf{w}\|_\infty \geq d$. □

Proof of Theorem 8. Throughout the proof, we will denote $(\mathbf{x}, z)$ the output of PreSamp, $z^* = z + \mathbf{a}^\top\mathbf{x}$ (the chosen value of z) and $(\mathbf{x}_i, z_i^*)_{i=1}^\nu$ the values sampled at each round[18]. Just within the scope of this proof, let $\iota : (\mathbb{N}\cup\{\perp\})^{\eta_3} \to \mathbb{N}^{\eta_3}$ be the identity over $\mathbb{N}^{\eta_3}$ and $\mathbf{0}$ elsewhere (i.e. ι is zero if one or more entries are $\perp$), and let $\delta^* = \iota\circ\delta$ (i.e. δ^* defaults to $\mathbf{0}$ if one or more entry do not have finite distance). Analogously $\delta_2^* = \iota\circ\delta_2$.

Let us define the sets:

$$\begin{aligned}\mathcal{W}^* &:= \{(\mathbf{x}_0, z_0^*) \in \mathbb{F}_2^{\eta_2}\times\mathbb{F}_q \,:\, B(M_1\oplus M_2)\mathbf{x}_0 = \mathbf{t}\oplus B\delta_2^*([\mathbf{v} + z_0^*\mathbf{u}]) \mod 2\} \\ \mathcal{V}^* &:= \{(\mathbf{x}_0, z_0^*) \in \mathcal{W}^* \,:\, \delta_{\mathsf{min}}([\mathbf{v} + z_0^*\mathbf{u} - M_1\mathbf{x}_0]) \geq d\}\end{aligned}$$

The proof then comprises three steps. First, using the fact that the fibers of $\mathcal{W}^*$ for any z_0^* are vector spaces of the same dimension, we claim that

Claim 7. *For each $i \in \{1,\ldots,\nu\}$, $(\mathbf{x}_i, z_i^*)$ is uniform in $\mathcal{W}^*$.*

Next, using Lemma 6, and calling again Bad the event that PreSamp returns $\perp$,

Claim 8. $(\mathbf{x}, z^*)_{|\neg\mathsf{Bad}}$ *is uniformly distributed over $\mathcal{V}^*$.*

Finally, let $\mathcal{V}$ be the target set, that is

$$\mathcal{V} := \left\{(\mathbf{x}_0, z_0) \in \mathbb{F}_2^{\eta_2}\times\mathbb{F}_q \;\middle|\; \begin{array}{l}\delta_{\mathsf{min}}([\mathbf{v} + A\mathbf{x}_0 + z_0\mathbf{u}]) \geq d \\ B\delta_2([\mathbf{v} + A\mathbf{x}_0 + z_0\mathbf{u} + M_2\mathbf{x}_0]) = \mathbf{t}\end{array}\right\}$$

We define a map $\psi : \mathcal{V}^* \to \mathcal{V}$ such that $\psi(\mathbf{x}_0, z_0^*) = (\mathbf{x}_0, z_0^* + \mathbf{a}^\top\mathbf{x}_0)$.

Claim 9. *The map $\psi : \mathcal{V}^* \to \mathcal{V}$ is a well defined bijection.*

From the last two claims, as conditioning on ¬Bad we have $(\mathbf{x}, z) = \psi(\mathbf{x}, z^*)$ and in this case $(\mathbf{x}, z^*)_{|\neg\mathsf{Bad}}$ is uniform over $\mathcal{V}^*$, then $(\mathbf{x}, z)_{|\neg\mathsf{Bad}}$ is uniform over $\mathcal{V}$. □

[18] Technically, these are only well defined if PreSamp does not terminate before the ν-th cycle. For the sake of a simpler analysis we may assume PreSamp to (more inefficiently) first compute all $(\mathbf{x}_i, z_i^*)_{i=1}^\nu$ and then continue with the first valid pair. Note this does not change the output distribution of PreSamp.

Proof of Claim 7. Consider the second-component projection $\pi : \mathcal{W}^* \to \mathbb{F}_q$. For any $z_0^* \in \mathbb{F}_q$, then $\pi^{-1}(z_0^*)$ consists of all the vectors $\mathbf{x}_0 \in \mathbb{F}_2^{\eta_2}$ such that $B(M_1 \oplus M_2)\mathbf{x}_0 = \mathbf{t} \oplus B\delta_2^*([\mathbf{v} + z_0^*\mathbf{u}])$. In particular $\pi^{-1}(z_0^*)$ is an $\mathbb{F}_2$ vector space, and since by hypothesis $M_1 \oplus M_2$ and B are full rank, $\dim(\pi^{-1}(z_0^*)) = \eta_2 - \eta_1$ and so $|\pi^{-1}(z_0^*)| = 2^{\eta_2 - \eta_1}$. Hence π is a perfectly balanced function.

Let now $(\widehat{\mathbf{x}}, \widehat{z}^*)$ be uniform over $\mathcal{W}^*$. We will prove $\Delta((\widehat{\mathbf{x}}, \widehat{z}^*), (\mathbf{x}_i, z_i^*)) = 0$. First, as π is perfectly balanced, then $\widehat{z}^* = \pi(\widehat{\mathbf{x}}^*, \widehat{z}^*)$ is uniform over $\mathbb{F}_q$ and so $\Delta(\widehat{z}^*, z^*) = 0$. Next, conditioning on $\widehat{z}^* = z_0^* = z_i^*$ for any $z_0^* \in \mathbb{F}_q$, by Lemma 7 $\widehat{\mathbf{x}}_{|\widehat{z}^* = z_0^*}$ is uniform over $\pi^{-1}(z_0^*)$. By construction, when $z_i^* = z_0^*$, then $S_i = \pi^{-1}(z_0^*)$ and so $\mathbf{x}_{i|z_i^* = z_0^*}$ is also uniform over $\pi^{-1}(z_0^*)$. Hence by Lemma 4

$$\Delta(\widehat{\mathbf{x}}_{|\widehat{z}^* = z_0^*}, \mathbf{x}_{i|z_i^* = z_0^*}) \;=\; 0 \quad \Rightarrow \quad \Delta((\widehat{\mathbf{x}}, \widehat{z}^*), (\mathbf{x}_i, z_i^*)) \;=\; 0. \qquad \square$$

Proof of Claim 8. As noted in the proof of Claim 7, the rank assumption on $M_1 \oplus M_2$ and B implies that the check at line 7 never fails. Hence, by Claim 7, the distribution of $(\mathbf{x}, z^*)$ (where we recall, $z^* \coloneqq z + \mathbf{a}^\top \mathbf{x}$) is equivalent to sampling $(\mathbf{x}_1, z_1^*), \ldots, (\mathbf{x}_\nu, z_\nu^*) \leftarrow^{\$} \mathcal{W}^*$ and returning the I-th with I being the smallest index such that $(\mathbf{x}_I, z_I^*) \in \mathcal{V}^*$, if at least one exists, or $\perp$ otherwise. By Lemma 6 it follows that given $\neg\mathsf{Bad}$, i.e. that at least one such index exists, then $(\mathbf{x}, z^*)_{|\neg\mathsf{Bad}}$ is uniform over $\mathcal{V}^*$. $\square$

Proof of Claim 9. $\psi : \mathcal{V}^* \to \mathbb{F}_2^{\eta_2} \times \mathbb{F}_q$ is a well defined, injective function. To conclude it suffices to prove $\psi(\mathcal{V}^*) = \mathcal{V}$.

Inclusion $\psi(\mathcal{V}^*) \subseteq \mathcal{V}$. Let $(\mathbf{x}, z) \in \psi(\mathcal{V})$. Then $(\mathbf{x}, z) = (\mathbf{x}, z^* - \mathbf{a}^\top \mathbf{x})$ with $(\mathbf{x}, z^*) \in \mathcal{V}^*$. We split the membership proof of $(\mathbf{x}, z) \in \mathcal{V}$ in two:

1. $\delta_{\mathsf{min}}([\mathbf{v} + A\mathbf{x} + z\mathbf{u}]) \geq d$. We begin observing that

$$\begin{aligned} A\mathbf{x} + z\mathbf{u} \;&=\; (\mathbf{u} \otimes \mathbf{a} - M_1)\mathbf{x} + (z^* - \mathbf{a}^\top \mathbf{x})\mathbf{u} \\ &=\; (\mathbf{a}^\top \mathbf{x}) \cdot \mathbf{u} - M_1\mathbf{x} + z^*\mathbf{u} - (\mathbf{a}^\top \mathbf{x}) \cdot \mathbf{u} \\ &=\; z^*\mathbf{u} - M_1\mathbf{x} \end{aligned}$$

   where we used the fact that $(\mathbf{u} \otimes \mathbf{a})\mathbf{x} = (\mathbf{a}^\top \mathbf{x}) \cdot \mathbf{u}$. Therefore

$$\delta_{\mathsf{min}}([\mathbf{v} + A\mathbf{x} + z\mathbf{u}]) \;=\; \delta_{\mathsf{min}}([\mathbf{v} + z^*\mathbf{u} - M_1\mathbf{x}]) \;\geq\; d.$$

2. $B\delta_2([\mathbf{v} + A\mathbf{x} + z\mathbf{u} + M_2\mathbf{x}]) = \mathbf{t}$. In order to exploit the preimage equation in the definition of $\mathcal{V}^*$, we first observe that $\delta_2^*([\mathbf{v} + z^*\mathbf{u}]) = \delta_2([\mathbf{v} + z^*\mathbf{u}])$. Indeed

$$\begin{aligned} \delta([\mathbf{v} + z^*\mathbf{u}]) \;&=\; \delta([\mathbf{v} + z^*\mathbf{u} - M_1\mathbf{x} + M_1\mathbf{x}]) \\ &=\; \delta([\mathbf{v} + z^*\mathbf{u} - M_1\mathbf{x}]) - M_1\mathbf{x} \\ \Rightarrow \quad \delta_{\mathsf{min}}([\mathbf{v} + z^*\mathbf{u}]) \;&\geq\; \delta_{\mathsf{min}}([\mathbf{v} + z^*\mathbf{u} - M_1\mathbf{x}]) - \|M_1\mathbf{x}\|_\infty \\ &\geq\; d - \|M_1\|_\infty \;\geq\; 0. \end{aligned}$$

The second equality is Lemma 3 since the first term on the RHS has distance greater that $d \geq \|M_1\|_\infty \geq \|M_1\mathbf{x}\|$ (since $\|\mathbf{x}\|_\infty \leq 1$). The implication follows lower-bounding the first term and upper-bounding the second on the RHS when taking the minimum. The second inequality follows as $(\mathbf{x}, z^*) \in \mathcal{V}^*$ and again since $\|M_1\mathbf{x}\|_\infty \leq \|M_1\|_\infty$. The last inequality holds by our hypothesis on d. In particular, as $\mathbf{v} + z^*\mathbf{u}$ has finite distance, by construction δ_2 and δ_2^* take the same, non $\perp$, value on this vector. We can finally conclude,

$$\begin{aligned} B\delta_2([\mathbf{v} + A\mathbf{x} + z\mathbf{u} + M_2\mathbf{x}]) &= B\delta_2([\mathbf{v} + z^*\mathbf{u} - M_1\mathbf{x} + M_2\mathbf{x}]) \\ &= B\delta_2([\mathbf{v} + z^*\mathbf{u}]) \oplus B(M_1 \oplus M_2)\mathbf{x} \\ &= B\delta_2^*([\mathbf{v} + z^*\mathbf{u}]) \oplus B(M_1 \oplus M_2)\mathbf{x} \\ &= \mathbf{t}. \end{aligned}$$

The first equality follows as $A\mathbf{x} + z\mathbf{u} = z^*\mathbf{u} - M_1\mathbf{x}$, and the second one is by Corollary 1.

Inclusion $\mathcal{V} \subseteq \psi(\mathcal{V}^*)$. Let $(\mathbf{x}, z) \in \mathcal{V}$. Then $(\mathbf{x}, z) = \psi(\mathbf{x}, z^*)$ with $z^* = z + \mathbf{a}^\top\mathbf{x}$. It suffices to prove that $(\mathbf{x}, z^*) \in \mathcal{V}^*$.

1. $\delta_{\mathsf{min}}(\mathbf{v} + z^*\mathbf{u} - M_1\mathbf{x}) \geq d$ follows as before using the identity $A\mathbf{x} + z\mathbf{u} = z^*\mathbf{u} - M_1\mathbf{x}$.
2. $B\delta_2^*([\mathbf{v} + z^*\mathbf{u}]) \oplus B(M_1 \oplus M_2)\mathbf{x} = \mathbf{t}$. As before we rely on Corollary 1.

$$\begin{aligned} \mathbf{t} &= B\delta_2([\mathbf{v} + A\mathbf{x} + z\mathbf{u} + M_2\mathbf{x}]) \\ &= B\delta_2([\mathbf{v} + z^*\mathbf{u} - M_1\mathbf{x} + M_2\mathbf{x}]) \\ &= B\delta_2([\mathbf{v} + z^*\mathbf{u}]) \oplus B(M_1 \oplus M_2)\mathbf{x} \\ &= B\delta_2^*([\mathbf{v} + z^*\mathbf{u}]) \oplus B(M_1 \oplus M_2)\mathbf{x} \end{aligned}$$

where again we used the identity $A\mathbf{x} + z\mathbf{u} = z^*\mathbf{u} - M_1\mathbf{x}$ in the second equation. The third equation follows by Corollary 1 and the previous point in this inclusion proof. The fourth finally follows as $B\delta_2([\mathbf{v} + z^*\mathbf{u}])$ takes value in $\mathbb{F}_2^{\eta_1}$, that is $\mathbf{t} \oplus B(M_1 \oplus M_2)\mathbf{x}$. Hence δ_2 and δ_2^* have the same output on $[\mathbf{v} + z^*\mathbf{u}]$. □

D Postponed Proofs: Constructions

D.1 Selectively Secure Scheme: Claims

Proof of Claim 1. The proof consists of two parts: First, we prove that, conditioning to $\mathsf{pv}^* = \mathsf{pv}_0^* = \widehat{\mathsf{pv}}^*$ and $k = k_0$ (which is necessary to define the set $\mathcal{U}^*$), sampling $(\mathbf{x}, z^*) \leftarrow^{\$} \mathcal{U}^*$ implies that $\mathbf{x}$ has high min-entropy. Then we conclude combining the LHL with an averaging argument.

For the first step, observe that sampling $(\mathbf{y}, w^*) \leftarrow^{\$} \mathsf{Samp}([A_2], [\mathbf{u}], d, \mathsf{dp})$ (see Figure 3), consist of

1. Sampling ν variables $(\mathbf{y}_i, w_i^*)$ uniformly in $\mathbb{F}_2^{n_2} \times \mathbb{F}_q$; and

2. Returning $(\mathbf{y}_I, w^*_I)$ for I a random variable distributed in $\{1, \ldots, \nu, \perp\}$, where $I = \perp$ iff Samp abort.

Since we conditioned on $k = k_0 \in \mathcal{K}^*_1$, then $\Pr[I = \perp] \leq \varepsilon_1(\lambda) \leq 1/2$ and in particular, by Lemma 8, projecting on the first component

$$\mathrm{H}_\infty\big(\mathbf{y}_{|I\neq\perp}\big) \;\geq\; n_2 - \log\nu + \log\Pr[I \neq \perp] \;\geq\; n_2 - \log(2\lambda) - 1.$$

Since by Theorem 4, if $(\mathbf{y}, w^*)$ is not $\perp$, it is uniform in $\mathcal{U}^*$. Therefore the tuple follows same distribution of $(\mathbf{x}, w^*)$ and in particular $\mathbf{y}, \mathbf{x}$ are identically distributed. Hence

$$\begin{aligned}\mathrm{H}_\infty\big(\mathbf{x} \,\big|\, \mathbf{a}_2^\top\mathbf{x} + z^*\big) \;&\geq\; \mathrm{H}_\infty(\mathbf{x}) - \log q \;=\; \mathrm{H}_\infty\big(\mathbf{y}_{|I\neq\perp}\big) - \log q \\ &\geq\; n_2 - \log(2\lambda) - 1 - \log q \;=\; n_1 + 4\lambda\end{aligned}$$

Next, observe that B_2 is distributed independently from $\rho, \mathbf{a}_1, \mathbf{a}_2, \mathbf{u}, \mathbf{t}, k$ by construction, and from $M^* = B_1 \oplus (P_{m^*} B_2)$ since B_1 is uniformly sampled and independent from B_2. Hence, B_2 is uniform in $\mathbb{F}_2^{n_1,n_2}$ and independent from[19] (x, z^*) conditioning on $\mathsf{pv}^* = \mathsf{pv}^*_0$ and $k = k_0$. Since $\mathbb{F}_2^{n_1,n_2}$ is a UHF family of output length n_1, by Theorem 1 we have that for a uniformly sampled $\mathbf{s} \leftarrow^{\$} \mathbb{F}_2^{n_1}$

$$\begin{aligned}2^{-2\lambda} \;&\geq\; \Delta((B_2, \mathbf{a}_2^\top\mathbf{x} + z^*, B_2\mathbf{x}), (B_2, \mathbf{a}_2^\top\mathbf{x} + z^*, \mathbf{s})) \\ &=\; \mathbb{E}_{B_2}\left[\,\Delta((\mathbf{a}_2^\top\mathbf{x} + z^*, B_2\mathbf{s}), (\mathbf{a}_2^\top\mathbf{x} + z^*, \mathbf{s}))\right].\end{aligned}$$

By Markov we thus conclude that $\Pr[B_2 \notin \mathcal{B}_2 | \mathsf{pv}^* = \mathsf{pv}^*_0, k = k_0] \leq 2^{-\lambda}$. □

Proof of Claim 2. For ease of notation let us denote $m, \widehat{m}$ the i-th message of $\mathcal{D}$ in the two games, which is a deterministic function of $\mathsf{pv}_i, \widehat{\mathsf{pv}}_i$ respectively, and $\sigma = \sigma_i, \widehat{\sigma} = \widehat{\sigma}_i$. Furthermore, as all relations will be studied given $\mathsf{pv}_i = \mathsf{pv}_{i,0} = \widehat{\mathsf{pv}}_i$ we omit such condition and instead assume all probability in this proof are taken in the relative measure conditioning to $\mathsf{pv}_i = \mathsf{pv}_{i,0} = \widehat{\mathsf{pv}}_i$.

We need to upper bound the following statistical distance

$$\begin{aligned}\Delta(\sigma, \widehat{\sigma}) \;&=\; \Delta\left((\mathbf{x}_1, \mathbf{x}_2, z),\, (\widehat{\mathbf{x}}_1, \widehat{\mathbf{x}}_2, \widehat{z})\right) \\ &=\; \Delta\left((\mathbf{x}_1, \mathbf{x}_2, z - \mathbf{a}_1^\top\mathbf{x}_1),\, (\widehat{\mathbf{x}}_1, \widehat{\mathbf{x}}_2, \widehat{z} - \widehat{\mathbf{a}}_1^\top\widehat{\mathbf{x}}_1)\right) \\ &=\; \Delta\left((\mathbf{x}_1, \mathbf{x}_2, z^*),\, (\widehat{\mathbf{x}}_1, \widehat{\mathbf{x}}_2, \widehat{z}^*)\right)\end{aligned}$$

where $z^* \coloneqq z - \mathbf{a}_1^\top\mathbf{x}_1$ and $\widehat{z}^* \coloneqq \widehat{z} - \widehat{\mathbf{a}}_1^\top\widehat{\mathbf{x}}_1$. In order to apply Theorem 1 we define the following set and functions:

$$\begin{aligned}\mathcal{U}^* \;&=\; \{(\mathbf{x}, z^*) \in \mathbb{F}_2^{n_2} \times \mathbb{F}_q \;:\; \delta_{\mathsf{min}}([A_2\mathbf{x} + z^*\mathbf{u}]) \geq d\} \\ f_1 : \mathbb{F}_2^{n_2} \to \mathbb{F}_2^{n_2} \quad &: \quad f_1(\mathbf{x}_1) = \mathbf{x}_1 \oplus \mathbf{t} \\ f_2 : \mathcal{U}^* \to \mathbb{F}_2^{n_2} \quad &: \quad f_2(\mathbf{x}_2, z^*) = \delta_2([A_2\mathbf{x}_2 + z^*\mathbf{u} + M\mathbf{x}_2])\end{aligned}$$

where $M = B_1 \oplus (P_m B_2)$. To conclude we will need the following claims:

[19] as (x, z^*) is a function of the random coins in Samp, $\mathbf{a}_2$, $\mathbf{u}$, M^*, k, $\mathbb{G}$, which are already fixed and independent from B_2

Claim 10. *For all* $(\mathbf{x}_2, z^*) \in \mathcal{U}^*$

$$f_2(\mathbf{x}_2, z^*) \;=\; \delta_2\left(\left[(\mathbf{a}_2^\top \mathbf{x}_2 + z^*)\cdot \mathbf{u}\right]\right) \oplus (P_{m-m^*}B_2)\mathbf{x}_2$$

Claim 11. f_1 *is* 0*-balanced and* f_2 *is* $2^{-\lambda}$*-balanced.*

Next, let $(\mathbf{y}_2, w^*) \leftarrow^{\$} \mathcal{U}^*$, $\mathbf{y}_2 \leftarrow^{\$} f_1^{-1}(f_2(\mathbf{y}_2, w^*))$. Analogously, sample $\widehat{\mathbf{y}}_1 \leftarrow^{\$} \mathbb{F}_2^{n_1}$ and $(\widehat{\mathbf{y}}_2, \widehat{w}^*) \leftarrow^{\$} f_2^{-1}(f_1(\widehat{\mathbf{y}}_1))$. Then we can further claim:

Claim 12. $\Delta((\mathbf{x}_1, \mathbf{x}_2, z^*), (\mathbf{y}_1, \mathbf{y}_2, w^*)) \le \varepsilon_1(\lambda)$.

Claim 13. $\Delta((\widehat{\mathbf{x}}_1, \widehat{\mathbf{x}}_2, \widehat{z}^*), (\widehat{\mathbf{y}}_1, \widehat{\mathbf{y}}_2, \widehat{w}^*)) \le \varepsilon_2(\lambda)$.

Given the Claim we conclude by Lemma 1 since

$$\begin{aligned}\Delta((\mathbf{x}_1, \mathbf{x}_2, z^*), (\widehat{\mathbf{x}}_1, \widehat{\mathbf{x}}_2, \widehat{z}^*)) \;&\le\; \Delta((\mathbf{x}_1, \mathbf{x}_2, z^*), (\mathbf{y}_1, \mathbf{y}_2, w^*)) + \\ &+\; \Delta((\mathbf{y}_1, \mathbf{y}_2, w^*), (\widehat{\mathbf{y}}_1, \widehat{\mathbf{y}}_2, \widehat{w}^*)) + \\ &+\; \Delta((\widehat{\mathbf{y}}_1, \widehat{\mathbf{y}}_2, \widehat{w}^*), (\widehat{\mathbf{x}}_1, \widehat{\mathbf{x}}_2, \widehat{z}^*)) \\ &\le\; \varepsilon_1(\lambda) + 2^{-\lambda} + \varepsilon_2(\lambda). \qquad \square\end{aligned}$$

Proof of Claim 10. As we restrict $(\mathbf{x}_2, z^*) \in \mathcal{U}^*$, and since $d \ge n_2$ is greater than both $\|M^*\mathbf{x}_2\|_\infty$ and $\|M\mathbf{x}_2\|_\infty$, applying Corollary 1 we have that

$$\begin{aligned} f_2(\mathbf{x}_2, z^*) \;&=\; \delta_2\left([A_2\mathbf{x}_2 + z^*\mathbf{u} + M\mathbf{x}_2]\right) \\ &=\; \delta_2\left(\left[(\mathbf{u}\otimes\mathbf{a}_2 - M^*)^\top \mathbf{x}_2 + z^*\mathbf{u} + M\mathbf{x}_2\right]\right) \\ &=\; \delta_2\left(\left[(\mathbf{a}_2^\top\mathbf{x}_2 + z^*)\cdot\mathbf{u}\right]\right) \oplus (M^* \oplus M)\mathbf{x}_2. \end{aligned}$$

Moreover, as $M^* = B_1 \oplus (P_{m^*}B_2)$ and $M = B_1 \oplus (P_m B_2)$, then $M^* \oplus M = (P_{m^*} \oplus P_m)B_2 = P_{m-m^*}B_2$ by Theorem 2. Note that as we operate modulo 2, then $m - m^* = m + m^*$. $\square$

Proof of Claim 11. f_1 is 0-balanced because it is a permutation. Regarding f_2, given $(\mathbf{x}_2, z^*) \leftarrow^{\$} \mathcal{U}^*$ we will show that $f_2(\mathbf{x}_2, z^*)$ has statistical distance at most $2^{-\lambda}$ from the uniform distribution.

By construction $B_2 = B_{2,0} \in \mathcal{B}_2$ implies that for a uniformly sampled $\mathbf{s} \leftarrow^{\$} \mathbb{F}_2^{n_1}$

$$\begin{aligned} 2^{-\lambda} \;&\ge\; \Delta\left((\mathbf{a}_2^\top\mathbf{x}_2 + z^*, B_2\mathbf{x}_2), (\mathbf{a}_2^\top\mathbf{x}_2 + z^*, \mathbf{s})\right) \\ &\ge\; \Delta\left(\delta_2\left(\left[(\mathbf{a}_2^\top\mathbf{x}_2 + z^*)\mathbf{u}\right]\right) \oplus P_{m-m^*}B_2\mathbf{x}_2,\; \delta_2\left(\left[(\mathbf{a}_2^\top\mathbf{x}_2 + z^*)\mathbf{u}\right]\right) \oplus P_{m-m^*}\mathbf{s}\right) \\ &=\; \Delta\left((f_2(\mathbf{x}_2, z^*), \delta_2\left(\left[(\mathbf{a}_2^\top\mathbf{x}_2 + z^*)\cdot\mathbf{u}\right]\right) \oplus P_{m-m^*}\mathbf{s}\right) \end{aligned}$$

where the second inequality follows by applying to both sides the same function, while the equality follows from Claim 10. Finally, since $m \ne m^*$, P_{m-m^*} is an invertible matrix and $P_{m-m^*}\mathbf{s}$ is uniformly distributed and independent from $\mathbf{x}_2, z^*$. Hence the term $\delta_2\left(\left[(\mathbf{a}_2^\top\mathbf{x}_2 + z^*)\cdot\mathbf{u}\right]\right) \oplus P_{m-m^*}\mathbf{s}$ is uniform in $\mathbb{F}_2^{n_2}$, concluding the proof. $\square$

Proof of Claim 12. By construction $(\mathbf{x}_2, z^*)$ is the output of $\mathsf{Samp}([A_2], [\mathbf{u}], d, \mathsf{dp})$. Let bad the event in which $(\mathbf{x}_2, z^*) = \perp$, occurring when Samp aborts. As we conditioned on $k = k_0 \in \mathcal{K}_1^*$, by Theorem 5 we have that $\Pr[\mathsf{bad}] \leq \varepsilon_1(\lambda)$. Moreover, by Theorem 4, we have that conditioning on $\neg\mathsf{bad}$, then $(\mathbf{x}_2, z^*)$ is uniform over $\mathcal{U}^*$. Therefore

$$\begin{aligned}
&\Delta((\mathbf{x}_2, z^*), (\mathbf{y}_2, w^*)) \ \leq \\
&\leq \Pr[\mathsf{bad}] \cdot \Delta((\mathbf{x}_2, z^*)_{|\mathsf{bad}}, (\mathbf{y}_2, w^*)) + \Pr[\neg\mathsf{bad}] \cdot \Delta((\mathbf{x}_2, z^*)_{|\neg\mathsf{bad}}, (\mathbf{y}_2, w^*)) \\
&\leq \Pr[\mathsf{bad}] + \Delta((\mathbf{x}_2, z^*)_{|\neg\mathsf{bad}}, (\mathbf{y}_2, w^*)) \\
&= \Pr[\mathsf{bad}] \ \leq \ \varepsilon_1(\lambda).
\end{aligned}$$

Next, conditioning on $\mathbf{x}_2 = \widetilde{\mathbf{x}}_2 = \mathbf{y}_2$ and $z^* = \widetilde{z}^* = w^*$ for any $(\widetilde{\mathbf{x}}_2, \widetilde{z}^*) \in \mathcal{U}^*$, we study the distribution of $\mathbf{x}_1, \mathbf{y}_1$. By construction

$$\begin{aligned}
\mathbf{x}_1 \ &= \delta_2([A_2\mathbf{x}_2 + z^*\mathbf{u}]) \oplus M\mathbf{x}_2 \oplus \mathbf{t} \ = \ \delta_2([A_2\mathbf{x}_2 + z^*\mathbf{u} + M\mathbf{x}_2]) \oplus \mathbf{t} \\
&= f_1^{-1}(f_2(\mathbf{x}_2, z^*)) \ = \ f_1^{-1}(f_2(\mathbf{y}_2, w^*)) \ = \ \mathbf{y}_1
\end{aligned}$$

where the second equality follows by Corollary 1 since $\delta_{\mathsf{min}}([A_2\mathbf{x}_2 + z^*\mathbf{u}]) \geq d \geq n_2 \geq \|M\mathbf{x}_2\|_\infty$. Hence $\mathbf{x}_1, \mathbf{y}_1$ have the same constant distribution. By Lemma 4 then

$$\Delta((\mathbf{x}_1, \mathbf{x}_2, z^*), (\mathbf{y}_1, \mathbf{y}_2, w^*)) \ \leq \ \Delta((\mathbf{x}_2, z^*), (\mathbf{y}_2, w^*)) \ \leq \ \varepsilon_1(\lambda).+$$

□

Proof of Claim 13. Recall $(\widehat{\mathbf{x}}_1, \widehat{\mathbf{x}}_2, \widehat{z})$ is the output of $\mathsf{S.Sign2}$ in Figure 6. By construction $\widehat{\mathbf{x}}_1, \widehat{\mathbf{y}}_1$ are uniformly sampled over $\mathbb{F}_2^{n_1}$. Hence they have zero statistical distance. Next, conditioning on $\widehat{\mathbf{x}}_1 = \widetilde{\mathbf{x}}_1 = \widehat{\mathbf{y}}_1$, we study the distance of $(\widehat{\mathbf{x}}_2, \widehat{z}^*)$ and $(\widehat{\mathbf{y}}_2, \widehat{w}^*)$.

Let bad the event $(\widehat{\mathbf{x}}_2, \widehat{z}) = \perp$. In order to apply Theorem 7

1. $\widehat{B}_2 \in \mathcal{B}_1$ implies $\widehat{B}_2$ is full rank. Since $\widehat{m} \neq \widehat{m}^*$, then P_{m-m^*} is invertible (Theorem 2) and therefore $\widehat{M}^* \oplus \widehat{M} = P_{\widehat{m}-\widehat{m}^*}\widehat{B}_2$ is full rank.
2. $\widehat{A}_1\widehat{\mathbf{x}}_1 = (\widehat{\mathbf{u}} \otimes \widehat{\mathbf{a}}_1)\widehat{\mathbf{x}}_1 = (\widehat{\mathbf{a}}_1^\top\widehat{\mathbf{x}}_1) \cdot \widehat{\mathbf{u}}$. Hence the first input of $\mathsf{PreSamp}$ is parallel to $[\widehat{\mathbf{u}}]$.
3. $d \geq n_2 \geq \|\widehat{M}^*\|_\infty$ and $d \geq n_2 \geq \|\widehat{M}\|_\infty$.

Hence, $\widehat{k} = k_0 \in \mathcal{K}_2^*$ implies $\Pr[\mathsf{bad}] \leq \varepsilon_2(\lambda)$. Furthermore by Theorem 8 we have that $(\widehat{\mathbf{x}}_2, \widehat{z})_{|\neg\mathsf{bad}}$ is uniform over

$$\left\{ (\mathbf{x}_0, z_0) \in \mathbb{F}_2^{n_2} \times \mathbb{F}_q \;\middle|\; \begin{array}{l} \delta_{\mathsf{min}}\left(\left[\widehat{A}_1\widehat{\mathbf{x}}_1 + \widehat{A}_2\mathbf{x}_0 + z_0\widehat{\mathbf{u}}\right]\right) \geq d \\ \delta_2\left(\left[\widehat{A}_1\widehat{\mathbf{x}}_1 + \widehat{A}_2\mathbf{x}_0 + z_0\widehat{\mathbf{u}} + \widehat{M}\mathbf{x}_0\right]\right) = \widehat{\mathbf{t}} \oplus \widehat{\mathbf{x}}_1 \end{array} \right\}.$$

Recalling that we defined $\widehat{z}^* = \widehat{z} + \widehat{\mathbf{a}}_1^\top\widehat{\mathbf{x}}_1$, and that $\widehat{\mathbf{t}} \oplus \widehat{\mathbf{x}}_1 = f_1(\widehat{\mathbf{x}}_1)$ we have that $(\widehat{\mathbf{x}}_2, \widehat{z}^*)_{|\neg\mathsf{bad}}$ is uniform over

$$\left\{ (\mathbf{x}_0, z_0^*) \in \mathbb{F}_2^{n_2} \times \mathbb{F}_q \;\middle|\; \begin{array}{l} \delta_{\mathsf{min}}\left(\left[\widehat{A}_2\mathbf{x}_0 + z_0^*\widehat{\mathbf{u}}\right]\right) \geq d \\ \delta_2\left(\widehat{A}_2\mathbf{x}_0 + z_0^*\widehat{\mathbf{u}} + \widehat{M}\mathbf{x}_0\right) \ = \ f_1(\widehat{\mathbf{x}}_1) \end{array} \right\}.$$

Notice the first condition means $(\mathbf{x}_0, z_0^*) \in \mathcal{U}^*$, while the second one is equivalent to $f_2(\mathbf{x}_0, z_0^*) = f_1(\widehat{\mathbf{x}}_1)$. Therefore $(\widehat{\mathbf{x}}_2, \widehat{z}^*)_{|\neg \mathsf{bad}}$ is uniform over $f_2^{-1}(f_1(\widehat{\mathbf{x}}_1))$ and in particular it follows the same distribution of $(\widehat{\mathbf{y}}_2, \widehat{w}^*)$. In conclusion

$$\Delta((\widehat{\mathbf{x}}_2, \widehat{z}^*), (\widehat{\mathbf{y}}_2, \widehat{w}^*)) \;\leq\; \Pr[\mathsf{bad}] \;\leq\; \varepsilon_2(\lambda)$$

which, by Lemma 4, implies $\Delta((\widehat{\mathbf{x}}_1, \widehat{\mathbf{x}}_2, \widehat{z}^*), (\widehat{\mathbf{y}}_1, \widehat{\mathbf{y}}_2, \widehat{w}^*)) \leq \varepsilon_2(\lambda)$. □

D.2 Adaptively Secure Scheme: Correctness

Proof of Theorem 11. The proof is analogous to that of Theorem 9. The main differences are that $\mathsf{S.Vfy}$ further checks the minimum distance, and that Samp's input depends on the message being signed. In order to bound the probability of $(\mathbf{x}_2, z^*) = \perp$, we will rely on Theorem 6 (as opposed to Theorem 5).
Regarding the first step, as per Table 3 we have $L > \log(10 n_2 d)$, $T > 2^L \cdot (1 + \ln(n_2)) + 2d$. Given $(\mathsf{vk}, \mathsf{sk}) \leftarrow^{\$} \mathsf{S.Gen}(1^\lambda)$, up to negligible probability we have $0 \neq u_i \neq u_j$ for all $i \neq j$. For any $m \in \mathbb{F}_2^\mu$ and $\sigma \leftarrow^{\$} \mathsf{S.Sign}(\mathsf{sk}, m)$, let us call $\alpha = \alpha_0 + m_1\alpha_1 + \ldots + m_\mu \alpha_\mu$. Then $\mathbf{u}^{(m)} = \alpha \mathbf{u}$, $A_1^{(m)} = \mathbf{u} \otimes (\alpha \cdot \mathbf{a}_1)$ and $A_2^{(m)} = \mathbf{u} \otimes (\alpha \cdot \mathbf{a}_2)$. If $\alpha = 0$, then the verifier always accepts. If $\alpha \neq 0$, conditioning on $\mathbf{u}$ satisfying the above conditions, also $\mathbf{u}^{(m)} = \alpha \mathbf{u}$ satisfies the same conditions; hence there exist a negligible $\varepsilon_1(\lambda)$ and a set $\widehat{\mathcal{K}}_1^* \subseteq \mathcal{K}_\lambda$ satisfying the three conditions of Theorem 6.
Next we argue that if $\sigma \neq \perp$ then the verifier accepts. By Theorem 4, $(\mathbf{x}_2, z^*) \neq \perp$ implies $\delta_{\mathsf{min}}([A_2^{(m)} \mathbf{x}_2 + z^* \mathbf{u}^{(m)}]) \geq d$ and so the verifier's condition in line 6, namely

$$\delta_{\mathsf{min}}([A_1^{(m)} \mathbf{x}_1 + A_2^{(m)} \mathbf{x}_2 + z \mathbf{u}^{(m)}]) \geq d,$$

holds true, since by construction $z = \mathbf{a}_1^\top \mathbf{x}_1 - z^*$. Regarding the second check we have that, calling $\sigma = (\mathbf{x}_1, \mathbf{x}_2, z)$

$$\begin{aligned}
& B \cdot \delta_2 \left(\left[A_1^{(m)} \mathbf{x}_1 + A_2^{(m)} \mathbf{x}_2 + z \mathbf{u}^{(m)} + B^+ \mathbf{x}_1 \right] \right) \\
&= B \cdot \delta_2 \left(\left[A_2^{(m)} \mathbf{x}_2 + z^* \mathbf{u}^{(m)} + B^+ \mathbf{x}_1 \right] \right) \\
&= B \cdot \delta_2 \left(\left[A_2^{(m)} \mathbf{x}_2 + z^* \mathbf{u}^{(m)} \right] \right) \oplus (B B^+ \mathbf{x}_1) \\
&= B \cdot \delta_2 \left(\left[A_2^{(m)} \mathbf{x}_2 + z^* \mathbf{u}^{(m)} \right] \right) \oplus \mathbf{x}_1 \;=\; \mathbf{t}
\end{aligned}$$

where the first equality follows because $z = \mathbf{a}_1^\top \mathbf{x}_1 - z^*$ and $A_1^{(m)} = \mathbf{u}^{(m)} \otimes \mathbf{a}_1$. The second one is by Lemma 3 as[20] $\|B^+ \mathbf{x}_1\|_\infty \leq n_1 \leq d$. The third follows as $B B^+ = I_{n_1}$. The last follows by construction of $\mathbf{x}_1$. Hence $\mathsf{S.Vfy}(\mathsf{vk}, \sigma, m) \to 1$ if $\sigma \neq \perp$.
Finally, to show $(\mathbf{x}_2, z^*) = \perp$ with negligible probability, we use the third implication of Theorem 6 (setting M as the zero matrix) because the image of $A_2^{(m)}$

[20] Note $B^+ \mathbf{x}_1 \in \mathbb{Z}^{n_2}$ is computed over the integers.

is in the linear span $\mathbf{u}$. Hence $\Pr\left[\mathsf{Samp}\left([A_2^{(m)}], [\mathbf{u}^{(m)}], d, \mathsf{dp}\right) = \perp\right] \leq \varepsilon_1(\lambda)$, which allows us to conclude that

$$\begin{aligned}\Pr\left[\mathsf{S.Vfy}(\mathsf{vk}, \sigma, m) = 0\right] &\leq \Pr\left[\sigma = \perp | \alpha = 0\right] + \Pr\left[\sigma = \perp | \alpha \neq 0\right] \\ &\leq 2\varepsilon_1(\lambda) + \frac{n_2(n_2+1)}{2q}.\end{aligned}$$

Notice that in the last inequality we used the fact that if $\alpha = 0$ then $\Pr[\sigma = \perp] = 0$ and we bounded the second term conditioning on the value of $\mathbf{u}^{(m)}$ (in the same way as we did in Theorem 9) in light of the remarks in the first step of this proof. □

D.3 Adaptively Secure Scheme: Unforgeability

Proof of Theorem 12. The proof combines techniques used in the proof of Theorem 2 with a partitioning strategy. We proceed through a sequence of hybrids against an adversary $\mathcal{A}$ which, without loss of generality, makes exactly $\vartheta = \vartheta(\lambda) = \mathsf{poly}(\lambda)$ queries.

- H_0: Real EUF-CMA game (see Figure 1).
- H_1: As H_0, but initially sample $h \leftarrow^{\$} \mathbb{F}_2^{\ell,\mu}$ and $y \leftarrow^{\$} \mathbb{F}_2^{\ell}$ where $\ell = \log(2\vartheta)$. At the end of the execution, let $m_1, \ldots, m_\vartheta$ the queried message and (m^*, σ^*) the final forgery. Return 1 iff the winning condition in H_1 is satisfied[21] and

$$h(m_1) \neq y, \quad \ldots \quad h(m_\vartheta) \neq y, \quad h(m^*) = y.$$

- H_2: As H_1, but when a signature for m such that $h(m) = y$ is requested, reply $\perp$.
- H_3: As H_2, but return 0 if $\left[\mathbf{u}_0 + m_1^*\mathbf{u}_1 + \ldots + m_\mu^*\mathbf{u}_\mu\right] = [\mathbf{0}]$.
- H_4: As H_3, but sample $\mathbf{u}_i \leftarrow^{\$} \mathbb{F}_q^{n_2}$ for $i \in \{0, \ldots, \mu\}$.
- H_5: As H_4, but sample $A_{2,i} \leftarrow^{\$} \mathbb{F}_q^{n_2, n_2}$ for $i \in \{0, \ldots, \mu\}$.
- H_6: As H_5, but set[22] $M_0 = P_y$, $M_i = P_{h(\mathbf{e}_i)}$ and $A_{2,i} \leftarrow \mathbf{u}_i \otimes \mathbf{a}_2 - M_i$ for all $i \in \{0, \ldots, \mu\}$.
- H_7: As H_6, but set $\mathbf{u}_i \leftarrow \alpha_i \cdot \mathbf{u}$ for uniformly sampled $\alpha_0, \ldots, \alpha_\mu \leftarrow^{\$} \mathbb{F}_q$.
- H_8: As H_7, but set $\mathsf{sk} = (\mathsf{vk}, \mathbf{a}_1, \mathbf{a}_2)$ and reply to each call $\mathcal{O}_{\mathsf{sk},Q}(m)$ with $\mathsf{S.Sign}((\mathsf{vk}, \mathbf{a}_1), m)$.
- H_9: As H_8, but reply to each call $\mathcal{O}_{\mathsf{sk},Q}(m)$ with $\mathsf{S.Sign2}(\mathsf{sk}, h, y, m)$, see Figure 10.
- H_{10}: As H_9, but sample $\mathbf{u}_i \leftarrow^{\$} \mathbb{F}_q^{n_2}$ for $i \in \{0, \ldots, \mu\}$.
- H_{11}: As H_{10}, but sample $A_{1,i} \leftarrow \mathbb{F}_q^{n_2, n_1}$ for $i \in \{0, \ldots, \mu\}$.
- H_{12}: As H_{11}, but set $A_{1,i} \leftarrow \mathbf{u}_i \otimes \mathbf{a}_1$ for $1 \leq i \leq \mu$ and $A_{1,0} \leftarrow \mathbf{u}_0 \otimes \mathbf{a}_1 - B^+$.

[21] i.e. (m^*, σ^*) is a valid forgery and m^* was not previously queried

[22] we denote $\mathbf{e}_1, \ldots, \mathbf{e}_\mu$ the canonical base of $\mathbb{F}_2^\mu$.

- H_{13}: As H_{12}, but set $\mathbf{u}_i \leftarrow \alpha_i \cdot \mathbf{u}$.

We will prove any adversary for H_0 wins in H_1 with comparable advantage up to a $1/4\vartheta$ factor loss, H_1 is not harder than H_2, H_2 is no harder than H_3 if the DLP is hard and the remaining hybrids are computationally indistinguishable. Finally, we show winning in H_{13} is statistically hard.

$\mathsf{S.Sign2}(\mathsf{sk}, h, y, m)$:

1 : Parse $\mathsf{sk} = (\mathsf{vk}, \mathbf{a}_1, \mathbf{a}_2)$
2 : Parse $\mathsf{vk} = (([A_{1,i}], [A_{2,i}], [\mathbf{u}_i])_{i=0}^{\mu}, \mathbf{t}, k, B, \mathbb{G})$
3 : $\mathsf{dp} \leftarrow (\mathbb{G}, G, q, k, L, T)$ // deriving G, q from $\mathbb{G}$
4 : // Evaluate Algebraic Hash
5 : $[A_1^{(m)}] \leftarrow \left[A_{1,0} + \sum_{i=1}^{\mu} m_i A_{2,i}\right]$, $[\mathbf{u}^{(m)}] \leftarrow \left[\mathbf{u}_0 + \sum_{i=1}^{\mu} m_i \mathbf{u}_i\right]$
6 : $M_0 \leftarrow P_y$, $M_i \leftarrow P_{h(\mathbf{e}_i)}$ // $\in \mathbb{F}_2^{n_2, n_2}$
7 : $M^{(m)} \leftarrow M_0 + \sum_{i=1}^{\mu} m_i M_i$ // $\in \mathbb{Z}^{n_2, n_2}$
8 : // Corner-case Signatures
9 : **If** $[\mathbf{u}^{(m)}] = [\mathbf{0}]$: **Return** $\sigma = \mathbf{0}$
10 : // Preimage-Sampling using $\mathbf{a}_2$
11 : $\mathbf{x}_1 \leftarrow^{\$} \mathbb{F}_2^{n_1}$
12 : $[\mathbf{v}] \leftarrow [A_1^{(m)} \mathbf{x}_1]$ // $\in \mathbb{F}_q^{n_2}$
13 : $(\mathbf{x}_2, z) \leftarrow^{\$} \mathsf{PreSamp}([\mathbf{v}], [\mathbf{u}^{(m)}], \mathbf{a}_2, M^{(m)}, \Omega, B, \mathbf{t} \oplus \mathbf{x}_1, d, \mathsf{dp})$
14 : **Return** $\sigma = (\mathbf{x}_1, \mathbf{x}_2, z)$

Fig. 10: Alternative signature scheme using $\mathbf{a}_2$ to sign any m such that $h(m) \neq y$.

Advantage in $\mathsf{H}_0, \mathsf{H}_1$. We show $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{H}_0}(\lambda) \leq 4\vartheta \cdot \mathsf{Adv}_{\mathcal{A}}^{\mathsf{H}_1}(\lambda)$, where the advantage refers to the probability that a given hybrid returns 1 at the end of its execution with $\mathcal{A}$. Let $m_1, \ldots, m_\vartheta, m^*$ be as above, $Q = \{m_1, \ldots, m_\vartheta\}$ and $\mathsf{Valid} : \mathsf{S.Vfy}(\mathsf{vk}, m^*, \sigma^*) = 1$. Then

$$\begin{aligned} \mathsf{Adv}_{\mathcal{A}}^{\mathsf{H}_1}(\lambda) &= \Pr\left[h(m^*) = y \wedge (\wedge_{i=1}^{\vartheta} h(m_i) \neq y) \wedge m^* \notin Q \wedge \mathsf{Valid}\right] \\ &\geq \frac{1}{4\vartheta} \cdot \Pr\left[m^* \notin Q \wedge \mathsf{Valid}\right] = \frac{1}{4\vartheta} \cdot \mathsf{Adv}_{\mathcal{A}}^{\mathsf{H}_0}(\lambda) \end{aligned}$$

where the inequality is by Lemma 2, which can be applied since $\ell = \log(2\vartheta)$ and (h, y) are not given to the adversary and are in particular independent from $m_1, \ldots, m_\vartheta, m^*, \sigma^*$ and vk.

Advantage in $\mathsf{H}_1, \mathsf{H}_2$. Given an adversary $\mathcal{A}^*$ for H_1, we describe a reduction $\mathcal{R}$ breaking H_2. Initially $\mathcal{R}(1^\lambda, \mathsf{vk})$ runs $\mathcal{A}^*(1^\lambda, \mathsf{vk})$. When $\mathcal{A}^*$ queries a signature for m, $\mathcal{R}(1^\lambda, \mathsf{vk})$ forwards the query to get σ. If $\sigma = \perp$ it aborts, or else it forwards σ to $\mathcal{A}^*$. Finally, when $\mathcal{A}^*$ returns (m^*, σ^*), so does $\mathcal{R}$.

Call r the random coins of $\mathcal{A}^*$ and ρ those of H_1. Without loss of generality we can assume r to also be the random coins of $\mathcal{R}$, i.e. $\mathcal{R}(1^\lambda, \mathsf{vk}; r)$ runs $\mathcal{A}^*(1^\lambda, \mathsf{vk}; r)$. Similarly we can assume ρ are also the random coins of H_2, and that $\mathsf{H}_1(1^\lambda; \rho)$, $\mathsf{H}_2(1^\lambda; \rho)$ produce the same $\mathsf{vk}, \mathsf{sk}, h, y$ and signatures as long as no message m_i such that $h(m_i) = y$ is queried. Then for all fixed random tapes $r = r_0, \rho = \rho_0$, $\mathcal{R}$ wins in H_2 if $\mathcal{A}^*$ would win in H_1. Indeed if $\mathcal{A}^*$ would win in H_1, then it never queries m_i such that $h(m_i) = y$. In particular $\mathcal{R}$ does not abort and returns the same accepting (m^*, σ^*) as $\mathcal{A}^*$. Thus $\mathsf{Adv}^{\mathsf{H}_2}_{\mathcal{R}}(\lambda) \geq \mathsf{Adv}^{\mathsf{H}_1}_{\mathcal{A}^*}(\lambda)$.

Advantage in $\mathsf{H}_2, \mathsf{H}_3$. We show the hardness of H_2 reduces to that of H_3 and that of the discrete logarithm problem. Given $\mathcal{A}$, we describe $\mathcal{R}(\mathbb{G}, H_0, \ldots, H_\mu)$ finding a non-zero linear relation among these group elements, for randomly sampled $(H_i)_{i=0}^{\mu}$. The problem is tightly equivalent to the DLP due to random self-reducibility.

Calling $H_i = [\alpha_i]$, initially $\mathcal{R}$ samples $\mathbf{u}$, $\mathbf{a}_1, \mathbf{a}_2$ as per $\mathsf{S.Gen}$, assigning $[\mathbf{u}_i] = [\alpha_i \mathbf{u}]$ and $[A_{j,i}] = [\mathbf{u}_i \otimes \mathbf{a}_j]$. The public key vk is completed sampling $\mathbf{t}, k$ as in $\mathsf{S.Gen}$ and (h, y) as in H_1. Signature queries are answered with $\mathsf{S.Sign}(\mathsf{sk}, \cdot)$. Finally, when $\mathcal{A}$ returns (m^*, σ^*), the reduction returns $(1, m_1^*, \ldots, m_\mu^*)$.

Notice that by how we defined H_3, upon fixing the adversary's and hybrid's random coins, $\mathcal{A}$ wins in H_2 iff it either wins in H_3 or $[\mathbf{u}_0 + m_1^* \mathbf{u}_1 + \ldots + m_\mu^* \mathbf{u}_\mu] = [\mathbf{0}]$. When $\mathbf{u} \neq \mathbf{0}$ the latter is equivalent to $H_0 + m_1^* H_1 + \ldots + m_\mu^* H_\mu = 0$. Since $\mathcal{R}$ never returns a zero-vector (the first entry is always 1), calling Win_3 the event in which $\mathcal{A}$'s interaction would be accepting in H_3, then

$$
\begin{aligned}
\mathsf{Adv}^{\mathsf{H}_2}_{\mathcal{A}}(\lambda) \;&=\; \Pr\left[\left[\mathbf{u}_0 + \sum\nolimits_{i=1}^{\mu} m_i^* \mathbf{u}_i\right] = [\mathbf{0}] \;\vee\; \mathsf{Win}_3\right] \\
&\leq\; \Pr\left[\left[\mathbf{u}_0 + \sum\nolimits_{i=1}^{\mu} m_i^* \mathbf{u}_i\right] = [\mathbf{0}]\right] + \Pr\left[\mathsf{Win}_3\right] \\
&\leq\; \Pr\left[\left[\mathbf{u}_0 + \sum\nolimits_{i=1}^{\mu} m_i^* \mathbf{u}_i\right] = [\mathbf{0}] \wedge \mathbf{u} \neq \mathbf{0}\right] + \Pr\left[\mathbf{u} = \mathbf{0}\right] + \mathsf{Adv}^{\mathsf{H}_3}_{\mathcal{A}}(\lambda) \\
&\leq\; \Pr\left[H_0 + \sum\nolimits_{i=1}^{\mu} m_i^* H_i = 0\right] + \Pr\left[\mathbf{u} = \mathbf{0}\right] + \mathsf{Adv}^{\mathsf{H}_3}_{\mathcal{A}}(\lambda) \\
&=\; \mathsf{Adv}_{\mathcal{R}}(\lambda) + q^{-n_2} + \mathsf{Adv}^{\mathsf{H}_3}_{\mathcal{A}}(\lambda) \;=\; \mathsf{negl}(\lambda) + \mathsf{Adv}^{\mathsf{H}_3}_{\mathcal{A}}(\lambda).
\end{aligned}
$$

Indistinguishability of $\mathsf{H}_3, \mathsf{H}_4$. Given a distinguisher $\mathcal{D}$, we describe in Figure 11 a reduction $\mathcal{R}_1$ to $(n_2, \mu + 1)$-MDDH. Initially $\mathcal{R}_1(\mathbb{G}, [C])$ with $[C] \in \mathbb{G}^{n_2, \mu+1}$ sets $[\mathbf{u}_i]$ as the i-th column of $[C]$. Then, it computes $(\mathsf{vk}, \mathsf{sk})$ along with (h, y) as prescribed, setting $[A_{j,i}] = [\mathbf{u}_i \otimes \mathbf{a}_j]$, and replies to signature queries via $\mathsf{S.Sign}(\mathsf{sk}, \cdot)$ with $\mathsf{sk} = (\mathsf{vk}, \mathbf{a}_1)$.

By Lemma 9 and Corollary 2 $\mathcal{R}_1$ has negligible advantage in distinguishing a uniformly sampled $[C_1]$ from $[C_0]$ with $C_0 = \mathbf{v} \otimes \mathbf{w}$ and $\mathbf{v}, \mathbf{w}$ uniformly distributed respectively over $\mathbb{F}_q^{n_1}$ and $\mathbb{F}_q^{\mu+1}$.

When $C = C_0 = \mathbf{v} \otimes \mathbf{w}$, then the i-th column is of the form $v_i \cdot \mathbf{w}$ with $\mathbf{w}$ and v_i uniformly sampled over $\mathbb{F}_q^{n_1}$ and $\mathbb{F}_q$. Hence $[\mathbf{u}_0], \ldots, [\mathbf{u}_\mu]$ are distributed as in H_3. Moreover, all the remaining components are correctly computed as a randomized function of $[\mathbf{u}_0], \ldots, [\mathbf{u}_\mu]$. Hence $\mathcal{R}_1$ perfectly simulates H_3 to $\mathcal{D}$.

$\mathcal{R}_1(\mathbb{G}, [C])$: // $[C] \in \mathbb{G}^{n_2,\mu+1}$

Derive $(\mathbb{G}, G, q)$ from $\mathbb{G}$
Parse $[C]$ as $([\mathbf{c}_0], \ldots, [\mathbf{c}_\mu]) \in (\mathbb{G}^{n_2})^{\mu+1}$ and set $[\mathbf{u}_i] \leftarrow [\mathbf{c}_i]$
Sample $h \leftarrow^{\$} \mathbb{F}_2^{\ell,\mu}$ and $y \leftarrow^{\$} \mathbb{F}_2^{\ell}$
$\mathbf{a}_1 \leftarrow^{\$} \mathbb{F}_q^{n_1}$, $\mathbf{a}_2 \leftarrow^{\$} \mathbb{F}_q^{n_2}$, $\mathbf{t} \leftarrow^{\$} \mathbb{F}_2^{n_1}$, $k \leftarrow^{\$} \mathsf{SUF.Gen}(1^\lambda)$
$B \leftarrow^{\$} \mathbb{F}_2^{n_1,n_2}$ such that $\mathsf{rk}(B) = n_1$
$[A_{j,i}] \leftarrow [\mathbf{u}_i \otimes \mathbf{a}_j]$ for $j \in \{1,2\}$ and $i \in \{0,\ldots,\mu\}$
$\mathsf{vk} = (([A_{1,i}], [A_{2,i}], [\mathbf{u}_i])_{i=0}^{\mu}, \mathbf{t}, k, B, \mathbb{G})$, $\mathsf{sk} = (\mathsf{vk}, \mathbf{a}_1)$
Run $\mathcal{D}(\mathsf{vk})$
When $\mathcal{D}$ queries $m \in \{0,1\}^\mu$: Reply $\sigma \leftarrow^{\$} \mathsf{S.Sign}(\mathsf{sk}, m)$ if $h(m) \neq y$
When $\mathcal{D}$ returns b: **Return** b

Fig. 11: Reduction of the indistinguishability of $\mathsf{H}_3, \mathsf{H}_4$ to $(n_2, \mu+1)$-MDDH.

Conversely, when $C = C_1$ uniformly sampled, so is every column of C and in particular $[\mathbf{u}_0], \ldots, [\mathbf{u}_\mu]$ are uniformly sampled in $(\mathbb{G}^{n_2})^{\mu+1}$. Hence $\mathcal{R}_1$ simulates perfectly H_4 toward $\mathcal{D}$. We then conclude that

$$\mathsf{negl}(\lambda) \;=\; \mathsf{Adv}_{\mathcal{R}_1}(\lambda) \;=\; \mathsf{Adv}_{\mathcal{D}}^{\mathsf{H}_3,\mathsf{H}_4}(\lambda).$$

Indistinguishability of $\mathsf{H}_4, \mathsf{H}_5$. Given a distinguisher $\mathcal{D}$ we define in Figure 12 a reduction $\mathcal{R}_2$ to $(n_2(\mu+1), n_2+1)$-MDDH. Initially, given $[C]$, $\mathcal{R}_2$ isolates the first column $\mathbf{v} \in \mathbb{G}^{n_2(\mu+1)}$, from the remaining entries $[V] \in \mathbb{G}^{n_2(\mu+1),n_2}$. Next it splits both matrices vertically into $\mu+1$ blocks of height n_2. Precisely

$$[\mathbf{v}] \;=\; \begin{pmatrix} [\mathbf{v}_0] \\ \vdots \\ [\mathbf{v}_{\mu+1}] \end{pmatrix} \in (\mathbb{G}^{n_1})^{\mu+1}, \qquad [V] \;=\; \begin{pmatrix} [V_0] \\ \vdots \\ [V_{\mu+1}] \end{pmatrix} \in (\mathbb{G}^{n_1,n_2})^{\mu+1}.$$

It then assigns $[\mathbf{u}_i] = [\mathbf{v}_i]$ and $[A_{2,i}] = [V_i]$. Finally, to complete the public key, it samples $\mathbf{a}_1 \in \mathbb{F}_q^{n_1}$ and sets $[A_{1,i}]$ as $[\mathbf{u}_i \otimes \mathbf{a}_1]$. Signature queries are answered as prescribed in both games with $\mathsf{S.Sign}(\mathsf{sk}, m)$ where $\mathsf{sk} = (\mathsf{vk}, \mathbf{a}_1)$.

By Lemma 9 and 10, the advantage of $\mathcal{R}_2$ of distinguishing C_1 uniformly sampled from $C_0 = \mathbf{v} \otimes (1, \mathbf{w})$ is negligible. When $C = C_1$ all sub-matrices of C are uniformly sampled. Thus $[\mathbf{u}_i]$ and $[A_{2,i}]$ follow the same distribution as in H_5, and so $\mathcal{R}_2(\mathbb{G}, [C])$ perfectly simulates H_5. Conversely, when $C = C_0 = \mathbf{v} \otimes (1, \mathbf{w})$ we have that $\mathbf{u}_i$ are uniformly sampled because $\mathbf{v}$ is, and $A_{2,i} = \mathbf{u}_i \otimes \mathbf{w}$ for a uniformly sampled $\mathbf{w}$. Hence $\mathcal{R}_2(\mathbb{G}, [C_0])$ perfectly simulates H_4. In conclusion

$$\mathsf{negl}(\lambda) \;=\; \mathsf{Adv}_{\mathcal{R}_2}(\lambda) \;=\; \mathsf{Adv}_{\mathcal{D}}^{\mathsf{H}_4,\mathsf{H}_5}(\lambda).$$

Indistinguishability of $\mathsf{H}_5, \mathsf{H}_6$. Given a distinguisher $\mathcal{D}$, we detail in Figure 13 a reduction $\mathcal{R}_3$ to $(n_1(\mu+1), n_2+1)$-MDDH. Given $[C]$ it initially isolates the

$\mathcal{R}_2(\mathbb{G}, [C])$: // $[C] \in \mathbb{G}^{n_2(\mu+1), n_2+1}$

Derive $(\mathbb{G}, G, q)$ from $\mathbb{G}$

// Split the challenge matrix C in blocks

Parse $[C]$ as $([\mathbf{v}], [V]) \in \mathbb{G}^{n_2(\mu+1)} \times \mathbb{G}^{n_2(\mu+1), n_2}$

Split $[\mathbf{v}]$ into $([\mathbf{v}_0], \ldots, [\mathbf{v}_\mu])$ with $[\mathbf{v}_i] \in \mathbb{G}^{n_2}$

Split vertically $[V]$ into $([V_0], \ldots, [V_\mu])$ with $[V_i] \in \mathbb{G}^{n_2, n_2}$.

// Sample the UHF for partitioning

Sample $h \leftarrow^{\$} \mathbb{F}_q^{\ell,\mu}$ and $y \leftarrow^{\$} \mathbb{F}_2^{\ell}$

// Compute the verification and secret key

Set $[\mathbf{u}_i] = [\mathbf{v}_i]$ and $[A_{2,i}] = [V_i]$

Sample $\mathbf{a}_1 \leftarrow^{\$} \mathbb{F}_q^{n_1}$, $\mathbf{t} \leftarrow^{\$} \mathbb{F}_2^{n_1}$, $k \leftarrow^{\$} \mathsf{SUF.Gen}(1^\lambda)$, $B \leftarrow^{\$} \mathbb{F}_2^{n_1, n_2}$: $\mathsf{rk}(B) = n_1$

$[A_{j,i}] \leftarrow [\mathbf{u}_i \otimes \mathbf{a}_j]$ for $j \in \{1, 2\}$ and $i \in \{0, \ldots, \mu\}$

$\mathsf{vk} = (([A_{1,i}], [A_{2,i}], [\mathbf{u}_i])_{i=0}^{\mu}, \mathbf{t}, k, B, \mathbb{G})$, $\mathsf{sk} = (\mathsf{vk}, \mathbf{a}_1)$

Run $\mathcal{D}(\mathsf{vk})$ // Interact with the distinguisher

When $\mathcal{D}$ queries $m \in \{0,1\}^\mu$: Reply $\sigma \leftarrow^{\$} \mathsf{S.Sign}(\mathsf{sk}, m)$ if $h(m) \neq y$

When $\mathcal{D}$ returns b: **Return** b

Fig. 12: Reduction of the ind. of $\mathsf{H}_4, \mathsf{H}_5$ to $(n_2(\mu+1), n_2+1)$-MDDH.

first columns from the other entries, obtaining $[\mathbf{v}]$, $[V]$, and then splits both matrices vertically to obtain $\mu+1$ blocks $[\mathbf{v}_i]$, $[V_i]$ of height n_2. As per H_6, it proceeds sampling h, y and computing the matrices $M_0, M_1, \ldots, M_\mu$ in $\mathbb{F}_2^{n_2, n_2}$. It then assigns $[\mathbf{u}_i] = [\mathbf{v}_i]$ and $[A_{2,i}] = [V_i - M_i]$. The verification key is completed sampling $\mathbf{a}_1, \mathbf{t}, k$ as prescribed and setting $[A_{1,i}] = [\mathbf{u}_i \otimes \mathbf{a}_1]$. Signature queries for m are again answered with $\mathsf{S.Sign}(\mathsf{sk}, m)$ with $\mathsf{sk} = (\mathsf{vk}, \mathbf{a}_1)$.

By Lemma 9 and 10 the advantage of $\mathcal{R}_3$ in distinguishing C_1 uniformly sampled from $C_0 = \mathbf{v} \otimes (1, \mathbf{w})$ is negligible. Moreover, $C = C_1$ implies $\mathbf{v}_i, V_i$ uniformly sampled and in particular so are $\mathbf{u}_i = \mathbf{v}_i$ and $A_{2,i} = V_i - M_i$, since M_i are independent from C. Thus in this case $\mathcal{R}_3$ perfectly simulates H_5.

Conversely, for $C = C_0 = \mathbf{v} \otimes (1, \mathbf{w})$ we have that $\mathbf{u}_i = \mathbf{v}_i$ and $A_{2,i} = \mathbf{v}_i \otimes \mathbf{w} - M_i = \mathbf{u}_i \otimes \mathbf{w} - M_i$ for a uniformly sampled $\mathbf{w} \in \mathbb{F}_q^{n_2}$. Hence $\mathcal{R}_3$ perfectly simulates H_6. Therefore

$$\mathsf{negl}(\lambda) \;=\; \mathsf{Adv}_{\mathcal{R}_3}(\lambda) \;=\; \mathsf{Adv}_{\mathcal{D}}^{\mathsf{H}_5, \mathsf{H}_6}(\lambda).$$

Indistinguishability of $\mathsf{H}_6, \mathsf{H}_7$. Given a distinguisher $\mathcal{D}$, we provide a reduction $\mathcal{R}_4$ to $(n_1, \mu+1)$-MDDH. As done for $(\mathsf{H}_3, \mathsf{H}_4)$, given $C \in \mathbb{G}^{n_1, \mu+1}$, the adversary parses C into $\mu+1$ columns of length n_1, interpret them as $[\mathbf{u}_0], \ldots, [\mathbf{u}_\mu]$. It then samples $M_0, \ldots, M_\mu$ as specified in H_6, along with $\mathbf{a}_j$ for $j \in \{1, 2\}$, from which it computes $[A_{1,i}] = [\mathbf{u}_i \otimes \mathbf{a}_1]$ and $[A_{2,i}] = [\mathbf{u}_i \otimes \mathbf{a}_2 - M_i]$. Finally it completes vk with $\mathbf{t} \leftarrow^{\$} \mathbb{F}_2^{n_1}$ and $k \leftarrow^{\$} \mathsf{SUF.Gen}(1^\lambda)$ and replies to signature queries with $\mathsf{S.Sign}(\mathsf{sk}, m)$ with $\mathsf{sk} = (\mathsf{vk}, \mathbf{a}_1)$.

$\mathcal{R}_3(\mathbb{G}, [C])$: // $[C] \in \mathbb{G}^{n_2(\mu+1),n_2+1}$

Derive $(\mathbb{G}, G, q)$ from $\mathbb{G}$
// Split the matrix C in blocks
Parse $[C]$ as $([\mathbf{v}], [V]) \in \mathbb{G}^{n_2(\mu+1)} \times \mathbb{G}^{n_2(\mu+1),n_2}$
Split $[\mathbf{v}]$ into $([\mathbf{v}_0], \ldots, [\mathbf{v}_\mu])$ with $[\mathbf{v}_i] \in \mathbb{G}^{n_2}$
Split vertically $[V]$ into $([V_0], \ldots, [V]_\mu)$ with $[V_i] \in \mathbb{G}^{n_2,n_2}$.
// Sample the UHF and B for the partitioning
Sample $h \leftarrow^{\$} \mathbb{F}_2^{\ell,\mu}$, $y \leftarrow^{\$} \mathbb{F}_2^{\ell}$
Set $M_0 \leftarrow P_y$ and $M_i \leftarrow P_{h(\mathbf{e}_i)}$ // all in $\mathbb{F}_2^{n_2,n_2}$
// Compute the verification and secret key
Set $[\mathbf{u}_i] = [\mathbf{v}_i]$ and $[A_{2,i}] = [V_i - M_i]$
Sample $\mathbf{a}_1 \leftarrow^{\$} \mathbb{F}_q^{n_1}$, $\mathbf{t} \leftarrow^{\$} \mathbb{F}_2^{n_1}$, $k \leftarrow^{\$} \mathsf{SUF.Gen}(1^\lambda)$, $B \leftarrow^{\$} \mathbb{F}_2^{n_1,n_2}$: $\mathsf{rk}(B) = n_1$
$[A_{j,i}] \leftarrow [\mathbf{u}_i \otimes \mathbf{a}_j]$ for $j \in \{1,2\}$ and $i \in \{0, \ldots, \mu\}$
$\mathsf{vk} = (([A_{1,i}], [A_{2,i}], [\mathbf{u}_i])_{i=0}^{\mu}, \mathbf{t}, k, B, \mathbb{G})$, $\mathsf{sk} = (\mathsf{vk}, \mathbf{a}_1)$
Run $\mathcal{D}(\mathsf{vk})$ // Interact with the distinguisher
When $\mathcal{D}$ queries $m \in \{0,1\}^\mu$: Reply $\sigma \leftarrow^{\$} \mathsf{S.Sign}(\mathsf{sk}, m)$ if $h(m) \neq y$
When $\mathcal{D}$ returns b: **Return** b

Fig. 13: Reduction of the ind. of $\mathsf{H}_5, \mathsf{H}_6$ to $(n_2(\mu+1), n_2+1)$-MDDH.

It readily follows $\mathcal{R}_4$ simulates H_6 when C is uniform, while it simulates H_7 when $C = \mathbf{v} \otimes \mathbf{w}$ for freshly sampled $\mathbf{v}, \mathbf{w}$. Thus by Lemma 9 and Corollary 2

$$\mathsf{negl}(\lambda) \;=\; \mathsf{Adv}_{\mathcal{R}_4}(\lambda) \;=\; \mathsf{Adv}_{\mathcal{D}}^{\mathsf{H}_6,\mathsf{H}_7}(\lambda).$$

Indistinguishability of $\mathsf{H}_7, \mathsf{H}_8$. The two hybrids differ only on the definition of sk. However vk and all signature replies follow the same distribution in the two games, meaning $\mathsf{H}_7, \mathsf{H}_8$ are perfectly indistinguishable.

Indistinguishability of $\mathsf{H}_8, \mathsf{H}_9$. Let $\mathcal{D}$ be a distinguisher for the two hybrids. Its final output bit in the two executions is a deterministic function of its random tape ρ and its view, that is

$$\begin{aligned}
\mathsf{H}_8 \;&:\; \left(\rho, ([A_{1,i}], [A_{2,i}], [\mathbf{u}_i])_{i=0}^{\mu}, \mathbf{t}, B, \mathbb{G}, \sigma_1, \ldots, \sigma_\vartheta\right), \\
\mathsf{H}_9 \;&:\; \left(\widehat{\rho}, ([\widehat{A}_{1,i}], [\widehat{A}_{2,i}], [\widehat{\mathbf{u}}_i])_{i=0}^{\mu}, \widehat{\mathbf{t}}, \widehat{k}, \widehat{B}, \widehat{\mathbb{G}}, \widehat{\sigma}_1, \ldots, \widehat{\sigma}_\vartheta\right).
\end{aligned}$$

Hence the two games are indistinguishable if the two vectors have negligible statistical distance. To prove this we consider the following two vectors:

$$\begin{aligned}
\mathsf{view} \;&\coloneqq\; (\rho, \mathbb{G}, \mathbf{u}, \mathbf{a}_1, \mathbf{a}_2, (\alpha_i)_{i=0}^{\mu}, \mathbf{t}, h, y, k, B, \sigma_1, \ldots, \sigma_\vartheta) \\
\widehat{\mathsf{view}} \;&\coloneqq\; \left(\widehat{\rho}, \widehat{\mathbb{G}}, \widehat{\mathbf{u}}, \widehat{\mathbf{a}}_1, \widehat{\mathbf{a}}_2, (\widehat{\alpha}_i)_{i=0}^{\mu}, \widehat{\mathbf{t}}, \widehat{h}, \widehat{y}, \widehat{k}, \widehat{B}, \widehat{\sigma}_1, \ldots, \widehat{\sigma}_\vartheta\right).
\end{aligned}$$

Note the actual views of $\mathcal{D}$ are a deterministic function of respectively $\mathsf{view}, \widehat{\mathsf{view}}$, since $\mathbf{u}_i = \alpha_i \cdot \mathbf{u}$, $A_{1,i} = \mathbf{u}_i \otimes \mathbf{a}_1$ and, calling $M_0 = P_y$, $M_i = P_{h(\mathbf{e}_i)}$, then $A_{2,i} = \mathbf{u}_i \otimes \mathbf{a}_2 - M_i$. It then suffices to show that $\Delta(\mathsf{view}, \widehat{\mathsf{view}}) \leq \mathsf{negl}(\lambda)$. We do so studying the distribution of their entries one by one.

$\mathsf{H}_8 \approx_s \mathsf{H}_9$*: Trivial components.* Define for each view the respective *partial view* $\mathsf{pv}^* = (\rho, \mathbb{G}, \mathbf{u}, \mathbf{a}_1, \mathbf{a}_2, (\alpha_i)_{i=0}^{\mu}, \mathbf{t}, h, y)$ and $\widehat{\mathsf{pv}}^* = (\widehat{\rho}, \widehat{\mathbb{G}}, \widehat{\mathbf{u}}, \widehat{\mathbf{a}}_1, \widehat{\mathbf{a}}_2, (\widehat{\alpha}_i)_{i=0}^{\mu}, \widehat{\mathbf{t}}, \widehat{h}, \widehat{y})$. By construction, pv^* and $\widehat{\mathsf{pv}}^*$ follows the same distribution. In light of Lemma 4 we then proceed conditioning on $\mathsf{pv}^* = \mathsf{pv}_0^* = \widehat{\mathsf{pv}}^*$ with $u_i \neq u_j \neq 0$ for all $i < j$. Note that since $\mathbf{u}$ is uniformly distributed in $\mathbb{F}_q^{n_2}$

$$\Pr\left[\exists i : u_i = 0 \ \vee \ \exists i \neq j : u_i = u_j\right] \ \leq \ \frac{n_2(n_2+1)}{2q}.$$

$\mathsf{H}_8 \approx_s \mathsf{H}_9$*: SUF key.* Again $k, \widehat{k}$ are respectively independent from pv^*, $\widehat{\mathsf{pv}}^*$ and by construction they follow the same distribution. Next, as we already fixed $\mathbb{G}, \mathbf{u}, \mathbf{a}_2$, let $\widehat{\mathcal{K}}_1^*$ be the set whose existence is implied by Theorem 6. Similarly, having fixed $\mathbb{G}, \mathbf{u}, \mathbf{a}_2$, let $\mathcal{K}_2^*$ be the set whose existence is guaranteed by Theorem 7. We then proceed conditioning on $k = k_0 = \widehat{k}$ with $k_0 \in \widehat{\mathcal{K}}_1^* \cap \mathcal{K}_2^*$. Note that by Theorem 6 and 7

$$\Pr\left[k \notin \widehat{\mathcal{K}}_1^* \cap \mathcal{K}_2^*\right] \ \leq \ \Pr\left[k \notin \widehat{\mathcal{K}}_1^*\right] + \Pr\left[k \notin \mathcal{K}_2^*\right] \ \leq \ \varepsilon_1(\lambda) + \varepsilon_2(\lambda).$$

$\mathsf{H}_8 \approx_s \mathsf{H}_9$*: UHF key.* In both distributions, $B, \widehat{B}$ are independent from pv^*, k and $\widehat{\mathsf{pv}}^*, \widehat{k}$, so their conditional statistical distance is 0. To proceed, we condition $B, \widehat{B}$ to lie on the intersection of a family of "good" sets of UHFs. First, let $\mathcal{M} = \{m \in \mathbb{F}_2^{\mu} \ : \ h(m) \neq y\}$ be the set of message that can be signed by both hybrids. For each $m \in \mathcal{M}$ below we define the domain $\mathcal{U}_m^*$ (as done in Section 3.3) and specify these sets of good UHFs.

$$\mathcal{U}_m^* \ = \ \{(\mathbf{x}, z^*) \,|\, \delta_{\mathsf{min}}\left([A_2^{(m)}\mathbf{x} + z^*\mathbf{u}^{(m)}]\right) \geq d\}$$

$$\mathcal{B}_m \ = \ \left\{ B \in \mathbb{F}_2^{n_1, n_2} \;\middle|\; \begin{array}{l} (\mathbf{x}, z) \leftarrow^{\$} \mathcal{U}_m^*, \ \mathbf{s} \leftarrow^{\$} \mathbb{F}_2^{n_1} \\ \Delta((\alpha^{(m)}(\mathbf{a}_2^{\top}\mathbf{x} + z), BM^{(m)}\mathbf{x}), (\alpha^{(m)}(\mathbf{a}_2^{\top}\mathbf{x} + z), \mathbf{s})) \leq 2^{-\lambda} \end{array} \right\}$$

where $\alpha^{(m)} = \alpha_0 + \sum_{i=1}^{\mu} m_i \alpha_i$, $A_2^{(m)} = A_{2,0} + \sum_{i=1}^{\mu} m_i A_{2,i}$ and $M^{(m)} = M_0 + \sum_{i=1}^{\mu} m_i M_i \in \mathbb{F}_2^{n_2, n_2}$. In the appendix, Section D.4 we prove through the LHL the following claim.

Claim 14. *$\forall m \in \mathcal{M} : \mathbf{u}^{(m)} \neq \mathbf{0}$ then* $\Pr\left[B \notin \mathcal{B}_m | \mathsf{pv}^* = \mathsf{pv}_0^*, k = k_0\right] \leq 2^{-(\lambda+\mu)}$.

We proceed conditioning on $B = B_0 = \widehat{B}$ with $B_0 \in \bigcap_{m \in \mathcal{M}} \mathcal{B}_m$. In view of Lemma 4 this introduces a statistical error term smaller than

$$\begin{aligned} \Pr\left[B \notin \bigcap\nolimits_{m \in \mathcal{M}} \mathcal{B}_m \;\middle|\; \begin{array}{l} \mathsf{pv}^* = \mathsf{pv}_0^* \\ k = k_0 \end{array}\right] \ &\leq \ \sum\nolimits_{m \in \mathcal{M}} \Pr\left[B \notin \mathcal{B}_m \;\middle|\; \begin{array}{l} \mathsf{pv}^* = \mathsf{pv}_0^* \\ k = k_0 \end{array}\right] \\ &\leq 2^{\mu} \cdot 2^{-\lambda} \cdot 2^{-\mu} \ = \ 2^{-\lambda}. \end{aligned}$$

$\mathsf{H}_8 \approx_s \mathsf{H}_9$*: Signatures.* Let $\mathsf{pv}_i = (\mathsf{pv}^*, k, B, \sigma_1, \ldots, \sigma_{i-1})$ and analogously $\widehat{\mathsf{pv}}_i = (\widehat{\mathsf{pv}}^*, \widehat{k}, \widehat{B}, \widehat{\sigma}_1, \ldots, \widehat{\sigma}_{i-1})$. In the Appendix, Section D.4, we prove that for any $\mathsf{pv}_{i,0}$ satisfying the previous constraints on $\mathbf{u}, k, B$ the following claim holds:

Claim 15. $\Delta(\sigma_{i|\mathsf{pv}_i=\mathsf{pv}_{i,0}}, \widehat{\sigma}_{i|\widehat{\mathsf{pv}}_i=\mathsf{pv}_{i,0}}) \leq \varepsilon_1(\lambda) + 2^{-\lambda} + \varepsilon_2(\lambda)$.

By induction and Lemma 4 we get $\Delta(\mathsf{pv}_{\vartheta+1}, \widehat{\mathsf{pv}}_{\vartheta+1}) \leq$

$$\leq \vartheta(\varepsilon_1(\lambda) + 2^{-\lambda} + \varepsilon_2(\lambda)) + \frac{n_2(n_2+1)}{2q} + 2^{-\lambda} + \varepsilon_1(\lambda) + \varepsilon_2(\lambda)$$

which is negligible. Since $\mathsf{view} = \mathsf{pv}_{\vartheta+1}$ and $\widehat{\mathsf{view}} = \widehat{\mathsf{pv}}_{\vartheta+1}$ we conclude that

$$\mathsf{Adv}^{\mathsf{H}_8,\mathsf{H}_9}_{\mathcal{D}}(\lambda) \leq \Delta(\mathsf{view}, \widehat{\mathsf{view}}) \leq \mathsf{negl}(\lambda).$$

Indistinguishability of $\mathsf{H}_9, \mathsf{H}_{10}$. Given a distinguisher $\mathcal{D}$, we describe a reduction $\mathcal{R}_5$ to $(n_2, \mu+1)$-MDDH. The reduction is analogous to that for $\mathsf{H}_3, \mathsf{H}_4$: given $(\mathbb{G}, [C])$ it computes vk by setting $[\mathbf{u}_i]$ as the i-th column of $[C]$. It then computes vk as in H_9 by sampling $\mathbf{t}, k, h, y, B$ and setting $[A_{1,i}] = [\mathbf{u}_i \otimes \mathbf{a}_1]$ and $[A_{2,i}] = [\mathbf{u}_i \otimes \mathbf{a}_2 - M_i]$ where as usual $M_0 = P_y$ and $M_i = P_{h(\mathbf{e}_i)}$ for $i \geq 1$.

When $C = C_0$ uniformly sampled, then $\mathcal{R}_5$ perfectly simulates H_{10}, since all $\mathbf{u}_i$ are uniformly distributed in this case. Conversely, when $C = C_1 = \mathbf{v} \otimes \mathbf{w}$ for a uniformly sampled $\mathbf{v} \in \mathbb{F}_q^{n_2}$ and $\mathbf{w} \in \mathbb{F}_q^{\mu+1}$, then $\mathbf{u}_i = w_i \cdot \mathbf{v}$ and in particular $\mathcal{R}_5$ perfectly simulates H_9. Since MDDH is assumed to be hard, by Lemma 9 and Corollary 2

$$\mathsf{negl}(\lambda) = \mathsf{Adv}_{\mathcal{R}_5}(\lambda) = \mathsf{Adv}^{\mathsf{H}_9,\mathsf{H}_{10}}_{\mathcal{D}}(\lambda).$$

Indistinguishability of $\mathsf{H}_{10}, \mathsf{H}_{11}$. Given a distinguisher $\mathcal{D}$, we define a reduction $\mathcal{R}_6$ to $((\mu+1)n_2, n_1+1)$-MDDH. The reduction is analogous to that for $\mathsf{H}_4, \mathsf{H}_5$: Given $(\mathbb{G}, [C])$, $\mathcal{R}_6$ parses the matrix as $[\mathbf{v}], [V] \in \mathbb{G}^{(\mu+1)n_2} \times \mathbb{G}^{(\mu+1)n_2, n_1}$ and then further splits vertical both the matrix and the vector into blocks of height n_1, i.e. $[\mathbf{v}_0], \ldots, [\mathbf{v}_\mu]$ and $[V_0], \ldots, [V_\mu]$ with $\mathbf{v}_i \in \mathbb{F}_q^{n_2}$ and $V_i \in \mathbb{F}_q^{n_2, n_1}$. Next, it computes vk sampling $\mathbf{a}_2, \mathbf{t}, k, h, y, B$ as per $\mathsf{S.Gen}$ and setting $[\mathbf{u}_i] = [\mathbf{v}_i]$, $[A_{1,i}] = [V_i]$.

When $C = C_0$ is uniformly sampled, then so are $\mathbf{u}_i$ and $A_{1,i}$ as in H_{10}. Conversely when $C = C_1 = \mathbf{v} \otimes (1, \mathbf{w})$ for uniformly sampled $\mathbf{v} \in \mathbb{F}_q^{(\mu+1)n_2}$ and $\mathbf{w} \in \mathbb{F}_q^{n_2}$, then $\mathbf{u}_i$ are again uniformly sampled as prescribed and $A_{1,i} = \mathbf{u}_i \otimes \mathbf{w}$ as in H_{11}. Thus, by Lemma 9 and 10

$$\mathsf{negl}(\lambda) = \mathsf{Adv}_{\mathcal{R}_6}(\lambda) = \mathsf{Adv}^{\mathsf{H}_{10},\mathsf{H}_{11}}_{\mathcal{D}}(\lambda).$$

Indistinguishability of $\mathsf{H}_{11}, \mathsf{H}_{12}$. Given a distinguisher $\mathcal{D}$, we define a reduction $\mathcal{R}_7$ to $((\mu+1)n_2, n_1+1)$-MDDH. The reduction is identical to $\mathcal{R}_6$ up to the fact that, with the same notation, $[A_{1,0}] = [V_0 - B^+]$ and $[A_{1,i}] = [V_i]$. Again by Lemma 9 and 10 it follows that

$$\mathsf{negl}(\lambda) = \mathsf{Adv}_{\mathcal{R}_7}(\lambda) = \mathsf{Adv}^{\mathsf{H}_{11},\mathsf{H}_{12}}_{\mathcal{D}}(\lambda).$$

Indistinguishability of $\mathsf{H}_{12}, \mathsf{H}_{13}$. Given a distinguisher $\mathcal{D}$, we define a reduction $\mathcal{R}_8$ to $(n_2, \mu+1)$-MDDH. The reduction is identical to $\mathcal{R}_5$ up to setting $[A_{1,0}] = [\mathbf{u}_0 \otimes \mathbf{a}_1 - I]$. By Lemma 9 and Corollary 2, we have

$$\mathsf{negl}(\lambda) \;=\; \mathsf{Adv}_{\mathcal{R}_8}(\lambda) \;\geq\; \mathsf{Adv}_{\mathcal{D}}^{\mathsf{H}_{12},\mathsf{H}_{13}}(\lambda).$$

Hardness of H_{13}. Given vk define $\mathcal{T} = \{B\delta_2([\rho\mathbf{u}]) : \rho \in \mathbb{F}_q\}$. By construction $\mathcal{T} \subseteq \mathbb{F}_2^{n_1}$ has size $|\mathcal{T}| \leq q$. Since $\mathbf{t}$ is uniform over $\mathbb{F}_2^{n_1}$, then

$$\Pr\left[\mathbf{t} \in \mathcal{T}\right] \;\leq\; \frac{q}{2^{n_1}} \;=\; \frac{1}{2^{\lambda}}$$

because $n_1 = \lambda + \log q$. Next we show that $\mathcal{A}$ could win only when $\mathbf{t} \in \mathcal{T}$. If $\mathcal{A}$ returns (m, σ) such that H_{13} returns 1 then m is a valid forgery, that is $\mathsf{S.Vfy}(\mathsf{vk}, m, \sigma) = 1$ and $h(m) = y$. To fix notation, let $\sigma = (\mathbf{x}_1, \mathbf{x}_2, z)$, $M_0 = P_y$, $M_i = P_{h(\mathbf{e}_i)}$ and $M^{(m)} = M_0 + m_1 M_1 + \ldots + m_\mu M_\mu \in \mathbb{Z}^{n_2, n_2}$. We further denote for clarity $\bar{M}^{(m)} = (M^{(m)} \mod 2) \in \mathbb{F}_2^{n_1, n_2}$. Then the signature satisfies:

$$\begin{aligned}
\mathbf{t} \;&= B\delta_2\left(\left[A_1^{(m)}\mathbf{x}_1 + A_2^{(m)}\mathbf{x}_2 + z\mathbf{u}^{(m)} + B^+\mathbf{x}_1\right]\right) \\
&= B\delta_2\left(\left[(\mathbf{u}^{(m)} \otimes \mathbf{a}_1 - B^+)\mathbf{x}_1 + (\mathbf{u}^{(m)} \otimes \mathbf{a}_2 - M^{(m)})\mathbf{x}_2 + z\mathbf{u}^{(m)} + B^+\mathbf{x}_1\right]\right) \\
&= B\delta_2\left(\left[(\mathbf{a}_1^\top\mathbf{x}_1 + \mathbf{a}_2^\top\mathbf{x}_2 + z)\cdot\mathbf{u}^{(m)} - M^{(m)}\mathbf{x}_2\right]\right) \\
&= B\delta_2\left(\left[(\mathbf{a}_1^\top\mathbf{x}_1 + \mathbf{a}_2^\top\mathbf{x}_2 + z)\cdot\mathbf{u}^{(m)}\right]\right) \oplus \bar{M}^{(m)}\mathbf{x}_2.
\end{aligned}$$

The last step follows by Corollary 1, which we can apply since $\left\|M^{(m)}\mathbf{x}_2\right\|_\infty \leq (\mu+1)n_2 \leq d - n_1$, and because σ being valid implies the following bound:

$$\begin{aligned}
&\delta_{\mathsf{min}}\left(\left[A_1^{(m)}\mathbf{x}_1 + A_2^{(m)}\mathbf{x}_2 + z\mathbf{u}^{(m)}\right]\right) \geq d \;\Rightarrow \\
\Rightarrow\; &\delta_{\mathsf{min}}\left(\left[A_1^{(m)}\mathbf{x}_1 + A_2^{(m)}\mathbf{x}_2 + z\mathbf{u}^{(m)} + B^+\mathbf{x}_1\right]\right) \geq d - n_1 \;\Rightarrow \\
\Rightarrow\; &\delta_{\mathsf{min}}\left(\left[(\mathbf{a}_1^\top\mathbf{x}_1 + \mathbf{a}_2^\top\mathbf{x}_2 + z)\cdot\mathbf{u}^{(m)} - M^{(m)}\mathbf{x}_2\right]\right) \;\geq\; d - n_1
\end{aligned}$$

where the first implication follows as $\|B^+\mathbf{x}_1\| \leq n_1$. Next, as $h(m) = y$ in $\mathbb{F}_2^\ell$, we have that $\bar{M}^{(m)}$ is zero in $\mathbb{F}_2^{n_2, n_1}$, indeed $\bar{M}^{(m)} =$

$$= P_y \oplus \left(\bigoplus\nolimits_{i=1}^{\mu} m_i P_{h(\mathbf{e}_i)}\right) = P_{y \oplus m_1 h(\mathbf{e}_1) \oplus \ldots \oplus m_\mu h(\mathbf{e}_\mu)} = P_{y \oplus h(m)} = P_{\mathbf{0}} = \Omega.$$

where we used the fact that $P_{(\cdot)} : \mathbb{F}_2^\ell \to \mathbb{F}_2^{n_2, n_2}$ is $\mathbb{F}_2$-linear (Theorem 2), and so is $P_{h(\cdot)} : \mathbb{F}_2^\mu \to \mathbb{F}_2^{n_2, n_2}$. In particular

$$\mathbf{t} = B\cdot\delta_2\left(\left[(\mathbf{a}_1^\top\mathbf{x}_1 + \mathbf{a}_2^\top\mathbf{x}_2 + z)\cdot\mathbf{u}^{(m)}\right]\right) = B\cdot\delta_2\left(\left[\alpha^{(m)}\cdot(\mathbf{a}_1^\top\mathbf{x}_1 + \mathbf{a}_2^\top\mathbf{x}_2 + z)\cdot\mathbf{u}\right]\right)$$

which lies in $\mathcal{T}$, with $\alpha^{(m)} = \alpha_0 + \sum_{i=1}^{\mu} m_i\alpha_i$. We thus conclude that

$$\Pr\left[\mathsf{H}_{13}^{\mathcal{A}}(\lambda) \to 1\right] \;\leq\; \Pr\left[\mathbf{t} \in \mathcal{T}\right] \;\leq\; 2^{-\lambda}. \qquad \square$$

D.4 Adaptively Secure Scheme: Claims

Proof of Claim 14. At a high level, we first prove that sampling $(\mathbf{x}, z^*) \leftarrow^{\$} \mathcal{U}_m^*$ when $\mathbf{u}^{(m)}$ is non-zero, implies $\mathbf{x}$ has high min-entropy. Then, we derive the claim combining the leftover hash lemma with an averaging argument.

Regarding the first step, let $(\bar{\mathbf{x}}, \bar{z}^*) \leftarrow^{\$} \mathsf{Samp}([A_2^{(m)}], [\mathbf{u}^{(m)}], d, \mathsf{dp})$. By construction, this procedure is equivalent to sampling $(\bar{\mathbf{x}}_1, \bar{z}_1^*), \ldots (\bar{\mathbf{x}}_\nu, \bar{z}_\nu^*)$ from $\mathbb{F}_2^{n_2} \times \mathbb{F}_q$ and return $(\bar{\mathbf{x}}_I, \bar{z}_I^*)$ with $I \in \{1, \ldots, \nu, \perp\}$ denoting either the index of the first tuple in $\mathcal{U}_m^*$, or $\perp$.

Calling $\alpha^{(m)} = \alpha_0 + \sum_{i=0}^{\mu} m_i \alpha_i$ and $M^{(m)} = M_0 + \sum_{i=1}^{\mu} m_i M_i$, then $A_2^{(m)} = \mathbf{u}^{(m)} \otimes \mathbf{a}_2 - M^{(m)}$ where $\left\| M^{(m)} \right\|_\infty \leq (\mu + 1) n_2 \leq d$ and $\mathbf{u}^{(m)} = \alpha^{(m)} \cdot \mathbf{u} \neq \mathbf{0}$. Moreover by construction $k = k_0 \in \widehat{\mathcal{K}}_1^*$, therefore by Theorem 6 we derive $\Pr[(\bar{\mathbf{x}}, \bar{z}^*) = \perp] \leq \varepsilon_1$. Calling bad the event $(\bar{\mathbf{x}}, \bar{z}^*) = \perp$ then we have that $(\bar{\mathbf{x}}, \bar{z}^*)_{|\neg \mathsf{bad}}$ is uniform over $\mathcal{U}_m^*$. Hence, projecting on the first component, we have that $\mathbf{x}$ and $\bar{\mathbf{x}}_{|\neg \mathsf{bad}}$ are identically distributed. By Lemma 8 and Theorem 13

$$\begin{aligned} \mathrm{H}_\infty\Big(\mathbf{x} \,\Big|\, \alpha^{(m)}(\mathbf{a}_2^\top \mathbf{x} - z)\Big) \;&\geq\; \mathrm{H}_\infty(\mathbf{x}) - \log q \;=\; \mathrm{H}_\infty\big(\bar{\mathbf{x}}_{|\neg \mathsf{bad}}\big) - \log q \\ &\geq n_2 - \log \nu + \log(\Pr[\neg \mathsf{bad}]) - \log q \\ &\geq n_2 - \log 2\lambda - 1 - \log q \\ &= n_1 + 4\lambda + 2\mu \end{aligned}$$

where the third inequality follows as $\Pr[\neg \mathsf{bad}] \geq 1 - \varepsilon_1(\lambda) \geq 1/2$. As we assumed $m \in \mathcal{M}$, that is $h(m) \neq y$, then modulo 2 we have that $M^{(m)} = P_{y \oplus h(m)} \in \mathbb{F}_2^{n_2, n_2}$ is invertible by Theorem 2 because $h(m) \oplus y \neq \mathbf{0}$. Moreover, $M^{(m)}$ is uniquely determined by h, y, and in particular by pv^*. Hence

$$\mathrm{H}_\infty\Big(M^{(m)}\mathbf{x} \,\Big|\, \alpha^{(m)}(\mathbf{a}_2^\top \mathbf{x} - z)\Big) \;\geq\; n_1 + 4\lambda + 2\mu.$$

Next, since B is uniform over $\mathbb{F}_2^{n_1, n_2}$ of rank n_1 and independent[23] from $(\mathbf{x}, z^*)$, Theorem 1 implies that[24], for a uniformly sampled $\mathbf{s} \in \mathbb{F}_2^{n_1}$

$$\begin{aligned} 2^{-2\lambda - \mu} \;&\geq\; \Delta((B, \alpha^{(m)}(\mathbf{a}_2^\top \mathbf{x} - z^*), BM^{(m)}\mathbf{x}),\, (B, \alpha^{(m)}(\mathbf{a}_2^\top \mathbf{x} - z^*), \mathbf{s})) \\ &\geq\; \mathbb{E}_B\left[\Delta((\alpha^{(m)}(\mathbf{a}_2^\top \mathbf{x} - z^*), BM^{(m)}\mathbf{x}),\, (\alpha^{(m)}(\mathbf{a}_2^\top \mathbf{x} - z^*), \mathbf{s}))\right] \end{aligned}$$

Markov inequality thus implies that the statistical distance is larger than $2^{-\lambda}$ only with probability $2^{-\lambda - \mu}$, that is, $\Pr[B \notin \mathcal{B}_{2,m}] \leq 2^{-\lambda - \mu}$. □

Proof of Claim 15. For simplicity let us denote $m, \widehat{m}$ the i-th message $\mathcal{D}$ sent in the two executions, and $\sigma, \widehat{\sigma}$ the reply. Note m is a deterministic function of pv_i and $\widehat{m}$ is the same function of $\widehat{\mathsf{pv}}_i$. Hence conditioning on $\mathsf{pv}_i = \mathsf{pv}_{i,0} = \widehat{\mathsf{pv}}_i$

[23] Note $\mathbf{x}, z$ is a function of the random coins in Samp, of $\mathbf{a}_2, \mathbf{u}_i, M_i, k, \mathbb{G}$ which are uniquely determined upon conditioning on $\mathsf{pv}^* = \mathsf{pv}_0^*$ and $k = k_0$, and of m which is a fixed string in $\mathcal{M}$.

[24] Recall the matrices of rank n_1 in $\mathbb{F}_2^{n_1, n_2}$ are a UHF family by Proposition 1.

we have $m = \widehat{m}$. Furthermore, as all events considered in this claim will be conditioned to $\mathsf{pv}_i = \mathsf{pv}_{i,0} = \widehat{\mathsf{pv}}_i$ we omit such condition and instead assume all probability hereafter to be taken in the relative measure space.

We notice that if $\mathsf{pv}_{i,0}$ is such that $h(m) = y$, then in both games the hybrid returns $\perp$ and in particular $\Delta(\sigma, \widehat{\sigma}) = 0$. Similarly, if $\mathbf{u}^{(m)} = \mathbf{0}$ then in both games the hybrid returns $\sigma = \mathbf{0}$ by construction. Hence it only remains to consider those $\mathsf{pv}_{i,0}$ such that $h(m) \neq y$ and $\mathbf{u}^{(m)} \neq \mathbf{0}$.

Denote $\sigma = (\mathbf{x}_1, \mathbf{x}_2, z)$ and $\widehat{\sigma} = (\widehat{\mathbf{x}}_1, \widehat{\mathbf{x}}_2, \widehat{z})$. Setting $z^* = z + \mathbf{a}_1^\top \mathbf{x}_1$ and $\widehat{z}^* = \widehat{z} + \mathbf{a}_1^\top \widehat{\mathbf{x}}_1$, our goal is to upper bound $\Delta(\sigma, \widehat{\sigma}) = \Delta((\mathbf{x}_1, \mathbf{x}_2, z^*), (\widehat{\mathbf{x}}_1, \widehat{\mathbf{x}}_2, \widehat{z}^*))$ via the key-switching lemma (Lemma 1). Consider the following two functions:

$$\begin{aligned} f_1 &: \mathbb{F}_2^{n_1} \to \mathbb{F}_2^{n_1} & f_1(\mathbf{x}_1) &= \mathbf{x}_1 \oplus \mathbf{t} \\ f_2 &: \mathcal{U}_m^* \to \mathbb{F}_2^{n_1} & f_2(\mathbf{x}_2, z^*) &= B \cdot \delta_2([A_2^{(m)} \mathbf{x}_2 + z^* \mathbf{u}^{(m)}]) \end{aligned}$$

f_2 is well defined as any $(\mathbf{x}_2, z^*) \in \mathcal{U}_m^*$ has finite distance by definition of $\mathcal{U}_m^*$.

Claim 16. *f_1 and f_2 are respectively 0 (i.e. perfectly) and $2^{-\lambda}$-balanced.*

Next, we introduce the following distributions, as in Lemma 1.

- $(\mathbf{v}_2, w^*) \leftarrow^{\$} \mathcal{U}_m^*$ and $\mathbf{v}_1 \leftarrow^{\$} f_1^{-1}(f_2(\mathbf{v}_2, w^*))$
- $\widehat{\mathbf{v}}_1 \leftarrow^{\$} \mathbb{F}_2^{n_1}$ and $(\widehat{\mathbf{v}}_2, \widehat{z}^*) \leftarrow^{\$} f_2^{-1}(f_1(\widehat{\mathbf{v}}_1))$

The following claims are respectively consequences of Theorem 6 and 7.

Claim 17. $\Delta((\mathbf{x}_1, \mathbf{x}_2, z^*), (\mathbf{v}_1, \mathbf{v}_2, w^*)) \leq \varepsilon_1(\lambda)$.

Claim 18. $\Delta((\widehat{\mathbf{x}}_1, \widehat{\mathbf{x}}_2, \widehat{z}^*), (\widehat{\mathbf{v}}_1, \widehat{\mathbf{v}}_2, \widehat{w}^*)) \leq \varepsilon_2(\lambda)$.

Assuming the claims hold, we then conclude as $\Delta(\sigma, \widehat{\sigma}) =$

$$\begin{aligned} = \Delta((\mathbf{x}_1, \mathbf{x}_2, z^*), (\widehat{\mathbf{x}}_1, \widehat{\mathbf{x}}_2, \widehat{z}^*)) &\leq \Delta((\mathbf{x}_1, \mathbf{x}_2, z^*), (\mathbf{v}_1, \mathbf{v}_2, w^*)) \\ &\quad + \Delta((\mathbf{v}_1, \mathbf{v}_2, w^*), (\widehat{\mathbf{v}}_1, \widehat{\mathbf{v}}_2, \widehat{w}^*)) \\ &\quad + \Delta((\widehat{\mathbf{v}}_1, \widehat{\mathbf{v}}_2, \widehat{w}^*), (\widehat{\mathbf{x}}_1, \widehat{\mathbf{x}}_2, \widehat{z}^*)) \\ &\leq \varepsilon_1(\lambda) + 2^{-\lambda} + \varepsilon_2(\lambda) \end{aligned}$$

where the first inequality is the triangular inequality, while the second one hold applying the claims to the first and third term, and Lemma 1 to the second one, as f_1 is 0-balanced and f_2 is $2^{-\lambda}$ balanced. □

Proof of Claim 16. f_1 is a bijection, because it is an involution, and in particular 0-balanced. Regarding f_2, let $(\mathbf{x}, z^*) \leftarrow^{\$} \mathcal{U}_m^*$. We need to show $f_2(\mathbf{x}, z^*)$ is $2^{-\lambda}$-close to the uniform distribution over $\mathbb{F}_2^{n_1}$.

For the sake of clarity, we denote $M^{(m)} = (M^{(m)} \mod 2) \in \mathbb{F}_2^{n_2, n_2}$. Since $h(m) \neq y$ then $B \in \mathcal{B}_m$ due to our conditions (see the proof of Claim 15), we

have that for a uniformly sampled vector $\mathbf{s}$ in $\mathbb{F}_2^{n_1}$

$$\begin{aligned} 2^{-\lambda} \;&\geq\; \Delta((\alpha^{(m)} \cdot (\mathbf{a}_2^\top \mathbf{x} + z^*), B\bar{M}^{(m)}\mathbf{x}), (\alpha^{(m)} \cdot (\mathbf{a}_2^\top \mathbf{x} + z^*), \mathbf{s})) \\ &\geq\; \Delta\Big(B \cdot \delta_2([(\mathbf{u}^{(m)} \otimes \mathbf{a}_2)\mathbf{x} + z^*\mathbf{u}^{(m)}]) \oplus (B\bar{M}^{(m)}\mathbf{x}), \\ &\qquad B \cdot \delta_2([(\mathbf{u}^{(m)} \otimes \mathbf{a}_2)\mathbf{x} + z^*\mathbf{u}^{(m)}]) \oplus \mathbf{s}\Big)\,. \end{aligned}$$

where the second inequality follows applying to each distribution the function[25] mapping $c_1, \mathbf{c}_2 \mapsto B\delta_2([c_1 \cdot \mathbf{u}^{(m)}]) \oplus \mathbf{c}_2$. The second term is clearly uniform as $\mathbf{s}$ is independent from $\mathbf{x}, z^*$. To conclude we show the first term to be $f_2(\mathbf{x}, z^*)$. Indeed

$$\begin{aligned} &B \cdot \delta_2([(\mathbf{u}^{(m)} \otimes \mathbf{a}_2)\mathbf{x} + z^*\mathbf{u}^{(m)}]) \oplus (B\bar{M}^{(m)}\mathbf{x}) \\ &= B \cdot \Big(\delta_2([A_2^{(m)}\mathbf{x} + z^*\mathbf{u}^{(m)} + M^{(m)}\mathbf{x}]) \oplus (\bar{M}^{(m)}\mathbf{x})\Big) \\ &= B \cdot \delta_2([A_2^{(m)}\mathbf{x} + z^*\mathbf{u}^{(m)}]) \;=\; f_2(\mathbf{x}, z^*). \end{aligned}$$

The first equality follows since $A_2^{(m)} = (\mathbf{u}^{(m)} \otimes \mathbf{a}_2) - M^{(m)}$. The second follows by Lemma 3 as $\left\|M^{(m)}\mathbf{x}\right\|_\infty \leq (\mu+1)n_2 \leq d$ and the distance of $[A_2^{(m)}\mathbf{x} + z^*\mathbf{u}^{(m)}]$ is at least d because $(\mathbf{x}, z^*) \in \mathcal{U}_m^*$. □

Proof of Claim 17. Recall $(\mathbf{x}_2, z^*)$ is the output of $\mathsf{Samp}([A_2^{(m)}], [\mathbf{u}^{(m)}], d, \mathsf{dp})$. Let bad be the event $(\mathbf{x}_2, z^*) = \perp$. Then $k = k_0 \in \widehat{\mathcal{K}}_1^*$ implies by Theorem 6 that $\Pr[\mathsf{bad}] \leq \varepsilon_1(\lambda)$. Note the theorem can be applied as we assumed $\mathbf{u}^{(m)} \neq \mathbf{0}$ (see the proof of Claim 15) and the entries of $\mathbf{u}$ to be all distinct and non-zero, implying the same holds for the entries of $\mathbf{u}^{(m)}$.

Theorem 4 instead implies that $(\mathbf{x}_2, z^*)_{|\neg\mathsf{bad}}$ is uniformly distributed in $\mathcal{U}_m^*$. Since $(\mathbf{v}_2, w^*)$ is uniform in $\mathcal{U}_m^*$, we conclude that[26] $\Delta((\mathbf{x}_2, z^*), (\mathbf{v}_2, w^*)) \leq \Pr[\mathsf{bad}] \leq \varepsilon_1(\lambda)$. Finally, conditioning on $(\mathbf{x}_2, z^*) = (\bar{\mathbf{x}}_2, \bar{z}^*) = (\mathbf{v}_2, w^*)$ with $(\bar{\mathbf{x}}_2, \bar{z}^*) \in \mathcal{U}_m^*$, then by construction

$$\mathbf{x}_1 \;=\; (B\delta_2([A_2^{(m)}\bar{\mathbf{x}}_2 + \bar{z}^*\mathbf{u}^{(m)}])) \oplus \mathbf{t} \;=\; f_1^{-1}(f_2(\bar{\mathbf{x}}_2, \bar{z}^*)) \;=\; \mathbf{v}_1.$$

Therefore $\mathbf{x}_1, \mathbf{v}_1$ have zero conditional statistical distance. By Lemma 4 we conclude

$$\Delta((\mathbf{x}_1, \mathbf{x}_2, z^*), (\mathbf{v}_1, \mathbf{v}_2, w^*)) \;\leq\; \Delta((\mathbf{x}_2, z^*), (\mathbf{v}_2, w^*)) \;\leq\; \varepsilon_1(\lambda). \qquad \square$$

Proof of Claim 18. Recall that by construction $\widehat{\mathbf{x}}_1$ is uniformly sampled in $\mathbb{F}_2^{n_1}$, and in particular $\Delta(\widehat{\mathbf{x}}_1, \widehat{\mathbf{v}}_1) = 0$. Next, conditioning on $\widehat{\mathbf{x}}_1 = \bar{\mathbf{x}}_1 = \widehat{\mathbf{v}}_1$ for all $\bar{\mathbf{x}}_1 \in \mathbb{F}_2^{n_1}$, we study the distance of $(\widehat{\mathbf{x}}_2, \widehat{z}^*)$ and $(\widehat{\mathbf{v}}_2, \widehat{w}^*)$. Recall $(\widehat{\mathbf{x}}_2, \widehat{z})$ in $\mathsf{S.Sign2}$ is the output of

$$\mathsf{PreSamp}([A_1^{(m)}\mathbf{x}_1], [\mathbf{u}^{(m)}], \mathbf{a}_2, M^{(m)}, \Omega, B, \mathbf{t} \oplus \mathbf{x}_1, d, \mathsf{dp})\,.$$

[25] Note the probability is taken only over $\mathbf{x}, z^*$ and $\mathbf{s}$ as all other variables are fixed by our conditions.

[26] Note that if X and Y are two random variables and bad is an event such that $\Delta(X|_{\neg\mathsf{bad}}, Y|_{\neg\mathsf{bad}}) = 0$, then $\Delta(X, Y) \leq \Pr[\mathsf{bad}]$.

Call bad the event $(\widehat{\mathbf{x}}_2, \widehat{z}) = \perp$. Then by Theorem 7 $\Pr[\mathsf{bad} \,|\, \widehat{\mathbf{x}}_1 = \bar{\mathbf{x}}_1] \leq \varepsilon_2(\lambda)$, which we can apply because:

- $k = k_0 \in \mathcal{K}_2^*$;
- $A_1^{(m)} \bar{\mathbf{x}}_1 = \alpha^{(m)} \cdot \mathbf{a}_1^\top \bar{\mathbf{x}}_1 \cdot \mathbf{u}$ is parallel to $\mathbf{u}$;
- $\mathbf{u}^{(m)} = \alpha^{(m)} \mathbf{u}$ is parallel to $\mathbf{u}$ and non-zero due to our assumption (see the proof of Claim 15);
- $M^{(m)} = P_{y \oplus h(m)} \mod 2$ is full rank in $\mathbb{F}_2^{n_2, n_2}$ since $y \neq h(m)$, and $B \in \mathbb{F}_2^{n_1, n_2}$ is full rank.
- $\left\| M^{(m)} \right\|_\infty \leq \|M_0\|_\infty + \sum_{i=1}^{\mu} \|m_i M_i\|_\infty \leq (\mu + 1) n_2 \leq d$.

Next, by Theorem 8 we have $(\widehat{\mathbf{x}}_2, \widehat{z})_{|\neg \mathsf{bad}}$ is uniform over

$$\left\{ (\mathbf{x}_0, z_0) \in \mathbb{F}_2^{n_2} \times \mathbb{F}_q \;\middle|\; \begin{array}{l} \delta_{\mathsf{min}}([A_1^{(m)} \bar{\mathbf{x}}_1 + A_2^{(m)} \mathbf{x}_0 + z_0 \mathbf{u}^{(m)}]) \geq d \\ B \delta_2([A_1^{(m)} \bar{\mathbf{x}}_1 + A_2^{(m)} \mathbf{x}_0 + z_0 \mathbf{u}^{(m)}]) = \mathbf{t} \oplus \bar{\mathbf{x}}_1 \end{array} \right\}$$

Hence $(\widehat{\mathbf{x}}_2, \widehat{z}^*)_{|\neg \mathsf{bad}}$, where we recall $\widehat{z}^* = \widehat{z} + \mathbf{a}_1^\top \bar{\mathbf{x}}_1$, is uniform over

$$\left\{ (\mathbf{x}_0, z_0^*) \in \mathbb{F}_2^{n_2} \times \mathbb{F}_q \;\middle|\; \begin{array}{l} \delta_{\mathsf{min}}([A_2^{(m)} \mathbf{x}_0 + z_0^* \mathbf{u}^{(m)}]) \geq d \\ B \delta_2([A_2^{(m)} \mathbf{x}_0 + z_0^* \mathbf{u}^{(m)}]) = \mathbf{t} \oplus \bar{\mathbf{x}}_1 \end{array} \right\}.$$

Note the first condition is equivalent to $(\mathbf{x}_0, z_0^*) \in \mathcal{U}_m^*$, while the second is equivalent to $f_2(\mathbf{x}_0, z_0^*) = f_1(\bar{\mathbf{x}}_1)$. Hence $(\widehat{\mathbf{x}}_2, \widehat{z}^*)_{|\neg \mathsf{bad}}$ conditioned to $\widehat{\mathbf{x}}_1 = \bar{\mathbf{x}}_1$ is uniform over $f_2^{-1}(f_1(\bar{\mathbf{x}}_1))$, and in particular

$$\Delta((\widehat{\mathbf{x}}_2, \widehat{z}^*)_{|\widehat{\mathbf{x}}_1 = \bar{\mathbf{x}}_1}, (\widehat{\mathbf{v}}_2, \widehat{w}^*)_{|\widehat{\mathbf{v}}_1 = \bar{\mathbf{x}}_1}) \leq \Pr[\mathsf{bad} | \widehat{\mathbf{x}}_1 = \bar{\mathbf{x}}_1] \leq \varepsilon_2(\lambda).$$

By Lemma 4 we conclude $\Delta((\widehat{\mathbf{x}}_1, \widehat{\mathbf{x}}_2, \widehat{z}^*), (\widehat{\mathbf{v}}_1, \widehat{\mathbf{v}}_2, \widehat{w}^*)) \leq$

$$\leq \Delta(\widehat{\mathbf{x}}_1, \widehat{\mathbf{v}}_1) + \sum\nolimits_{\bar{\mathbf{x}}_1 \in \mathbb{F}_2^{n_1}} \Pr[\widehat{\mathbf{v}}_1 = \bar{\mathbf{x}}] \cdot \Delta((\widehat{\mathbf{x}}_2, \widehat{z}^*)_{|\widehat{\mathbf{x}}_1 = \bar{\mathbf{x}}_1}, (\widehat{\mathbf{v}}_2, \widehat{w}^*)_{|\widehat{\mathbf{v}}_1 = \bar{\mathbf{x}}_1}) \leq \varepsilon_2(\lambda).$$

which concludes the proof. □